



e-proceedings

Editors: Michele Mosca
Gaby Lenhart
Mark Pecen



Partner:



Sponsor:



Supporters::



**2nd Quantum-Safe-Crypto
Workshop**

Ottawa, Canada, 6-7 October 2014

Preface

The 2nd ETSI Workshop on Quantum-Safe Cryptography, in partnership with the Institute for Quantum Computing (IQC), was held in Ottawa on 6th – 7th October, 2014.

Building upon the momentum of the 1st ETSI workshop held in September 2013, this workshop brought together a growing community of colleagues from industry, government and academic sectors to continue to develop a road-map to quantum-proofing our cybersecurity infrastructure.

The advent of full-fledged scalable quantum computers is a threat to many of our cyber systems. Although much work remains to be done, there is hope for not only the security of our data secured in an era with quantum computers, but also for forward-security of data encrypted today. Two main approaches for quantum-safe cryptography are:

- basing cryptography upon mathematical tools assumed to be hard
- basing cryptography on the laws of physics.

Society must rise now to the challenge of creating quantum-safe cryptography, so that the advent of large-scale quantum computing will be an entirely positive development in human history.

The workshop participants brought many helpful insights and suggestions to the group. For example, in order to help drive short term interest in adopting quantum-safe tools, Burt Kaliski emphasized the benefits of finding and highlighting short-term benefits through added features and functionality beyond “merely” being quantum-safe. Such incentives are especially important in the absence of a mandate to make systems quantum-safe.

Furthermore, we need to look not just at cryptographic algorithms, but also the bigger picture of whether our current infrastructure can handle quantum-safe cryptography. Consequently, we need to think about not only the standards on cryptography itself, but also:

- standards for practical application of quantum-safe cryptosystems
- a systems-level analysis of how to integrate primitives, protocols, etc. to create a quantum-safe environment.

In parallel to driving interest in adopting-quantum safe solutions, much work remains to be done in terms of aggressive review and cryptanalysis of quantum-safe cryptographic primitives, in order to boost confidence in their readiness for practical wide-scale deployment.

For “post-quantum” conventional cryptography tools, cryptography challenges are an important part of encouraging such aggressive analysis of these systems by researchers. Historical precedents include the NIST SHA candidate contest, for example. Quantum technologies are maturing (e.g. several long-distance trusted quantum networks are in development), and a new focus for QKD technologies is to have these technologies battle-tested and certified, in particular against attacks on the physical assumptions underlying the security of QKD. In the short term, the strategy is to adapt the technology to meet the currently available certifications. The longer-term strategy is to develop standards and certifications specifically for quantum technologies. Quantum random number generators are also developing in maturity, and serve very important applications.

In summary, people are working on many fields of quantum-safe cryptography, including some very novel approaches. We can take advantage of the momentum generated by this event to move toward standardization. One next step towards a standardized, quantum-safe suite of tools discussed was setting up a Quantum-Safe Cryptography Industry Specification Group (ISG) within ETSI in addition to the already since 2008 operating ETSI ISG on QKD.

An ISG covers both pre-standardization activities (problem identification and the generation of suggestions for possible solutions of improvements) as well as the standardization process. This work can also be leveraged by other standards organizations, who may cite and use it within their standards.

The new ISG on QSC is taking a proactive approach to define the standards that will secure our information in the face of technological advance. Quantum-safe cryptography and security is essential for:

- Protecting government and military communications
- Securing financial and banking transactions
- Assuring the confidentiality of medical data and healthcare records

- Safeguarding the storage of personal data in the cloud
- Restricting access to confidential corporate networks

The ETSI Quantum Safe Cryptography (QSC) ISG aims to assess and make recommendations for quantum-safe cryptographic primitives and protocols, taking into consideration both the current state of academic cryptology and quantum algorithm research, as well as industrial requirements for real-world deployment. ETSI-QSC ISG seeks to standardise the relevant algorithms, primitives, and risk management practices as needed to seamlessly preserve our global information security infrastructure.

The group will consider the security properties of the proposed algorithms and protocols along with practical considerations, such as extensible security architectures and technology switching costs, which will allow these recommendations to support a variety of industrial use cases. We aim to make pragmatic comparisons and concrete characterisations and recommendations to assist the global technology community to select and deploy the best available quantum-safe alternatives.

ETSI Quantum-Safe Cryptography 2014 Program Committee

We had the great honor and pleasure of being joined by the following people on our Program Committee:

- **Johannes Buchmann**, Prof. of Informatics and Mathematics at TU Darmstadt
- **Matthew Campagna**
- Donna Dodson, Deputy Chief Cybersecurity Advisor & Division Chief for Computer Security Division at NIST
- **Nicolas Gisin**, University of Geneva
- **Gaby Lenhart**, Senior Research Officer at ETSI
- **Michele Mosca**, Deputy Director at IQC, University of Waterloo
- **Mark Pecan**, Approach Infinity, Inc.
- **Bart Preneel**, Past-President of IACR
- **Masahide Sasaki**, Director Quantum ICT Laboratory at NICT
- **Andrew Shields**, Chairman of ETSI QKD, Toshiba
- **Colin Whorlow**, Head of International Standards, CESG

whom we would like to thank for accepting the difficult challenge of selecting the topics to be presented from a vast number of submissions. All these submissions were of very high quality therefore the only selection-criterion we were able to apply was their relevance for the given sub-topics from the call for presentations.

Editors:

Michele Mosca, University of Waterloo

Gaby Lenhart, ETSI

Mark Pecan, Approach Infinity



Agenda

Clicking on presentations titles links to corresponding paper and/or slides

SESSION 1: SETTING THE SCENE

Session chair: Gaby Lenhart, ETSI

Welcome

Luis Jorge Romero, ETSI Director-General

Michele Mosca, Institute for Quantum Computing, University of Waterloo

KEYNOTE Speech 1

Corinne Charette, Chief Information Officer of the Government of Canada

KEYNOTE Speech 2: Quantum Information Processing

Nicolas Gisin, University of Geneva

KEYNOTE Speech 3: The next 20 years of public-key cryptography

Bart Preneel, KU Leuven

KEYNOTE Speech 4: Quantum Safe Cryptography - Perspectives

Johannes Buchmann, TU Darmstadt

SESSION 2: SETTING THE SCENE

Session Chair: Bob Crow, IQC

KEYNOTE Speech 5: Why Quantum technologies do matter for Europe

Stephan Lechner, DG Joint Research Centre

KEYNOTE Speech 6: R&BD strategy for Quantum Information and Communication

Sean Kwak, SKT obo Steven Rim, MSIP

KEYNOTE Speech 7: QKD applications and new physical layer cryptography

Masahide Sasaki, NICT

KEYNOTE Speech 8: Quantum-safe cryptography and security

An Introduction, Benefits, Enablers and Challenges – white paper summary

Mark Pecan, Approach Infinity, Inc.

SESSION 3: DEPLOYMENT

Session Chair: Donna Dodson

Rethinking the Adoption of Hash Signatures

Burt Kaliski, Verisign

Neither do people pour new wine into old wineskins

Lily Chen, NIST

Agenda

Clicking on presentations titles links to corresponding paper and/or slides

Towards A Standard for Practical Hash-based Signatures

Andreas Hülsing, Technische Universiteit Eindhoven

PQTor: Integrating quantum-safe cryptography into Tor

William Whyte, Security Innovation

Questions and Answers

Panel Discussion

SESSION 4: STANDARDIZATION AND CERTIFICATION

Session Chair: Matthew Campagna

Traceable characterisation of the optical components of faint-pulse QKD systems – results from the Metrology for Industrial Communications (MIQC) project

Christopher Chunnillall, National Physical Laboratory (UK)

Multivariate Quadratic Challenge

Takanori Yasuda, ISIT

ETSI's role in the deployment of Quantum Key Distribution

Andrew Shields, Toshiba

Questions and Answers

Panel Discussion

SESSION 5: INDUSTRY

Session Chair: Nicolas Gisin, University of Geneva

A Certifiable QKD Relay Node Network

Nino Walenta, Battelle

Quantum Random Number Generator

Grégoire Ribordy, IDQ

Efficient Quantum-Immune Keyless Signatures with Identity

Risto Laanoja, Guardtime AS

Demonstration of quantum cryptography system for keyless authentication of machine-to-machine communications

Duncan Earl, Qubitekk Inc.

Questions and Answers

Panel Discussion

Agenda

Clicking on presentations titles links to corresponding paper and/or slides

SESSION 6: SYSTEMS AND ATTACKS

Session Chair: Norbert Luetkenhaus

Testing Quantum Crypto

Vadim Makarov, Institute for Quantum Computing, University of Waterloo

Codes for security against computationally unbounded adversaries

Rei Safavi-Naini, University of Calgary

Questions and Answers

Panel Discussion

SESSION 7: SYSTEMS AND ATTACKS, continued

Session Chair: Colin Whorlow, CESG

SOLILOQUY: A Cautionary Tale

Michael Groves, CESG, UK

The topology of quantum information flow

Jamie Vicary, Oxford University

An efficient and provably secure authenticated key exchange with forward security from RLWE

Jintai Ding, University of Cincinnati

SESSION 8: CONFERENCE CONCLUSIONS

Session Chair: Michele Mosca, Institute for Quantum Computing, University of Waterloo

Summary of each session by session chair + general event conclusion

Michele Mosca, IQC

Speakers

SESSION 1 SETTING THE SCENE



Gaby Lenhart, ETSI

born 1964. 1983 - 87 study of electrical engineering with emphasis on communications electronics at the Technical University Vienna in parallel study of English and Russian as translator at the University Vienna 2001 - 04 study of ICSS (Intelligent Communication Systems and Services) at the Technikum Vienna. Project Leader in the division 'Network Building & Infrastructure at Max-Mobil Austria (now T-Mobile Austria) 2002 - 2005 Standardization Expert in the division „International Standardization at T-Mobile International; Head of Delegation, Chairman of OMA POC. 2005 - 2007 Project Leader for Smart Cards and Project Leader for eHealth at ETSI. Gaby is member of various Boards, such as the Steering Committee of the Future Internet Assembly and the Advisory Board of Net!works. Currently she is Senior Research Officer at the Strategy & New Initiatives department at ETSI and, besides foresight, responsible for all aspects of quantum technologies.

Welcome

Luis Jorge Romero Saro, ETSI



Luis Jorge Romero, Director-General of ETSI has over 20 years international experience in the telecommunications sector. Previously he has held diverse Director positions in Spain, Morocco and Mexico, predominantly with Telefonica. As Global Director for International Roaming and Standards, and Director of Innovation and Standards, he oversaw Telefonica's participation in global standardization activities, and participated directly in the work of the Next Generation Mobile Networks (NGMN) Alliance and in the GSM Association (GSMA). Before joining ETSI in July 2011, he held the position of Director General of Innosoft and was also a partner and board member of Madrid-based Innology Ventures.

Michele Mosca, Institute for Quantum Computing at the University of Waterloo



Michele Mosca (DPhil, Oxford) is co-founder and Deputy Director of the Institute for Quantum Computing at the University of Waterloo, and a founding member of the Perimeter Institute for Theoretical Physics. He is co-founder and director of the NSERC CREATE Training Program in Building a Workforce for the Cryptographic Infrastructure of the 21st Century (CryptoWorks21.com). His current research interests include quantum algorithms and complexity, and the development of cryptographic tools that will be safe against quantum technologies. Awards and honours include the 2010 Canada's

Top 40 Under 40 award, Canada Research Chair in Quantum Computation (2002-2012), Fellow of the Canadian Institute for Advanced Research (2010-present), University Research Chair (2012-present), and Queen Elizabeth II Diamond Jubilee Medal (2013).

Keynote Speech 1

Corinne Charette, Chief Information Officer of the Government of Canada



Corinne Charette was appointed to the position of Chief Information Officer of the Government of Canada, effective May 4, 2009. Corinne comes to Treasury Board Secretariat from Transat A.T. Inc. where she was Vice-President and CIO since May 2006. Previously, Ms. Charette was Deputy Director and Chief Information Officer of FINTRAC. During her 30+ year professional career, she served as Senior Vice-President, Internet Channel, for the Canadian Imperial Bank of Commerce, has been a Partner with KPMG Consulting leading their e-Business practice and has worked for IBM Global Services. Corinne holds a Bachelor of Science degree in engineering from Concordia University and is a Professional Engineer. On

June 21, 2011, Corinne received an honorary degree of Doctor of Laws from Concordia University, in recognition of her distinguished career and achievements. As the Chief Information Officer for the Government of Canada, Ms. Charette is responsible for leading policy development and enablement, management oversight and community capacity development for six policy areas: information management, information technology, identity management and security, access to information, privacy, and internal and external services. CIOB leads the development of strategy and provides direction and leadership to federal departments and agencies for the government-wide pursuit of excellence in these policy domains. CIOB also collaborates actively with other Canadian and international jurisdictions on the development of best practices and on cross-jurisdictional initiatives.

Keynote Speech 2: Quantum Information Processing



Nicolas Gisin, University of Geneva

Prof. Nicolas Gisin was born in Geneva, Switzerland, in 1952. He received his Ph.D. degree in theoretical physics from the University of Geneva in 1981. After a post-doc at the University of Rochester, NY, and four years in industry, he joined the Group of Applied Physics at the University of Geneva where he has led the optics section since 1988. His activities range from the foundations of quantum physics to applications in quantum communications. In 2009 he was the first awardee of the John Stewart Bell prize.

Keynote Speech 3: The next 20 years of public-key cryptography



Bart Preneel, KU Leuven

Prof. Bart Preneel is a full professor at the KU Leuven; he heads the COSIC research group, that is a member of the iMinds Security Department. He was visiting professor at five universities in Europe. He has authored more than 400 scientific publications and is inventor of 4 patents. His main research interests are cryptography, information security and privacy. Bart Preneel has coordinated the Network of Excellence ECRYPT, has served as panel member and chair for the European Research Council and has been president of the IACR (International Association for Cryptologic Research). He is a member of the Permanent Stakeholders group of ENISA (European Network and Information Security Agency) and of the Academia Europaea. He has been invited speaker at more than 90 conferences in 40 countries. In 2014 he received the RSA Award for Excellence in the Field of Mathematics.

Keynote Speech 4: Quantum Safe cryptography - Perspectives



Johannes Buchmann, TU Darmstadt

Johannes Buchmann received a PhD from the Universität zu Köln, Germany in 1982. 1985 and 1986 he was a PostDoc at the Ohio State University on a Fellowship of the Alexander von Humboldt Foundation. From 1988 to 1996 he was a professor of Computer Science at the Universität des Saarlandes in Saarbrücken. Since 1996 he is a professor of Computer Science and Mathematics at Technische Universität Darmstadt. From 2001 to 2007 he was Vice President Research of TU Darmstadt. In 1993 he received the Leibniz-Prize of the German Science Foundation and in 2012 the Tsugming Tu Award of Taiwan. He is a member of the German Academy of Science and Engineering acatech and of the German Academy of Science Leopoldina.

Speakers

SESSION 2
SETTING THE SCENE, continued**Bob Crow, IQC**

Robert E. (Bob) Crow is an experienced public policy and technology industry leader, currently serving as Interim Vice President, University Relations at the University of Waterloo. Bob continues in his role as Executive in Residence, Institute for Quantum Computing. Bob's career includes lengthy service in the private, NGO, and university sectors as an executive, consultant, and teacher. He is especially known as a strategic thinker and builder of organizational capacity in settings where technology and public policy intersect. A frequent speaker, Bob is an informed and articulate advocate for his organizations and their missions. Bob is the former Vice President for Industry, Government and University Relations at Research In Motion Limited, where he built and led RIM's global programs in government relations, community relations, corporate responsibility, market intelligence and university research. Bob's teams supported RIM's rapid international expansion from 2001 – 2011 and were especially noted for their ability to create and defend access to foreign markets, often under challenging circumstances. Prior to joining RIM in July 2001, Bob was Vice President Policy at the Information Technology Association of Canada (ITAC) where he successfully positioned ITAC as a business association of credibility and influence in the Canadian policy milieu. Prior to this, he served from 1975 – 1998 at Ryerson University in Toronto as both professor of planning and senior administrator in a wide variety of roles including ICT strategy development, establishment of a technology centre, and leader of Ryerson's advancement activities. Bob holds a bachelor's degree in engineering from Cornell University and master's degrees in planning and economics from the University of North Carolina at Chapel Hill and the University of Toronto, respectively. He also studied engineering and public policy at Carnegie Mellon University at the advanced graduate level.

Keynote Speech 5: Why Quantum technologies do matter for Europe?**Stephan Lechner, DG joint Research Centre**

Dr Lechner is the Director of the Institute for the Protection and the Security of the Citizen (IPSC) at the European Commission's Joint Research Centre (JRC). The IPSC is located in Ispra, Italy and employs over 300 researchers on technical and scientific security aspects of various sectors (buildings, networks, financial systems, society) crisis management, maritime security and new Information Technology. Dr Lechner's background is in mathematics and computer sciences and he holds a PhD in cryptography. Before joining the European Commission, Dr Lechner used to be Global Department Head for Security Research at Siemens Corporate Research from 2002 to 2007. He worked as head of Corporate Security and as IT Security in the telecommunications sector in Germany from 1993 to 2002 and started his professional career as network security researcher at Siemens in 1989. Dr Lechner was member of the European Security Research advisory Board (ESRAB) and Member of the Permanent Stakeholders' Group of the European Network and Information Security Agency ENISA. He was also chairman of the Secure IST Advisory Board for the respective co-ordination action in Framework Programme 6. Dr Lechner used to work in European Standardisation in ETSI and ECMA and holds an active CISSP (Certified Information Systems Security Professional) qualification.

Keynote Speech 6: R&BD strategy for Quantum Information and Communication**Sean Kwak, SKT obo Steven Rim, MSIP**

Sean Kwak leads Quantum Tech. Lab at SK Telecom, the largest South Korean telecom operator. He is also a member of the Korean government's Quantum Information and Communication Technology (QICT) Task Force. Since joining SKT in 1997, He had also managed commercialization of SMS, PDSN (Packet Data Serving Node), and IMS (IP Multimedia Subsystem) at SK Telecom since 1997. He was responsible for CDMA core network development and represented SKT in 3GPP2 developing CDMA global standards. While working on solutions for packet core security, he became acquainted with Quantum Cryptography and led the founding of Quantum Tech. Lab in 2011. The Lab has been developing QKD systems and Quantum Repeater and Computer based on Ion-trap. Sean holds a Master's degree in electronics engineering.

Keynote Speech 7: QKD applications and new physical layer cryptography**Masahide Sasaki, NICT,**

Masahide Sasaki received the B.S., M.S., and Ph.D. degrees in physics from Tohoku University, Sendai Japan, in 1986, 1988 and 1992, respectively. From 1992 to 1996, he worked on the development of Si devices in Nippon Kokan Company (presently JFE holdings), Kanagawa Japan. In 1996, He joined the Communications Research Laboratory, Ministry of Posts and Telecommunications (since 2004, National Institute of Information and Communications Technology, Ministry of Internal Affairs and Communications), Tokyo, Japan, working on quantum information and communications technology. He has published more than 200 papers in refereed journals, edited two books, and written three book chapters. Dr. Sasaki is currently a Director of Quantum ICT Laboratory, and serves as the Chair of Quantum ICT Forum, conducting the Project UQCC (Updating Quantum Cryptography and Communications). He is a member of Japanese Society of Physics, and the Institute of Electronics, Information and Communication Engineers of Japan.

Keynote Speech 8: Quantum-safe cryptography and security**An introduction, benefits, enablers and challenges - White paper summary****Mark Pecan, Approach Infinity, Inc.**

Mark Pecan serves as CEO of Approach Infinity, Inc., providing advisory services to firms requiring technology due diligence and management consulting in the areas of wireless communication and emerging technologies, rapidly growing technology companies and their venture capital funding partners. The firm comprises a network of senior executives and experts in the management of technology, innovation, research and development, marketing, sales, global standards, patents, technology entrepreneurship, and individuals with specific technical disciplines such as information theory, radio frequency systems, wireless system protocols, cryptography and others. Pecan retired as Sr. Vice President, Research and Advanced Technology and technology advisor to the CEO of BlackBerry, maker of wireless smart phones. He was responsible for the creation and management of BlackBerry's Advanced Technology Research Centre and a significant portion of BlackBerry's wireless patent portfolio. A past Distinguished Innovator and member of the Science Advisory Board at Motorola, Pecan also managed consultation work for clients in North America and Europe. Pecan invented a number of technologies that have later been adopted in global standards, including the Global System for Mobile Telecommunication (GSM), Universal Mobile Telecommunication System (UMTS), High-Speed Packet Access (HSPA+), Long-Term Evolution (LTE) for 4G wireless and others. Pecan serves as an advisor to several industry and academic organizations, and is a regular advisor to the Canadian government on wireless communication and research. He holds board positions on University of Waterloo Institute for Quantum Computing, École Polytechnique, Wilfred Laurier University School of Business, Quantum Works academic network for quantum information research, Canadian Digital Media Network, the Communication Research Centre (CRC) of Industry Canada and others. A veteran of the wireless industry, he is an author and editor of a number of text books in the area of wireless technology and holds more than 100 fundamental patents in areas of wireless communication, networking and computing, and is a graduate of the University of Pennsylvania, Wharton School of Business and the School of Engineering and Applied Sciences.

Speakers

SESSION 3
DEPLOYMENT**Donna Dodson**, Information Technology Laboratory, NIST

Donna Dodson is also the Division Chief of the Computer Security Division (CSD) and the Acting Executive Director of the National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST). Donna oversees the CSD cybersecurity research program to develop standards, guidelines, technology, tests and metrics for the protection of unclassified Federal information and systems.

Through partnerships with industry, Dodson also ensures NIST cybersecurity contributions help secure the Nation's sensitive information and systems. This includes establishing public-private collaborations for accelerating the widespread adoption of integrated cybersecurity tools and technologies. Dodson received one Department of Commerce Gold Medal and three NIST Bronze Medals. She was a recipient of a 2011 Federal 100 Award for her contributions to advancements in cybersecurity and included in the Top 10 Influential People in Government Information Security.

Rethinking the adoption of Hash Signatures**Burt Kaliski**, Verisign

Dr. Burt Kaliski Jr., senior vice president and chief technology officer, is responsible for developing the company's long-term technology vision. He is the leader of Verisign Labs, which focuses on applied research, university collaboration, industry thought leadership and intellectual property strategy. He also facilitates the technical community within Verisign. Prior to joining Verisign in 2011, Kaliski served as the founding director of the EMC Innovation Network, the global collaboration among EMC's research and advanced technology groups and its university partners. He joined EMC from RSA Security, where he served as vice president of research and chief scientist. Kaliski started his career at RSA in 1989, where as the founding scientist of RSA Laboratories, his contributions included the development of the Public-Key Cryptography Standards (PKCS), now widely deployed in internet security. Kaliski has held appointments as a guest professor at Wuhan University's College of Computer Science, and as a guest professor and member of the international advisory board of Peking University's School of Software and Microelectronics. He has also taught at Stanford University and Rochester Institute of Technology. Kaliski is a trustee emeritus of the Massachusetts Technology Leadership Council, and a member of the Institute of Electrical and Electronics Engineers (IEEE) Computer Society and Tau Beta Pi. Kaliski holds a Bachelor of Science in computer science and engineering, Master of Science in electrical engineering and computer science and doctorate in electrical engineering and computer science from the Massachusetts Institute of Technology, where his research focused on cryptography.

Neither do people pour new wine into old wineskins**Lily Chen**, NIST

Dr. Lily Chen is a mathematician and the acting group manager of cryptographic technology group in Computer Security Division, Information Technology Laboratory, NIST. Dr. Chen received her Ph.D in applied mathematics from Aarhus University, Denmark. Her research areas include cryptographic protocols, special featured digital signatures, security protocol design, network security, and security for wireless and mobility applications. Besides authoring research papers, Dr. Chen has edited and actively contributed to various industry standards in cryptography and security.

Towards a standards for Practical Hash-based Signatures



Andreas Hüsling, Technische Universiteit Eindhoven

Since December 2013 Andreas Huelsing is a postdoctoral researcher in the cryptographic implementations group at TU Eindhoven, working with Daniel J. Bernstein. Before that, Andreas did his PhD in the cryptography and computer algebra group at TU Darmstadt under the supervision of Johannes Buchmann. Andreas received his Diploma in computer science from TU Darmstadt in 2007. Before he came back to university in 2010 to do my PhD, he was a research fellow at Fraunhofer SIT in Darmstadt. His research focuses on digital signature schemes that can withstand quantum-computer aided attacks. Andreas is interested in the more theoretical topic of constructing digital signature schemes as well as in the applications of these schemes. So far, he spent most of his time working on so called hash-based signature schemes. On the more applied side, Andreas was working on improvements of current PKI solutions, especially in the context of long-term security. Andreas also got some side-projects on lattice-based cryptography and quantum cryptography. For more details see Andreas' publications and talks at <http://huelsing.wordpress.com/publications/>. During his time at Fraunhofer, Andreas mainly worked on projects concerned with the German eHealth infrastructure and the new German identity card. Besides, Andreas did some work on systematic security analysis and design of security policies for the "Internet of Things" as well as some penetration testing.

PQTor: Integrating quantum-safe cryptography into Tor



William Whyte, Security Innovation

William Whyte is Chief Scientist at Security Innovation, where he leads research and prototyping initiatives in Connected Vehicle and post-quantum cryptography. He was previously CTO at NTRU Cryptosystems, and Senior Cryptographer at Baltimore Technologies. With a focus on how standardization enables deployment of good technology, he has served in a leadership role in IEEE working groups and has served as technical editor of two IEEE standards and has contributed to standards in ETSI, ANSI X9, IEEE, and the IETF. He has a BA from Trinity College Dublin and a DPhil from Oxford University.

Matthew Campagna, University of Waterloo

Matthew Campagna is the Director of Certicom Research at BlackBerry. Matthew has conducted and managed research in cryptography and its standardization for BlackBerry, participating in ANSI, ZigBee, SECG, ETSI's SAGE, and the 3GPP-SA3 working group. Matthew has specialized in development of efficient implementation of cryptography and the development of new cryptographic primitives using elliptic curve cryptography suitable for emerging and embedded platforms. Prior to joining Certicom, Matthew managed the Secure Systems research group at Pitney Bowes. In addition to managing Matthew functioned as the company's lead cryptographic researcher. Matthew's focus was on developing, engineering and deploying efficient public key systems for low cost and low computing power devices communicating over restricted communication channels. Matthew worked for the United States' National Security Agency (NSA) as a senior cryptologic mathematician focused on symmetric key cryptologic design and commercial cryptography. He holds a Ph.D. in mathematics from Wesleyan University in group theory, and a bachelor's degree in mathematics and economics from Fordham University.

Traceable characterisation of the optical components of faint-pulse QKD systems – results from the Metrology for Industrial Communications (MIQC) project**Christopher Chunnillall, National Physical Laboratory (UK)**

Dr Christopher Chunnillall is a Senior Scientist at the National Physical Laboratory (NPL), the UK's National Measurement Institute. He received his Ph.D. in Physics from King's College London and has worked at NPL since 1995. His research interests are in the metrology of single photon sources and detectors; applying these to quantum-enhanced measurements; and developing measurements for testing and validating technologies based on the production, manipulation, and detection of single and entangled photons, e.g. quantum key distribution. He is a member of the European Telecommunications Standards Institute's Industry Specification Group on Quantum Key Distribution, and the Discussion Forum on Few-photon Metrology of the Consultative Committee for Photometry and Radiometry.

Multivariate Quadratic Challenge**Takanori Yasuda, ISIT**

Takanori Yasuda received the PhD. degrees in mathematics from Kyushu University in 2007. He was a postdoctoral fellow in Osaka City University from 2007 through 2008, in Kyushu University from 2008 through 2011. He is currently a researcher in Institute of Systems, Information Technologies and Nanotechnologies. His current research interests are pairing cryptography, multivariate public-key cryptosystem, and automorphic representations.

ETSI's role in the deployment of Quantum Key Distribution**Andrew Shields, Toshiba**

Andrew Shields is Assistant Managing Director at Toshiba Research Europe in Cambridge, UK, where he leads the Quantum Information Group. His research interests include Quantum Cryptography, Quantum Computing and Semiconductor Quantum Photonics. He is the current Chair of the ETSI ISG in Quantum Key Distribution.

Speakers

SESSION 5
INDUSTRY**Nicolas Gisin, University of Geneva**

Prof. Nicolas Gisin was born in Geneva, Switzerland, in 1952. He received his Ph.D. degree in theoretical physics from the University of Geneva in 1981. After a post-doc at the University of Rochester, NY, and four years in industry, he joined the Group of Applied Physics at the University of Geneva where he has led the optics section since 1988. His activities range from the foundations of quantum physics to applications in quantum communications. In 2009 he was the first awardee of the John Steward Bell prize.

A Certifiable QKD relay node network**Nino Walenta, Battelle**

Nino Walenta received the Diploma degree in physics from the University of Potsdam, Germany, and the Ph.D. degree in physics from the University of Geneva, Switzerland, in 2013. From 2007 to 2008, he was a research assistant at the University of Potsdam, and in 2013, he was a Postdoctoral researcher at the University of Geneva. He joined Battelle UK Ltd., Geneva, Switzerland in December 2013. At present, he is a Principle Research Scientist at Battelle Memorial Institute, Columbus, Ohio, USA. His research has been concerned with quantum optics and quantum communication, with focus on single photon detection and implementations for fiber based quantum key distribution devices. Dr. Nino Walenta is member of the German Physical Society (DPG).

Quantum Random Number Generator**Grégoire Ribordy, IDQ**

Mr. Ribordy has over 15 years of experience in various R&D and management roles in the field of photonics and quantum technologies. He co-founded ID Quantique in 2001 and has managed the company since then. Prior to this, he was a research fellow at the Group of Applied Physics of the University of Geneva from 1997-2001. In this position, he actively developed quantum cryptography technology. In 1995-1996, Mr. Ribordy worked for one year in the R&D division of Nikon Corp. in Tokyo. Mr. Ribordy is the recipient of several awards such as the 2001 New Entrepreneurs in Science and Technology prize, the 2002 de Vigier Award for Entrepreneurship and the Swiss Society for Optics and Microscopy 1999 prize.

Efficient Quantum-Immune Keyless Signatures with Identity**Risto Laanoja, Guardtime AS**

Risto Laanoja is Guardtime's Security Architect. Risto was part of the original engineering team, responsible for building trusted and standard-compliant security procedures and cryptographic schemes. He is a key member of Guardtime's Research & Development directorate. His field of expertise covers security infrastructure, internet protocols, trust services etc; delivering patents, academic articles, and working prototypes of innovative ideas. Risto's role spans across research, development, integration and operations. Before joining Guardtime Risto spent 10 years at SEB in data security management and infrastructure development positions. Back then, he was responsible for security and pioneering online-banking and national digital signature infrastructure applications. He has graduate and undergraduate level teaching experience. Risto is pursuing his PhD degree at Tallinn University of Technology, working on provable security of KSI and its applications.

**Demonstration of quantum cryptography system for keyless authentication of machine-to-machine communications****Duncan Earl, Qubitekk Inc.**

Dr. Duncan Earl is the founder and Chief Technology Officer for Qubitekk, Inc. Dr. Earl is a serial entrepreneur who has helped found and grow three startups over the past decade. He is also a former researcher with Oak Ridge National Laboratory, where he spent nearly 20 years researching quantum cryptography, quantum computing, meta-materials, and a variety of optical sensing technologies.

Speakers

SESSION 6
SYSTEMS AND ATTACKS**Norbert Luetkenhaus, University of Waterloo**

Norbert Lütkenhaus studied at the RWTH Aachen and the LMU Munich, from which he graduated with a thesis in general relativity. Then he changed the field to study quantum optics and quantum cryptography under the supervision of Stephen M. Barnett at the University of Strathclyde, Scotland, UK. In 1996 he obtained his PhD. After postdoc positions in Innsbruck (Peter Zoller and Ignacio Cirac) and the Helsinki Institute of Physics (Kalle-Antti Suominen) he worked for MagiQ Technologies (New York) to initiate the project of commercial realisation of quantum key distribution. Returning to academia in 2001, he build up and lead an Emmy-Noether Research Group at the University of Erlangen-Nürnberg, during which time he did his habilitation (2004). Currently he is an Associate Professor in the Physics Department at the University of Waterloo and a member of the Institute of Quantum Computing.

Testing QKD systems**Vadim Makarov, Institute for Quantum Computing, University of Waterloo**

Dr. Vadim Makarov is one of world leaders in the practical security of quantum key distribution (QKD) systems. He obtained his PhD in 2007 from the Norwegian University of Science and Technology in Trondheim; his work had uncovered several practical attack methods against QKD systems. Postdoctoral work in South Korea followed, and in 2008 he returned to Norway to establish and run a quantum hacking laboratory under supervision of Prof. Johannes Skaar. Dr. Makarov moved to Canada in 2012 to start his own research group with a focus on practical QKD security, and create an advanced laboratory for security analysis <http://www.vad1.com/lab/> Dr. Makarov has led international collaborations culminating in successful hacks of both commercial QKD systems on the market. He has demonstrated a full field implementation of an eavesdropper stealing the complete 'secret' key from a research prototype QKD system. Dr. Makarov's work includes responsible disclosure, for the first time providing QKD companies advance information on security weaknesses in their products. Security patches have been issued, and close cooperation developed with manufacturers.

Codes for security against computationally unbounded adversaries**Rei Safavi-Naini, University of Calgary**

Rei Safavi-Naini is the AITF Strategic Chair in Information Security and a Professor in the Department of Compute at the University of Calgary. Her research interests includes cryptography, information theoretic security and protocols and systems for providing security and privacy. <http://pages.cpsc.ucalgary.ca/~rei/>

Speakers

SESSION 7
SYSTEMS AND ATTACKS, continued**Colin Whorlow, CESG**

Colin Whorlow has worked in CESG, the UK National Technical Authority for Information Assurance, for 15 years. Now Head of International Standards he was formerly Head of International Relations where he led CESG's engagement on EU and NATO information assurance issues. Colin is a member of the Management Board of ENISA (European Network and Information Security Agency) and of the SOG-IS Management Committee. He has led workshops on the impact of Cybersecurity on Critical Information Infrastructure Protection as part of the Meridian Process and at the Budapest Conference on Cyberspace. Previously Head of Export Control Colin chaired the Information Security Technical Working Group at the Wassenaar Arrangement for some years. Colin's degree is in mathematics, which he read at Oxford University.

Soliloquy: a cautionary tale**Michael Groves, CESG, UK**

Michael Groves is a Technical Director for Cryptographic Research at CESG

The topology of quantum information flow**Jamie Vicary, Oxford University**

Jamie Vicary did an undergraduate degree in Physics at Mansfield College, Oxford, followed by the Part III mathematics course at DAMTP and Trinity Hall, Cambridge. Jamie then did a PhD in category theory and the foundations of quantum information with Chris Isham at Imperial College London, which he completed in 2008. Since then Jamie has had a postdoctoral research position in the Quantum Group in Oxford. Jamie also has an affiliation with the Centre for Quantum Technologies at the National University of Singapore, where he is a Research Fellow.

An efficient and provably secure authenticated key exchange with forward security from RLWE**Jintai Ding, University of Cincinnati**

Jintai Ding is a professor at the Department of Mathematical Sciences of the University of Cincinnati. He received his B.A. from Xian Jiaotong University in 1988, his M.A. in mathematics from the University of Science and Technology of China in 1990 and his Ph.D in mathematics from Yale in 1995. He was a lecturer at the Research Institute for Mathematical Sciences of Kyoto University from 1995 to 1998. He has been a faculty member at the University of Cincinnati since 1998. From 2006 to 2007, he was a visiting professor and Alexander Von Humboldt Fellow at Technical University of Darmstadt. From 2009 to 2012, he was a Distinguished Adjunct Professor at South China University of Technology. Since 2011, he has been an adjunct Professor at Chongqing University. He received the Zhong Jia Qing Prize from by the Chinese Mathematical Society in 1990. He was a Taft fellow at Taft Research Center in 2009-2010. His main research interests are in cryptography, computational algebra and information security. He holds patents in cryptographic algorithms in China and USA.



Summary of each session by session chair and general event conclusion

Michele Mosca, Institute for Quantum Computing at the University of Waterloo

Michele Mosca (DPhil, Oxford) is co-founder and Deputy Director of the Institute for Quantum Computing at the University of Waterloo, and a founding member of the Perimeter Institute for Theoretical Physics. He is co-founder and director of the NSERC CREATE Training Program in Building a Workforce for the Cryptographic Infrastructure of the 21st Century (CryptoWorks21.com). His current research interests include quantum algorithms and complexity, and the development of cryptographic tools that will be safe against quantum technologies. Awards and honours include the 2010 Canada's Top 40 Under 40 award, Canada Research Chair in Quantum Computation (2002-2012), Fellow of the Canadian Institute for Advanced Research (2010-present), University Research Chair (2012-present), and Queen Elizabeth II Diamond Jubilee Medal (2013).

KEYNOTE Speech 2

Nicolas Gisin, University of Geneva





Quantum Information Processing

Nicolas Gisin and Hugo Zbinden
GAP-Optique, University of Geneva

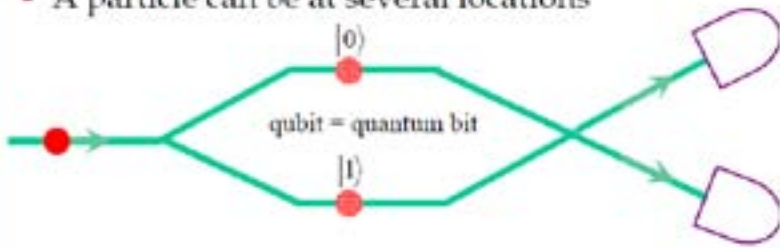
- Quantum Computing
- Quantum Key Distribution
- Quantum Random Number Generators

1



Quantum mechanics (all physics you need to know)

- A particle can be at several locations



qubit = quantum bit

- Likewise one can have $|0\rangle + |1\rangle + |2\rangle + |3\rangle + \dots + |n\rangle$
- 100 qubits can number all the particles there are in the entire universe !
- Upon a measurement one single result shows up

2



GAP Quantique

Computing

- **Process information: input $x \Rightarrow$ output $fct(x)$**
- **Quantum computer:**
quantum processing of classical information
input $|0\rangle + |1\rangle + |2\rangle + \dots + |n\rangle \Rightarrow |fct(0)\rangle + |fct(1)\rangle + |fct(2)\rangle + \dots + |fct(n)\rangle$
- **A measurement can provide only one result**
- **This single result can provide information about a global property of the function fct .**
- **For example, the maximum value, the mean value, or information about the periodicity of the function.**

3



GAP Quantique

Fact

- **Period of a function + a bit of number theory**
- **\Rightarrow break all of today's public key cryptographic**
- **i.e. allows one to decipher all encrypted messages**
- **Hence, a quantum computer will render today's public key cryptography obsolete**
- **RSA is finished**

4



What happens if RSA is gone?

- All electronic money loses instantaneously all value
- An enormous economic crisis, compared to which 2008 will look like a pleasant joke
- All encrypted messages can be deciphered retroactively
- Our information based society rests on an enormous bet: the bet that RSA will not be broken!


3



Our society rests on an enormous bet: the bet that RSA will not be broken!

- The bet is likely to be lost
- A mathematician could find an efficient algorithm to break RSA
- This could happen in a century or tomorrow
- Nobody knows when it will happen, but most specialist agree that it is likely to happen someday (though some disagree)
- Everybody agrees that a quantum computer will break RSA

4



When shall we have a quantum computer ?

- I bet in 10 years
- Note that 5 years ago I was betting on 20 years. Seems things are accelerating.
- My bet is based on the tremendous progress and investments in superconducting qubits

7



The Quantum computer is around the corner




Google has long been an advocate of quantum computing. It was one of the first

8



In 10 years Google, NSA, etc will know all our secrets


- All governmental, financial, industrial, health etc, secrets encoded with RSA will be readable.
- Not only future secrets, but also today's secrets.
- Indeed, all encrypted messages send today are registered and will be available in clear format.
- \Rightarrow if you want your secrets to hold for a decade, it is already too late.
- \Rightarrow you better change your crypto infrastructure as soon as possible.



How soon do we need to worry?

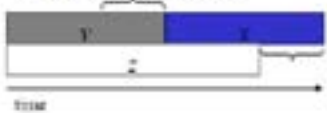
Depends on:

- How long do you need encryption to be secure? (x years)
- How much time will it take to re-tool the existing infrastructure with large-scale quantum-safe solution? (y years)
- How long will it take for a large-scale quantum computer to be built (or for any other relevant advance)? (z years)



Theorem 1: If $x + y > z$, then worry.

What do we do here??



Courtesy of Prof. Michele Mosca



There are only two alternatives

1. In 10 years I will be retired, hence do nothing.
2. **Act today.**

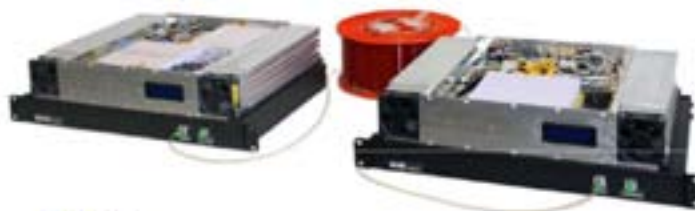
What to do ? \Rightarrow Quantum Safe Cryptography.

- Make a new bet, betting on a new problem believed to be hard.
- Exploit the gifts of nature and base future cryptography on quantum physics: Quantum Key Distribution (QKD).
The only solution proven to be robust against a quantum computer.

11



Integrated QKD system



Future:

- Integration into ATCA blades
- Standard telecom format

• N. Walenta et al., "A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing," *New J. Phys.* 10, 012047 (2014)

GAP Quantique

Secret key rates

Optimum detector temperature found for each fiber length

- Trade off between dark counts and afterpulsing

3.2 bits/s at 307 km

B. Kozth, C. W. Lim et al., "Provably Secure and Practical Quantum Key Distribution over 307 km of Optical Fibre," arXiv1407.7427 (2014)

GAP Quantique

Short distance, high rate QKD

Work by Toshiba:

- Decoy state BB84 protocol
- Self-differencing detectors
- Over 1 Mbps
 - Enough for video live video call encryption with One-Time Pad

M. Lucamarini et al. "Efficient decoy-state quantum key distribution with quantified security", Opt. Express 24551 (2013)
 L. C. Comandó et al. "Room-temperature single-photon detectors for high bit rate quantum key distribution", Appl. Phys. Lett. 104, 021101 (2014)
 N. Waksita et al. "Time gating detectors with simple filtering for low-loss intra-net single-photon detector at room temperature", J. Appl. Phys. 112, 063106 (2012)

Example of a commercial link running continuously since 2011

67 km
Installed multiplexed quantum channel for commercial users.

IDQ

37

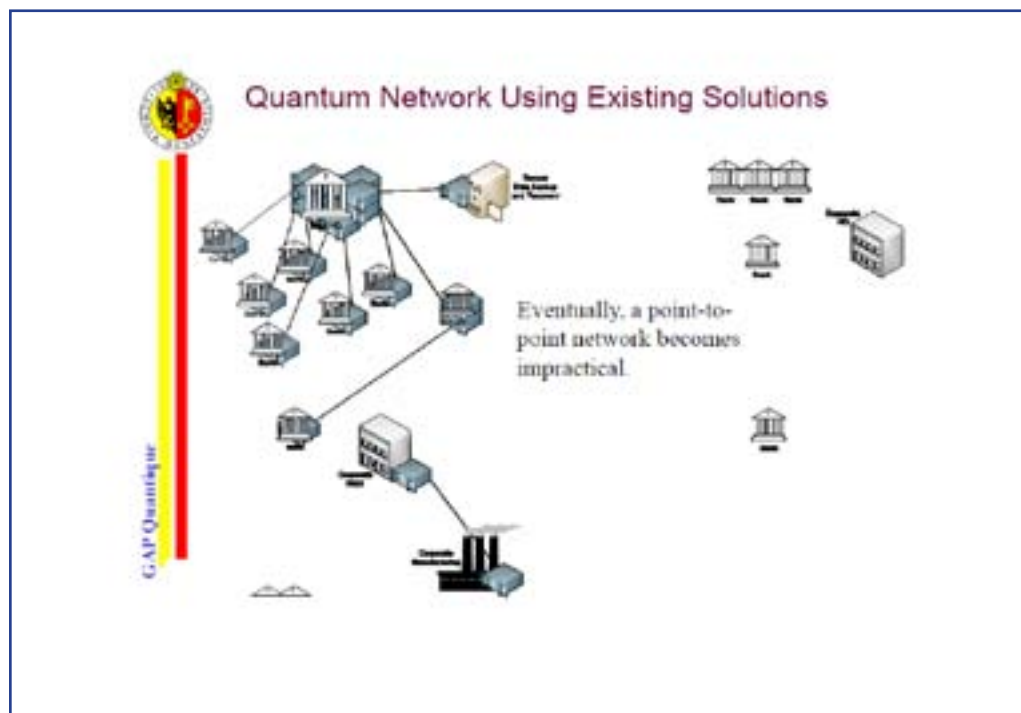
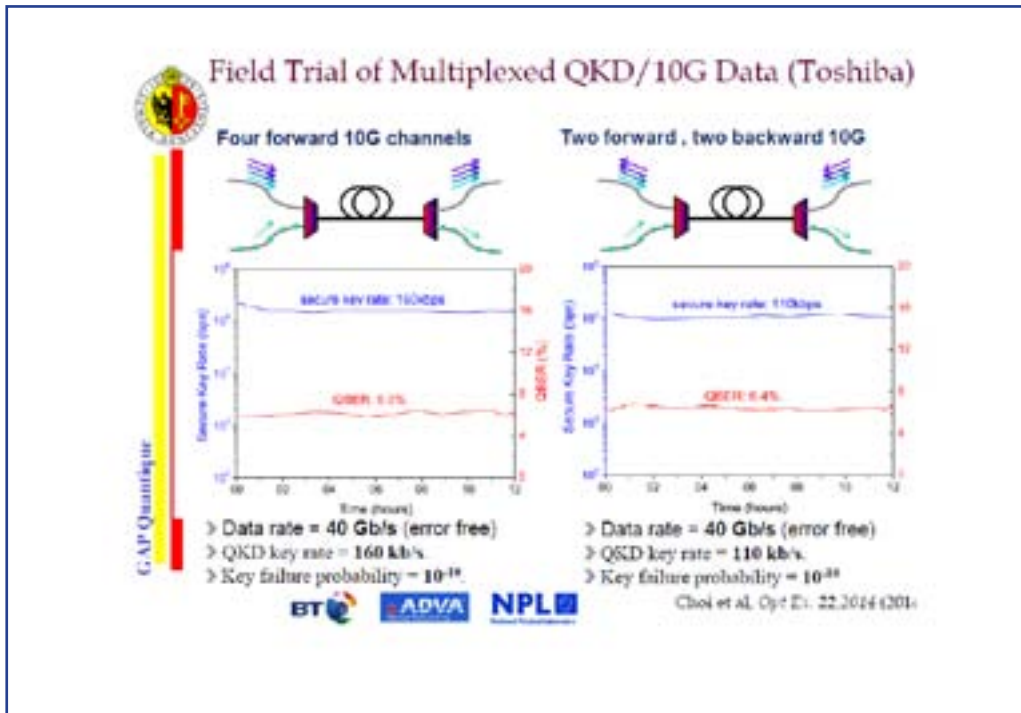
WDM: multiplex the Quantum and Classical = 10^9 times more intense !!!

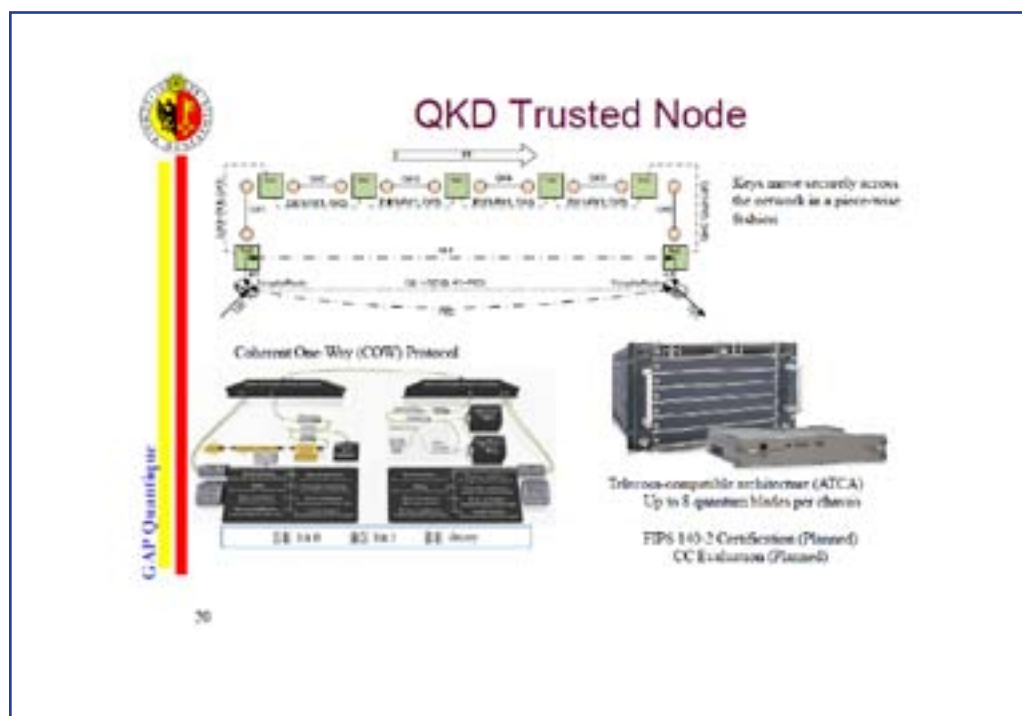
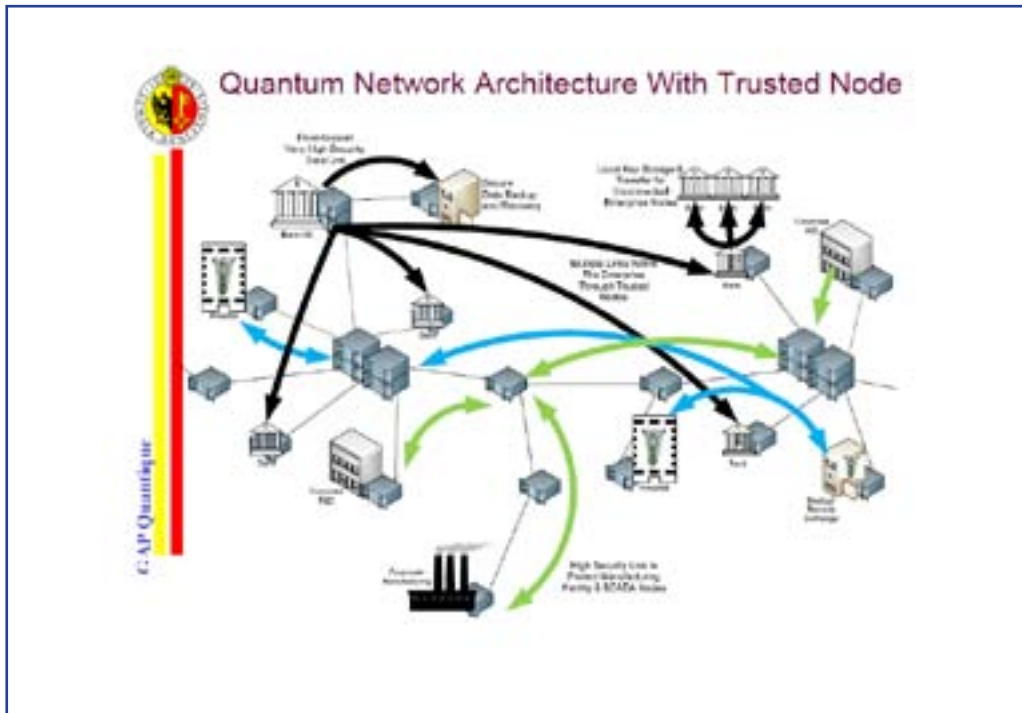
$QBER = QBER_{opt} + QBER_{det} + QBER_{noise/WDM}$

What are the noise sources?

- Crosstalk of other wavelengths into quantum channel
- Generation of parasitic light at the wavelength of the Q channel
 - by Raman scattering (dominant for lengths > 10 km)
 - by Four Wave Mixing (FWM)

38





Long Range QKD with trusted nodes



Battelle **CIDQ**
The Business of Innovation

Battelle Q&K Backbone
• Columbus OH to Washington DC Area
• > 770 km
• Deployment targeted in 2015



GAP Quantum

North American Quantum Network



Our goal – a network of nodes that can be used as the basis for secure network across North America (and the rest of the world!)

GAP Quantum

22

Korean government plan

[Quantum R&D Trusted Node - (22)]

- Daejeon - Suwon - Seoul

[National Administrative Network - (21)]

- Nationwide network

[Quantum Backbone - (17)]

- Seoul - Suwon - Daejeon - Suwon - Daejeon

Extend the number of nodes

Category	# of nodes	MS
Public Administration	141	National wide office
Provincial & Police Office	238	National wide office
Post Office	1342	National wide office

- Extend to defense and financial institute
 - Defense com. 518 nodes
 - Financial Institute 228 nodes (incl. branch)

Chinese Trusted Node Quantum Network

Based on trustable relay, setting up "Quantum Backbone"

The map shows a quantum network backbone connecting four major cities in China: Shanghai, Hefei, Jinan, and Beijing. The backbone is represented by a blue line with nodes at each city. The map also shows other cities like Nanjing and Hangzhou.

Chinese Trusted node Quantum network


- Total Length 2000 km
- 2013.6-2016.12
- 32 trustable relay nodes
- 31 fiber links
- Metropolitan networks
 - Existing: Hefei, Jinan
 - New: Beijing, Shanghai
- Total Investment: 560 M RMB. Half by NDRC, Half by Local government
- Customer: China Industrial & Commercial Bank; Xinhua News Agency; CBRC



GAP Quantum

Chinese Trusted node Quantum network





Mind your Random Number Generator!

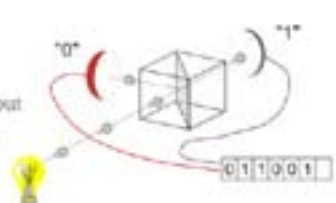
To appear in Proceedings of the 11th ETSI Security Symposium, August 2012, Initial public release, July 2, 2013. For the latest version of this paper, please contact us, and we will be happy to send you the latest version. email: Etsi@etsi.org

Mixing Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices


Nicolas Braspineux^{1*} John Dumas^{2*} Eric Wastner¹ J. Alex Halperin²
¹University of California, San Diego ²The University of Wisconsin
 nicolas@cs.ucsd.edu john@cs.wisc.edu wastner@cs.ucsd.edu alex@cs.wisc.edu

Advantages

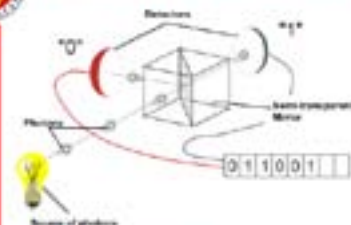


- Truly random process
 → produces truly random sequences
- Simple process that can be modelled
 → influence of environment can be ruled out
- Live monitoring of elementary components



27




Quantum Random Number Generator

4 Mb per second of balanced random bits

28



Evaluation and Certification




GAP Quantique

Non-Deterministic (Physical) RNG

- **PTG.1**
Physical RNG with internal tests that detect a total failure of the entropy source and non-tolerable statistical defects of the internal random numbers
- **PTG.2**
PTG.1, additionally a stochastic model of the entropy source and statistical tests of the raw random numbers
- **PTG.3**
PTG.2, additionally with cryptographic post-processing (hybrid PTRNG)








Conclusions




GAP Quantique

- ❑ Quantum Computer is already today a serious threat to standard cryptography.
- ❑ Not taking this fact seriously would lead to a devastating economical crisis.
- ❑ Solutions exist.
- ❑ Quantum Key Distribution is a possible solution.
- ❑ Today QKD is limited to point to point, but developments by several key players will soon make QKD networks with trusted nodes available.
- ❑ Trusted Random Number Generators is another urgent need.
- ❑ Quantum Random Number Generator is an existing solution.




Winter school 2015



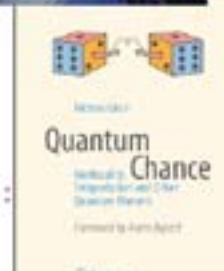
- 7th Winter school on practical quantum communications
- January 18th to January 22th 2015
- In Les Diablerets, Switzerland
- Keynote speakers
 - Whitfield Diffie
 - Nicolas Gisin
 - Dr. Colin P Williams, D-Wave,
 - Sandu Popescu
 - Eleni Diamanti
 - ...

Website:
www.idquantique.com/instrumentation/training

Contact: info@idquantique.com



Further reading :



GAP Quantique

21

Proposals for quantum communication in space

Dual-downlink (ROM R&D 47 M€)



Simultaneous optical downlink: 1400 km separation.

R. Usua et al., *European Phys. J. B*, 28, 25, 45-49 (2015)

Single-uplink (ROM R&D 1 M€)




Astronaut: A. Kuipers

Using a motorized photo-lens-pod (existing) and a dedicated quantum detector as "satellite".



T. Scheidl, E. Sillke, and R. Ursin, *New Journal of Physics*, 11, 043008 (2014)

Report Class@nasa.gov - Institute for Quantum Optics and Quantum Information, American Academy of Sciences



nature photonics

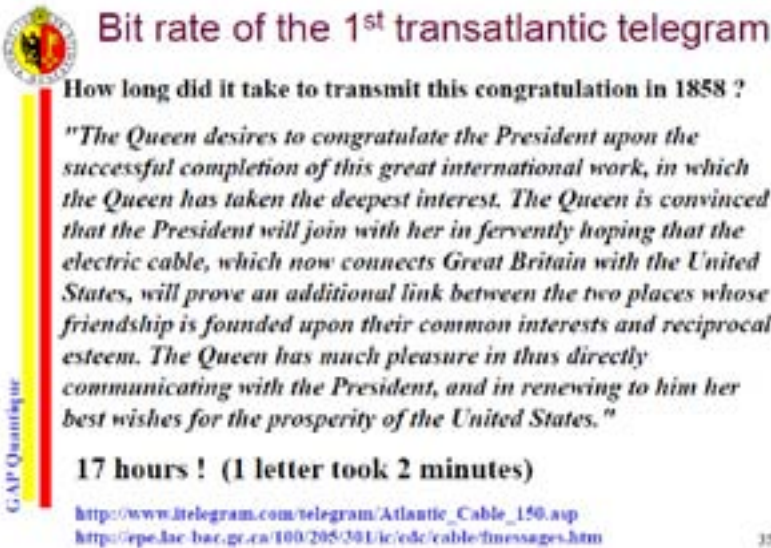
There is nothing like cracking QKD !

The principle of QKD will never be attacked, only the implementation may be faulty.

The implementation must be checked, as is the case for all hardware and all software.

August 29, 2010

The Norwegian University of Science and Technology (NTNU) and the University of Erlangen-Nürnberg together with the Max Planck Institute for the Science of Light in Erlangen have recently developed and tested a technique exploiting imperfections in quantum cryptography systems to implement an attack. Countermeasures were also implemented within an ongoing collaboration with leading manufacturer ID Quantique.



Bit rate of the 1st transatlantic telegram

How long did it take to transmit this congratulation in 1858 ?

"The Queen desires to congratulate the President upon the successful completion of this great international work, in which the Queen has taken the deepest interest. The Queen is convinced that the President will join with her in fervently hoping that the electric cable, which now connects Great Britain with the United States, will prove an additional link between the two places whose friendship is founded upon their common interests and reciprocal esteem. The Queen has much pleasure in thus directly communicating with the President, and in renewing to him her best wishes for the prosperity of the United States."

17 hours ! (1 letter took 2 minutes)

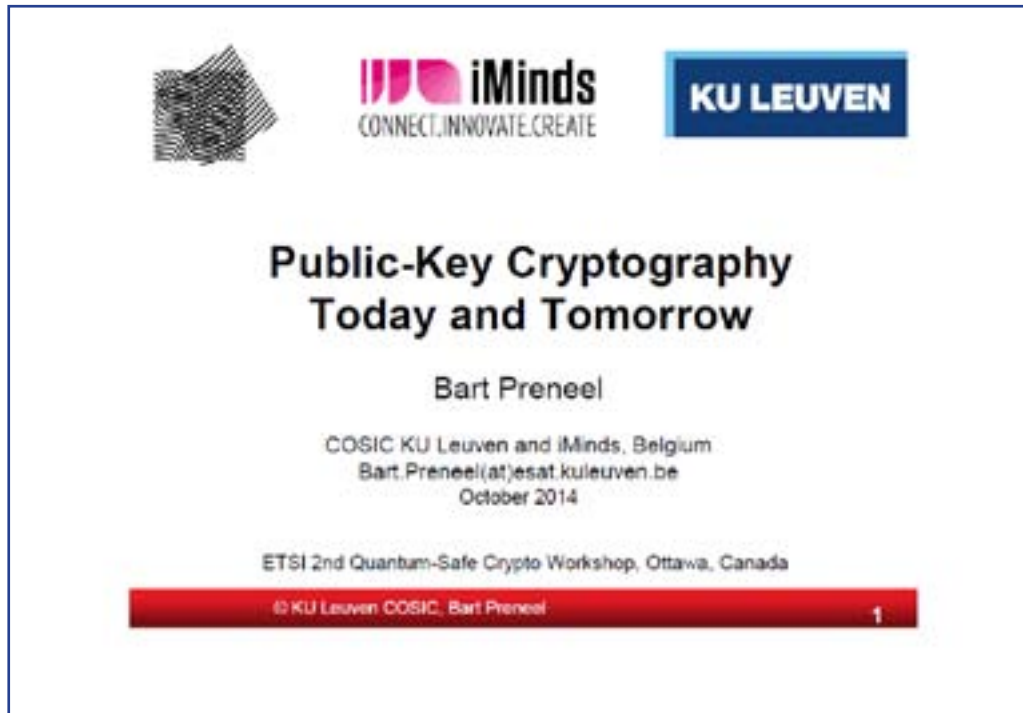
http://www.telegram.com/telegram/Atlantic_Cable_150.asp
<http://epe.lac-bac.gc.ca/100/205/301/icc/odc/cable/messages.htm>

GAP-Quantique

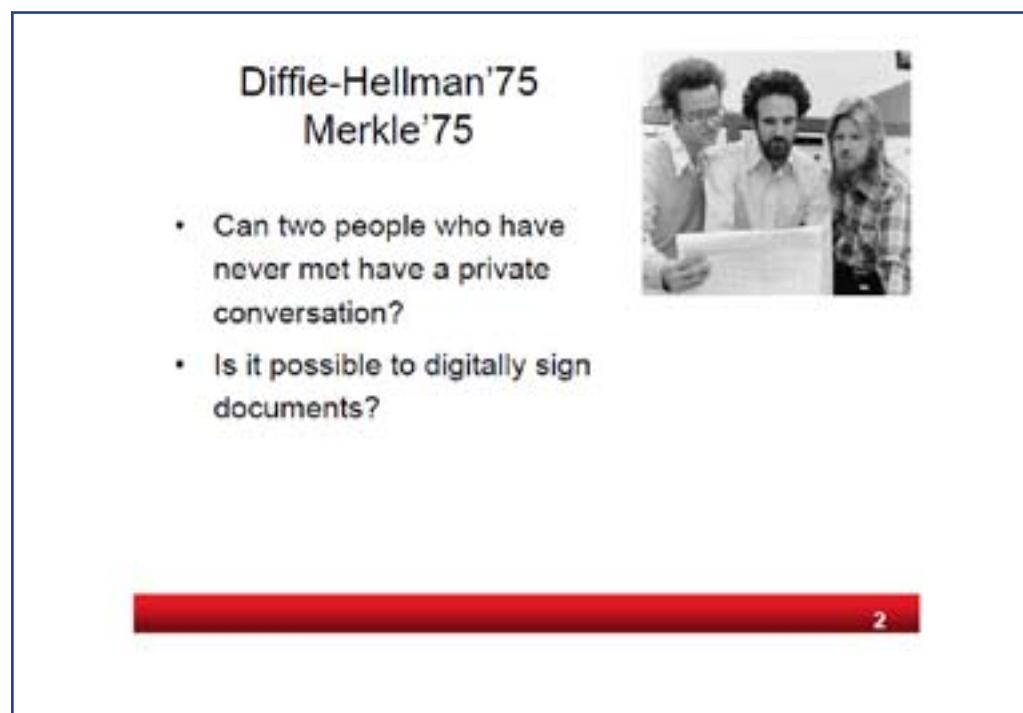
35

KEYNOTE Speech 3: The next 20 years of public-key cryptography

Bart Preneel, KU Leuven



The slide features logos for a grid pattern, iMinds (CONNECT, INNOVATE, CREATE), and KU LEUVEN. The title is "Public-Key Cryptography Today and Tomorrow" by Bart Preneel. It lists his affiliation as COSIC KU Leuven and iMinds, Belgium, with email Bart.Preneel(at)esat.kuleuven.be and the date October 2014. The event is the ETSI 2nd Quantum-Safe Crypto Workshop in Ottawa, Canada. A red footer bar contains the copyright notice "© KU Leuven COSIC, Bart Preneel" and the number "1".



The slide is titled "Diffie-Hellman '75" and "Merkle '75". It contains two bullet points: "Can two people who have never met have a private conversation?" and "Is it possible to digitally sign documents?". A black and white photograph of three people (two men and one woman) looking at a document is on the right. A red footer bar contains the number "2".

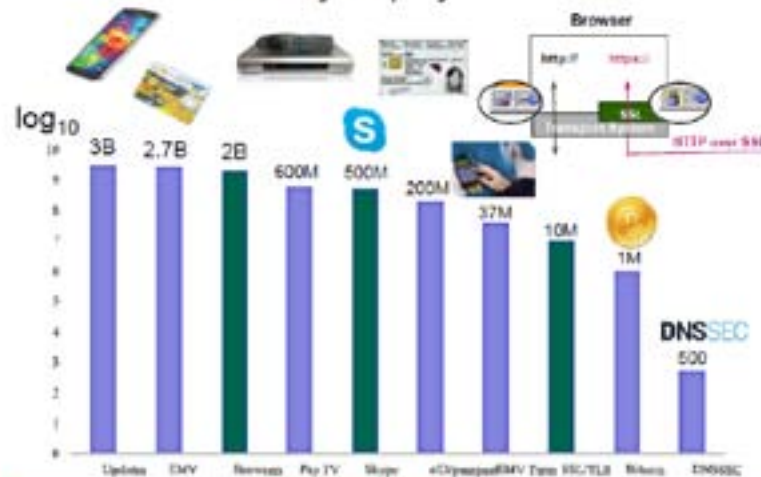
Deployment of cryptography

- most crypto in volume and market serves for data and entity authentication
 - code updates
 - payments: credit/debit/ATM/POS and SSL/TLS

- confidentiality
 - government/military secrets
 - DRM/content protection
 - ehealth (growing market)
 - telco: not end-to-end or with a backdoor
 - hard disk encryption: backdoored?
 - most data in the cloud is not encrypted

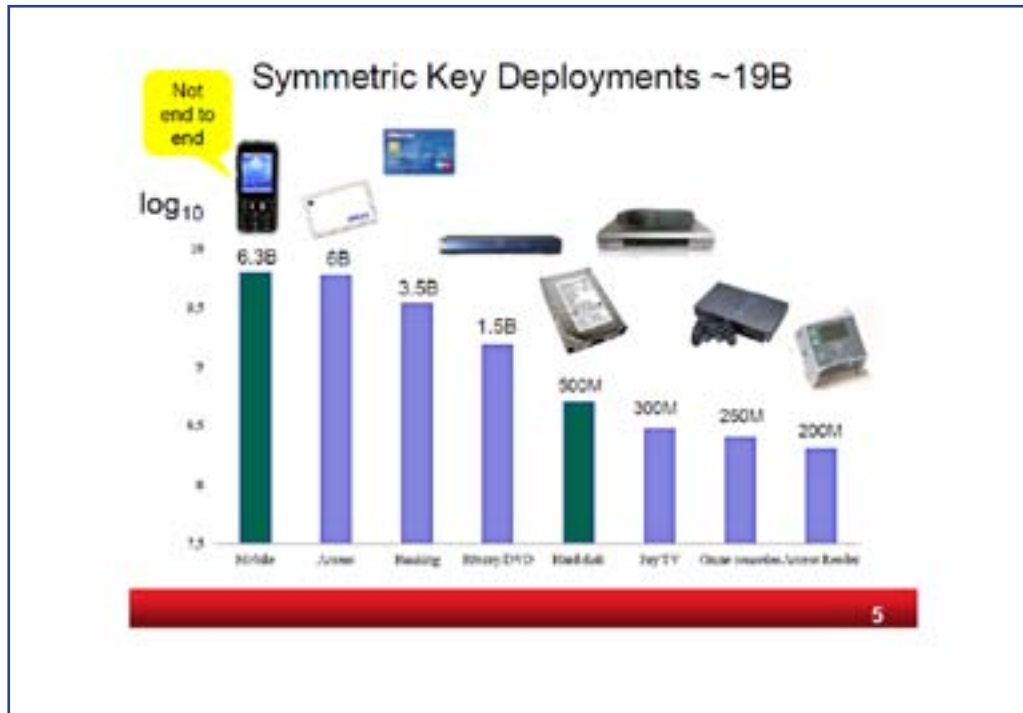
3

Public Key Deployments ~9B



Missing: IPsec, SSH

4



Status of Cryptography

COMSEC:

- limited fraction (a few %) of traffic is protected.
- very small fraction of traffic is protected **end-to-end** with a **high security level** and without a backdoor (email/voice)
 - exception: Blackphone
- need authenticated encryption/secure channels
 - reordering, replay, deletion of packets
- protection of **meta-data is very hard**

6

Status of Cryptography

COMPUSEC

data at rest: key management problem

- hard disk encryption
- cloud: FHE is not a panacea

secure configuration/boot/execution

the Internet of Things/Everything in 2020 (- 20-50B)

Cryptography is **NOT** (yet) used to protect Alice and Bob
but to protect the (intellectual) property of corporations

7

Upgrade problem: what if large quantum computers arrive?

Problem is larger for confidentiality:

- require lead time determined by data life time
- while resigning is possible for data authentication

Upgrades are slow and painful

- probably a few banks are still using single DES
- EMV upgrade from RSA to ECC: 2014-2030
- embedded environments are harder (shellshock)

Many systems have defense-in-depth

- if public key crypto is broken, there is a fall-back mechanism
- examples: EMV, Pay TV

8

All widely used public-key systems rely on three problems from algebraic number theory

Integer factorization: RSA ($n = p \cdot q$)

Discrete **LOG**arithm : Diffie-Hellman, DSA: $y = a^x$

Elliptic Curve Discrete **LOG**arithm, ECDSA: $Q = x \cdot P$

RSA-1024 - DLOG-1024 - ECC-146

RSA-2048 - DLOG-2048 - ECC-206

RSA-4096 - DLOG-4096 - ECC-282

Are these problems hard?

A hard problem is a problem that nobody works on
(James L. Massey)

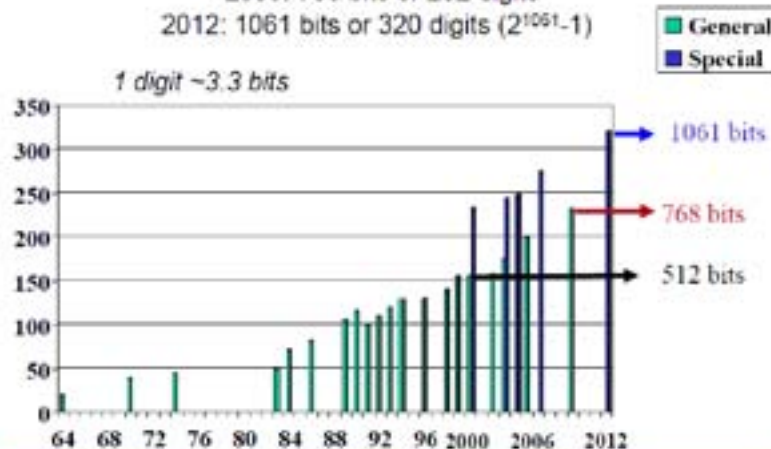
9

Factorisation records (RSA)

2009: 768 bits or 232 digits

2012: 1061 bits or 320 digits ($2^{1061} - 1$)

1 digit ~3.3 bits

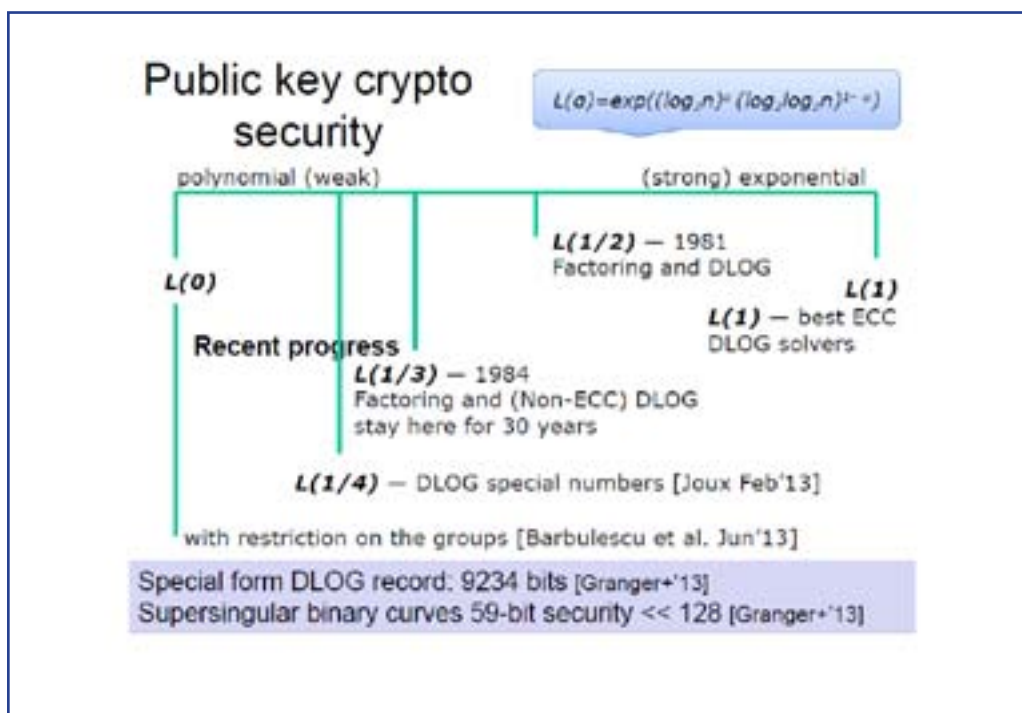


10

The Cryptocalypse?

2013 breakthrough for DLOG in group of special form

11

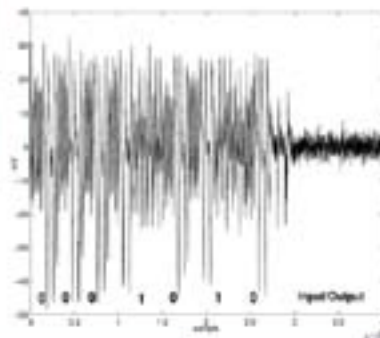


Security in Practice



13

Physics trumps Mathematics



14

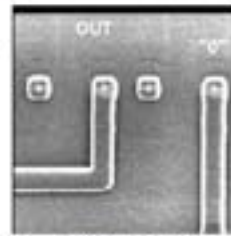
Invasive attacks

Passive: micro-probing



Active: modify circuits

- connect or disconnect security mechanism
 - disconnect security sensors
 - RNG stuck at a fixed value
 - reconstruct blown fuses
- cut or paste tracks with laser or focused ion beam



15

Implementation attacks (CHES conference)

Academic



- ever more sophisticated attacks
- broad range of countermeasures: well understood
- new constructions with security proofs: leakage resilience
- cost in practice: 2-100 times more

Industry

- needs security at cost 20-50% more
- return to security by obscurity
- expensive (but confidential) validation program under Common Criteria

16

Post-Quantum Cryptography

- Go back to the 1970s
 - digital signatures based on one-way functions 
 - public-key encryption based on Error Correcting Coding [McEliece'78]
 - public key encryption based on lattices (inspired by knapsack problems)
- Go back to the 1980s:
 - multivariate polynomial equations 
- So far no good quantum algorithms known to break these systems

17

COMSEC - Communication Security

Undermining of end systems (cf. Snowden)

Do **not** move problems to the authenticity of a single public key

Do **not** move problems to a single secret key

– solution: threshold cryptography; proactive cryptography

Do protect meta-data



18

COMPUSEC - Computer Security

- Simplify to reduce attack surface
- Secure local computation
 - with threshold security
 - Multi Party Computation
 - hardware support: TPM, SMART, Sancus, SGX,...
- Centralized computation on encrypted data
- Secure and open implementations
- Community driven open audit

19

Reconsider every stage



20

Predictions on the Next 40 Years of Public-Key Cryptography

- ??????????: Computers, communications, storage are all quantum and all classical cryptography disappears
- **Highly unlikely:** public-key cryptography will disappear completely
 - everything online: symmetric cryptography could make a comeback for many applications (e.g. EMV, web security, DRM)
- **Probable:** within 10-20 years massive deployment of post-quantum cryptography (hash-based signatures and lattice-based encryption)
- **Probable:** much more sophisticated protocols with distributed crypto and multi-party computation are more widely used
- **Perhaps:** RSA/DLOG/ECC stays around but with much larger key lengths

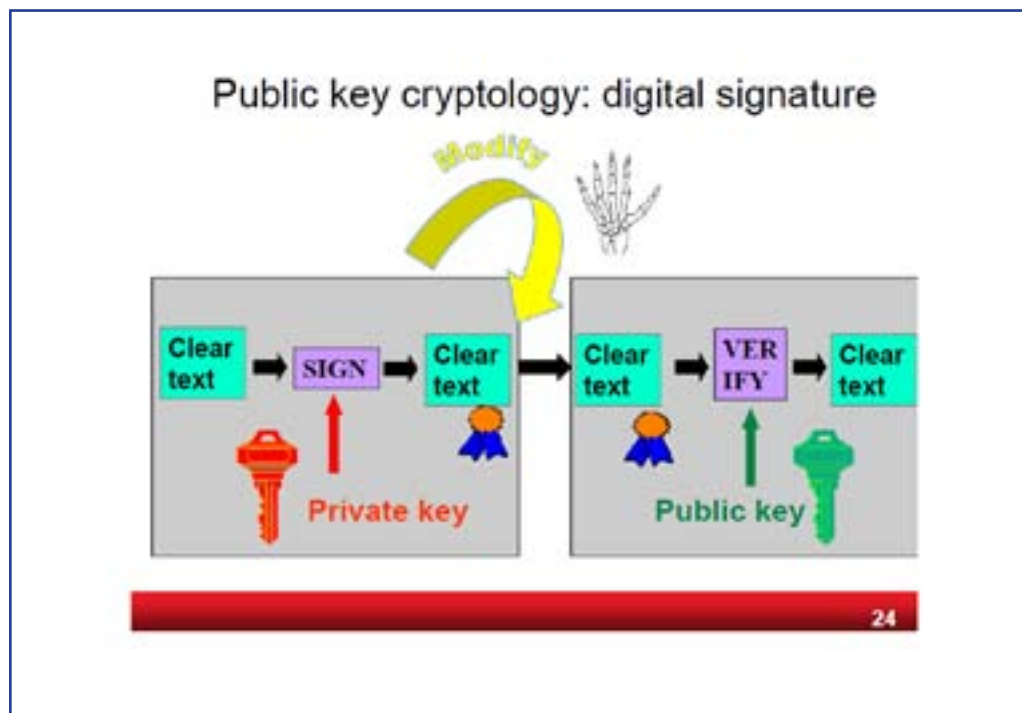
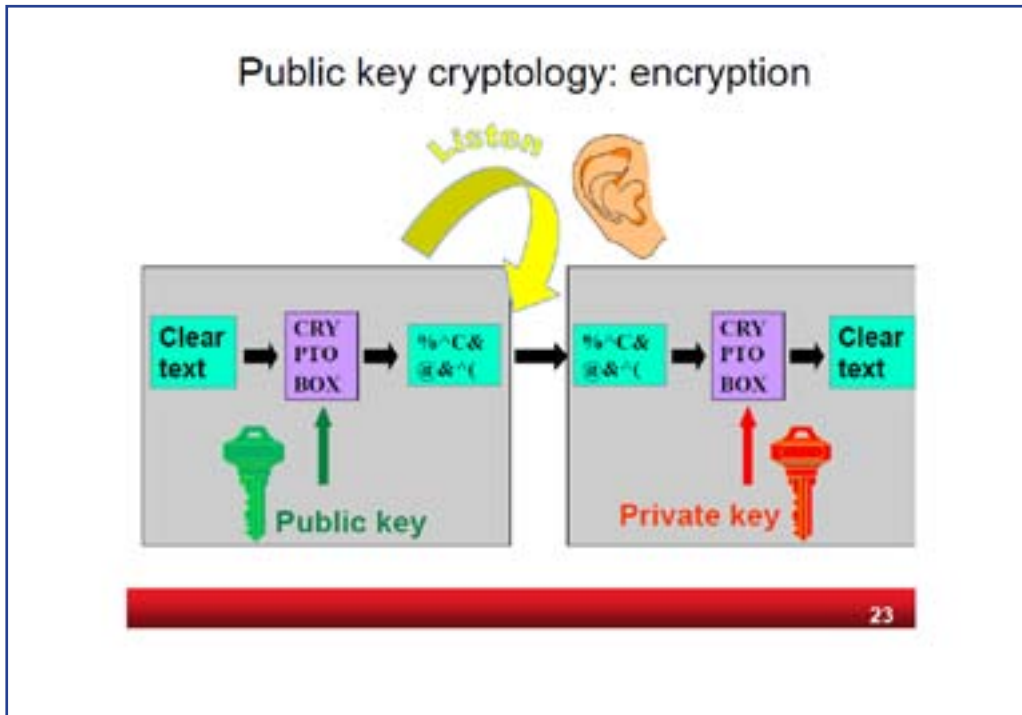
21

The end



Thank you for
your attention

22



Hash-Based Signatures

Slide credit: Andreas Hübsing 25

Hash-Based Signatures: variant XMSS

C Implementation using OpenSSL on Intel(R) Core(TM) i5-2520M CPU @ 2.50GHz with Intel AES-NI [BDH'11]

	Sign (ms)	Verify (ms)	Signature (bit)	Public Key (bit)	Secret Key (byte)	Bit Security	Comment
XMSS-SHA-2	35.00	1.98	15,672	13,600	3,364	157	$h = 20,$ $w = 64,$
XMSS-AES-NI	0.52	0.07	19,616	7,328	1,684	84	$h = 20,$ $w = 4$
RSA 2048	3.08	0.09	~2,048	~4,096	~512	87	

Slide credit: Andreas Hübsing 26

McEliece (1978): code-based public-key crypto

Public key	Private key
a random-looking binary linear code given by a matrix H weight w	random-looking code is a disguised Goppa code with error-correction capability w
Encryption	Decryption
encode a plaintext as weight- w word e and send syndrome $s=H e$	after conversion use standard Goppa-code decoders to determine low-weight solution e

Slide credit: Christiane Peters
27

McEliece security notions

Private key security
Relies on the difficulty of retrieving inner code from public matrix H and thus getting access to efficient decoding

Message security
decryption security relies on NP-hardness of the syndrome-decoding problem for random code - assuming that structure of H does not leak
(best known algorithms take exponential time)

Slide credit: Christiane Peters
28

Performance McEliece

C Implementation on Intel Core i5-3210M, Ivy Bridge (encryption times are estimates)

	Decrypt (cycles)	Encrypt (cycles)	Public Key	Secret Key	Bit Security	Comment
RSA-1024	1,340,040	(92,000)	1024 bits	1024 bits	80	
DH binary ECC	77,468	(78,000)	508 bits	508 bits	127	
McEliece	60,493	(73,000)	187 kByte	187 kByte	128	(n,w) = (212,41)

29

Key Aspects of Lattice-based Systems

Pros

- efficient and parallizable
 - matrix-vector arithmetic, Fast-Fourier Transform for polynomial multiplication
- worst-case to average-case reductions

Cons

- difficult to find good sampling methods
- difficult to assess exact security
- large keys

Slide credit: Christiane Peters

30

Multivariate Quadratic Equations

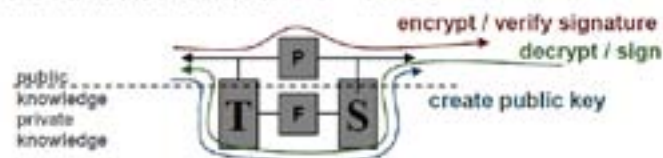
Public Key:

- system of quadratic polynomials $P : F_q^n \rightarrow F_q^m$

Private Key:

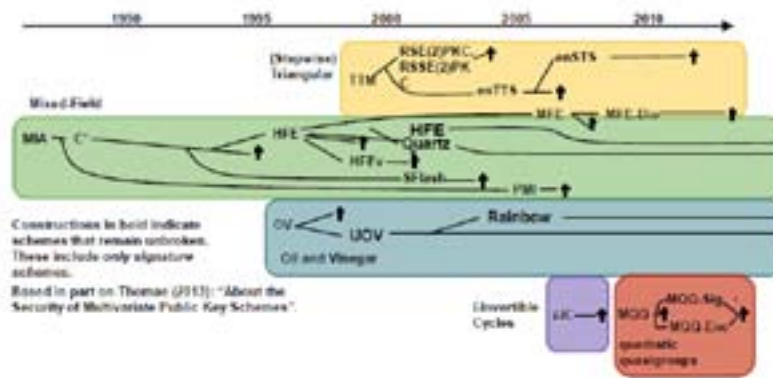
- affine transformations $T : F_q^m \rightarrow F_q^m$ (on output variables) and $S : F_q^n \rightarrow F_q^n$ (on input variables)
- central system of quadratic polynomials $F : F_q^n \rightarrow F_q^m$ (easily invertible)

S and T hide the structure of F: $P = T \circ F \circ S$



Slide credit: Alan Szepieniec 31

Multivariate Quadratic Equations




Constructions in bold indicate schemes that remain unbroken. These include only signature schemes.
Based in part on Thomas (2013): "About the Security of Multivariate Public Key Schemes".

Slide credit: Alan Szepieniec 32

COMPUSEC - Computer Security

Complex ecosystem developed over 40 years by thousands of people that has many weaknesses

- **Errors** at all levels leading to attacks (think )
 - governments have privileged access to those weaknesses
- Continuous remote **update** needed
 - entity that controls updates is in charge
- Current **defense technologies** (firewall, anti-virus) not very strong
 - cannot resist a motivated attacker
- Not designed to resist **human factor** attacks: coercion, bribery, blackmail
- **Supply chain** of software and hardware vulnerable and hard to defend
 - **backdoors** are hard to detect

KEYNOTE Speech 4: Quantum Safe Cryptography - Perspectives

Johannes Buchmann, TU Darmstadt



Quantum Safe Cryptography:
Perspectives
Johannes Buchmann

TECHNISCHE UNIVERSITÄT DARMSTADT

Navigation icons: back, forward, search, refresh, home, list



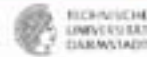
Why quantum-safe cryptography?

- Cryptography indispensable for cyber security
- In particular for long-term protection
- Quantum computers will break today's public-key cryptography

TECHNISCHE UNIVERSITÄT DARMSTADT

Navigation icons: back, forward, search, refresh, home, list

The challenge



- Find quantum-safe mechanisms for
 - Key distribution over insecure channels
 - Public-key encryption
 - Digital signatures
 - Advanced functionalities



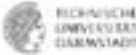
Process




- Specify scheme
- Prove its security
- Determine secure parameters for given security level
- Optimize scheme for relevant security levels and computing environments
- Standardize schemes
- Provide implementations
- Incorporate into applications




Candidates




- Key distribution:
 - QKD and new lattice-based schemes
- Public-key encryption schemes
 - Code-based
 - Lattice-based
 - Multivariate
- Digital signatures
 - Hash-based
 - Multivariate
 - Lattice-based
 - Code-based



Security foundations



- QKD: The laws of quantum mechanics + classical assumptions for authentication
- Hash-based signatures: secure hash functions exist
- Code-based schemes: special decoding problems, e.g. Goppa code decoding, are hard
- Lattice-based schemes: computing short and near vectors in special classes of lattices is hard
- Multivariate schemes: solving special classes of systems of multivariate quadratic equations over finite fields



Security foundations quantum-safe?



- QKD: The laws of quantum mechanics + classical assumptions for channel authentication
- Hash-based signatures: secure hash function required
- Computational problems:
 - Code-based schemes: special decoding problems are hard
 - Lattice-based schemes: computing short and near vectors in special classes of lattices is hard
 - Multivariate schemes: solving special classes of systems of multivariate quadratic equations over finite fields



Secure hash functions



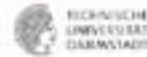
SHA-2
SHA-3
BLAKE
Grostl
JH
Keccak
Skein
VSH
MCH
MSCQ
SWIFFTX
RFSB
...

From block ciphers:

AES
Blowfish
3DES
Twofish
Threefish
Serpent
IDEA
RC5
RC6
...



Computational problems



- Decoding
- Finding short and near vectors
- Solving multivariate quadratic systems

- Quantum algorithms?

- Classical algorithms
 - In the presence of modern computing architectures
 - Using internal structures



Security



- QKD: reduction to laws of quantum mechanics
- Hash-based signatures: XMSS has minimal security requirements
- Lattice-based: (Worst-to-average-case) reductions for some schemes
- Code-based: RSA-like
- Multivariate: RSA-like




Performance




- QKD: deployed for point-to-point communication



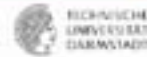
Performance



- Hash-based signatures: XMSS has excellent performance except for somewhat large signatures – IETF standard draft
- Code-based public-key encryption: McEliece/Niederreiter excellent performance except for large keys
- Code-based signatures: insufficient performance
- Lattice-based: schemes with good performance exist, e.g. NTRU
- Multivariate signature schemes: rainbow has excellent performance except for large keys
- Multivariate public-key encryption: still under development



Recommendations



- Standardize and integrate into standard applications: XMSS + NTRU-Encrypt/McEliece-Niederreiter
- Study (ideal) lattice, code, multivariate problems in the presence of modern computing architectures -> parameter selection
- Optimize lattice, code, multivariate schemes for secure parameters- Consider side channels.
- Provide security proofs for code-based and multivariate schemes
- Integrate QKD with other techniques for everlasting security





THANK YOU
VERY MUCH



KEYNOTE Speech 5: Why Quantum technologies do matter for Europe

Stephan Lechner, DG Joint Research Centre



Why Quantum Technologies do matter for Europe
2nd ETSI Quantum Safe Crypto Workshop, Ottawa, Oct 6th 2014



Dr. Stephan Lechner
Director
Institute for the Protection and Security of the Citizen
Joint Research Centre
The European Commission's in-house science service
Serving society
Stimulating innovation
Supporting legislation
www.jrc.ec.europa.eu



The European level





The European Commission



- 28 Commissioners
- Proposing EU legislation
- Funding European Research (Horizon 2020)
- In-house scientific service (JRC)

Jean-Claude Juncker,
President-elect
of the European Commission



- Funding quantum technologies research collaboration
- Bringing science and policy-making together
- Looking into the future of Europe : INNOVATION



Quantum Technologies: Innovation?



- Disruptive
- Game-changing
- Cross-cutting
- First commercial applications

Timeline???

**Europe cannot afford missing out
on key enabling technologies!**





Getting things done at EU level

	EU	US
Founded:	1958	1776
Population:	500M	300M
Central Research Funding:	10%	90%
Member States (nations):	28	1
Languages:	24	1
Currencies:	11	1
Standardisation Organisations	28+3	1+
Motto:	"United in diversity" (since 2000)	"In God we trust" (was: "E pluribus unum", 1782 - 1956)



Europe: Effectiveness is key!

At present, there is no central EU mechanism for evaluating quantum technologies, assessing their fitness for purpose, and identifying vulnerabilities or other weaknesses.



The diagram illustrates the flow of resources and expertise between the National and European levels. At the National Level, there is 'Funding' (represented by a stack of coins) and 'Laboratories' (represented by various scientific equipment icons). An arrow points from National Level Funding to European Level Funding. From European Level Funding, an arrow points to Scientific Expertise (represented by a brain icon). A bracket at the bottom groups the National Level Funding and Laboratories under the label 'Laboratories'.



A administrative Quantum Leap?

- JRC Work Programme 2015 features QT
- New recruitments selected
- Internal scientists trained
- Ready for a genuinely European contribution



The way ahead: long and steep...

- Sorting out the EU level role
- Identifying needs for harmonisation
- Blending in with research and funding
- Consulting future policy makers
- Some patience required!

... but QT is too important to not go ahead.



KEYNOTE Speech 7: QKD applications and new physical layer cryptography

Masahide Sasaki, NICT

Quantum-Safe Cryptography Workshop 6th Oct 2014

**QKD applications
and
new physical layer cryptography**



Quantum ICT Lab
Masahide Sasaki

1

Contents

(1) QKD applications

Two facts on user attitude

➡ Our current efforts

(2) Security in global networks

Intrinsic limit on QKD

➡ A new physical layer cryptography

2

Fact (1)

High end users (MoD, ...) are seriously worried about security threats on the physical layer after the Snowden files, but have not decided yet to introduce QKD. They are still watching.

The strongest security is not necessarily a reason for the scheme to be adopted.

There are many strong crypto-schemes, but most of them have not been used in practice yet.

3

Most of users still use RSA1024.



4

Implication from Fact (1)

- Stand-alone QKD is hard to be accepted.
- Start with an **existing** security system, then integrate QKD into it, and realize **new values**.

Algorithmic cryptography	New values of QKD
1. Not provable --> Need to be updated	1. Updating the scheme itself is not necessary
2. Cannot detect hacking	2. Can detect hacking
3. Specs of high-end solutions are usually not disclosed. -->Hard to interconnect the systems of different divisions even in the same organization.	3. Simplest encryption : one-time pad, $C=X + K$ --> No processing latency --> Seamless cryptic connectivity can be realized if key IDs are properly managed.

5

Fact (2)

Responses to our press releases on QKD applications remarkably increased this year.

Ex. QKD-assisted secure smart phone (May 2014)

Potential customers who have asked us on it include

- Ministries (MIC, MHLW)
- Prefectural office
- General construction company
- Banks
- Car company
- Print company

They are looking at future society based on the Internet of Things, and want to know what kind of security technology they should introduce, and how to revise their security systems.

Conversation with them are very inspiring.

QKD-key + smart phone is something marvelous !

6

QKD-assisted secure smart phone

Hierarchical access control to confidential data files

Useful to protect state secrets and medical chart


7

Implication from Fact (2)

There are **new fields** where security is becoming a new concern. That is, **modern crypto and QKD are at the same start line.**

- Medical network
- Controller Area Network (CAN)
- Robot network
-

How to share symmetric keys between control units and how to manage them?



Security standards have not been decided yet.

Latest model of QKD (Decoyed BB84, by NEC)

Key rate 100kbps
Distance 60km
(for fiber loss 0.2dB/km)
Clock rate 1.24GHz

9

Integrate QKD with a commercial product, Comciper

Data layer encryptor

Most of mission critical channels are made in the 2nd layer (data layer), not going up to the 3rd layer (IP network layer)

Comciper (AES)
Throughput 10Gbps

Layer-2 switch
Data center

Layer-2 switch
Users

QKD

- Enhance the security of AES by key refresh
- One-time pad mode is optional for high-end use.

10



Make a QKD show case for Tokyo Olympic 2020
Safest Tokyo Network

ImPACT Program (Oct 2014-Mar 2019) by the Cabinet office
Impulsing PAradigm Change through disruptive Technologies



13

Contents

(1) QKD applications

Two facts on user attitude

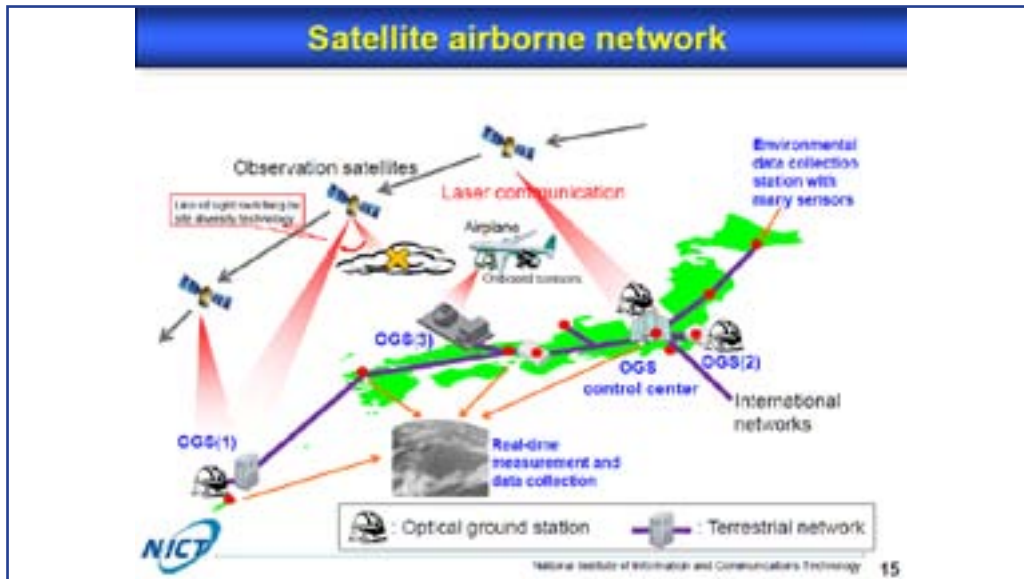
➡ Our current efforts

(2) Security in global networks

Intrinsic limit on QKD


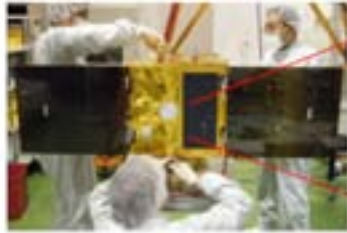

➡ A new physical layer cryptography

14



Small satellite SOCRATES (NICT, AES, NEC, JAXA)

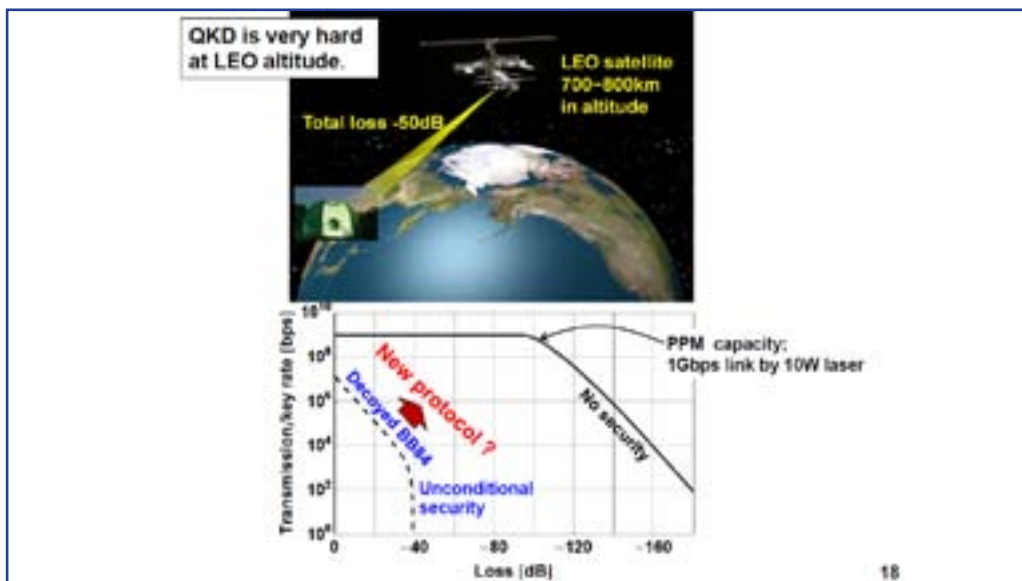
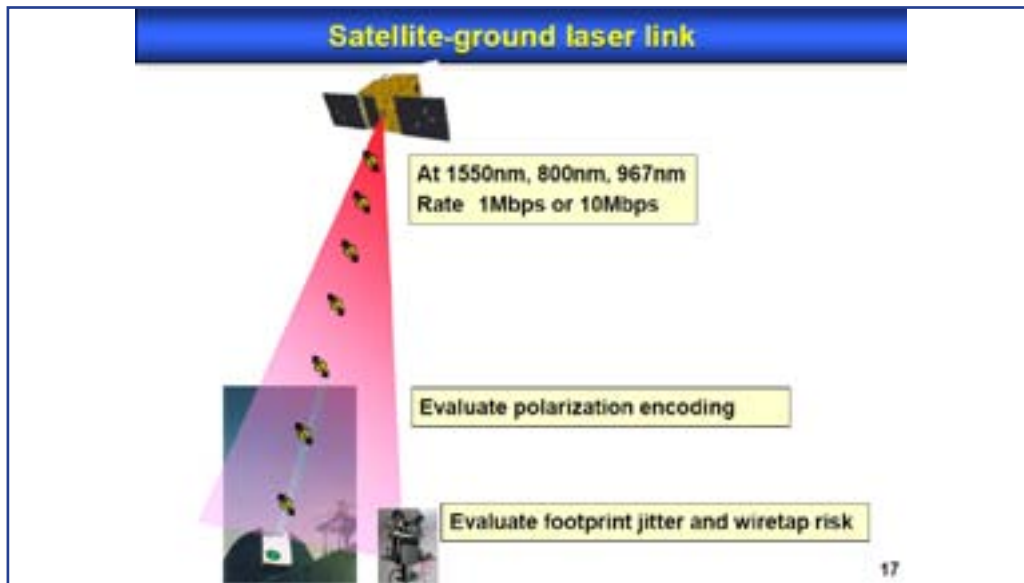
- Launched on 24 May 2014
- Successfully put on the orbit (628km)
- Now under preparation for operation

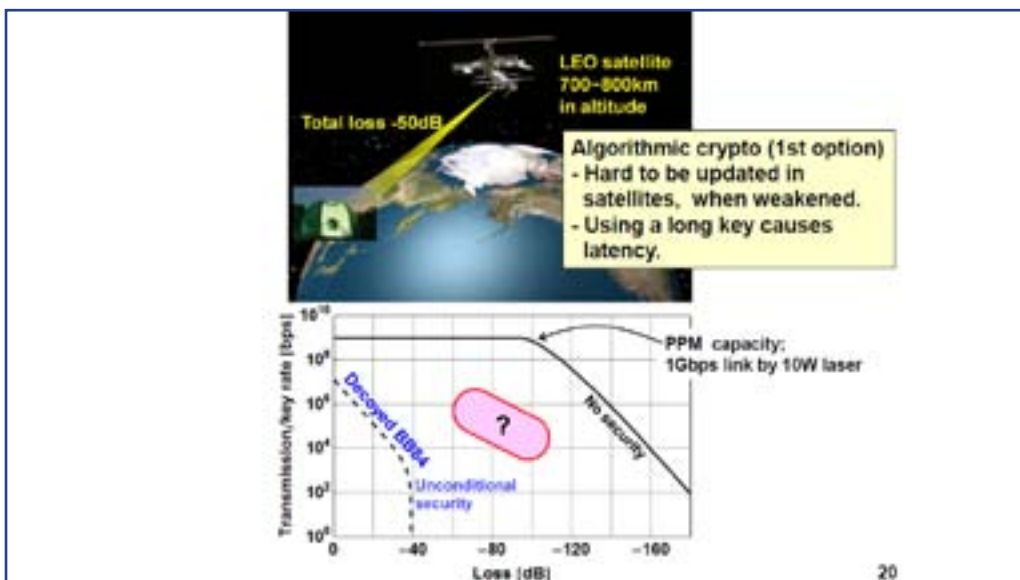
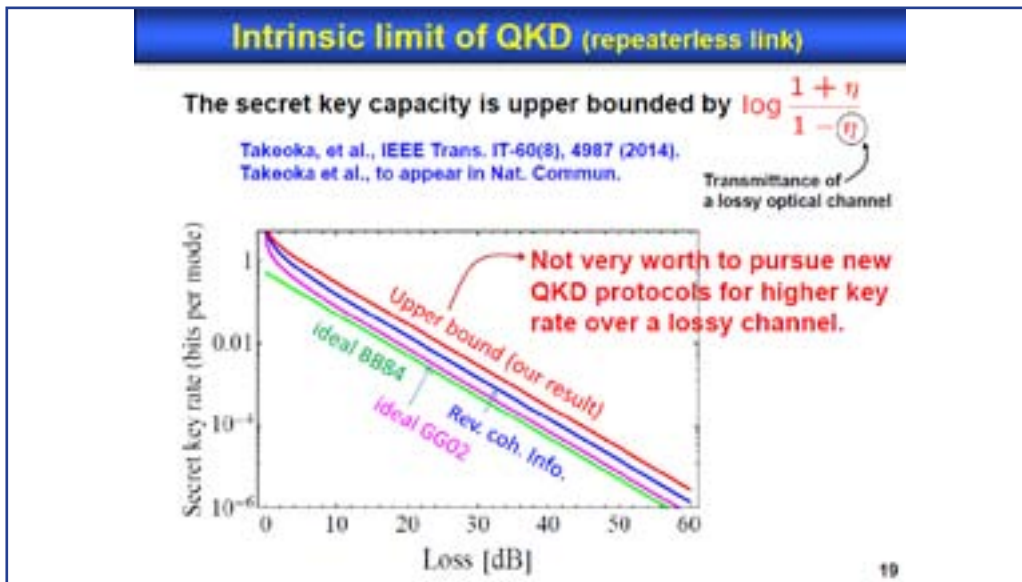


50kg-satellite bus

Small optical transponder
6.2kg

16





Physical layer cryptography

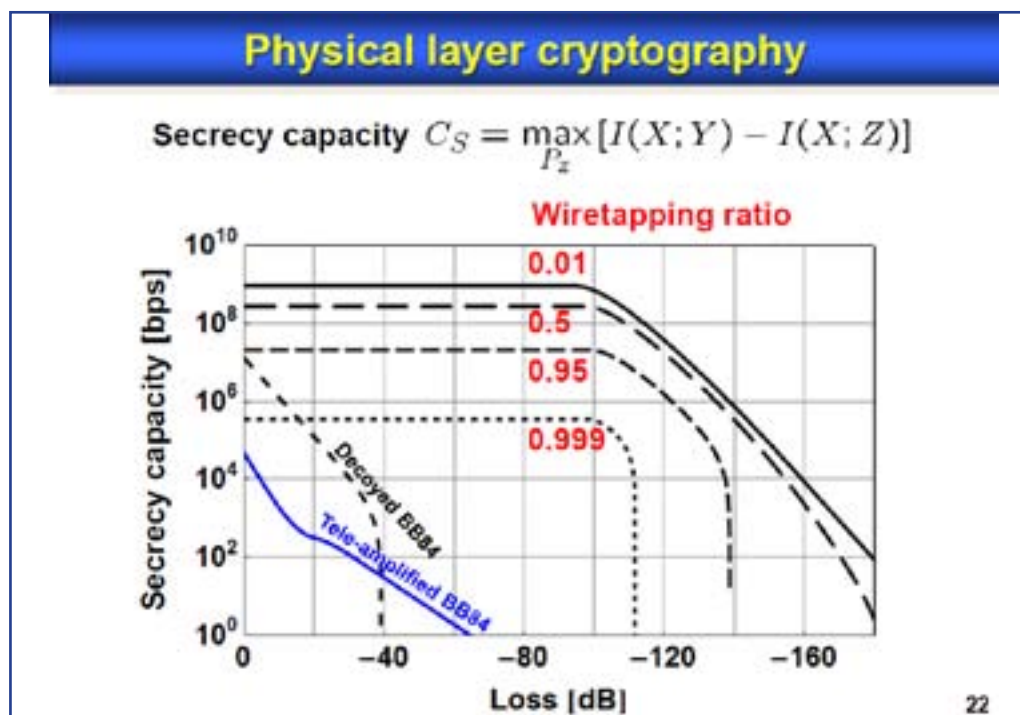
Opportunistic link when Eve's channel is physically bounded.

"Information theoretic security" at higher rate

Ex. Line-of-sight communication

Wyner, Bell Syst. Tech. J., 54(8),1355 (1975).
Csiszár and Körner, IEEE Trans. Inf. Theory, IT-24(3), 339 (1978).

21



Theory of finite length analysis

Han, Endo, & Sasaki, arXiv:1307.0608 [cs.IT]
To appear in IEEE IT

Power constraint

$$\sum_x q(x)n(x) \leq \Gamma$$

A priori prob.

$q(0)$
 $q(1)$

X
0
1

$W_B(y|x)$

Y
0
1

Decoding error

$\epsilon_n^B \leq 2e^{-nF(q,R_B,R_E,n)}$

$W_E(z|x)$

Z
0
1

KL distance "Strongest measure"

$\delta_n^E \leq 2e^{-nH(q,R_E,n)}$

Reliability function

$$F_c(q, R_B, R_E, \infty) = \sup_{0 \leq \rho \leq 1} \sup_{r \geq 0} [\phi(\rho | W_B, q, r) - \rho(R_B + R_E)]$$

Secrecy function

$$H_c(q, R_E, \infty) = \sup_{0 < \rho < 1} \sup_{r \geq 0} [\phi(-\rho | W_E, q, r) + \rho R_E]$$

23

Tradeoff engineering : reliability vs secrecy

Rate shifting

Stronger secrecy but lower reliability

nR_B nR'_E

Rate exchange

Stronger secrecy with the same reliability (Message rate is degraded)

nR'_B nR'_E

Reliability and secrecy functions

Y-axis: 0.00 to 0.10

X-axis: 0 to R

Intersection point: R_E

Shifted intersection point: $R'_E = R_E + \Delta$

Message: nR_B Randomness: nR_E

Message: nR'_B Randomness: nR'_E

Constraint: $R_B + R_E = R'_B + R'_E$

24

Physical layer crypto in fiber network

It is unrealistic to assume that Alice and Bob know Eve's channel.
 → Coding must be designed to withstand multiple possible realizations for the wiretap channel.

Multi-level-security embedding network coding

High-security message can be embedded into low-security message.
 When Eve is strong, a prescribed part of the bits remain secure.

Statistically independent messages from other users can be the random bits to deceive Eve.

25

New generation secure network

QKD

↔

Phys Layer Crypto

↔

Algorithmic Crypto

Combine Physics laws, Coding, PA, & Algorithms

Quantum noise
(Optical domain)

Thermal noise
(RF domain)

26

Presentations

SESSION 2 SETTING THE SCENE


KEYNOTE Speech 8: Quantum-safe cryptography and security
An Introduction, Benefits, Enablers and Challenges – white paper summary
Mark Pecan, Approach Infinity, Inc.




Quantum-safe cryptography and security:
An Introduction, Benefits, Enablers and Challenges – white paper summary
Mark Pecan - ETSI 2nd Quantum-Safe Crypto Workshop (October 2014)

© ETSI 2014. All rights reserved.

The ETSI Quantum-Safe Whitepaper, 2014




- Primary purpose is to help raise awareness of the potential impacts of quantum computing on information security globally
 - Threat of quantum computing to the effectiveness of the current cryptographic state of the art
 - Possibilities for risk mitigation – quantum-safe cryptographic techniques – economic and technical practicalities
 - Economic and technical challenges to the deployment of quantum-safe security and the role and impact of global standards
- Document is 49 pages long, library identifier ISBN 979-10-92620-03-0

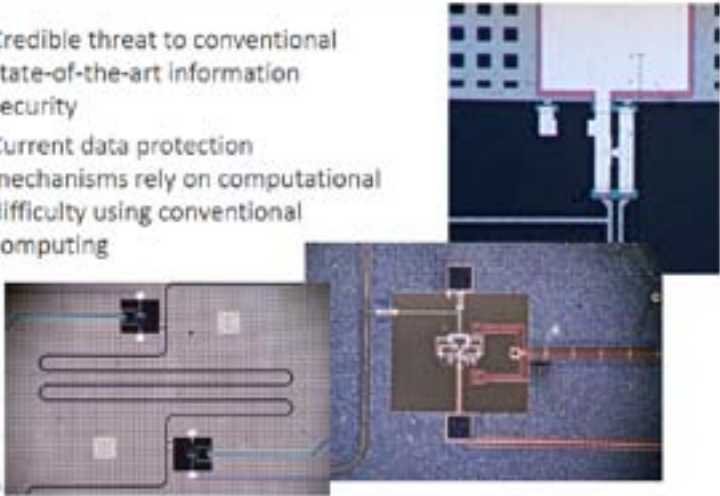


© ETSI 2014. All rights reserved.


Recent research in quantum computing



- Credible threat to conventional state-of-the-art information security
- Current data protection mechanisms rely on computational difficulty using conventional computing



We survey the current state-of-the-art



- Quantum computing challenges our notion of computational hardness, because certain types of hard problems for a conventional computer become trivial for a quantum computer:
 - Integer factorization
 - Discrete logarithms
- We examine some of the most widely-deployed cryptosystems in security products today including
 - Rivest Shamir Adleman (RSA)
 - Elliptic Curve cryptography (ECC)
 - Diffie-Hellman key generation
- All of these cryptosystems will be broken by large-scale quantum computers

What, exactly, is vulnerable?




The diagram consists of three overlapping ovals. The largest, outermost oval is purple and labeled 'PRODUCTS which derive their security from these protocols and cryptosystems'. Inside it is a green oval labeled 'SECURITY PROTOCOLS relying upon any of these cryptosystems'. The smallest, innermost oval is blue and labeled 'CRYPTOSYSTEMS that have been built on the presumed difficulty of discrete log or integer factorization'.

- Basically, anything that's been encrypted and residing on mass storage instantly becomes available to anyone with access to a quantum computing platform!

© ETSI 2012. All rights reserved.


Consider a definition for "Quantum-Safe"




1. Cryptography based upon problems that neither classical nor quantum computers can efficiently solve:
 - Code-based cryptography
 - Lattice-based cryptography
 - Multivariate quadratic cryptography
 - Hash-based digital signatures
2. Cryptosystems that use basic physical laws of quantum mechanics to protect data:
Quantum key distribution

© ETSI 2012. All rights reserved.

Discussions – general to fairly specific




- Survey of current state-of-the-art
 - Elliptic Curve Cryptography (ECC)
 - Rivest Shamir Adleman (RSA)
- Quantum-safe approaches
 - Computational quantum safe approaches, e.g. code-based, lattice-based, hash-based, etc.
 - Quantum Key Distribution (QKD), etc.
- Examination of security protocols potentially to upgrade
 - X.509 certificates
 - Internet key exchange version 2 (IKEv2)
 - Transport layer security (TLS) version 1.2
 - S/MIME
 - Secure shell (SSH) version 2




© ETSI 2022. All rights reserved.

Fields of application



- **Use cases** such as:
 - Encryption of endpoint devices
 - Network infrastructure encryption
 - Cloud storage and computing
 - Big data, machine learning, and data mining
 - SCADA systems for industrial control
- **Industries** such as:
 - Medicine, biotechnology, & health
 - Financial services
 - Mobile networks



© ETSI 2022. All rights reserved.

Economics of upgrading




- Managing technology switching costs
 - Cost and complexity to quantum-safe a system
- Challenges to quantum-safety
 - Some network security protocols may be too rigid to accommodate the increased key lengths
 - Changes in ciphers may be required to make them quantum-safe – expensive & impractical
 - Standardisation requires time – start soon
- Risk management
 - Economic view of security risks
 - An insurance model view
 - The role of standards




© ETSI 2022. All rights reserved.

Practical considerations – how urgent?




- It depends on the category of information and how long it needs to be protected
 - x: how many years we need our encryption to be secure
 - y: how many years it will take us to make our IT infrastructure quantum-safe
 - z: how many years before a large-scale quantum computer will be built



The diagram shows a horizontal timeline with an arrow pointing right labeled 'Time'. There are two rows of bars. The top row has a yellow bar labeled 'Y' followed by a light blue bar labeled 'X'. The bottom row has an orange bar labeled 'Z' followed by a red bar labeled 'Secrets Divulged'. The 'Secrets Divulged' bar starts at the end of the 'Z' bar and extends further to the right.

© ETSI 2022. All rights reserved.

Not all data are equal



- 1 The value of x must be carefully considered:
 - What are the practical consequences of a certain category of information becoming public knowledge after x number of years?
 - For example, would it be a problem if your credit card numbers of today are made available to everyone in the world after $x = 5$ years? Probably not, because its very likely that you would have a new credit card issued, having a new expiry date and security code.
- 2 On the other hand, if your personal identity information is made public after $x = 5$ years, you may be exposed to identity theft and any resulting consequences.
- 3 Caution is also required for other information categories such as top-secret military information, e.g. the orbits of secret military satellites, location of military bases and their resources and capabilities - defining the value of x is a non-trivial matter

© ETSI 2022. All rights reserved.

Conclusions and way forward



- 1 Quantum computing indeed poses a credible threat to conventional information security systems
- 2 The ICT community nevertheless has the ability to analyse and better understand this threat and its consequences for the various categories of information that requires protection
- 3 Recommendations and opportunities for further work are presented
 - Recommendations for enterprises
 - Recommendations for security product vendors
 - Opportunities for further research



© ETSI 2022. All rights reserved.

Special thanks to our contributors

Authors:
Matthew Campagna, Ph.D., IQC Affiliate
Lidong Chen, Ph.D., Mathematician, National Institute of Standards and Technology
Dr Özgür Dagdelen, TU Darmstadt
Jintai Ding, Ph.D. Department of Mathematical Sciences, University of Cincinnati
Jennifer K. Forniok, B.Sc, Institute for Quantum Computing, University of Waterloo
Nicolas Gisin, Department of Applied Physics, University of Geneva, Switzerland
Donald Hayford, National Security Division, Babelio
Norbert Lutkenhaus, PhD, Institute for Quantum Computing, University of Waterloo
Michele Mosca, D.Phil., Institute for Quantum Computing, University of Waterloo
Brian Neill, CISSP, CSSLP, Institute for Quantum Computing, University of Waterloo

Mark Pezon, Approach Infinity, Inc
Ray Perlner, Computer Scientist, National Institute of Standards and Technology
Gregoire Ribordy, PhD, Chief Executive Officer, ID Quantique
John M. Schanck, Institute for Quantum Computing - University of Waterloo
Dr Douglas Stebila, Queensland University of Technology
Nino Walenta, Ph.D., Babelio
William Whylo, D. Phil., Chief Scientist, Security Innovation
Dr Zhenfei Zhong, Security Innovation Inc

Other contributors:
Sarah Kaser, B.Sc, Institute for Quantum Computing, University of Waterloo
Albrecht Potzold, Technical University of Darmstadt
Daniel Smith-Tone, Mathematician, National Institute of Standards and Technology
Assistant Professor, University of Louisville

10 | © ETSI 2022. All rights reserved.

Presentations

SESSION 3
DEPLOYMENT**Rethinking the adoption of Hash-Signatures***Burt Kaliski, Verisign*

Hash function-based digital signature schemes ? in particular, the classic Merkle tree signature scheme ? are among the earliest forms of public-key cryptography. However, perhaps due to their large signature size, or perhaps to their lack of a corresponding asymmetric encryption scheme, hash signatures have not entered the mainstream over the past three decades. The current emphasis on post-quantum cryptography provides a strong motivation for their adoption, but will that be enough? In addition to the promise of long-term resilience, it may also be necessary to demonstrate some near-term advantages of hash signatures over conventional approaches.

This talk will describe some of those advantages, as a basis for a more general discussion on what other advantages may be needed to move hash signatures into the mainstream.



Hash Signatures

Version Public

powered by VERISIGN

8

Hash Signatures: Background

- For purposes of this discussion, “hash signature” = **Merkle Tree Signature** with one-time signature scheme based on hash function (e.g., Lamport-Diffie-Winternitz)
- References:
 - [MC14] D. McGrew and M. Curcio. *Hash-Based Signatures*. Internet-Draft draft-mcgrew-hash-sigs-02, July 4, 2014.
 - [BDH11] J. Buchmann, E. Dahmen and A. Hülsing. *XMSS – A Practical Forward Secure Signature Scheme based on Minimal Security Assumptions*. *PQCrypto 2011*.
- “Conventional signature” = RSA, ECDSA, etc.
- Assumption: Hash signatures “quantum safe” as a general construction (with appropriate parameter sizes)
 - May need to replace hash function over time, but easier to develop new hash function than entirely new signature scheme!

Version Public

powered by VERISIGN

9

Hash Signatures: General Model

Signature includes:

- **One-time signature** with one-time private key
- **Index** of one-time key pair
- **Authentication path** from one-time public key to root



Verizon Public

powered by VERIZON

8

Key Question: Driving Adoption

- Assuming that hash signatures are better in the long term, what do we need to encourage adoption?
- Challenge: Long-term advantages generally aren't enough

Verizon Public

powered by VERIZON

8

Long-Term Advantages Aren't Enough

- Historically, crypto algorithm adoption has been motivated by three factors: **mandates**, **algorithm breaks**, and **significant new functionality**
 - Similar point for key size increases
- Partial breaks often patched
- Potential future breaks (e.g., via quantum computers, or advances in cryptanalysis) generally ignored
- **Premise:** Long-term advantages of hash signatures, other quantum-safe crypto **not enough to motivate adoption**
 - Even in new applications where interoperability isn't as important ...
 - Economic tradeoff: If it's not broken – fix something else!
- Without mandates or breaks in other algorithms, also need **near-term advantages**: new functionality

Version 1.0.0

powered by VERISIGN

7

What Kinds of New Functionality?

- Primarily, improvements in **trust model** – which parties have to be trusted, for what purposes, and for how long
- “Shorter” and “faster” help but only they change the game – e.g., by making other functionality practical sooner
 - Moore's Law, hardware accelerators, hybrid algorithms, etc. quickly level the playing field
- Public-key cryptography enabled **encryption**, **authentication without prior establishment of shared secrets** – advantage even though size, speed were not!
- Elliptic curve cryptography shorter, faster than RSA for most operations – but especially for key generation, which enables **forward secrecy**

Version 1.0.0

powered by VERISIGN

7

A Health Care Analogy

- "... despite decades of effort and millions of dollars, only between 3% and 34% of people in poor countries regularly wash their hands ..."
- "The bigger problem is that **long-term health considerations do not drive behavior ...**"
- "What does are things like love, fear, and wanting to be accepted and admired"



Source: It's a wash: Hands-on hygiene in Peru. Science, 12 September 2014.

Some Near-Term Advantages of Hash Signatures

#1: Short Backdating Windows

- With conventional signatures, adversary who compromises private key can **backdate signatures** all the way to start of **validity period** for public key
 - e.g., as published in certificate
- With hash signatures, and [BDH11] "forward-secure" enhancement, adversary can only backdate to start of validity period for **current one-time private key**
- Advantage: Short backdating windows **without frequent key rollovers** / certificate updates
 - Trust model improvement: Signer can **bound impact of private key compromise** to shorter time period
- Application: Time-based transaction signing

Copyright ETSI

powered by WERISMAN

16

Short Backdating Windows

Forward-secure enhancement (based on [BDH11]):

- Generate next one-time private key as **one-way function** of previous one
 - ... or of related state
- Associate indices with specific **sub-intervals** of overall validity period



Copyright ETSI

powered by WERISMAN

17

#2: Coarse-Grained Delegation

- With conventional signatures, signer can only delegate limited signing capabilities to another party by signing a **“delegation of authority”** to the other party’s public key
- With hash signatures, signer can delegate by providing a **subset of its one-time private keys**
 - Delegation scope defined by *index semantics*; what 1, ..., N mean
- **Advantage:** Coarse-grained delegation **without a second level of keys**
 - Trust model improvement: Signer can involve other parties in signing, while setting (coarse) bounds on their authority
- **Applications:** Load-balanced / proxy signing with traceable signatures

Verizon Public

powered by VERIZON

18

Coarse-Grained Delegation

Delegation enhancement:

- Delegate **subsets of one-time private keys** to other parties
- Associate indices with **specific meanings or limitations**
 - e.g., second half = “may be delegated”: verifier may treat these differently than first half



Verizon Public

powered by VERIZON

18

A Proposed Adoption Strategy for Hash Signatures

Version Public

powered by VERISIGN

18

Three Steps toward Adoption

1. Fit into existing framework, but extend with new functionality
 - Hash signature specifications should fit into existing framework for signing, verification, key management, to simplify integration
 - Specifications should also describe new functionality, e.g., short backdating windows, coarse-grained delegation
2. Develop supporting tools, challenge assumptions as needed to leverage new functionality
 - Index-based policies for valid signing times, delegation scope
 - Forensics based on traceable signatures
 - Challenge assumptions: valid signing time = public key validity period; delegation requires fine-grained statement; signatures don't identify where they were generated
3. Find applications where new functionality matters

Version Public

powered by VERISIGN

18

A Candidate Application: DNSSEC Signing

- Domain Name System Security Extensions (DNSSEC) add signatures to records for **end-to-end data integrity**
 - Records, signatures returned in response to lookup requests to **name servers**
- Signatures typically **precomputed offline** when records are updated – not in real time
 - Advantage: Reduce risk of private key compromise; name server instances don't need to be trusted to sign
 - Disadvantage: Dynamic range limited to what's been precomputed
- If hash signatures were adopted, signing operations could be **delegated with traceability** to name server instances
- Application question: Would it matter if signatures could be computed in real time in some cases?

Verizon Public

powered by VERIZON

18

Summary

- Long-term advantages hard to sell on their own – need near-term advantages as well
- Hash-based signatures offer significant new functionality
- To sell hash-based signatures, find applications where new functionality matters, focus on these for early adoption
- Operational experience with these applications will facilitate adoption elsewhere in the long term

Verizon Public

powered by VERIZON

19

Presentations

SESSION 3
DEPLOYMENT**Neither do people pour new wine into old wineskins***Lily Chen, NIST*

Quantum computing tackles today's widely deployed public key cryptographic algorithms such as RSA and DH. It should not diminish the security of the protocols used in today's network e.g. TLS, IKE, and SSH. Theoretically, if those algorithms are replaced with quantum computing resistant cryptographic algorithms, the protocols should be as secure as it is supposed to be. On the other hand when the protocols were designed more than two decades ago, the protocols were to accommodate the existing public key cryptography algorithms. The question is: can we pour the new wine into old wineskins? This presentation looks into some potential possibilities and impossibilities when using some quantum. computing resistant cryptographic algorithms in TLS, IKE and SSH.

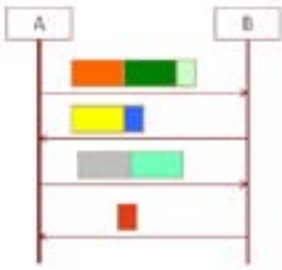


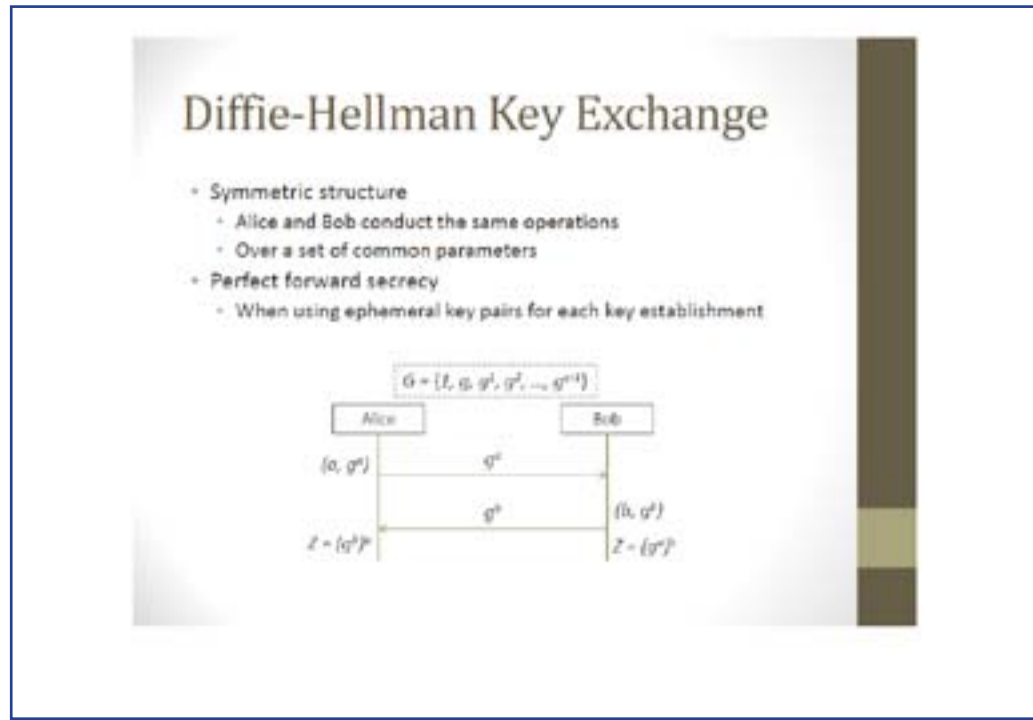
Outline

- The current security protocols
- Possible migration path
- Issues and strategies

Security Protocols

- Security protocols are widely deployed to secure the network and communication systems such as
 - Internet Key Exchange (IKE)
 - Transport Layer Security (TLS)
- When the protocols were designed, it targeted on *accommodating certain cryptographic schemes*
- To build quantum resistant security protocols, can we just replace these schemes with quantum resistant schemes?





Diffie-Hellman Key Exchange in IKE

- Establish keys between any two IP hosts using Diffie-Hellman key exchange
- Use a group number to indicate the DH group (parameters)
- *Internet Key Exchange is indeed Diffie-Hellman Key Exchange for Internet*

Quantum Resistant IKE

- IKE does not support negotiation of different key establishment schemes
- Currently no exact quantum resistant DH counterpart can be used with symmetry
 - Some quantum resistant key exchange is not as symmetric as DH
- It is very likely that a quantum resistant encryption scheme will be used to establish keys
 - Use one time public key to obtain perfect forward secrecy
 - Require a fast key pair generation

Quantum Resistant IKE Discussion

- Key pair generation with compatible efficiency is possible for quite a few existing quantum resistant schemes
- It lost the symmetric property but security may not be reduced
- The parameters need to be sent, probably together with the public key, which is not accommodated in the current IKE
- It is not straightforward to extend IKE to support multiple schemes
 - Additional extensions are needed

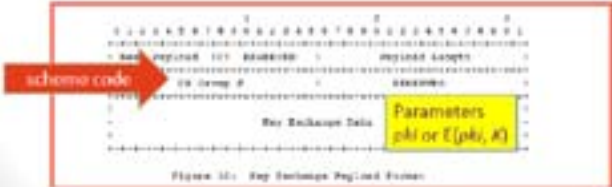


Figure 10: Key Exchange Request Format

RSA Encryption/Signature

- RSA encryption and signature have a specific asymmetry property when selecting e small, e.g. $e = 2^{16} + 1$
 - Light operations using (n, e) for
 - Encryption M^e ; and
 - Signature verification $S^e, H(M)$
 - Heavy operations using (d, p, q) , where $d \cdot e = 1 \pmod{\Phi(n)}$ for
 - Decryption C^d ; and
 - Signing $H(M)^d$
- Certified RSA public key can be used for authentication
 - Explicitly by signature
 - Implicitly by key confirmation on the transported key

Transport Layer Security (TLS)

- A protocol between a server and a client
 - In early days, the client can have limited processing capabilities
 - The purpose is for a client to securely login an authenticated server
 - Server authentication is required, while client authentication is optional
- Support three major methods for key establishment
 - **RSA key transport (most commonly supported)**
 - Ephemeral static DH
 - Ephemeral DH
- TLS support ciphersuite negotiation
 - TLS ciphersuite examples
 - TLS_RSA_WITH_AES_128_CBC_SHA
 - TLS_DH_WITH_AES_128_CBC_SHA
 - TLS_DHE_WITH_RSA_AES_CBC_SHA

TLS 1.2 (or lower version). TLS 1.3 will change the handshake

RSA in TLS

- RSA key transport
 - Client selects a pre-master secret, encrypts with server's certified public key
 - Server conducts implicit authentication by key confirmation
- The server's RSA key is certified
 - The client verifies CA's RSA signature (again, to take advantage of RSA with small "e")

Key confirmation

Quantum Resistant TLS

- Introduce quantum resistant ciphersuite, e.g.
 - TLS_NTRU_AES_128_CBC_SHA
- Today's TLS clients may be powerful to handle the processing requirements for PQ crypto schemes
 - Asymmetry capacity for client and server may not be as important as in the early days in selecting schemes
- When perfect forward secrecy property is required, TLS needs to adapt to one-time encryption key pair schemes

Possible Migration Path

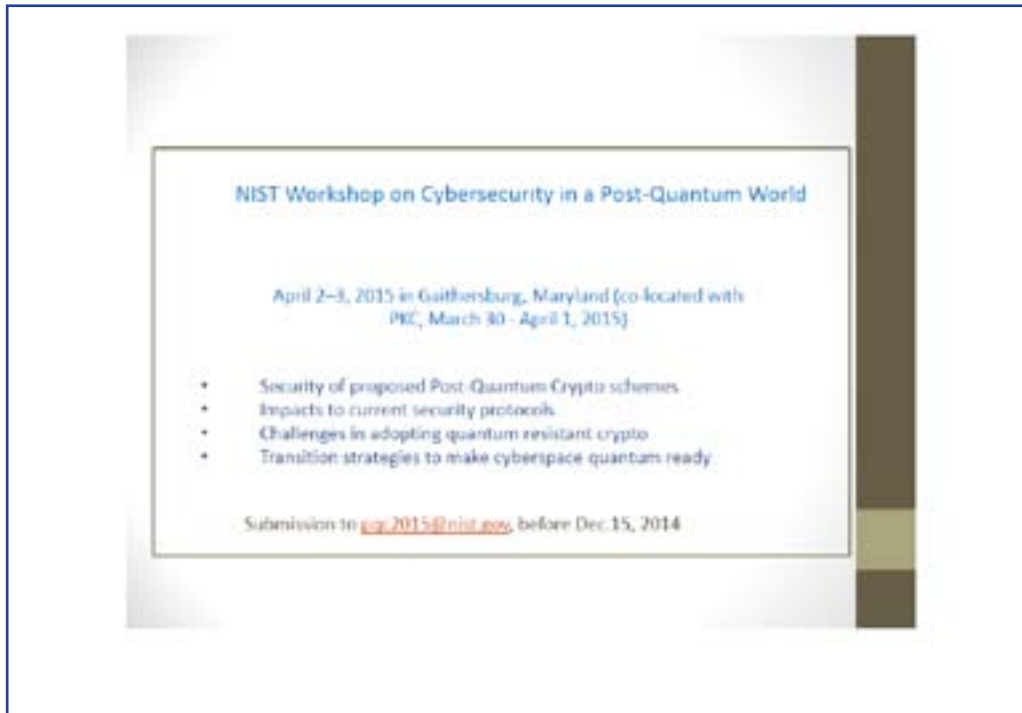
- High priority: Introduce quantum resistant schemes for key establishment
 - Early migration will provide backward security, i.e. keep confidentiality for the information protected by the old schemes
- For digital signature schemes used for entity authentication, backward security is not required
 - Move to quantum computing resistant signature schemes can identify practical impact
- One step migration is ideal, if we have mature candidates for both encryption (key exchange) and signature

How about Security?

- The security proofs for IKE and TLS were published after they have been deployed
 - with formalized assumptions on the underlying crypto schemes (and attack models)
- The results may not hold with the new schemes
 - That is, new schemes are based on new assumptions
- The security vulnerability may or may not be identified right away
- The extensive research can be motivated by the deployments
 - For possible vulnerabilities, early stage discovery is good and can avoid disasters
 - The current information system cannot afford disasters

Summary

- The security protocols shall not be considered as old wineskins
- The agility can be introduced, with certain effort
- The practical impact will be more clear when the new schemes are implemented in the protocols
- The trigger for more serious security analysis is the deployment
- We may not know every thing until the new schemes are plugged in
 - We do need to know something to start



Towards a standard for practical Hash-based Signatures

Andres Hülsing, Technische Universiteit Eindhoven

Variants of the Merkle scheme are promising candidates for quantum-safe digital signatures. An Internet-Draft on hash-based signatures was published last year [1]. It covers Merkle's traditional tree-based signature scheme, instantiated with Winternitz one-time signatures. Our talk presents this recent draft and motivates work on follow-up drafts. It is shown why it is important to standardize collision-resilient multi-tree schemes. The argument is backed up by performance figures keys and signature size, execution speed and additional security benefits achieved like forward-security and increased long-term security. As a preview, we also present first results for stateless hash-based signatures, overcoming a major practical hurdle of existing Merkle-based schemes.

[1] David McGrew, Michael Curcio. "Hash-Based Signatures".

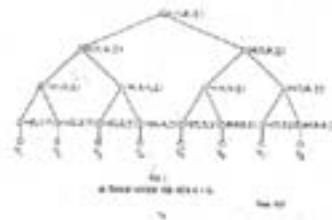
Internet-Draft, Version 02, Crypto Forum Research Group, IETF, 2014.

Available at <https://datatracker.ietf.org/doc/draft-mcgrew-hash-sigs/>



Hash-based Signature Schemes [Mor89]

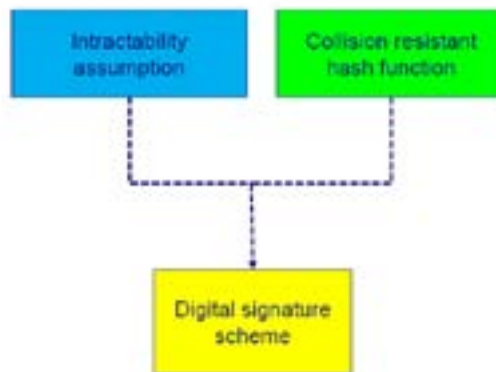
- Post quantum
- Only secure hash function
- Security well understood
- Fast



ALISON PHILLIPS

TU/e Technische Universiteit
Eindhoven
University of Technology

Security



ALISON PHILLIPS

TU/e Technische Universiteit
Eindhoven
University of Technology

Post-Quantum Security

n-bit hash function

Grover'96:

Preimage finding $O(2^n) \rightarrow O(2^{\frac{n}{2}})$

Brassard et al. 1998:

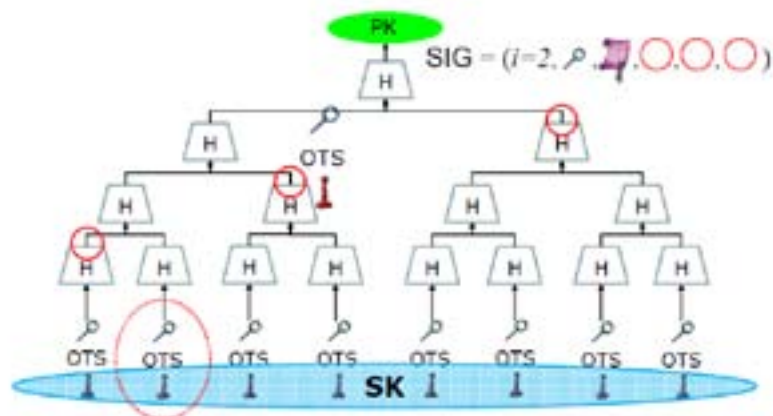
Collision finding $O(2^{\frac{n}{2}}) \rightarrow O(2^{\frac{n}{3}})$

Aaronson & Shi'04:

Quantum collision finding $2^{\frac{n}{3}}$ is lower bound

SLIDE PAGE 1

Merkle's Hash-based Signatures



SLIDE PAGE 2

Practical Challenge: Handle State

- Can be avoided in theory, paid with efficiency
- Different API
 - Handle integration
- Prevent copies
 - No key back-up
- Multi-threading safety
- Industry input appreciated

© ETSI 2019

TU/e Technische Universiteit
Eindhoven
University of Technology

McGrew & Curcio'2014



© ETSI 2019

TU/e Technische Universiteit
Eindhoven
University of Technology

McGrew & Curcio'2014

- Merkle Tree + Winternitz OTS
- Parameter Sets = Cipher Suites
- Security = collision resistance

4/22/24 PAGE 7

TU/e Technische Universiteit
Eindhoven
University of Technology

XMSS
eXtended Merkle Signature
Scheme

4/22/24 PAGE 8

TU/e Technische Universiteit
Eindhoven
University of Technology

Reduced Security Requirements

- Change WOTS -> WOTS+
- Change Tree

Security from second-preimage resistance
 ↓
 „Collision-resilient“ scheme
 ↓
 No birthday-attacks

TU/e Technische Universiteit
Eindhoven
University of Technology

Size reduction

Hash function $h: \{0, 1\}^* \rightarrow \{0, 1\}^m$

Assume:

- only generic attacks,
- security level n

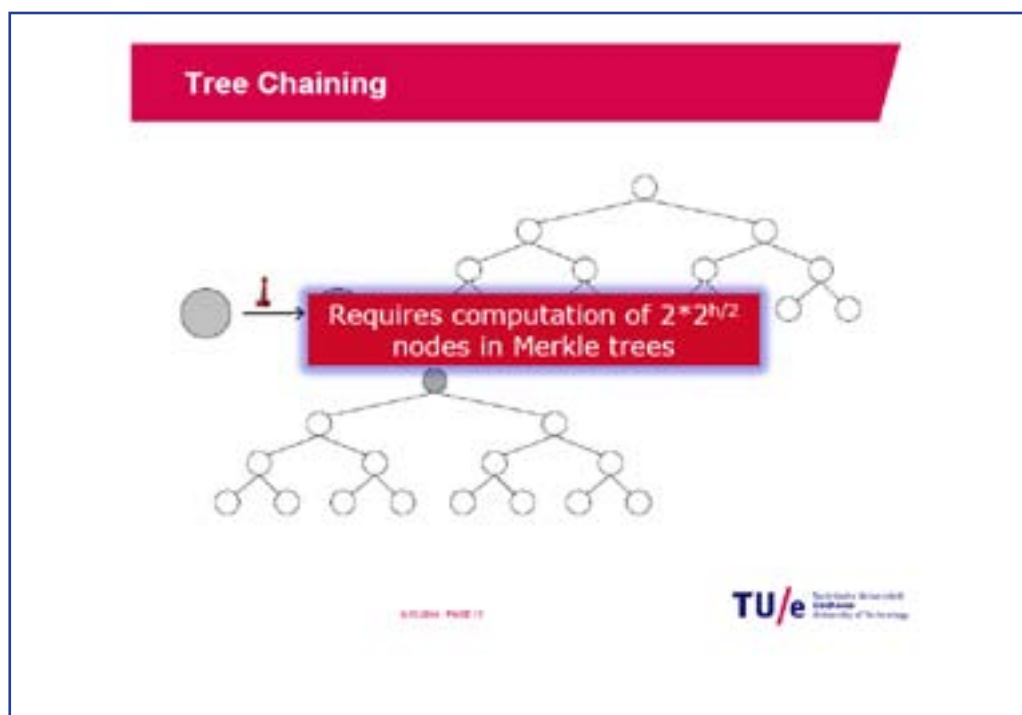
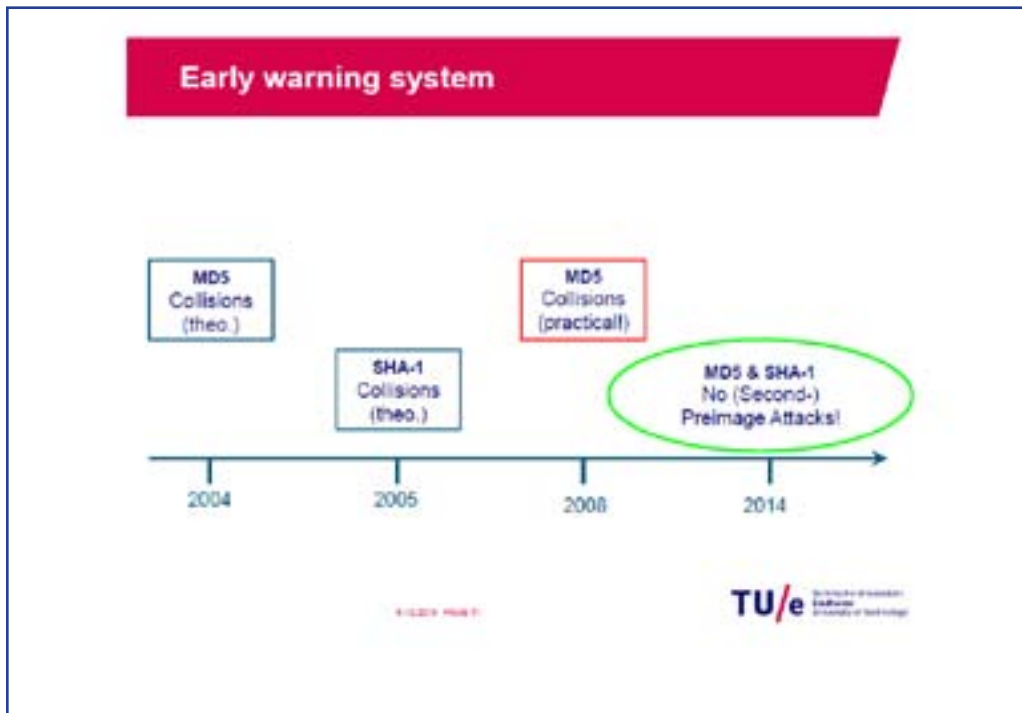
Collision Halfes Signature Size!

→ generic attack = birthday attack → $m = 2n$

Second-preimage resistance required:

→ generic attack = exhaustive search → $m = n$

TU/e Technische Universiteit
Eindhoven
University of Technology



Tree Chaining

- Can be extended to d layers
- Reduces signature and key generation time
- Necessary for smartcards & $h \gg 20$

© 2024 NXP B.V.

TU/e Technische Universiteit
Eindhoven
University of Technology

Tree Chaining

	Sign (ms)	Verify (ms)	Keygen (ms)	Signature (byte)	Public Key (byte)	Secret Key (byte)	Bit Sec.	Comment
SPHINX	134	23	925,489	2,308	800	2,418	92	$H = 15,$ $W = 9$
SPHINX*	106	20	5,689	3,476	544	3,160	94	$H = 15,$ $W = 4$
SSA 2048	190	7	11,090	≤ 256	≤ 512	≤ 512	97	

Infineon SLE78 16Bit-CPU@33MHz, 8KB RAM, TRNG, sym. & asym. co-processor

NVM: Card 16.5 million write cycles/ sector,
XMSS* < 5 million write cycles ($h=20$)

[HBB12]

© 2024 NXP B.V.

TU/e Technische Universiteit
Eindhoven
University of Technology

Forward Security

A SLIDE FROM E

TU/e Technische Universiteit Eindhoven University of Technology

Forward Security

A SLIDE FROM E

TU/e Technische Universiteit Eindhoven University of Technology

Requires special KeyGen

TU/e Technische Universiteit Eindhoven University of Technology

PoC Implementation

C Implementation, using OpenSSL [BDH2011]

	Sign (ms)	Verify (ms)	Signature (bit)	Public Key (bit)	Secret Key (byte)	Bit Security	Comment
SMSS-SHA-2	35.98	1.98	16,672	11,000	3,304	157	$k = 20$, $w = 64$
SMSS-AES-62	8.52	6.67	16,616	7,328	1,654	64	$k = 20$, $w = 4$
SMSS-48%	1.96	0.11	16,616	7,328	1,654	64	$k = 20$, $w = 4$
SSA 2018	3.09	6.09	≤ 2,048	≤ 4,096	≤ 512	87	

Intel(R) Core(TM) i5-2520M CPU @ 2.50GHz with Intel AES-NI

TU/e Technische Universiteit Eindhoven University of Technology

Conclusion

- Current draft: Great first step

... BUT ...

- XMSS: Additional important features
 - More efficient
 - Stronger Security Guarantees
 - Forward-security

Add-on to draft required.

4/12/14 10:52:11

TU/e
Technische Universiteit
Eindhoven
University of Technology

Thank you!
Questions?



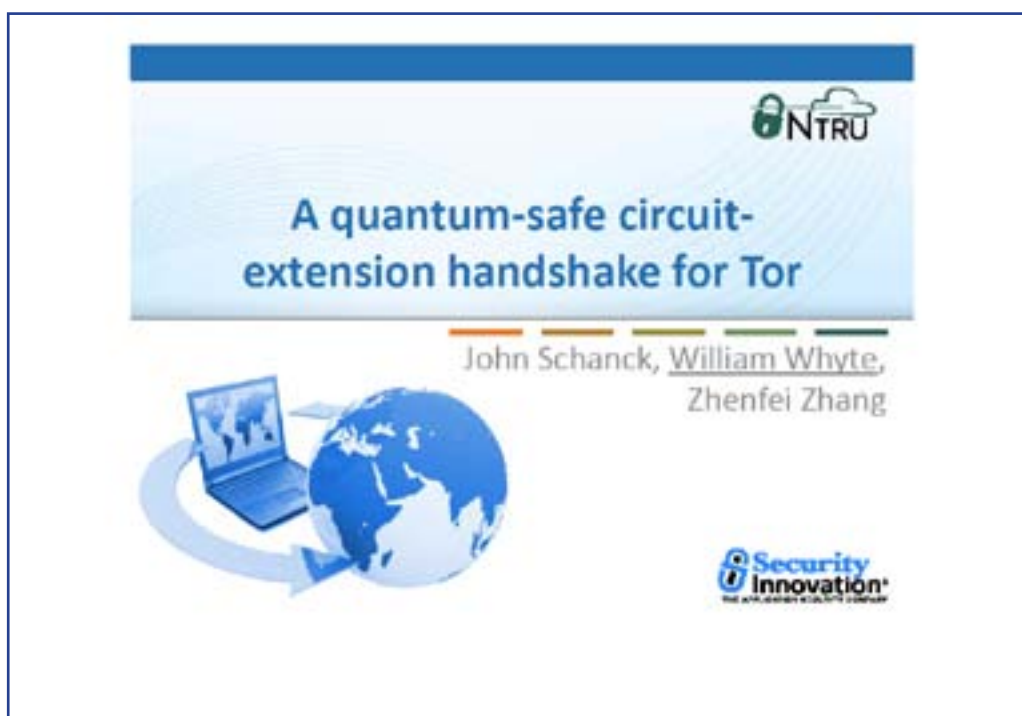
4/12/14 10:52:11

TU/e
Technische Universiteit
Eindhoven
University of Technology

PQTor: Integrating quantum-safe cryptography into Tor*William Whyte, Security Innovation*

We propose a method for integrating NTRUEncrypt into the ntor key exchange protocol as a means of achieving quantum-resistance. The proposal is a minimal change to ntor, essentially consisting of an NTRUEncrypt-based key exchange performed in parallel with the ntor handshake. Performance figures are provided demonstrating that the client bears most of the additional overhead, and that the added load on the router side is acceptable. We also analyze the security model and explain why the more heavyweight approach to multiple encryption of Dodis and Katz is unnecessary in this setting.

We make this proposal for two reasons. First, we believe it to be an interesting case study into the practicality of quantum-safe cryptography and into the difficulties one might encounter when transitioning to quantum-safe primitives within real-world protocols and code-bases. Second, we believe that Tor is a strong candidate for an early transition to quantum-safe primitives, as its users may be justifiably concerned about adversaries who record traffic in the present and store it for decryption when technology or cryptanalytic techniques improve.



Key exchange protocols

- Allow two users to agree keying material without an existing shared secret

Alice	Bob
Agree G, G	
$a \leftarrow \text{rand } \mathbb{Z}_G$	$b \leftarrow \text{rand } \mathbb{Z}_G$
$A = aG$	$B = bG$
A \rightarrow	
\leftarrow B	
$S = abG = abG$	$S = baG = abG$
$K = \text{KDF}(S, \dots)$	$K = \text{KDF}(S, \dots)$

Unauthenticated Diffie-Hellman



Key exchange protocols

- Properties can include
 - One-way or mutual authentication
 - Anonymity
 - Forward secrecy
- Rely on public key cryptography for confidentiality and authentication

Alice	Bob
Agree G, G	
$a \leftarrow \text{rand } \mathbb{Z}_G$	$b \leftarrow \text{rand } \mathbb{Z}_G$
$A = aG$	$B = bG$
Publish A, B in authenticated way	
$x \leftarrow \text{rand } \mathbb{Z}_G$	$y \leftarrow \text{rand } \mathbb{Z}_G$
$X = xG$	$Y = yG$
X \rightarrow \leftarrow Y	
$S1 = aY = ayG$	$S1 = yA = ayG$
$S2 = xB = xbG$	$S2 = bX = xbG$
$K = \text{KDF}(S1, S2, "A", "B", \dots)$	$K = \text{KDF}(S1, S2, "A", "B", \dots)$

KEA+: Two-way authenticated Diffie-Hellman with F



Key transport

- Alternative to key exchange
- Only one side contributes secret randomness
 - Not clear this is a problem, but it can be fixed if so
- Traditionally has been hard to provide forward secrecy due to long keygen times for public key encryption algorithms
 - i.e. RSA
 - Modern public key encryption algorithms don't have this drawback

Alice	Bob
Agree P	
$(b, B) \leftarrow \text{rand}$ Keygen (P)	
Publish B in authenticated way	
$S \leftarrow \text{rand} (1^k)$ $c = \text{Encrypt}(B, S)$	
$c \rightarrow$	
$K = \text{KDF}(S, "B", \dots)$	$S = \text{Decrypt}(b, c)$ $K = \text{KDF}(S, "B", \dots)$

Key Transport

Tor

- Allows for improved privacy for internet connections
 - Web browsing
- Run through a series of volunteer relays
- Increased interest following Snowden revelations
 - Firefox “may consider including” in future version (2014-10-01)



Tor encryption

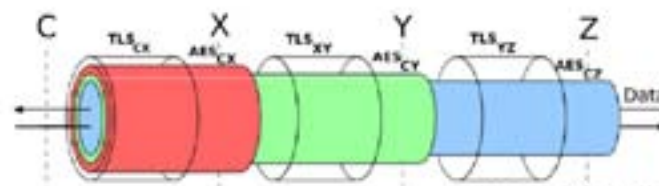


Illustration 2: Tor Encryption

Image courtesy of Steven Murdoch



Tor circuit extension

- Client has Tor circuit through to node N1, wants to extend to node N2
- Uses existing Tor circuit to contact N2 and establish keying material
 - N1 is aware that circuit extension handshake is going on
 - N1 & N2 have mutually authenticated TLS connection
- N2 authenticates, client is (naturally) anonymous
- Different handshake protocols have been used in practice, current is ntor



ntor

- Designed to be as efficient as possible
- Instantiated with curve25519 for key exchange
- Authenticated publication = signing with self-certified long-term key

Client	Node
G, G given as system parameters	
$b \leftarrow \text{rand} @G$	
$B = bG$	
Publish B in authenticated way	
$x \leftarrow \text{rand} @G$	$y \leftarrow \text{rand} @G$
$X = xG$	$Y = yG$
$X \rightarrow$	
$S1 = yX \parallel bX$	
$\leftarrow Y$	
$S1 = xY \parallel xB$	
$K = \text{KDF}(S1, "R", X, Y, \dots)$	

ntor

How long do your secrets need to live?

- If you send something now...
 - Encrypted with an algorithm that's later broken...
 - And someone's stored your message...
 - They can decrypt it
- Encryption needs to take into account the lifetime for which your data might remain sensitive
- Attacker who doesn't actively get involved at the time of the interaction, but passively records traffic for later analysis
- Fits known attacker pattern
- Attacks:
 - Quantum computing
 - Other yet-to-be-discovered classical



Why choose NTRU?

- **Small Footprint**
 - Tiny compiled code (8 kb), ideal for embedded and mobile devices
- **Highest Performing**
 - 5 to 200 times faster than RSA and ECC at equivalent security levels
 - Consumes minimal CPU and battery resources
- **Most Secure**
 - Resistant to all known Quantum Computing attacks
 - The higher level of security, the higher performance gains versus competition
 - Ideal for systems where users expect data to remain encrypted for 10+ years
 - Open source code
- **Implementations**
 - NTRU in SSL for embedded systems or web application
 - NTRU SDK for C/C++ or Java



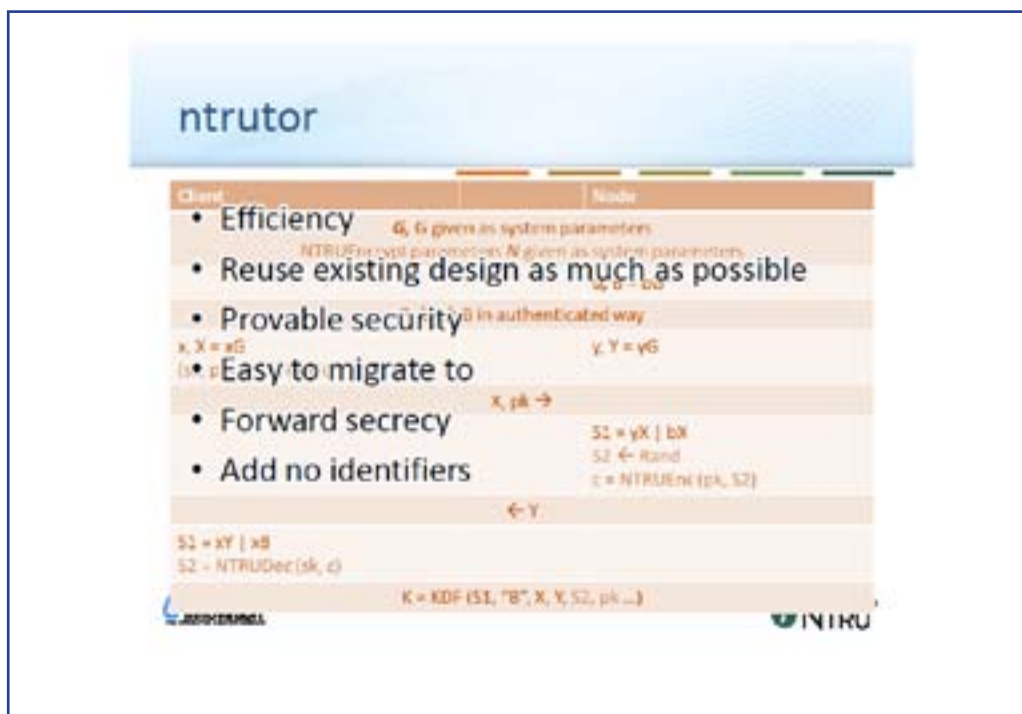
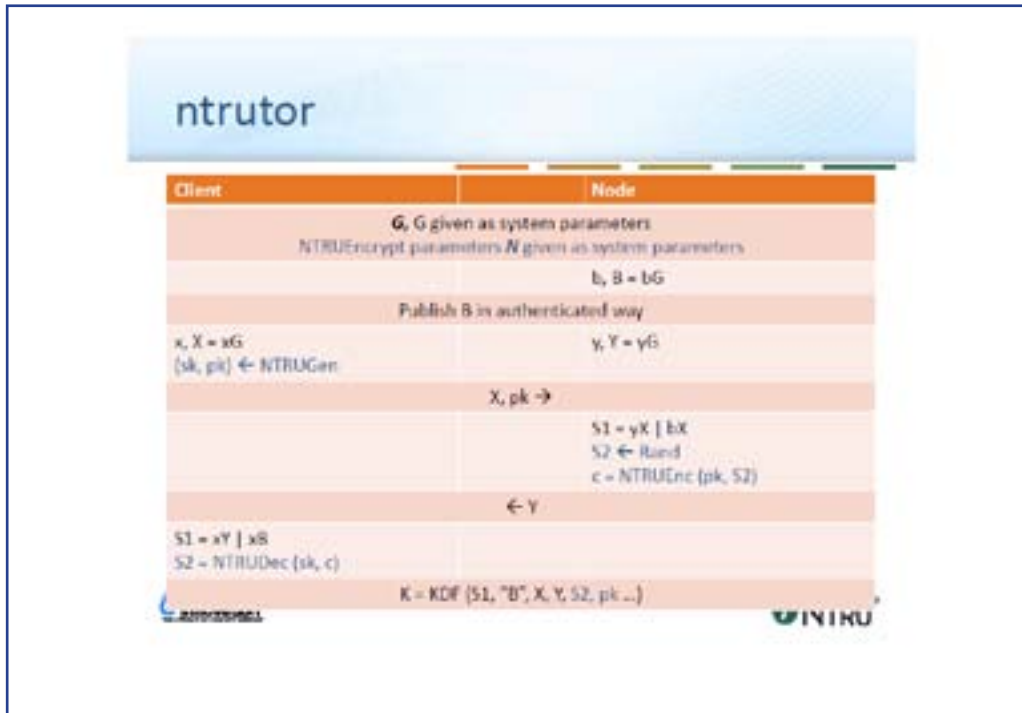
Open Source GPL v2 available at:
[GitHub.com/NTRUOpenSourceProject](https://github.com/NTRUOpenSourceProject)



Post-quantum circuit extension: goals

- Efficiency
- Reuse existing design as much as possible
- Provable security
- Easy to migrate to
- Forward secrecy
- Add no identifiers





Performance

	TAP	ntru	ntruoe
Client → server bytes	186	84	693
Server → client bytes	148	64	673
Client comp. 1	280 μs	84 μs	272 μs
Server comp.	771 μs	263 μs	307 μs
Client comp. 2	251 μs	180 μs	223 μs
Total comp. time	1302 μs	527 μs	802 μs
Server + client 2	1022 μs	443 μs	530 μs

- Note that client sees bulk of the delta due to keygen – appropriate given Tor setup



Security arguments

- Two different settings
 - Active attacker, want to show that system is as secure as the stronger of either so long as auth succeeds: "active classical adversary"
 - Passive attacker, want to show that system is as strong as NTRU: "passive quantum adversary"
- Security against active classical adversary:
 - If authentication is not compromised, confidentiality is at least as strong as the stronger of the two algorithms
 - Shown by standard reduction proof: if one key exchange algorithm is assumed weak, a breaker for the protocol has an efficient mapping to a breaker for the remaining key exchange algorithm
- Security against passive quantum adversary:
 - Confidentiality is as strong as NTRU
 - Shown by standard reduction as above



Implementation issues

- This can't simply be implemented as written
 - Problems:
 - Tor packets are limited to 512 bytes
 - Tor handshake messages are limited to one packet
 - Solutions:
 - Change one of the above
 - Both have been discussed within the Tor project in other contexts
- Is this the correct approach?
 - Should there instead be a handshake for ntor + QuantumSafeKE with identifier for different QuantumSafeKE algorithms?
 - More modular, allows other quantum safe algorithms to be implemented straightforwardly
 - Tor has 2^{16} handshake type identifiers but has only allocated 3, and one is "reserved" for test purposes



Deployment

- Needs two Tor proposals
 - One to change handshake size
 - One to add the protocol
- Code will integrate quickly into main Tor path if and when change proposals are discussed and accepted within Tor project



Conclusions

- Quantum safe Tor handshake is practical
 - Without any compromise on current security
 - Without significantly increasing performance burden on relays
 - While preserving forward secrecy against a passive eavesdropper
 - With provable security
- When deploying systems with new algorithms, often the most difficult part is not the crypto but
 - Protocol issues
 - Deciding to make the jump
- These lessons apply beyond the context of Tor



**Traceable characterisation of the optical components of faint-pulse QKD systems-
results from the Metrology for Industrial Communications (MIQC) project**

Christopher Chunnillall, National Physics Laboratory (UK)

The lack of validation and standardisation is a barrier to the wider commercialisation of QKD. A joint research project [1] has developed measurement techniques to underpin standards for specifying and validating faint-pulse QKD implemented over fibre, the most commercially advanced QKD technology.

These systems typically use phase encoding in the 1550 nm telecom band. Key components of the transmitter are an attenuated pulsed laser, an interferometer, and intensity and phase modulators. Those of the receiver are gated photon counting detectors, an interferometer, and a phase modulator. Random-number generators are essential components of both modules.

Developing techniques traceable to the SI for characterising the performance of these components, which can affect security and/or efficiency, was the focus of this project. Key parameters identified for characterisation were: (transmitter) clock frequency, photon number distribution and mean photon number(s), timing jitter, wavelength, spectral line width, spectral and temporal indistinguishability; (receiver) photon detection probability, dark count probability, afterpulse probability, dead time, recovery time, maximum count rate, timing jitter and spectral responsivity.

An overview of the project, and a review of its achievements, will be presented. The latter includes new quantum measurement techniques and devices, as well as work to characterize an open-system quantum random-number generator.

[1] The Metrology for Industrial Quantum Communications (MIQC) project IND06 was funded under the European Metrology Research Programme (EMRP) from September 2011 to August 2014. The partners were: the National Measurement Institutes of the Czech Republic (CMI), Estonia (Metrosert), Finland (MIKES), Germany (PTB), Italy (INRIM) (co-ordinator), the United Kingdom (NPL), and South Korea (KRISS); idQuantique; the Austrian Institute of Technology (AIT); Aalto University; Oulu University; and the Polytechnic of Milan. The EMRP is jointly funded by the EMRP participating countries within EURAMET and the European Union.

<http://projects.npl.co.uk/MIQC/>



Traceable characterisation of the optical components of faint-pulse QKD systems – results from the Metrology for Industrial Communications (MIQC) project

Christopher Chunnillal
christopher.chunnillal@npl.co.uk

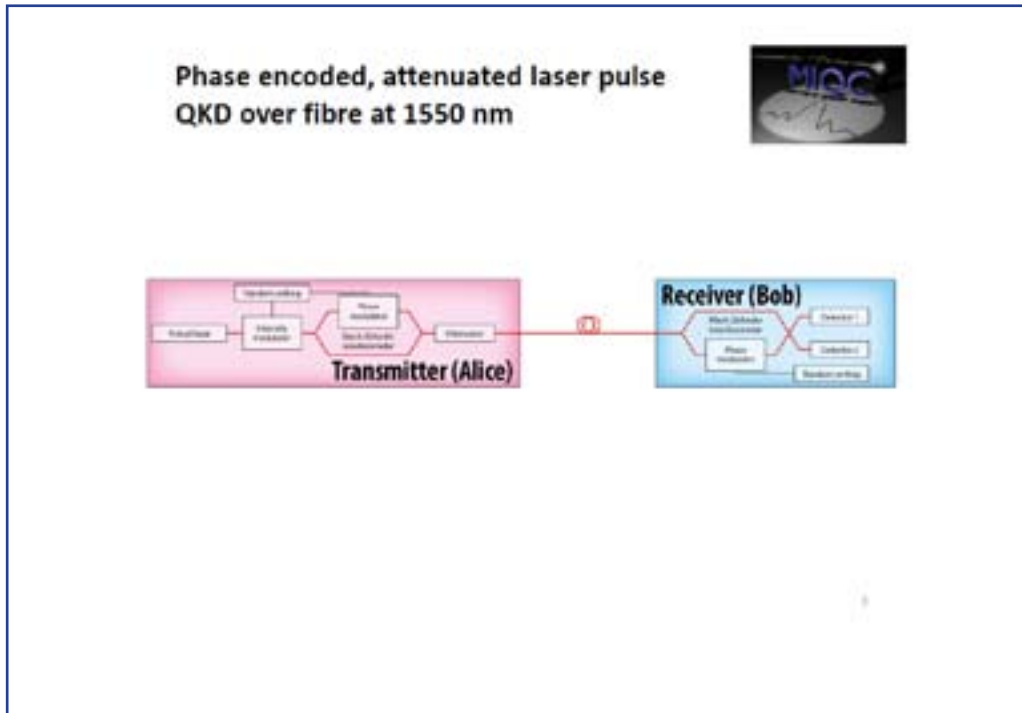
ETSI/IQC Quantum-Safe-Crypto-Workshop
Ottawa, Canada
8 October 2014

IND06: Metrology for Industrial Quantum Communications

<http://www.miqc.org/>




- Objective : to develop a pan-European measurement infrastructure to develop standards and characterisation facilities for commercial Quantum Key Distribution (QKD) devices.
- Independent physical characterisation to demonstrate that the technology is working within specification
- Focus on faint-pulse (weak coherent pulse) QKD over fibre at 1550 nm
- 3 year project
- Sept 2011 – Aug 2014






Key Measurement Outputs of MIQC

Phase encoded, attenuated laser pulse QKD over fibre at 1550 nm






- Photon emitters**
Traceable characterisation of commercial QKD sources:
 - Attenuated laser pulses, phase encoding
- Quantum channel (optical fibre)**
 - Traceable characterisation of single mode optical fibre
 - Characterisation of propagation of photon state in single mode fibre
- Random number generator (IdQuantique)**
 - Open system true physical random number generator (TRNG)
 - Physically characterised and tested under different operating conditions
- Photon receivers**
Traceable calibration of commercial QKD receivers:
 - Gated photon counting detectors




Primary properties requiring characterisation


- Mean photon number
- Probability distribution Time-topology photon number resolving detector
- Temporal pulse jitter, duration
- Wavelength
- Spectral bandwidth
- Spectral indistinguishability High-resolution single-photon spectrometer




- Spectral attenuation
- Chromatic dispersion
- Optical length
- Back-scatter
- Polarisation mode dispersion, dependent loss, decoherence
- Wavelength multiplexed fibre links

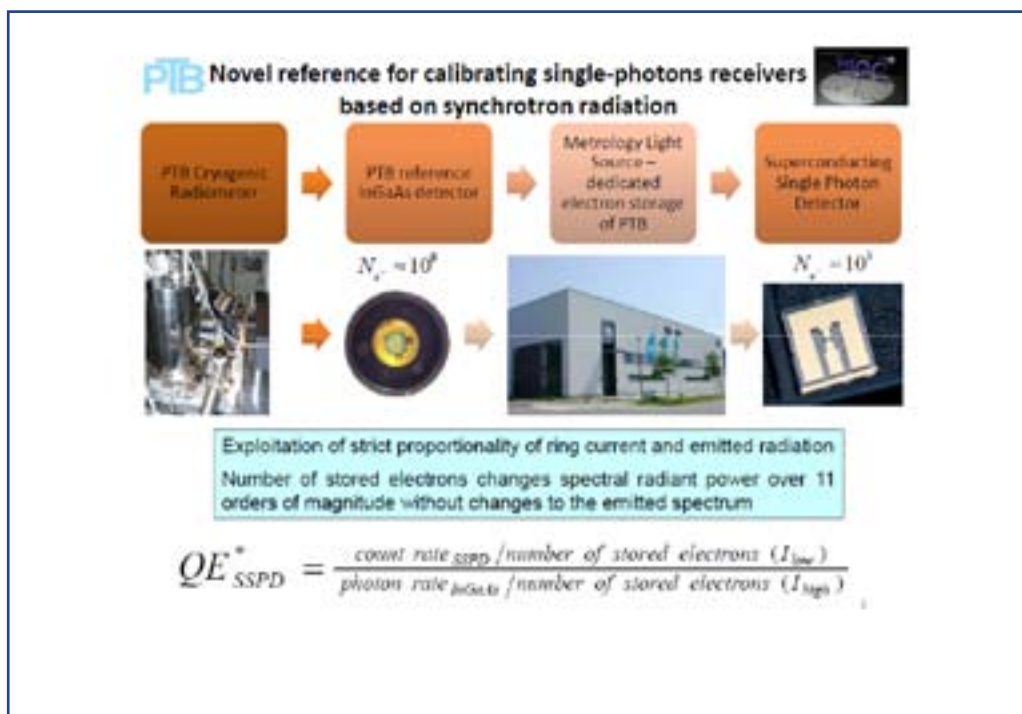
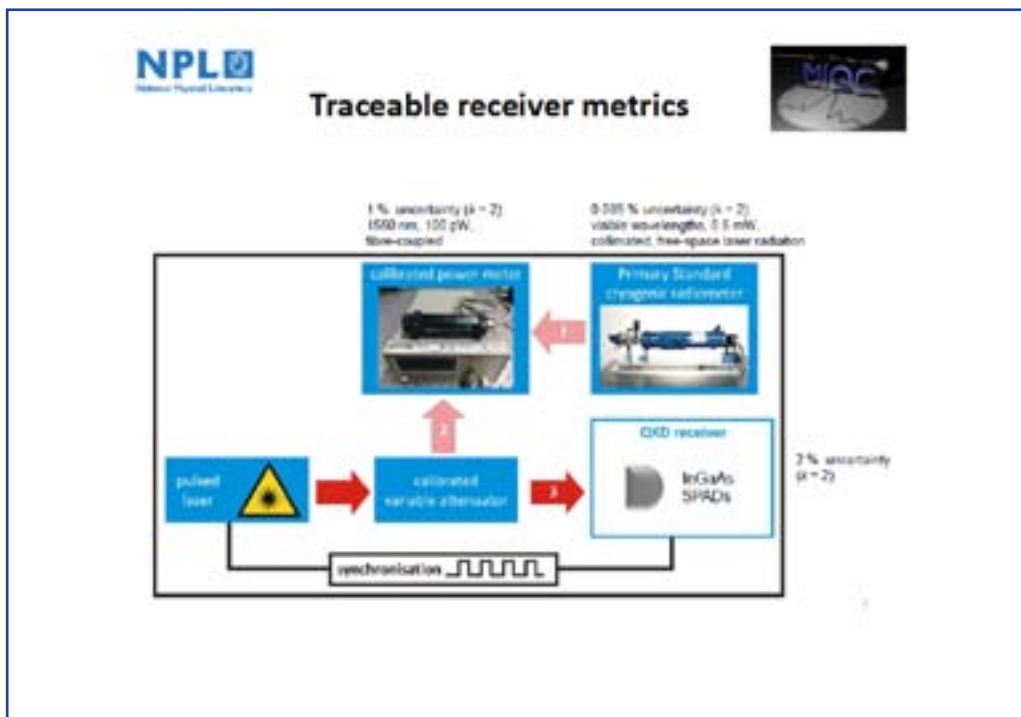
- Detection efficiency Calculable, scalable light source (synchrotron)
- Detection linearity Telecom wavelength attenuator
- Dark count probability
- After-pulse probability
- Deadtime and recovery time
- Temporal jitter
- Back flash
- Detector indistinguishability (multi-detector receiver)

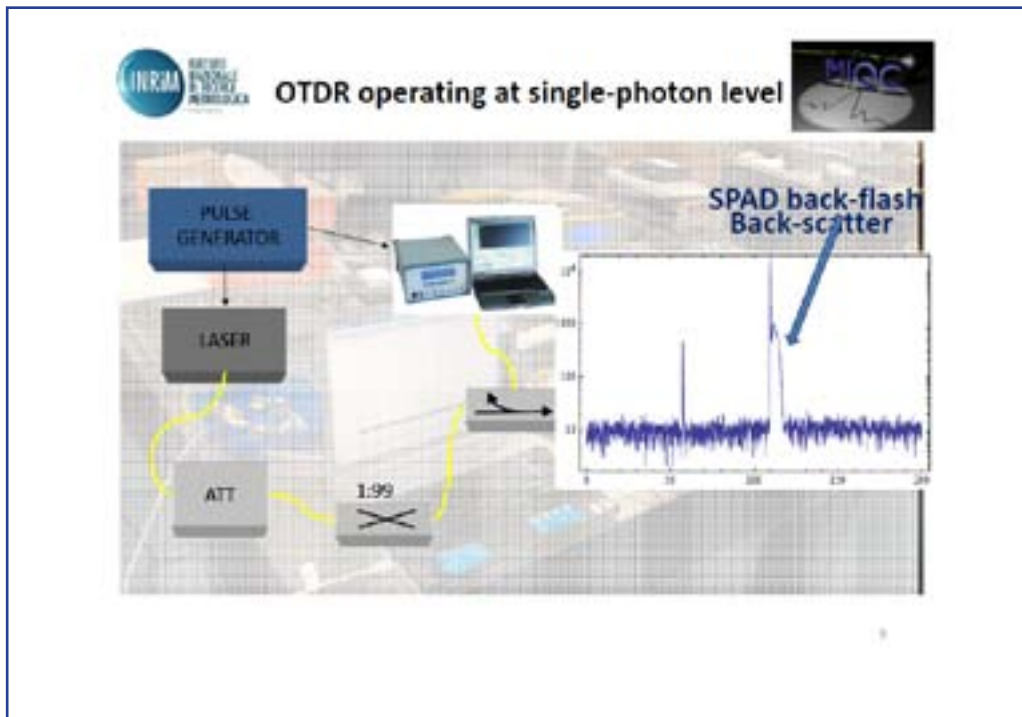




Detector characterisation (gated detector)







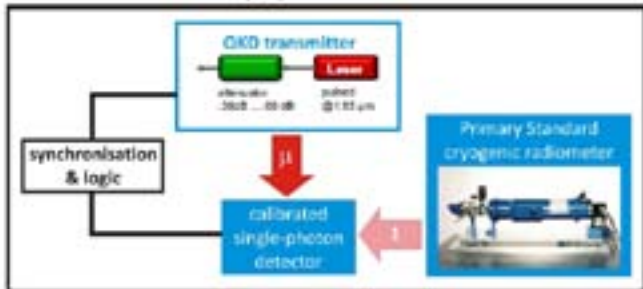


**Source characterisation
(pulsed sources)**

A photograph showing a pulsed source characterization setup, including a laser, attenuator, and detector.


NPL Source photon number statistics  

a) Calibrated detector and commercial attenuator



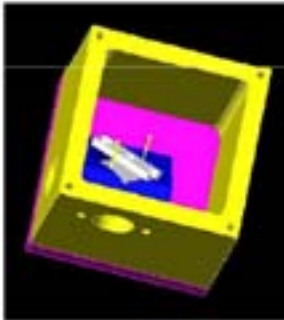
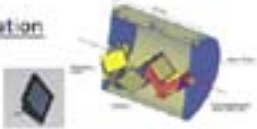

1% uncertainty (k=2)

2% uncertainty (k=2)




Source photon number statistics 

b) Calibrated detector and traceable attenuator based on InGaAs photodiodes

Attenuator based on transmission trap detector configuration

Current attenuation $\sim 6 \times 10^4$ @ 1.55 μm

Source photon number statistics

c) Reconstruction of probability distribution

"ON/OFF" Tomography

For on/off detectors like SPAD with quantum efficiency η , the probability of no-clicks is:

$$p_0(\eta) = \sum_{n=0}^{\infty} (1-\eta)^n \rho_n = \sum_{n=0}^{\infty} A_n(\eta) \rho_n$$

-Truncating the p.d. to a certain N
-Changing the value of the quantum efficiency η_μ

Photos number distribution $\rho_n \equiv \rho_{nn}$

Source photon number statistics

d) PNR detector based on tree configuration

Deconvolving the p.d. of incoming photons

Detector Tree: 4 click/no-click detectors

- Novel [entanglement-assisted] quantum characterisation technique for PNR detector
Orús et al., PRL 108, 253601 (2012)
- By measuring higher-order $g^{(n)}$, it is possible to deconvolve the underlying number and kind (poissonian, pseudo-thermal or single-photon) of occupied modes of a light field.
Goldschmidt et al., PRA 88, 013822 (2013)

$$g^{(2)}, g^{(3)}, g^{(4)} \quad g^{(n)} = \frac{P(n)}{[P(1)]^n}$$

NPL

Source Spectrum

Tunable single-photon spectrometer

- Operating range 1270 → 1630 nm
- FSR = 119 GHz, $\Delta\nu_{\text{cavity}} = 600$ MHz
- Low drift rate & single-photon sensitivity
- Tune to resonance and scan across QKD source spectrum
- Can be used to analyse different source encoding spectra
- Technically challenging to improve spectral resolution

active research
www.ect.ac.uk/research/au

Four on-demand web lectures discussing basic aspects of QKD

- "Introduction to QKD" by Momchil Peev, AIT (Austria)
- "Practical QKD systems" by Grégoire Ribordy, ID Quantique (Swiss)
- "Security of QKD systems" by Norbert Lütkenhaus, Univ. of Waterloo (Canada) & Vadim Makarov, Univ. of Waterloo (Canada)
- "Metrology for QKD" by Christopher Chunnell, NPL (UK)

Summary

- Methods developed to address the measurement requirements required of QKD (benign environment)
- These include new, beyond state-of-the-art, methods and instruments

- Close interaction with ETSI QKD-45G
- 14 peer-reviewed papers, plus 7 accepted for publication
- 55 presentations at meetings and conferences
- 4 on-line web-lectures
- Best practice guide
- Project website: <http://www.miqc.org>
- Continue to take this work into future – MIQC2?

The MIQC-project: Metrology for Industrial Quantum Communications

M L Rastello, I P Degiovanni, G Brieda

S Kück, I Müller, R Klein

A Vaigu, F Manaccheri, E Ilkkanen

D Stucki

K S Hong

A G Sinclair, C J Chunnifall, J Y Cheung

G Porrovecchio, M Smid

T Kubarsepp

A Tosi

A Al Natsheli

Further metrology ... MIQC2? 

- MIQC is just the beginning ...
 - Metrology for side-channel and Trojan-horse attacks, and their countermeasures
 - Free-space QKD (visible wavelengths)
 - Other protocols, e.g. entanglement-based
 - ...

MIQC1 Consortium +  **TOSHIBA**
Leading Innovation >>>

23



Thank you!

<http://www.miqc.org>

24

Multivariate Quadratic Challenge

Takanori Yasuda, ISIT

In this talk, we report on the activities of a research project concerning multivariate public key cryptosystems carried out in Japan. The Principal investigator, Takanori Yasuda (ISIT) is a researcher working on multivariate public key cryptosystems [3],[4],[5]. Kouichi Sakurai (Kyushu University), Tsuyoshi Takagi (Kyushu University) and Xavier Dahan (ISIT) are the collaborators of the project. Our research team is leading the research in multivariate public key cryptography in Japan in recent years.

We have been conferred a three years research program, until March 2016, by the Ministry of Internal Affairs and Communications in Japan to study multivariate public-key cryptosystems towards its standardization as a candidate for Post-Quantum cryptography. The project belongs to the Strategic Information and Communications R&D Promotion Programme (SCOPE), under which large-scale projects in telecommunication chosen after a selection process get funded. This follows a preliminary project started one year and half ago, which aims to establish a Post-Quantum research Hub in Japan, during which two workshops in relation with this theme were held [1],[2].

In this new phase of the program, we plan to test various parameters of cryptosystems/signature schemes based on multivariate polynomials, by measuring speed of encryption and decryption, as well as testing the resistance to best known attacks. The aim is to define parameters that can be safely recommended in a standardization process. To this end, we plan to setup a contest, « MQ challenge » for solving quadratic multivariate polynomial systems. During the presentation, along with introducing the MQ challenge and the infrastructure that we plan to acquire for achieving this aim, we would explain the different aspects of a governmental project related to Post-Quantum cryptography.

[1] Forefront Workshop for the Promotion of the Academia-Industry Cooperation “Application of Computational Number Theory to Secure Social Infrastructure (II)- Solving Multivariate Polynomial Systems and Related Topics -”

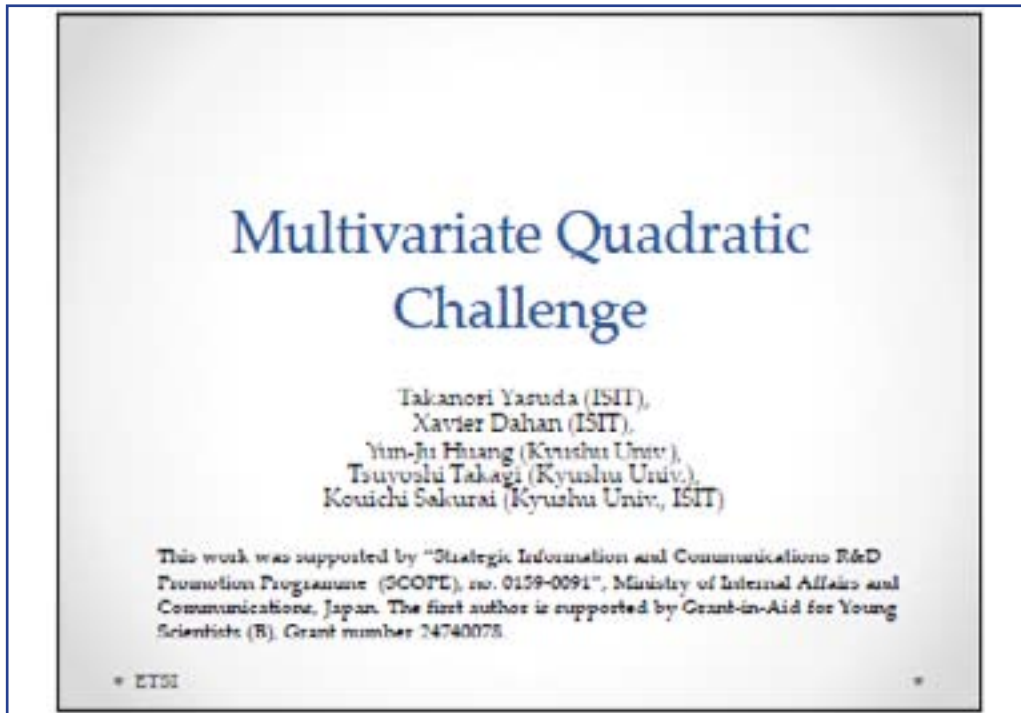
<http://www.isit.or.jp/lab2/2013/01/17/multivariate-polynomial-workshop/>

[2] Workshop: Post-Quantum Cryptography and Its Related Topics <http://www.isit.or.jp/lab2/2013/11/28/post-quantum-cryptography-workshop/>

[3] Takanori Yasuda, Kouichi Sakurai, “A security analysis of uniformly-layered Rainbow --- Revisiting Sato-Araki’s non-commutative approach to Ong-Schnorr-Shamir signature towards PostQuantum Paradigm ---”, PQCrypto’11, Springer LNCS vol. 7071, pp. 275–294, 2011.

[4] Takanori Yasuda, Kouichi Sakurai, Tsuyoshi Takagi, “Reducing the Key Size of Rainbow using Non-commutative Rings”, CT-RSA’12, Springer LNCS vol. 7178, pp. 68–83, 2012.

[5] Takanori Yasuda, Tsuyoshi Takagi, Kouichi Sakurai, “Multivariate Signature Scheme Using Quadratic Forms”, PQCrypto2013, Springer LNCS vol. 7932, pp. 243–258, 2013.



**Multivariate Quadratic
Challenge**

Takanori Yasuda (ISIT),
Xavier Dahan (ISIT),
Yim-Ji Hwang (Kyushu Univ.),
Tsuyoshi Takagi (Kyushu Univ.),
Kouichi Sakurai (Kyushu Univ., ISIT)

This work was supported by "Strategic Information and Communications R&D Promotion Programme (SCOPE), no. 0159-0091", Ministry of Internal Affairs and Communications, Japan. The first author is supported by Grant-in-Aid for Young Scientists (B), Grant number 24740075.

• ETSI



Contents

1. Multivariate Public Key Cryptosystems(MPKC)
 1. Fundamental structure
 2. Encryption
 3. Signature
2. MQ challenge
 1. Motivation
 2. Theoretical complexity
 3. Our construction of problems
 4. How to describe problem and answer
3. Conclusion

• ETSI Quantum Safe Workshop

2014/10/6 •

Multivariate Public Key Cryptosystem (MPKC)

- **Advantage**
 - Candidate for post-quantum cryptography
 - Used for both encryption and signature schemes
 - Encryption: Simple Matrix scheme (ABC scheme), ZHFE scheme
 - Signature: UOV, Rainbow
 - Efficient encryption and decryption and signature generation and verification.
- **Problems**
 - Exact estimate of security of MPKC schemes
 - Huge length of secret and public keys in comparison with RSA
 - New application and function

• ETSI Quantum Safe Workshop
2014/10/4 •

MQ problem

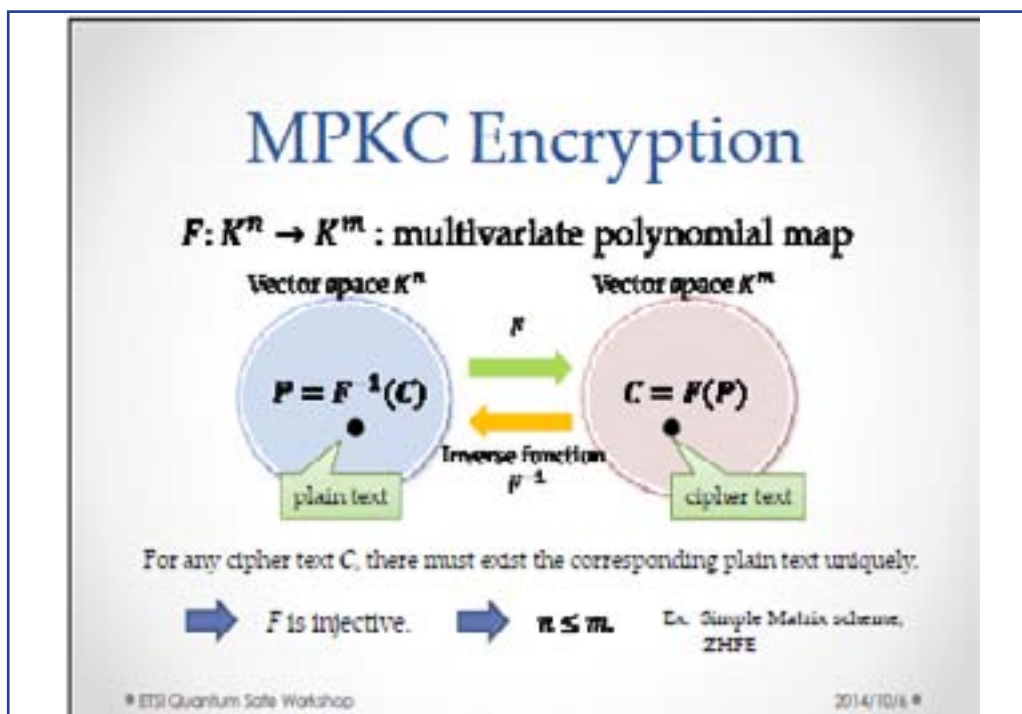
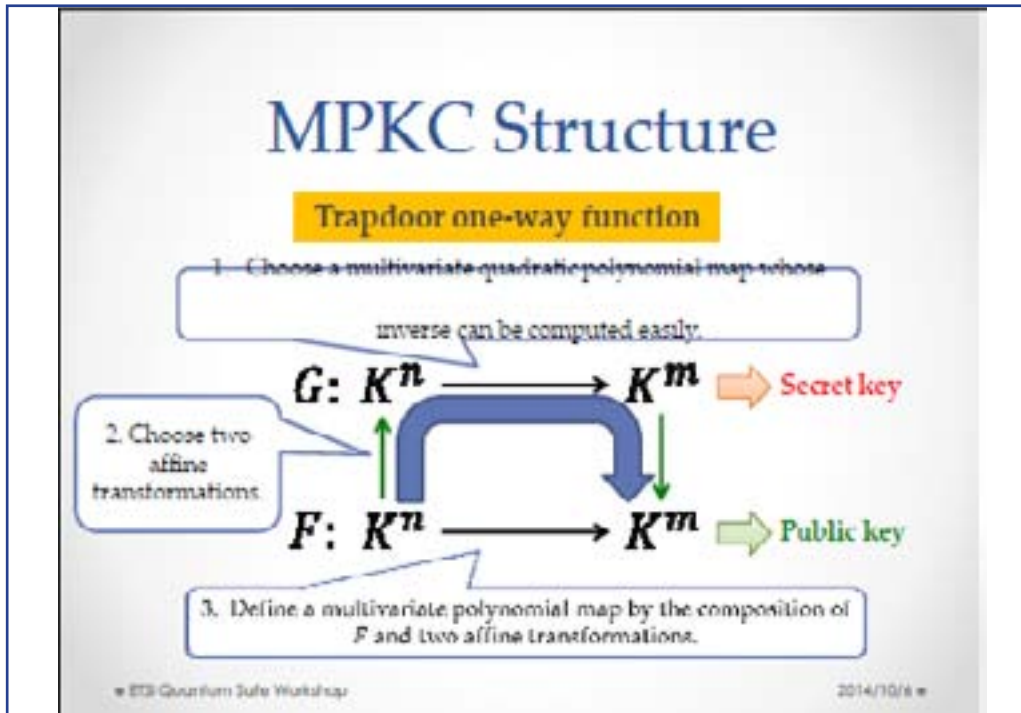
MPKC are public key cryptosystems whose security depends on the difficulty in solving a system of multivariate quadratic polynomials with coefficients in a finite field K .

MQ problem: find a solution of the system of multivariate equations.

$$\begin{cases} f_1(x_1, \dots, x_n) = \sum_{1 \leq i, j \leq n} a_{ij}^{(1)} x_i x_j + \sum_{1 \leq i \leq n} b_i^{(1)} x_i + c^{(1)} = d_1 \\ f_2(x_1, \dots, x_n) = \sum_{1 \leq i, j \leq n} a_{ij}^{(2)} x_i x_j + \sum_{1 \leq i \leq n} b_i^{(2)} x_i + c^{(2)} = d_2 \\ \vdots \\ f_m(x_1, \dots, x_n) = \sum_{1 \leq i, j \leq n} a_{ij}^{(m)} x_i x_j + \sum_{1 \leq i \leq n} b_i^{(m)} x_i + c^{(m)} = d_m \end{cases}$$

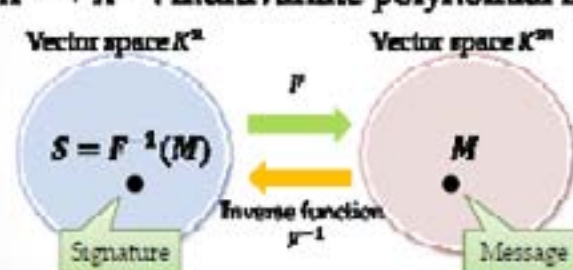
It is believed that it is difficult to solve (general) MQ problem.

• ETSI Quantum Safe Workshop
2014/10/4 •



MPKC Signature

$F: K^n \rightarrow K^m$: multivariate polynomial map



For any message M , there must exist the corresponding signature.

➔ F is surjective ➔ $n \geq m$ Ex. UOV, Rainbow

• ETSI Quantum Safe Workshop
2014/10/6 •

Necessity of MQ challenge

- Several public key cryptosystems held contests which solve the associated basic mathematical problems.
 - RSA challenge(RSA Laboratories), ECC challenge(Certicom), Lattice challenge(TU Darmstadt)
- Lattice challenge (<http://www.latticechallenge.org/>)
 - Target: Short vector problem
 - 2008 – now continued
- MPKC also need to evaluate the current state-of-the-art in practical MP problem solvers.

We are planning to hold MQ challenge.

• ETSI Quantum Safe Workshop
2014/10/6 •

Gröbner basis attack

A fundamental tool for solving MQ problem is Gröbner basis. Faugère proposed efficient algorithms as F_4 and F_5 to improve original algorithm [1][2].

Complexity for solving MQ problem [3]

$$O\left(m \cdot \binom{n + d_{reg}}{d_{reg}}\right)^\omega$$

where $2 < \omega < 3$, and d_{reg} is an invariant determined by the multivariate polynomial system.

References:

[1] Faugère, J.C., A New Efficient Algorithm for Computing Gröbner Bases (F4), *Journal of Pure and Applied Algebra*, vol. 139, 1999.

[2] Faugère, J.C., A New Efficient Algorithm for Computing Gröbner Bases (F5), *ISSAC, ACM press*, 2002.

[3] Bettale, L., Faugère, J.C. and Perret, L., Hybrid approach for solving multivariate systems over finite fields*, *J. Math. Crypt.*, vol. 2, 2008.

© ETSI Quantum Safe Workshop 2014/10/6

Encryption and Signature

- **Encryption**
 - Simple matrix scheme (ABC scheme), ZHFE, ...
 - Many encryption schemes use systems of $n \leq m$.
 - Solving system of $n \leq m$ can be reduced to solving system of $n = m$.

- **Signature**
 - UOV, Rainbow, ...
 - Rainbow is the multilayered UOV.
 - In Rainbow, parameters $n \approx 1.5m$ are often used.

- In MPKC schemes, finite fields with small size is used.
 - Finite field with small size has an efficient arithmetic.
 - We narrow to $GF(2^8)$, $GF(31)$.

© ETSI Quantum Safe Workshop 2014/10/6

Systems of 4 types

- We will create sequences of MQ problems of 4 types.

Type	Relation of n and m and s	Base field	Target
I	$n = m$	$GF(2^n)$	encryption
II	$n = m$	$GF(31)$	encryption
III	$n = 1.5m$	$GF(2^n)$	signature
IV	$n = 1.5m$	$GF(31)$	signature

• ETSI Quantum Safe Workshop
2014/10/6 •

Our construction of MQ problem

$$\left\{ \begin{array}{l} f_1(x_1, \dots, x_n) = \sum_{1 \leq i, j \leq n} a_{ij}^{(1)} x_i x_j + \sum_{1 \leq i \leq n} b_i^{(1)} x_i + c^{(1)} = d_1 \\ f_2(x_1, \dots, x_n) = \sum_{1 \leq i, j \leq n} a_{ij}^{(2)} x_i x_j + \sum_{1 \leq i \leq n} b_i^{(2)} x_i + c^{(2)} = d_2 \\ \vdots \\ f_m(x_1, \dots, x_n) = \sum_{1 \leq i, j \leq n} a_{ij}^{(m)} x_i x_j + \sum_{1 \leq i \leq n} b_i^{(m)} x_i + c^{(m)} = d_m \end{array} \right.$$

- Step 1: choose randomly quadratic coefficients, and linear coefficients .
- Step 2: choose randomly a solution.
- Step 3: compute constant coefficients such that the corresponding MQ problem has at least one solution.

• ETSI Quantum Safe Workshop
2014/10/6 •

Toy Example

- Input: A random MQ system

For example, a magma code:

```

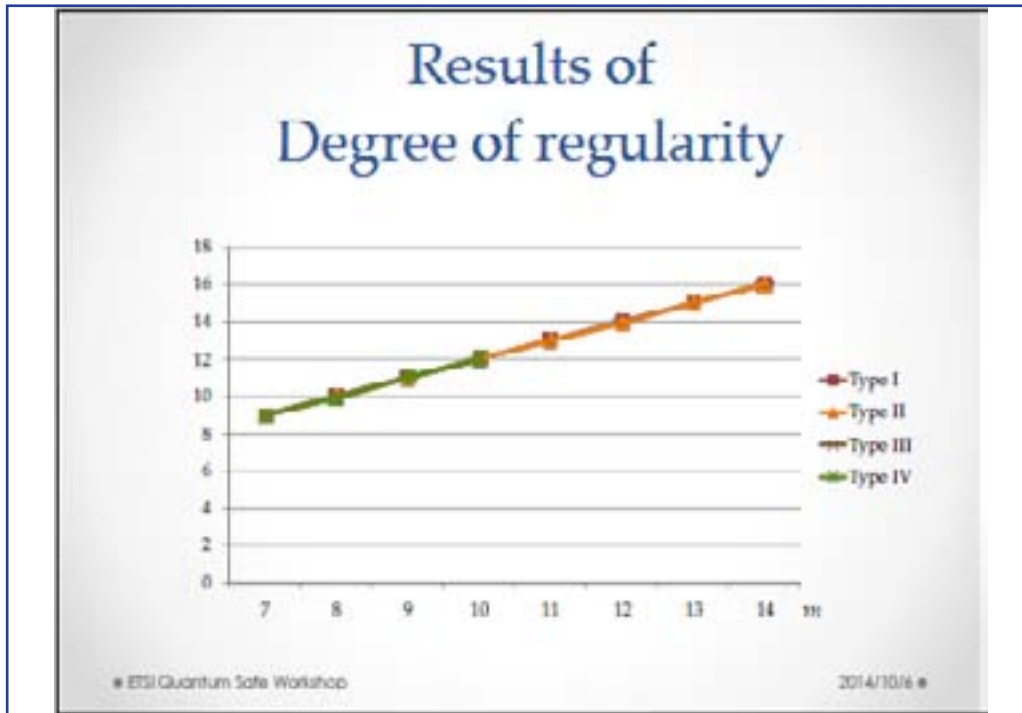
n:=2;
n:=2;
F:=GF(31);
R<x>:=PolynomialRing(F,n,"grevlex");
E:=[R 1
12*x[1]*x[1]+3*x[1]*x[2]+17*x[2]*x[2]+29*x[1]+30*x[2]+26,
26*x[1]*x[1]+13*x[1]*x[2]+9*x[1]+21*x[2]
];

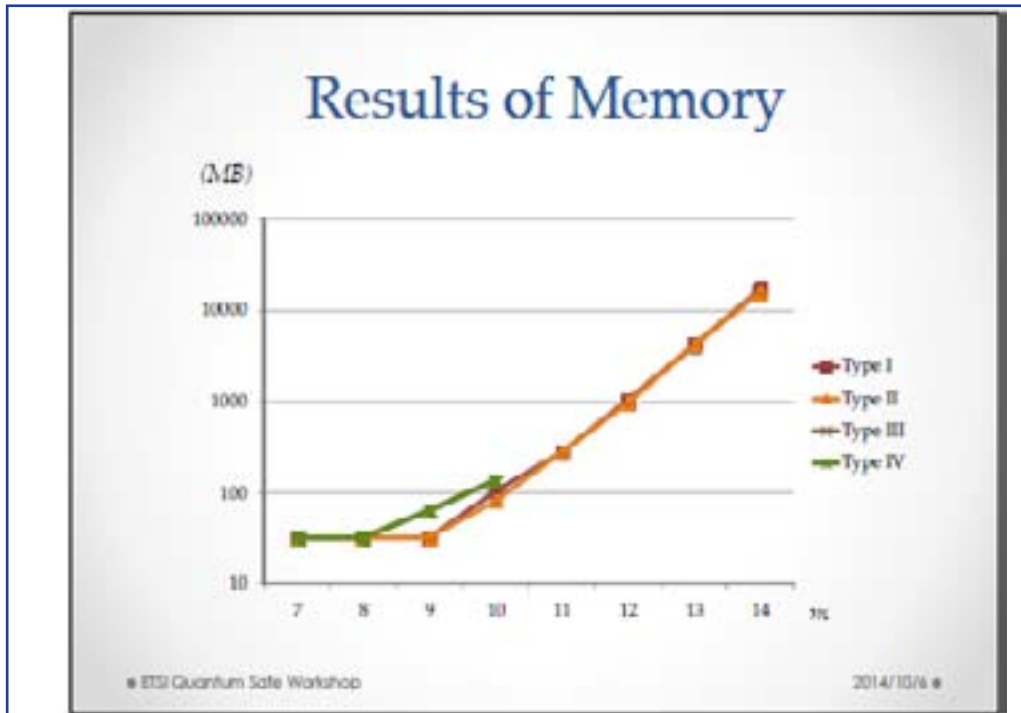
```

- Output: A solution of the MQ system
In this example, it would output <9, 1> or <15, 2>

Experiments

- CPU: Intel(R) Xeon(R) CPU E5-4617, 2.90GHz, 6 cores
- OS: Linux Mint 15 Olivia
- RAM: 1TB
- Platform: Magma V2.19-9
- Each parameter is executed for 10 times and averaged.





Conclusion

- We are planning to hold MQ challenge which is a contest for solving MQ problem.
- Preprint & homepage will be prepared soon.

ETSI Quantum Safe Workshop 2014/10/16

ETSI's role in the deployment of Quantum Key Distribution

Andrew Shields, Toshiba

Abstract

Quantum Key Distribution (QKD) offers a solution to the challenge of distributing key material securely over optical networks. Recently significant government investments have been seen globally to develop systems and demonstrator networks while technical capabilities continue to advance rapidly. However, wide-scale adoption of these technologies will require the development of technical standards upon which products and networks can be built. Customers will require appropriate security assurance that implementations are secure, systems from different manufactures should be designed for interoperability with each other and for integration with ordinary telecommunications networks.

Developing standards for security systems based on quantum technologies presents many challenges from analysing the security of QKD implementations through to specifying and characterising components for operation in the quantum regime that will help to stimulate a component / technology supply chain for quantum technologies.

ETSI is leading the way in formulating standards for QKD through the work of the ISG QKD. The ISG includes companies with QKD development programmes, leading academics and national metrology laboratories. It is building on experiences gained from early demonstrator networks and metrology programmes and is stimulating relevant research work on both theoretical and experimental aspects. Current activities include Group Specification documents addressing implementation security, optical component characterisation and deployment parameters.



Quantum Key Distribution

Quantum Communications
-each bit encoded on a single photon

Secrecy can be tested directly!!
-quantum theory dictates that eavesdropping unavoidably alters encoding of single photons

- > Detect unauthorised tapping of optical fibre networks
- > Distribute verifiably-secret digital keys

Quantum Key Distribution – Use Cases

National Security

Link Encryption
data centre back-up centre

Healthcare Networks


Quantum Key Distribution

Mobile devices


Financial Sector

Critical Infrastructure

Long Term Perspective – “Quantum-Safe” Cryptography



- > Large-scale Quantum Computer would have devastating effect on e-commerce, e-government, critical infrastructure security, individual privacy etc
- > Shor’s algorithm will break security of current Public Key Crypto (based on integer factorisation problem)
- > New crypto systems take long time to deploy, so need to plan now.




Courtesy of Qualcomm Systems Inc.


Two Solutions for Quantum-Safe Crypto

- > Research on new PK methods
 - > with resilience to Shor’s algorithm
- > Quantum Crypto based on Laws of Nature
 - > not threatened by quantum computer ... or any conventional computer

Address different applications
BOTH are important


Nearer Term: Physical Layer Quantum Encryption



- > Using installed fibre in BT network
 -  26 km, 10dB loss


TOSHIBA **BT** **ADVA** **NPL**
Leaders in Quantum Cryptography
 Choi et al, Optics Exp 22, 23121 (2014)

- > Commercial 10G DWDM transmission
 - > multiple 10 Gb/s data channels
 - > wire speed data encryption using AES



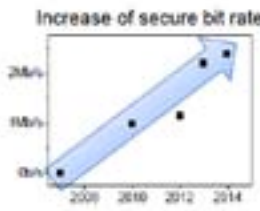
- > Data bandwidths over 1 Tb/s possible in the future

Recent Advances in QKD Technology


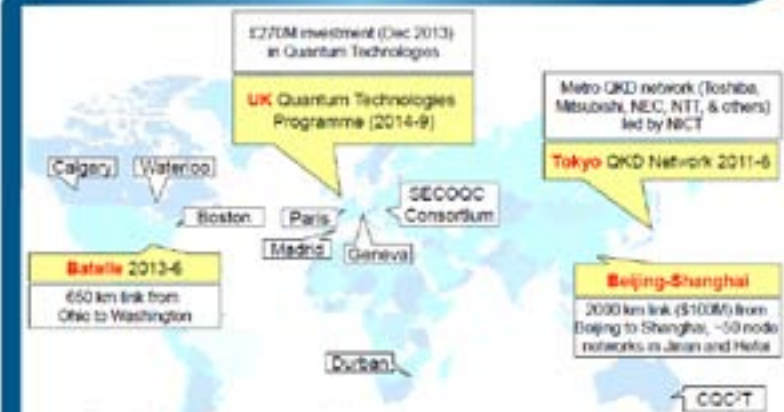


Remarkable **technological advances** in recent years

- Secure key rates**
 - Increased from kb/s to multiple Mb/s
 - Single link range increased to > 300 km
- Security**
 - Rigorous security proofs developed
 - Failure probability now quantified
 - Implementation security is better understood
- Quantum Networks**
 - Integration in core, metro, access, mobile now demonstrated
 - No longer necessary to use expensive dedicated dark fibre



Global QKD Network Installations

- £270M investment (Dec 2013) in Quantum Technologies
- UK Quantum Technologies Programme (2014-9)
- Metro QKD network (Toshiba, Mitsubishi, NEC, NTT, & others) led by NICT
- Tokyo QKD Network 2011-6
- SECOQC Consortium (Boston, Paris, Madrid, Geneva)
- Beijing-Shanghai 2000 km link (\$100M) from Beijing to Shanghai, ~50 node networks in Japan and Hebei
- Beijing 2013-6 650 km link from Orléans to Washington
- COQIT (Dubai)

Pilot deployments are taking place
 - it is meaningful to define requirements and standards now

Industrial Standards


Industrial Standards are essential for ...

- Interoperability of systems from different manufacturers
- Integration into ordinary telecom networks
- Stimulate application development on common interfaces
- Stimulate a component supply chain for Quantum Technologies
- Security assurance
 - Ensure that QKD is implemented securely

ETSI Industry Specification Group in QKD


- ISG-QKD established in 2008
- Published Group Standardisation Documents on QKD Use Cases, Application Interfaces, Security Proofs, QKD Module specification, Ontology, Components and Internal Interfaces
- Membership comprises large industry, telecom operators, SMEs, NMIs, government labs, universities
- New members are welcome

Current Work Items of ETSI ISG



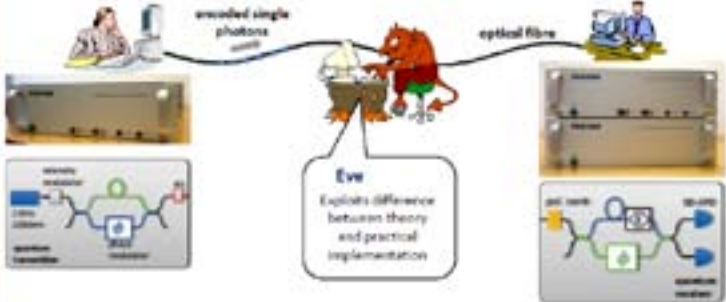
- ❶ Deployment parameters
 - User requirements for implementing QKD
 - Combining classical and quantum channels on a common optical fibre
- ❷ Quantum component specification
 - Parameters and test procedures for quantum components
 - Impact on system security
 - see talk by Chris Chunnillal
- ❸ Implementation security
 - Ensure that implementations are secure and robust against attack

Implementation Security



Objective: Investigate and close security loopholes of real QKD systems

<p>Motivation</p> <ul style="list-style-type: none"> ➢ Deviations between ideal and real system could be exploited by Eve through either active or passive attacks 	<p>Approach</p> <ul style="list-style-type: none"> ➢ Study and quantify known attacks ➢ Introduce appropriate countermeasures ➢ Modify the QKD protocol if necessary
--	--



Security by Measurement

Secure key rate after privacy amplification (ideal system) ...

$$N_{\text{ideal}} \geq N_Z^{(1)} [1 - h(\bar{q}_X^{(1)})] - N_{EC} - \Delta_\epsilon$$

For given ϵ = prob of key failure
Typically $\epsilon = 10^{-10}$
(< 1 "bad" key per 30000 years)

Info leakage due to error correction

Finite key size effect

Modified secure key rate (real system) ...

$$N_{\text{real}} \geq N_{\text{ideal}} - \delta_1 - \delta_2 \dots$$

Info leakage due to imperfection 1

Info leakage due to imperfection 2

etc


Trojan Horse Attack

> Eve injects bright light (J_E) and measures back-reflection ($J_{E,R}$) to determine Alice's or Bob's phase modulator settings

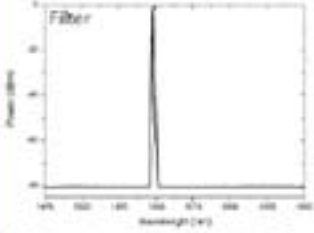
Recent experimental studies (reported at QCrypt, Paris, Sept 14)

- > CV QKD : Khan et al, Erlangen, Paris Telecom Tech & SecureNet
- > "two-way" QKD : Sajeed et al, IQC & IdQuantique
- > "one-way" QKD : considered here

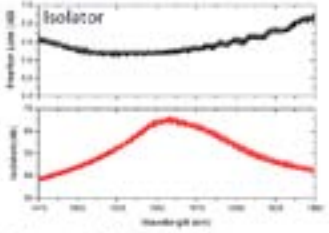
Shutting out the Trojan Horse



> 150dB isolation provided by spectral filtering and optical isolator(s)



Filter



Isolator

> Extinction > 80dBm (limited by dynamic range of measurement)


> Insertion loss < 1dB

> Isolation > 60dB at quantum λ

	Reflectivity	Attenuation	Isolation	Total
Alice	40dB	2x25dB	60dB	150dB
Bob	40dB	0	110dB	150dB

> Trojan horse attacks blocked both at Alice & Bob using passive components

Summary



- Several large QKD network deployments underway worldwide
- Standards are essential ... for future interoperability
- To assure customers that technology implemented securely
- And to stimulate markets for components, systems and applications

Thank you!

Contact: andrew.shields@cri.toshiba.co.uk

Presentations

SESSION 5
INDUSTRY**A certifiable QKD Relay Node Network***Nino Walenta, Battelle*

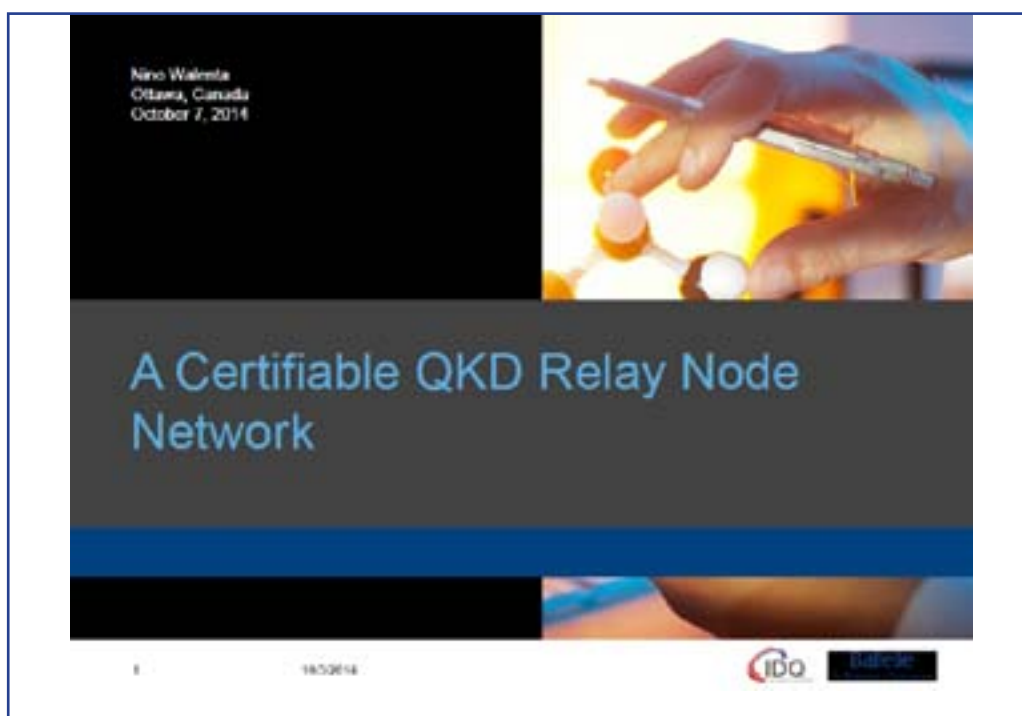
Besides the obvious benefits and strengths of quantum key distribution (QKD) of securely distributing cryptographic keys [1], the widespread adoption of commercial QKD systems has mainly been hindered by their range, limited to a few hundred kilometers, and their intrinsic point-to-point connectivity. To address both, range and scalability limitations, Battelle and ID Quantique currently develop architecture and hardware for a telecom-compatible QKD Relay Node network, where quantum keys are distributed between end users over intermediate relay nodes. Our approach removes any constraints concerning maximum number of users or range, making a scalable and cost-efficient integration of QKD possible on a national scale.

While our architecture is independent of the underlying QKD protocol, the implemented QKD system is based on a fast and compact implementation of the coherent one-way QKD protocol with hardware key distillation engine and quantum entropy sources [2]. Our development focuses on the integration in standard, small-size ATCA (Advanced Telecommunications Computing Architecture) form factor in order to seamlessly integrate into the existing infrastructure and workflow of potential users. Moreover, we target, for the first time, compliance with security certification standards such as Common Criteria EAL 4 and the Federal Information Processing Standard (FIPS 140-2) for security level 3. Here, we present the design of our QKD relay node network, and results from the prototype development phase.

References:

[1] N. Gisin et al. Quantum cryptography. Review of Modern Physics 74, 145–95 (2002).

[2] N Walenta et al. A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing. New Journal of Physics 16, 013047 (2014).



Overview

1. The QKD Trusted Node network architecture
2. The Coherent one-way QKD engine
3. Roadmap for certification
4. The Battelle Quantum Network



2

18/3/2014



Current limitations of QKD

Advantages of QKD

- Security based on fundamental physical principles instead of computational hardness
- Information-theoretically provable against most powerful adversaries:
 - not weakened by quantum computing, mathematical discoveries, massively parallel computing networks
- Forward security:
 - Secret now – secret forever

Limits of QKD

- Point-to-point
 - Suitable for operations like secure data storage, disaster recovery
 - Less suitable for sharing keys between large number of users
- Distance limitations
 - Few hundred kilometer
 - Incremental increase in effective range expected through detector improvements (~400 km)

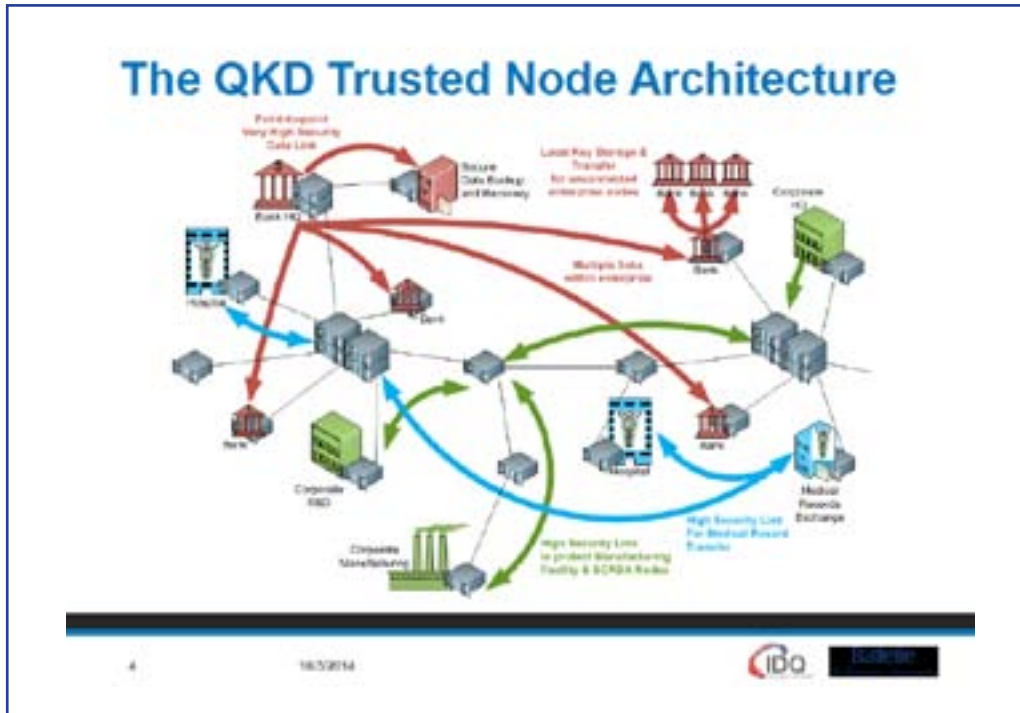
Our solution: A QKD Trusted Node network

- A single design to handle both short comings

3


18/3/2014





The QKD Trusted Node hardware

- The QKD-TN is built on the Advanced Telecommunication Computing Architecture (ATCA)
 - Provides standardized mechanical, power, and data interfaces
 - Provides network services, cooling, power supplies
 - Scalable architecture, familiar to potential clients



ATCA slot, network switches, local services			
Trusted Node Controller			
Quantum Key Controller	Quantum Key Controller	...	Quantum Key Controller
Quantum Key Engine	Quantum Key Engine		Quantum Key Engine

Quantum State

- Redundant node controller in a single node
 - Manages node discovery and provides route tables for quantum network
 - Manages and routes key transactions
- Fault tolerant dynamic path finding algorithm
 - Routing balances security and quality of service
 - Finds least cost path across the QKD network
 - Uses alternate routes when available

5
18/3/2014

QKD Trusted Node Key Transfer



User keys move securely across the network in a piece-wise fashion:

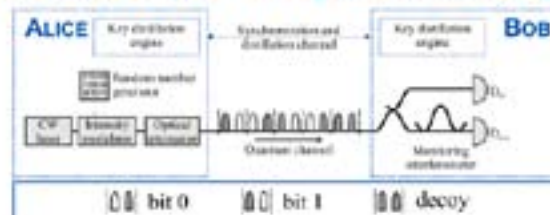
1. User keys K are first encrypted by public key cryptography PK
2. Then hop from node to node while they are additionally encrypted using quantum keys QK .

6

18/3/2014



Coherent One-Way QKD engine



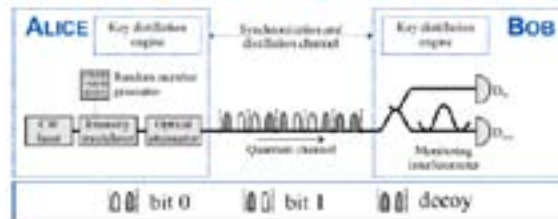
1. **Preparation:** Alice encodes information in sequence of pairs of weak coherent states
2. **Measurement:** Bob randomly chooses to measure either pulse arrival time (bit value) or coherence between successive pulses (eavesdropper's potential information about key)
3. **Sifting:** Bob tells Alice publicly, in which basis he measured (bit or coherence measurement), incompatible measurements are discarded
4. **Error correction, parameter estimation and privacy amplification:** Alice and Bob eliminate quantum bit errors, measure and reduce eavesdropper's potential information about the key
5. **Authentication:** Alice and Bob verify that public communication was authentic

7

18/3/2014



Coherent One-Way QKD engine



Characteristics

- No active elements at Bob
- Robust bit measurement basis
- Inherent robustness against PNS-attacks
- Security proof for zero error attacks certain class of USD attacks
- General security proof for slightly modified COW protocol

8

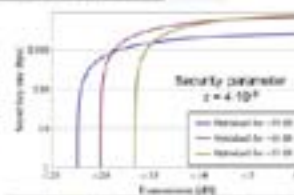
18/3/2014



Coherent One-Way QKD engine



- 625 Mbps clocked quantum key distribution engine
- Quantum random entropy source
- Continuous operation due to fast hardware key distillation
- 1-fiber dense wavelength-multiplexing option



8

18/3/2014



IT security standards



IT security standards for cryptographic equipment include

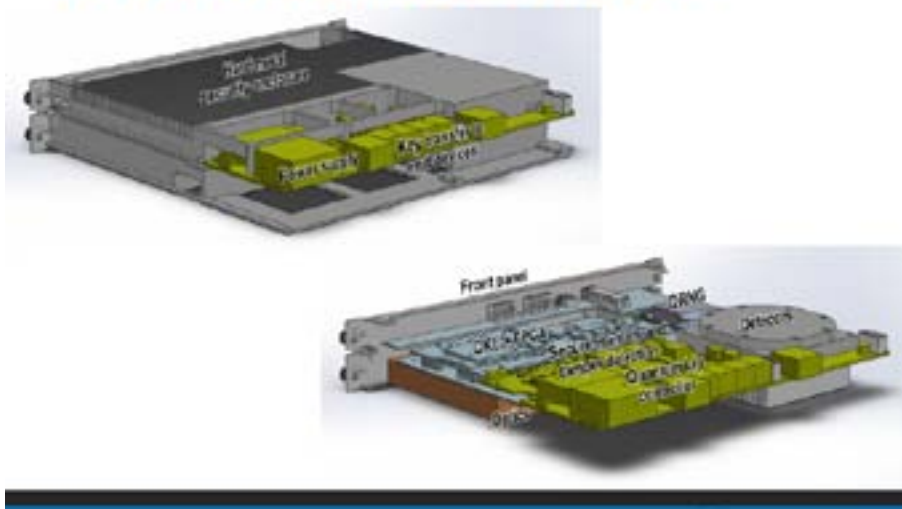
- FIPS 140-2 (2001), FIPS 140-3 (draft)
- Common Criteria (2012)
- ISO/IEC 19790 (2012)
- FIPS 140-2 approval or Common Criteria evaluation are de facto requirements for most commercial users
- FIPS 140-2 is the preferred standard for US hardware (required for US government use)
- QKD-TN will be seeking FIPS 140-2 Level 3+4 certification and CC EAL4 evaluation

No existing standards include QKD as an approved key distribution method

FIPS Security requirements

	Security Level 1	Security Level 2	Security Level 3	Security Level 4
Roles, Services, and Authentication	Logical separation of roles and services.	Role-based or identity-based authentication.	Identity-based operator authentication.	
Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests, Conditional tests.			
Cryptographic Key Management	Random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization.		Manual secret and private keys input/output shall be encrypted or using split knowledge.	
Physical Security	Production grade enclosure.	Locks and tamper-evident coating or tamper-evident enclosure.	Level 2 + tamper detection and response for covers and doors. Zeroization circuitry.	Level 3 + environmental failure protection or testing.

Physical Security Concept

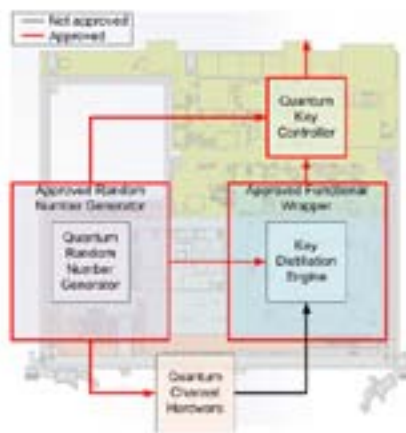


12

18/3/2014



Certifying quantum keys for QKD-TN




- Quantum key controller only implements FIPS approved methods
- All inputs need to be FIPS approved keys
- Quantum random number generator needs to be combined with FIPS approved random number generator
- Challenges for QKD:
 - Needs FIPS approved functional wrapper to output certified keys for approved further use in QKC
 - Wrapper needs to maintain information-theoretical security of keys

13

18/3/2014



Battelle Quantum Network



- First commercial QKD network in the US, in operation since September 2013
- In use with IDQ Cerberis QKD system to secure communication between Battelle's headquarter and production facility
- ~400 km of dark fiber, 3 (4) connection points at Battelle facilities in Columbus
- Fiber access on non-profit basis for researchers engaged in the development of quantum communications systems
- In 2015, all Battelle facilities in Central Ohio will be protected by QKD-TN
- In 2016, a 550 km QKD-TN link between Ohio and Washington, DC area is planned

14 18/3/2014 IDQ

Battelle Quantum Network



Our goal
A network of nodes that can be used as the basis for QKD secured communication across North America.

- Phase 1
- Phase 2
- Phase 3

15 18/3/2014 IDQ

Use case scenarios

The diagram illustrates six use case scenarios for quantum-secured networks:

- Off-site backup:** Shows a primary site connected to a backup site via a quantum-secured link.
- Key and signature server:** Shows a central server connected to multiple client sites.
- High security cloud storage:** Shows a central server connected to multiple storage nodes.
- High security private networks:** Shows a mesh network of interconnected nodes.
- Critical infrastructure protection:** Shows a network of nodes connected to a central control point, with a quantum-secured link for key distribution.
- Backbone link protection:** Shows a network of nodes connected to a central control point, with a quantum-secured link for key distribution.

16 18/3/2014 IDQ

Summary

1. The QKD Trusted Node network provides a versatile and scalable architecture in telecom-standard ATCA hardware and enables quantum secured key distribution amongst multiple users
2. It uses a fast and compact Coherent one-way QKD engine, but is open to other QKD implementations in the future as well
3. It aims at certification for application in highest security environments
4. The Battelle Quantum Network provides a testbed for quantum communications systems and is open for researchers on a non-profit basis

The image shows a rack of quantum-secured hardware and a map of the Battelle Quantum Network, which is a testbed for quantum communications systems.

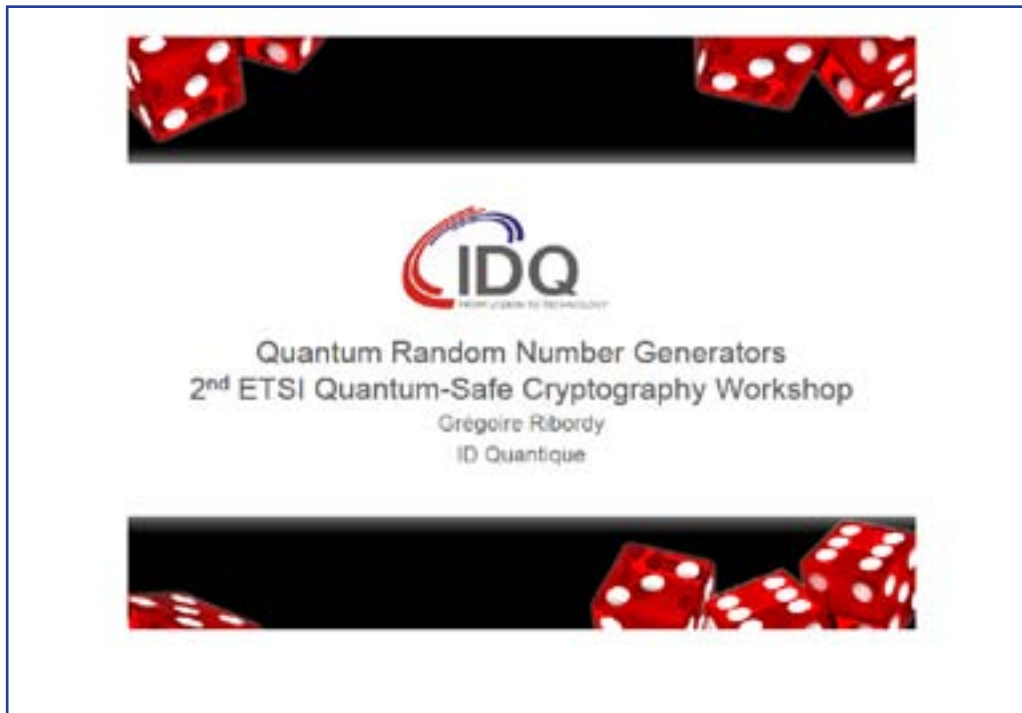
17 18/3/2014 IDQ

Presentations

SESSION 5 INDUSTRY

Quantum Random Number Generator

Grégoire Ribordy, IDQ



Random Numbers


- Very useful in a variety of applications
 -  Games
 -  Cryptography
 -  Numerical Simulations
 -  Web Applications (e-commerce, etc.)
- Difficult to produce
 - Computers cannot produce random numbers without special hardware
- Impossible to prove randomness of a finite sequence a posteriori
 - When generating random numbers, understanding the method used is important

The slide also features the IDQ logo and a decorative border at the bottom consisting of several red dice with white pips.

Outline


- ❑ Challenges with Random Number Generators
- ❑ Example of a Quantum Random Number Generator
- ❑ Security Evaluation and Certification
- ❑ New Approach to QRNG






Finding Weak RNG'S


- ❑ Collecting public keys on the Internet
 - + Lenstra: 5 million PGP keys
 - + Heninger: 22 million keys in network devices
- ❑ Look for matching keys
- ❑ Identify weak keys
 - + Keys sharing one factor with another key
- ❑ Finding the GCD is easier than factoring

- ❑ Heninger's finding:
 - + Keys served more than once: 60%
 - + Weak keys: 5.6%
 - 3.3% Default keys
 - 0.3% Weak keys
 - + Vendors: Cisco, Dell, IBM, etc.
- ❑ Use of software RNG's
 - + Gathering of entropy and post-processing
 - + Poor implementation (key generation too early in boot process)
 - + Not enough entropy due to isolation of devices

A. Lenstra et al., « Ron was wrong, What is right », SACR Cryptology ePrint Archive 2012: 64 (2012)

N. Heninger et al., « Mining your Ps and Qs: Detection of widespread weak keys in network devices », Usenix Security 2012






Hardware Trojan Horse

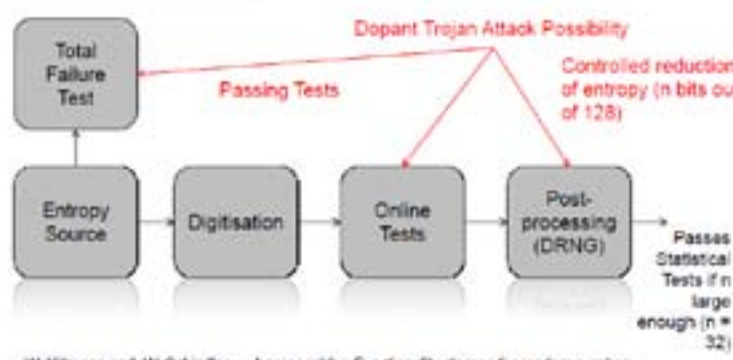
- ❑ Modification functionality of chips by change of dopant polarity (n or p)
 - Inverter
 - 0 → 1 & 1 → 0
 - 0 → 1 & 1 → 1
- ❑ Change of dopant masks
- ❑ Chip validation
 - Pre-manufacturing: code review
 - Post-manufacturing
 - Optical inspection
 - Built-in tests

- ❑ Illustration of possible vulnerability: RNG in Intel Ivy Bridge Processors
 - Metastable Entropy Source
 - Generation of blocks of 128 bits of randomness

G. Becker et al., « Stealthy Dopant Level Hardware Trojans », CHES-2013



TRNG Model



```

graph LR
    A[Entropy Source] --> B[Digitisation]
    B --> C[Online Tests]
    C --> D[Post-processing (DRNG)]
    D --> E[Passes Statistical Tests if n large enough (n = 32)]
    
    F[Dopant Trojan Attack Possibility] -- "Passing Tests" --> G[Total Failure Test]
    F -- "Controlled reduction of entropy (n bits out of 128)" --> D
    
```

W. Kilian and W. Schindler, « A proposal for Functionality classes for random number generators », AIS31


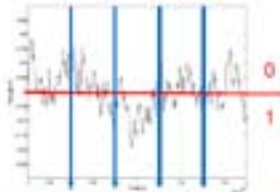

Bullrun and Dual EC DRBG

- ❑ NSA: "Insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets"
- ❑ Example: Dual EC DRBG
 - Slow
 - Backdoor known since 2007
 - Generator used by prominent vendors until 2013



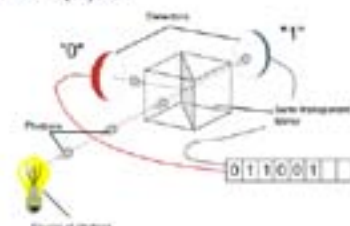

True Random Number Generator based on Classical Physics

- ❑ Physical Random Number Generator exploiting a phenomenon described by classical physics
 - Coin tossing, Roulette ball, electronic noise signal, etc.
- ❑ Not random but « difficult » to predict
- ❑ Origin of Impredictability
 - Initial conditions (Chaos)
 - Environment
- ❑ Example: Sampling of Noise Signal
 - Difficulties
 - Speed
 - Influence of environment
 - Detection of « partial » total failure



True Random Number Generator based on Quantum Physics

- Physical Random Number Generator exploiting a phenomenon described by quantum physics
- Truly random




Advantages

- Speed
- Simple process that can be modeled → influence of environment can be ruled out
- Live monitoring of elementary components possible to detect total failure



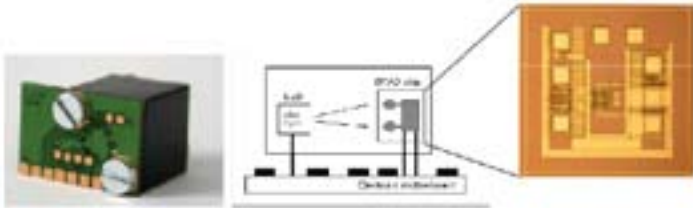
Quantis (Q)TRNG Implementation

- Complex Programmable Logic Device (CPLD) to implement the logic
- Low EMI oscillator spread spectrum clock oscillator
- Two voltage regulators
- Micropower DC/DC converter (for the detectors bias voltage)
- Passive electrical components
- Optical Sub-System





Optical Subsystem

- ❑ Emitter: printed-circuit board and LED
- ❑ Receiver: printed-circuit board and detectors
- ❑ Packaging: black aluminum cube



Technology qualified for automotive applications → High reliability



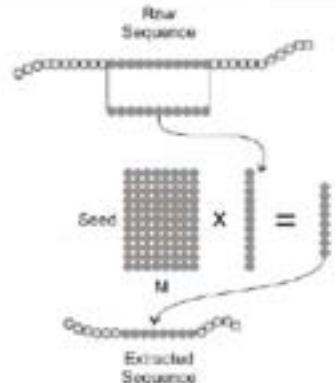
QRNG Solution



- ❑ Random bit rate:
 - 4 Mbps or 15 Mbps
- ❑ Applications
 - Security and cryptography
 - Scientific research
 - Gaming




Randomness Extraction



The diagram illustrates the randomness extraction process. It starts with a 'True Sequence' of bits. This sequence is processed through a 'Seed' matrix (represented as a grid of 'M' rows and 'X' columns) to produce an 'Extracted Sequence'. The process is shown as a transformation from the true sequence to the seed matrix, then through a multiplication-like operation (indicated by 'X' and '=') to the final extracted sequence.


- $\sim 2 \times 10^{36}$ before a deviation is observed
- Bit rate reduction: 25%

[1] D. Freuchiger, R. Renner, and M. Troyer. True randomness from realistic quantum devices. arXiv preprint arXiv:1311.4547, 2013.
[2] M. Troyer and R. Renner. A randomness extractor for the quantis device. Id Quantique technical report, 2012.




Happy Birthday QRNG!

- Quantis is 10 years old!




Special Gold Plated Edition




THE NATIONAL MUSEUM OF COMPUTING

Addition of Quantis to the collection of the National Museum of Computing at Bletchley Park UK, as an illustration of emerging quantum technologies



Evaluation and Certification

- ❑ **National Metrology Laboratory**
 - Focus: Physical Principle, Statistical Properties
 - Products covered: PCI, PCIe, USB (+ component)
- ❑ **Gaming Test Houses**
 - Focus: Statistical Properties, Software, Scaling
 - Products covered: PCI, PCIe, USB (+ component)
- ❑ **National Security Government Agencies**
 - Focus: Physical Principle, Implementation
 - Products covered: Component

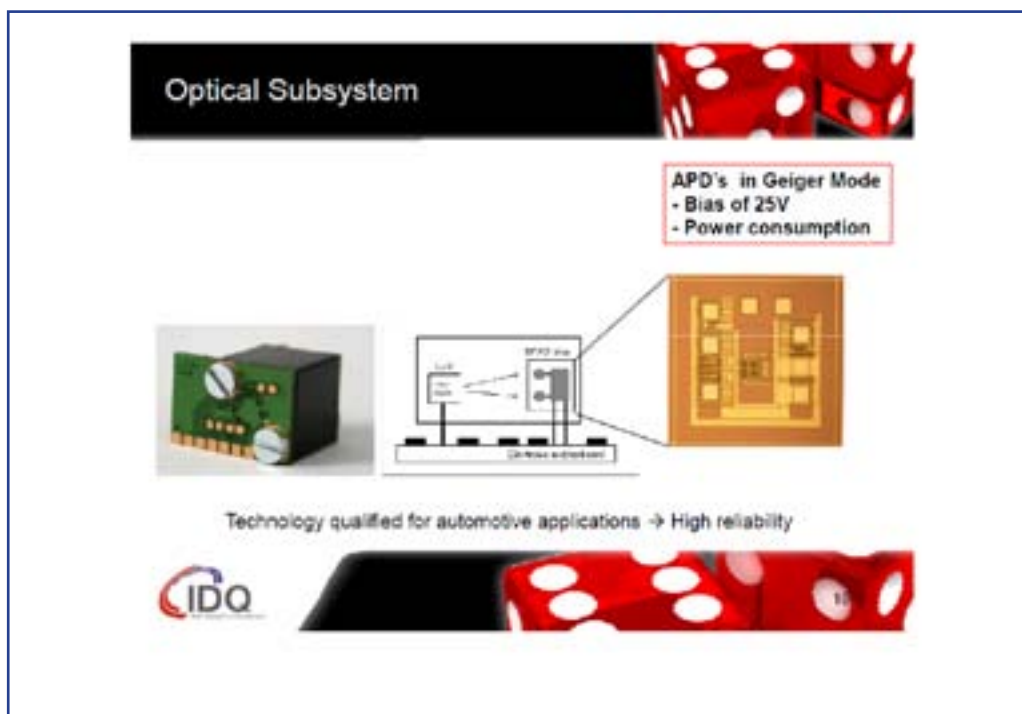
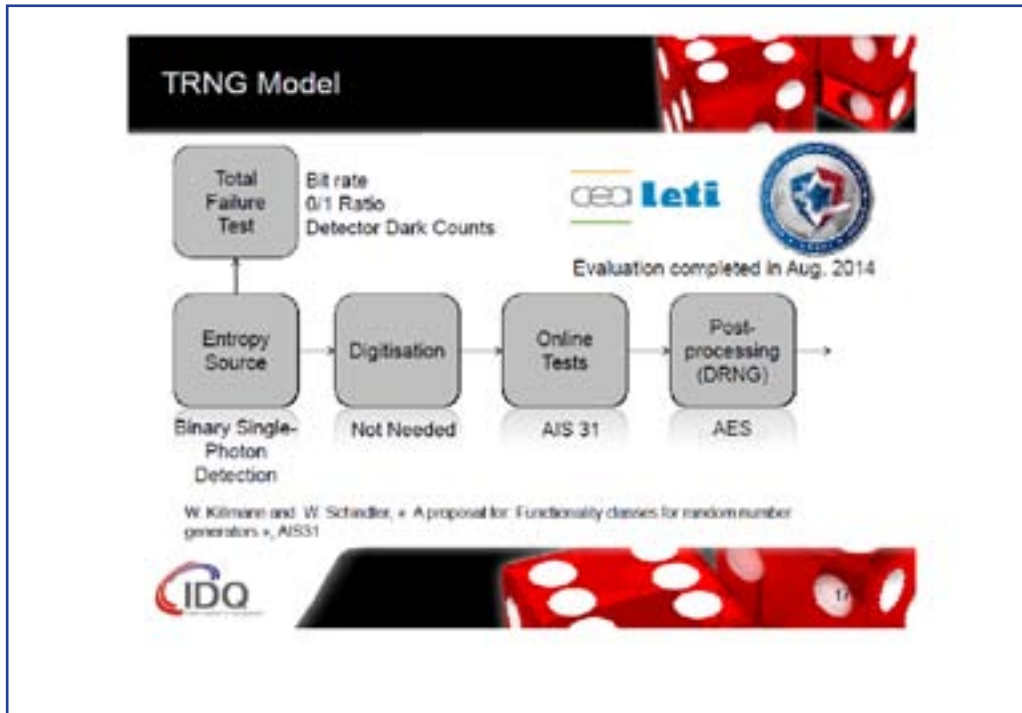




AIS31 - Context

"A proposal for: Functionality classes for random number generators", Version 2.0, 18 September 2011
 Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn

<p>Deterministic (Pseudo) RNG</p> <ul style="list-style-type: none"> • DRG.1 • DRG.2 • DRG.3 • DRG.4 • NTG.1 	<p>Non-Deterministic (Physical) RNG</p> <ul style="list-style-type: none"> • PTG.1 Physical RNG with internal tests that detect a total failure of the entropy source and non-tolerable statistical defects of the internal random numbers • PTG.2 PTG.1, additionally a stochastic model of the entropy source and statistical tests of the raw random numbers • PTG.3 PTG.2, additionally with cryptographic post-processing (hybrid PTDRNG)
--	--



New Approach for QRNG

LED
OR Fibre
Camera
Extractor
Random numbers


$P(n)$
 n
 σ_q

□ Bruno Sanguinetti, Anthony Martin, Hugo Zbinden and Nicolas Gisin

UNIVERSITÉ DE GENÈVE
sav. et inf. les sciences


Practical Tests

Astronomy CCD (ATIK 383L+)

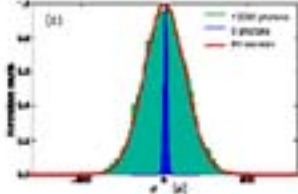


Noise: 10 e⁻

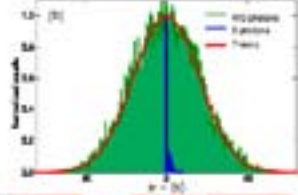
Phone CMOS (Nokia N9)



Noise: 3 e⁻



(a)



(b)

Real-World Imperfections

Even if Eve has full knowledge of the technical noise, the best she can do is recover the quantum noise.

Alice can extract randomness from quantum noise.

Integration Possibility

Sensor:
8 Megapixels x 30 frames/s x 3 bits
= 720 Mbit/s

Extractor:
software ~10 Mbps;
FPGA ~ 1.25 Gbps

Control
Clock

Image sensor

Data (10e)
800 Mbit 1000 Mbit

CPU/OS/FPGA

Thank you for your attention

- 7th Winter school on practical quantum communications
- January 2015
- In Les Diablerets, Switzerland
 - Whitfield Diffie
 - Nicolas Gisin
 - Dr. Colin P Williams, D-Wave,
 - Sandu Popescu
 - Eleni Diamanti
- New – Track on Security Evaluation and Certification

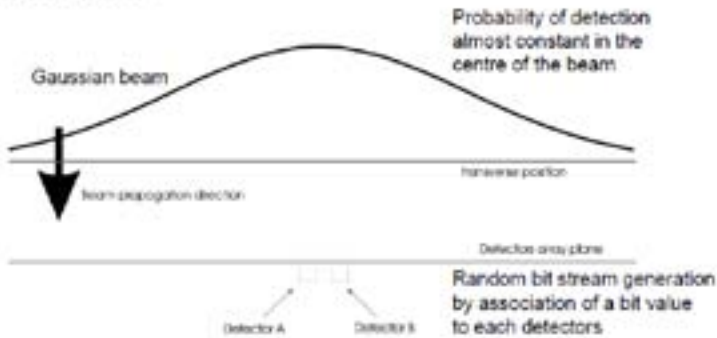


Website: <http://www.idquantique.com/instrumentation/training.html>
Contact: info@idquantique.com or gregoire.ribordy@idquantique.com



Physical Principle Explanation

on detection probability



Gaussian beam

beam propagation direction

horizontal position



Detector array plane

Detector A

Detector B

Probability of detection almost constant in the centre of the beam

Random bit stream generation by association of a bit value to each detectors



Efficient Quantum-Immune Keyless Signatures with Identity

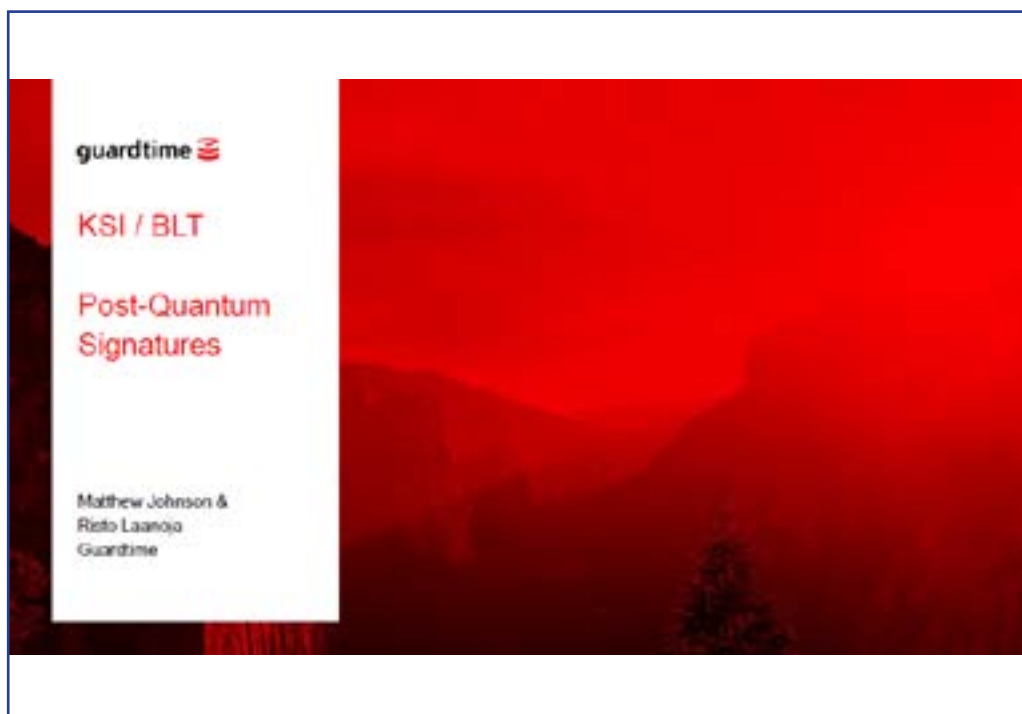
Risto Laanoja, Guardtime AS

We show how to extend hash-tree keyless signatures to server-assisted personal signatures by using only cryptographic hash functions and being thereby resistant to known quantum attacks. To authenticate the signer, we use hash sequences as one-time passwords. A message m is signed by time-stamping a concatenation of m and a one-time pseudo-random password $z[t]$ that is intended to sign messages during a particular unit t of time. The signature is valid if both $z[t]$ and the timestamp both point to t . Therefore, $z[t]$ cannot be abused without back-dating timestamps.

Secure implementation of such scheme requires dedicated hardware. Thereby, reducing the (secure) memory and computational time is important. The memory size needed for hash sequence reversal is about $O(\log^2 L)$, where L is the total number of one-time passwords. Hence, to sign messages during one year ($\sim 2^{25}$ seconds) with one-second resolution, the device must store $25^2=625$ passwords which for SHA-256 hash means 20 Kb of memory.


We show that using hierarchical password management inside the device the memory consumption can be reduced twice. A master hash sequence is used to certify short term (about five minute) sequences so that a signature is a combination of a short term certificate (signature with using the master sequence) and an ordinary hash-chain signature.

Hash sequence reversal algorithms mostly do not allow to efficiently skip over portions of the chain, which means that the signature device is either always connected to the computer or has an internal power supply. We present a modified signature scheme in which the passwords $z[i]$ are not tied to particular time units and which is much more suitable for smartcard applications.



quantum


Estonia: a 100% Digital Society Built Post-Internet



NATO Cybersecurity Center of Excellence
Tallinn Estonia

- 100% Electronic Health Records
- 99.9% of banking transactions conducted online
- Home of NATO Cybersecurity Research
- Birthplace of Keyless Signature Infrastructure (KSI)
- The ONLY country which has deployed PKI at national scale
- Subject to nation-state cyber attack 2007
- KSI / BLT are based on lessons learned

• Symbol of Estonian Cyberdefense League:



quantum

Design goals

Prove: Time of signature, Integrity of signed data and identity (human or machine) of signer.

Scale-Free: The system should be able to sign and verify on exabytes per second.

Trust-Free: Does not rely on key-stores, administrators or trusted third parties.

Portable: Data can be verified even after that data has crossed organizational boundaries.

Real-Time: The signatures should be able to be verified in real-time.

Indefinite Expiry: The signatures should not have an operational lifetime.

Telecom Grade: The system should be able to deliver 99.999% availability.

Offline: The system should not require network connectivity for verification.

Post-Quantum: The system should be work assuming functioning quantum computers i.e. it cannot rely on traditional asymmetric key cryptography.

Quantum

"Keyless Signature Infrastructure"

System which creates Keyless Signatures

- Global, scalable
- Hash tree aggregation implemented by layered Aggregator clusters
- No single points of failure
- Immediate verification
- Reasonable latency
- Secure

Quantum

KSI Scalability

Each parent aggregator can support up to 1000 children giving a capacity of 10^{18} signatures per round where n is the number of layers.

KSI currently contains four layers of aggregation.

The top-level cluster "beats" once per second i.e. there is one top level root hash value generated each second.

Up to 10^{18} signatures per second can be generated with the system as configured.

quantis

Introducing Identity

Identity: the result of an authentication request (whether PKI, LDAP, Biometric etc) as an identity tag in the KSI distributed hash tree.

This works for machines but for a true signature system for humans we need non-repudiation.

HASH TREE OF THE PARENT AUTHENTICATION SERVER

PARENT SERVER

CHILD SERVER "A"

CHILD SERVER "B"

quantis

Introducing BLT: One way hash chains

Bob first generates a secret random number and generates a hash value of that number, then generates a hash value of that and repeats creating a chain of hash-values (Lampot one-time passwords)

The last hash value in the chain is then registered with a CA after Bob's identity is verified.

In PKI parlance the secret random number would be Bob's private key and the one registered with the CA would be his public key.

Secret Random Number x

Bob

$h(x)$ $h(h(x))$

Public Hash registered with CA $h(h(h(h(h(x))))))$

quantum

Signature Scheme from One Time Passwords

Bob wants to sign a document at time $t=4$.

First he will generate a hash-value (x_4) of the document he wants to sign. Then he will hash x_4 and the one-time password which is valid only for $t=4$ to create s_4 which he sends to the CA (KSI signing service).

Note that Bob does not reveal the one-time password for $t=4$, at least until $t=5$.

4

quantum

A Signed Document

The signed document then consists of the document plus x_4 , the one-time password for $t=4$, Bob's certificate and S , the KSI signature generated from the CA.

Bob then sends a document to Carol and Carol will want to verify it was signed by Bob and the time of signature.

4

Signature Verification Step 1

Carol simply needs to repeat the process for signing the document. She will generate a hash of the document and hash that together with x_4 to regenerate x_3 and hash that together with the certificate hash x_2 to regenerate x_1 .

She then verifies (x_1, S) . This will verify that this is a valid KSI signature issued by the KSI Gateway registered with the CA.

Signature Verification Step 2

Finally Carol needs to check that the one-time password has not been re-used.

To do this she simply needs to verify that the time of the Signature S is at $t=4$. Only Bob can know x_4 at $t=4$. If someone were to attempt to reuse x_4 and forge a signature the time extracted from S would be after $t=4$.

quantis

Encoding Time

All KSI signatures contain time which is measured using a hash-calendar. Every round the root of the aggregation hash tree is used to represent that second, hence time is non-deterministic and created by distributed consensus.

The "calendar" is an append-only data structure thanks to a Merkle tree on top of it. There's a deterministic algorithm to calculate root of this tree at each round. Time value of each leaf encoded as shape of the path from root to this leaf.

quantis

Optimizations

Signature verification complexity $O(l)$ is not acceptable.

Hash-tree built on top of one-time password chain allows to create compact proofs, reducing verification time to $O(\log(l))$.

Jakobsson's pebbles reduce chain+tree storage to $O(\log^2(l))$ and need password generation to $O(\log^2(l))$.

Implication: Simple Revocation Management

The CA will check revocation status before issuing a signature. It will not issue signatures if Bob has revoked his certificate.

Because of this there is no need for managing and distributing Certificate Revocation Lists (CRLs). Carol doesn't need access to a CRL to check if Bob's certificate was valid at the time he signed a document. This removes a lot of complexity with traditional PKI.

The diagram shows a box labeled 'CA' containing a 'Signature Service' box and a database. The database lists 'Alice' with a green checkmark and 'Bob' with a red 'X'. An arrow labeled 'Signature Request' points up to the Signature Service, but it is blocked by a large red 'X'.

Implication: Limited Liability

Traditional PKI was designed such that signatures could be generated offline (by signing offline with a private key). This is a problem as if the private key is stolen there is unlimited liability. The thief can generate an infinite number of signatures, all of which will be valid.

In BLT the signatures are "server assisted" – they require the CA to assist in the process of generating a signature. This is valuable as the CA can limit/monitor the number of signatures issued by a user.

The diagram shows a box labeled 'CA' containing a 'Signature Service' box and a database. The database lists 'Alice' with a green checkmark and 'Bob' with a green checkmark. A user icon is shown with a 'Doc' icon. An arrow labeled 'Signature Request' points from the user to the Signature Service. A return arrow labeled 'Signature Response (S)' points from the Signature Service back to the user.

quantis

Implication : Non-Repudiation

Note that a CA cannot generate signatures on behalf of Bob. The CA does not see the one-time passwords until after they have been used. If a CA (or anyone) attempts to forge a document by using x_u after $t=4$ the time of KSI signature will be after $t=4$.

Bob just needs to ensure that he does not sign a document with x_u before $t=4$.

The diagram illustrates the interaction between Bob and a CA. Bob sends a 'Signature Request' to the CA's 'Signature Service'. The CA responds with a 'Signature Response (S)'. The CA's database contains records for Alice and Bob. Below this, Bob is shown signing a document 'Doc' using a sequence of keys, with a specific key x_u highlighted.


quantis

Implication : Long Term Validity

In traditional PKI it is necessary to use a time-stamping server to prove the certificate was valid when the signature occurred. It is then necessary to periodically re-stamp after the time-stamping keys are rotated (typically 5 years).

All of this complexity is gone with ELT as the time and integrity of the signature can be proven mathematically without reliance on the security of keys or trusted parties.

The image shows a newspaper clipping with the word 'MARKET' at the top. A red box highlights a small text area in the top left corner, which contains the text 'quantis'.


quantum 

Efficiency

Example instantiation: SHA2-256, one key (signature) for each second, keys are pre-generated for one year.

- Key-generation takes considerable time and should be done outside of the signing device
- Secure storage: 10K bytes
- Signing time: 625 hashing operations, faster than RSA 1024!
- Signature size and verification complexity: 25 hashes (+ KSI signature)

21


quantum 

Summary

	PKI (RSA)	KSI (BII)
1. Signature creation	off-line	Server-assisted
2. Consequence of key abuse	The number of forgeries is unlimited	Limited, server side signatures
3. Revocation check	During signature verification	During signature creation
4. Revocation solution	Complex	Simple
5. Evidence integrity	Relies on TTP confirmations	Mathematically provable
6. Quantum threat	Insecure	Quantum immune

22

guardtime



Ahto Buldas
Risto Laanoja
Ahto Truu

Thank You !

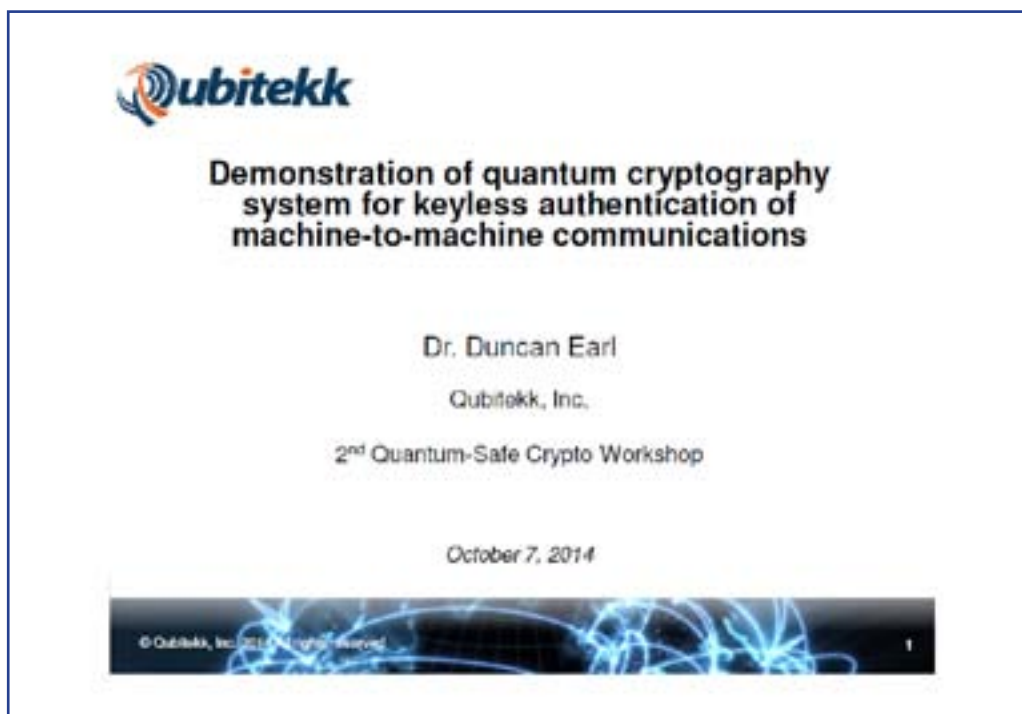
matthew.johnson@guardtime.com
[@MJGuardtime](#)

Efficient Quantum-Immune Keyless Signatures with Identity - <http://eprint.iacr.org/2014/321>
Efficient Implementation of Keyless Signatures with Hash Sequence Authentication - <http://eprint.iacr.org/2014/689>
Security Proofs for the BLT Signature Scheme - <http://eprint.iacr.org/2014/595>

Demonstration of quantum cryptography system for keyless authentication of machine-to-machine communications

Duncan Earl, Qubitekk Inc.

We present a new method of authentication that uses quantum cryptographic techniques to replace traditional digital signing algorithms based on secret keys and one-way functions. A recent demonstration of this technique for authenticating machine-to-machine communications associated with infrastructure automation is described. The demonstrated system provides authentication of communications over wireless and wired channels, representing an important improvement over traditional QKD systems that offer security over fiber-only channels. Using multiple quantum entangled photon sources and an NxN fiber optic switch, the technique involves sending a classical message over classical channels and then encoding the message for authentication through a series of fiber optic switch configurations. Based on the switch configuration, pairs of entangled photons are transmitted to multiple, decentralized quantum receivers which then post their correlated measurements publicly. The correlations among receiver measurements is evaluated by devices to validate that they agree with the classically sent message. This new method of authentication is not susceptible to a quantum computer attack since it does not rely on secret keys or mathematical algorithms. Although this quantum cryptographic technique can only be used to authenticate messages and not encrypt them, we argue that it more effectively overcomes interoperability issues and has immediate application.





The North American Grid

Cyber Security Challenges
SOM control devices in "hostile" environments
Requires broadcast control of many devices (AES media)
PK crypto used extensively for authentication/encryption, representing a single-point vulnerability
If you crack utility's PK, you can impersonate utility and destroy hard-to-replace equipment
Fragile system (break 9 transformers for nationwide blackout)
Industry cannot roll back (reliance on optimization)
Industry is slow to adopt/adopt
Devices computationally constrained (need lightweight crypto)
Data latency can be critical (<4ms for GOOSE)
Wireless and wired comm channels dominate



Destruction of hydro plant due to faulty M2M communications.

© Qubitekk, Inc. (2015). All rights reserved.

2



Priorities...

A successful QC attack on the North American electrical grid is projected to cause over 65,000 deaths and over \$13 Trillion in losses.

If we don't solve the power grid vulnerability first, all other applications may be irrelevant...

© Qubitekk, Inc. (2015). All rights reserved.

3




How Qubitekk is Helping...

- Developing and offering components for quantum cryptography developers (quantum entangled source, programmable coincidence counter, quantum introduction kits, YouTube demonstrations, etc.)
- With support from the California Energy Commission, we are developing solutions that protect wireless M2M communications by leveraging quantum phenomena
- We are working with major U.S. utilities and National Labs to develop quantum, non-QKD, solutions for distributed machine security (DCE sponsored)
- In May 2014, we were invited to DC to brief senior U.S. Energy & Commerce Committee members on threat QC pose to the grid
- We are coordinating a follow-up briefing to provide policy suggestions and actionable next steps (contact: dsara@qubitekk.com for details)




© Qubitekk, Inc. 2015. All rights reserved.
4




Implementation Considerations

Good News...

Grid Communications
Low bandwidth requirements
"Wholesale" versus "Retail" attacks are the concern
Often short transmission distances (~20km)
Secrecy not important
Don't need a perfect solution, just need a usable interoperable solution

Bad News...



© Qubitekk, Inc. 2015. All rights reserved.
5



Qubitekk's Solution

- We use quantum entanglement to securely de-centralize data for keyless authentication of wired and wireless communications.
- Solution does not require optical fibers between communicating devices
- Security is not based on computational complexity and is not vulnerable to a QC attack
- We are not doing traditional QKD. We do not claim to have a QKD system that works over wireless wavelengths.
- System is still in prototype stage
- Successfully demonstrated prototype system for California Energy Commission in September 2014.

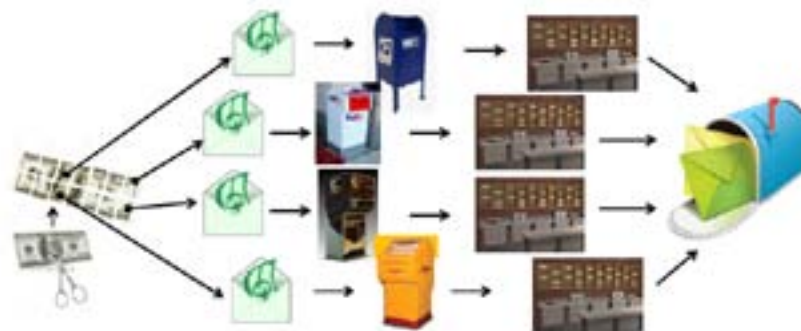


Qubitekk's Quantum Data Locking product

© Qubitekk, Inc. 2015. All rights reserved.




Security Through De-Centralization




De-Centralizing a message makes it more difficult to intercept
This is not a new idea. Aspects in group peer authentication, hyper-encryption, etc.

© Qubitekk, Inc. 2015. All rights reserved.




Authentication Method

- Two messages sent by Quantum Server:
 - One classical (bits) over air/mixed
 - One quantum (qubits) over optical fiber
- Devices receive classical message, Quantum Receivers receive quantum message
- Quantum Receivers broadcast (over classical channels) measurements on received qubits
- Quantum Receivers have correlated measurements based on message contents
- If classical message and receiver correlations agree, then message/sender authenticated
- Still possible to spoof one device but difficult to spoof many devices or Quantum Server.




$\# \text{ of Packet Intercept Points} = (\# \text{ of Quantum Receivers}) \times (\# \text{ of Devices Targeted}) = (1) \times (\text{Rate Correlation})$

© Qubitekk, Inc. 2015. All rights reserved.

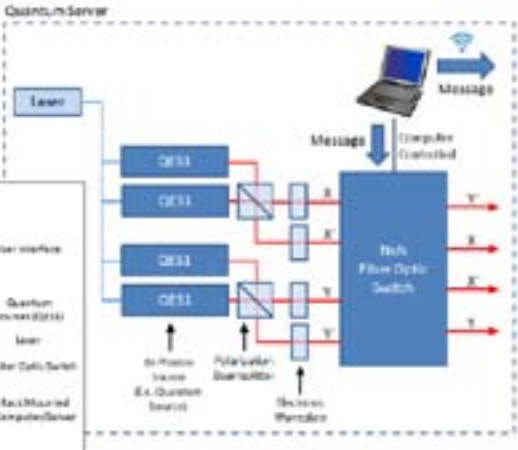


The Quantum Server

X/X' and Y/Y' basis are always opposite, Alternates every 15 msec.



- User Interface
- Quantum Server (QSS)
- Laser
- Fiber Optic Switch
- Back Mounted Computer/Server



© Qubitekk, Inc. 2015. All rights reserved.

Coding Characters

Inputs

0 or 1 0 or 1

Unique Outputs

SW1	SW2	Output 1	Output 2	Output 3	Output 4	Unique?	Character
0	0	X	X'	Y	Y'	Yes	A
0	1	X	X'	Y'	Y	No	-
1	0	X'	X	Y	Y'	Yes	B
1	1	X'	X	Y'	Y	Yes	C

© Qubitek, Inc. 2015. All rights reserved. 10

Switch Hardware

Truth Table:

SW1	SW2	Output
0	0	A
0	1	-
1	0	B
1	1	C

10 x 10 switch required to represent all 256 ASCII characters

© Qubitek, Inc. 2015. All rights reserved. 11

Testing Quantum Crypto

Vadim Makarov, Institute for Quantum Computing, University of Waterloo



Cryptography:	classical	vs.	quantum
Based on...	Unproven mathematical assumptions		Laws of physics
Convenient to implement?	Yes		No
Forward secure?	No		Yes
Authenticate via PKI?	Yes		Yes
Loopholes in implementations?	Yes		

Crypto shocker: four of every 1,000 public keys provide no security (updated)

Almost 27,000 certificates used to protect webmail, e-commerce, and other ...

by Ben Swick - Feb 16 2013, 10:08 AM

An interesting four out of every 1,000 public keys protecting webmail, online banking, and other sensitive online services is the last private key ever used to generate it.

900 SINs stolen due to Heartbleed bug: Canada Revenue Agency

By Anne O'Grady - Global News

TORONTO - Roughly 900 Canadians have had their social insurance numbers stolen from the Canada Revenue Agency's systems after the federal agency's online services were hit by the so-called Heartbleed bug.

"CRA has been notified by the Government of Canada's lead security agencies of a major breach of taxpayer information that occurred on the Revenue Agency's website in a statement on Social Insurance numbers (SIN) of ..."

Date: Wed, 1 Oct 2014 15:01:29 -0900
 From: Matt Cooper <mtt.cooper@water100.ca>
 To: "vukobrad@rediffmail.com"; "vukobrad@rediffmail.com"
 Subject: [URGENT] Network device compromised

Good morning Vadie,

We have received notice from IST that your NAS has been compromised due to the Shellshock exploit and it must be removed from the network immediately.


Here is an excerpt from IST Security:

"It looks very much like your NAS qbackup.lgc.water100.ca has been compromised by Shellshock. Last night (29 Sept) at 2:00h we saw a Shellshock-type HTTP request to the login script for this device, intended to cause it to execute code to download some scripts and binaries, followed by it actually downloading some."

Cryptography:	classical	vs.	quantum
Based on...	Unproven mathematical assumptions		Laws of physics
Convenient to implement?	Yes		No
Forward secure?	No		Yes
Authenticate via PKI?	Yes		Yes
Loopholes in implementations?	Yes		Yes
Exploitable retroactively?	Sometimes		No*

* Single exception: A. Lamas-Linares & C. Kurtsiefer, Opt. Express 16, 9388 (2007)

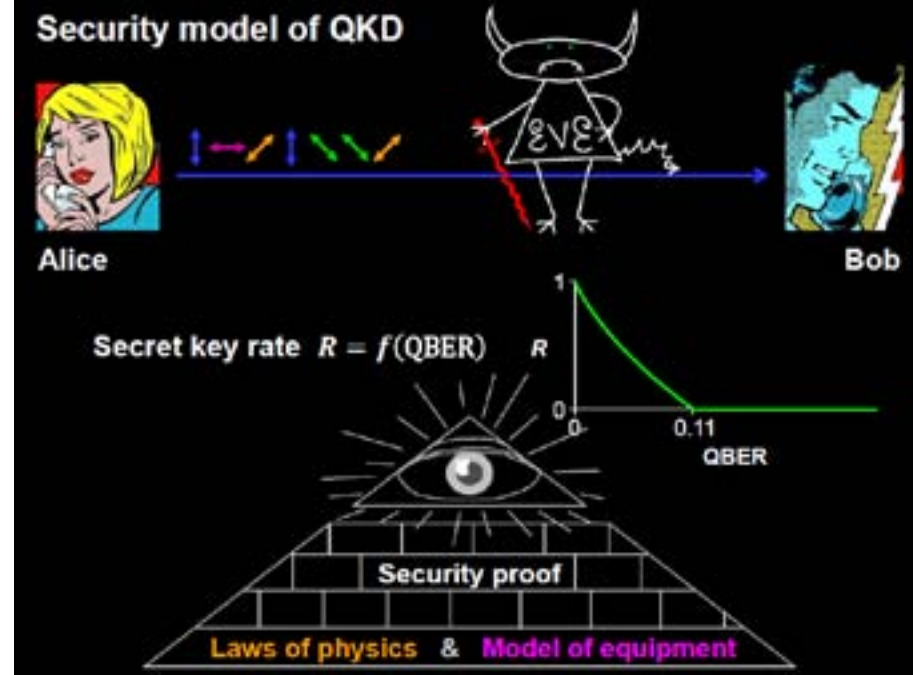
Classical hacking vs. quantum hacking



Often, just a computer (~\$0 equipment) **Optics lab (≥\$0.5M equipment)**

The image shows two side-by-side photographs. The left photo shows a person sitting at a desk with multiple computer monitors, representing classical hacking. The right photo shows a person in a dark room with various optical equipment and cables, representing quantum hacking.

Security model of QKD



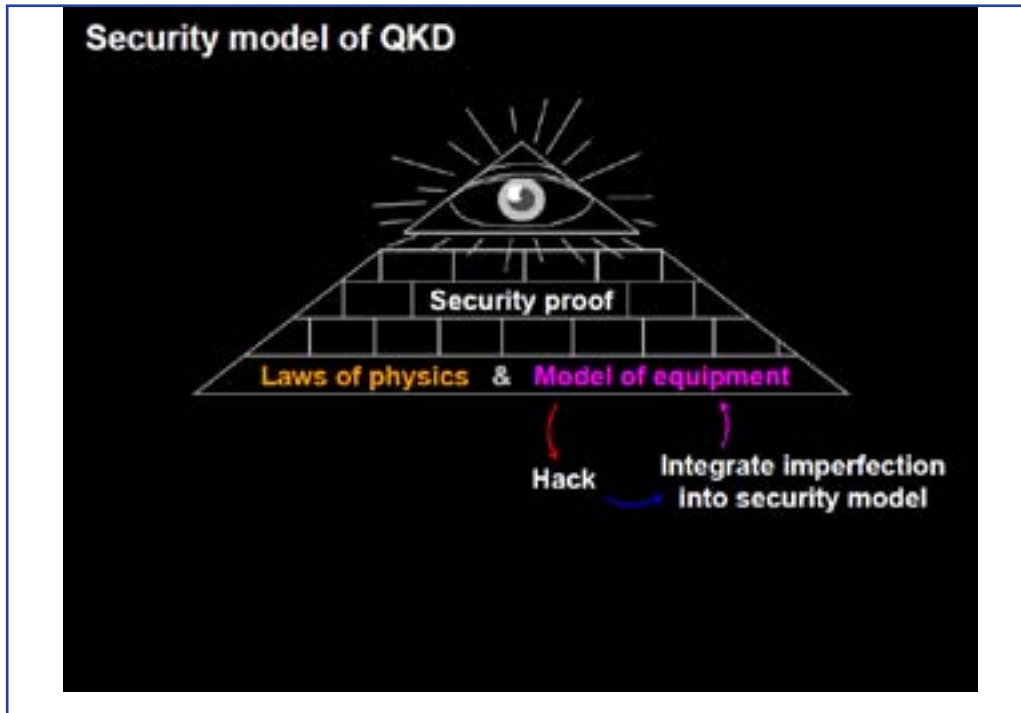
Alice **EVE** **Bob**

Secret key rate $R = f(\text{QBER})$

Security proof

Laws of physics & Model of equipment

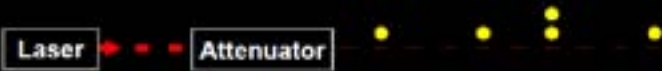
The diagram illustrates the security model of QKD. It shows Alice on the left and Bob on the right, with a central figure of Eve representing an eavesdropper. A blue arrow represents the quantum channel between Alice and Bob, with a red arrow from Eve indicating an interception attempt. Below this is a graph of Secret key rate R versus QBER, showing a curve that starts at $R=1$ for $\text{QBER}=0$ and drops to $R=0$ at $\text{QBER}=0.11$. At the bottom, a pyramid structure represents the security proof, with the top layer labeled 'Security proof' and the base labeled 'Laws of physics & Model of equipment'.



Example of vulnerability and countermeasures

Photon-number-splitting attack

C. Bennett, F. Besselle, G. Brassard, L. Salvati, J. Smolin, J. Cryptology 5, 3 (1992)
 G. Brassard, N. Lütkenhaus, T. Mor, B. C. Sanders, Phys. Rev. Lett. 85, 1330 (2000)
 N. Lütkenhaus, Phys. Rev. A 61, 052304 (2000)
 S. Félix, N. Gisin, A. Stokanov, H. Zbinden, J. Mod. Opt. 48, 2009 (2001)
 N. Lütkenhaus, M. Jahma, New J. Phys. 4, 44 (2002)



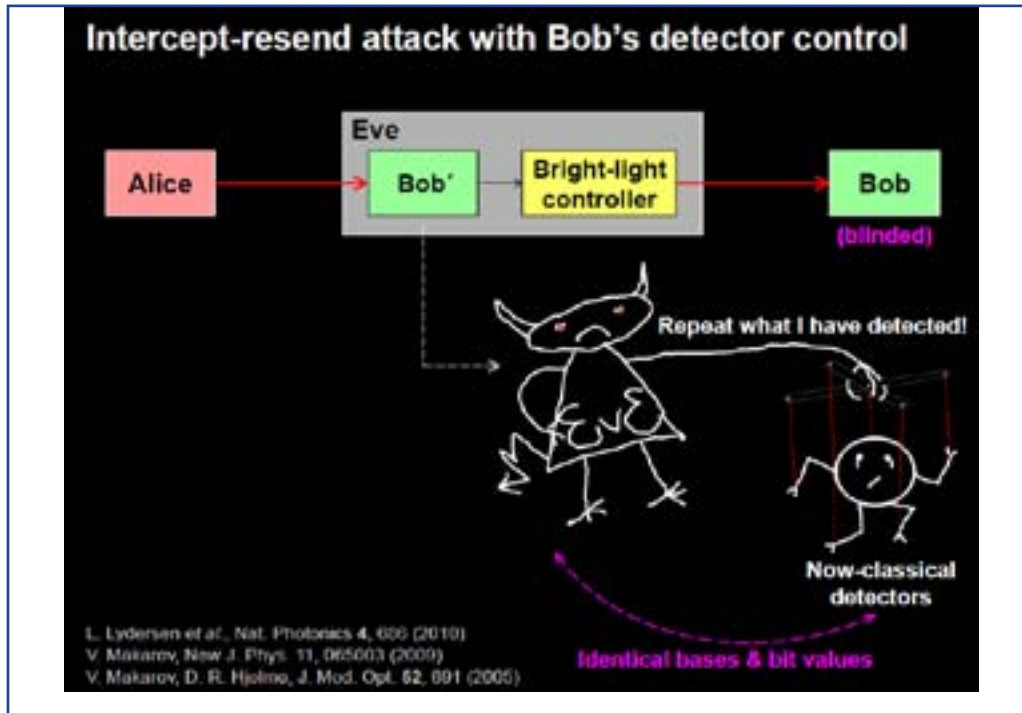
- ★ **Decoy-state protocol**
W.-Y. Hwang, Phys. Rev. Lett. 91, 057901 (2003)
- ★ **SARG04 protocol**
V. Scarani, A. Acín, G. Ribordy, N. Gisin, Phys. Rev. Lett. 92, 057901 (2004)
- ★ **Distributed-phase-reference protocols**
K. Inoue, E. Waks, Y. Yamamoto, Phys. Rev. Lett. 89, 037902 (2002)
 K. Inoue, E. Waks, Y. Yamamoto, Phys. Rev. A 68, 022317 (2003)
 N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, V. Scarani, arXiv:quant-ph/0411022v1 (2004)

Attack	Target component	Tested system
Pulse energy calibration <i>S. Sajadi et al., presentation at QCrypt (2014)</i>	classical watchdog detector	ID Quantique
Trojan-horse <i>I. Khan et al., presentation at QCrypt (2014)</i>	phase modulator in Alice	SeQureNet
Trojan-horse <i>N. Jain et al., arXiv 1406.5813</i>	phase modulator in Bob	ID Quantique*
Detector saturation <i>H. Qin, R. Kumar, R. Allouane, presentation at QCrypt (2013)</i>	homodyne detector	SeQureNet
Shot-noise calibration <i>P. Jouguet, S. Kunz-Jacques, E. Diamant, Phys. Rev. A 87, 062313 (2013)</i>	classical sync detector	SeQureNet
Wavelength-selected PNS <i>M.-S. Jiang, S.-H. Sun, C.-Y. Li, L.-M. Liang, Phys. Rev. A 86, 032310 (2012)</i>	intensity modulator	(theory)
Multi-wavelength <i>H.-W. Li et al., Phys. Rev. A 84, 062308 (2011)</i>	beam splitter	research syst.
Deadline <i>H. Weier et al., New J. Phys. 13, 073024 (2011)</i>	single-photon detector	research syst.
Channel calibration <i>N. Jain et al., Phys. Rev. Lett. 107, 110501 (2011)</i>	single-photon detector	ID Quantique
Faraday-mirror <i>S.-H. Sun, M.-S. Jiang, L.-M. Liang, Phys. Rev. A 83, 062331 (2011)</i>	Faraday mirror	(theory)
Detector control <i>I. Gerhardt et al., Nat. Commun. 2, 349 (2011); L. Lydersen et al., Nat. Photonics 4, 686 (2010)</i>	single-photon detector	ID Quantique, MagIQ, research syst.
Phase-remapping <i>F. Xu, B. Qi, H.-K. Lo, New J. Phys. 12, 113026 (2010)</i>	phase modulator in Alice	ID Quantique*
Time-shift <i>Y. Zhao et al., Phys. Rev. A 78, 042303 (2008)</i>	single-photon detector	ID Quantique

* Attack did not break security of the tested systems, but may be applicable to a different implementation.

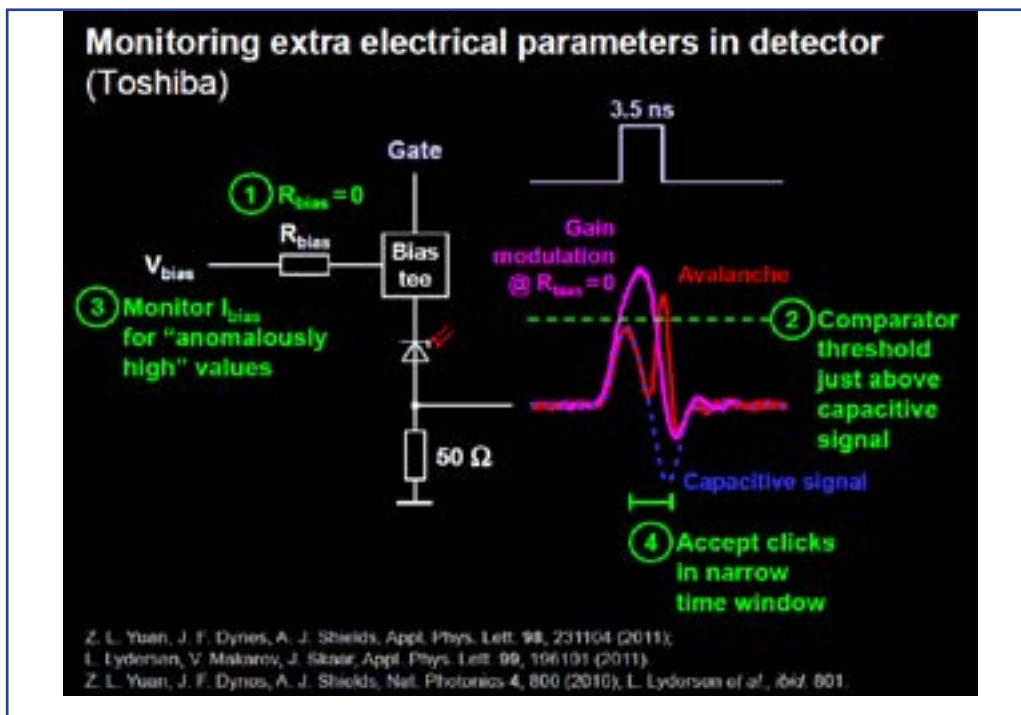
Attack	Target component	Tested system
Pulse energy calibration <i>S. Sajadi et al., presentation at QCrypt (2014)</i>	classical watchdog detector	ID Quantique
Trojan-horse <i>I. Khan et al., presentation at QCrypt (2014)</i>	phase modulator in Alice	SeQureNet
Trojan-horse <i>N. Jain et al., arXiv 1406.5813</i>	phase modulator in Bob	ID Quantique*
Detector saturation <i>H. Qin, R. Kumar, R. Allouane, presentation at QCrypt (2013)</i>	homodyne detector	SeQureNet
Shot-noise calibration <i>P. Jouguet, S. Kunz-Jacques, E. Diamant, Phys. Rev. A 87, 062313 (2013)</i>	classical sync detector	SeQureNet
Wavelength-selected PNS <i>M.-S. Jiang, S.-H. Sun, C.-Y. Li, L.-M. Liang, Phys. Rev. A 86, 032310 (2012)</i>	intensity modulator	(theory)
Multi-wavelength <i>H.-W. Li et al., Phys. Rev. A 84, 062308 (2011)</i>	beam splitter	research syst.
Deadline <i>H. Weier et al., New J. Phys. 13, 073024 (2011)</i>	single-photon detector	research syst.
Channel calibration <i>N. Jain et al., Phys. Rev. Lett. 107, 110501 (2011)</i>	single-photon detector	ID Quantique
Faraday-mirror <i>S.-H. Sun, M.-S. Jiang, L.-M. Liang, Phys. Rev. A 83, 062331 (2011)</i>	Faraday mirror	(theory)
Detector control <i>I. Gerhardt et al., Nat. Commun. 2, 349 (2011); L. Lydersen et al., Nat. Photonics 4, 686 (2010)</i>	single-photon detector	ID Quantique, MagIQ, research syst.
Phase-remapping <i>F. Xu, B. Qi, H.-K. Lo, New J. Phys. 12, 113026 (2010)</i>	phase modulator in Alice	ID Quantique*
Time-shift <i>Y. Zhao et al., Phys. Rev. A 78, 042303 (2008)</i>	single-photon detector	ID Quantique

* Attack did not break security of the tested systems, but may be applicable to a different implementation.



Countermeasures to detector attacks

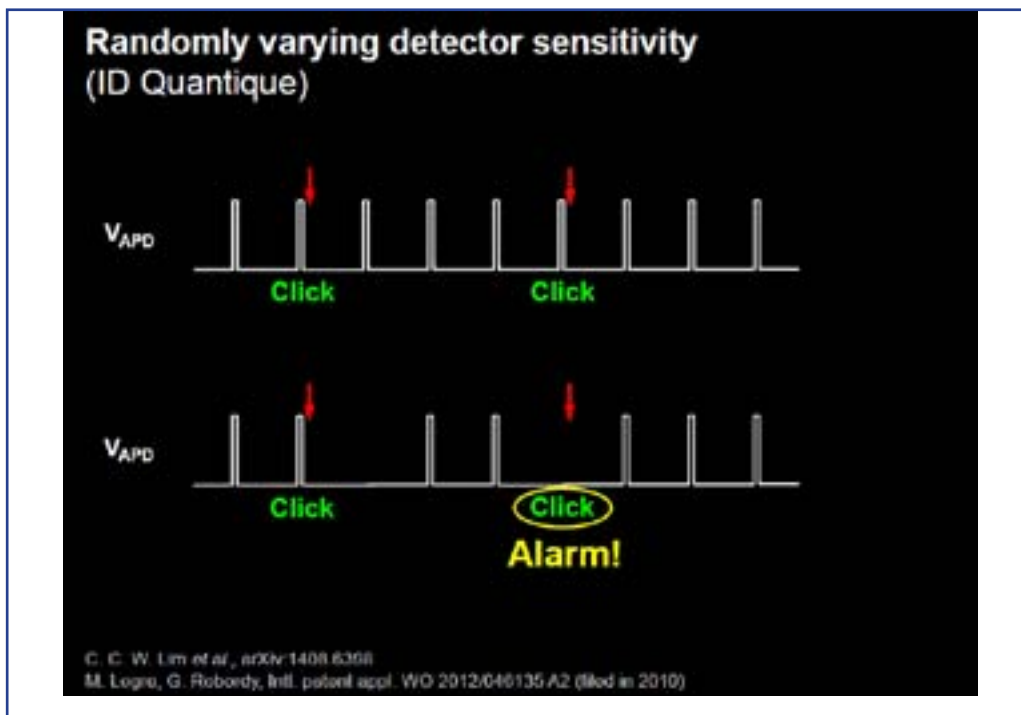
<p>Technical</p>	<ul style="list-style-type: none"> • Monitoring extra electrical parameters in detector <small>Z. L. Yuan, J. F. Dynes, A. J. Shields, Appl. Phys. Lett. 98, 231104 (2011)</small> • Randomly varying detector sensitivity <small>M. Legre, G. Robenly, Int'l. patent appl. WO 2012/046135 A2 (filed in 2010) C. C. W. Lim et al., arXiv:1403.6399</small>
<p>Integrated into security model</p>	<ul style="list-style-type: none"> • Measurement-device-independent QKD <small>H. K. Lo, M. Curty, B. Qi, Phys. Rev. Lett. 108, 130503 (2012)</small>



I: Can we test your detector?
 Toshiba: No.
 I: Why not?
 Toshiba: Still no.

Chinese way: build a copy and hack it.

M.-S. Jiang et al., Phys. Rev. A 88, 062335 (2013)



Countermeasures to detector attacks

Technical ☹️

- Monitoring extra electrical parameters in detector
Z. L. Yuan, J. F. Dynes, A. J. Shields, Appl. Phys. Lett. 98, 231104 (2011)
- Randomly varying detector sensitivity
M. Legre, G. Robordy, Int'l. patent appl. WO 2012/046135 A2 (filed in 2010)
C. C. W. Lim et al., arXiv:1408.6368

Integrated into security model 😊

- Measurement-device-independent QKD
H. K. Lo, M. Curty, B. Qi, Phys. Rev. Lett. 108, 130503 (2012)

Alice: Photon source, Mod., RNG

Charlie (untrusted): BSM, publicly announces BSM result

Bob: Photon source, Mod., RNG

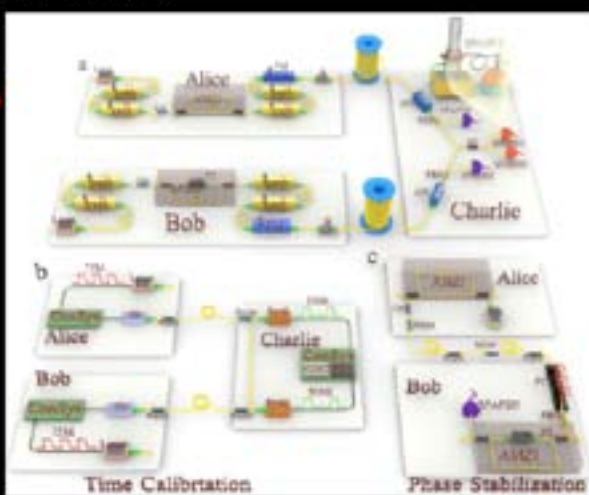
Measurement-device-independent QKD: experiments

Calgary, 28 km
A. Rubenok et al., arXiv:1204.0738v2

Rio de Janeiro, 17 km
T. Ferreira da Silva et al., Phys. Rev. A 88, 052303 (2013)

Toronto, 10 km
Z. Tang et al., Phys. Rev. Lett. 112, 190503 (2014)

Hefei, 200 km →
Y.-L. Tang et al., arXiv:1407.8012



Responsible disclosure is important

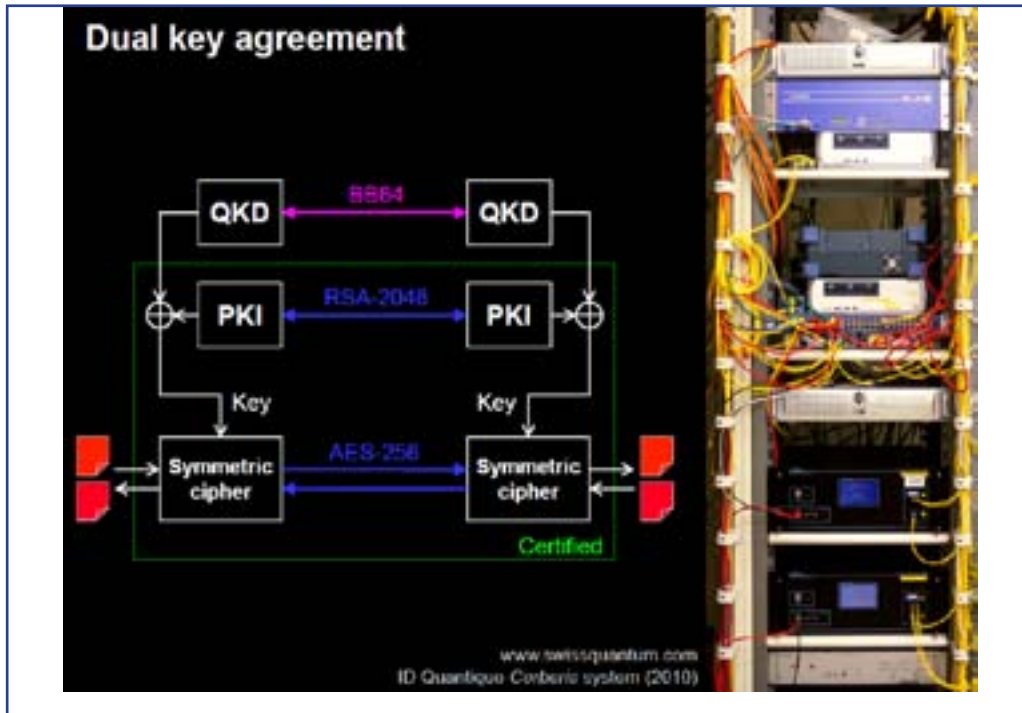
Example: hacking commercial systems

2009

- ID Quantique got a detailed vulnerability report
 - reaction: requested time, developed a patch
 - M. Legre, G. Ribordy, int'l. patent appl. WO 2012/046135 A2 (filed in 2010)

2010

- MagiQ Technologies got a detailed vulnerability report
 - reaction: informed us that QPN 5505 is discontinued
- Results presented orally at a scientific conference
- Public disclosure in a journal paper
 - L. Lydersen et al., Nat. Photonics 4, 686 (2010)



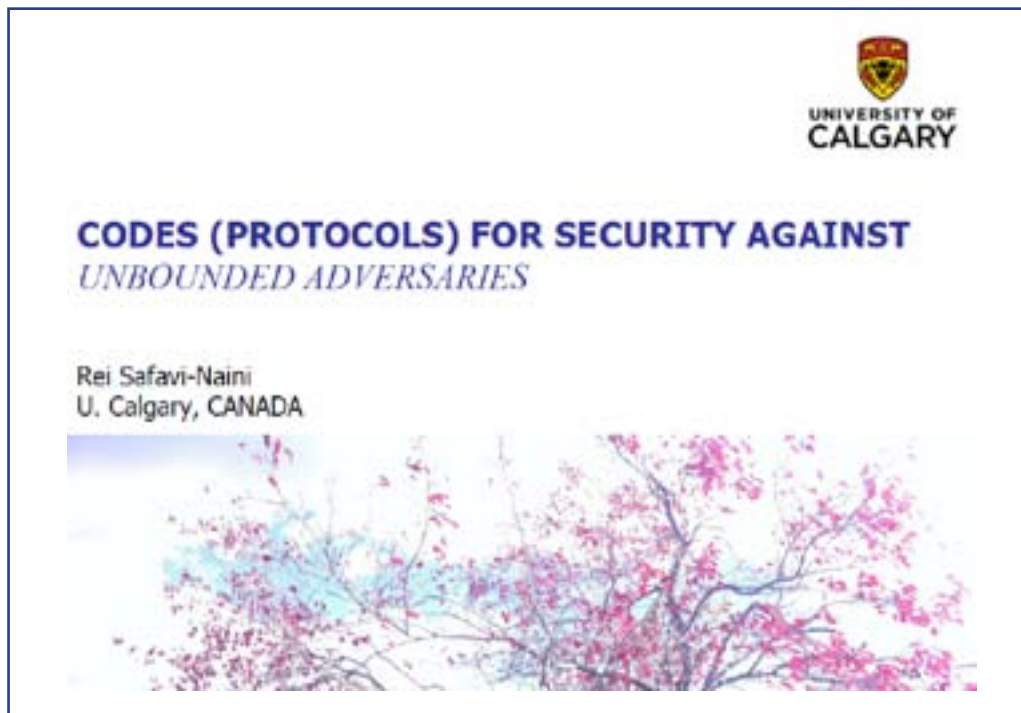
Codes for security against computationally unbounded adversaries*Rei Safavi-Naini, University of Calgary*

Modern cryptography assumes a computationally bounded adversary, and bases security on the hardness of mathematical problems. Advances in computer technologies combined with ground breaking developments in algorithms, rejuvenates the question of providing security without any computational assumptions.

We consider the problem of security and reliability of data against a computationally unbounded adversary, that has limitations on its access to the underlying physical system. Example scenarios are, a secure storage system that the adversary cannot read, but can corrupt by adding noise to it; or a scenario where a sender and a receiver are connected by multiple disjoint paths that only some are inaccessible to the adversary. A concrete example is “utilizes quantum noise to augment the security of the best state-of-the-art cryptographic algorithms.”


The common element in all these systems is that the adversary has partial access to the state of the system. In this talk we give an overview of this problem, define security and reliability goals and efficiency measures, and look at some of the current results- and in particular constructions that can be used for providing security. We also discuss open problems for future research.

[1] <http://www.nucrypt.net/noise-based-physical-layer-encryption.html>




It is year 2030....

2-computers are up and running....



*Alice wants to send a **private message** to Bob.*



Alice & Bob's options..

Quantum cryptography

1. Qubits
 - *Physical (quantum) assumption*
 - Implementation challenges
 - Side-channels
 - Trojan horse attack
- Estimating adversary

Classical cryptography

1. Computational assumption
2. No computational assumption

Classical cryptography: *Assumptions*

1. Comp Assumption

- *Eve's computation is limited.*
 - Hard problem
 - Hash based system
 - Symmetric key
- Eve can corrupt the channel.
- *Eve's corruption is limited.*



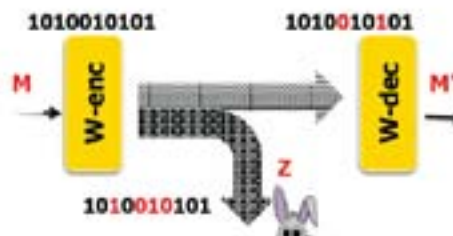
Image source : wikipedia

2. No Comp Assumption

- *Eve has a Q computer.*
- *Eve's view is limited.*
- *Eve's corruption ability is limited.*
- **Physical assumption** about (radio/fiber/network/token) environments.
Physical Layer Security

Wyner wiretap model (1975)

- Noisy channel



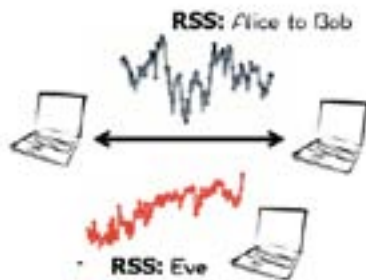
Secrecy: $\frac{1}{k} H(M|Z) \geq 1 - \epsilon$

Reliability: $\Pr(M' \neq M) \leq \epsilon$

→ *Perfect secrecy*

Limited view

- High speed communication
 - Channel reciprocity
- Near-field communication



Limited view

- Physical-Layer Quantum Encryption
 - "Ultra-Secure Air-to-Ground Gigabit-per-Second"
 - Make adversary's view noisy

"Our systems make use of fundamental, and thus unavoidable, noise called quantum noise. Quantum noise is not normally a factor in radio-frequency communications such as cell phones, but does come into play at optical frequencies. Our high-speed encrypted optical communication systems automatically force this noise to interfere with an eavesdropper's observation in such a way as to make the job of attacking the secure channel much more difficult"



Summary: *Post-quantum Crypto*

	Q-Crypto	Classical			
		PhyLayer	Hash	Symm	Hard Prob
Assum	Phys	Phys	Comp	Comp	Comp
Proof/Reduc	Yes	Yes	No	No	Yes

Rest of the talk

- Adversarial wiretap
 - Privacy & correct transmission
- Bound, capacity & construction
- Concluding remarks

Wyner wiretap & AWTP

Wiretap
(W '76)

- Perfect secrecy without secret key

Adversarial wiretap
(WS-N '13)

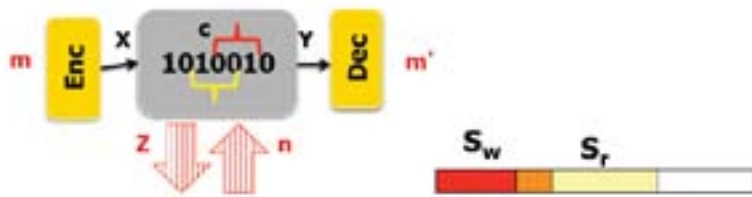
Wireless

Modeling insecure channel

- Eve can Read/Write
- limited access
- Secrecy
- Correctness

Adversarial wiretap

Private & Reliable communication



- Encoder:
Enc: $M \times R \rightarrow \Sigma^N$

- Decoder:
Dec: $\Sigma^N \rightarrow M$

$$|S_r| = \rho_r L, \quad |S_w| = \rho_w L$$

$$SD(V_A(m_1, r); V_A(m_1, r)) \leq \epsilon$$

$$\Pr(M' \neq M) \leq \delta$$

$$SD(X; Y) = \sum_v |\Pr(X = v) - \Pr(y = v)|$$

AWTP: *Efficiency*

- Information rate of a code

$$R(C) = \frac{\log |M|}{L \log |\Sigma|}$$

Capacity: $C = \max_{C, L \rightarrow \infty} R(C)$

- Encoding/Decoding complexity

Rate bound & Capacity

- Bound

$$C^\epsilon \leq 1 - \rho_r - \rho_w + 2\epsilon\rho_r(1 + \log_{|\Sigma|} \frac{1}{\epsilon})$$

- Capacity

$$C^0 = 1 - \rho_r - \rho_w$$

A capacity achieving construction

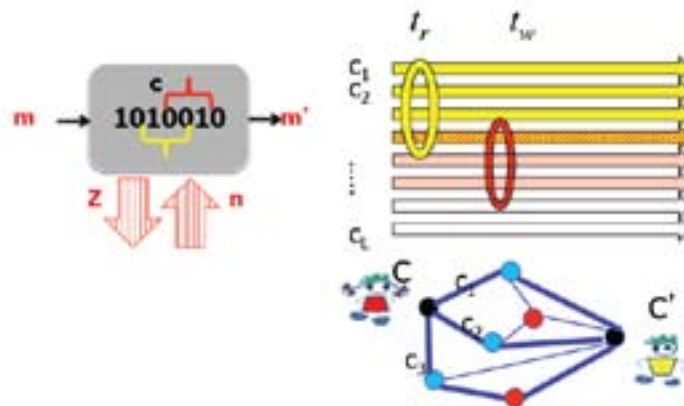
- $\Sigma = F_q$
- AWTPenc & AWTPdec
- Building blocks:
 1. AMD codes
 2. Subset evasive sets
 3. Folded Reed-Solomon codes

$$\text{AWTPenc} = \text{FRS}(\text{SEEnc}(\text{AMD}(m) \parallel [0]_g) \parallel [r]_{u\phi, L})$$

$$\text{AWTPdec} = \text{AMDdec}(\text{SEdec}(\text{FRSdec}(y)))$$

AWTP & *Secure Message Transmission*

- A more general adversary model



Concluding remarks

- Physical layer security: classical crypto with physical assumption
 - Key agreement
 - Encryption
- Guaranteeing eavesdropping assumptions
 - Environment dependence
- More research in,
 1. Adversary model for physical environments
 2. Constructions that gracefully degrade

Related publications

- Wang, Safavi-Naini, *Adversarial wiretap with Public Discussions*, CNS 2014
- Ahmadi, Safavi-Naini, *Private message transmission using multiple paths*, ACNS 2014
- Wang, Safavi-Naini, *A Model for Adversarial Wiretap Channel*, arXiv:1312.6457
- Safavi-Naini, Wang, *Efficient Codes for Limited View Adversarial Channels*, CNS 2013
- Safavi-Naini, Wang, *Codes for Limited View Adversarial Channels*, ISIT 2013.
- Ahmadi, Safavi-Naini, *Message Transmission and Key Establishment: Conditions for Equality of Weak and Strong Capacities*, FPS 2012
- Safavi-Naini, Tuhin, *Bounds and Constructions for 1-Round (t, k)-Secure Message Transmission against Generalized Adversary* AFRICACRYPT 2012
- Safavi-Naini, Tuhin & Wang, *A General Construction for 1-round RMT and (t, k)-SMT*, ACNS 2012.
- Tuhin, Safavi-Naini, *Optimal One Round Almost Perfectly Secure Message Transmission*, FC11
- Ahmadi, Safavi-Naini, *Secret Keys from Channel Noise*, Eurocrypt 2011.
- Ahmadi, Safavi-Naini, *Common Randomness and Secret Key Capacities of Two-way Channels*, ICITS 2011.
- Tuhin, Safavi-Naini, *Optimal Message Transmission Protocols with Flexible Parameters*, ASIACCS '11.
- Ahmadi, Safavi-Naini, *New Results on Secret Key Establishment over a Pair of Broadcast Channels*, ISITA 2010
- Ahmadi, Safavi-Naini, *Secret Key Establishment over a Pair of Independent Broadcast Channels*, ISITA 2010
- Shi, Jiang, Safavi-Naini, Tuhin, *Optimal Secure Message Transmission by Public Discussion*, ISIT '09

In collaboration with:

Ashraf Tuhin, Hongsong Shi, Shaoquan Jiang, Hadi Ahmadi, Pengwei Wang

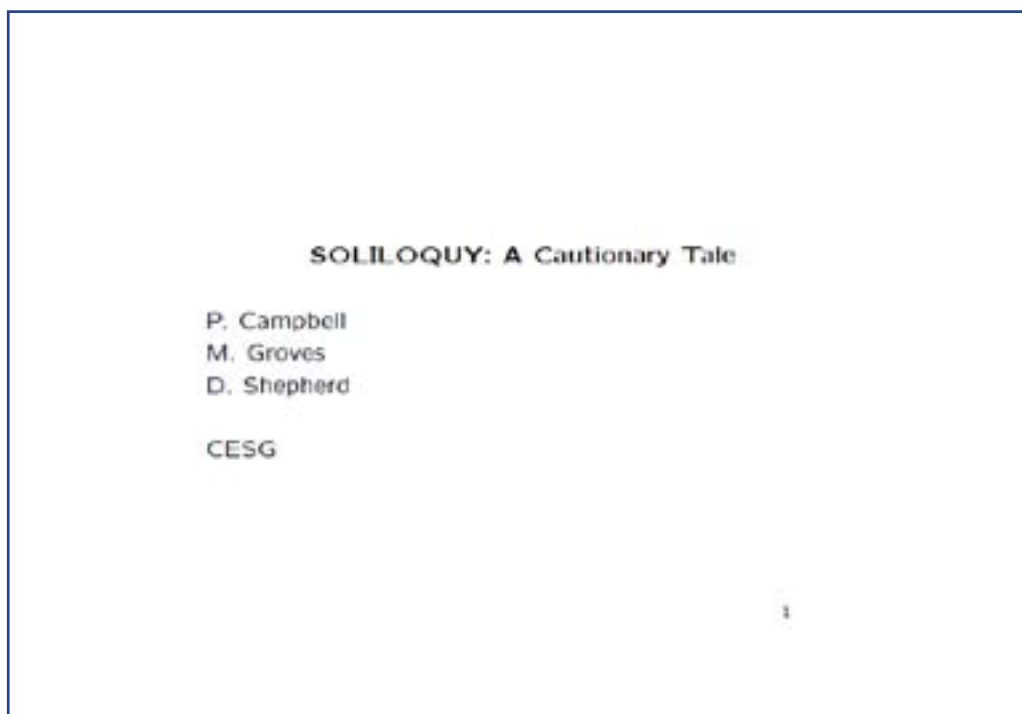
Thank you for listening and...questions?

SOLILOQUY: A Cautionary Tale*Michael Groves, CESG, UK*

We would like to offer a presentation on SOLILOQUY, a lattice-based primitive designed by CESG in 2007 as a basis for a key agreement protocol. After several years of analysis we have concluded that while SOLILOQUY should be classically secure, the hard problem on which it is based could in fact be solved by a quantum adversary and so the protocol would not be quantum-resistant as we had initially supposed.

Although we abandoned the development of SOLILOQUY in 2013, we believe that it contains several interesting ideas which would benefit from further study. For example, the public key for SOLILOQUY is very compact for a lattice-based PKC system, being only about the same size as a single RSA modulus. Also, the quantum algorithm extends work by Hallgren on computing generators of principal ideals in rings of algebraic integers and is, as far as we are aware, the first quantum attack on a lattice-based scheme.

The moral of the tale is that developing efficient quantum-safe cryptography is a very difficult task. The role of ETSI will be very important in ensuring that the many quantum-safe protocols currently being promoted for public use each receives a thorough and independent assessment.



Outline

We describe SOLILOQUY, a lattice-based primitive designed at CESG in 2007.

SOLILOQUY has several nice properties; in particular the public key is very compact for a lattice system.

We believe that SOLILOQUY is classically secure but were surprised to discover a potential quantum attack.

We sketch this attack, which we believe may be the first on a lattice-based PKC scheme.

Conclusions and further research.

2

SOLILOQUY

3

Some mathematical background

Let n be a prime and ζ a primitive n^{th} root of unity.

Let $K = \mathbb{Q}(\zeta)$ be the n^{th} cyclotomic field and $\mathcal{O} = \mathbb{Z}[\zeta]$ its ring of integers. Elements of \mathcal{O} are monic polynomials of the form $\alpha = \sum_{i=0}^{n-1} a_i \zeta^i \in \mathcal{O}$.

For primes $p \equiv 1 \pmod{n}$ the principal ideal $p\mathcal{O}$ decomposes into a product of prime ideals $p\mathcal{O} = \prod_{i=1}^{n-1} \mathcal{P}_i$.

The prime ideals \mathcal{P}_i are conjugates with norm $N(\mathcal{P}_i) = p$ and $\text{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$. They have a simple two-element representation $\mathcal{P} = p\mathcal{O} + (\zeta - e_i)\mathcal{O}$, where the e_i are n^{th} roots of unity in $\text{GF}(p)$.

We will be interested in the value $e = 2^{(p-1)/n} \pmod{p}$ and its prime ideal $\mathcal{P} = p\mathcal{O} + (\zeta - e)\mathcal{O}$.

4

Public and private keys

A candidate private key will be a "small" ring element $\alpha = \sum_{i=0}^{n-1} a_i \zeta^i \in \mathcal{O}$.

These are generated randomly (by sampling the coefficients from a discrete Gaussian distribution) and tested until we find an α such that $p = N(\alpha)$ is prime and $e \not\equiv 1 \pmod{p}$. Conjugate to get into the required form $\alpha\mathcal{O} = p\mathcal{O} + (\zeta - e)\mathcal{O}$.

Then set the SOLILOQUY private key to be α and its corresponding public key to be p .

5

The crypto primitive

For crypto applications we will want to define maps to encrypt and decrypt data.

We encode a ring element ϵ (plaintext or ephemerals) into an integer z (ciphertext) using the public key p :

$$\epsilon := \sum_{i=0}^{n-1} e_i \zeta^i \mapsto \sum_{i=0}^{n-1} e_i c^i \bmod p =: z$$

We can recover a "small" ϵ from z and the private key α by simply rounding:

$$\epsilon = z - \lfloor z\alpha^{-1} \rfloor \cdot \alpha.$$

6

SOLILOQUY as a GGH-type lattice scheme

Private / public lattice basis matrices with $H = \text{HNF}(C)$:

$$C = \begin{bmatrix} a_0 & \dots & a_{n-2} & a_{n-1} \\ a_{n-1} & & a_{n-3} & a_{n-2} \\ \vdots & & \ddots & \vdots \\ a_1 & & a_{n-1} & a_0 \end{bmatrix}, H = \begin{bmatrix} 1 & 0 & \dots & 0 & -e^{n-1} \\ 0 & 1 & & 0 & -e^{n-2} \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & & 1 & -e \\ 0 & 0 & & 0 & p \end{bmatrix}$$

Since α is small, C will be a reduced basis for the lattice and decryption is Babai's rounding algorithm.

The public key H can be reconstructed from just p , which is very compact for a lattice cryptosystem.

(Note: Smart-Vercauteren also used this HNF construction in their 2009 FHE scheme.)

7

Security

The security of SOLILOQUY can be analysed via the difficulty of two well known hard problems.

CVP. Classical CVP security via LBR is well understood. There is no known significant (exponential) quantum speed-up.

PIP: Given a representation of a principal ideal I of \mathcal{O} , compute a small generator α of I . The known (at that time) classical and quantum algorithms are only practical for number fields of small, fixed degree.

We believed for several years that since SOLILOQUY used large degree fields it should be quantum resistant.

8

Outline of a quantum attack

9

Some simplifying assumptions

Likely true for our specific situation but not in general: We know the generators for the unit group. We can recover α from any generator of $\alpha\mathcal{O}$. It is enough to recover $\alpha \cdot \alpha^*$ in the ring of integers $\mathcal{O}' = \mathbb{Z}[\zeta + \zeta^{-1}]$ of $K' = \mathbb{Q}(\zeta + \zeta^{-1})$.

We thus re-cast the problem as: Given a generating set u_1, \dots, u_{r-1} of the unit group \mathcal{O}^\times recover any generator of the principal ideal $\alpha\mathcal{O}$ in the ring of integers \mathcal{O} of a totally real field of degree r .

This special case turns out to be tractable. Our approach is similar the work of Hallgren and co-authors on unit groups and related number-theoretic problems.

10

SOLILOQUY as a hidden lattice problem

The embedding $\log(\omega) = (\log(|\sigma_0(\omega)|), \dots, \log(|\sigma_{r-1}(\omega)|))$ maps \mathcal{O}^\times to a rank $r-1$ lattice $\Lambda = \log(\mathcal{O}^\times)$. Encode α as the rank r lattice: $\Lambda_\alpha = \begin{bmatrix} -1 & \log(\alpha) \\ 0 & \Lambda \end{bmatrix}$.

Hide Λ_α by defining a function $F : \mathbb{Z} \times \mathbb{R}^r \rightarrow \mathbb{R}^r$, such that $F(k, v) = F(k', v')$ iff $(k, v) \equiv (k', v') \pmod{\Lambda_\alpha}$.

Restrict the input domain to $G \subset \mathbb{Z} \times \mathbb{R}^r$ where

$$G = \left\{ (k, v) \in \mathbb{Z} \times \mathbb{R}^r : \sum_{i=0}^{r-1} v_i = -k \log(N(\alpha, \mathcal{O})) \right\}$$

and set

$$F(k, v) = \exp(v) \cdot (\alpha\mathcal{O})^k.$$

11

The quantum algorithm

1**. For an input $(k, v) \in G$ compute a "quantum fingerprint" $\psi_{(k,v)}$ representing the lattice $F(k, v)$.

2**. Discretise and bound G and form the superposition

$$\sum_{(k,v) \in G} |k, v, 0\rangle \mapsto \sum_{(k,v) \in G} |k, v, \psi_{(k,v)}\rangle$$

3. Take a QFT over G and measure the third register to obtain an approximate basis for the dual lattice Λ_{α}^* .

4. Iterate the previous steps to produce many samples close to Λ_{α}^* .

5. Use classical LBR to compute an approximate basis for Λ_{α} and hence α . (Requires sufficient precision.)

12

Fingerprints and binning

13

Lattice fingerprints

Our “quantum fingerprint” will be a model for the superposition of the short vectors in a given lattice.

Let B be a Gram-Schmidt lattice basis matrix in \mathbb{R}^n and let $l \in \mathbb{R}$ be some fixed length. We use an ‘enumeration’ map $\phi: [0, l) \rightarrow \mathbb{Z}^n$ depending on n , B , and l , which can be inverted at integer points (to facilitate reversible quantum computation).

Let $C_n(B, l) := \{ \phi(x) : x \in [0, l) \cap \mathbb{Z} \}$. This is a discretised model for $E_n(\rho) := \text{Ball}_{n, \rho} \cdot B^{-1}$ in the sense that that it fits within an ellipsoid $E_n(\rho + \epsilon)$ and covers all the integer points in $E_n(\rho - \epsilon)$.

$$E_n(\rho - \epsilon) \cap \mathbb{Z}^n \subseteq C_n(B, l) \subseteq E_n(\rho + \epsilon) \cap \mathbb{Z}^n.$$

14

Let O be the isometry between the Gram-Schmidt and the “natural” bases for the lattice. Then $v \in C_n(B, l)$ indexes $v \cdot B$, a short vector in the Gram-Schmidt basis corresponding to the natural vector $v \cdot B \cdot O$.

We use another lattice to partition up natural space into cells or “bins”. Vector $v \cdot B \cdot O$ will be replaced by the label u of its bin, reducing precision by a carefully-chosen scaling factor q . Define *Simple binning* as:

$$u = \theta_B(v) := [q \cdot v \cdot B \cdot O].$$

(The *Randomised* variant $\theta_{R, w, B}(v) := [q \cdot v \cdot B \cdot O \cdot R + w]$ is preferable, because over many random choices R and w , the likelihood of two vectors going into the same bin depends *only* on their separation relative to q .)

15

Our (simple) quantum fingerprint generator computes

$$|k, v\rangle |0\rangle \rightarrow \frac{1}{\sqrt{[l]}} \sum_{x=0}^{[l]-1} |k, v\rangle |\theta_{B(k,v)}(\phi(x))\rangle$$

The pure state

$$|\psi_{(k,v)}\rangle := \frac{1}{\sqrt{[l]}} \sum_{x=0}^{[l]-1} |\theta_{B(k,v)}(\phi(x))\rangle$$

is called the (simple) quantum fingerprint of (k, v) .

The coherent randomised version is:

$$|\psi'_{(k,v)}\rangle := \frac{\sum_R \sum_w \sum_{x=0}^{[l]-1} |R\rangle |w\rangle |\theta_{R,w,B(k,v)}(\phi(x))\rangle}{\sqrt{\#R \cdot \#w \cdot [l]}}$$

16

The fingerprint structure allows us to define a *fidelity* between two different descriptions

$$Fid((k, v), (k', v')) := \langle \psi'_{(k,v)} | \psi'_{(k',v')} \rangle.$$

A fidelity of 1 would indicate that $C(B, l) \cdot B \cdot O$ and $C(B', l) \cdot B' \cdot O'$, activate exactly the same set of bins (for every R, w binning strategy) and so lattices must be very similar, or identical. When the two lattices are 'essentially different', there is no reason to expect significant overlap in any region, and so the fidelity should be small.

The idea is that, for correctly chosen (l, q) , the numerical instability arising from computing $F(k, v)$ is removed by the binning strategy, as (real, infinite) $F(k, v)$ is replaced with (discrete, bounded) $\psi'_{(k,v)}$.

17

Open questions and conclusions

18

We abandoned the development of SOLILOQUY in early 2013 and are not recommending it for any real-world applications.

However there are several interesting ideas presented here which might benefit from further study:

* A compact public key for lattice PKC. See also Smart-Vercauteren's application to FHE.

* This may be the first quantum attack on a lattice-based PKC protocol. However ours is a very special case (cyclotomics) that does not easily generalise.

* Other approaches to lattice fingerprints are possible. Hallgren et. al. have recently suggested using multiple Gaussian sampling.

19

Conclusion

We have outlined one approach to lattice fingerprints which we believe could be combined with a quantum PIP algorithm to give an attack on SOLILOQUY.

Designing quantum-safe cryptography is difficult. It took us several years to develop SOLILOQUY and several more to assess its potential quantum resistance.

At this time, when many novel types of quantum-safe cryptography are being proposed, the work of ETSI and others will be very important in ensuring these receive a thorough and independent assessment.

29

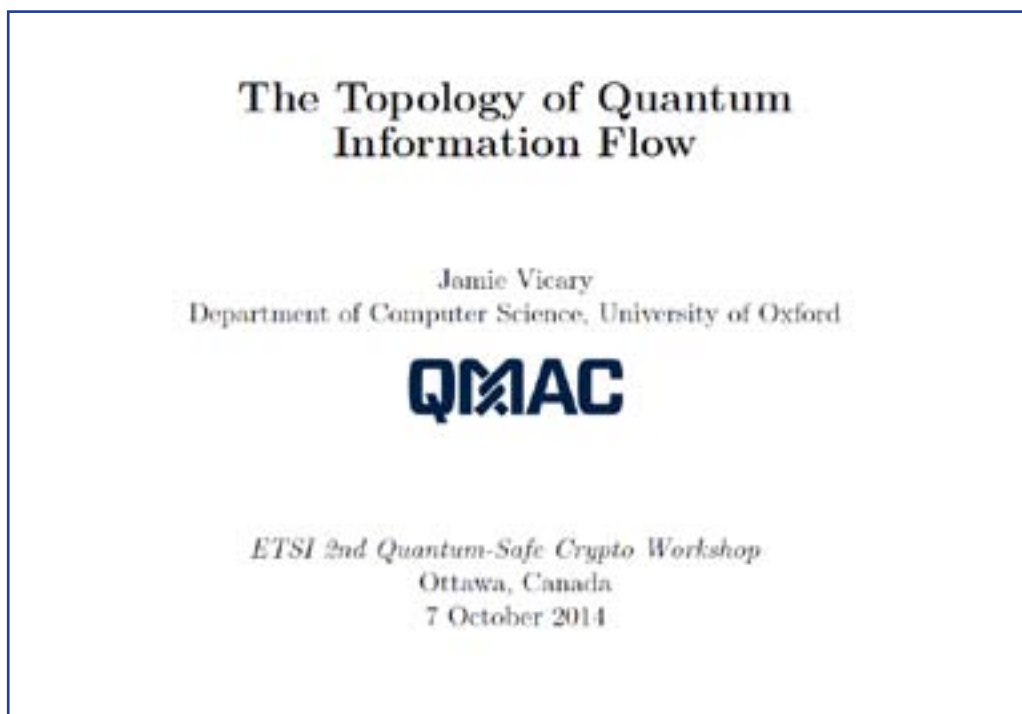
Presentations

SESSION 7
SYSTEMS AND ATTACKS, continued

The topology of quantum information flow

Jamie Vicary, Oxford University

Many of the strange properties of quantum information make more sense when we realize that quantum information behaves in a fundamentally topological way. I will give an overview of some of the research carried out in Oxford into the topology of quantum information, and show how it gives insight into the high-level mathematical foundations of perfectly secure quantum and classical encrypted communication.

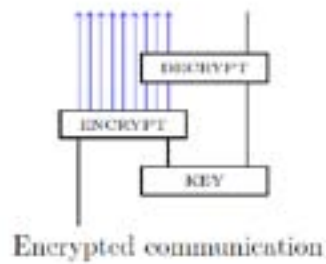


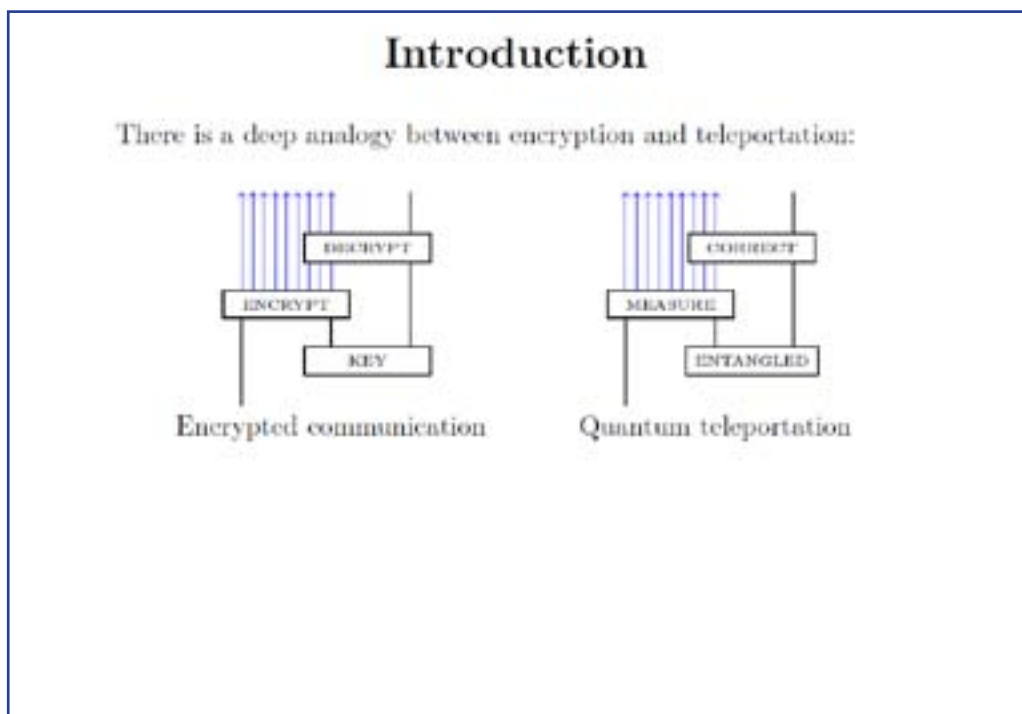
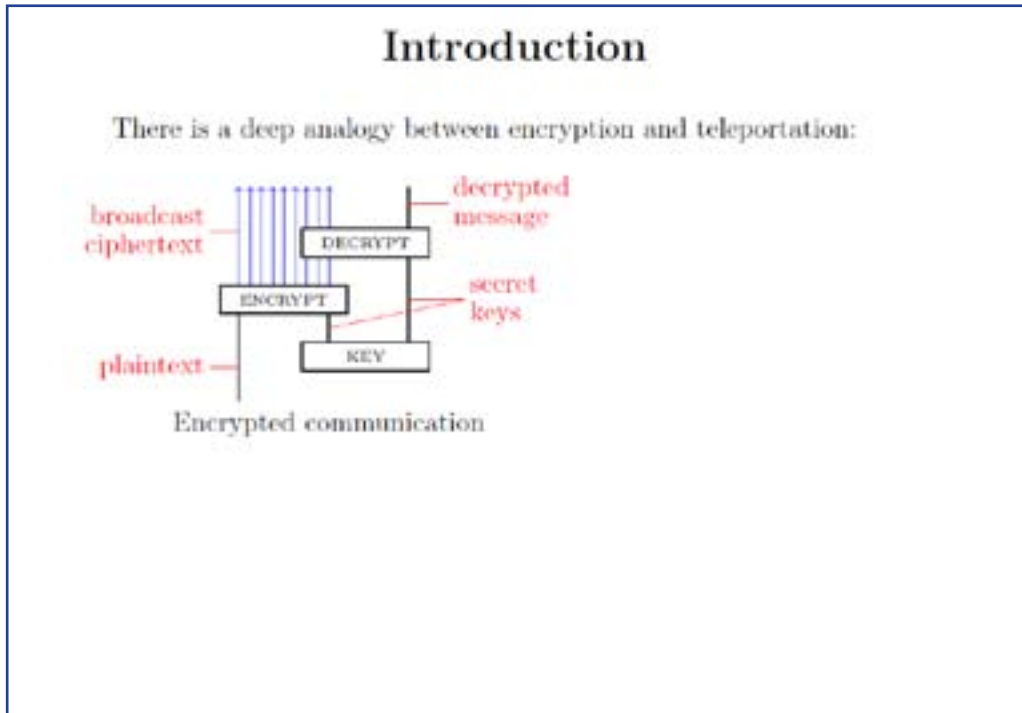
Introduction

There is a deep analogy between encryption and teleportation:

Introduction

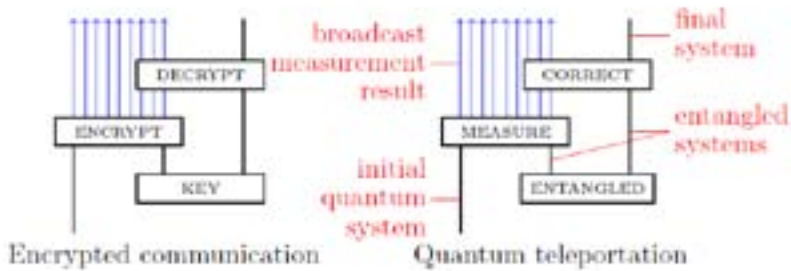
There is a deep analogy between encryption and teleportation:





Introduction

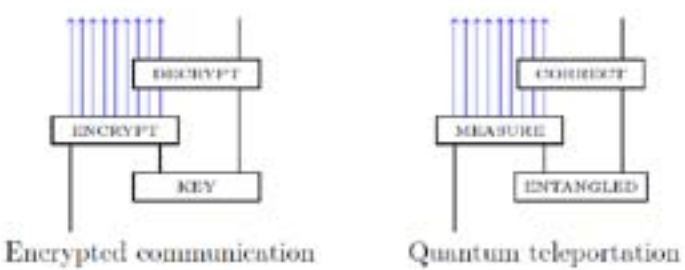
There is a deep analogy between encryption and teleportation:



Encrypted communication Quantum teleportation

Introduction

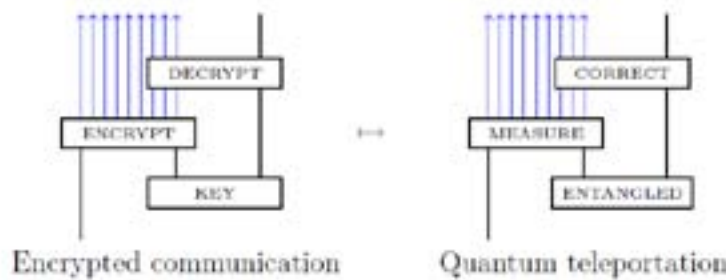
There is a deep analogy between encryption and teleportation:



Encrypted communication Quantum teleportation

Introduction

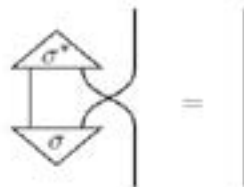
There is a deep analogy between encryption and teleportation:



New idea. We can make this precise using topological mathematics.
Nice result. There is a general classical-to-quantum construction.
 Part of the *categorical quantum computing* programme launched by Abramsky and Coecke in 2004.

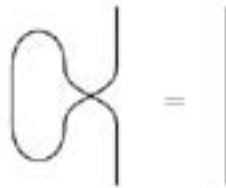
Strings and correlation

Consider the following equation, where σ is a bipartite state preparation and σ^* is the corresponding bipartite postselection:



Strings and correlation

Consider the following equation, where σ is a bipartite state preparation and σ^* is the corresponding bipartite postselection:



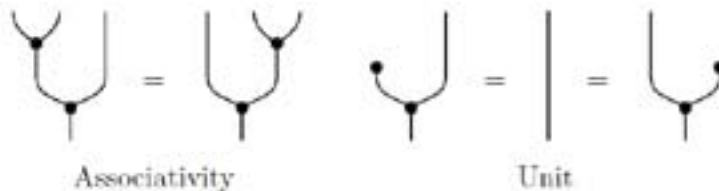
We change notation and use **topological strings**.

We can investigate consequences of this equation in different settings.

- ▶ **Quantum theory.**
The state σ is *maximally entangled*: $|\sigma\rangle = |00\rangle + |11\rangle$
- ▶ **Classical computation.**
The state σ is *perfectly correlated*: $\sigma = \{00\} \sqcup \{11\}$.

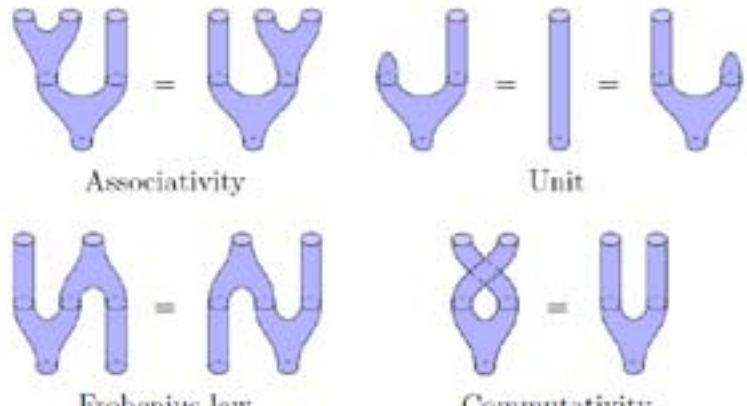
Surfaces and logic

We now think about basic properties of copying, comparing and deleting classical information:



Surfaces and logic

We now think about basic properties of copying, comparing and deleting classical information:



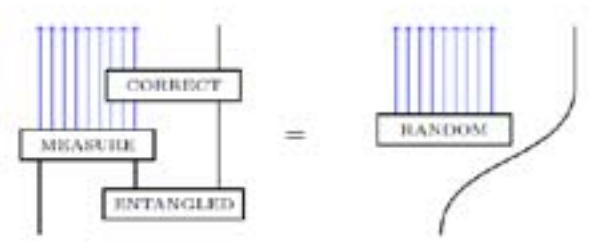
The diagrams show four types of topological surfaces with labels below them:

- Associativity:** A surface with three tubes merging into one, shown in two equivalent configurations.
- Unit:** A surface with one tube merging into two, shown as equivalent to a single tube.
- Frobenius law:** A surface with two tubes merging into one and another tube branching from the merge point, shown in two equivalent configurations.
- Commutativity:** A surface with two tubes crossing each other, shown as equivalent to a surface where the tubes do not cross.

These are the laws obeyed by surfaces up to deformation!
So we change notation and use **topological surfaces**.

Geometrical structure

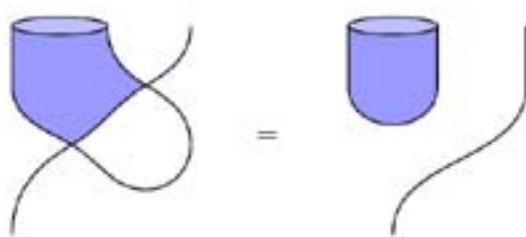
Here is ordinary teleportation:



The diagram illustrates the process of ordinary teleportation. On the left, a vertical line representing an input state enters a box labeled 'MEASURE'. This box is connected to another box labeled 'ENTANGLED'. A box labeled 'CORRECT' is also connected to the 'MEASURE' box. On the right, a vertical line representing the output state enters a box labeled 'RANDOM'. An equals sign is placed between the two sides of the diagram.

Geometrical structure

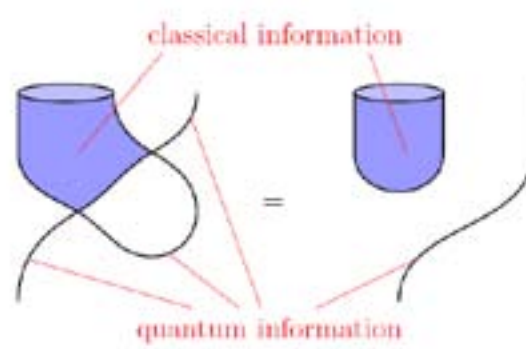
Here is ordinary teleportation:



We make it rigorous with this geometrical equation.

Geometrical structure

Here is ordinary teleportation:



We make it rigorous with this geometrical equation.

Geometrical structure

Here is ordinary teleportation:

We make it rigorous with this geometrical equation.

Theorem. Quantum solutions correspond exactly to implementations of quantum teleportation.

Geometrical structure

Here is ordinary teleportation:

We make it rigorous with this geometrical equation.

Theorem. Classical solutions correspond exactly to implementations of classical one-time-pad encryption.

So what?

- ▶ Allows us to reason logically about cryptographic primitives in both quantum and classical computation.
- ▶ Provides a formal foundation for computational support tools.
- ▶ Gives a unified setting to consider integrated classical and quantum phenomena—for example, QKD+OTP.
- ▶ Addresses fascinating conceptual questions:
 - What is the fundamental relationship between classical and quantum computation?
 - What is the mathematical structure of quantum information flow?

Thank you!

An efficient and provably secure authenticated key exchange with forward security from RLWE

Jintai Ding, University of Cincinnati



The second ETSI quantum-safe workshop

**A Simple Provably Secure Key Exchange Scheme
Based on the Learning with Errors Problem**

Jintai Ding
University of Cincinnati
This includes joint work with X. Ling, X. Xiang, J. Zhang, Z. Zhang, M. Seook, O. Dagdelen

Oct. 7, 2014

A slide of Dr. Lily Chen in the first ETSI workshop

Practical Challenge

- Quantum computing will break many public-key cryptographic algorithms/schemes
 - Key agreement (e.g. DH and MQV)
 - Digital signatures (e.g. RSA and DSA)
 - Encryption (e.g. RSA)
- These algorithms have been used to protect Internet protocols (e.g. IPsec) and applications (e.g. TLS)
- NIST is studying "quantum-safe" replacements
- This talk will focus on practical aspects
 - For security, see Yi-Kai Liu's talk later today

2 / 19



Where do we really need public key cryptosystems?

- ▶ Digital signature – authentication
 - Software update
- ▶ Public key encryption systems are almost never used to send information but keys — **key agreement**

SSL TLS
- ▶ We can achieve this goal with encryption or **key exchange** like Diffie-Hellmann.

3 / 19



Key Agreement from Encryption versus Key Exchange?

- ▶ Encryption (Key Transport): Party A uses Party B's public key to encrypt a random string and sends the ciphertext to B. B decrypts it and get the random string.

In practice, public key encryption is only used to transmit random keys. (The key is only determined by one party)

- ▶ Using PKE can not guarantee **forward security**.
 - ▶ If the attacker gets the static secret key, then he will learn every communication made before.
The **Heartbleed** problem.

4 / 19

◀ ▶ ⏪ ⏩ 🔍 🔄

What's Key Exchange



- ▶ Two parties get a shared secret key over an unsecure channel.

5 / 19

◀ ▶ ⏪ ⏩ 🔍 🔄

The Elegant Diffie-Hellman Protocol

$(g^b)^a$ $\xrightarrow{g^a}$ $\xleftarrow{g^b}$ $(g^a)^b$

▶ Using the simple and elegant fact:

$$g^{ab} = (g^b)^a = (g^a)^b.$$

◀ ▶ ⏪ ⏩ 🔍 🔄

6 / 19

Motivation and Results

Motivation:

- ▶ Can we get a DH analogy from other mathematical tools?
- ▶ Can we get KE from lattices (say, LWE, which is apparent resistance to quantum attacks)?
- ▶ If so, can we get better efficiency and better security guarantees.

Our Results:

- ▶ An Efficient (2-round) key exchange protocol from LWE and RLWE.
- ▶ It is provably secure and it is very efficient.

◀ ▶ ⏪ ⏩ 🔍 🔄

7 / 19

Learning with Errors (LWE) [Oded Regev 2005]

Goal: **distinguishing** "noisy inner products" from uniform.

$a_1 \leftarrow \mathbb{Z}_q^n;$	$b_1 = \langle a_1, s \rangle + e_1 \pmod q$
$a_2 \leftarrow \mathbb{Z}_q^n;$	$b_2 = \langle a_2, s \rangle + e_2 \pmod q$
\vdots	\vdots
$a_m \leftarrow \mathbb{Z}_q^n;$	$b_m = \langle a_m, s \rangle + e_m \pmod q$
<hr/>	
$a_1 \leftarrow \mathbb{Z}_q^n;$	$b_1 \leftarrow \mathbb{Z}_q$
$a_2 \leftarrow \mathbb{Z}_q^n;$	$b_2 \leftarrow \mathbb{Z}_q$
\vdots	\vdots
$a_m \leftarrow \mathbb{Z}_q^n;$	$b_m \leftarrow \mathbb{Z}_q$

In a matrix form

$$(A \cdot As + e) \approx_e (A, b)$$

Where $s \leftarrow \mathbb{Z}_q^n$, $m = \text{poly}(n)$, $q = \text{poly}(n)$ and $e_i \leftarrow \chi$ is some distribution in \mathbb{Z} . e_i has small size, much smaller than q .

8 / 19

Navigation icons

Provable security

Theorem (Informal)[Reg'05]

Let χ be a discrete Gaussian distribution with parameter $0 < \alpha < 1$, s.t. $\alpha q \geq 2\sqrt{n}$. If there exists a polynomial time algorithm solves LWE problem, then there exists a **quantum** algorithm solves (n/α) -SVP problems for **all** n -dimension lattices.

► $s \leftarrow \chi^n$ is as hard as standard LWE ($s \leftarrow \mathbb{Z}_q^n$) [ACPS'09].




8 / 19

Navigation icons


Our Protocol (basic idea)

Public Parameter: $M \leftarrow \mathbb{Z}_q^{n \times n}$



$s_A^T p_B$

$$\begin{aligned} & \xrightarrow{p_A = Ms_A + 2e_A} \\ & \xleftarrow{p_B = M^T s_B + 2e_B} \end{aligned}$$



$p_A^T s_B$

\approx

- ▶ $s_A^T p_B = s_A^T M^T s_B + 2s_A^T e_B \approx s_A^T M^T s_B + 2e_A^T s_B = p_A^T s_B$.
- ▶ note that s_A, s_B, e_A, e_B are "small".
- ▶ the difference between $s_A^T p_B$ and $p_A^T s_B$ is even

10 / 19
◀ ▶ ↻ 🔍

Our Robust Modular Extractor

We first define two functions: for $q > 2$ is prime

$$\sigma_0(x) = \begin{cases} 0, & x \in [-\lfloor \frac{q}{4} \rfloor, \lfloor \frac{q}{4} \rfloor]; \\ 1, & \text{otherwise.} \end{cases}; \quad \sigma_1(x) = \begin{cases} 0, & x \in [-\lfloor \frac{q}{4} \rfloor + 1, \lfloor \frac{q}{4} \rfloor + 1]; \\ 1, & \text{otherwise.} \end{cases}$$

The hint algorithm $S(y)$: $b \leftarrow \{0, 1\}, S(y) = \sigma_b(y)$.

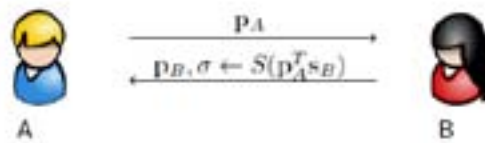
The robust extractor $E(x, \sigma)$:

$$E(x, \sigma) = \left(x + \sigma \cdot \frac{q-1}{2} \bmod q \right) \bmod 2$$

11 / 19
◀ ▶ ↻ 🔍

Removing the Approximation

Public Parameter: $M \leftarrow \mathbb{Z}_q^{n \times n}$



- ▶ A outputs $E(s_A^T p_B, \sigma)$
- ▶ B outputs $E(p_A^T s_B, \sigma)$

12 / 19



Security

- ▶ The security proof is given from a series of hybrid experiments.
- ▶ Next — **the problem of authentication** – man in the middle attack!!!
- ▶ We can build an authenticated key exchange (AKE) protocol, which can be seen as an HMQV-like AKE from lattices.
- ▶ The protocol is simple since it does not involve any other cryptographic primitives to achieve authentication (e.g., signatures) and the system is also very efficient.

13 / 19



AKE from ring-LWE

Party i

Public Key: $p_i = as_i + 2e_i \in R_q$
 Secret Key: $s_i \in R_q$
 where $s_i, e_i \leftarrow \chi_\alpha$

$x_i = ar_i + 2f_i \in R_q$
 where $r_i, f_i \leftarrow \chi_\beta$

$k_i = (p_j d + w_j)(s_i c + r_i) + 2g_i$
 where $g_i \leftarrow \chi_\beta$
 $\sigma_i = \text{Mod}_2(k_i, w_j) \in \{0, 1\}^n$
 $sk_i = H_2(i, j, x_i, w_j, \sigma_i)$

Party j

Public Key: $p_j = as_j + 2e_j \in R_q$
 Secret Key: $s_j \in R_q$
 where $s_j, e_j \leftarrow \chi_\alpha$

$y_j = ar_j + 2f_j \in R_q$
 $k_j = (p_i c + x_i)(s_j d + r_j) + 2g_j$
 where $r_j, f_j, g_j \leftarrow \chi_\beta$
 $w_j = \text{Cho}(k_j) \in \{0, 1\}^n$
 $\sigma_j = \text{Mod}_2(k_j, w_j) \in \{0, 1\}^n$
 $sk_j = H_2(i, j, x_i, w_j, \sigma_j)$

$\xrightarrow{x_i}$
 $\xleftarrow{w_j, \sigma_j}$

$c = H_1(i, j, x_i) \in R, d = H_1(j, i, y_j, x_i) \in R$

28 / 28
◀ ▶ ⏪ ⏩ 🔍 🔄

AKE from ring-LWE

Intuition for Security:

- We can prove the security of the system
- We can prove the forward security of the system
- We did preliminary implementation and it is very efficient.
- Parameters for implementation:

Parameters	n	Security (expt.)	α	γ	$\log \frac{\beta}{\alpha}$	$\log q$ (bits)
I*	1024	80 bits	3.397	101.919	8.5	40
II	2048	80 bits	3.397	161.371	27	78
III	2048	128 bits	3.397	161.371	19	63
IV	4096	128 bits	3.397	256.495	50	125
V	4096	192 bits	3.397	256.495	36	97
VI	4096	256 bits	3.397	256.495	28	81

29 / 28
◀ ▶ ⏪ ⏩ 🔍 🔄

AKE from ring-LWE

Communication Overheads:

Choice of Parameters	Size (KB)			
	pk	sk (expt.)	init. msg	resp. msg
I*	5 KB	0.75 KB	5 KB	5.125 KB
II	19.5 KB	1.5 KB	19.5 KB	19.75 KB
III	15.75 KB	1.5 KB	15.75 KB	16 KB
IV	62.5 KB	3 KB	62.5 KB	63 KB
V	48.5 KB	3 KB	48.5 KB	49 KB
VI	40.5 KB	3 KB	40.5 KB	41 KB

The bound 6ϵ with $\text{erfc}(6) \approx 2^{-55}$ is used to estimate the size of secret keys.

AKE from ring-LWE

Timings:

Parameters	Initiation	Response	Finish
I	3.22 ms (0.02 ms)	8.50 ms (4.60 ms)	5.23 ms (4.73 ms)
II	12.00 ms (0.04 ms)	29.33 ms (14.64 ms)	17.28 ms (14.61 ms)
III	10.33 ms (0.04 ms)	25.83 ms (13.46 ms)	15.58 ms (13.40 ms)
IV	83.61 ms (0.08 ms)	156.58 ms (39.86 ms)	73.11 ms (39.73 ms)
V	61.74 ms (0.08 ms)	117.81 ms (32.58 ms)	55.64 ms (32.20 ms)
VI	25.42 ms (0.08 ms)	62.31 ms (31.32 ms)	36.80 ms (31.20 ms)

Table : Timings of Proof-of-Concept Implementations in ms (The figures in the parentheses indicate the timings with pre-computing. For comparison, by simply using the "speed" command in openssl on the same machine, the timing for dsa1024 signing algorithm is about 0.7 ms, and for dsa2048 is about 2.3 ms).

We believe our systems are very suitable for practical applications and they have very strong security.

Summary

- ▶ We build KE and AKE based on LWE and RLWE.
- ▶ They are provably secure against both classical and quantum attacks.
- ▶ We can prove the Forward Security of the AKE.
- ▶ Our preliminary implementations are very efficient.
- ▶ Our KE and AKE are strong candidates for quantum-safe crypto.

18 / 19



Thank You!



