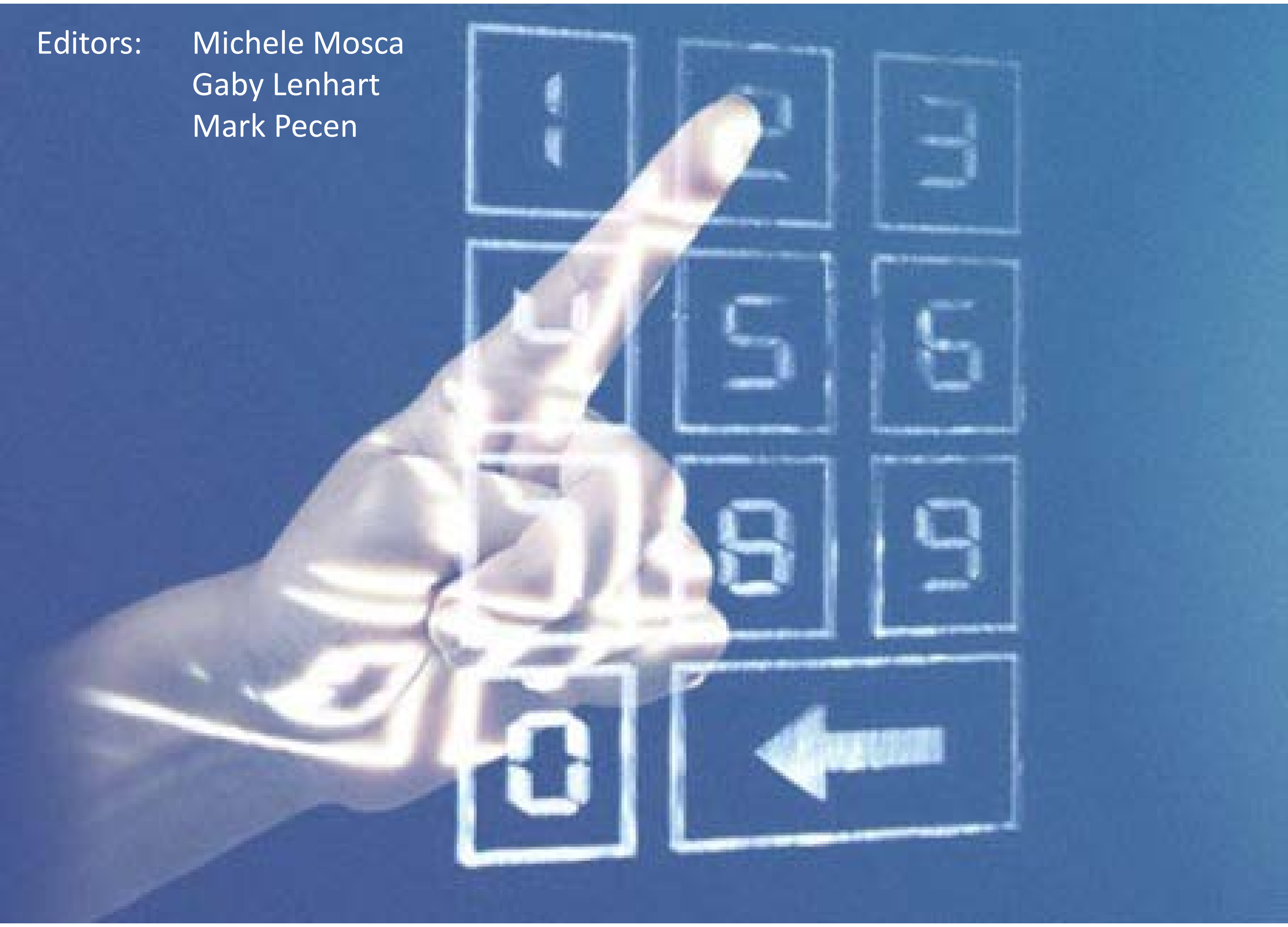
e-proceedings



Editors: Michele Mosca
Gaby Lenhart
Mark Pecen

Partner: IQC Institute for Quantum Computing

Sponsor: Cyber-sécurité VENUS Cybersecurity

Supporters:: CryptoWorks21

2nd Quantum-Safe-Crypto Workshop

Ottawa, Canada, 6-7 October 2014

ISBN 979-10-92620-04-7

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

ISBN 979-10-92620-04-7

- 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 Pecen**, 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 Pecen, Approach Infinity

ISBN 979-10-92620-04-7

ISBN 979-10-92620-04-7

ETSI World Class Standards

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 Pecen, 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

ISBN 979-10-92620-04-7

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 Chunnilall, 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

ISBN 979-10-92620-04-7

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

ISBN 979-10-92620-04-7

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 TMobile 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.

ISBN 979-10-92620-04-7

Speakers

SESSION 1
SETTING THE SCENE

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 Steward 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 Sience ate 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. His is a member of the German Academy of Science and Engineering acatech and of the German Academy of Science Leopoldina.

ISBN 979-10-92620-04-7

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 Quantun 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.

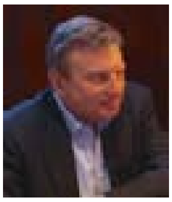
ISBN 979-10-92620-04-7

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 Pecen, Approach Infinity, Inc.

Mark Pecen 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. Pecen 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, Pecen also managed consultation work for clients in North America and Europe. Pecen 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. Pecen 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.

ISBN 979-10-92620-04-7

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, Verisigni

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.

ISBN 979-10-92620-04-7

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.

ISBN 979-10-92620-04-7

Speakers

SESSION 4 STANDARDIZATION AND CERTIFICATION

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 Chunnilall, National Physical Laboratory (UK)

Dr Christopher Chunnilall 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 postdoctal 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.

ISBN 979-10-92620-04-7

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 authentification 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.

ISBN 979-10-92620-04-7

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 habiliation (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

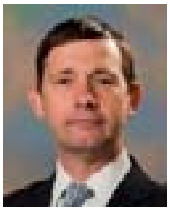
Rei Safavi-Naini, University of Calgary

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/

ISBN 979-10-92620-04-7

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

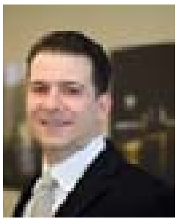
Jintai Ding is a professor at the Department of Mathematical Sciences of the University of Cincinnati. He received his B.A. from Xian Jiaotong University in 1988, his M.A. in mathematics from the University of Science and Technology of China in 1990 and his Ph.D in mathematics from Yale in 1995. He was 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.

ISBN 979-10-92620-04-7

Speakers

SESSION 8
CONFERENCE CONCLUSIONS

Summary of each session by session chair and general event conclusion



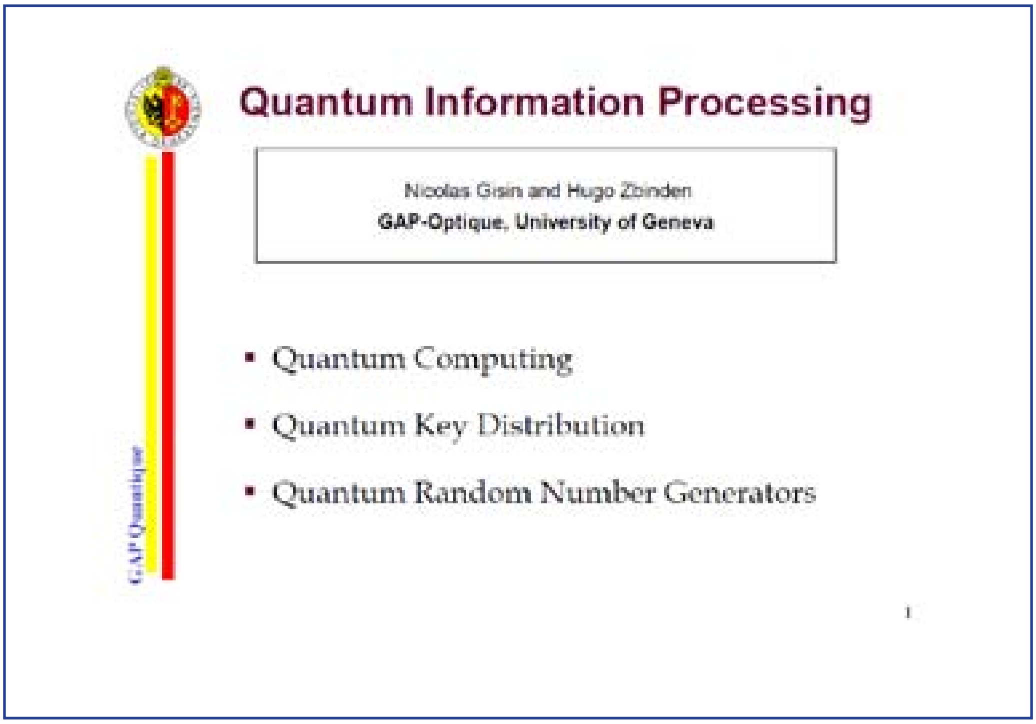
Michele Mosca, Institute for Quantum Computing at the University of Waterloo

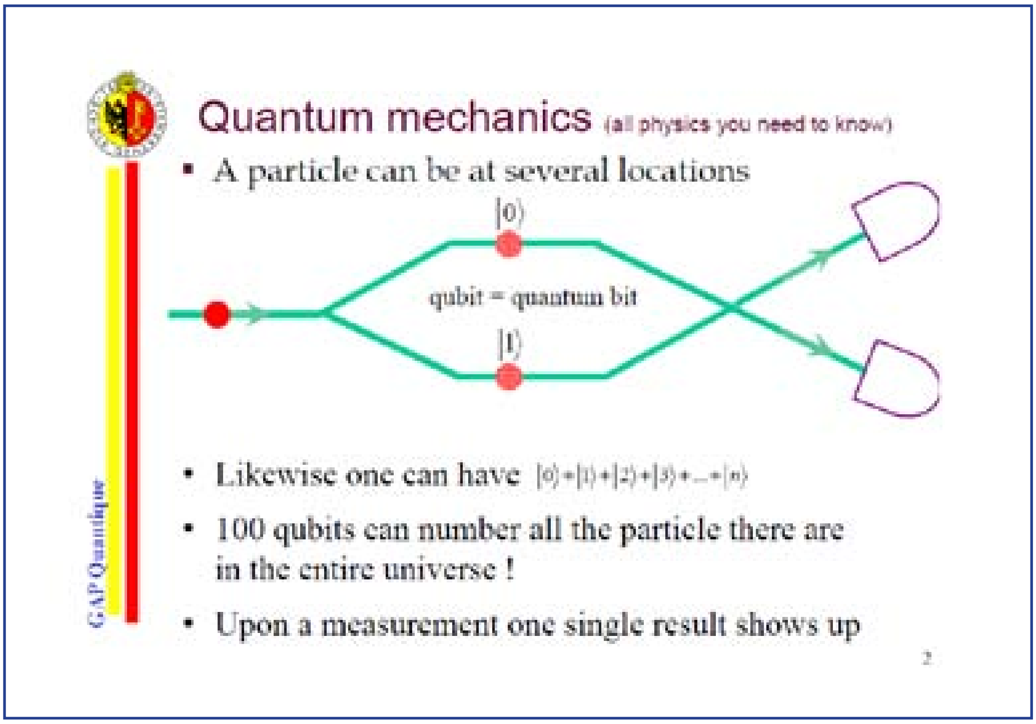
Michele Mosca (DPhil, Oxford) is co-founder and Deputy Director of the Institute for Quantum Computing at the University of Waterloo, and a founding member of the Perimeter Institute for Theoretical Physics. He is co-founder and director of the NSERC CREATE Training Program in Building a Workforce for 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).

ISBN 979-10-92620-04-7

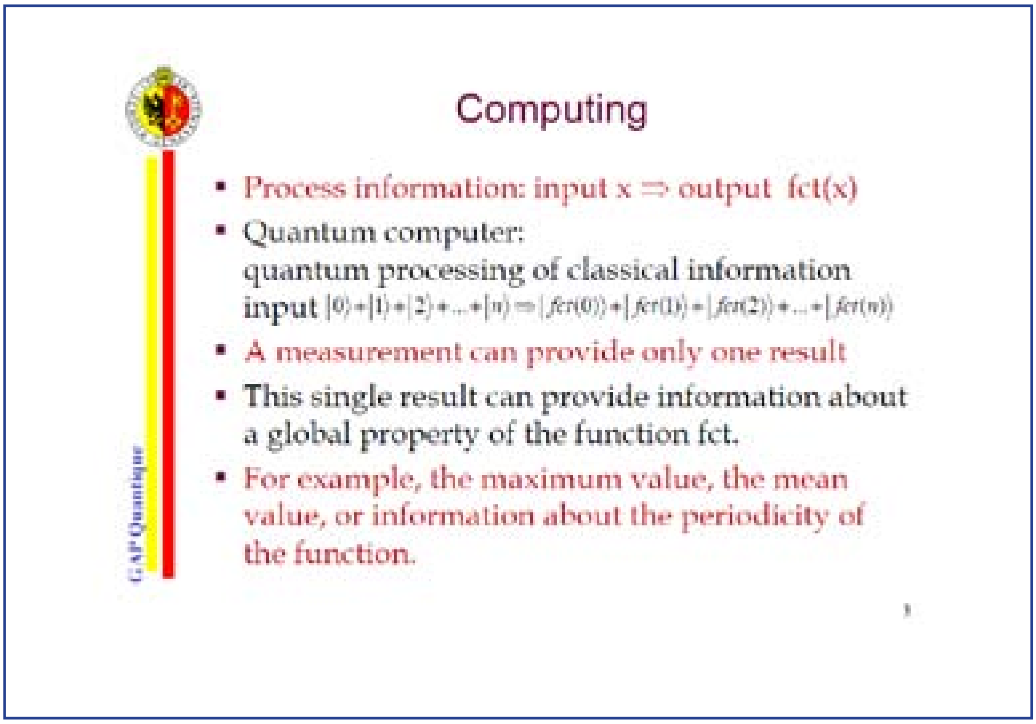
KEYNOTE Speech 2

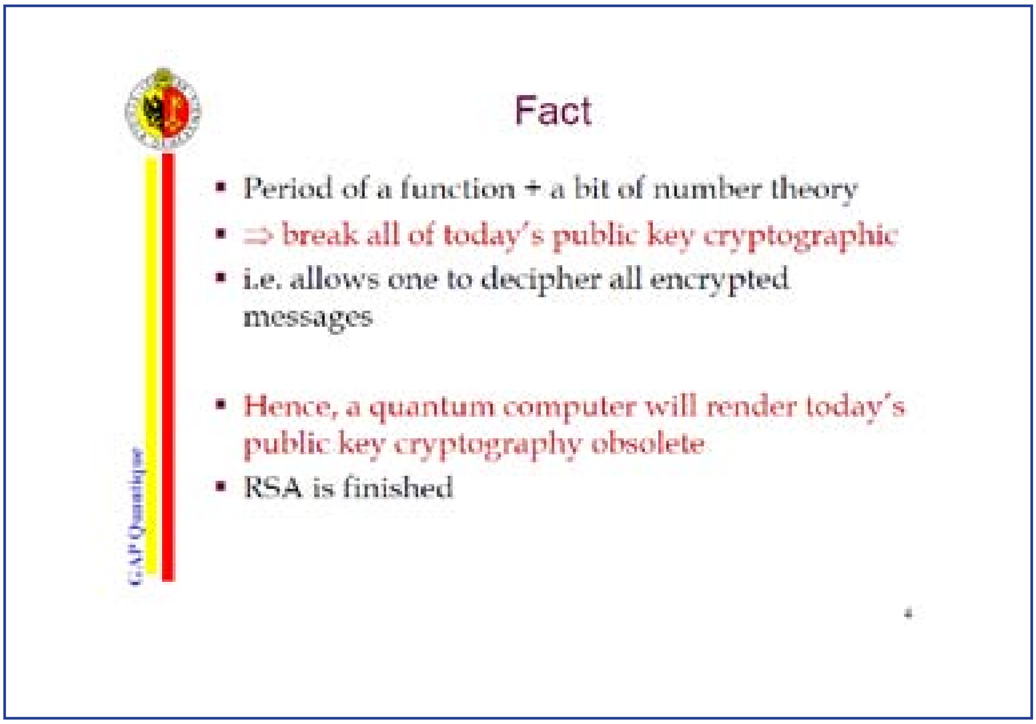
Nicolas Gisin, University of Geneva





ISBN 979-10-92620-04-7



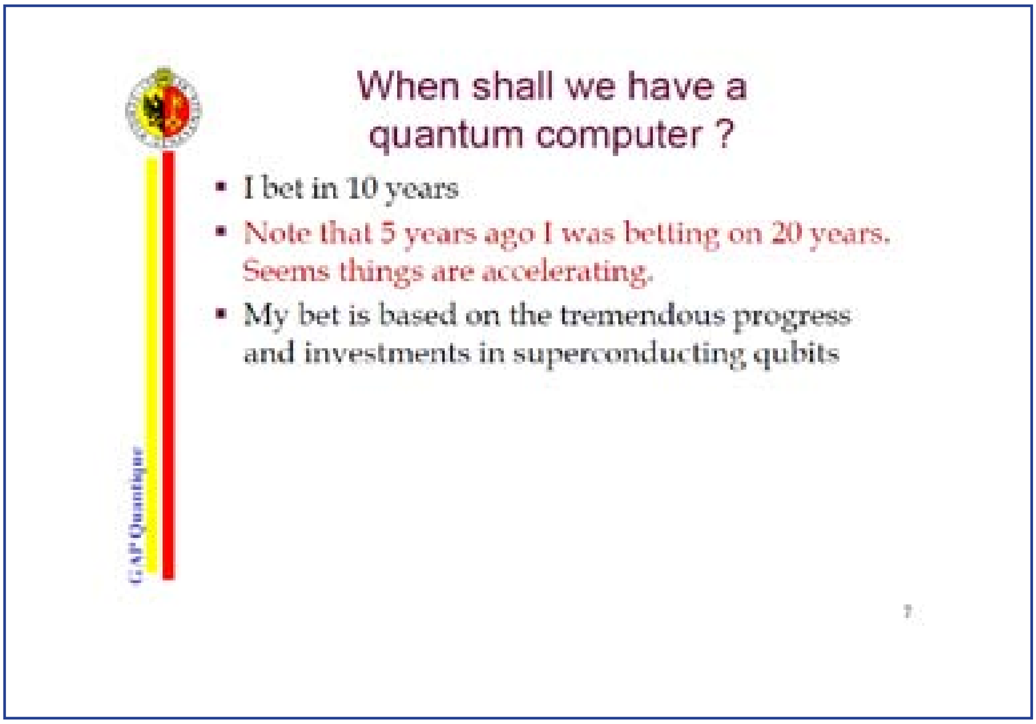


ISBN 979-10-92620-04-7

Presentations

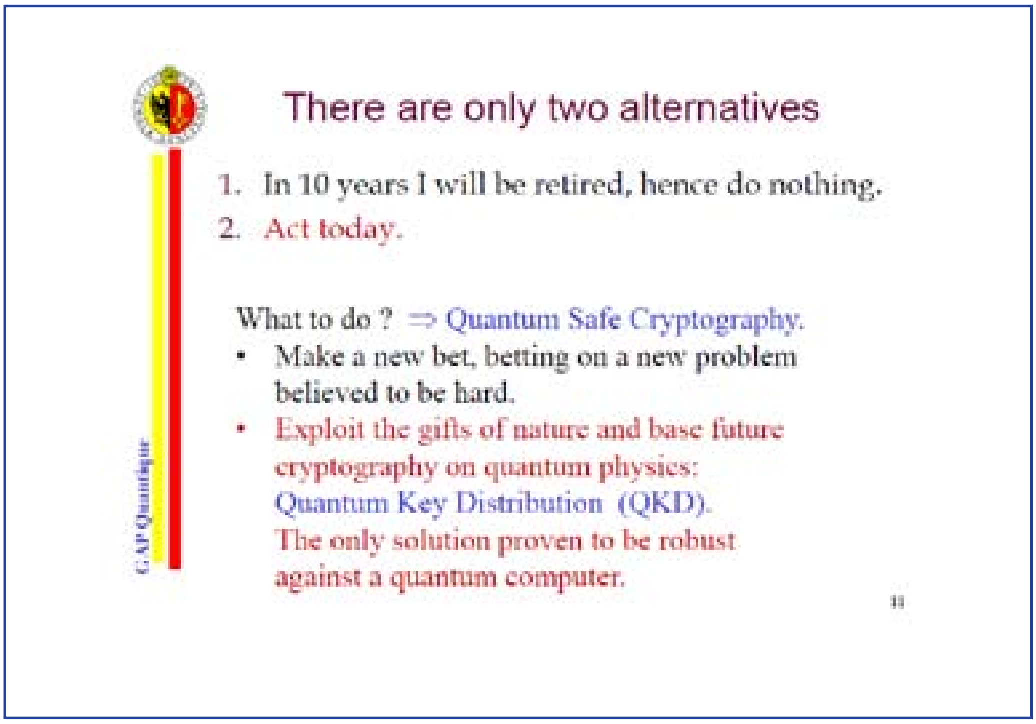
SESSION 1
SETTING THE SCENE

ISBN 979-10-92620-04-7

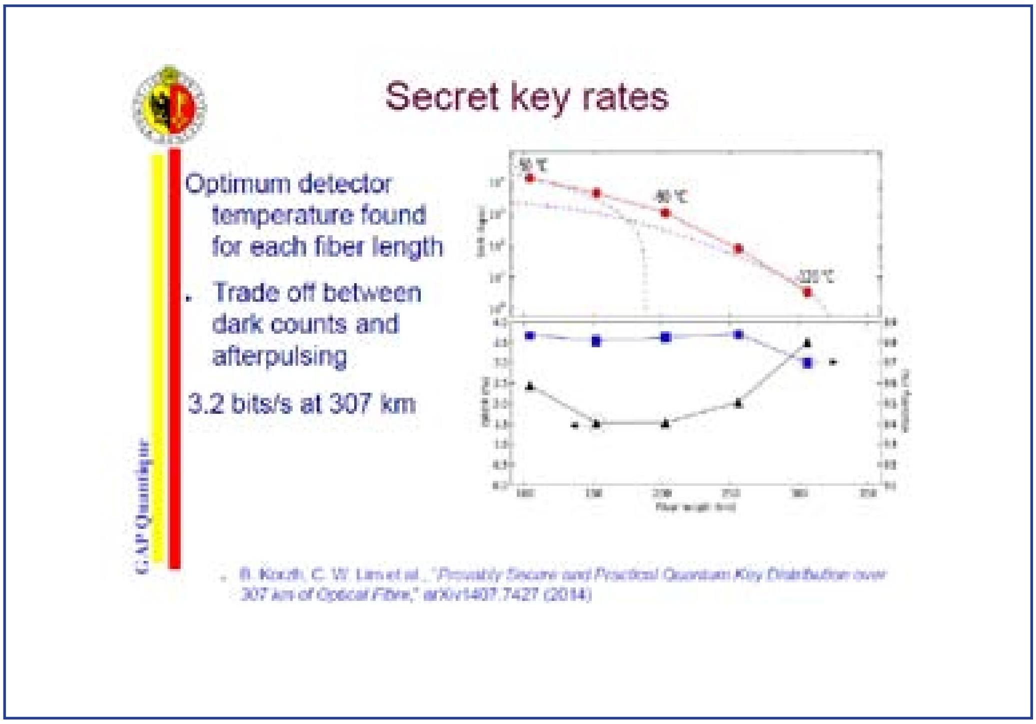


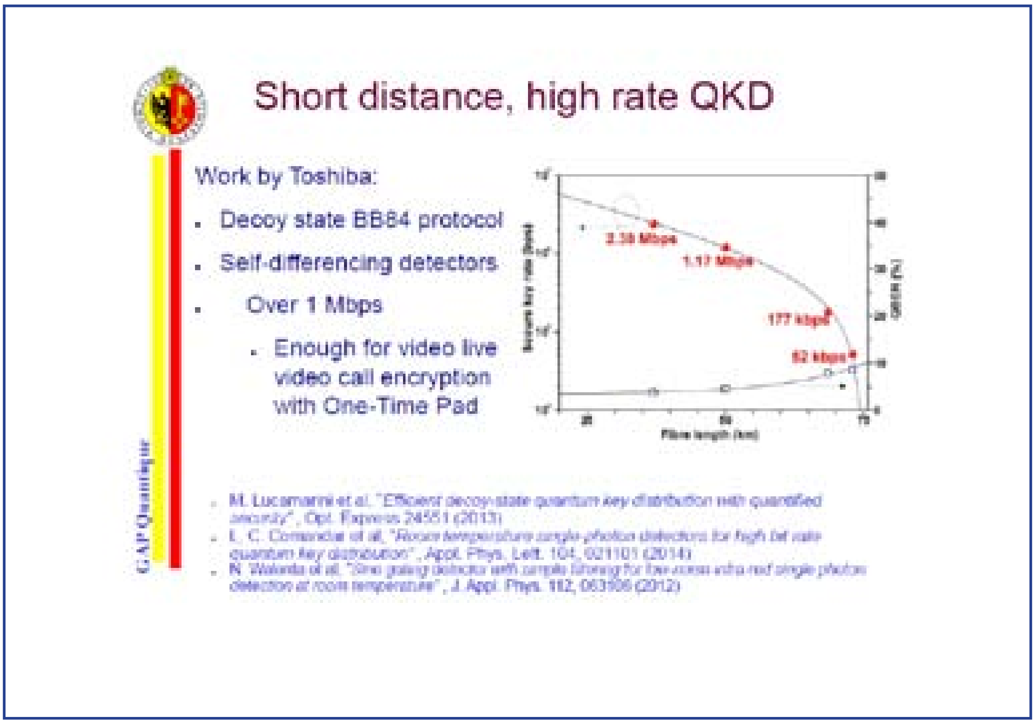
ISBN 979-10-92620-04-7

ISBN 979-10-92620-04-7

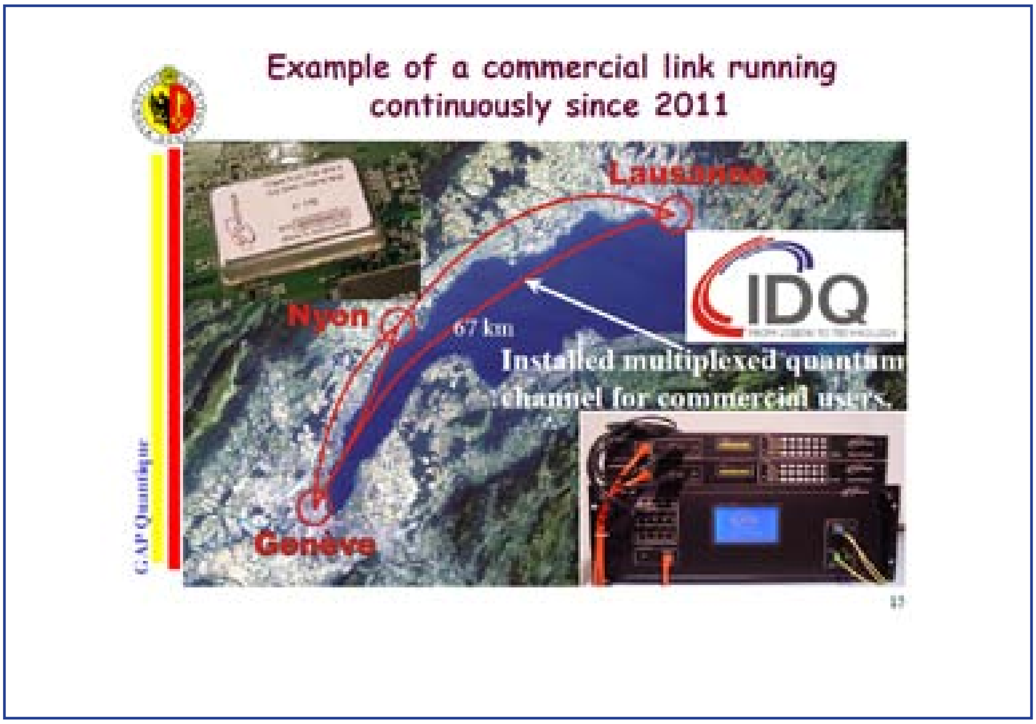


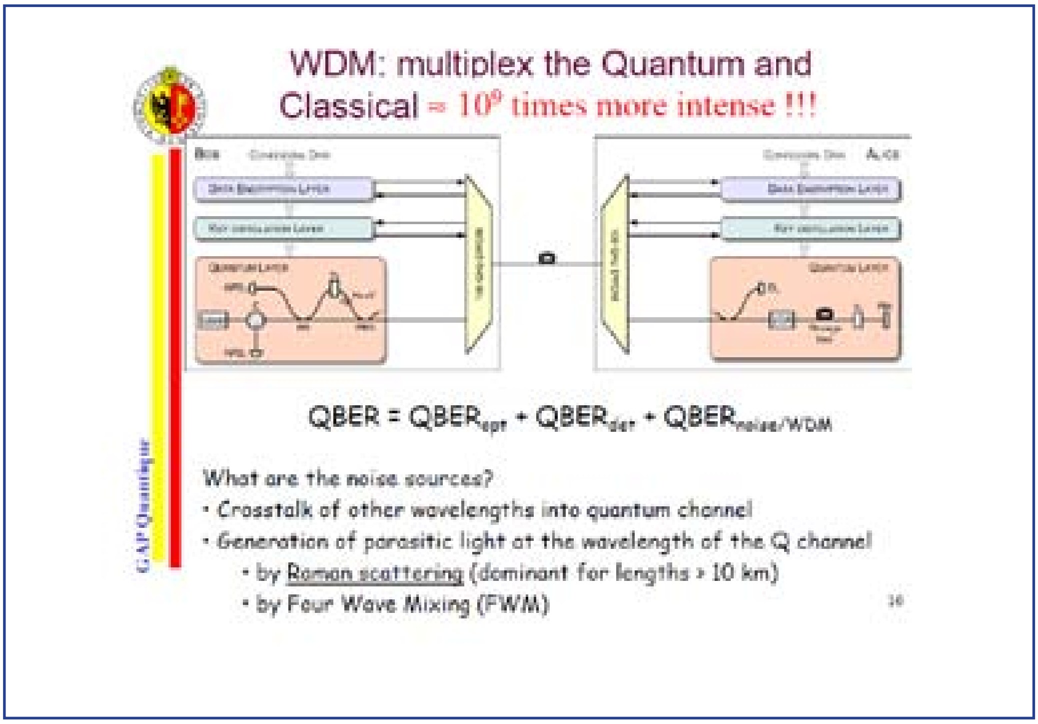
ISBN 979-10-92620-04-7



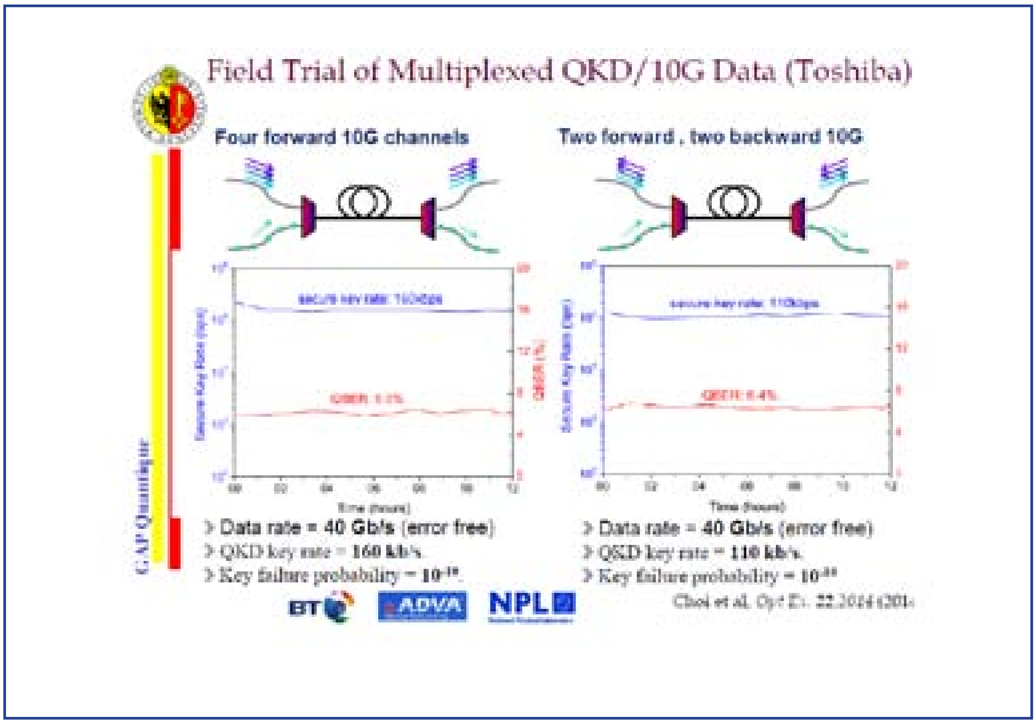


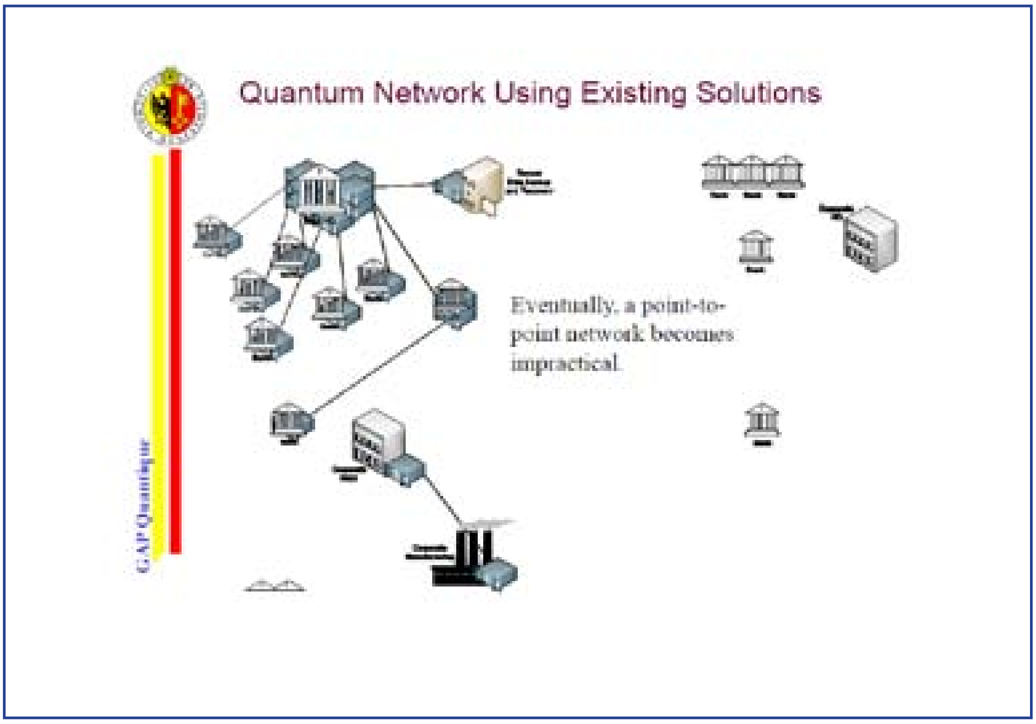
ISBN 979-10-92620-04-7



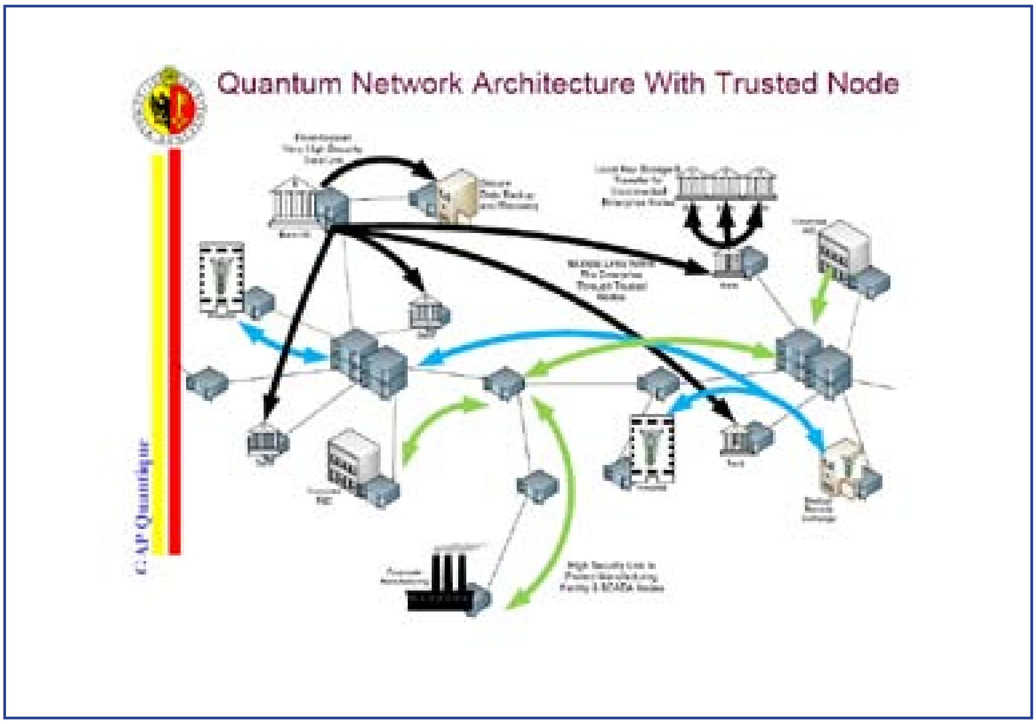


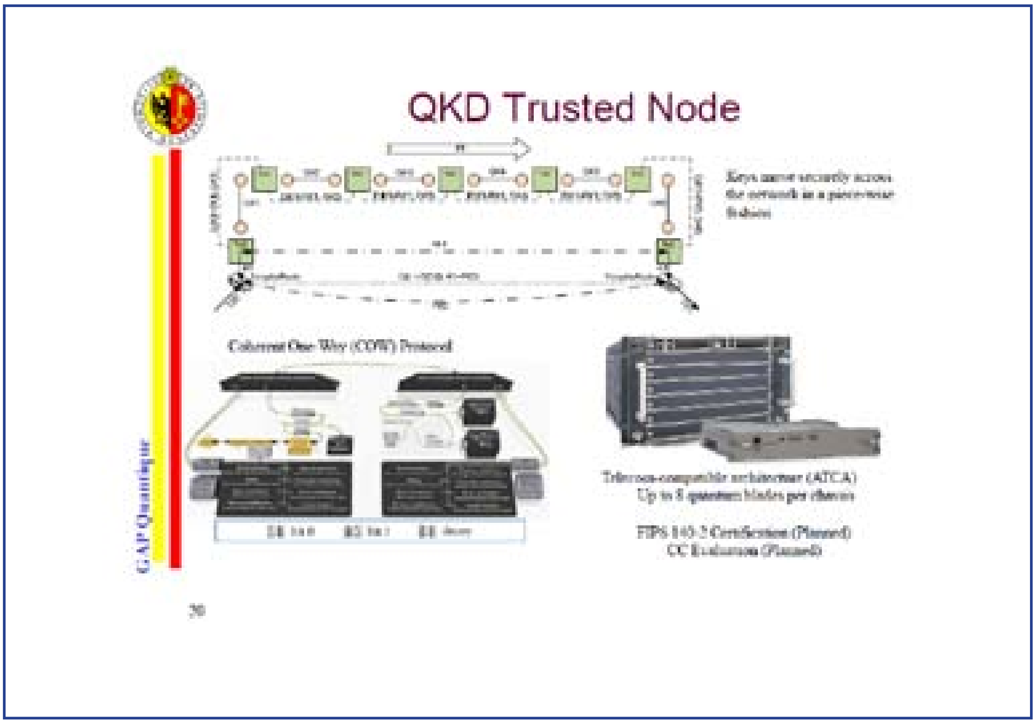
ISBN 979-10-92620-04-7



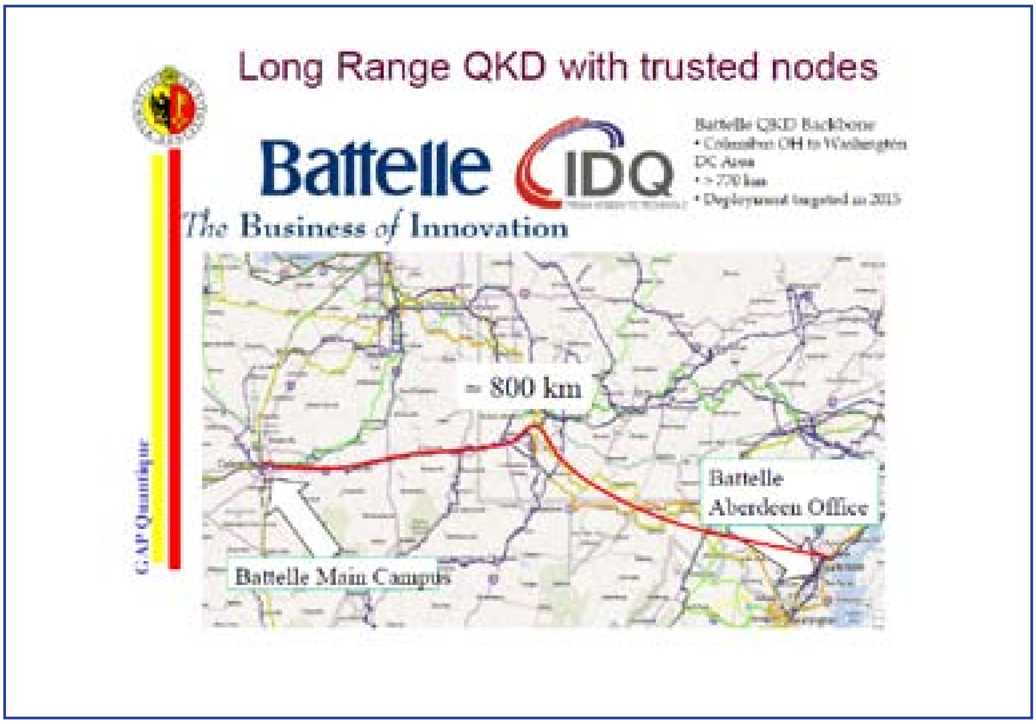


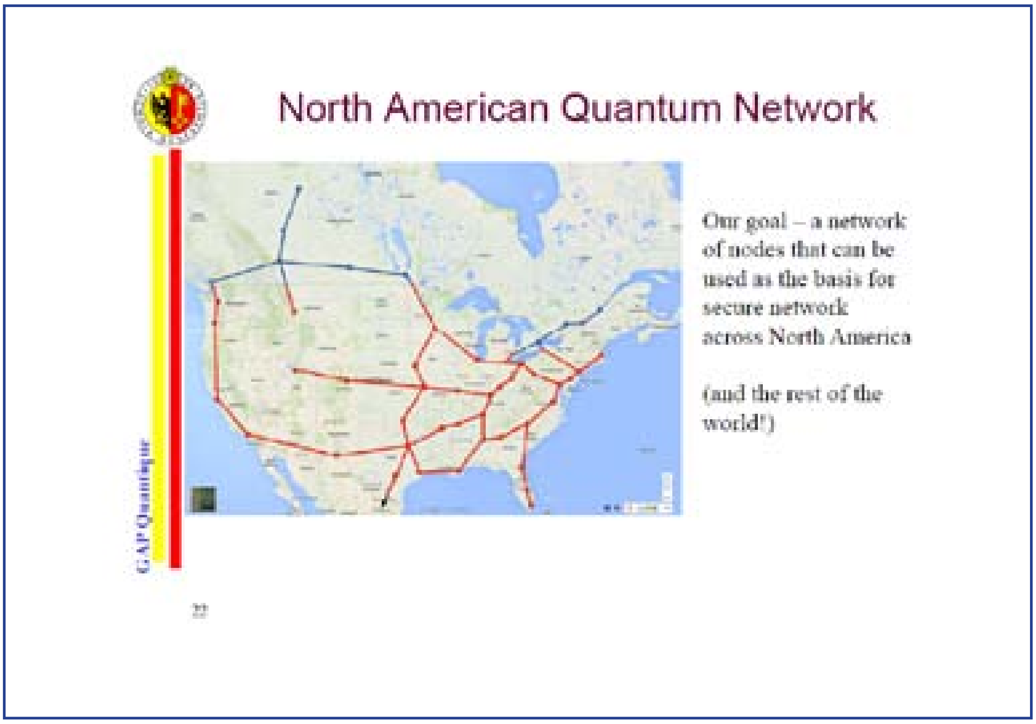
ISBN 979-10-92620-04-7





ISBN 979-10-92620-04-7

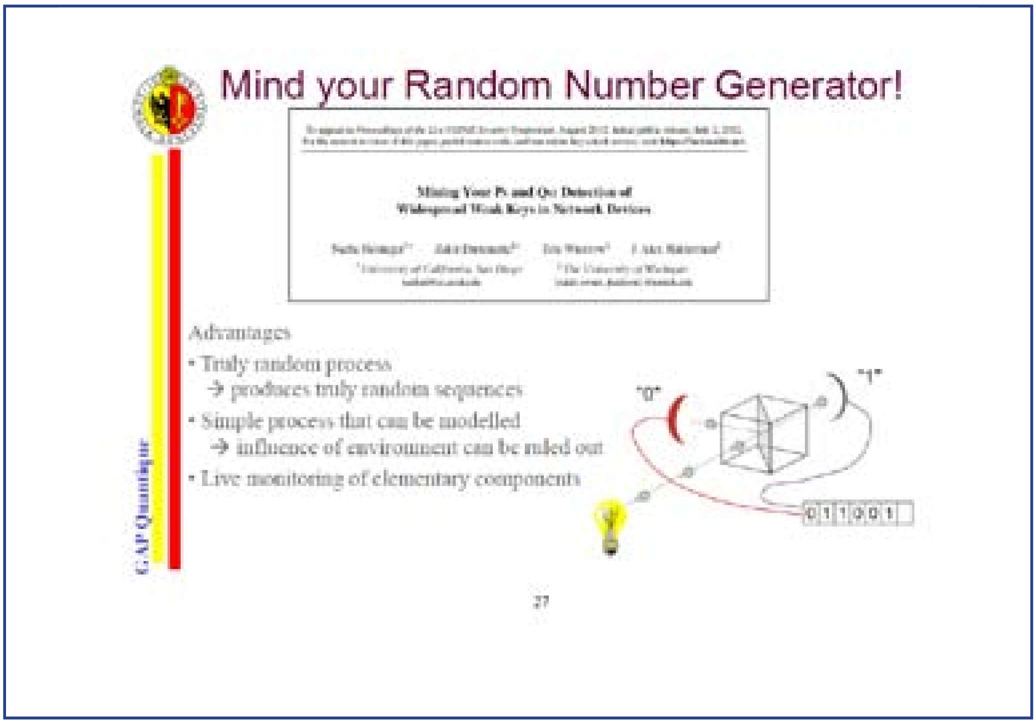


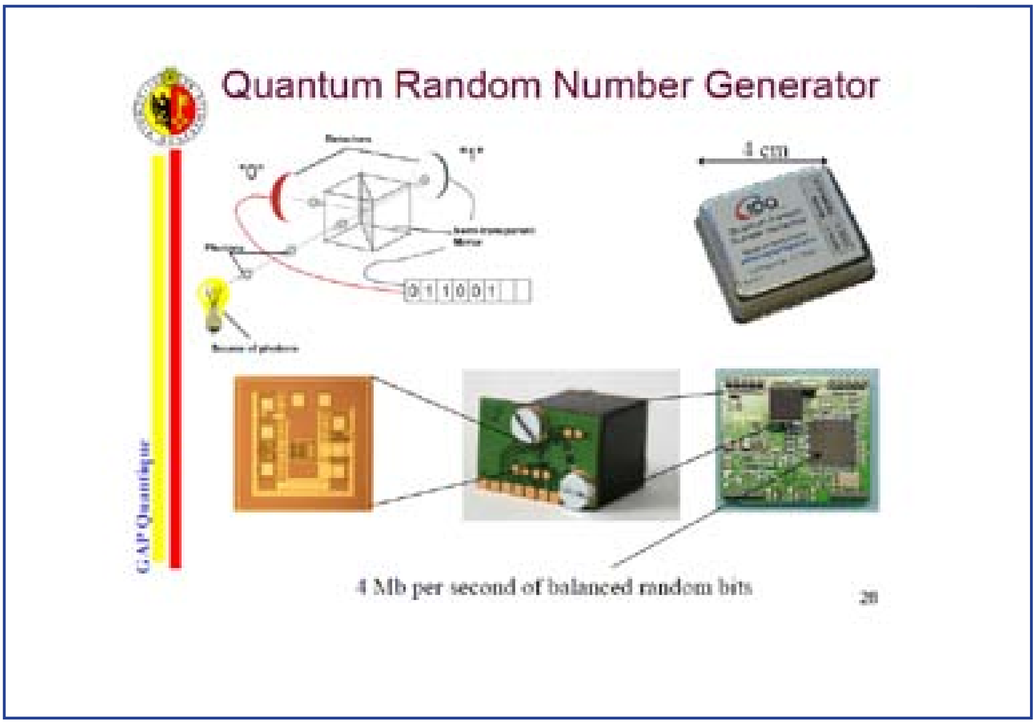


ISBN 979-10-92620-04-7

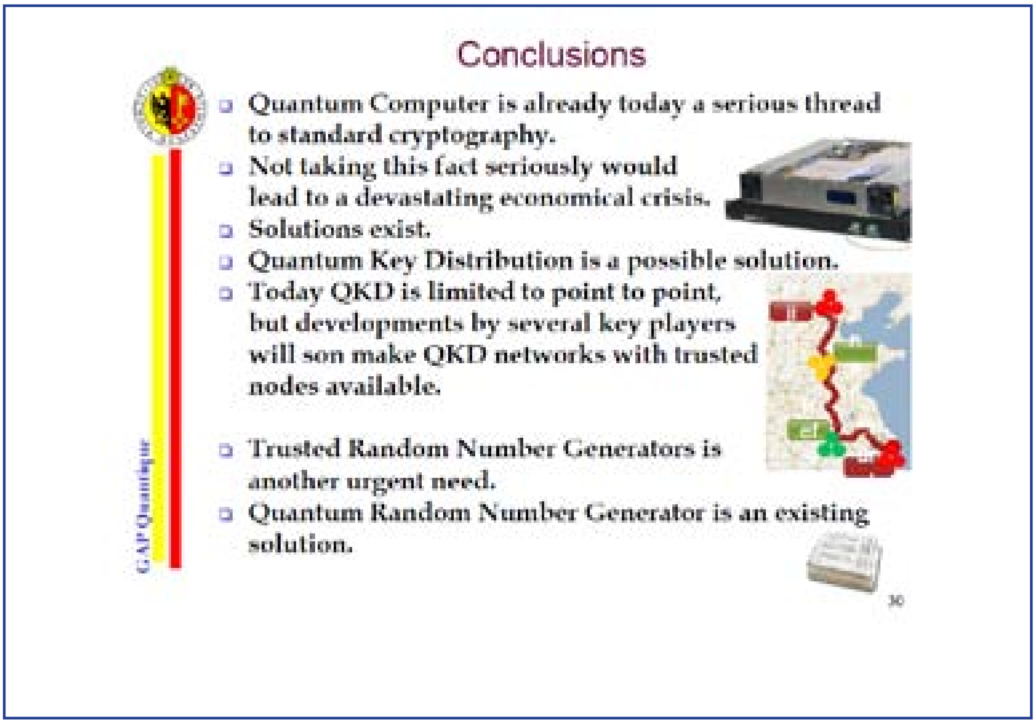
ISBN 979-10-92620-04-7

ISBN 979-10-92620-04-7

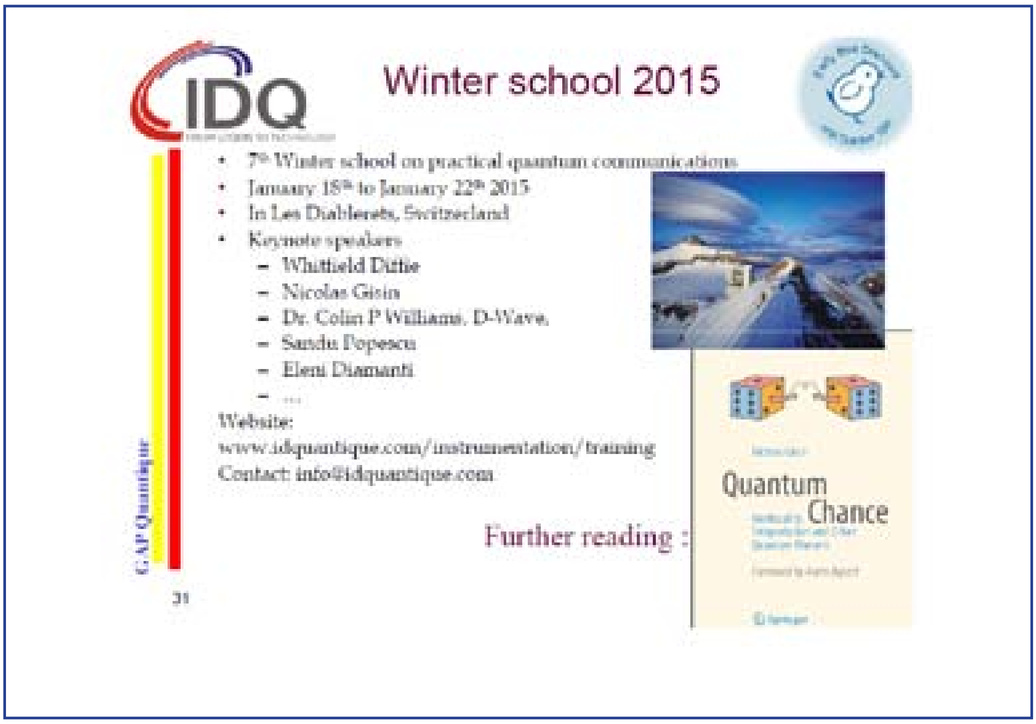


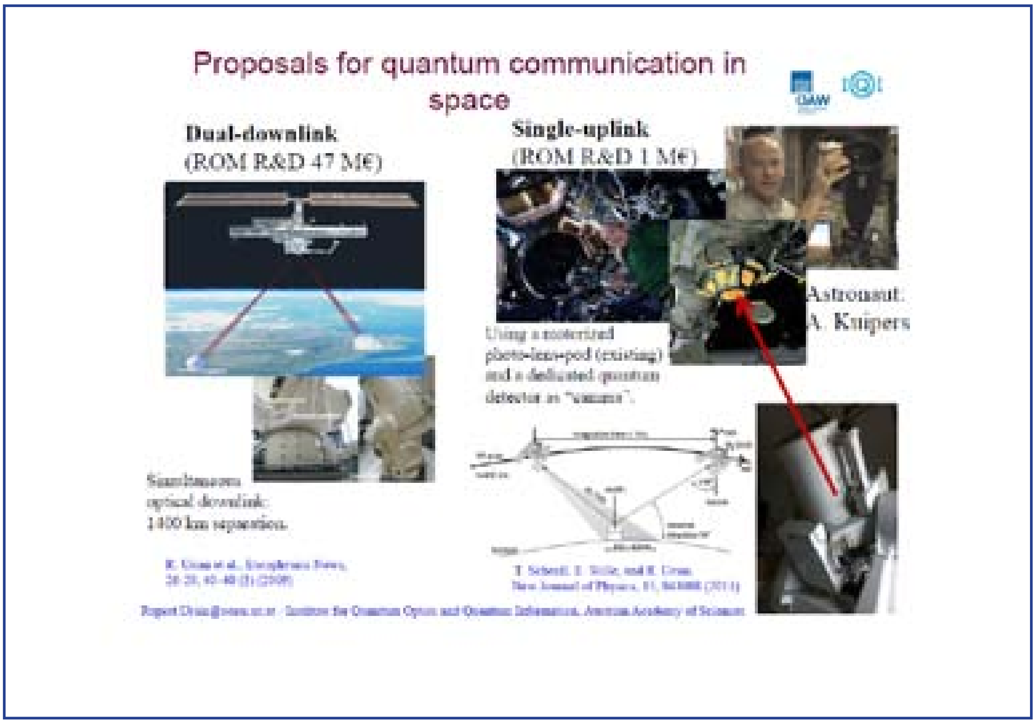


ISBN 979-10-92620-04-7



ISBN 979-10-92620-04-7

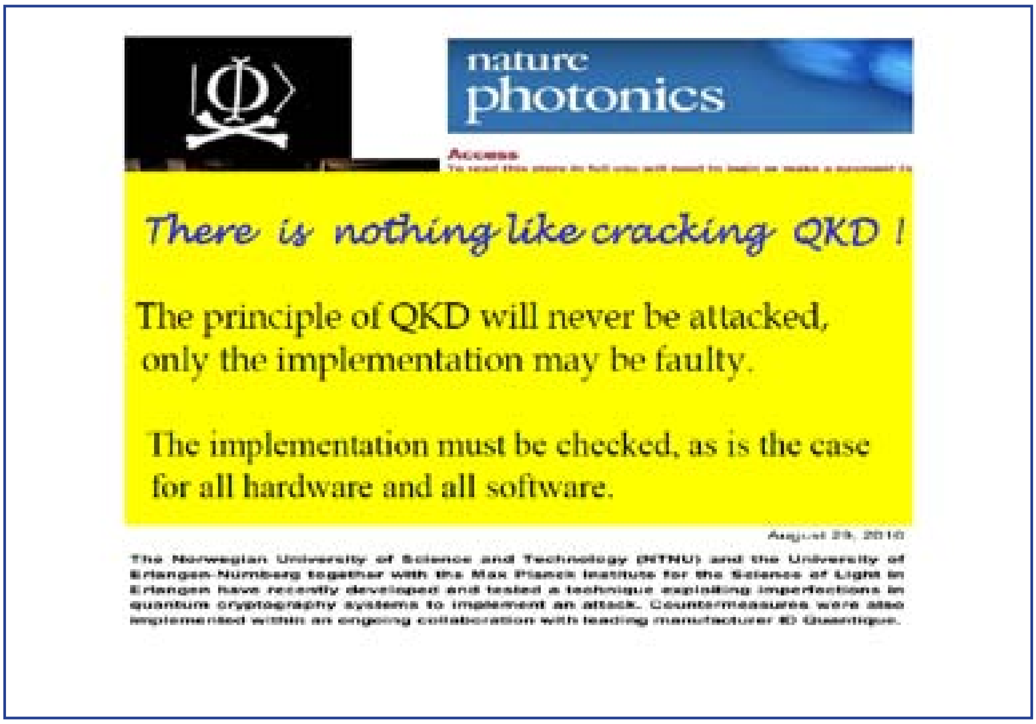




ISBN 979-10-92620-04-7

Presentations

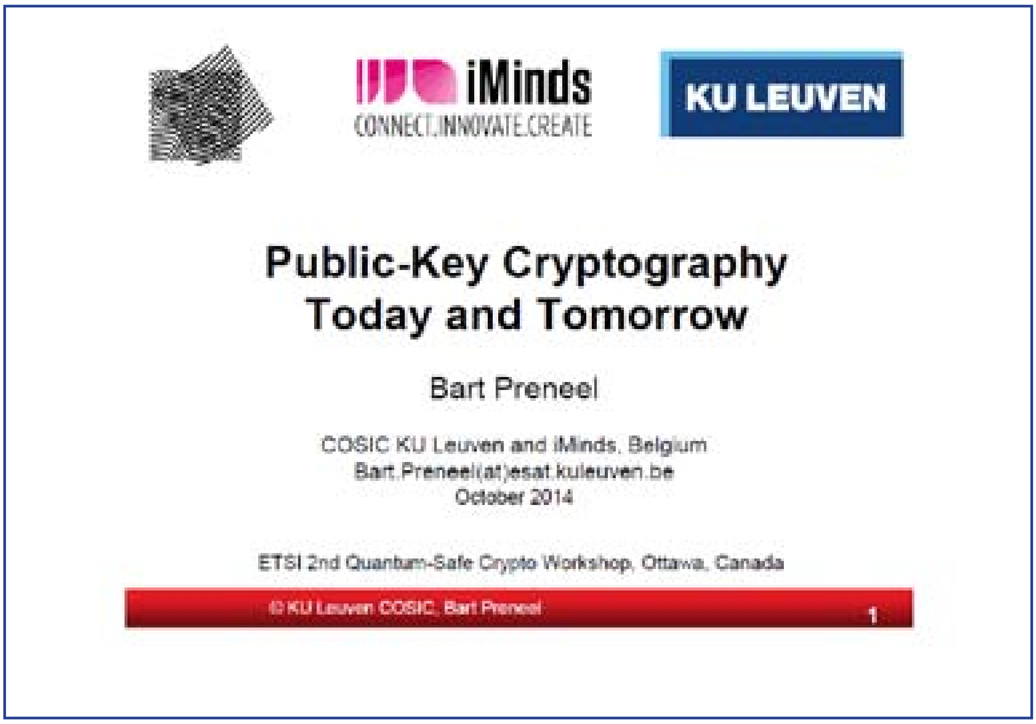
SESSION 1
SETTING THE SCENE

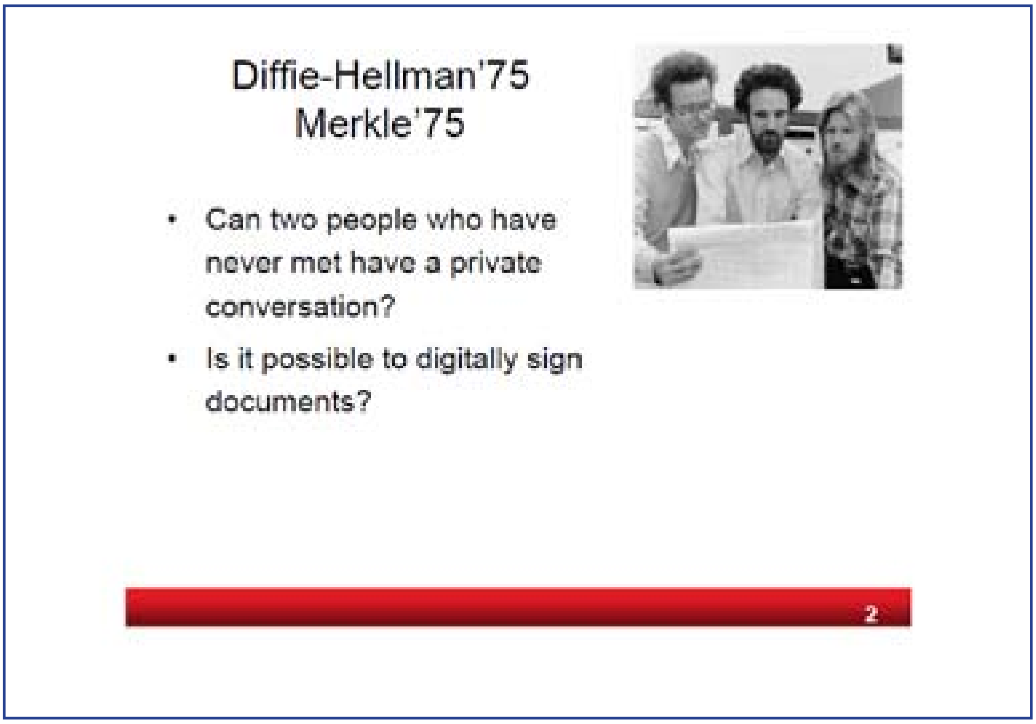


ISBN 979-10-92620-04-7

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

Bart Preneel, KU Leuven





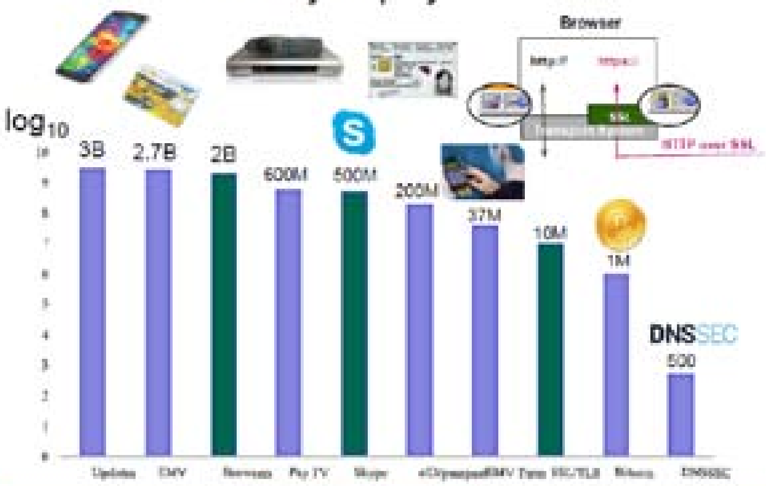
ISBN 979-10-92620-04-7

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

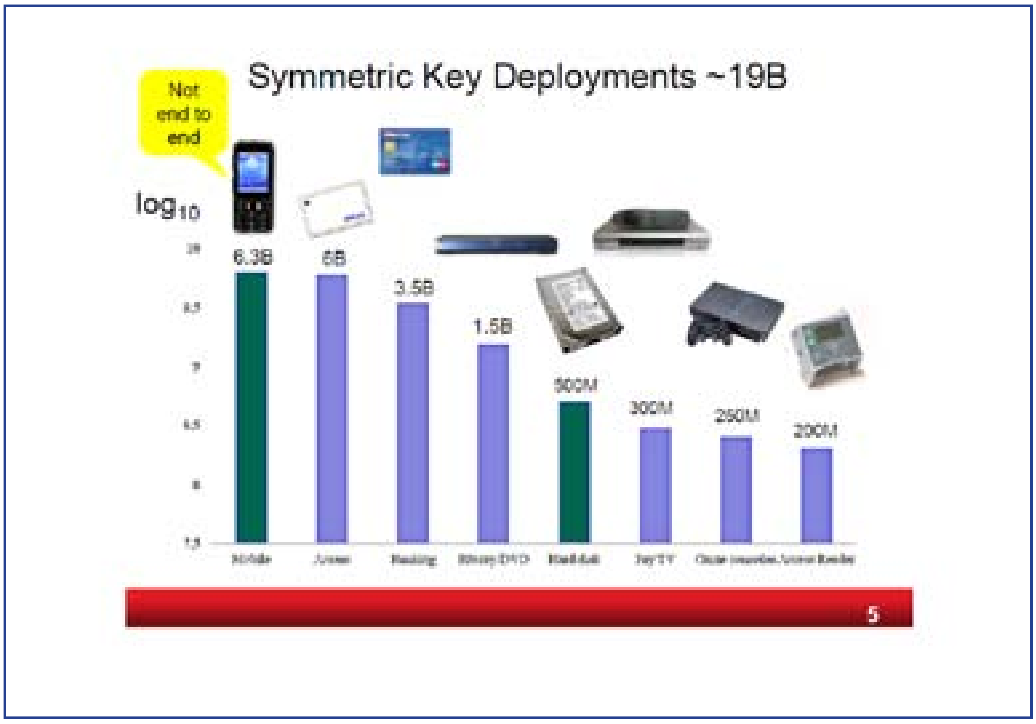
Public Key Deployments ~9B



Missing: IPsec, SSH

4

ISBN 979-10-92620-04-7

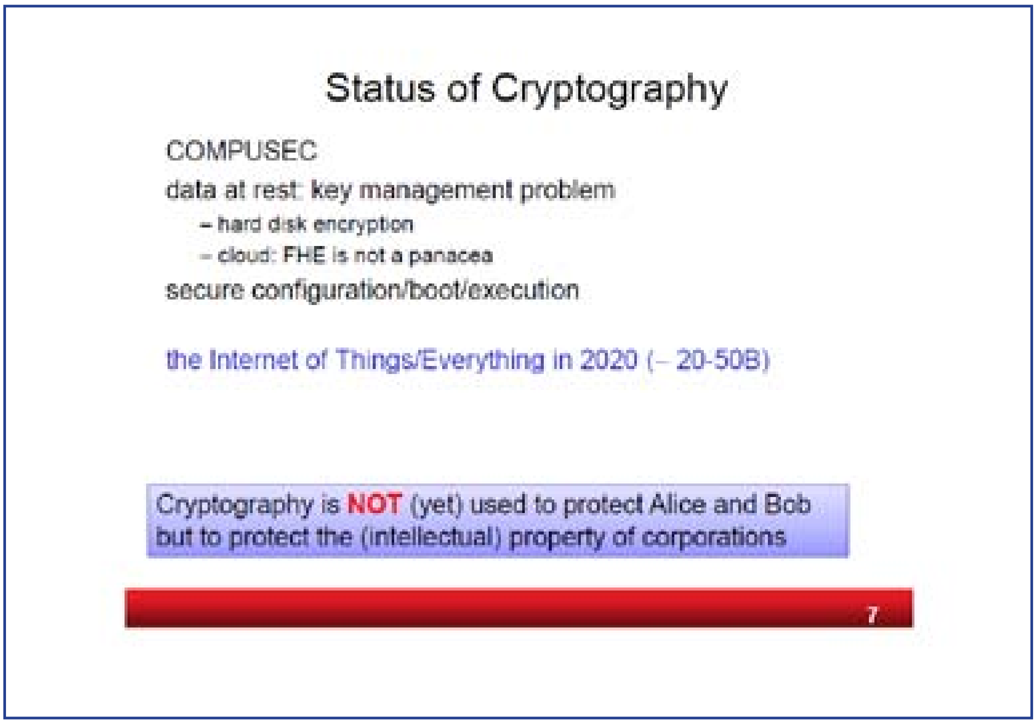


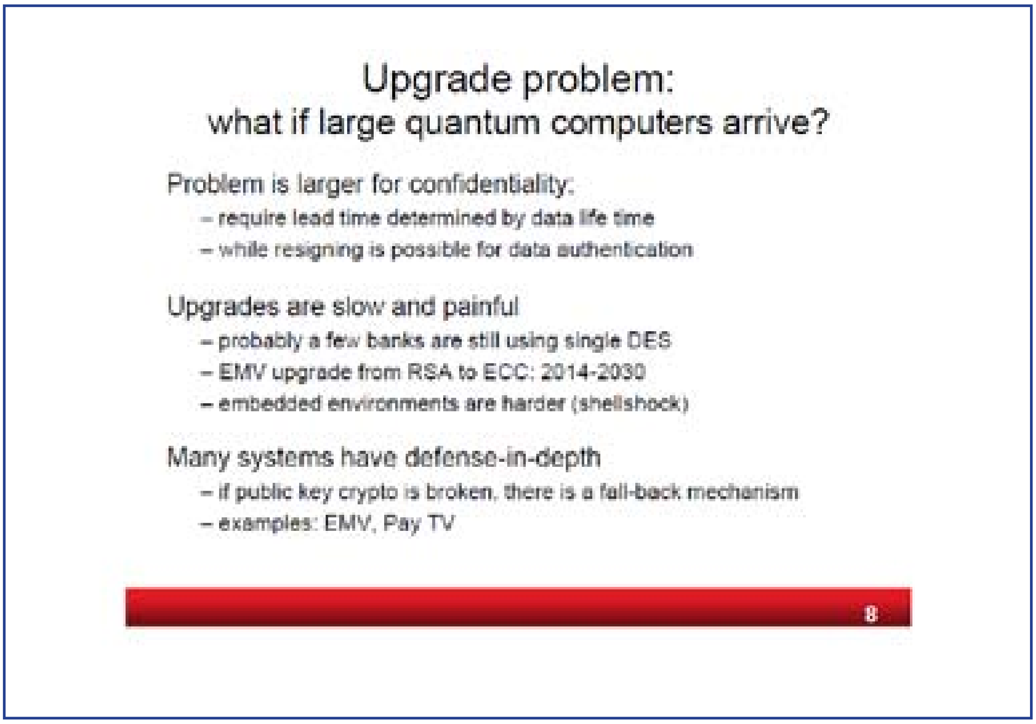
Status of Cryptography

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





ISBN 979-10-92620-04-7

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

Integer factorization: RSA (n = p.q)
Discrete **LOG**arithm : Diffie-Hellman, DSA: $y = \alpha^x$
Elliptic Curve **D**iscrete **LOG**arithm, ECDSA: Q = x.P

RSA-1024 – DLOG-1024 – ECC-146
RSA-2048 – DLOG-2048 – ECC-206
RSA-4096 – DLOG-4096 – ECC-282

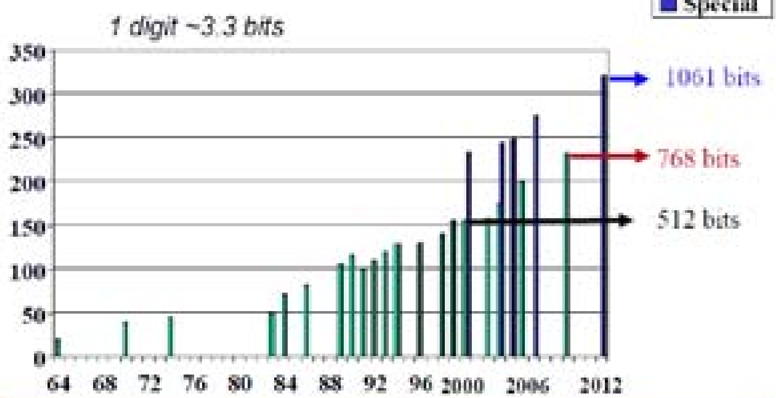
Are these problems hard?

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

9

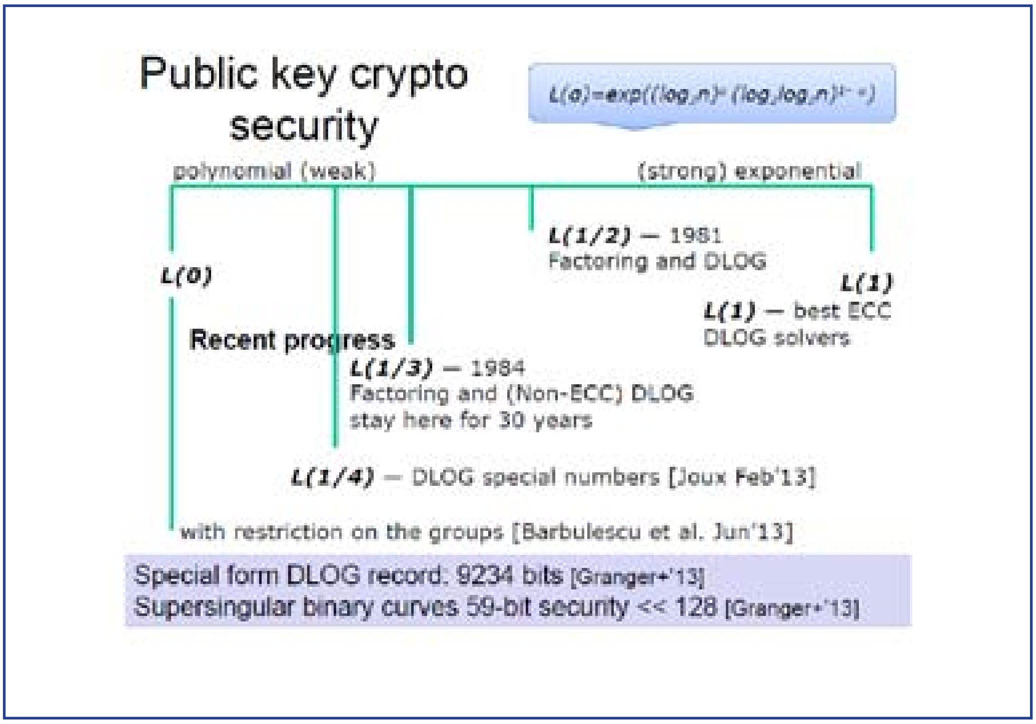
Factorisation records (RSA)

2009: 768 bits or 232 digits
2012: 1061 bits or 320 digits ($2^{1061}-1$)



10

ISBN 979-10-92620-04-7

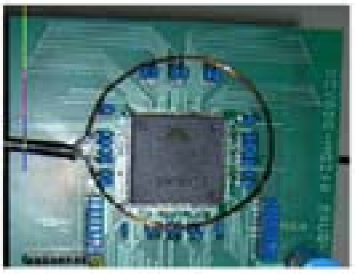


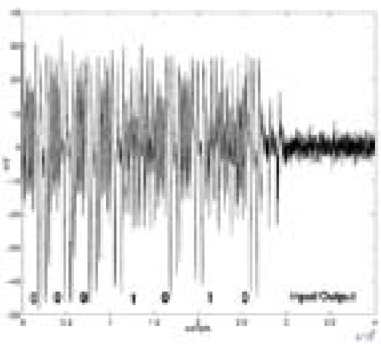
ISBN 979-10-92620-04-7

Security in Practice

13

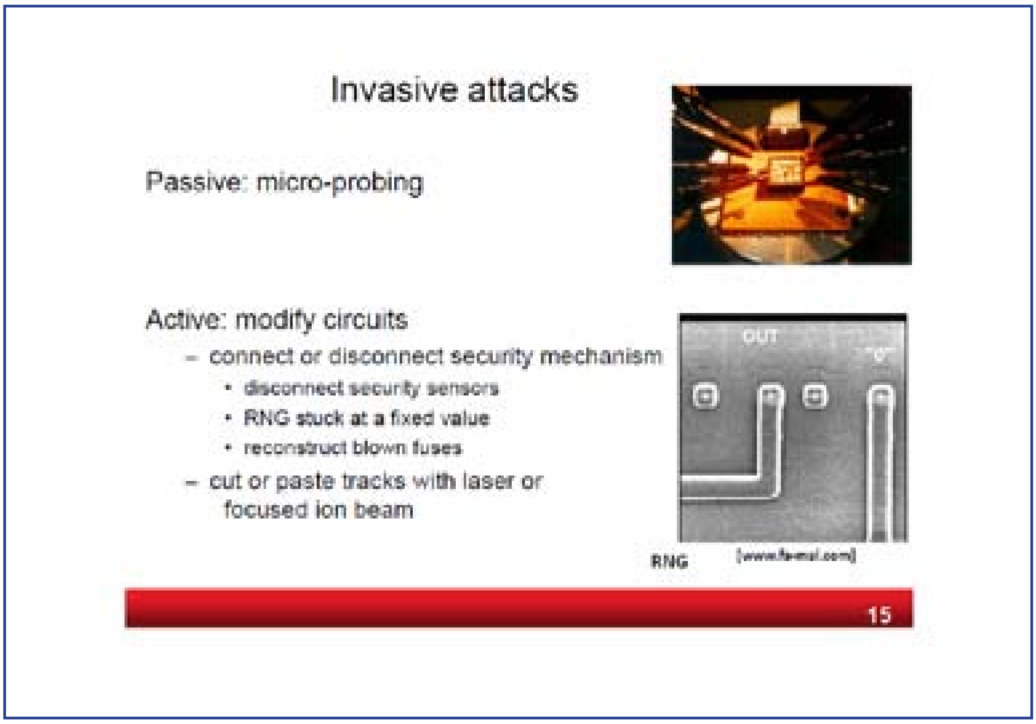
Physics trumps Mathematics



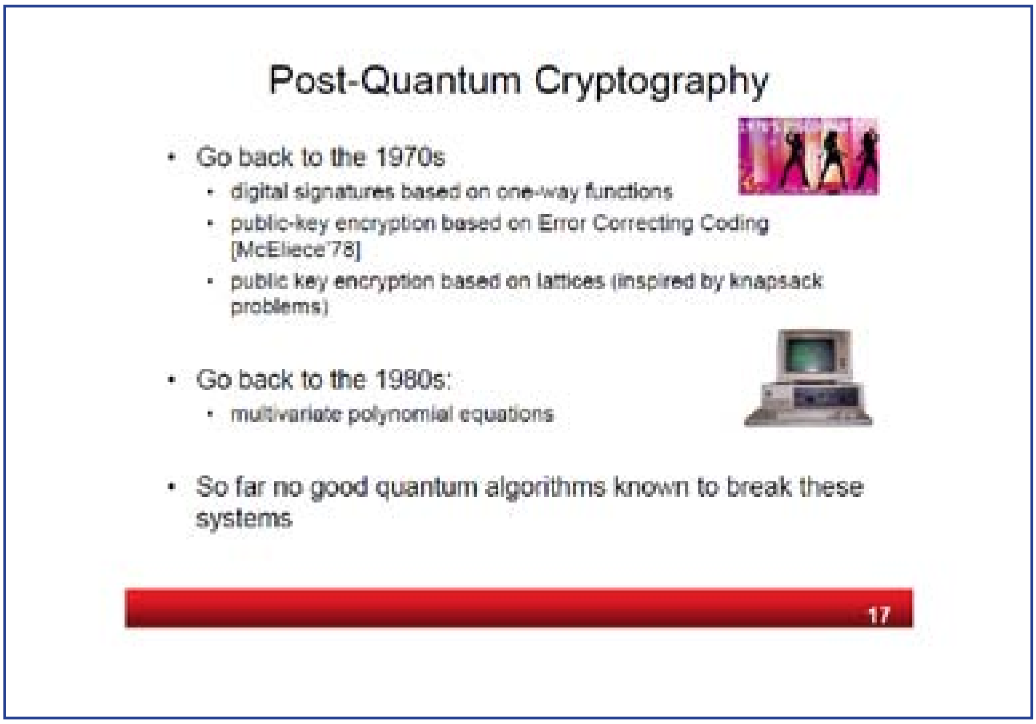


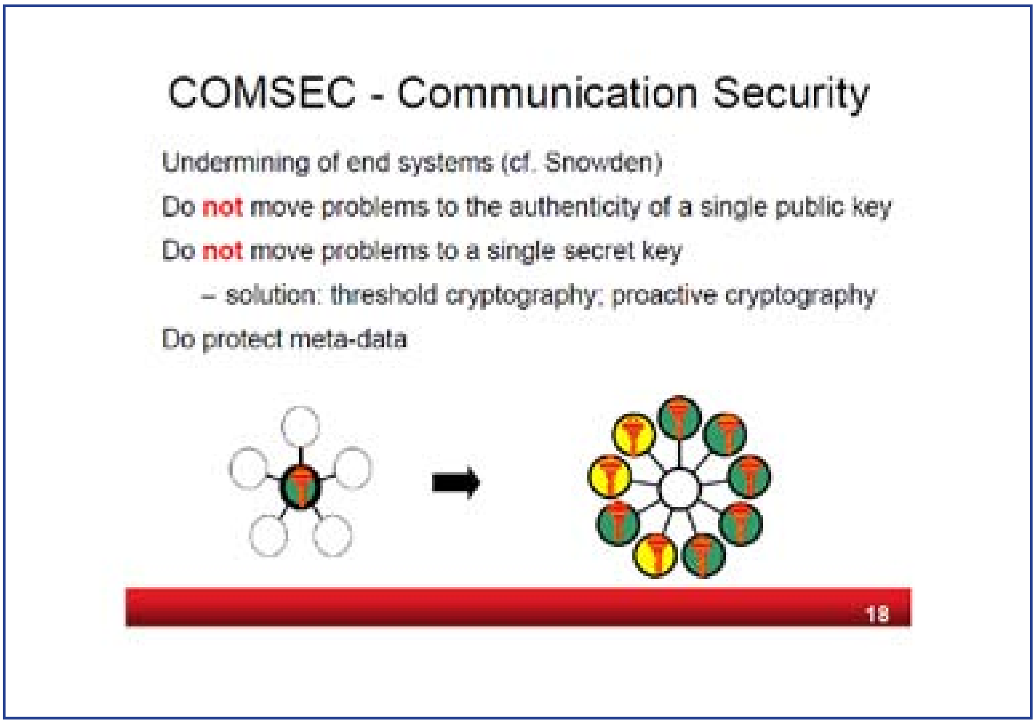
14

ISBN 979-10-92620-04-7

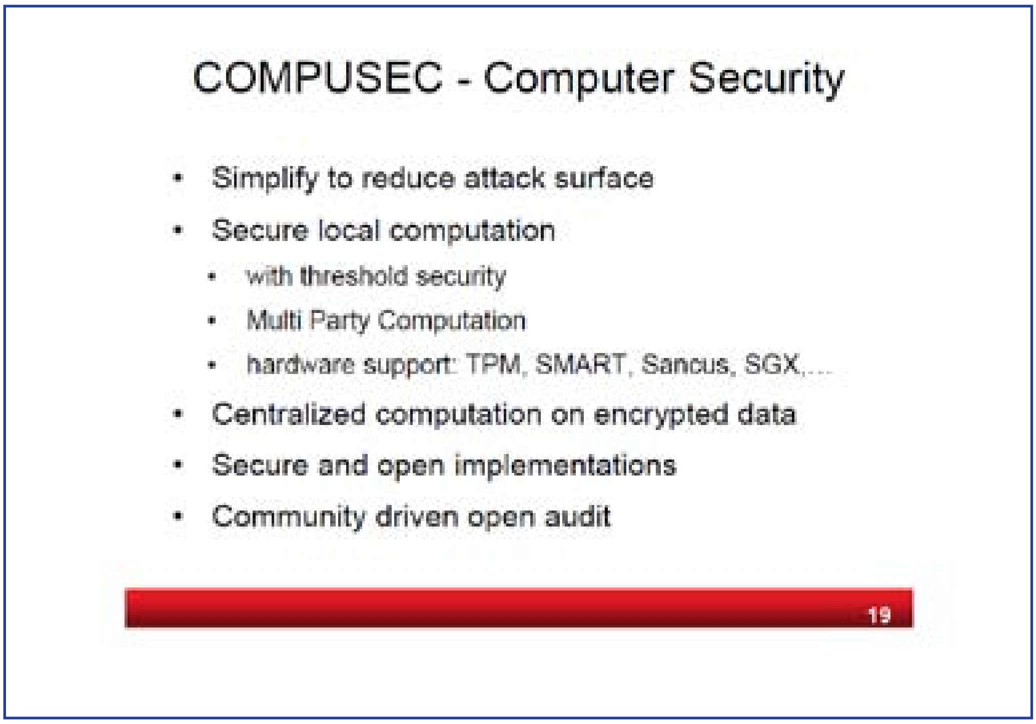


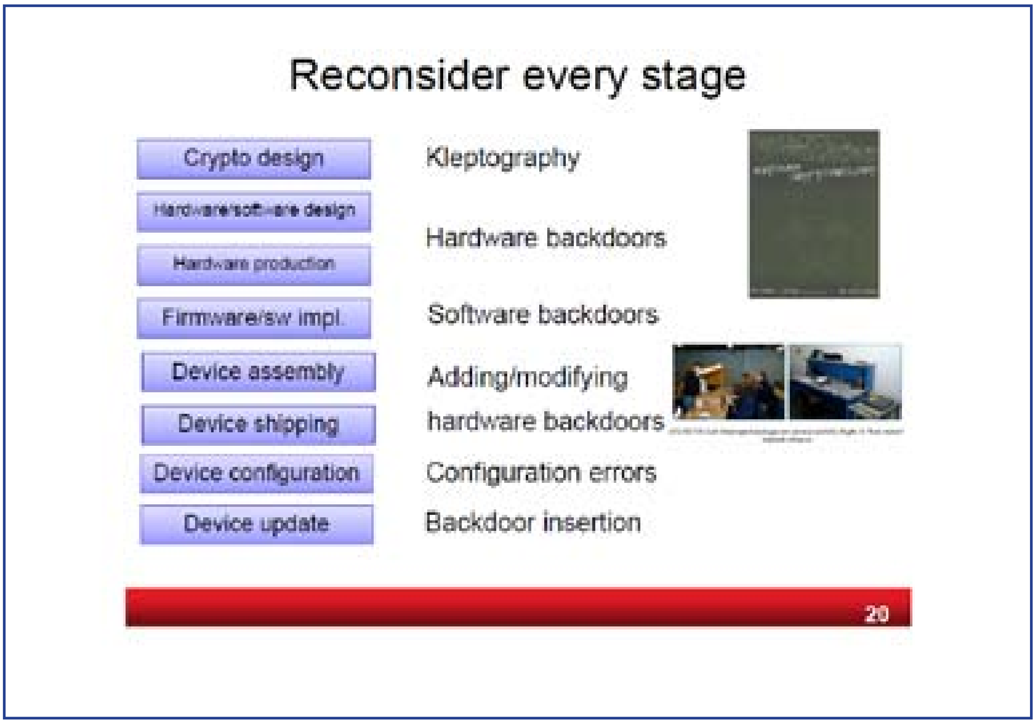
ISBN 979-10-92620-04-7





ISBN 979-10-92620-04-7





ISBN 979-10-92620-04-7

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

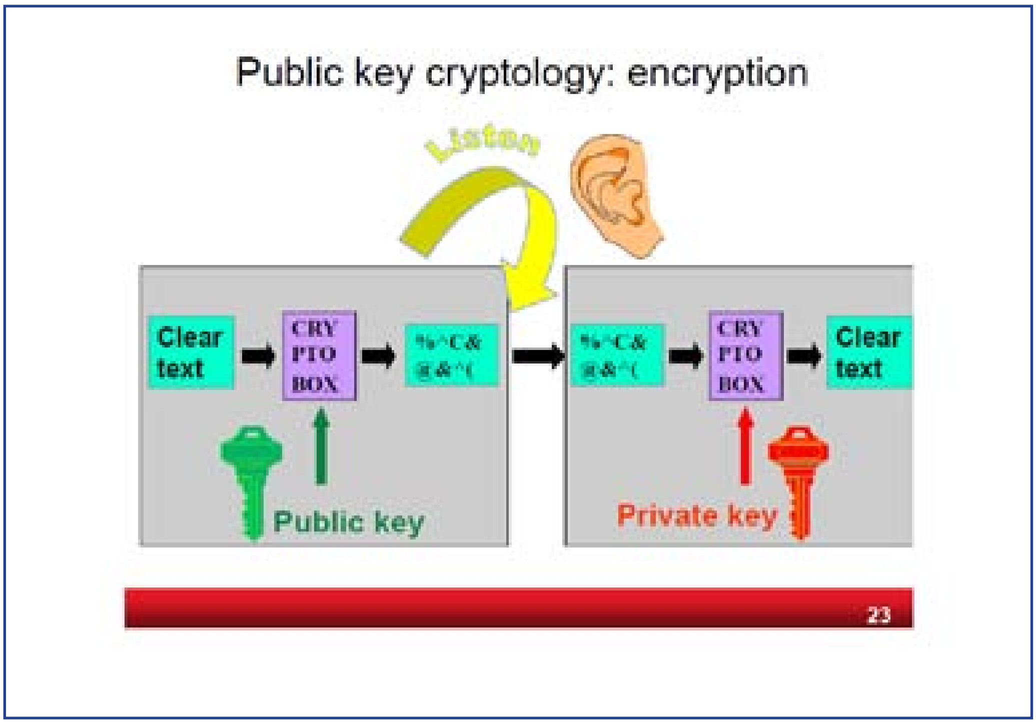
21

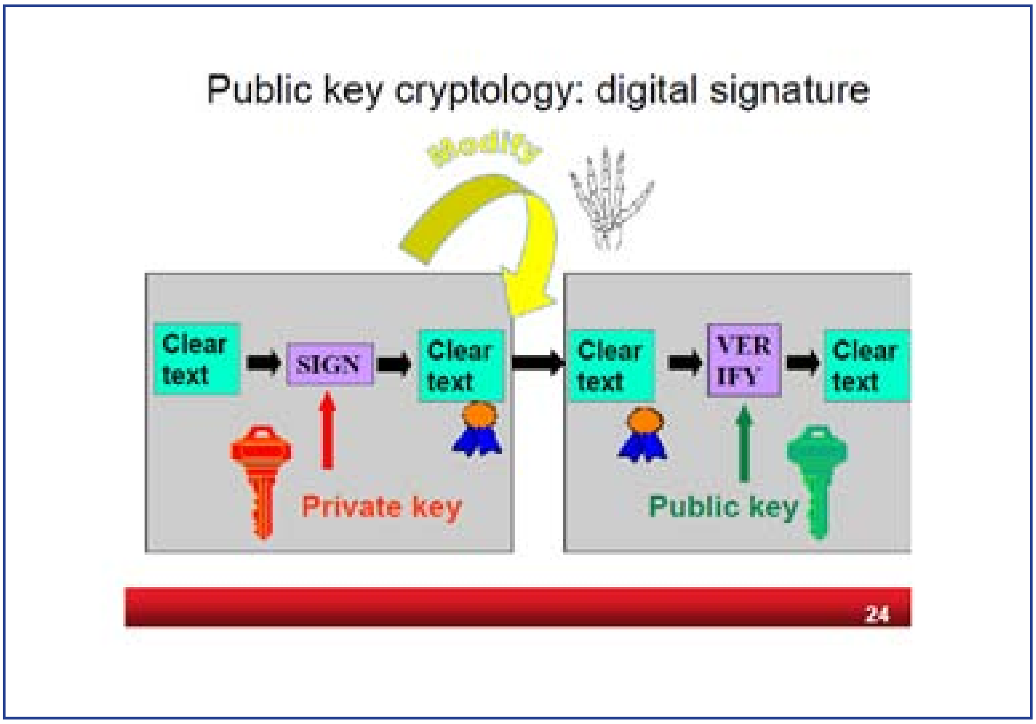
The end

Thank you for your attention

22

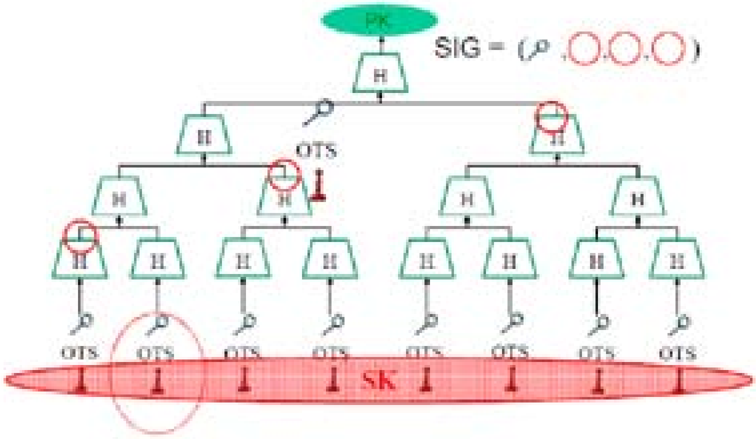
ISBN 979-10-92620-04-7





ISBN 979-10-92620-04-7

Hash-Based Signatures



Slide credit: Andreas Hulsing 25

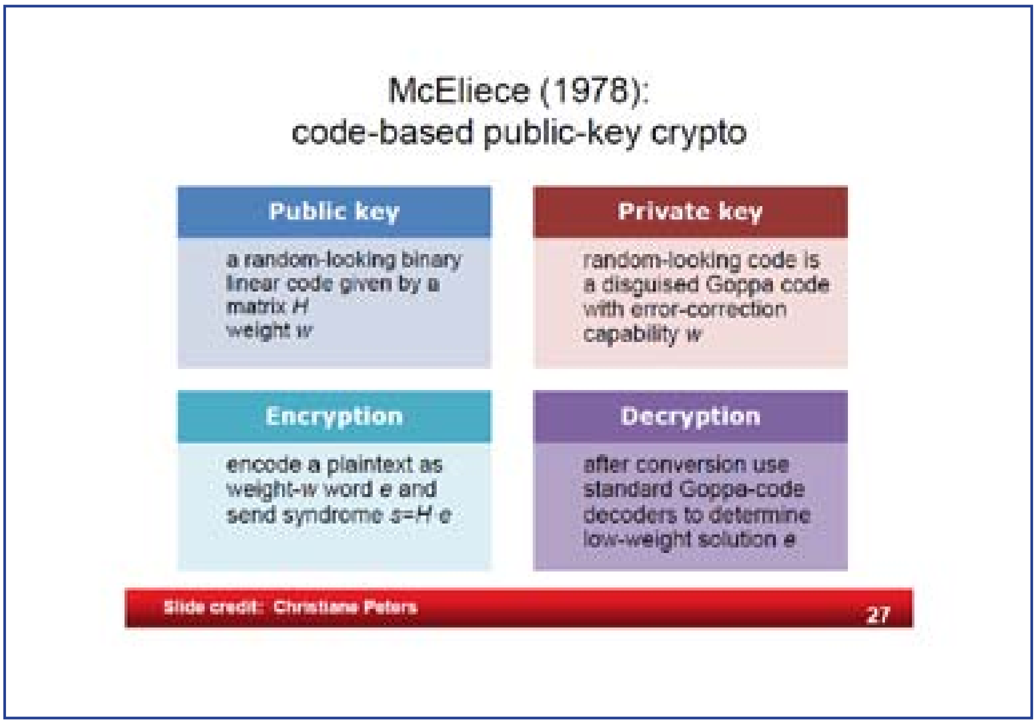
Hash-Based Signatures: variant XMSS

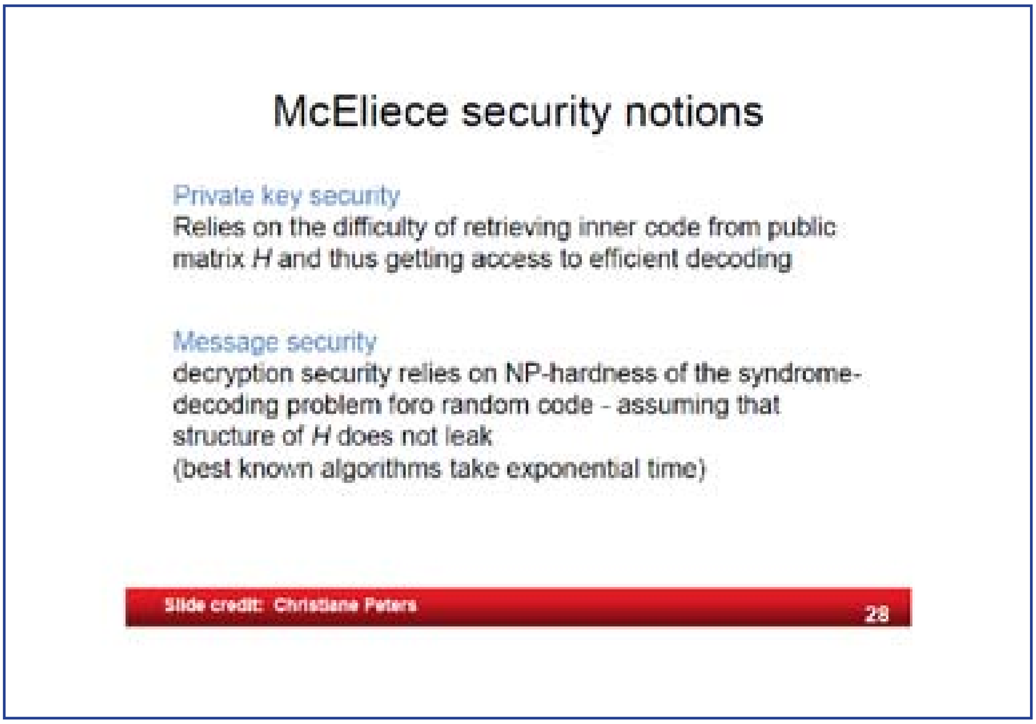
C Implementation using OpenSSL on Intel(R) Core(TM) i5-2520M CPU @ 2.50GHz with Intel AES-NI [BDH'11]

	Sign (ms)	Verify (ms)	Signature (bit)	Public Key (bit)	Secret Key (byte)	Bit Security	Comment
XMSS-SHA-2	35.60	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 Hulsing 26

ISBN 979-10-92620-04-7





ISBN 979-10-92620-04-7

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

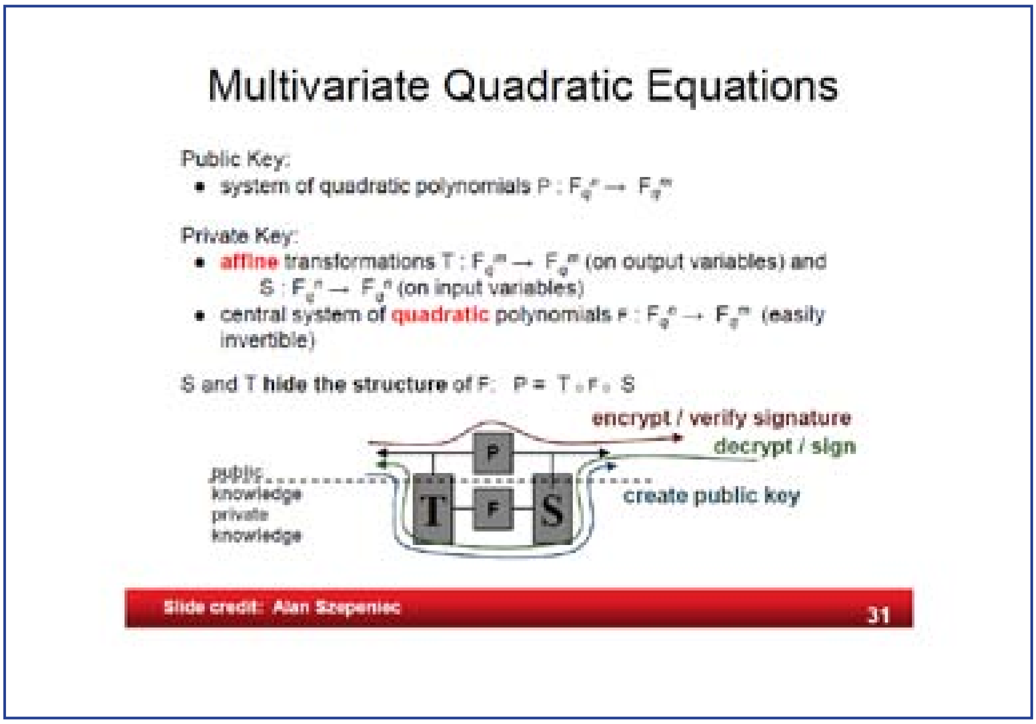
- efficient and parallelizable
  - matrix-vector arithmetic, Fast-Fourier Transform for polynomial multiplication
- worst-case to average-case reductions

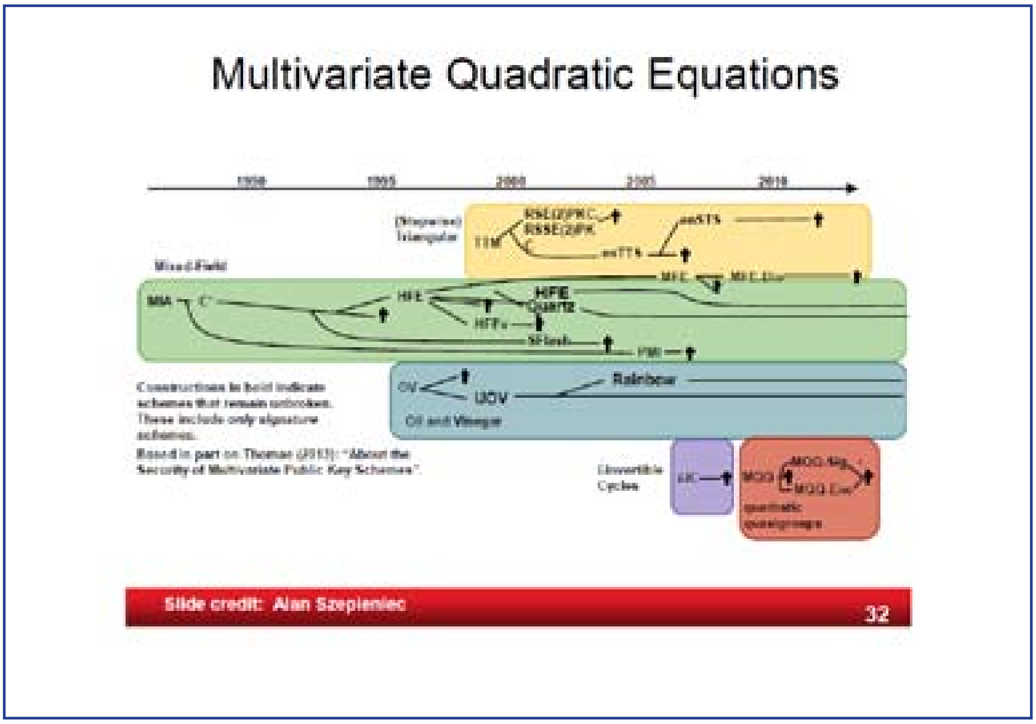
Cons

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

Slide credit: Christiane Peters 30

ISBN 979-10-92620-04-7



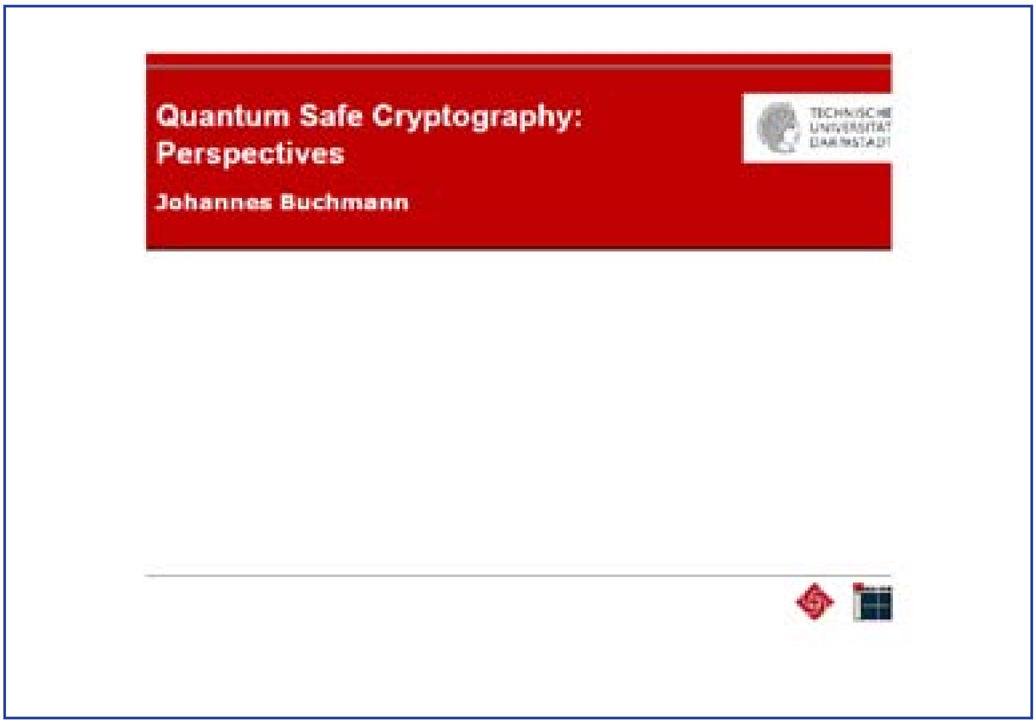


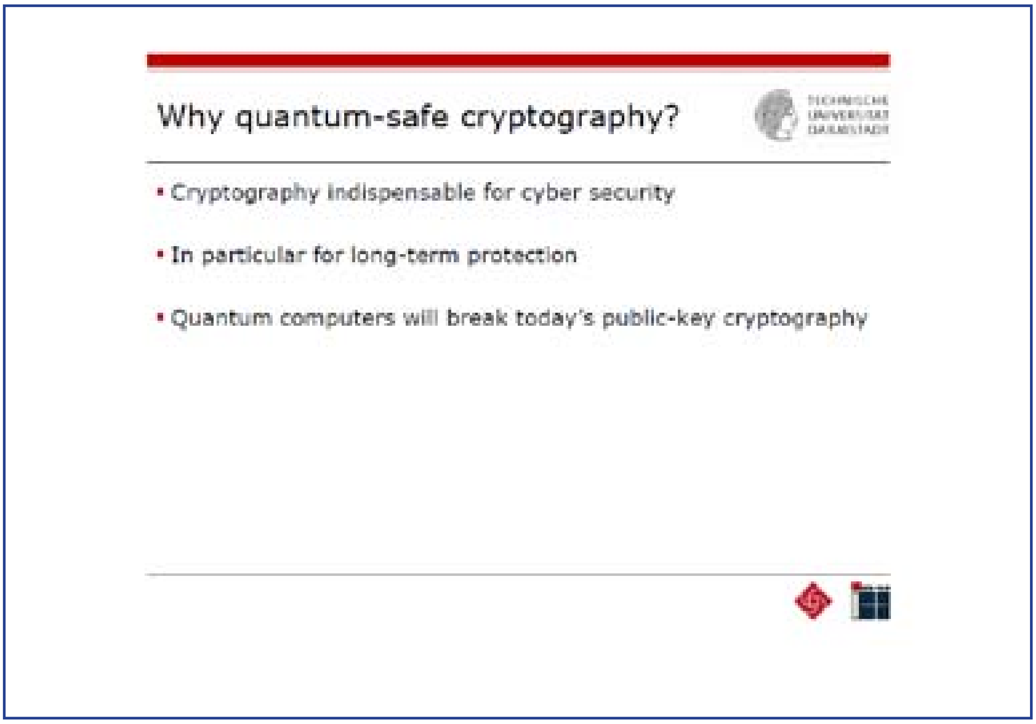
ISBN 979-10-92620-04-7

ISBN 979-10-92620-04-7

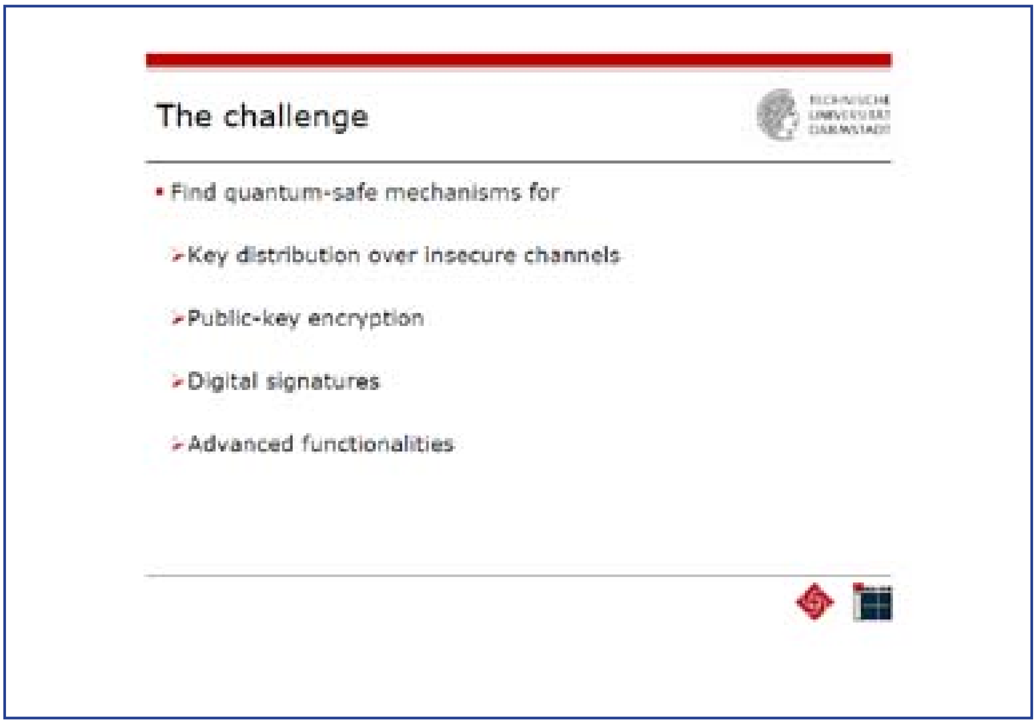
KEYNOTE Speech 4: Quantum Safe Cryptography - Perspectives

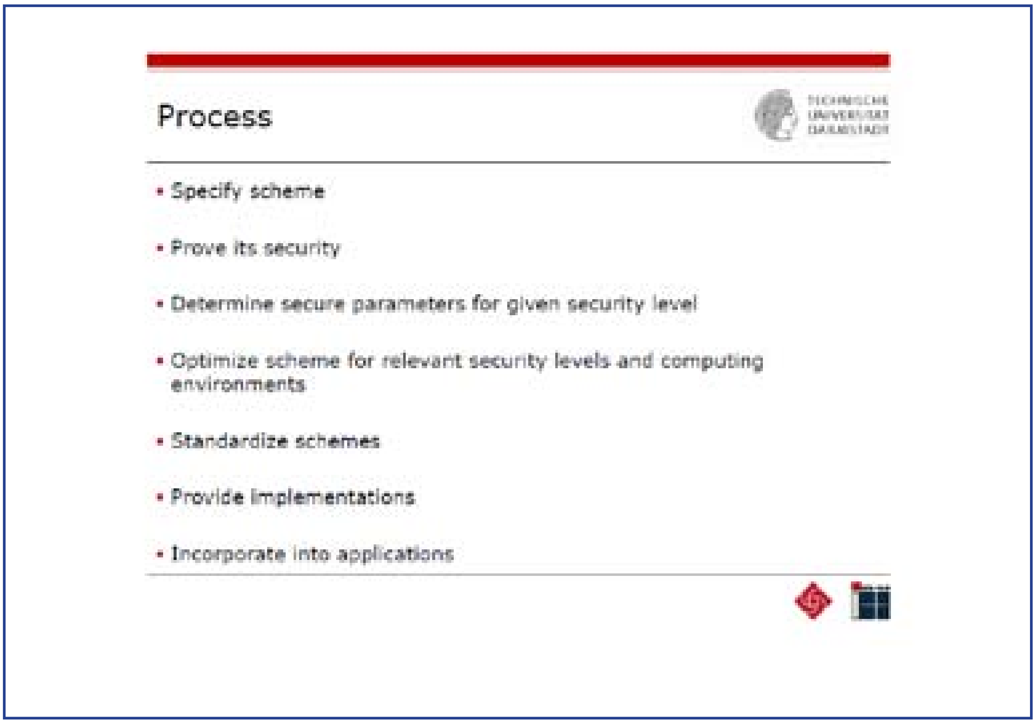
Johannes Buchmann, TU Darmstadt



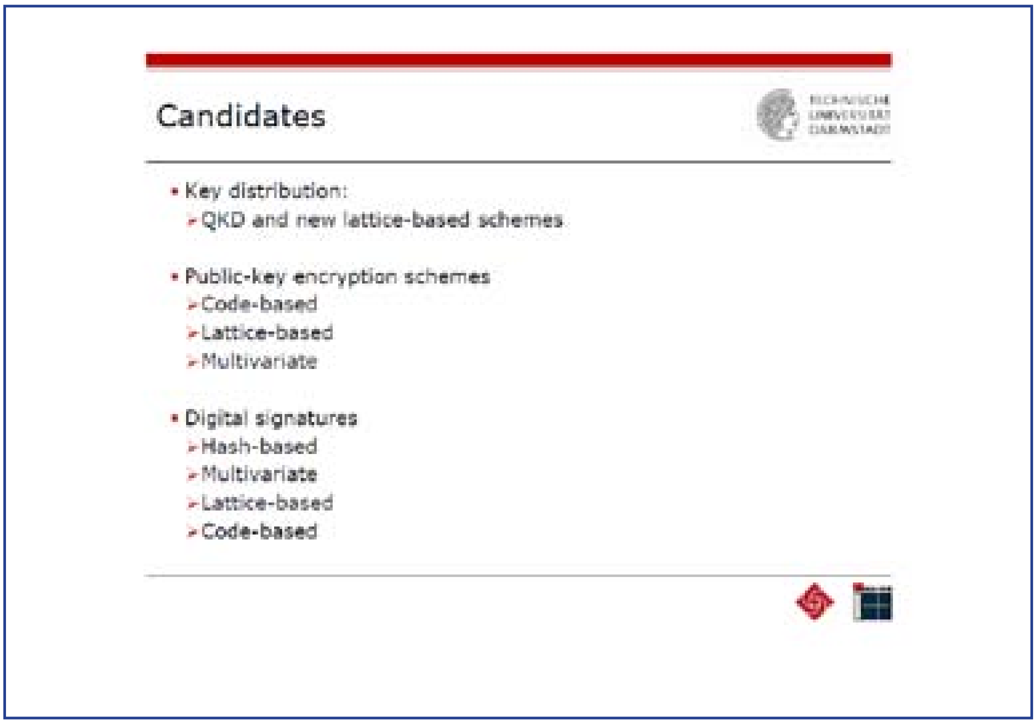


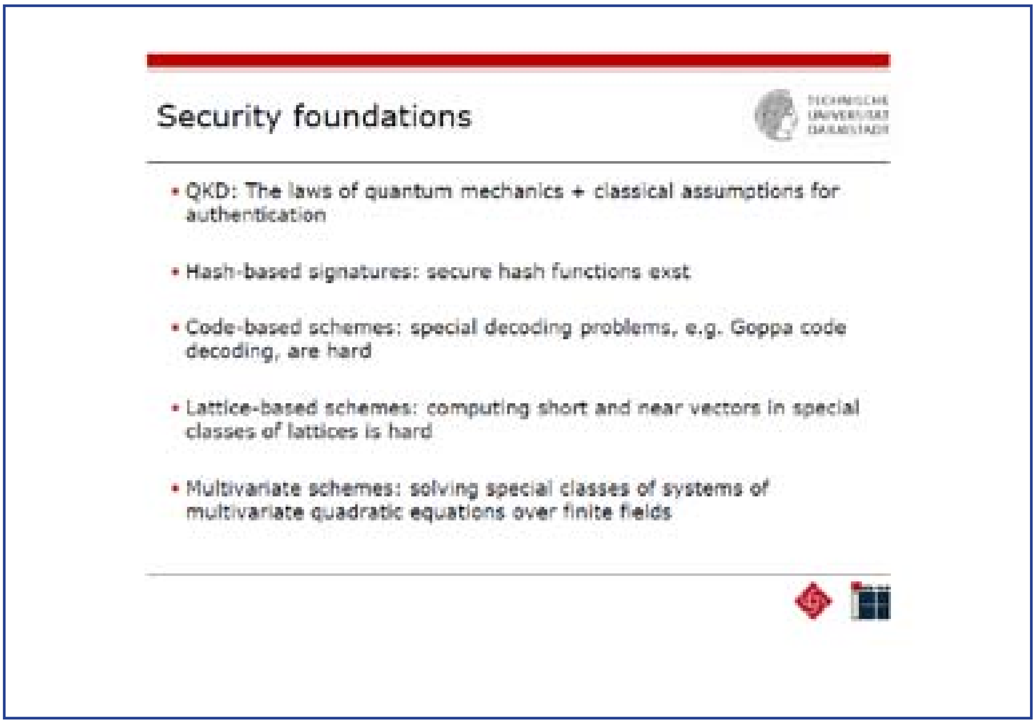
ISBN 979-10-92620-04-7



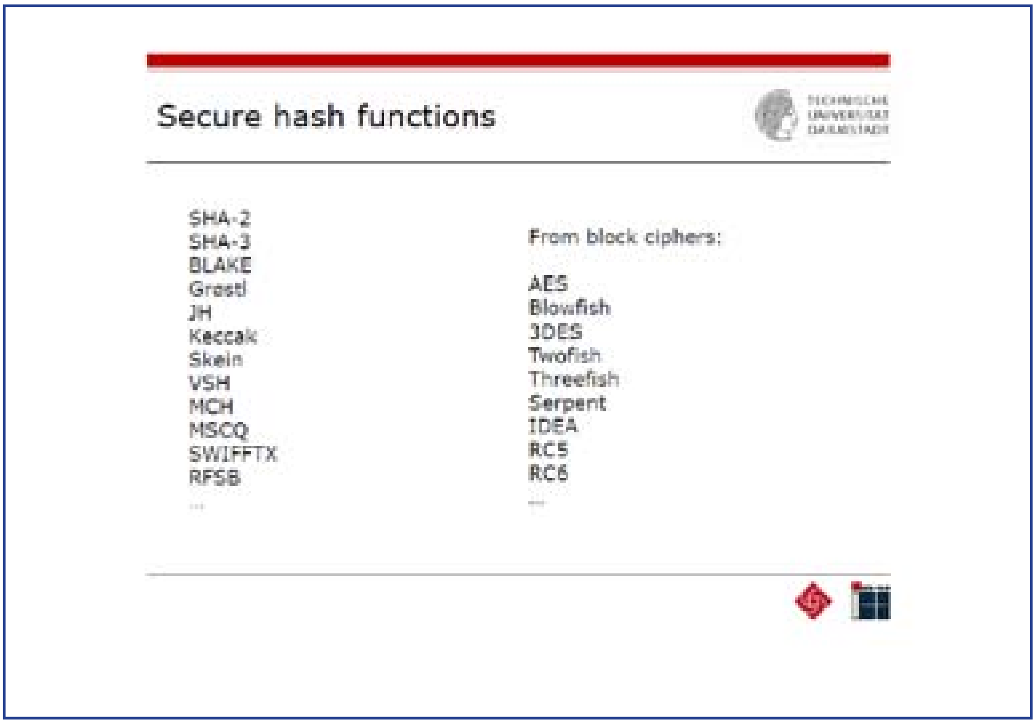


ISBN 979-10-92620-04-7

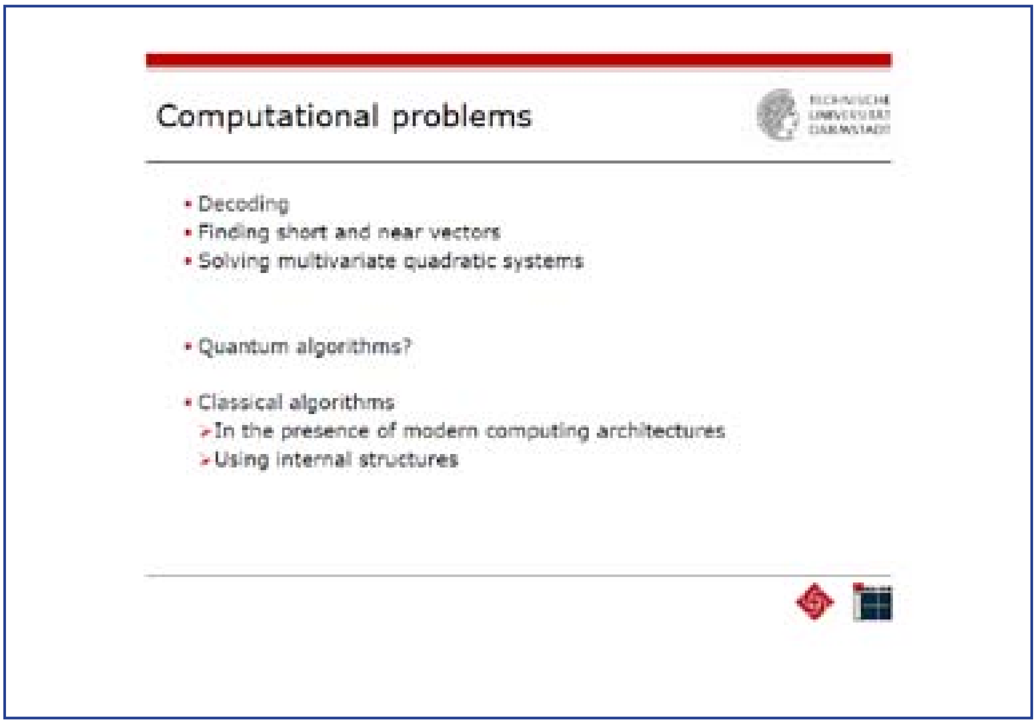


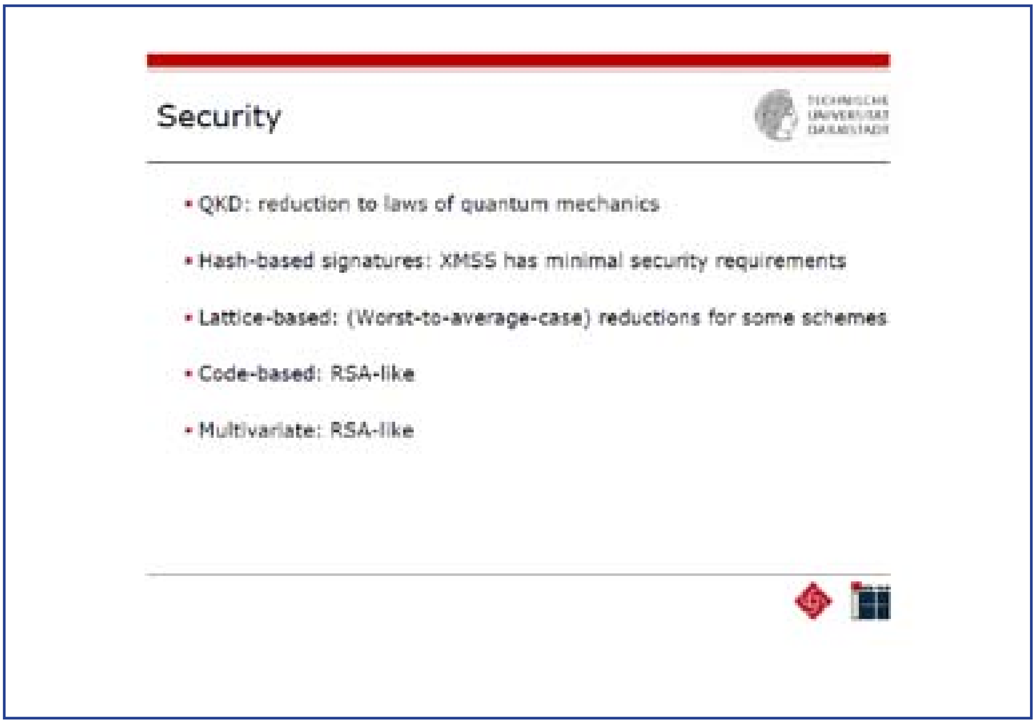


ISBN 979-10-92620-04-7

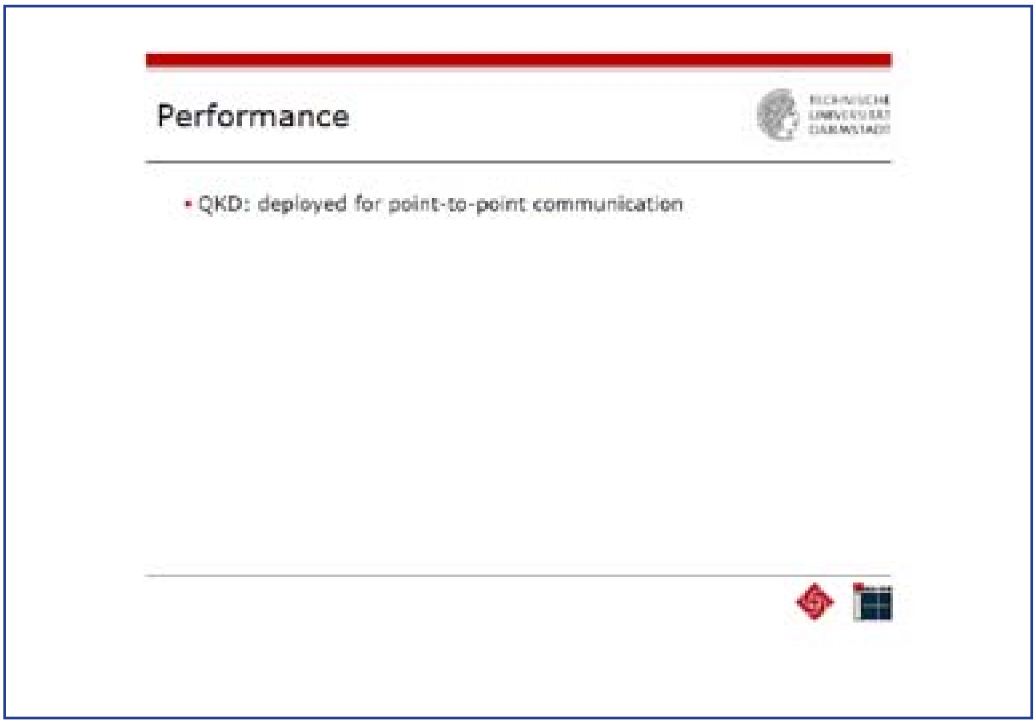


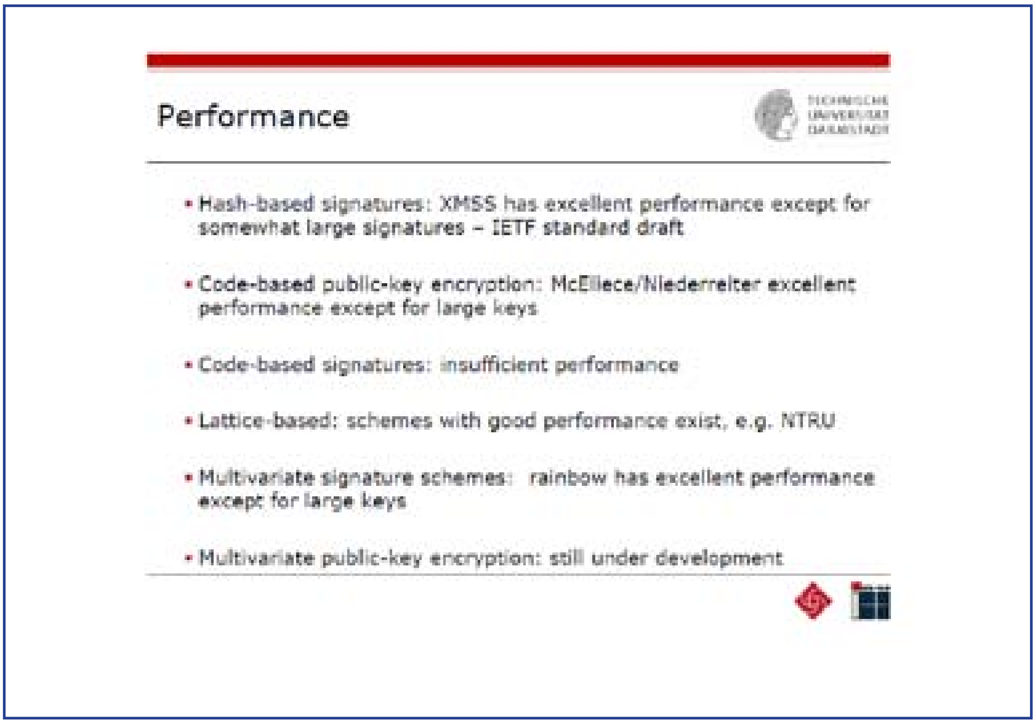
ISBN 979-10-92620-04-7





ISBN 979-10-92620-04-7





ISBN 979-10-92620-04-7

ISBN 979-10-92620-04-7

Presentations

SESSION 2
SETTING THE SCENE

KEYNOTE Speech 5: Why Quantum technologies do matter for Europe

Stephan Lechner, DG Joint Research Centre

ISBN 979-10-92620-04-7

ISBN 979-10-92620-04-7

Presentations

SESSION 2
SETTING THE SCENE

ISBN 979-10-92620-04-7

Presentations

SESSION 2
SETTING THE SCENE

ISBN 979-10-92620-04-7

Presentations

SESSION 2
SETTING THE SCENE

KEYNOTE Speech 7: QKD applications and new physical layer cryptography

Masahide Sasaki, NICT

ISBN 979-10-92620-04-7

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

ISBN 979-10-92620-04-7

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

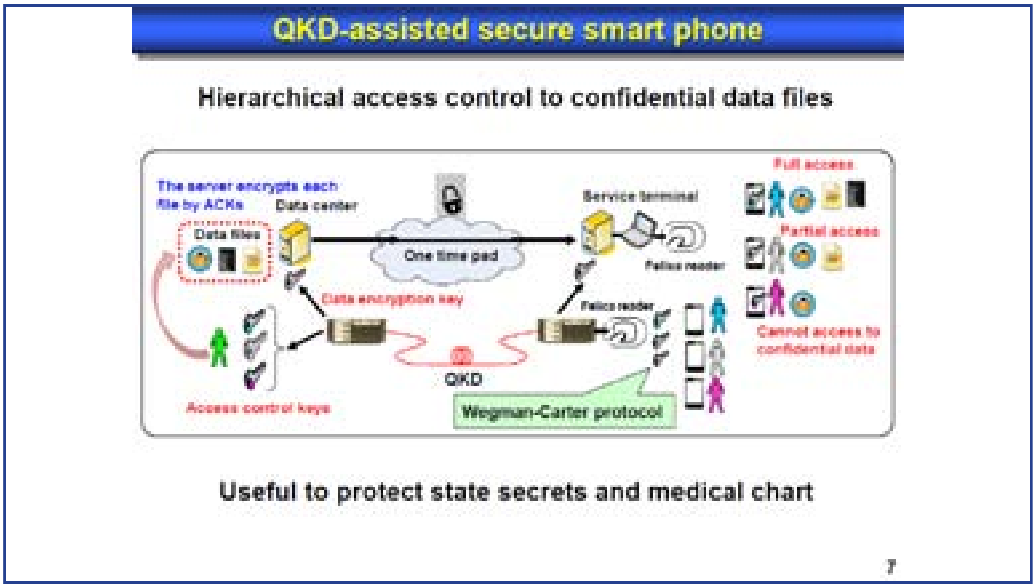
They are looking at future society based on the Internet of Things, and want to know what kind of security technology they should introduce, and how to revise their security systems.

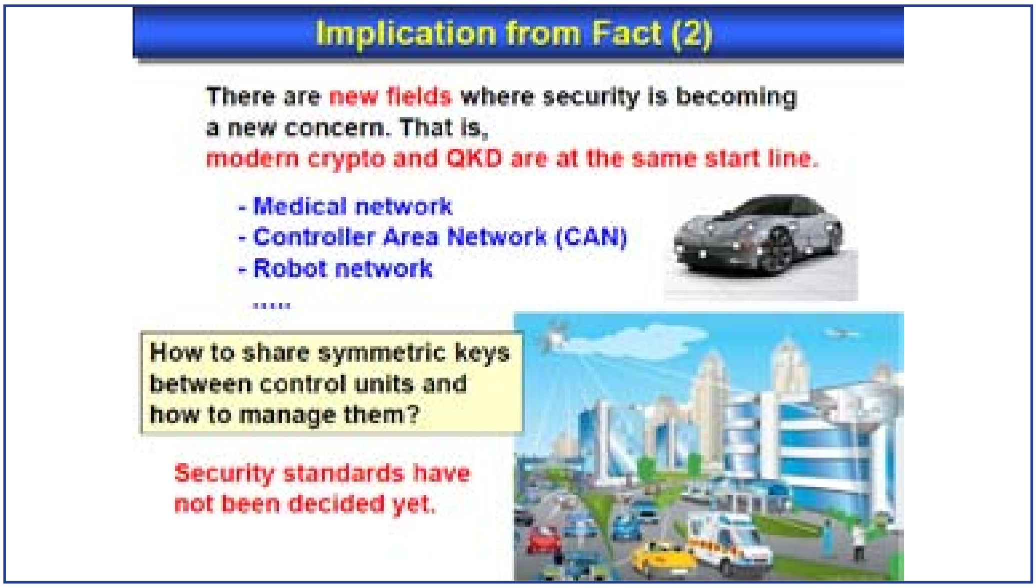
Conversation with them are very inspiring.

QKD-key + smart phone is something marvelous !

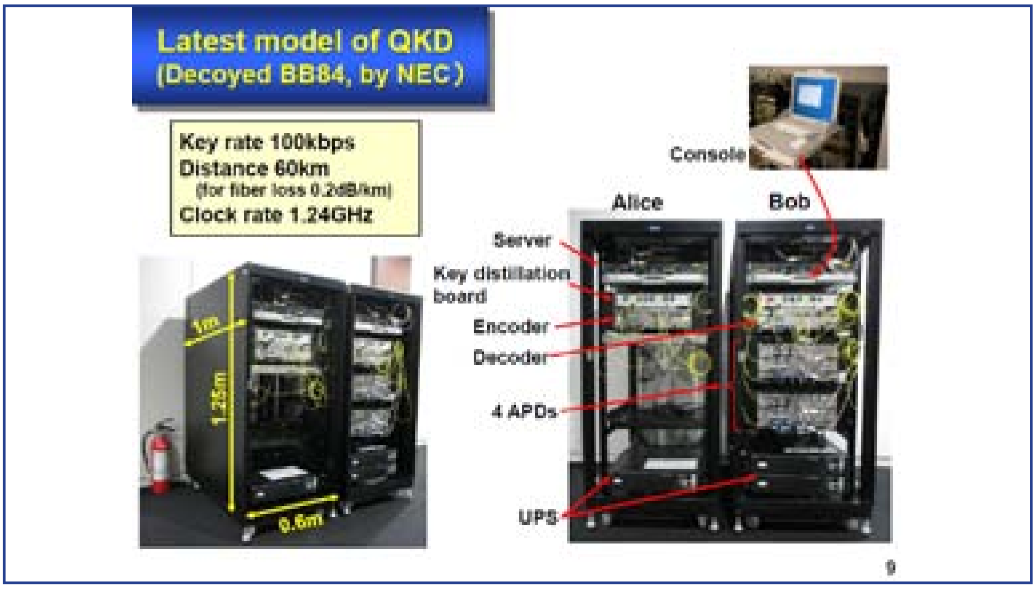
6

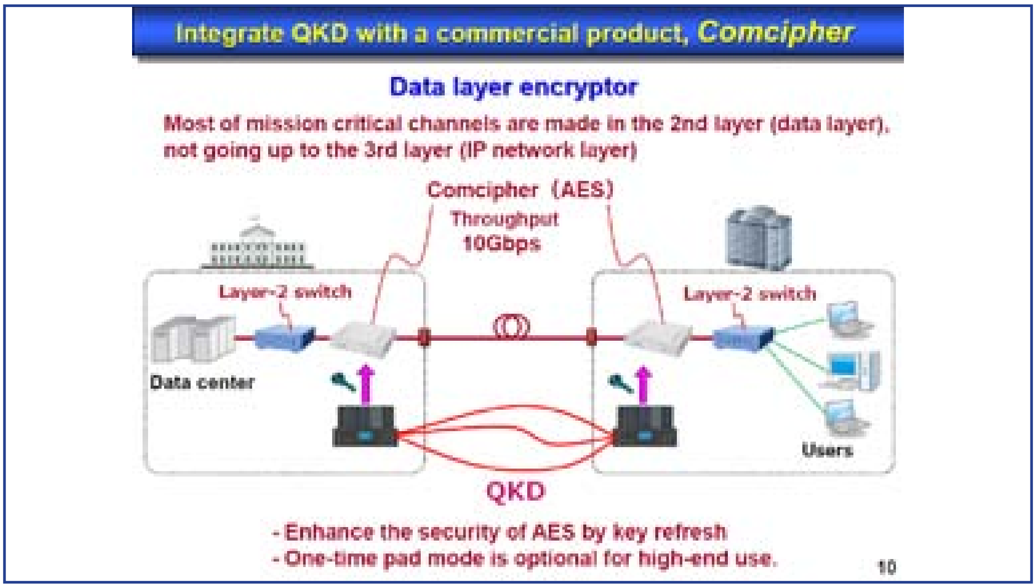
ISBN 979-10-92620-04-7





ISBN 979-10-92620-04-7





ISBN 979-10-92620-04-7

ISBN 979-10-92620-04-7

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

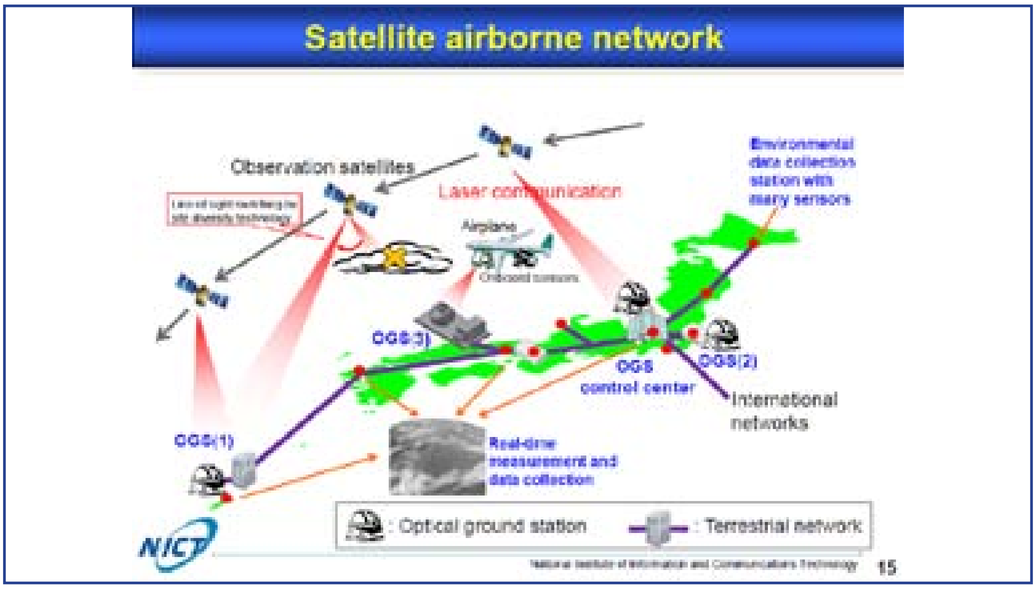
➡ A new physical layer cryptography

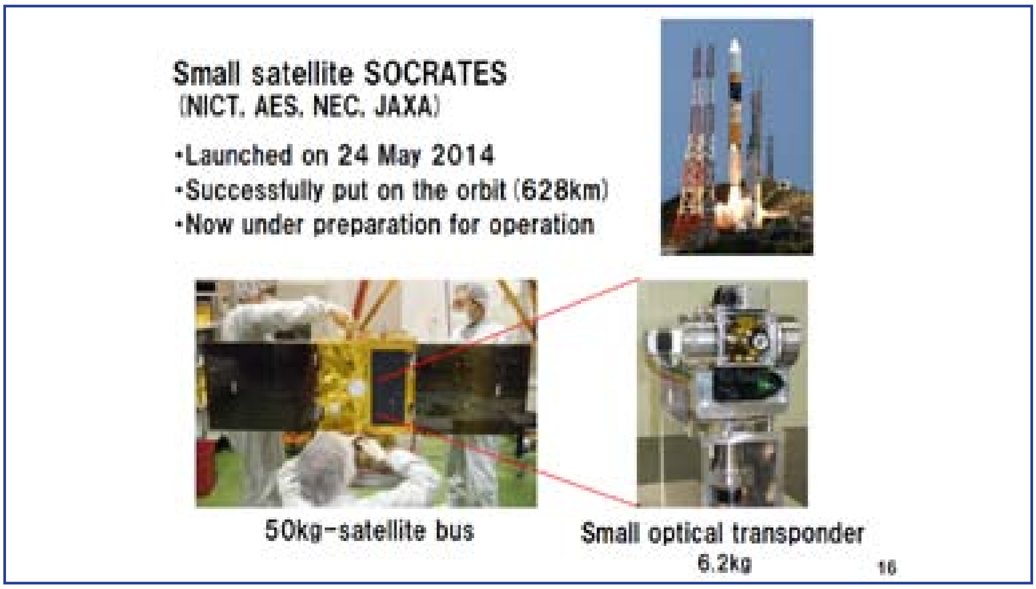
14

ISBN 979-10-92620-04-7

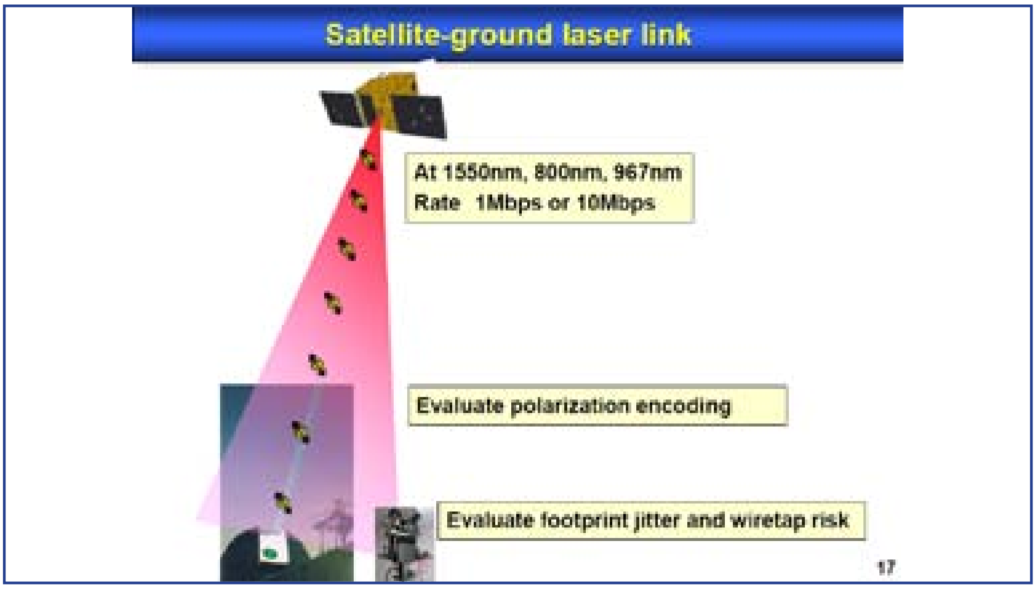
Presentations

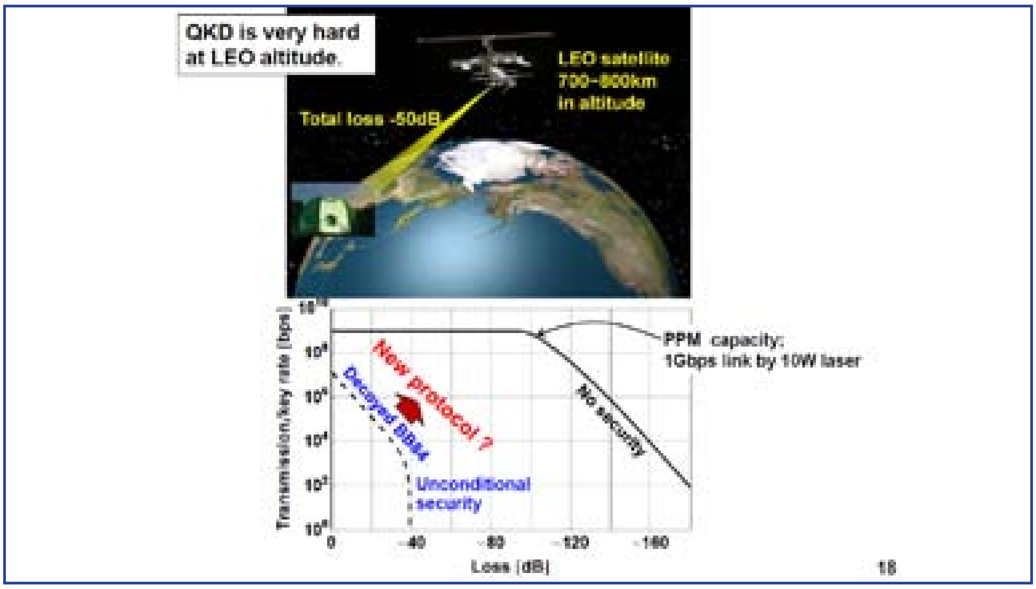
SESSION 2
SETTING THE SCENE



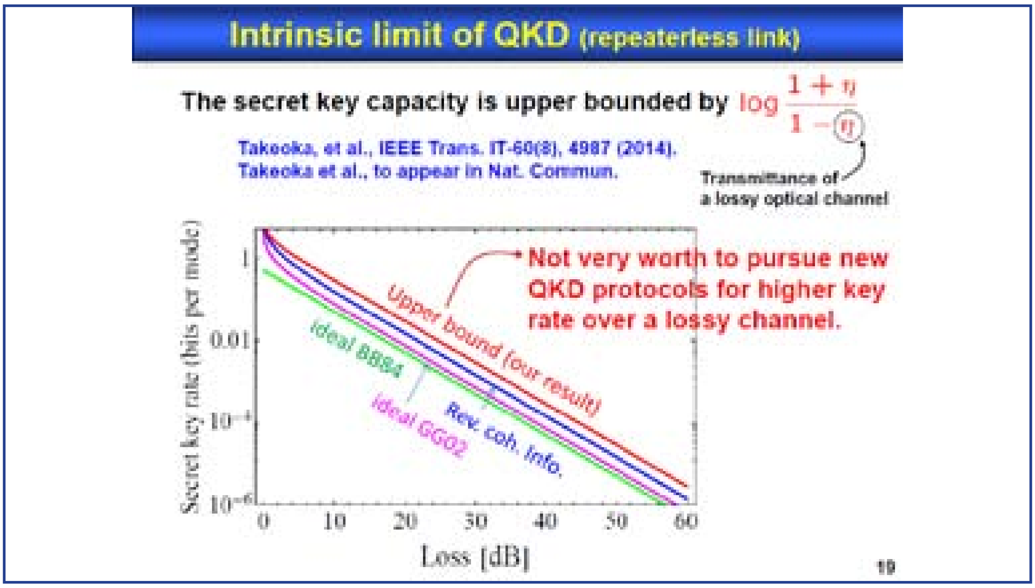


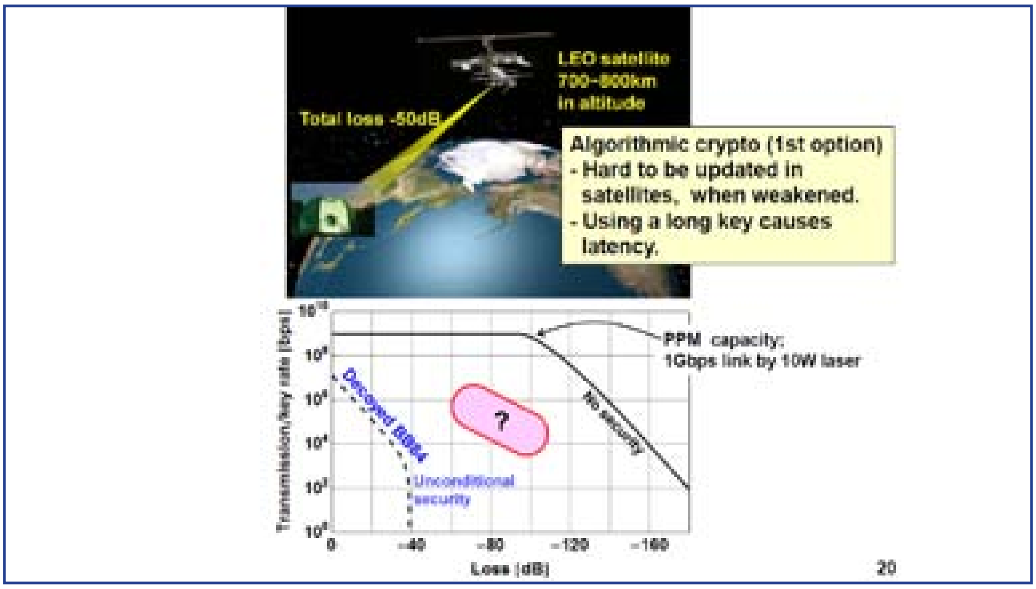
ISBN 979-10-92620-04-7

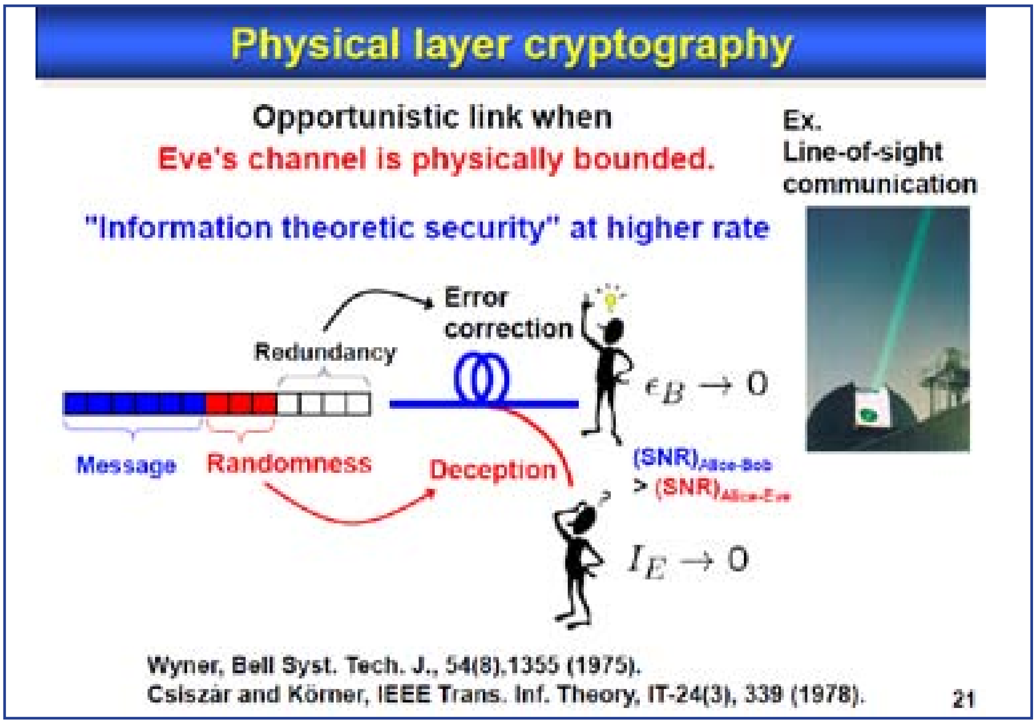


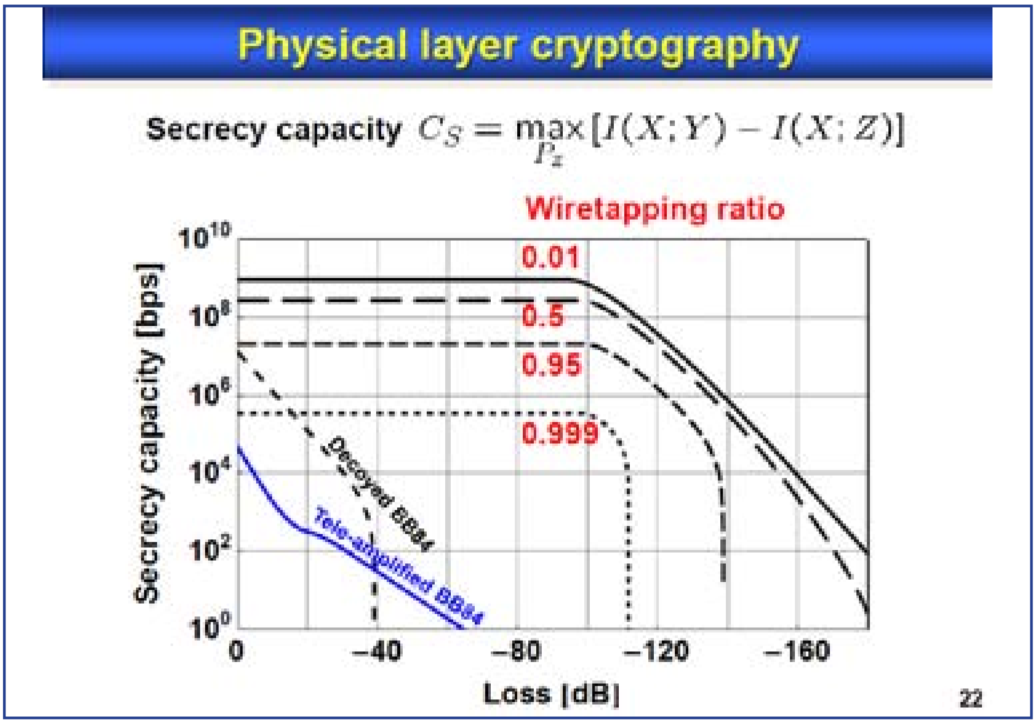


ISBN 979-10-92620-04-7

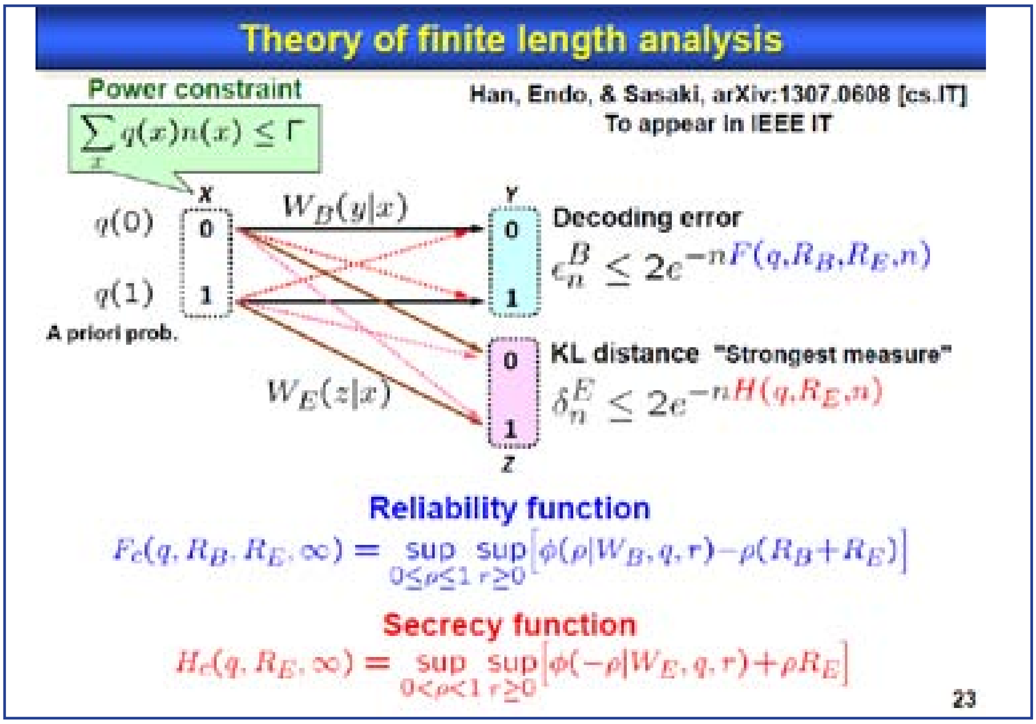

Intrinsic limit of QKD (repeaterless link)
The secret key capacity is upper bounded by log (1 + η)/(1 − η)
Takeoka, et al., IEEE Trans. IT-60(8), 4987 (2014).
Takeoka et al., to appear in Nat. Commun.
Transmittance of a lossy optical channel
Not very worth to pursue new QKD protocols for higher key rate over a lossy channel.
Upper bound (our result)
ideal BB84
Rev. coh. info.
ideal GG02
Secret key rate (bits per mode)
Loss [dB]
19

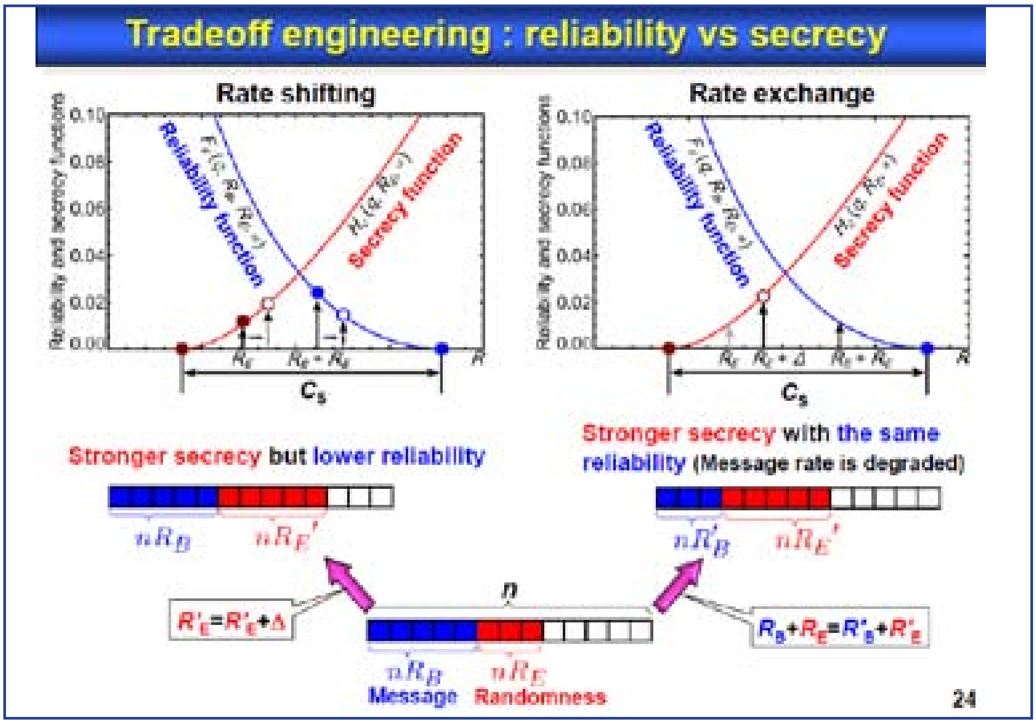

LEO satellite
700~800km
in altitude
Total loss -50dB
Algorithmic crypto (1st option)
- Hard to be updated in satellites, when weakened.
- Using a long key causes latency.
PPM capacity;
1Gbps link by 10W laser
Decoyed BB84
No security
?
Unconditional security
Transmission/key rate [bps]
Loss [dB]
20



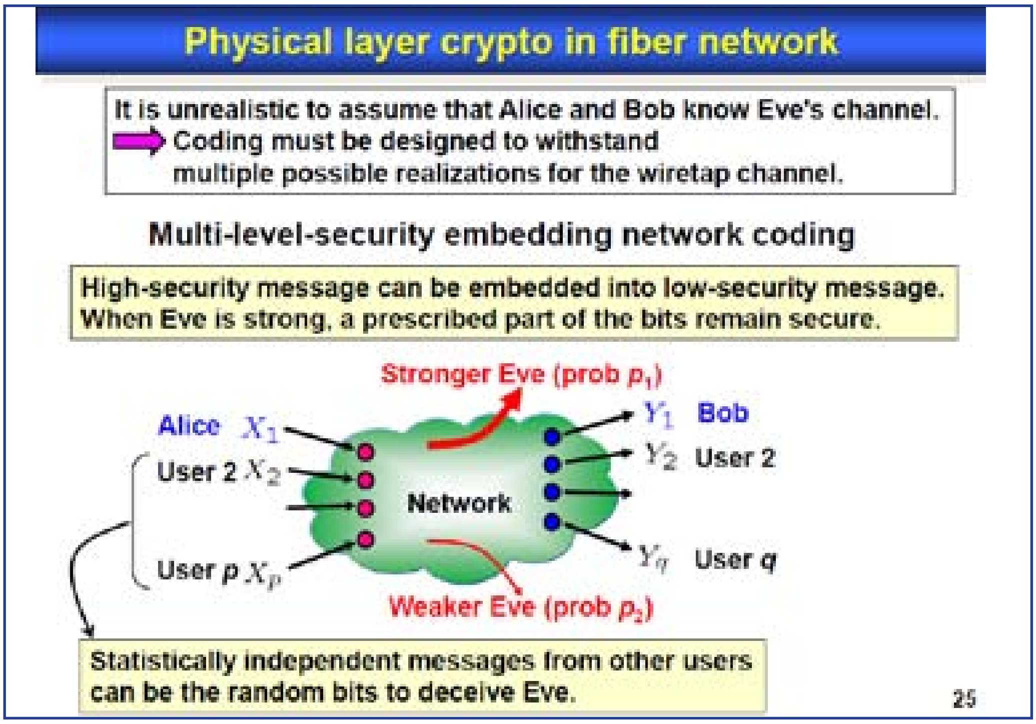


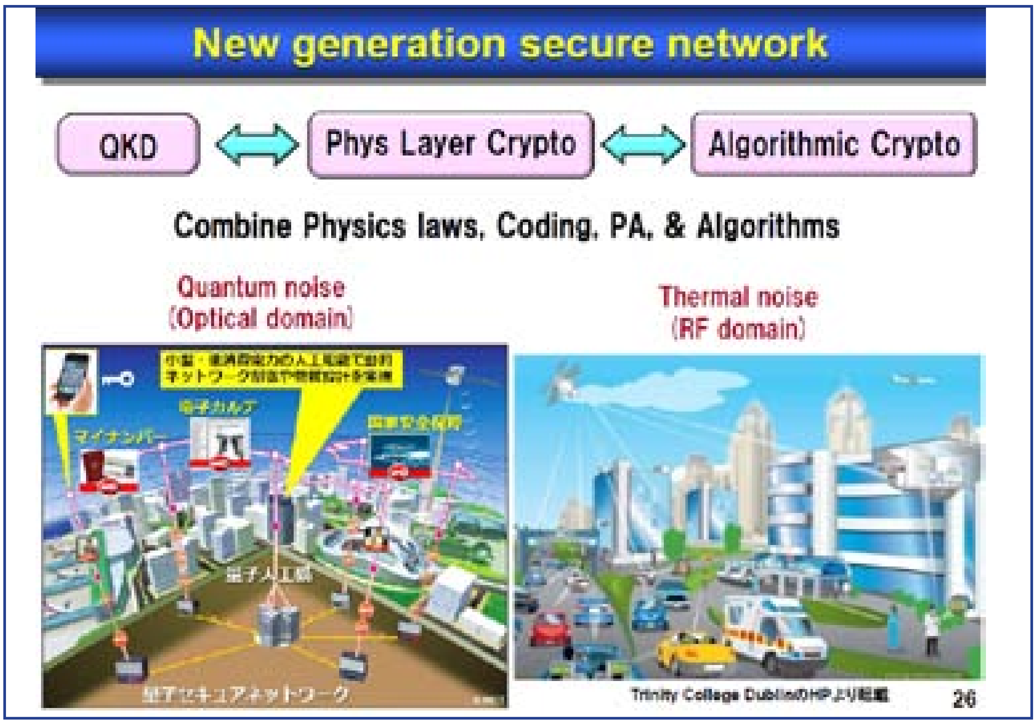
ISBN 979-10-92620-04-7





ISBN 979-10-92620-04-7





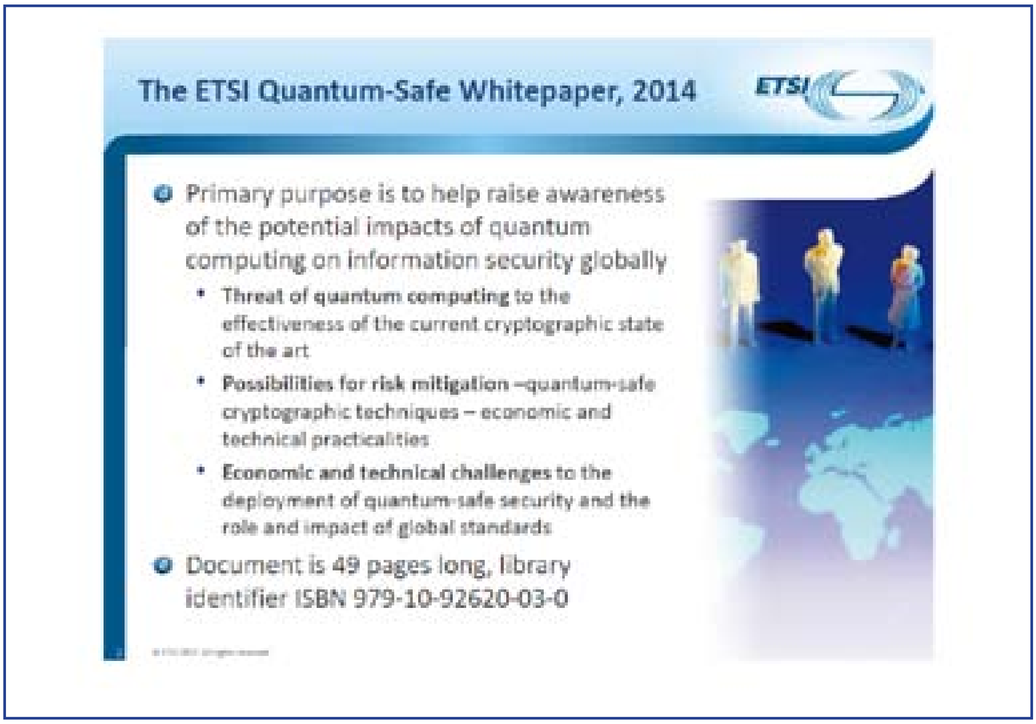
ISBN 979-10-92620-04-7

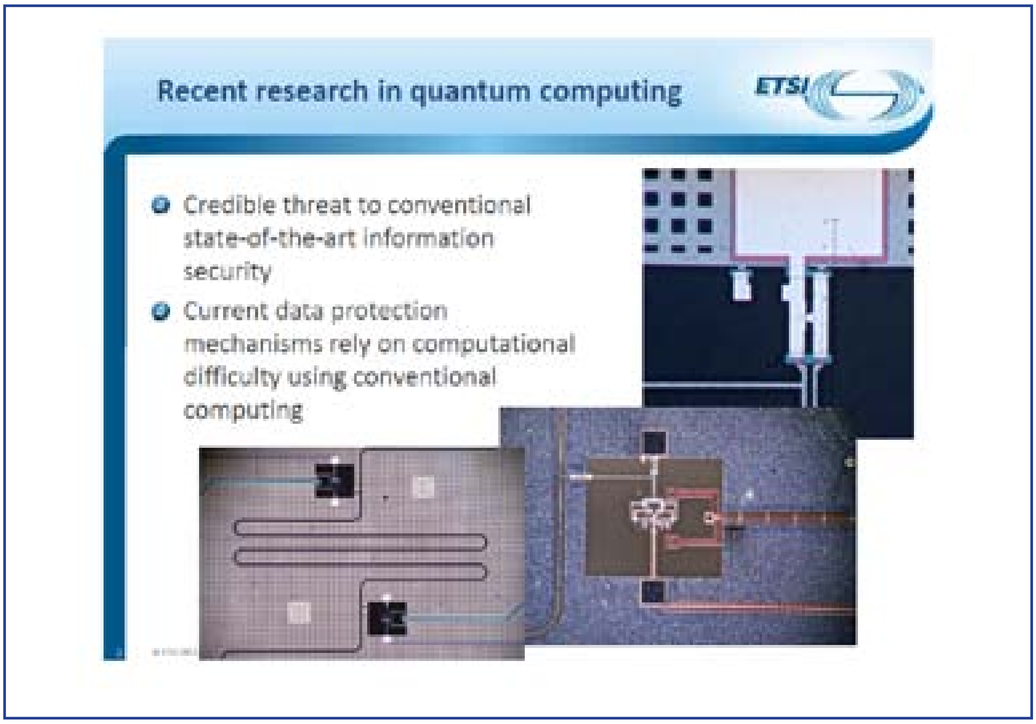
Presentations

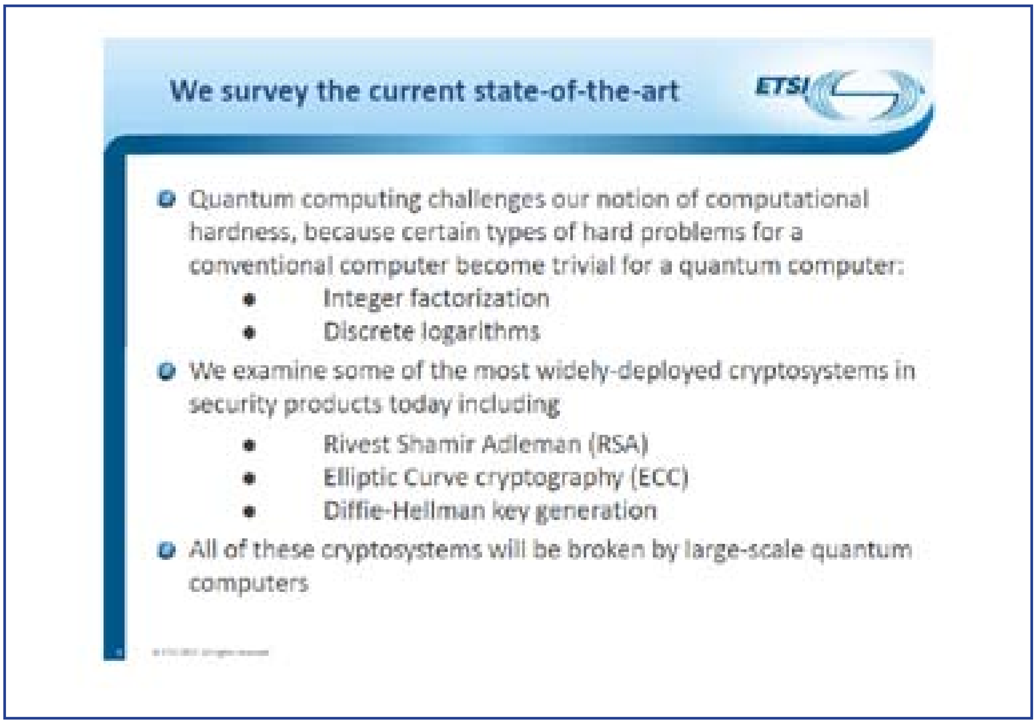
SESSION 2
SETTING THE SCENE

KEYNOTE Speech 8: Quantum-safe cryptography and security
An Introduction, Benefits, Enablers and Challenges – white paper summary

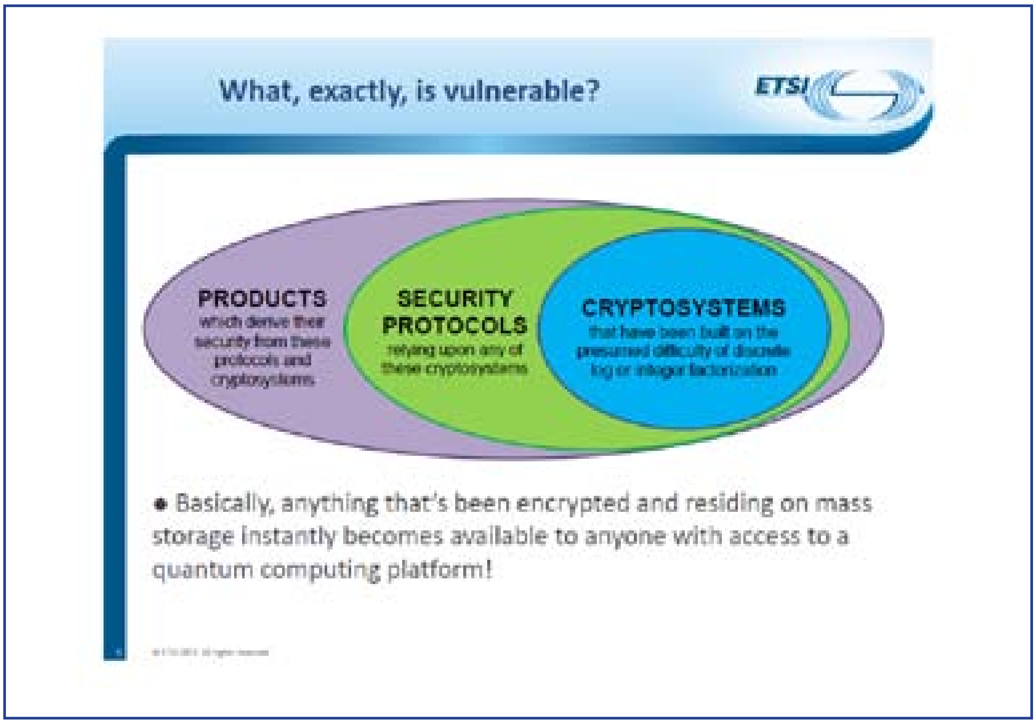
Mark Pecen, Approach Infinity, Inc.

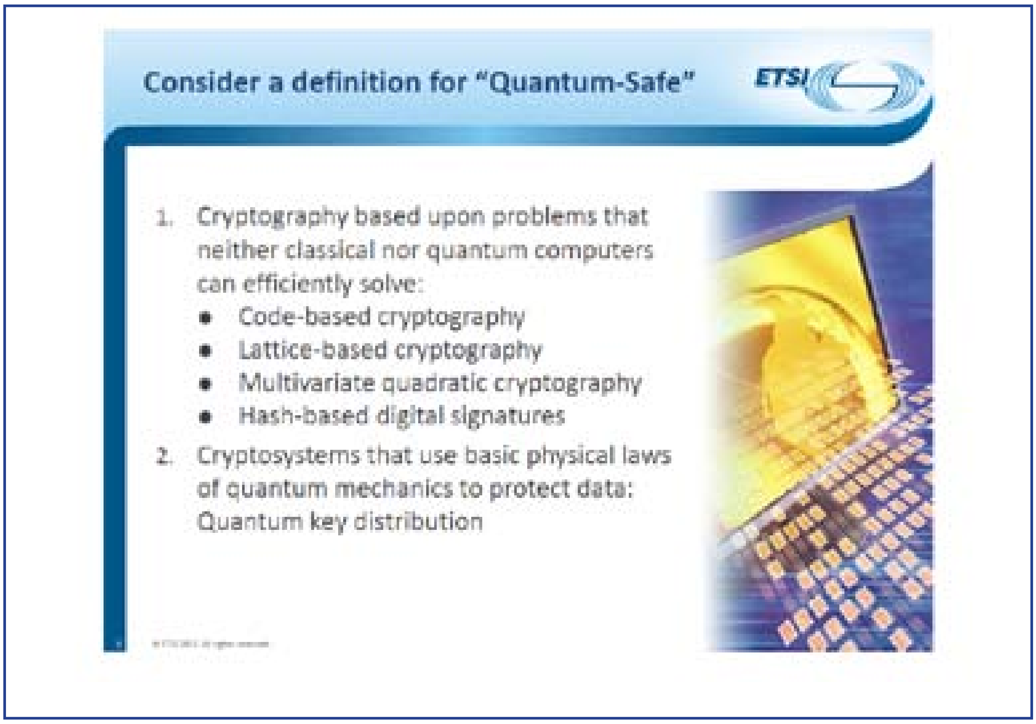




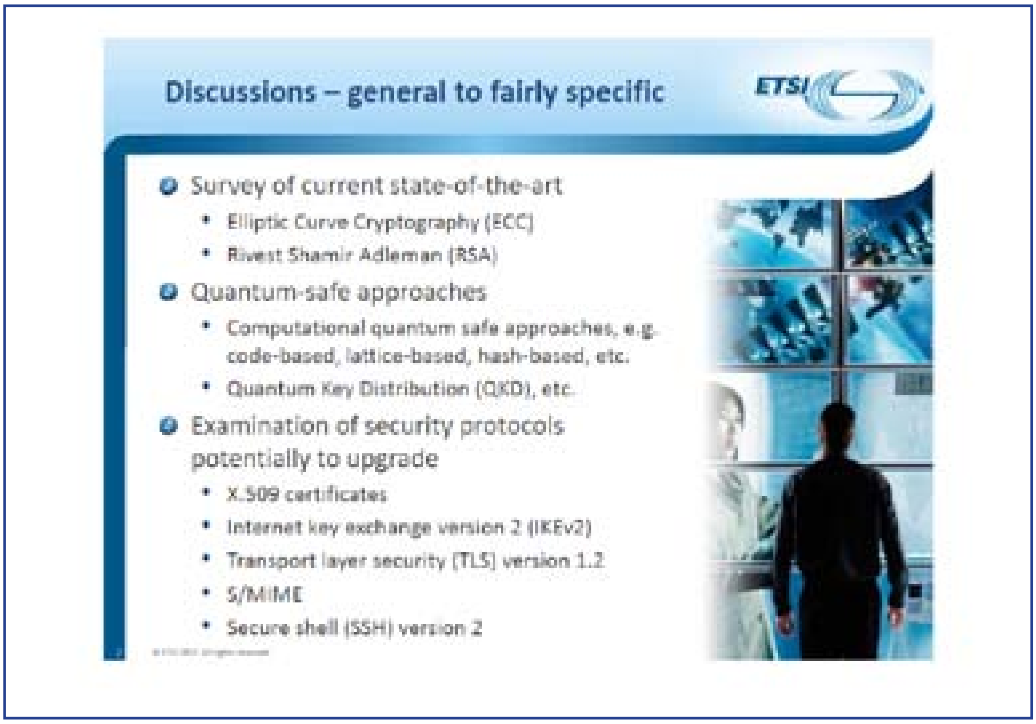


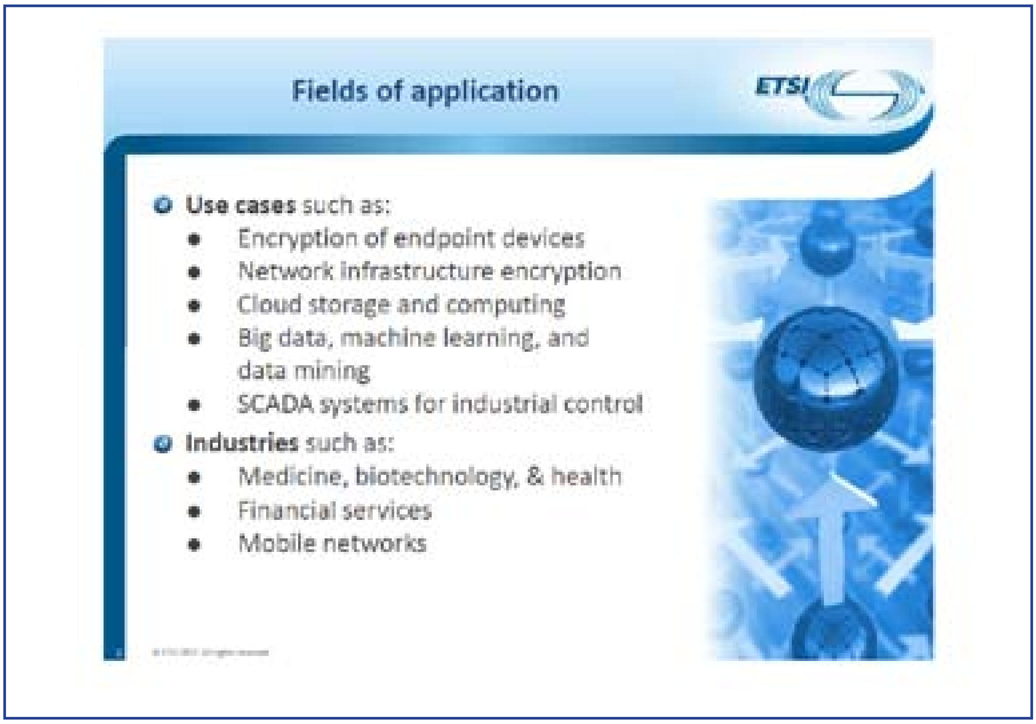
ISBN 979-10-92620-04-7





ISBN 979-10-92620-04-7

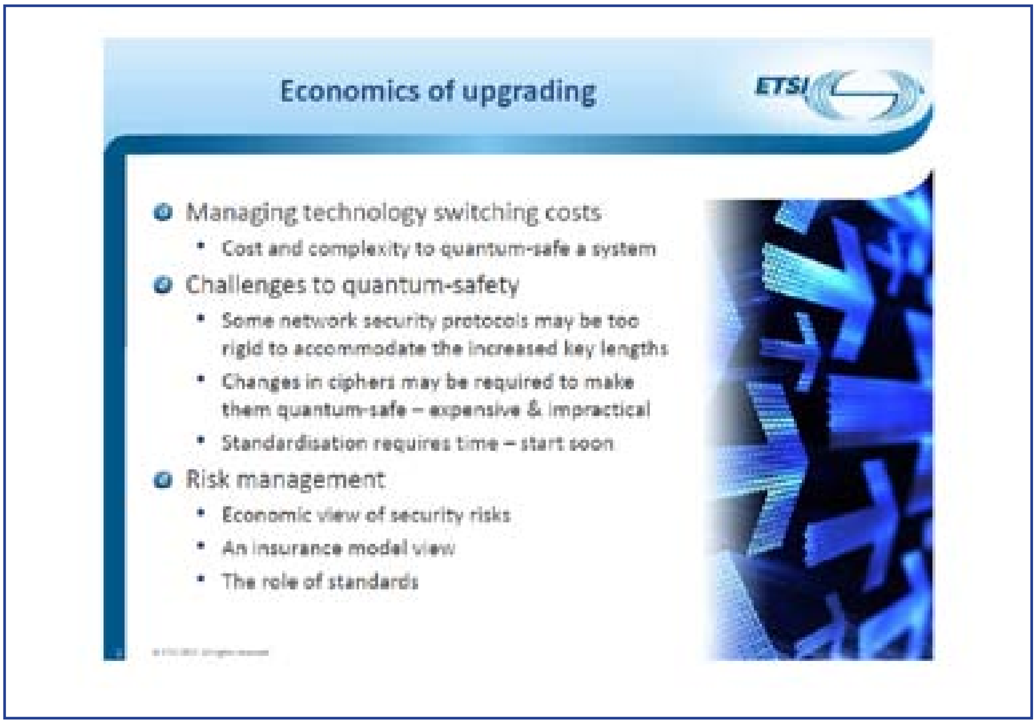


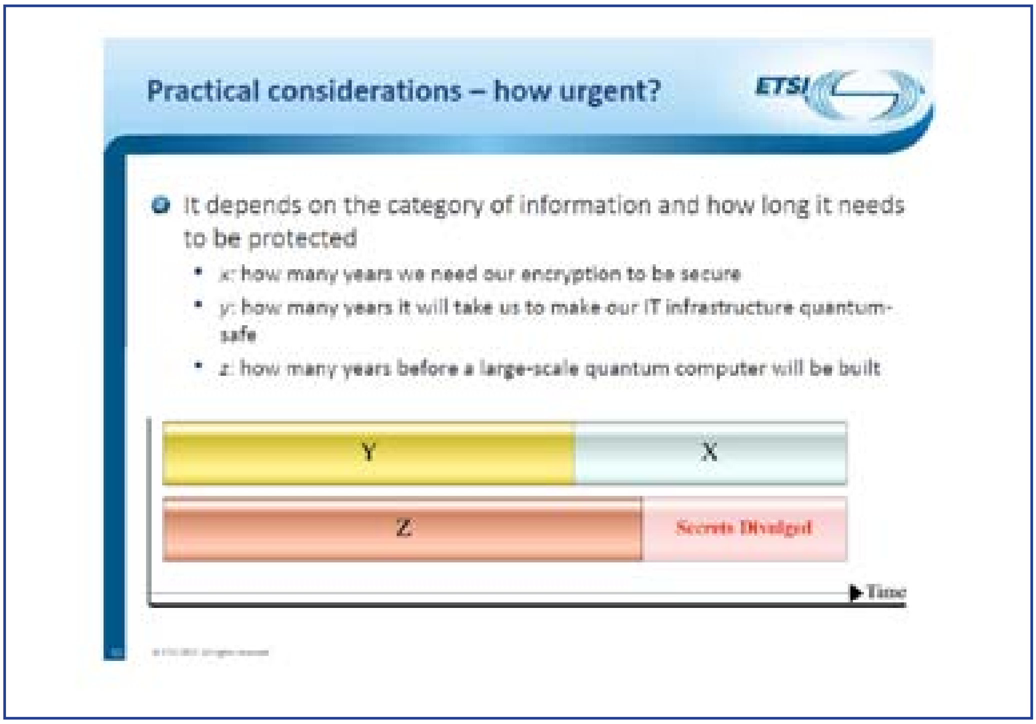


ISBN 979-10-92620-04-7

Presentations

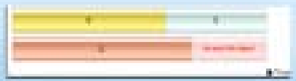
SESSION 2
SETTING THE SCENE





ISBN 979-10-92620-04-7

Not all data are equal



- 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.
- 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.
- 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

Conclusions and way forward

- Quantum computing indeed poses a credible threat to conventional information security systems
- 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
- Recommendations and opportunities for further work are presented
  - Recommendations for enterprises
  - Recommendations for security product vendors
  - Opportunities for further research

ISBN 979-10-92620-04-7

ISBN 979-10-92620-04-7

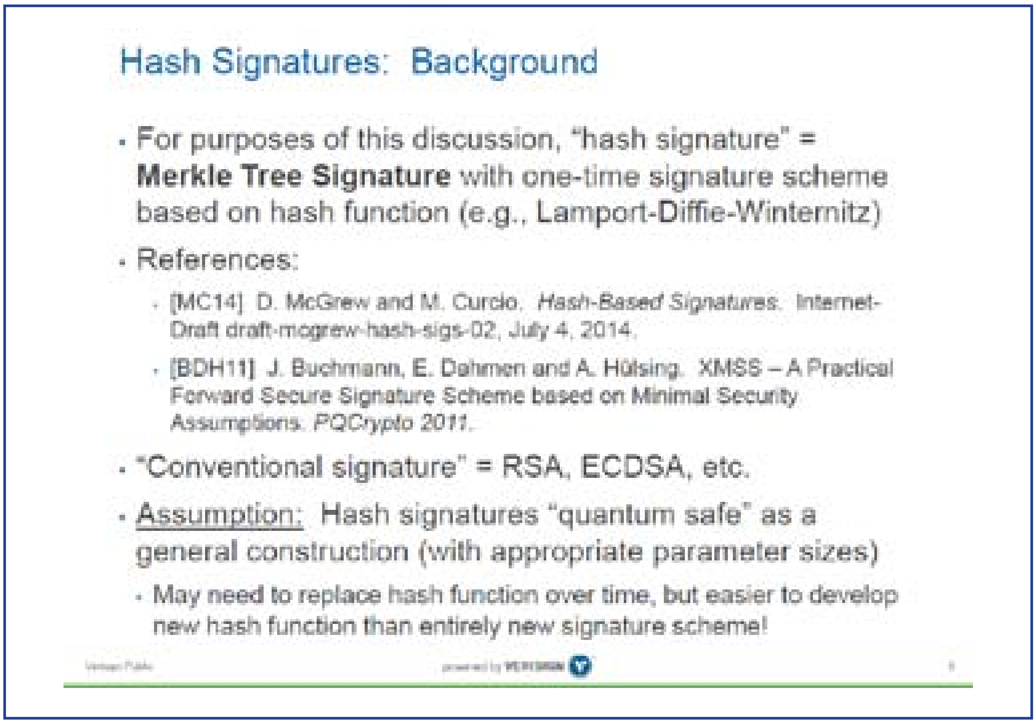
Rethinking the adoption of Hash-Signatures

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.

ISBN 979-10-92620-04-7

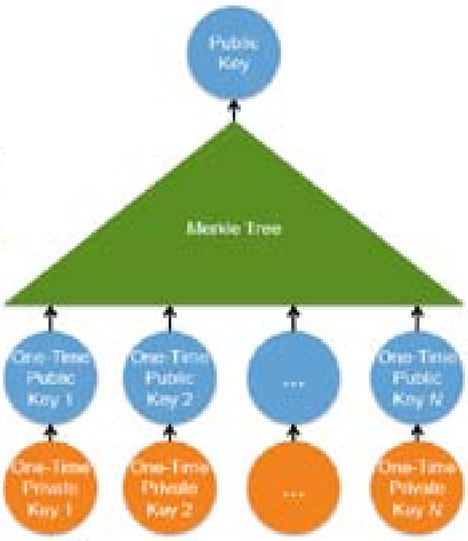


ISBN 979-10-92620-04-7

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



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

ISBN 979-10-92620-04-7

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

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**

ISBN 979-10-92620-04-7

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**

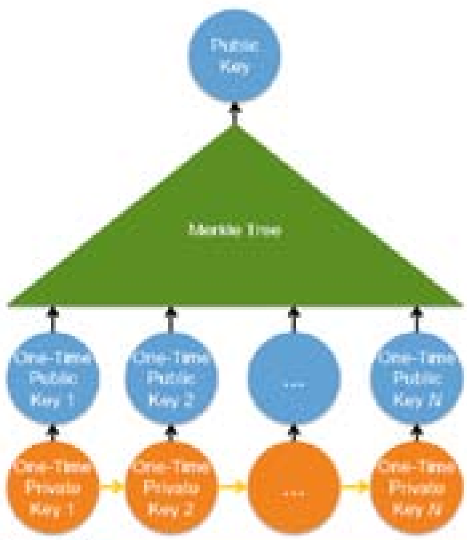
- Advantage: Short backdating windows **without frequent key rollovers** / certificate updates
  - Trust model improvement: Signer can **bound impact of private key compromise** to shorter time period
- Application: Time-based transaction signing

Verisign Public — powered by VERISIGN

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



Verisign Public — powered by VERISIGN

ISBN 979-10-92620-04-7

#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

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

ISBN 979-10-92620-04-7

A Proposed Adoption Strategy for Hash Signatures

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

ISBN 979-10-92620-04-7

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
- <u>Application question:</u> Would it matter if signatures could be computed in real time in some cases?

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

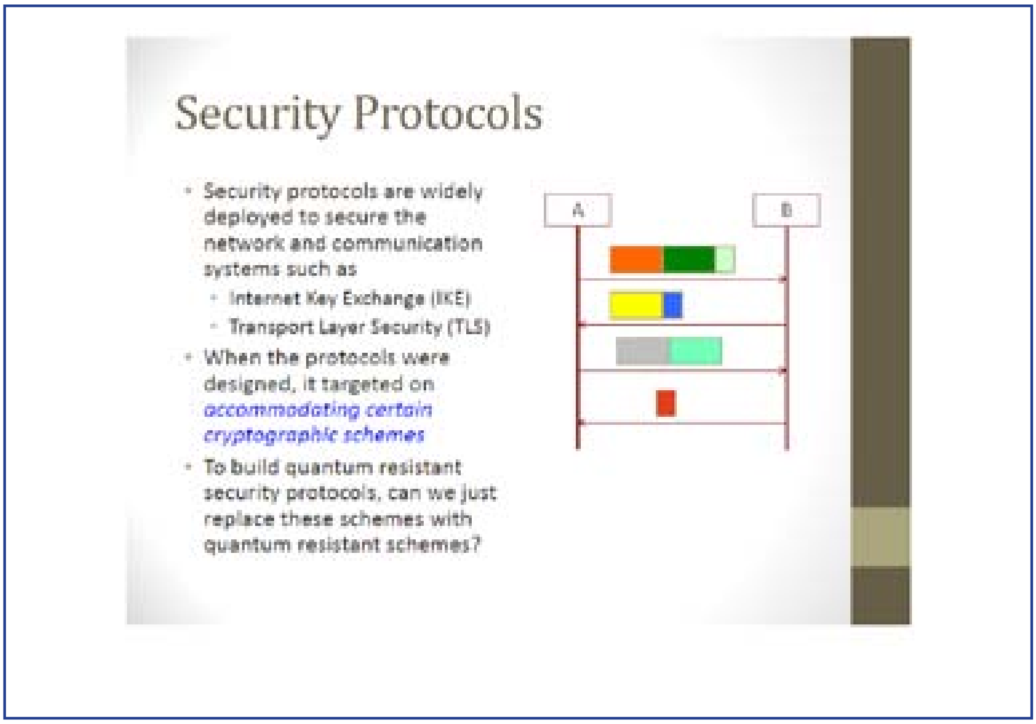
ISBN 979-10-92620-04-7

Neither do people pour new wine into old wineskins

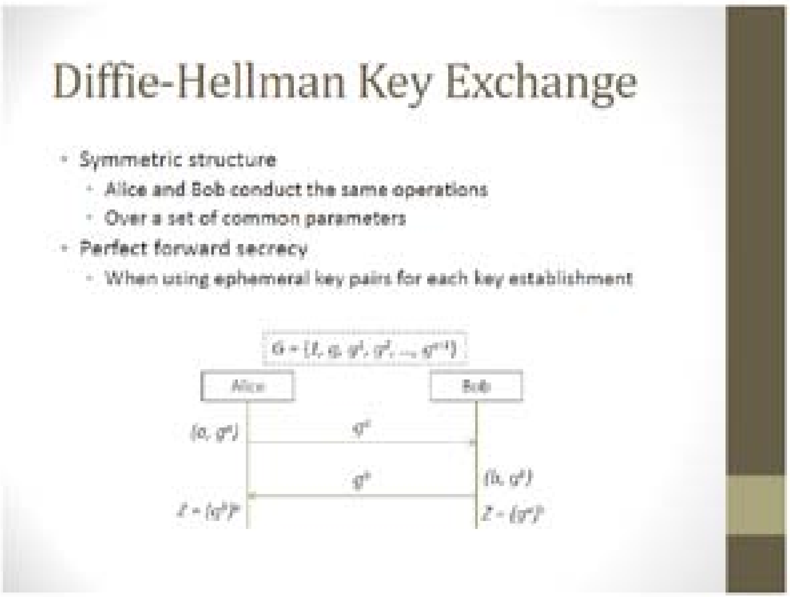
Lily Chen, NIST

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.

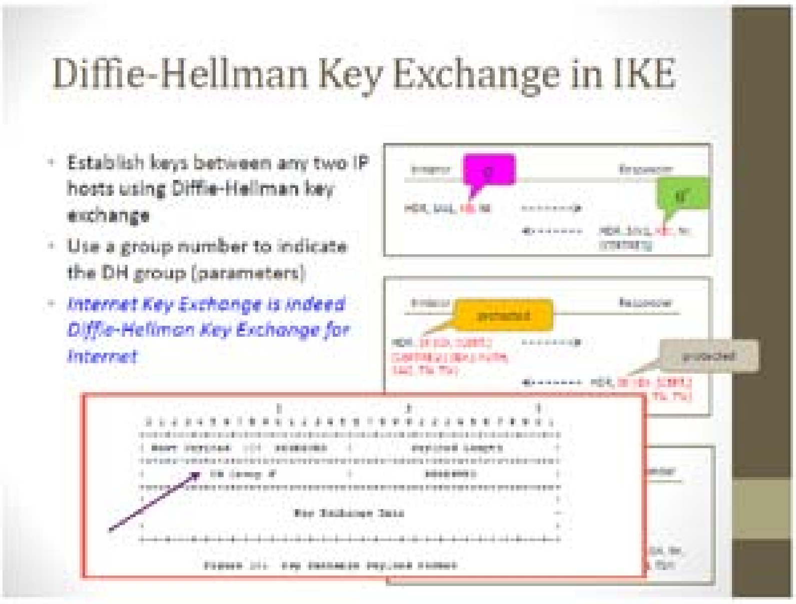
ISBN 979-10-92620-04-7

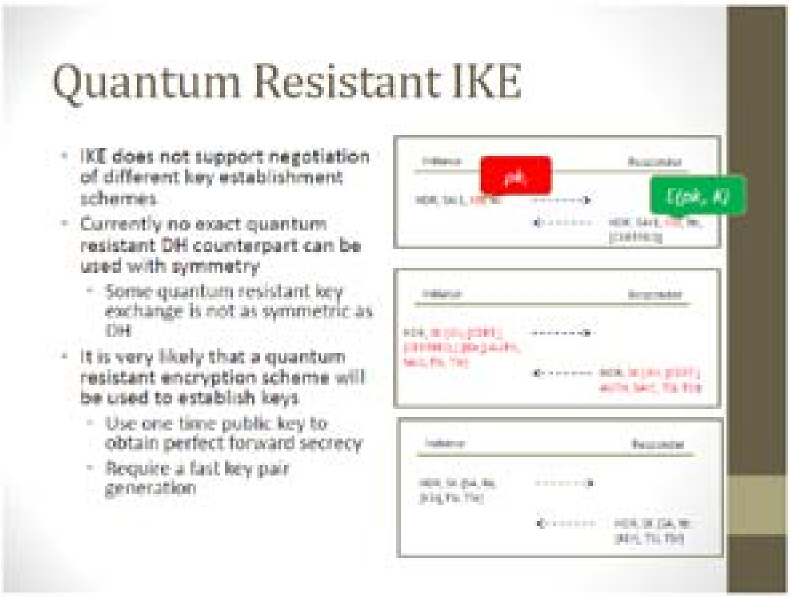


ISBN 979-10-92620-04-7

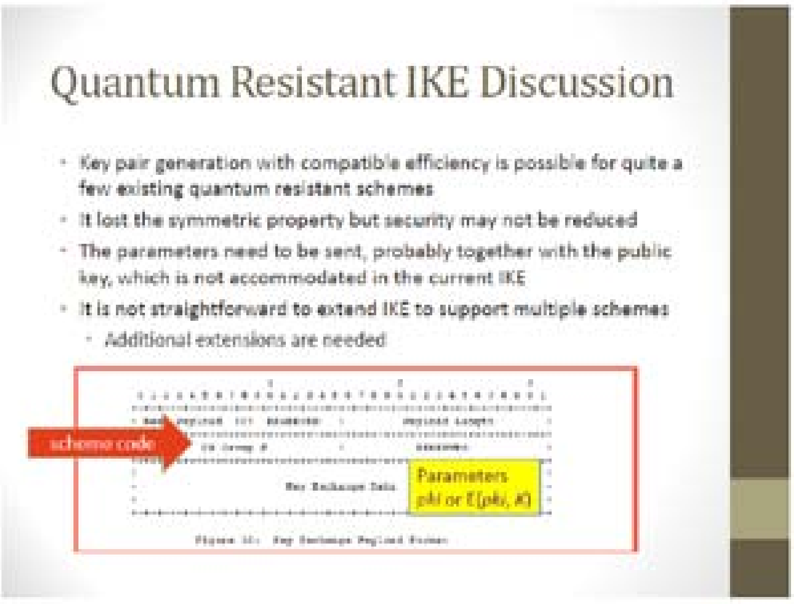


ISBN 979-10-92620-04-7

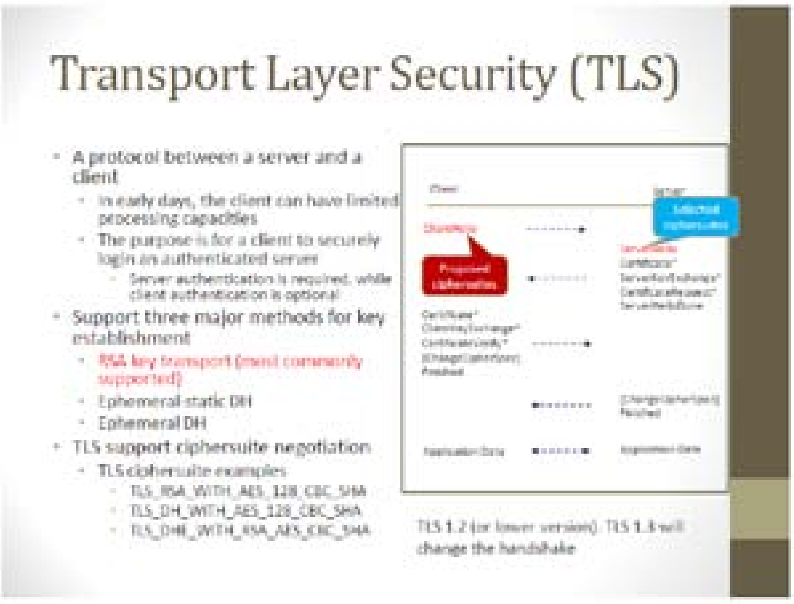


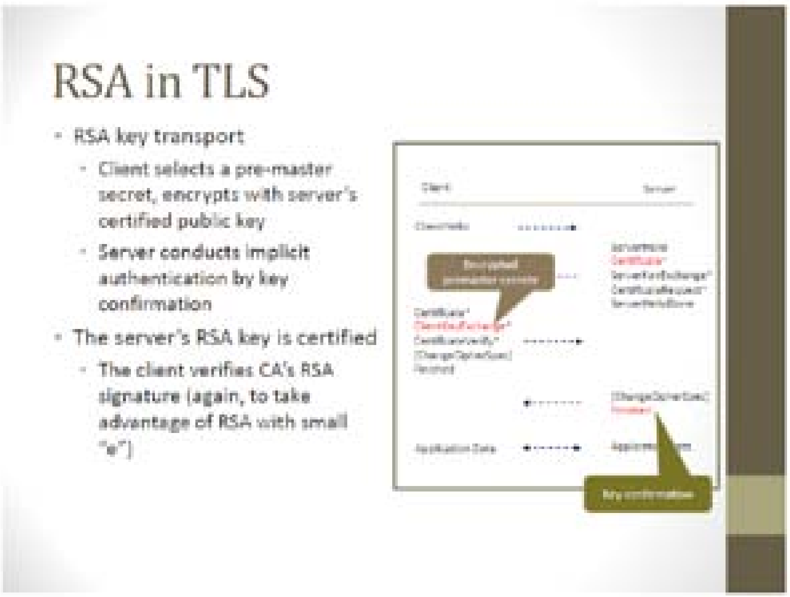


ISBN 979-10-92620-04-7

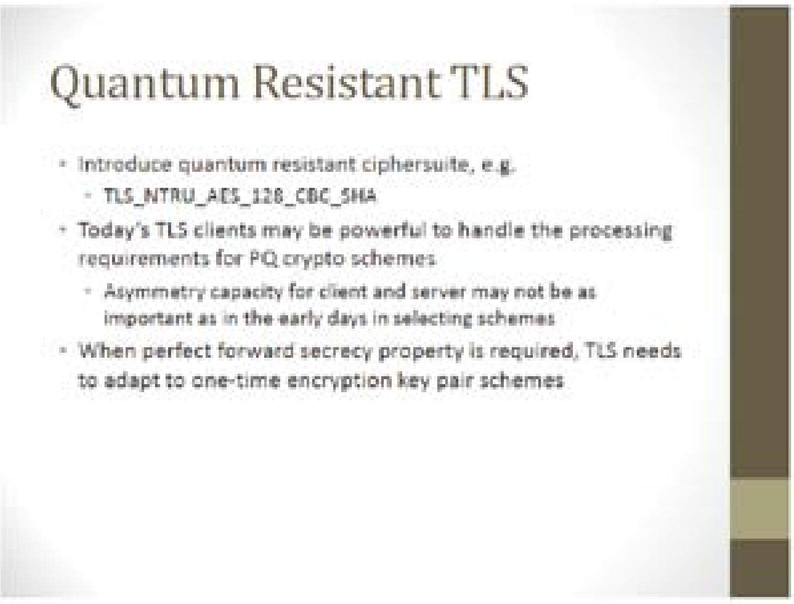


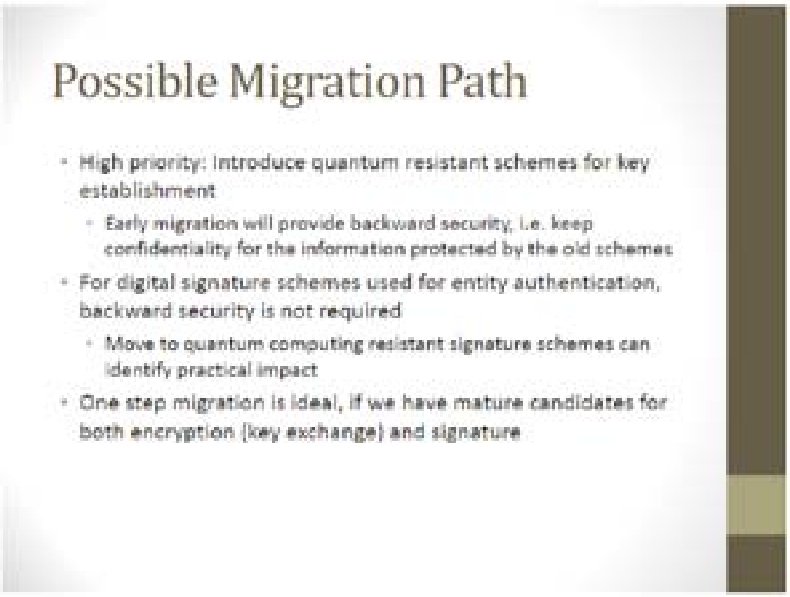
ISBN 979-10-92620-04-7



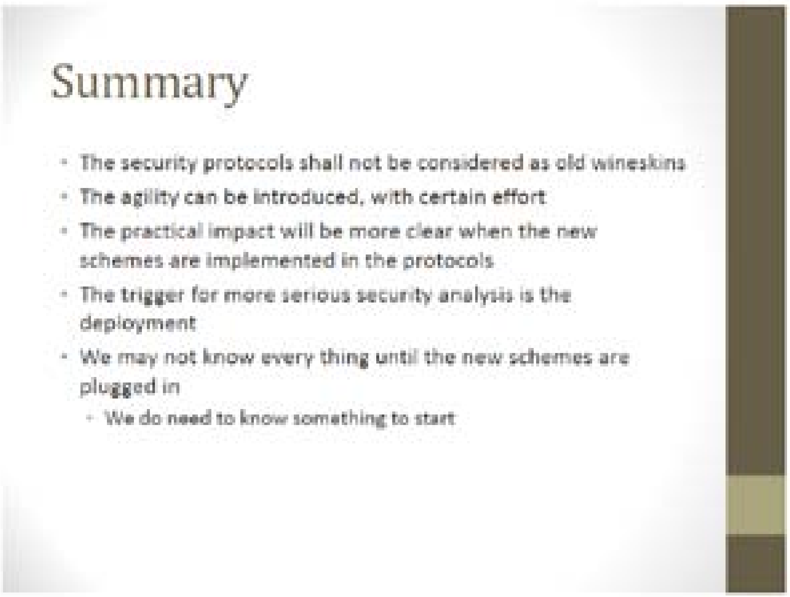


ISBN 979-10-92620-04-7





ISBN 979-10-92620-04-7



ISBN 979-10-92620-04-7

ISBN 979-10-92620-04-7

Towards a standard for practical Hash-based Signatures

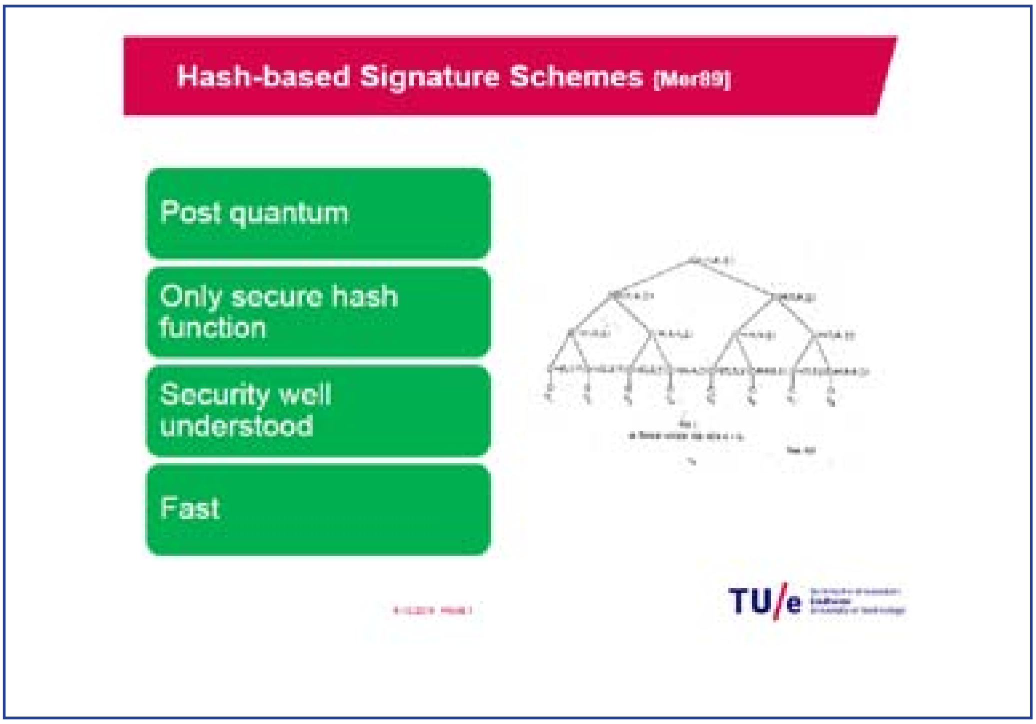
Andres Hüsling, Technische Universiteit Eindhoven

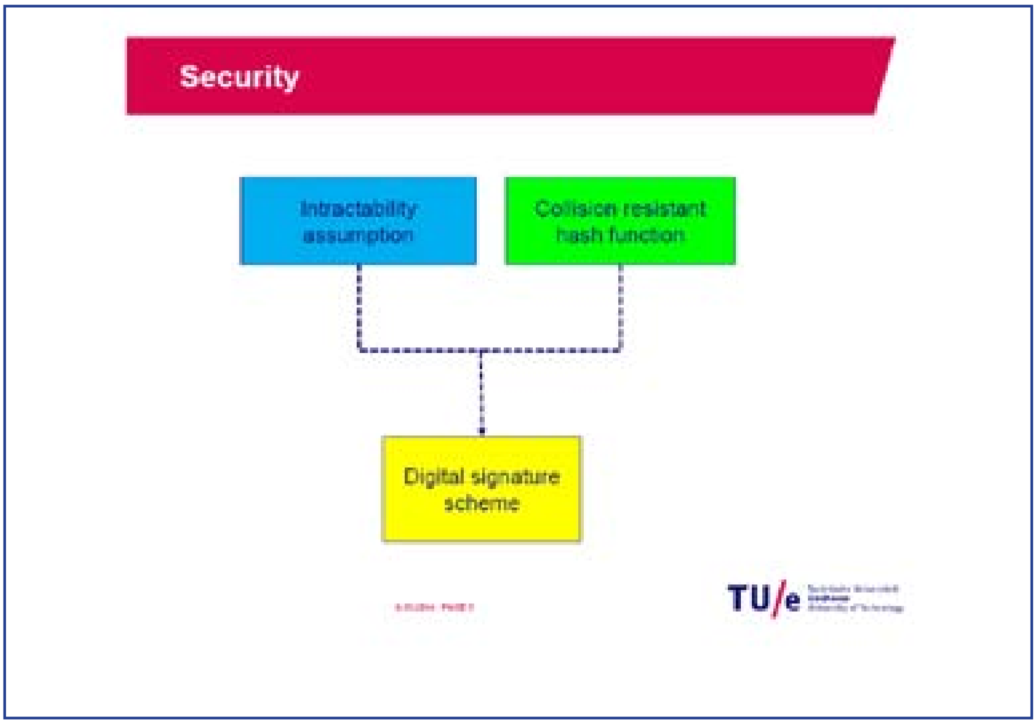
Variants of the Merkle scheme are promising candidates for quantum-safe digital signatures. An Internet-Draft on hash-based signatures was published last year [1]. It covers Merkle's traditional tree-based signature scheme, instantiated with Winternitz one-time signatures. Our talk presents this recent 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/





ISBN 979-10-92620-04-7

Post-Quantum Security

n-bit hash function

Grover'96:

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

Brassard et al. 1998:

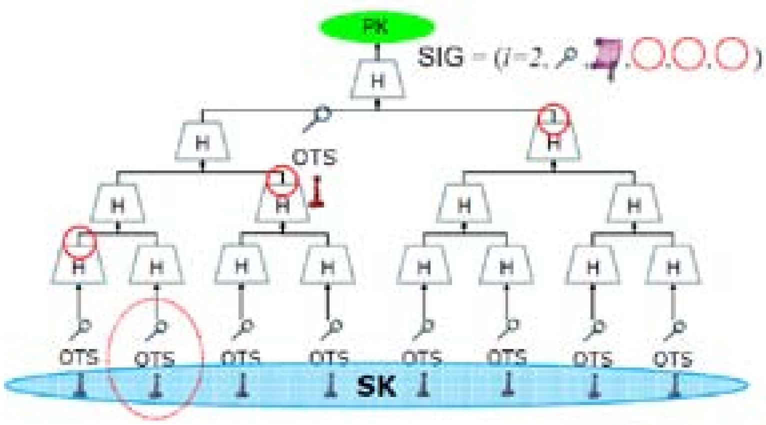
Collision finding $O(2^{\frac{n}{2}}) \to O(2^{\frac{n}{3}})$

Aaronson & Shi'04:

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

TU/e

Merkle's Hash-based Signatures



TU/e

ISBN 979-10-92620-04-7

Practical Challenge: Handle State

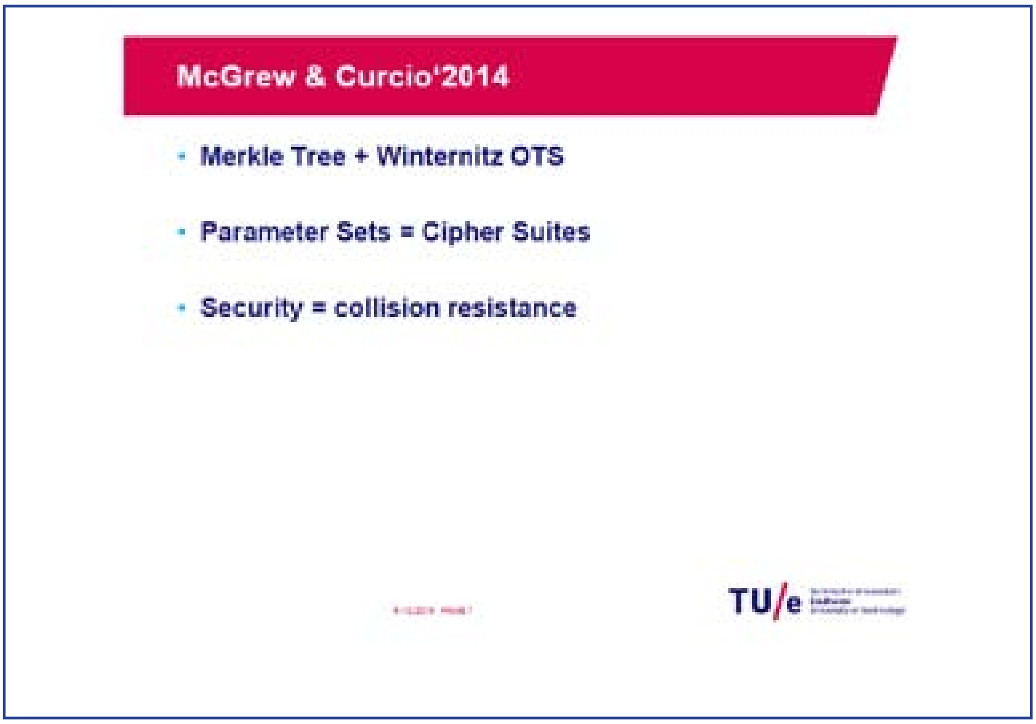
- Can be avoided in theory, paid with efficiency
- Different API
  - Handle integration
- Prevent copies
  - No key back-up
- Multi-threading safety
- Industry input appreciated

TU/e

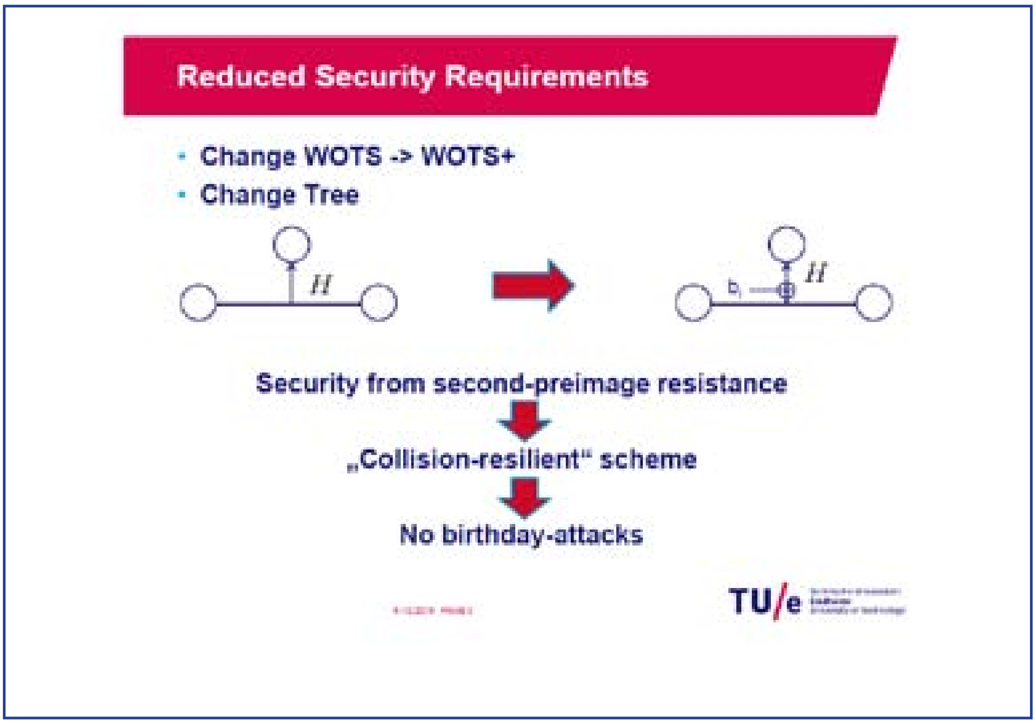
McGrew & Curcio'2014

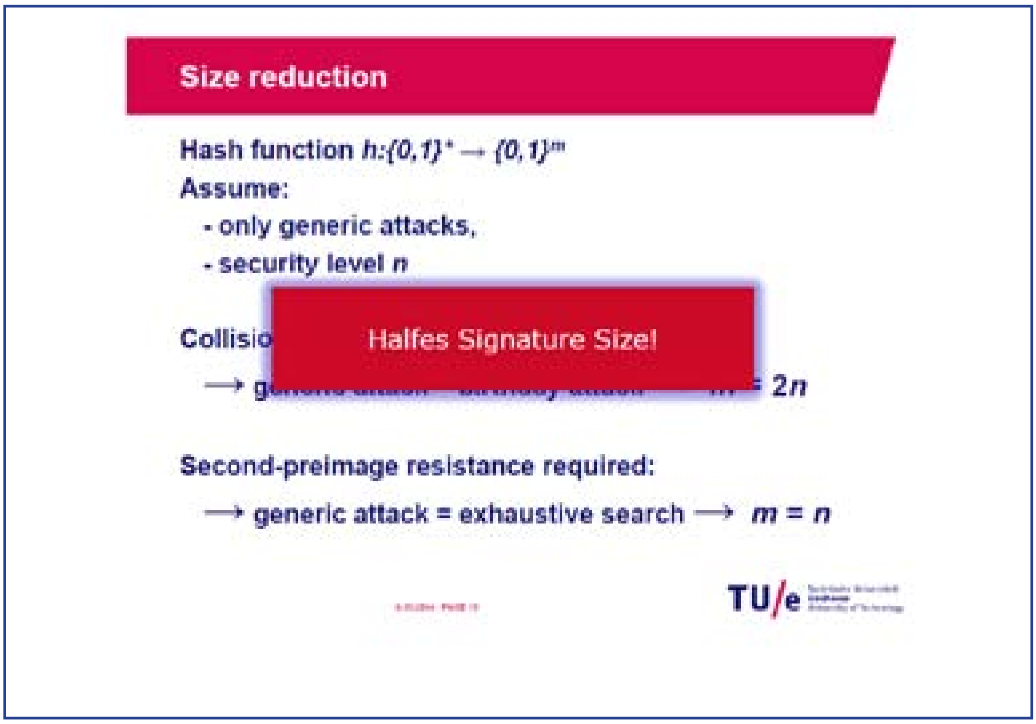
TU/e

ISBN 979-10-92620-04-7

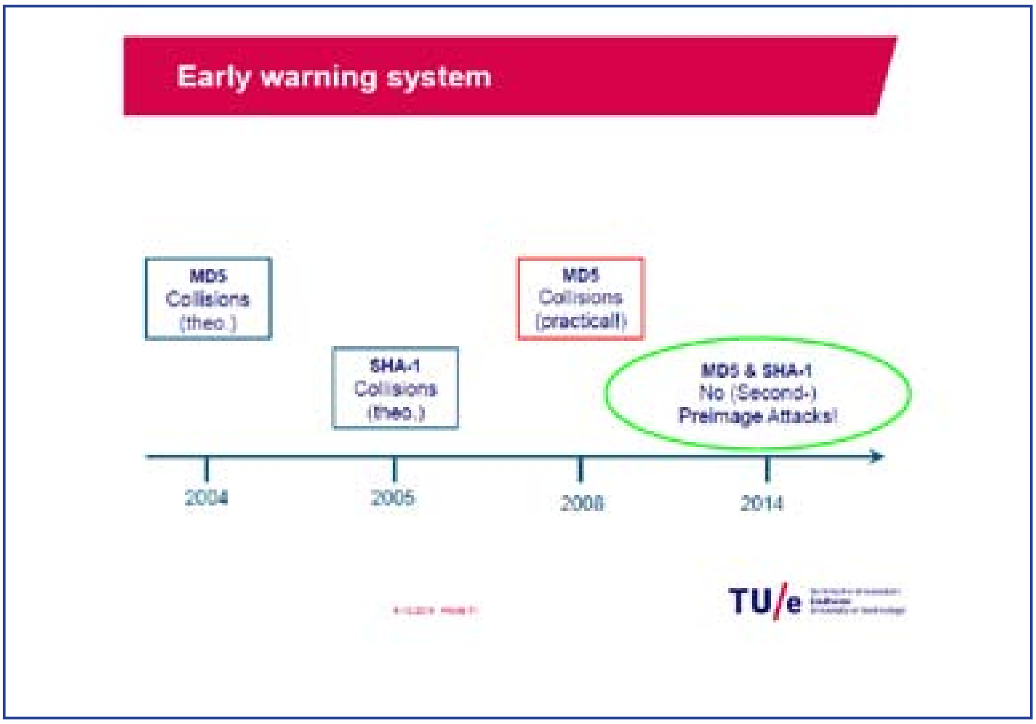


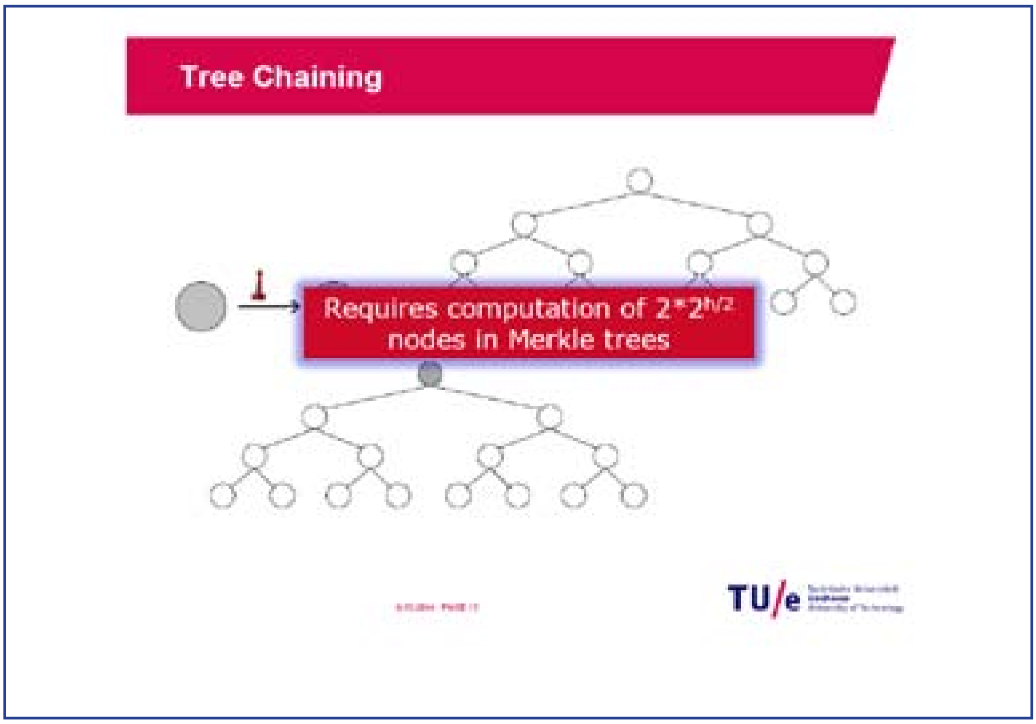
ISBN 979-10-92620-04-7



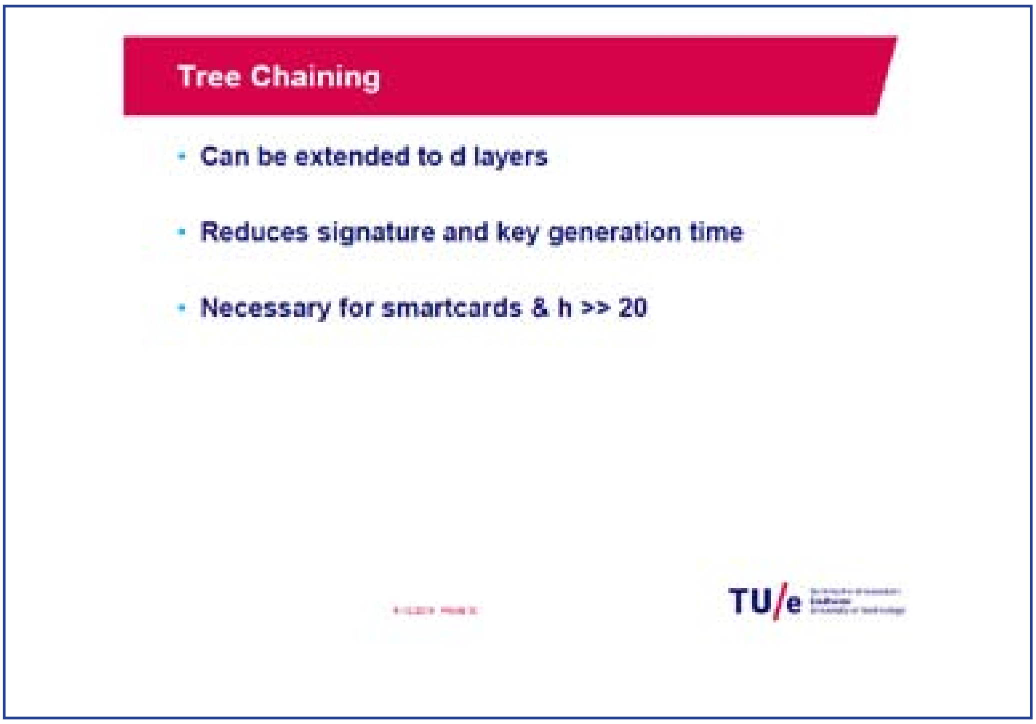


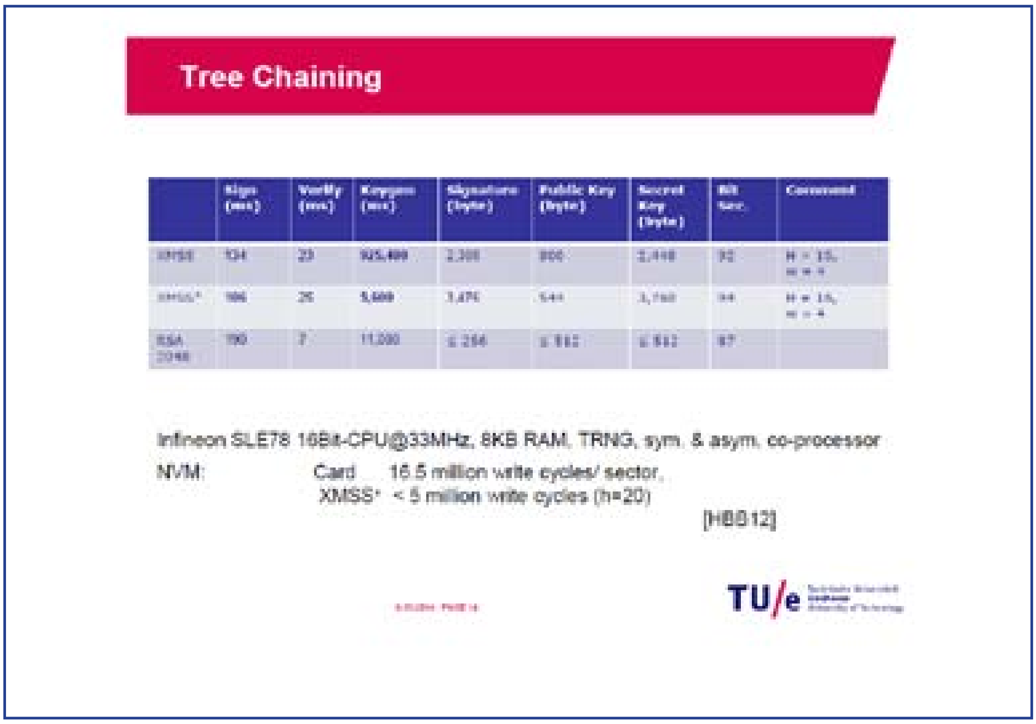
ISBN 979-10-92620-04-7





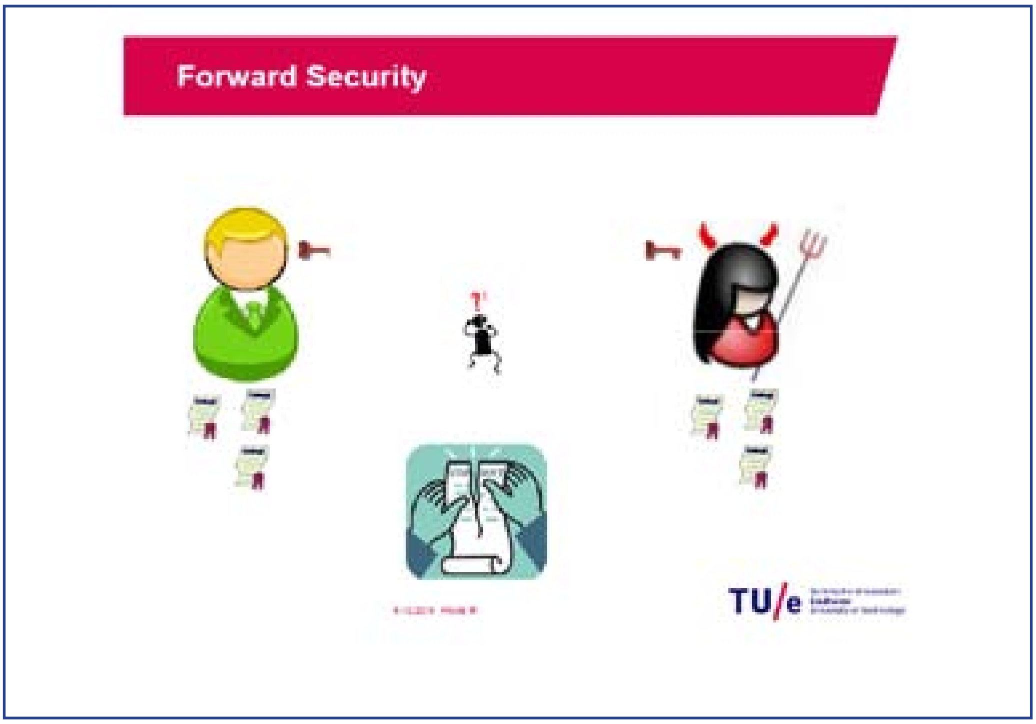
ISBN 979-10-92620-04-7

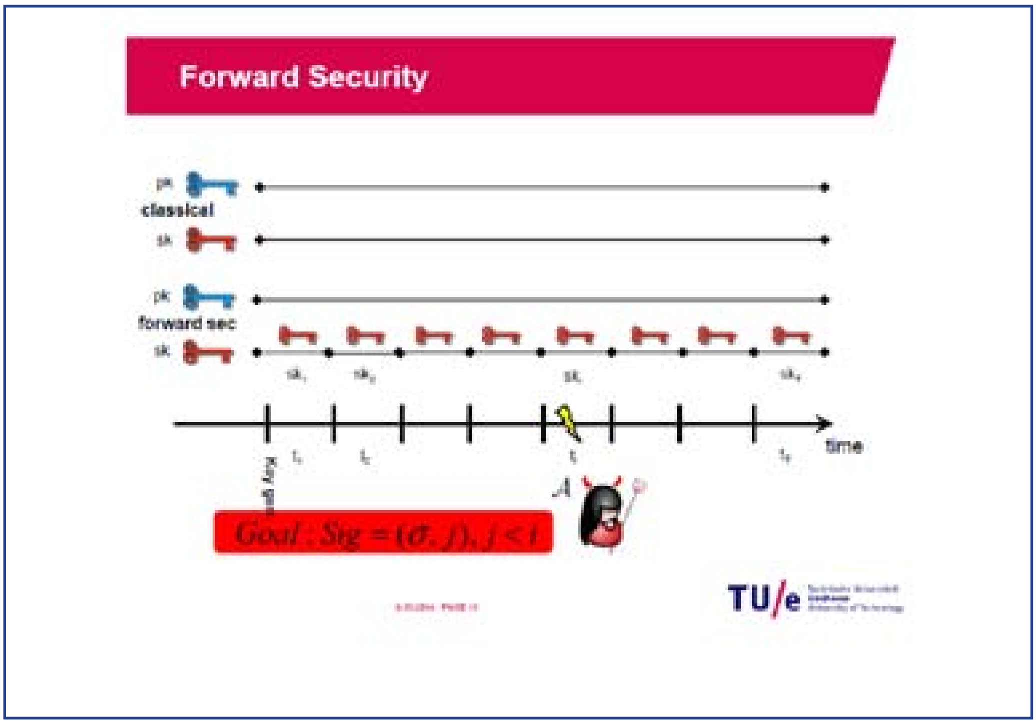

Tree Chaining
Can be extended to d layers
Reduces signature and key generation time
Necessary for smartcards & h >> 20


Tree Chaining

	Sign (ms)	Verify (ms)	Keygen (ms)	Signature (byte)	Public Key (byte)	Secret Key (byte)	Bit Sec.	Comment
XMSS	134	23	925,400	2,388	800	2,448	92	H = 16, w = 4
XMSS+	106	25	5,600	3,476	544	3,760	94	H = 16, w = 4
RSA 2048	190	7	11,000	≤ 256	≤ 512	≤ 512	87	

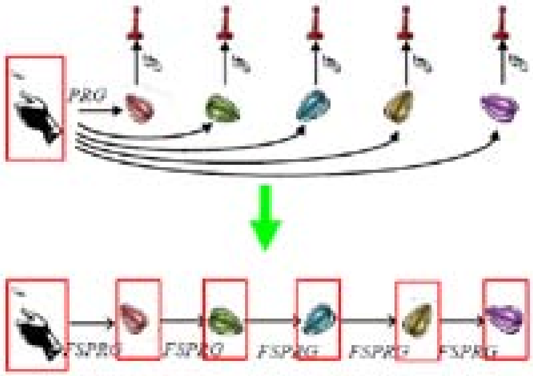
Infineon SLE78 16Bit-CPU@33MHz, 8KB RAM, TRNG, sym. & asym. co-processor
NVM: Card 16.5 million write cycles/ sector,
XMSS+ < 5 million write cycles (h=20)
[HBB12]





ISBN 979-10-92620-04-7

Requires special KeyGen



TU/e

PoC Implementation

C Implementation, using OpenSSL [BDH2011]

	Sign (ms)	Verify (ms)	Signature (bit)	Public Key (bit)	Secret Key (byte)	Bit Security	Comment
XMSS-SHA-2	35.60	1.98	16,672	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
XMSS-AES	1.06	0.11	19,616	7,328	1,684	84	h = 20, w = 4
RSA 2048	3.08	0.09	≤ 2,048	≤ 4,096	≤ 512	87	

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

TU/e

ISBN 979-10-92620-04-7

Conclusion

- Current draft: Great first step

... BUT ...

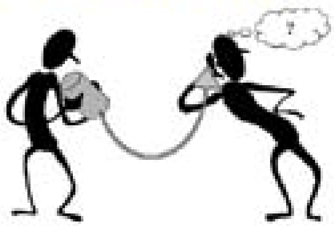
- XMSS: Additional important features
  - More efficient
  - Stronger Security Guarantees
  - Forward-security

Add-on to draft required.

TU/e

Thank you!

Questions?



TU/e

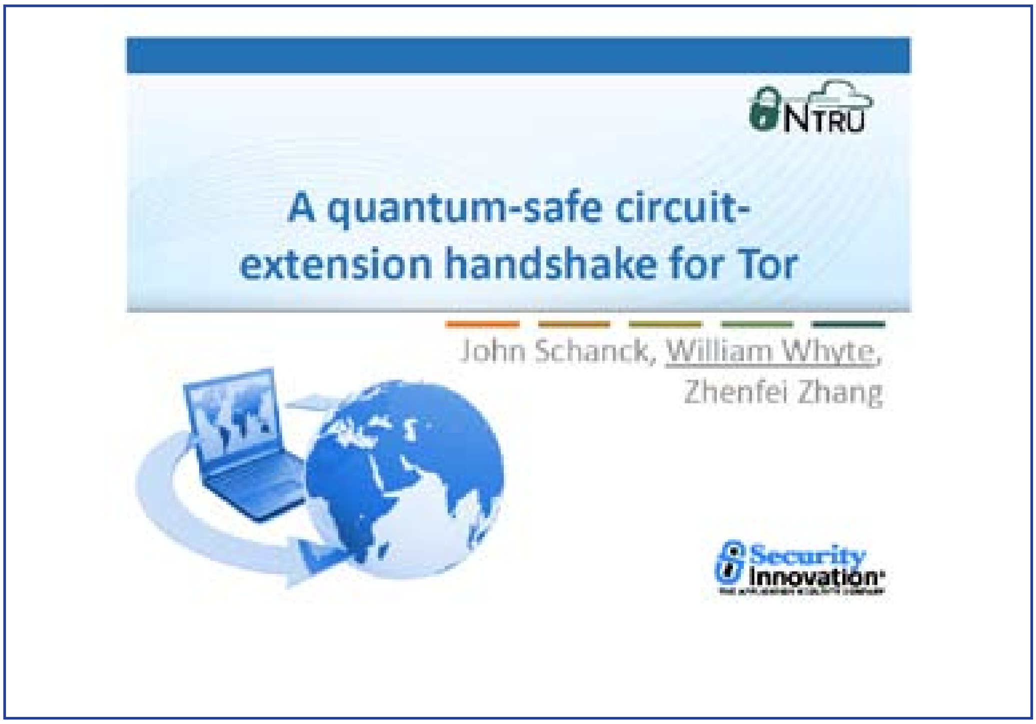
ISBN 979-10-92620-04-7

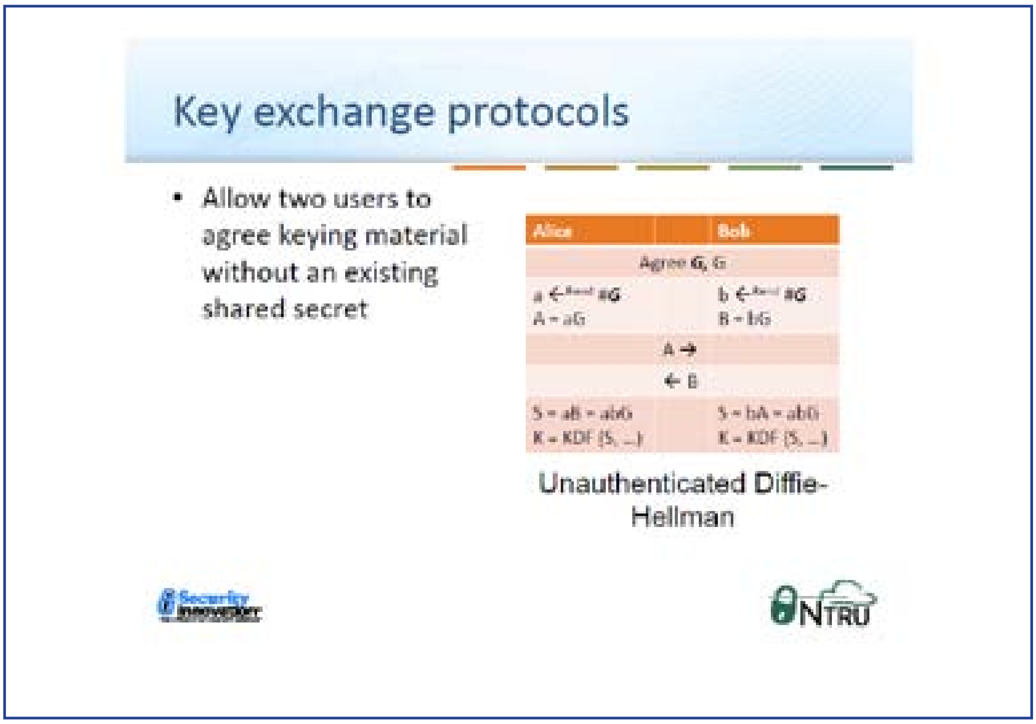
PQTor: Integrating quantum-safe cryptogrgaphy into Tor

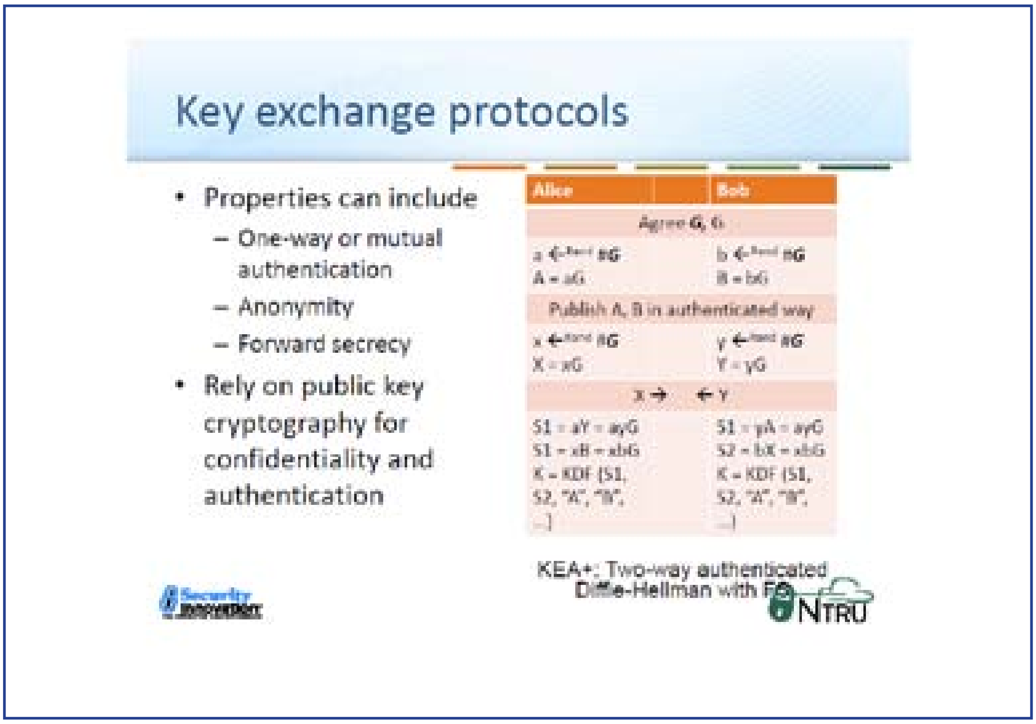
Willian Whyte, Security Innovation

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.







ISBN 979-10-92620-04-7

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

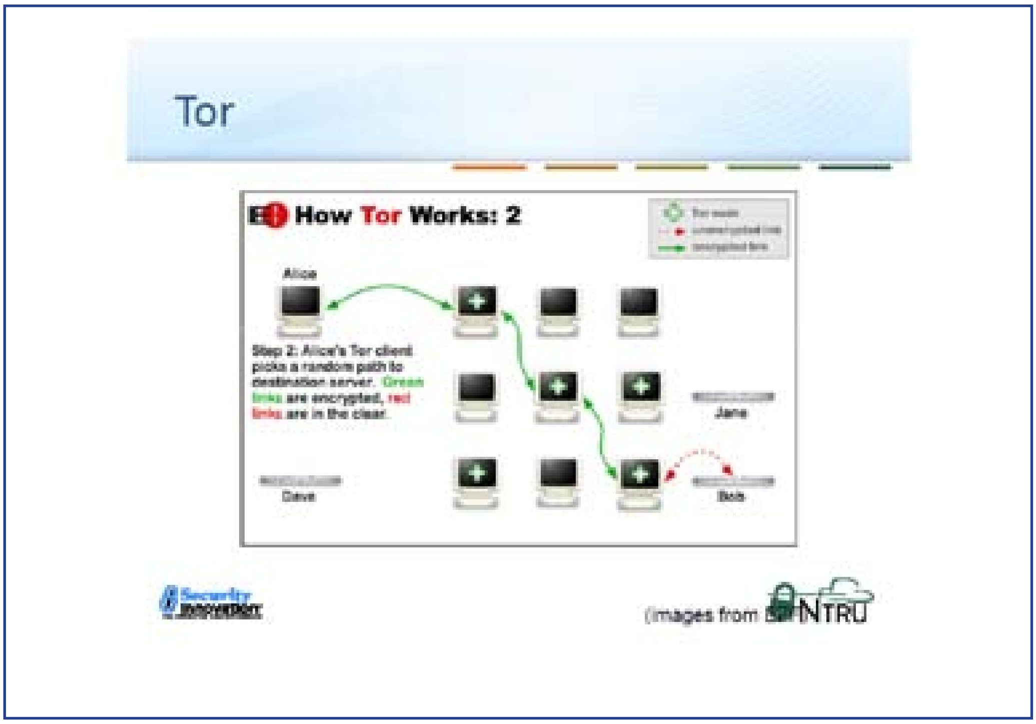
Alice	Bob
Agree *P*	
	(b, B) ←^{Rand} Keygen (*P*)
Publish B in authenticated way	
S ←^{Rand} {1^s} c = Encrypt[B, S]	
c →	
	S = Decrypt (b, c)
K = KDF (S, "B", ...)	K = KDF (S, "B", ...)

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)

ISBN 979-10-92620-04-7



ISBN 979-10-92620-04-7

Tor encryption

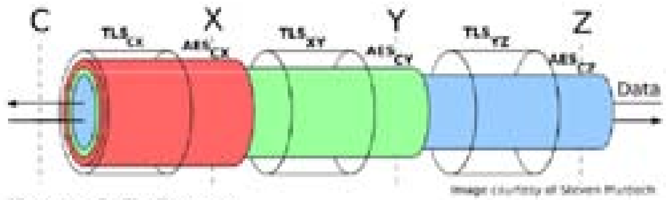


Illustration 2: Tor Encryption

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

ISBN 979-10-92620-04-7

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	
		$b \xleftarrow{rand} \mathbb{G}$ $B = bG$
	Publish B in authenticated way	
$x \xleftarrow{rand} \mathbb{G}$ $X = xG$		$y \xleftarrow{rand} \mathbb{G}$ $Y = yG$
	X →	
		$S1 = yX \mid bX$
	← Y	
$S1 = xY \mid xB$		
	K = KDF (S1, "B", X, Y ...)	

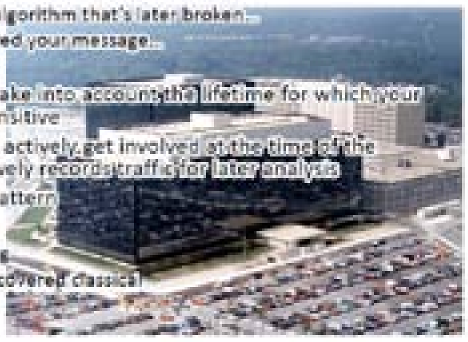
ntor

Security Innovation

NTRU

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



Security Innovation

NTRU

ISBN 979-10-92620-04-7

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

Security Innovation

NTRU

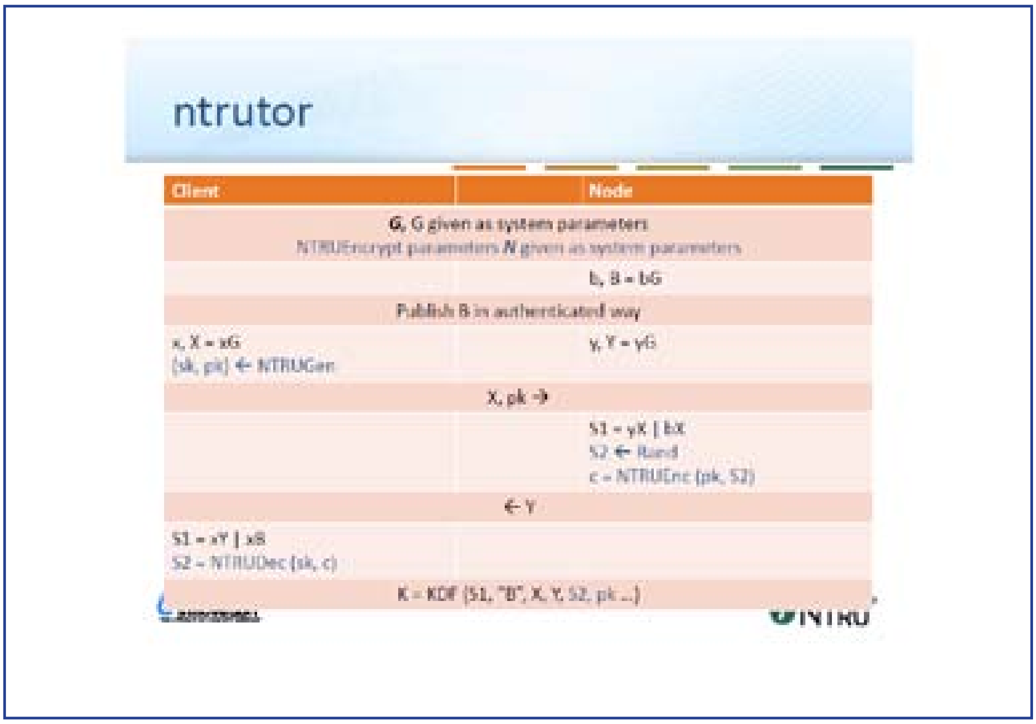
Post-quantum circuit extension: goals

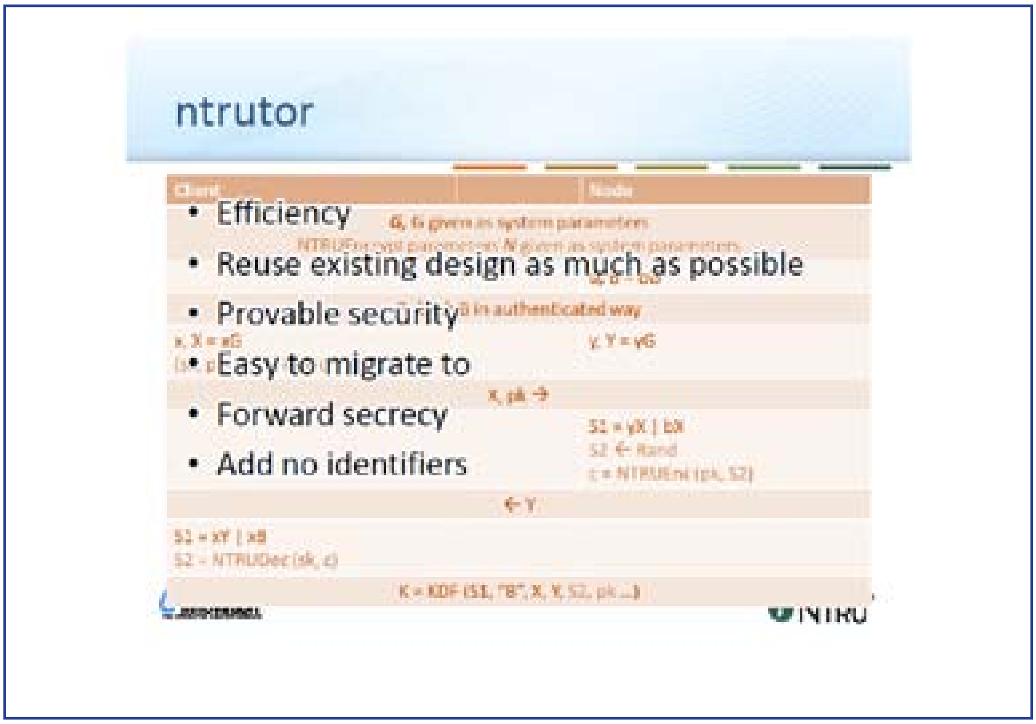
- Efficiency
- Reuse existing design as much as possible
- Provable security
- Easy to migrate to
- Forward secrecy
- Add no identifiers

Security Innovation

NTRU

ISBN 979-10-92620-04-7





ISBN 979-10-92620-04-7

Performance

	TAP	ntor	ntrutor
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

ISBN 979-10-92620-04-7

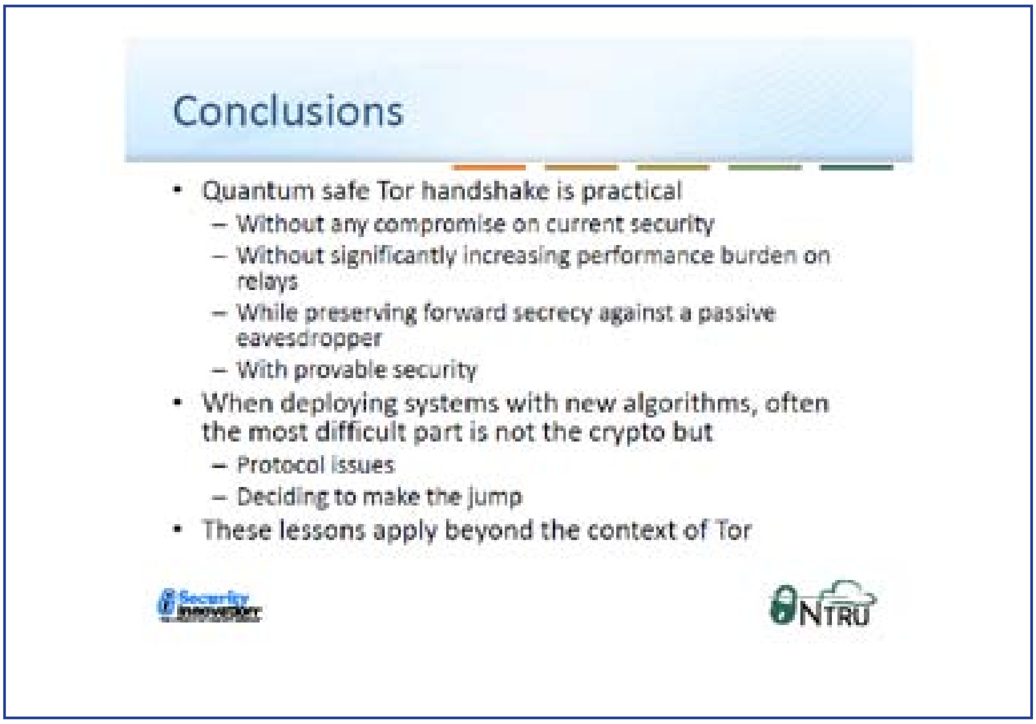
Implementation issues

- 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

ISBN 979-10-92620-04-7



ISBN 979-10-92620-04-7

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

Christopher Chunnilall, 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.

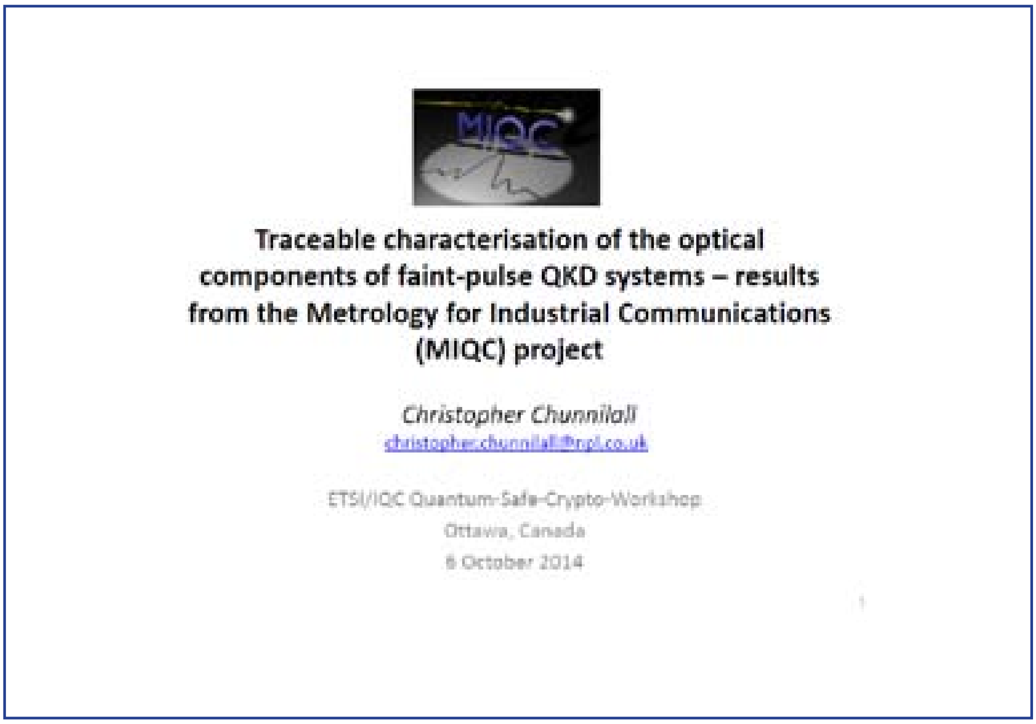
[1] The Metrology for Industrial Quantum Communications (MIQC) project IND06 was funded under the European Metrology Research Programme (EMRP) from September 2011 to August 2014. The partners were: the National Measurement Institutes of the Czech Republic (CMI), Estonia (Metrosert), Finland (MIKES), 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.

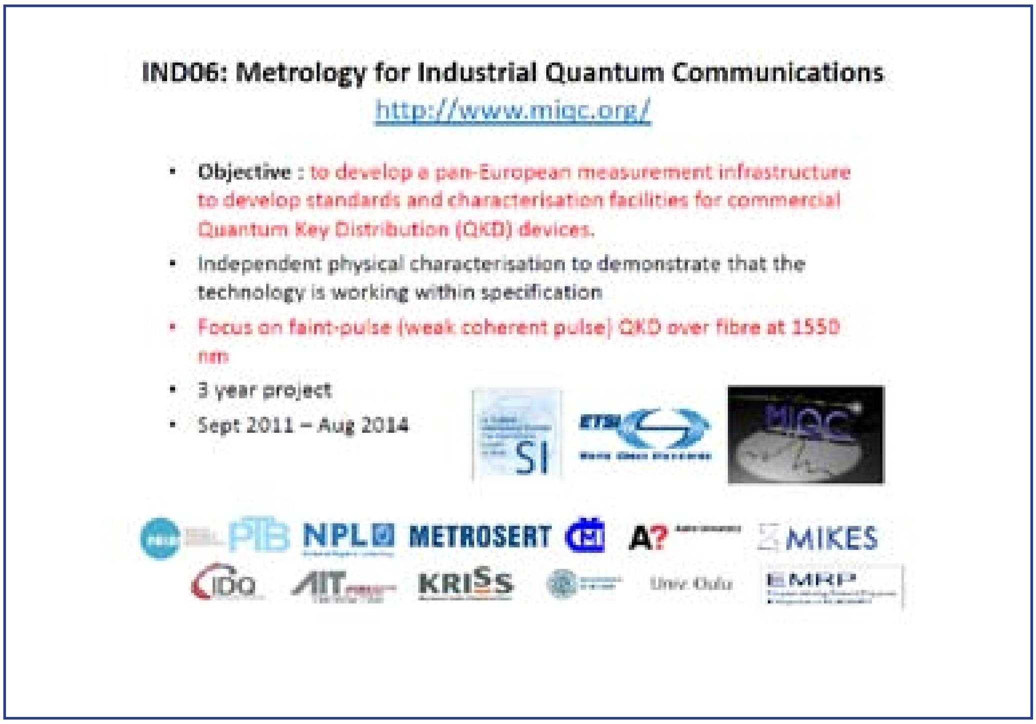
http://projects.npl.co.uk/MIQC/

ISBN 979-10-92620-04-7

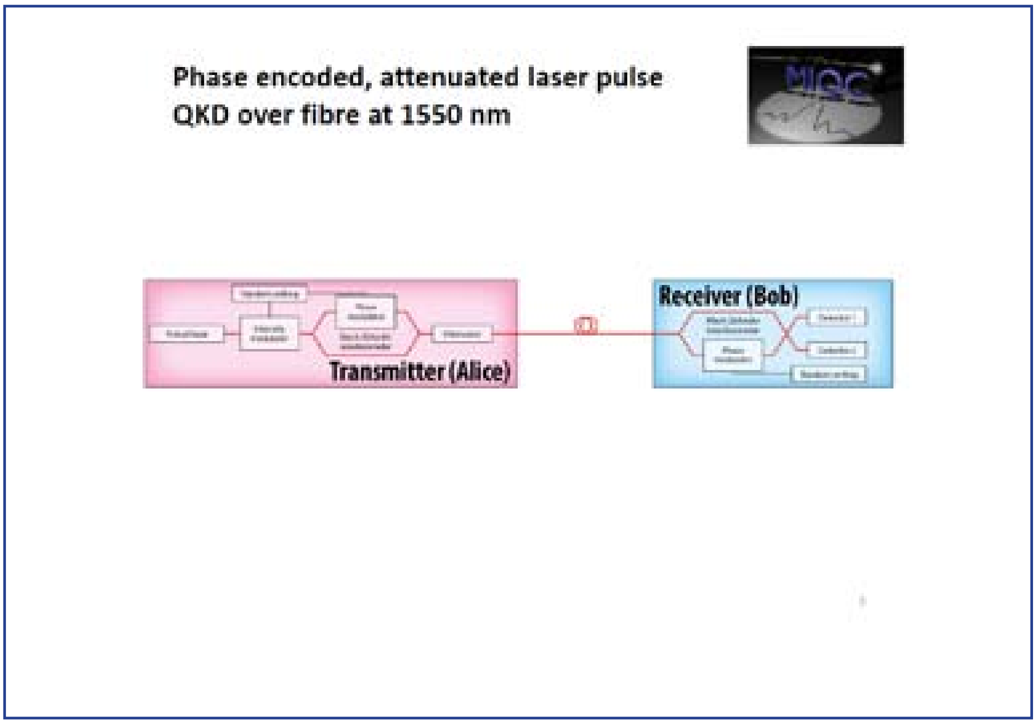
Presentations

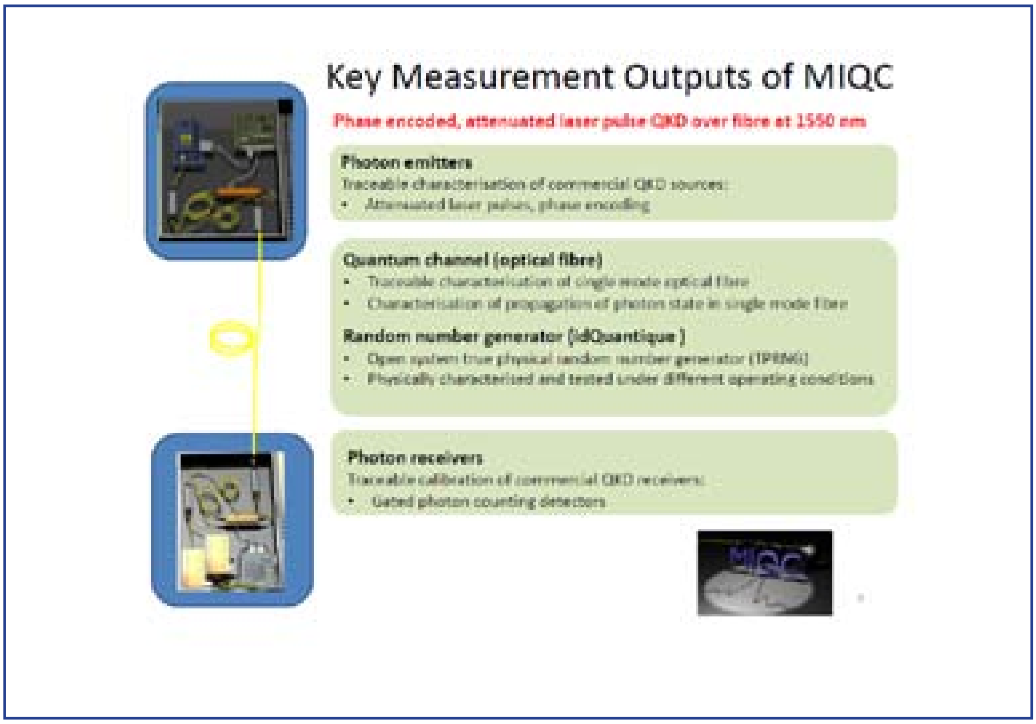
SESSION 4
STANDARDIZATION AND CERTIFICATION



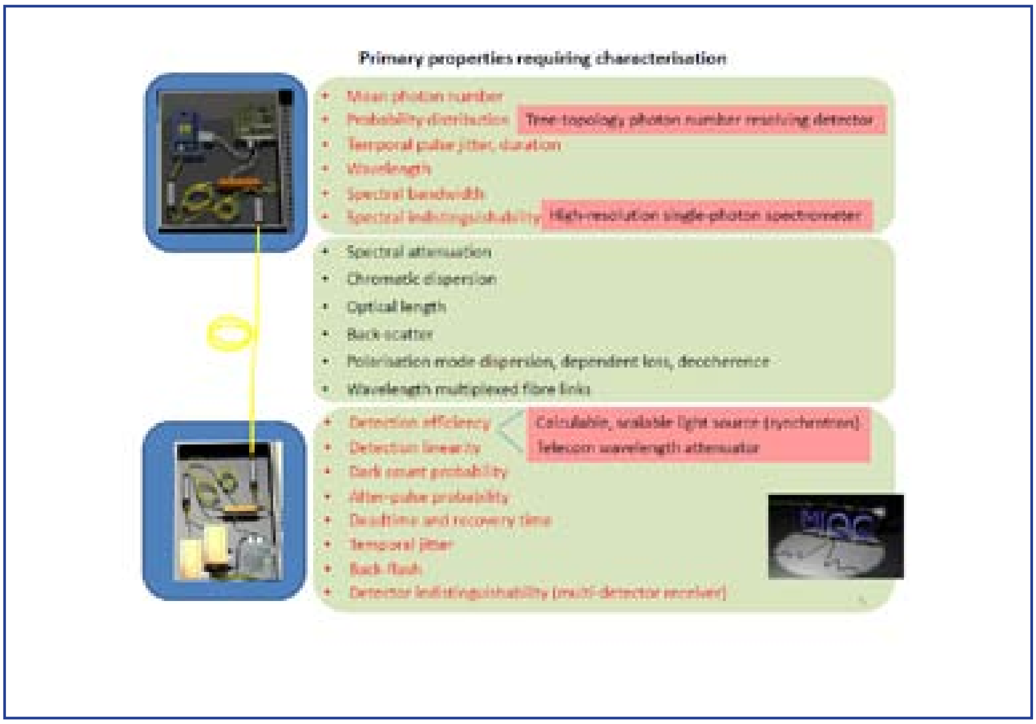


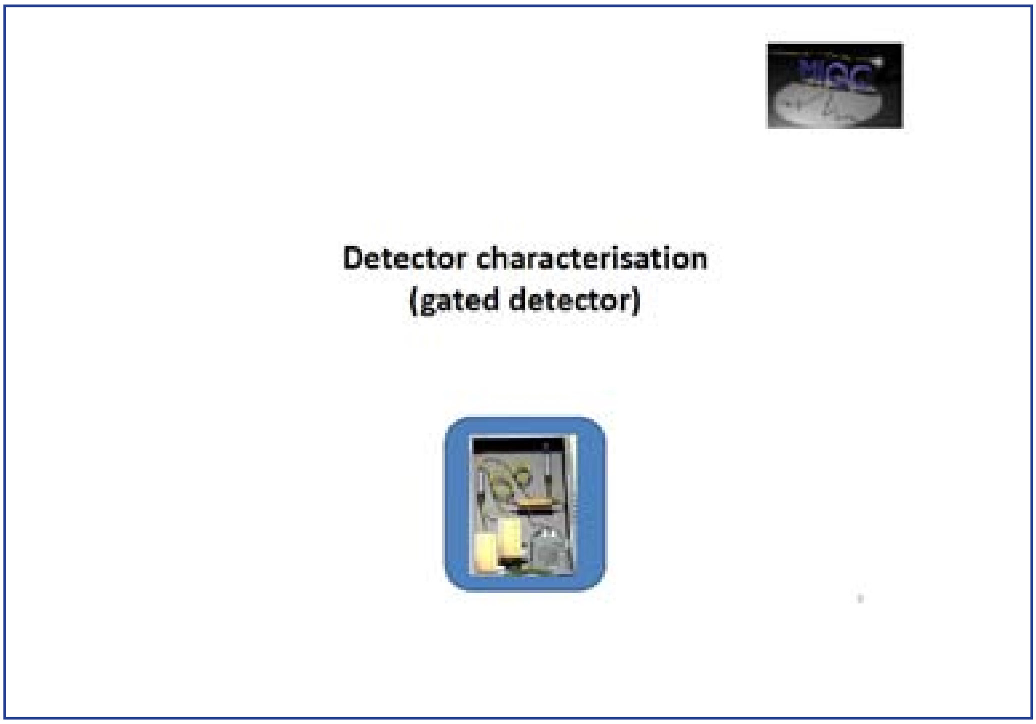
ISBN 979-10-92620-04-7



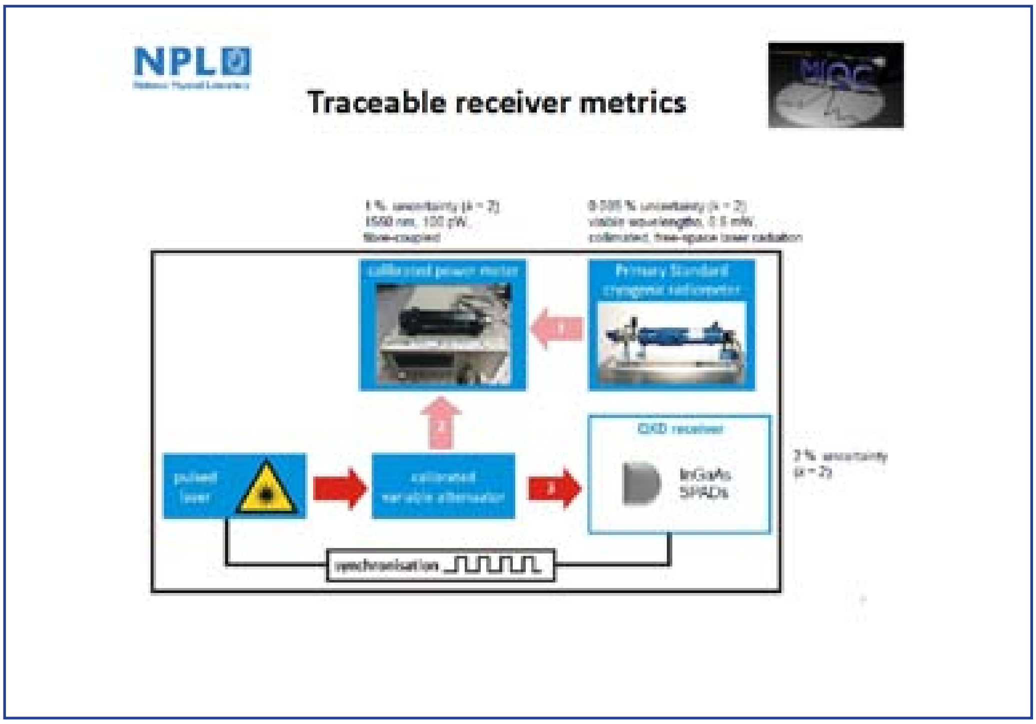


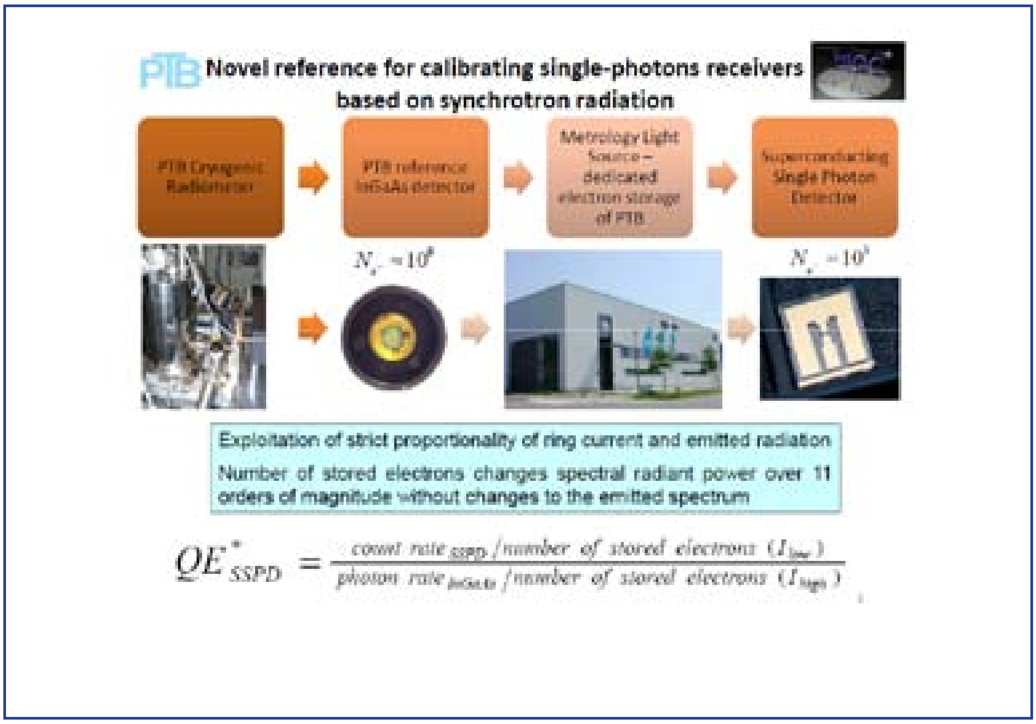
ISBN 979-10-92620-04-7



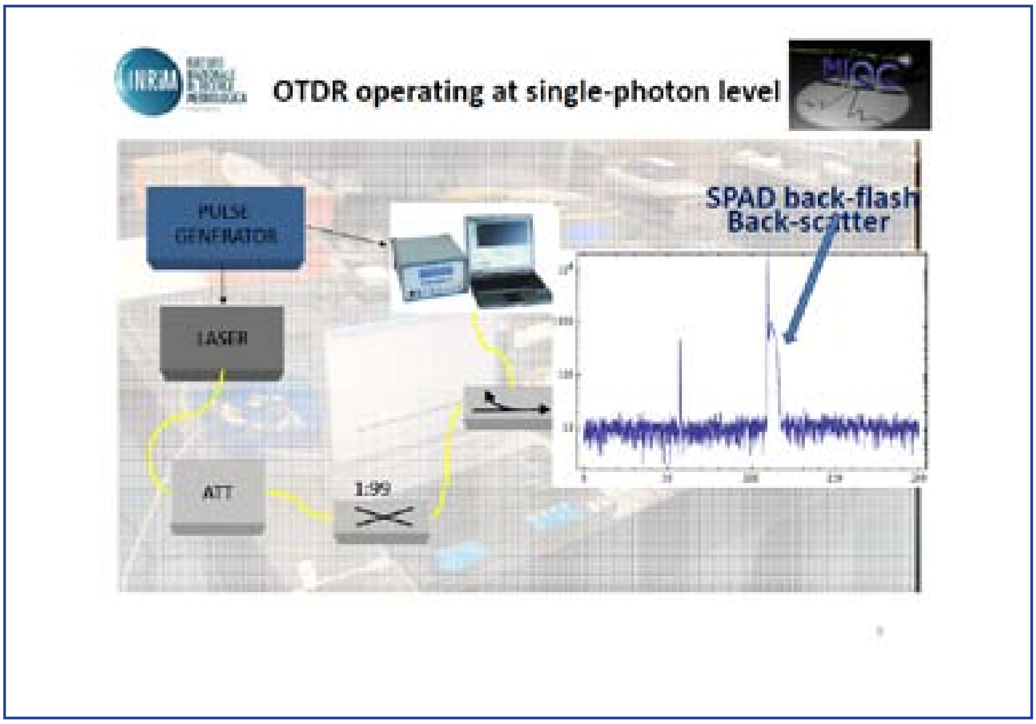


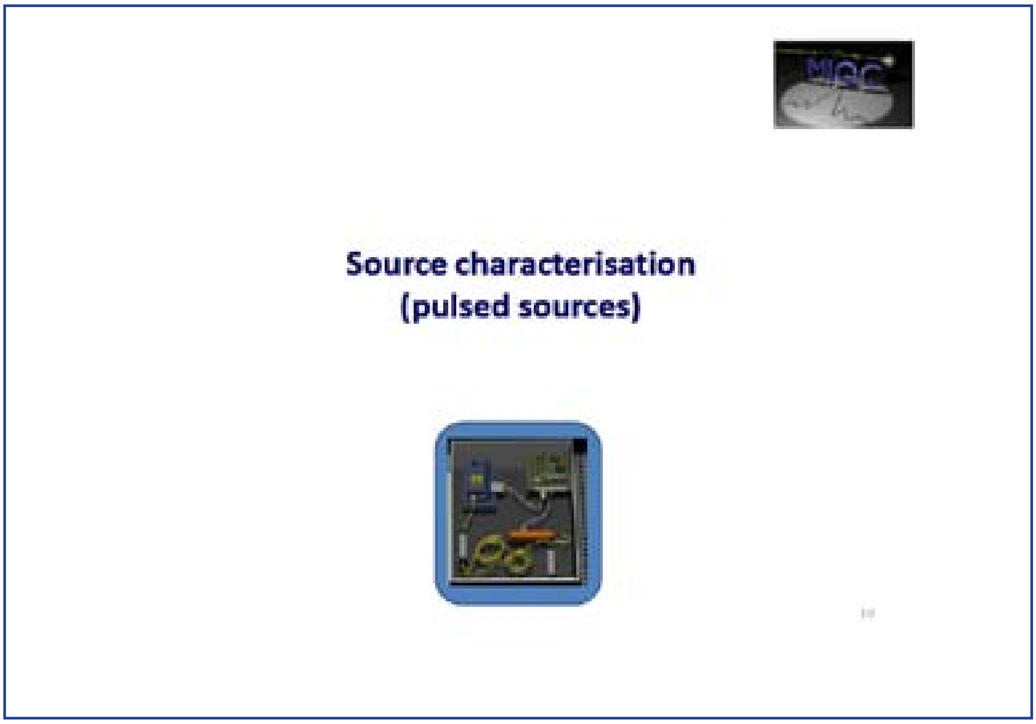
ISBN 979-10-92620-04-7



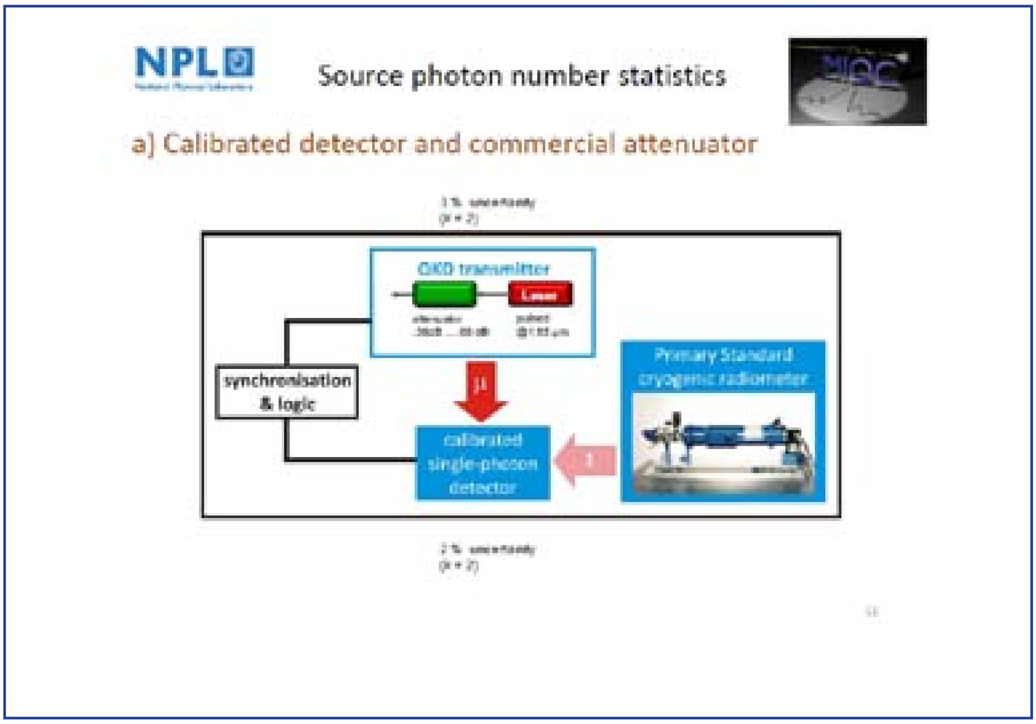


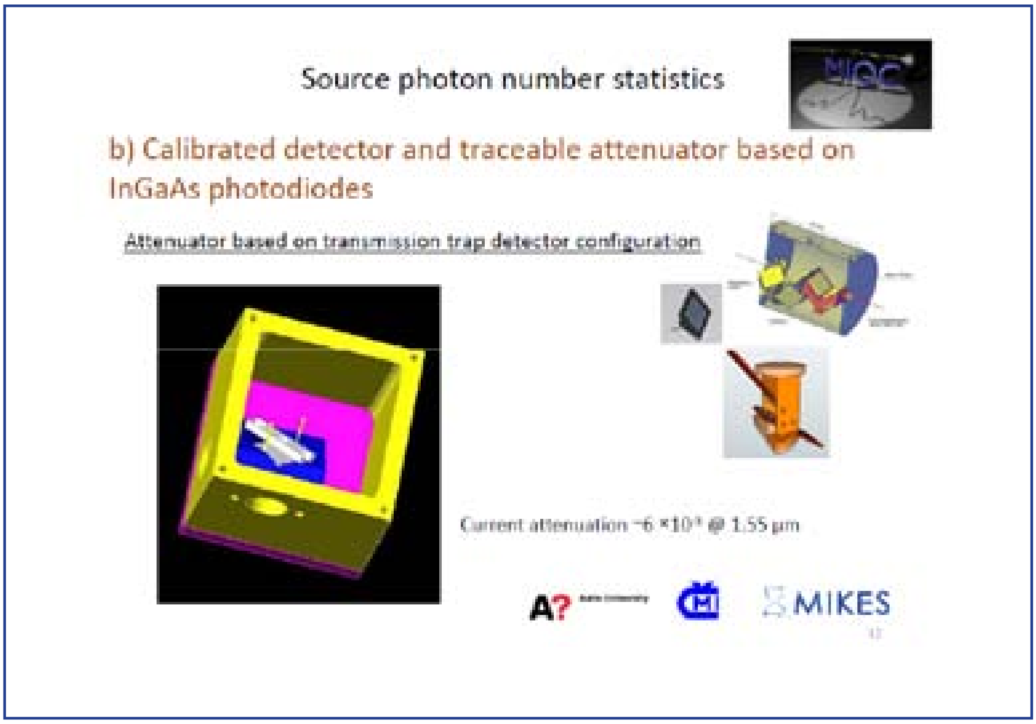
ISBN 979-10-92620-04-7



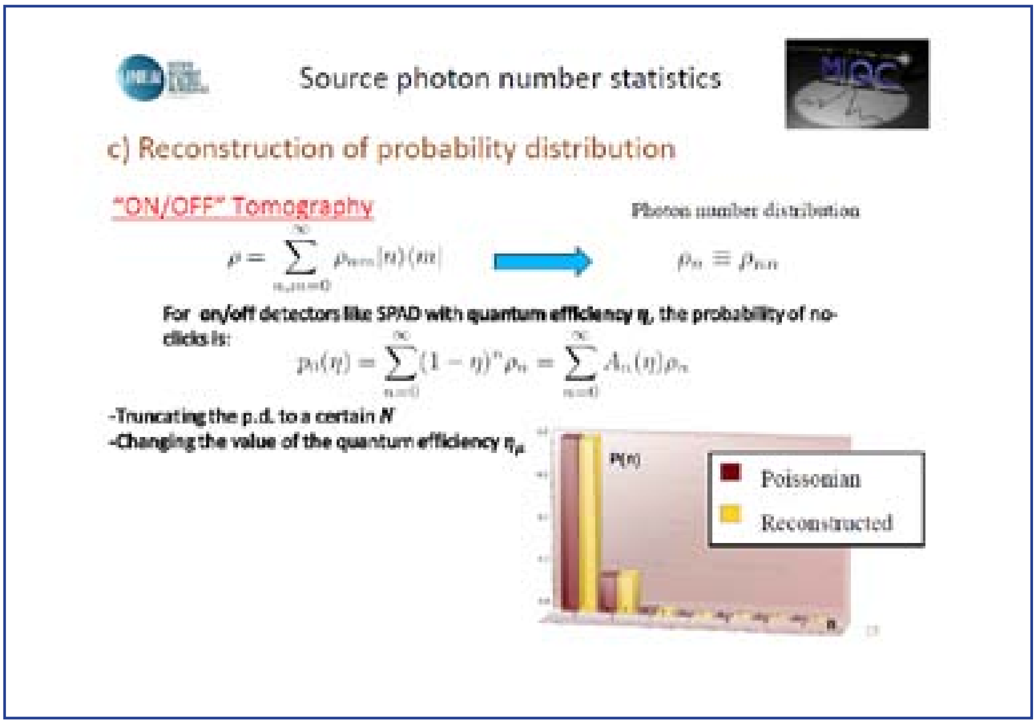


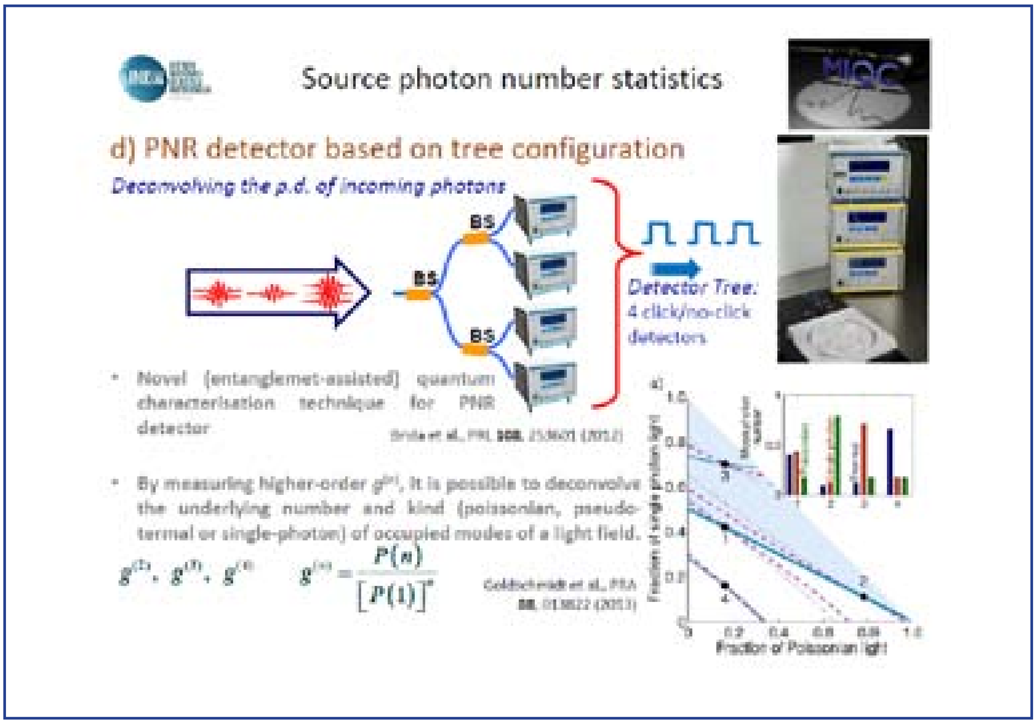
ISBN 979-10-92620-04-7



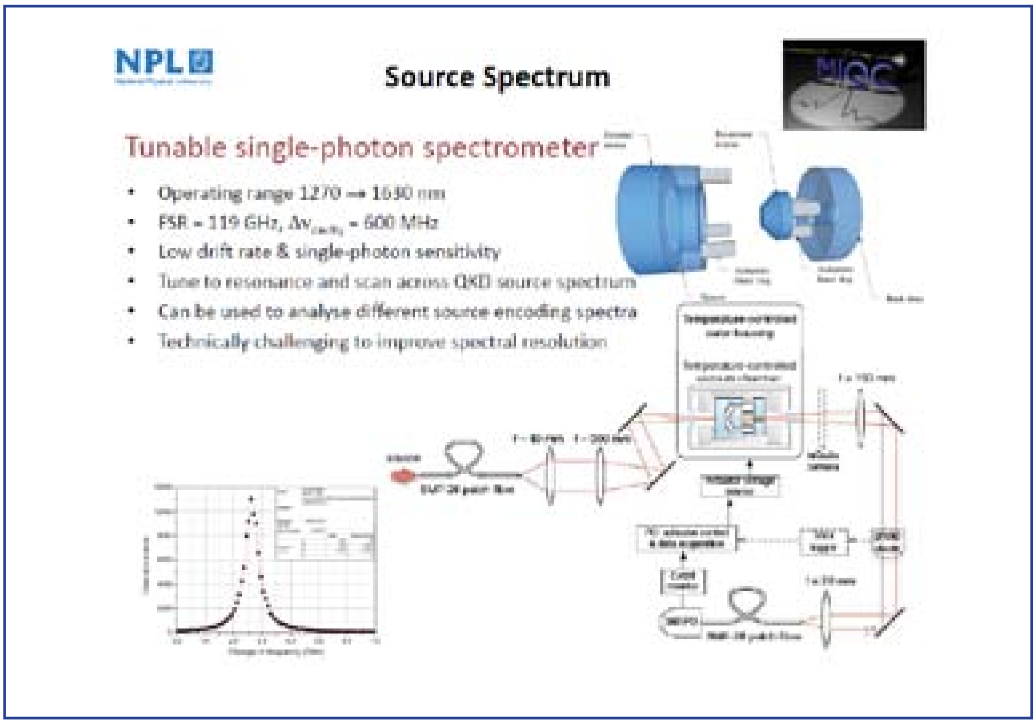


ISBN 979-10-92620-04-7

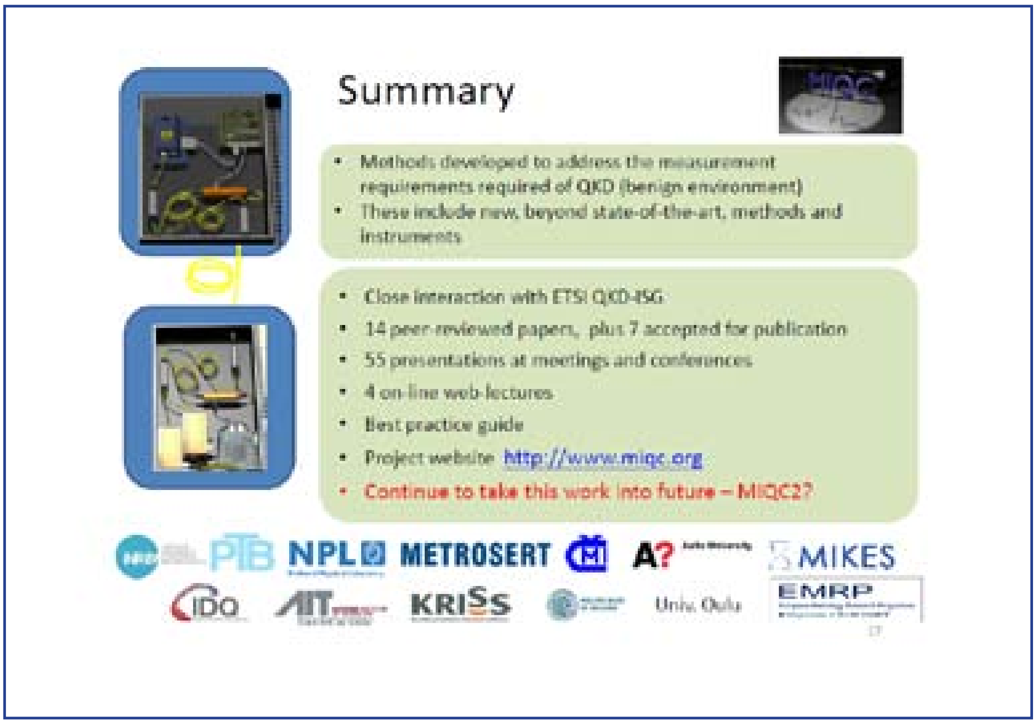


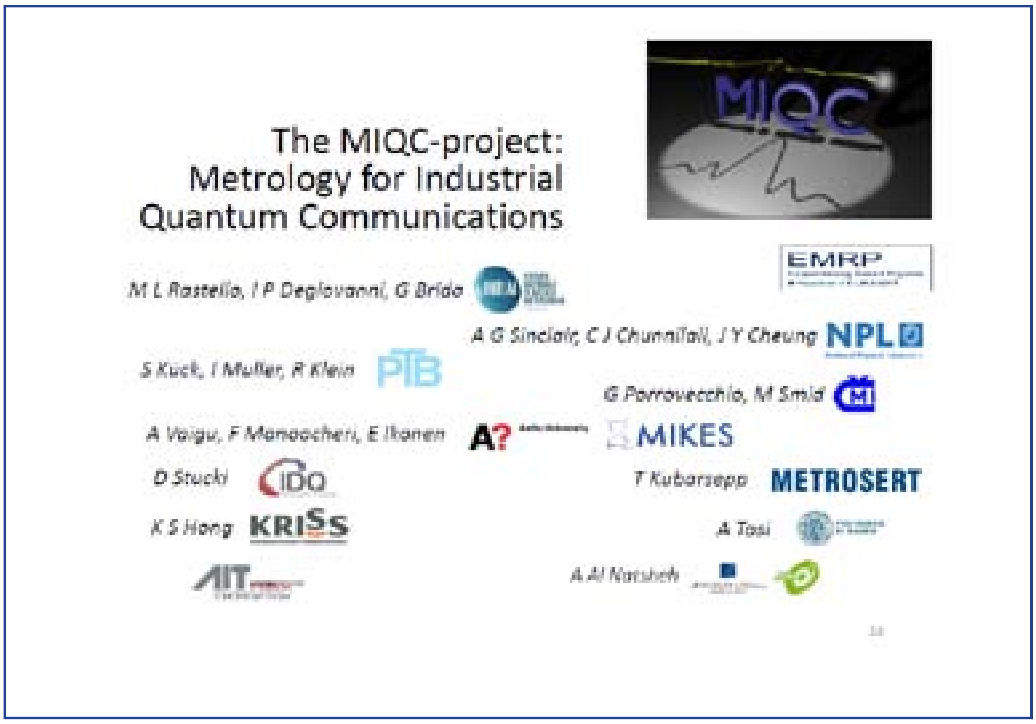


ISBN 979-10-92620-04-7



ISBN 979-10-92620-04-7


Summary
MIQC
• 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-ISG
• 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?
PTB
NPL
METROSERT
MIKES
EMRP
IDQ
KRISS
Univ. Oulu


The MIQC-project:
Metrology for Industrial
Quantum Communications
MIQC
EMRP
M L Rastello, I P Degiovanni, G Brida
A G Sinclair, C J Chunnilall, J Y Cheung
NPL
S Kück, I Muller, R Klein
PTB
G Porrovecchio, M Smid
A Vaigu, F Manoocheri, E Ikonen
MIKES
D Stucki
IDQ
T Kubarsepp
METROSERT
K S Hong
KRISS
A Tosi
A Al Natsheh


Further metrology ... MIQC2?
MIQC
• 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 >>>


MIQC
Thank you!
http://www.miqc.org

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.

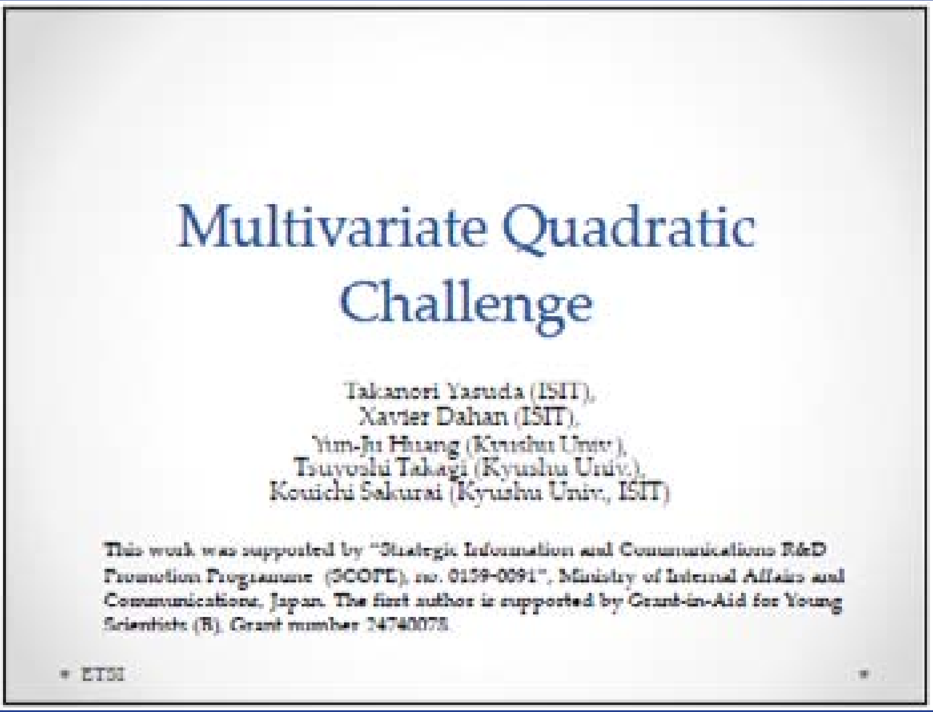
[4] Takanori Yasuda, Kouichi Sakurai, Tsuyoshi Takagi, "Reducing the Key Size of Rainbow using Non-commutative Rings", CT-RSA'12, Springer LNCS vol. 7178, pp. 68–83, 2012.

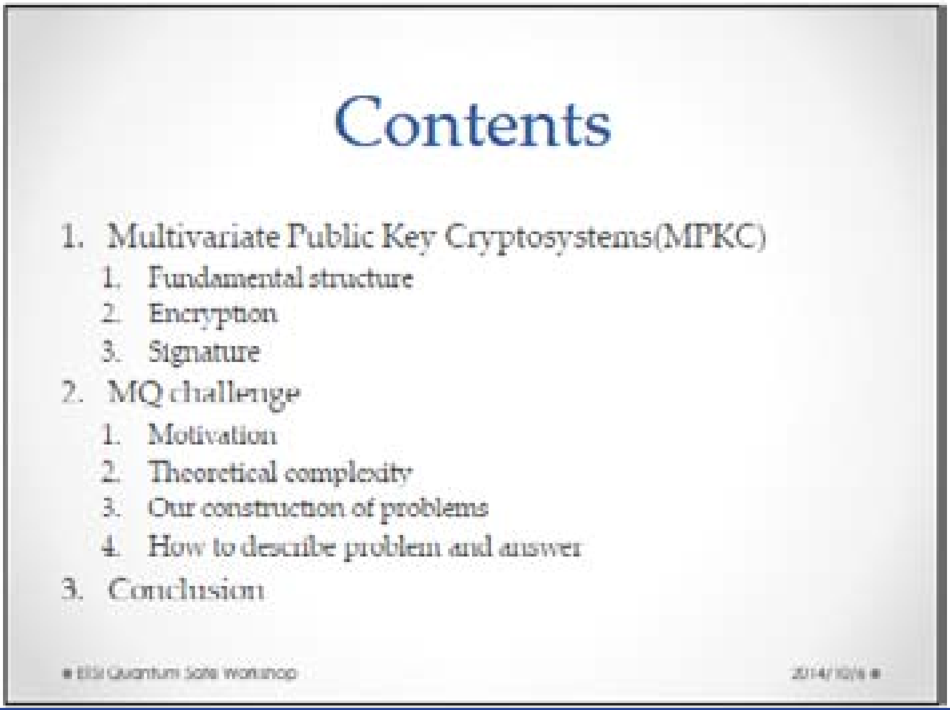
[5] Takanori Yasuda, Tsuyoshi Takagi, Kouichi Sakurai, "Multivariate Signature Scheme Using Quadratic Forms", PQCrypto2013, Springer LNCS vol. 7932, pp. 243-258, 2013.

ISBN 979-10-92620-04-7

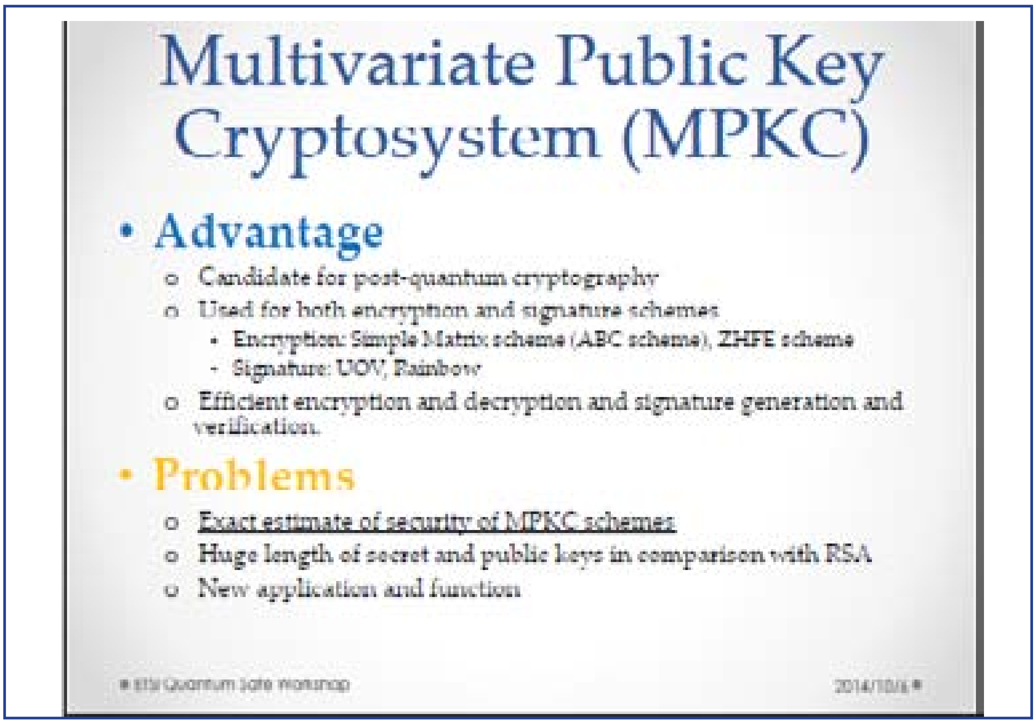
Presentations

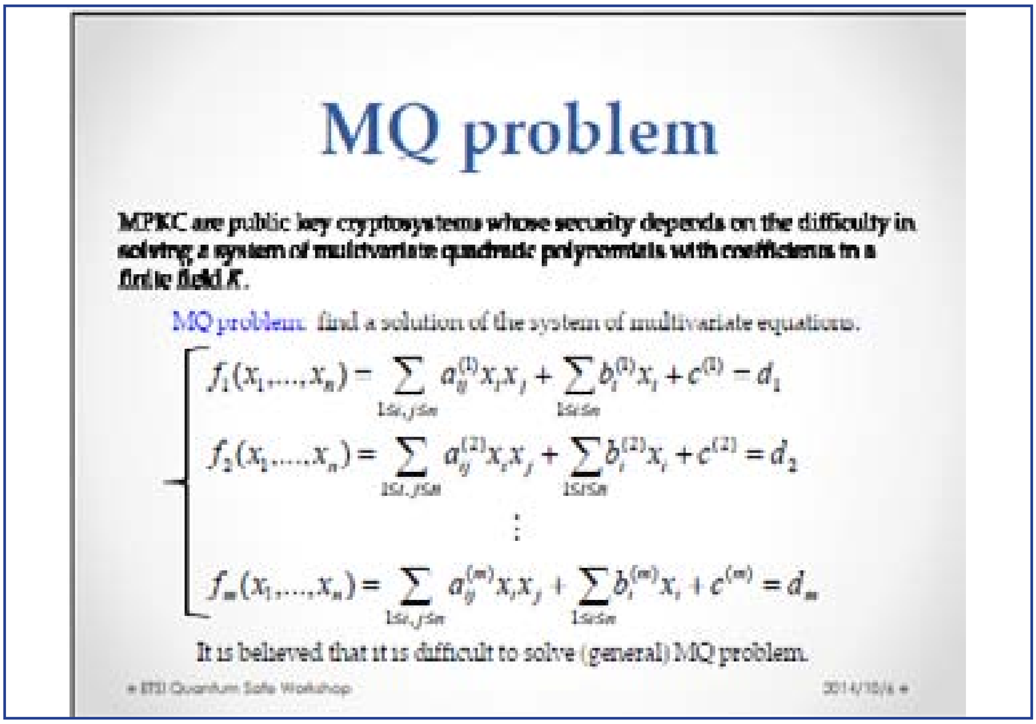
SESSION 4
STANDARDIZATION AND CERTIFICATION



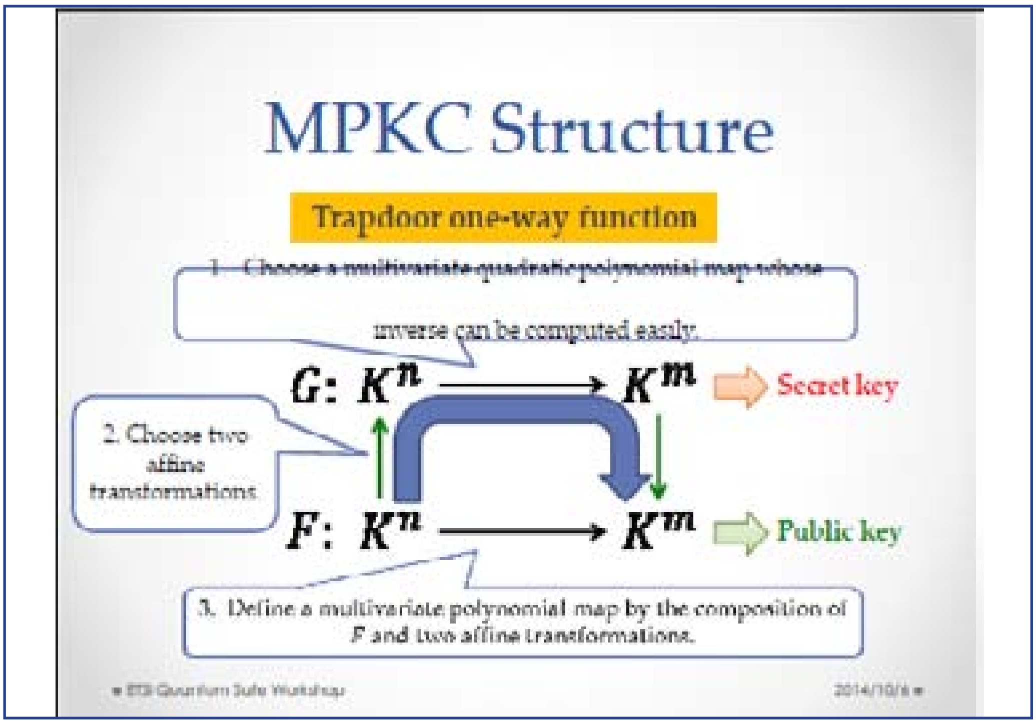


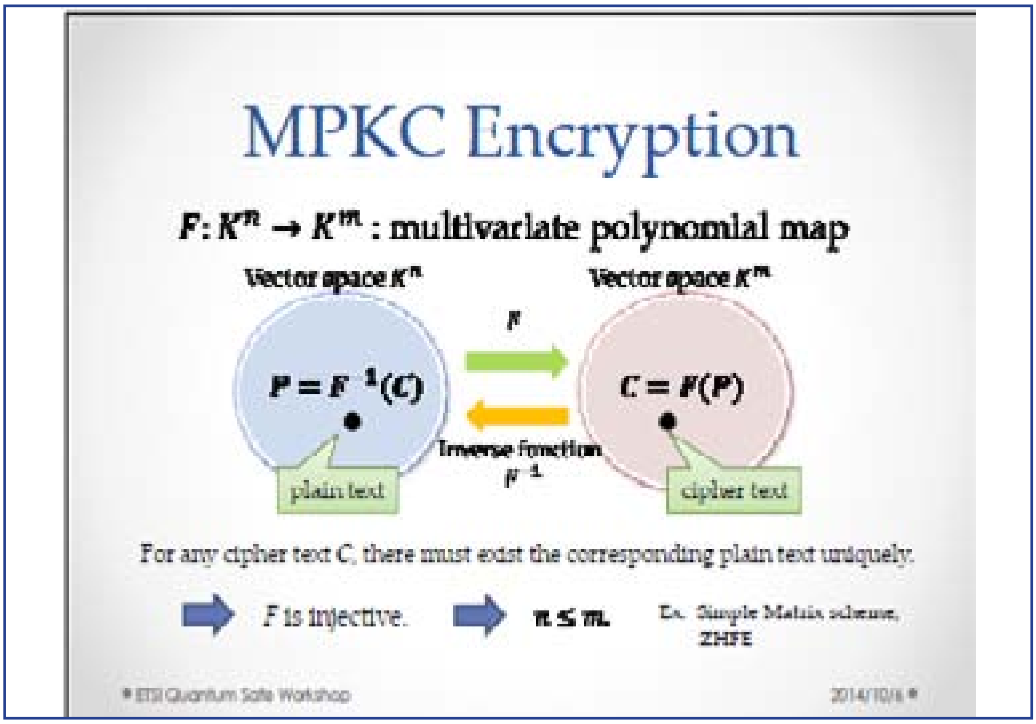
ISBN 979-10-92620-04-7



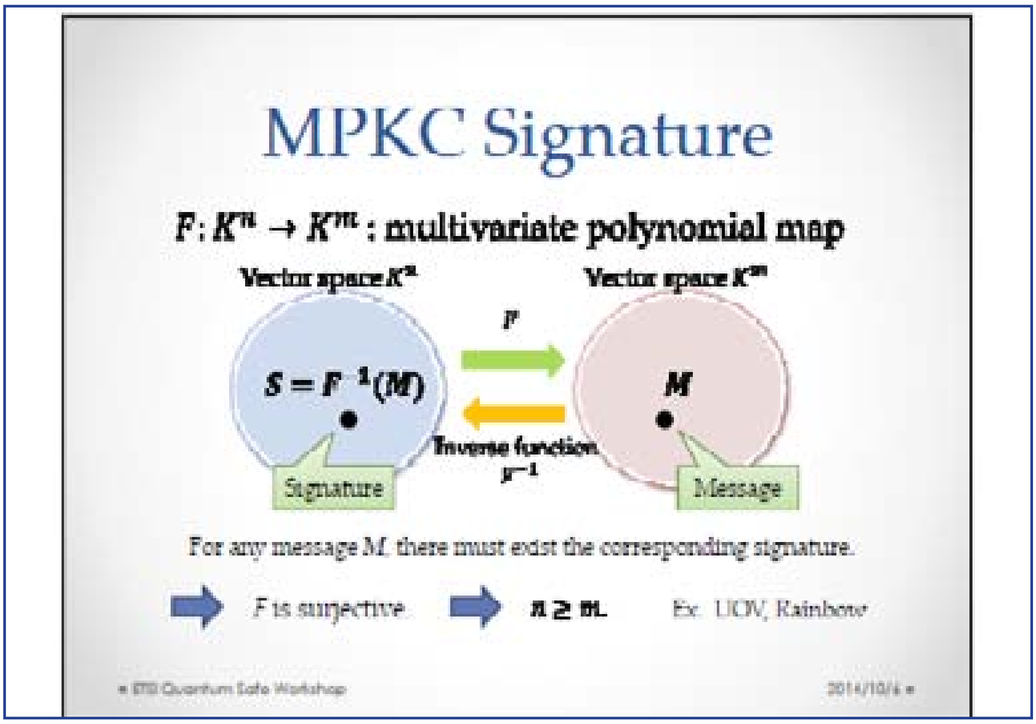


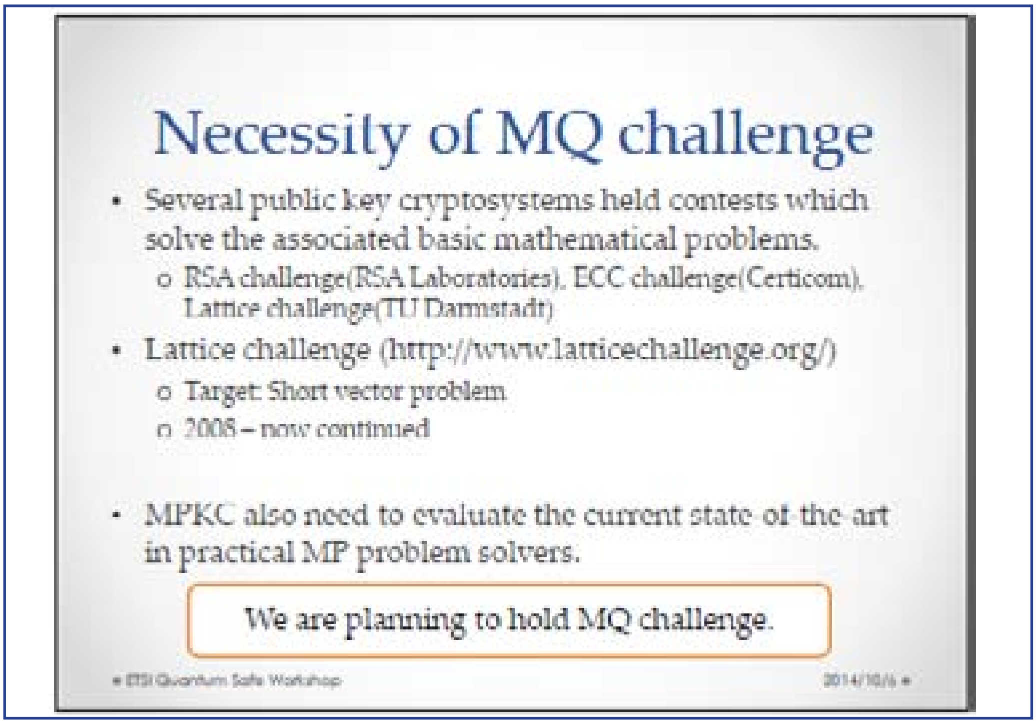
ISBN 979-10-92620-04-7



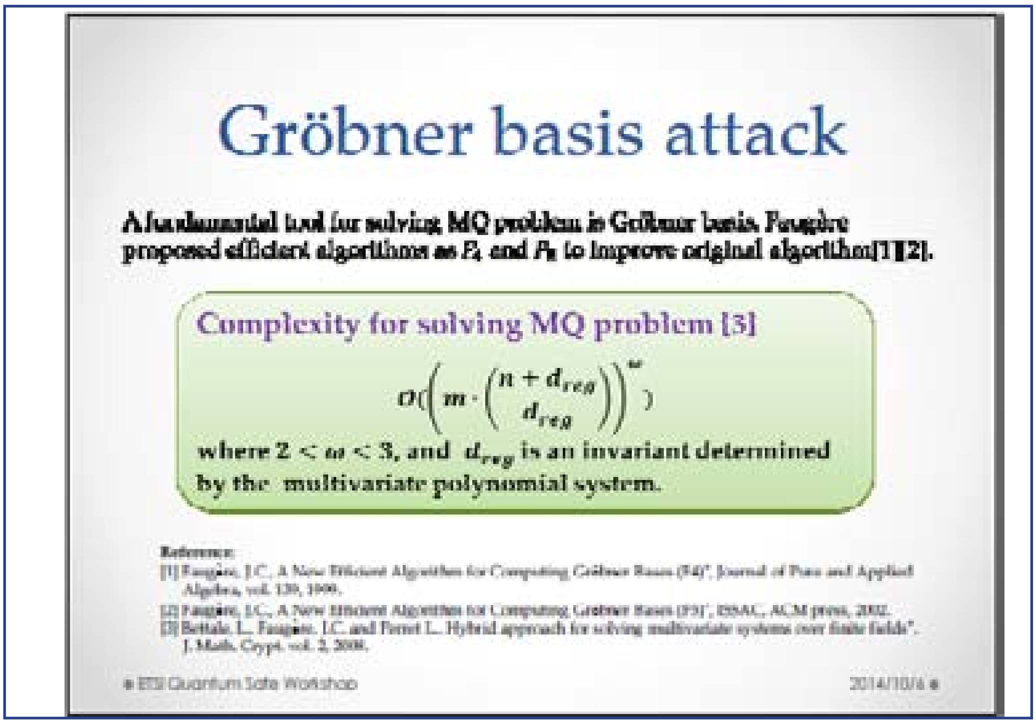


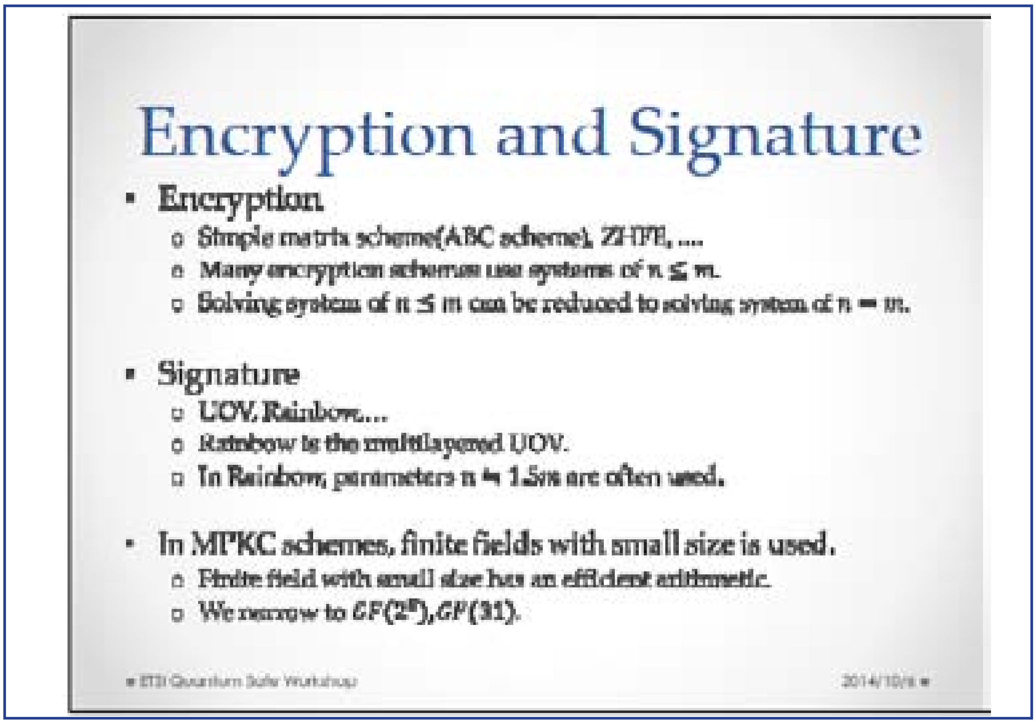
ISBN 979-10-92620-04-7





ISBN 979-10-92620-04-7


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]
$O\left(\left(m \cdot \binom{n+d_{reg}}{d_{reg}}\right)^{\omega}\right)$
where $2 < \omega < 3$, and d_{reg} is an invariant determined by the multivariate polynomial system.
Reference
[1] Faugère, J.C., A New Efficient Algorithm for Computing Gröbner Basis (F4)", Journal of Pure and Applied Algebra, vol. 139, 1999.
[2] Faugère, J.C., A New Efficient Algorithm for Computing Gröbner Basis (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 $n \fallingdotseq 1.5m$ 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 and m and n	Base field	Target
I	$n = m$	$GF(2^8)$	encryption
II	$n = m$	$GF(31)$	encryption
III	$n = 1.5m$	$GF(2^8)$	signature
IV	$n = 1.5m$	$GF(31)$	signature

ETSI Quantum Safe Workshop 2014/10/6

Our construction of MQ problem

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

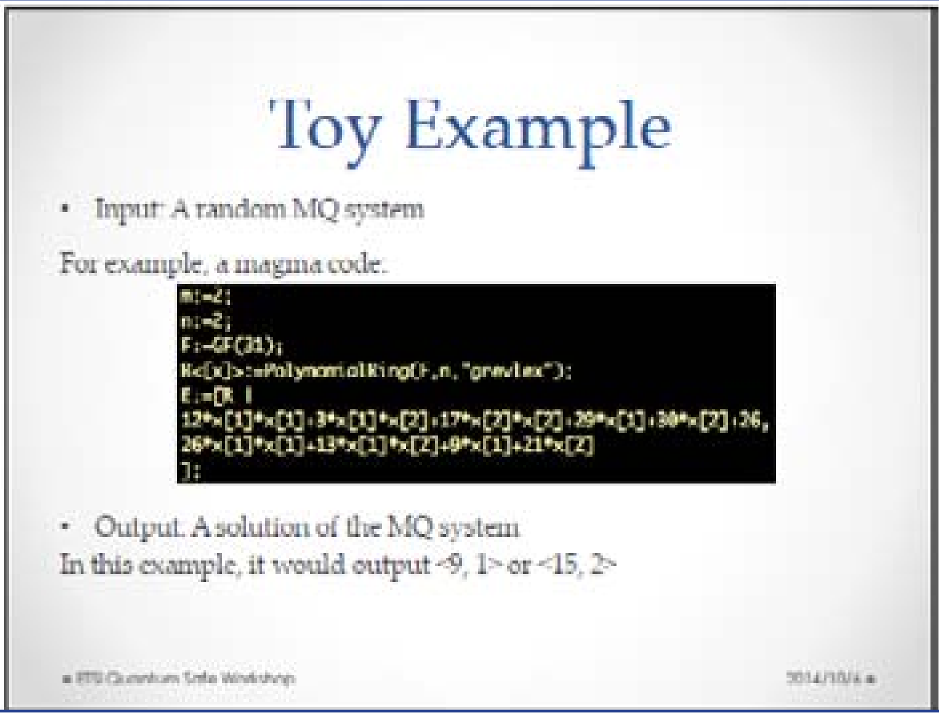
Step 1: choose randomly quadratic coefficients, and linear coefficients .

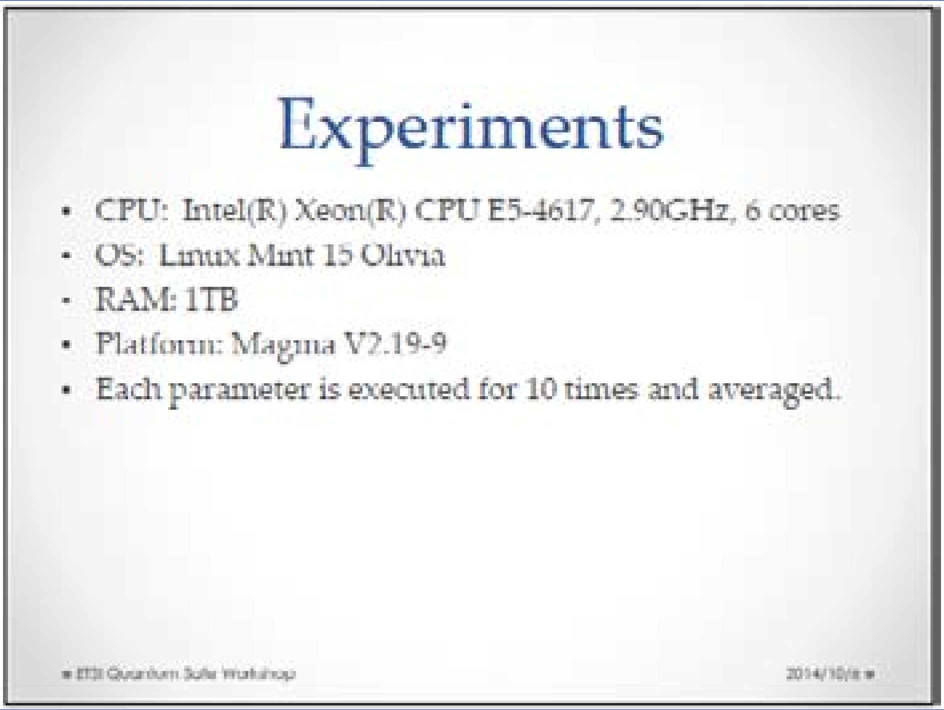
Step 2: choose randomly a solution.

Step 3: compute constant coefficients such that the corresponding MQ problem has at least one solution.

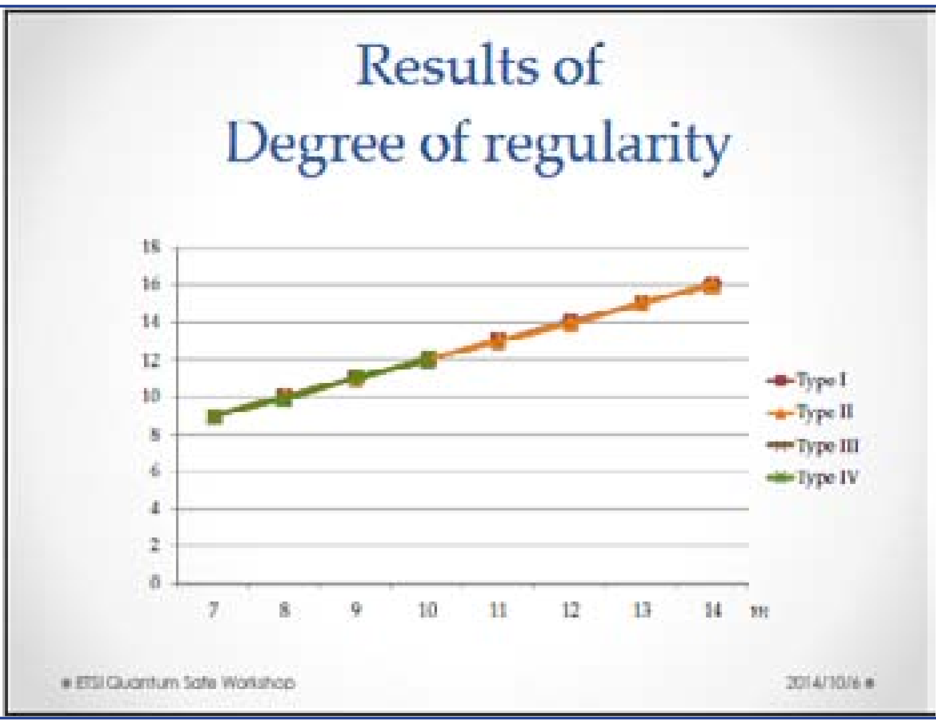
ETSI Quantum Safe Workshop 2014/10/6

ISBN 979-10-92620-04-7



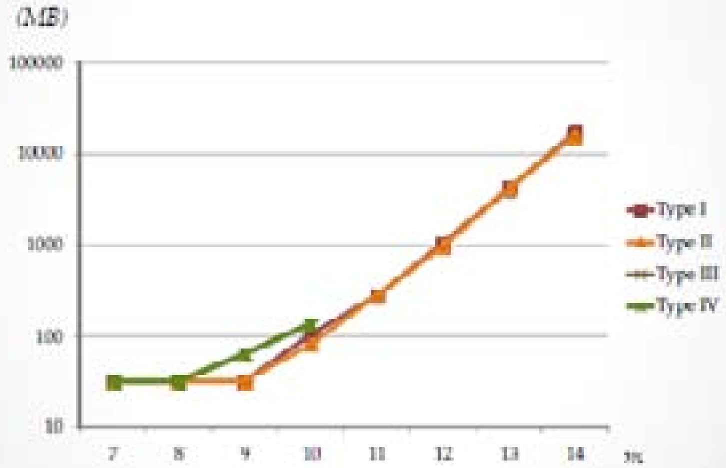


ISBN 979-10-92620-04-7



ISBN 979-10-92620-04-7

Results of Memory



Conclusion

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

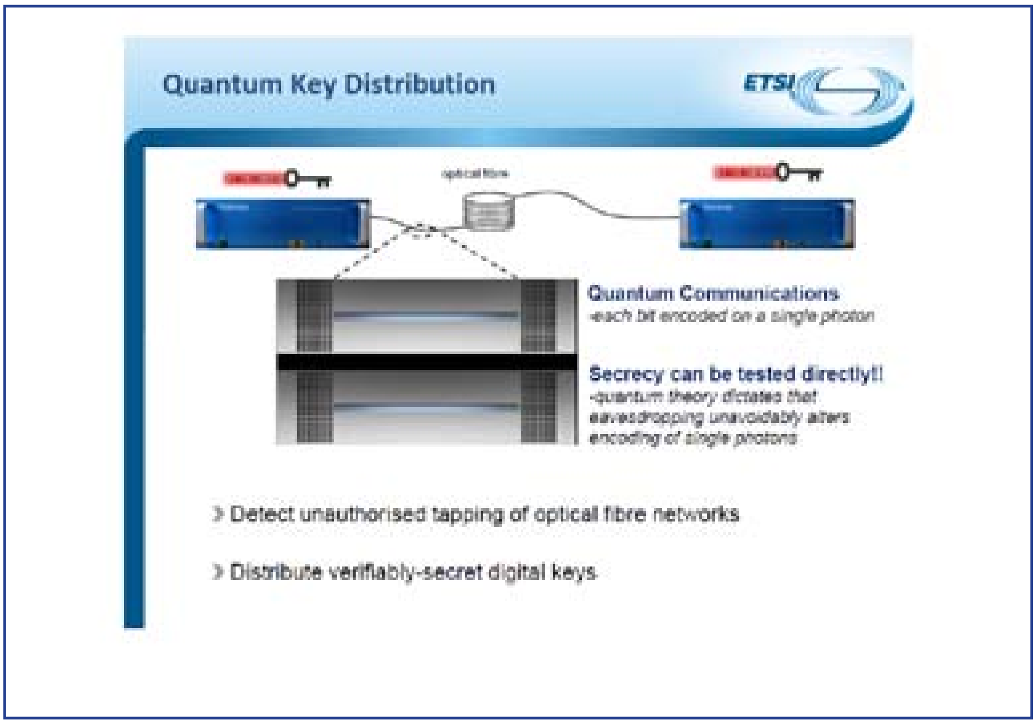
ISBN 979-10-92620-04-7

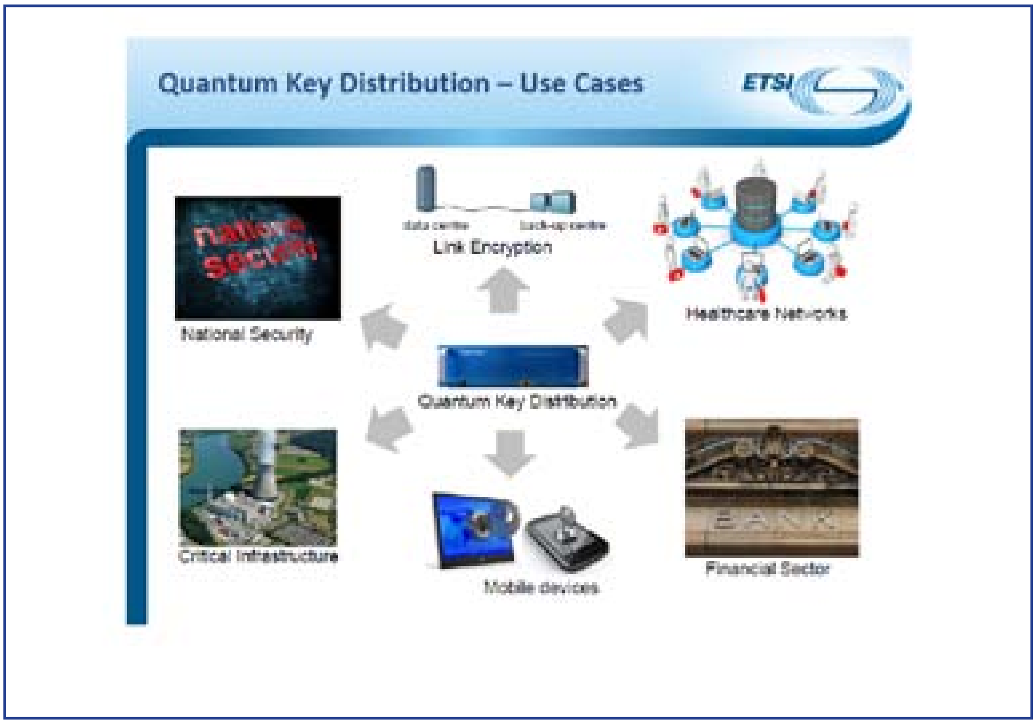
ETSI's role in the deployment of Quantum Key Distribution

Andrew Shields, Toshiba

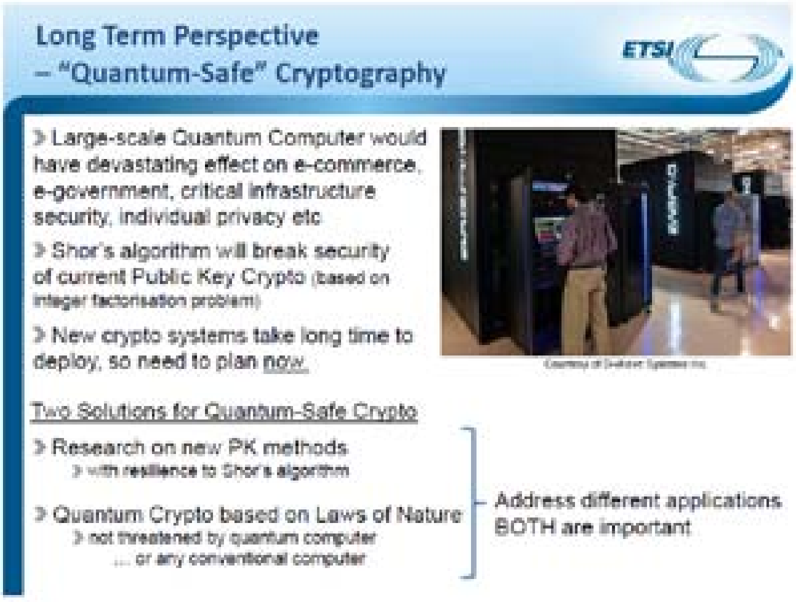
Abstract

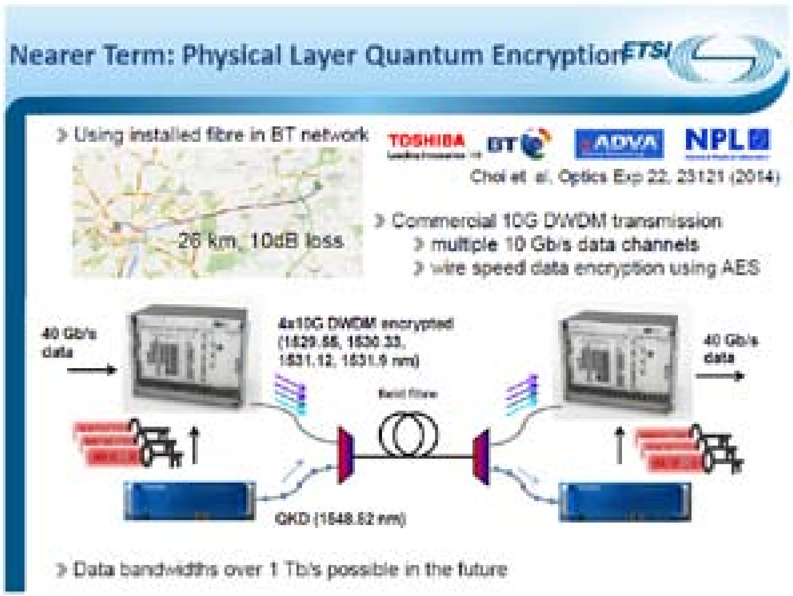
Quantum Key Distribution (QKD) offers a solution to the challenge of distributing key material securely over optical networks. Recently significant government investments have been seen globally to develop systems and demonstrator networks while technical capabilities continue to advance rapidly. However, 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.



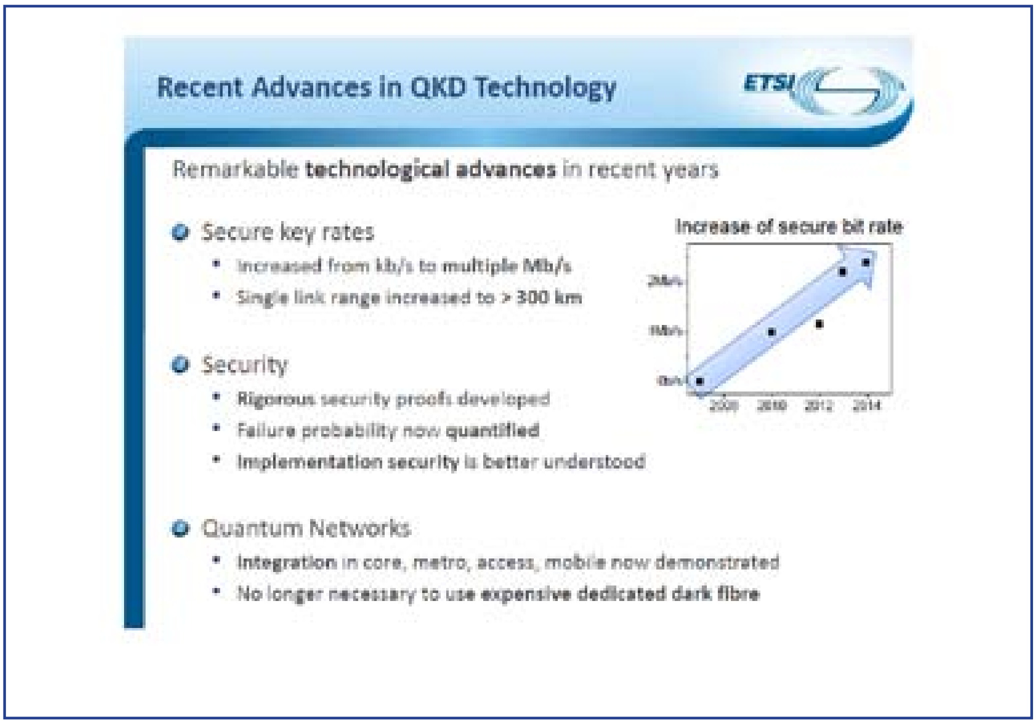


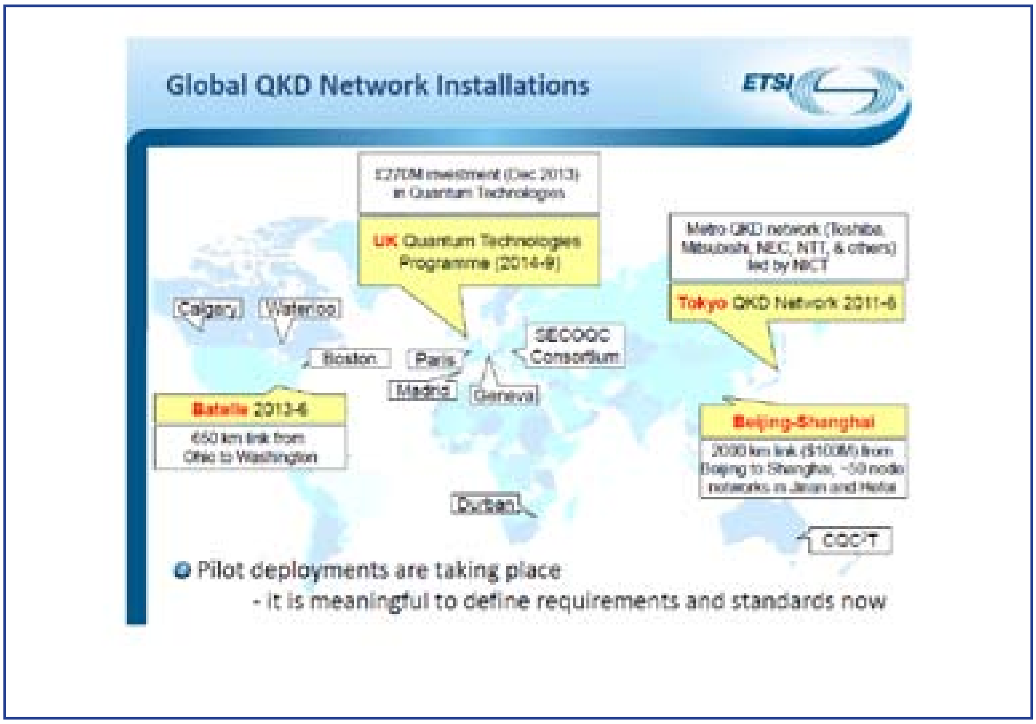
ISBN 979-10-92620-04-7





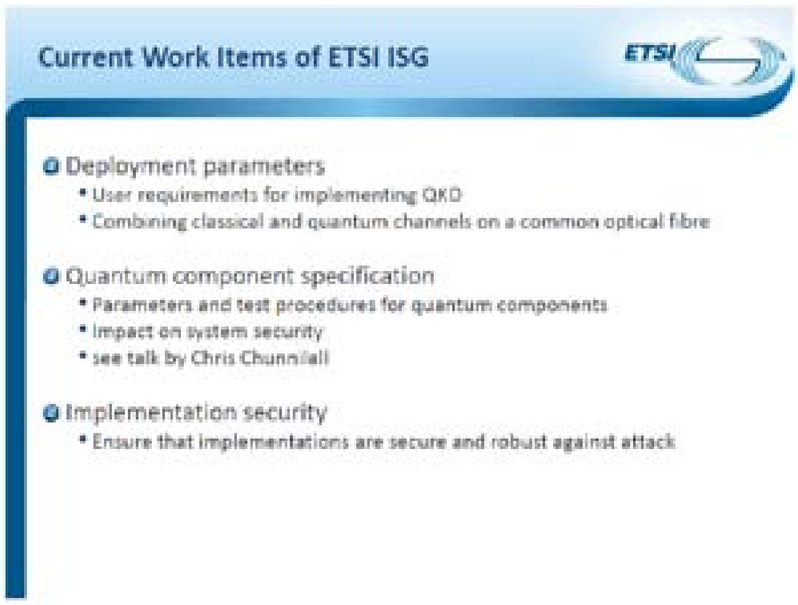
ISBN 979-10-92620-04-7

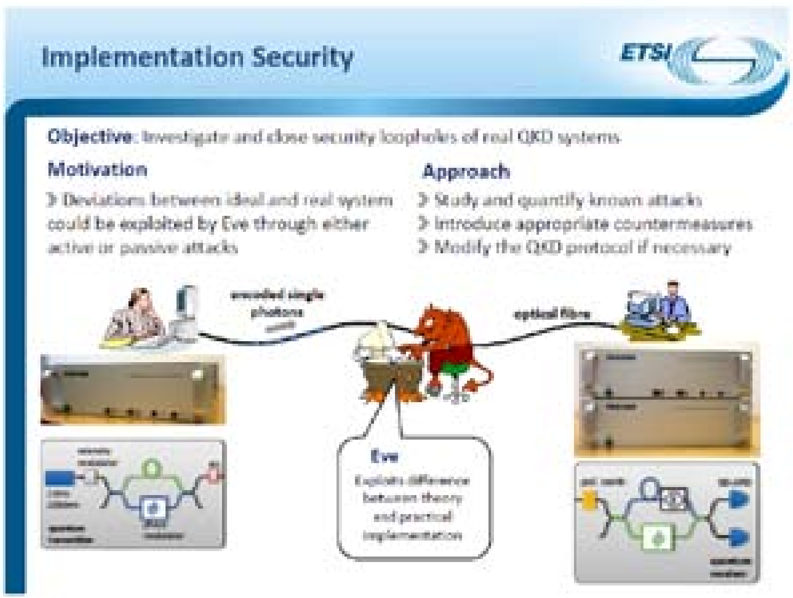




ISBN 979-10-92620-04-7

ISBN 979-10-92620-04-7





ISBN 979-10-92620-04-7

Security by Measurement

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

$$N_{\text{ideal}} \geq \underline{N}_Z^{(1)}[1 - h(\bar{q}_X{}^{(1)})] - N_{EC} - \Delta_\varepsilon$$

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

N_{EC}: Info leakage due to error correction

Δ_ε: Finite key size effect

Modified secure key rate (real system) ...

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

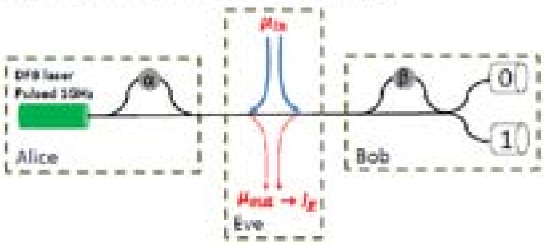
δ_1: Info leakage due to imperfection 1

δ_2: Info leakage due to imperfection 2

etc

Trojan Horse Attack

- Eve injects bright light (μ_{in}) and measures back-reflection (μ_{out}) to determine Alice's or Bob's phase modulator settings



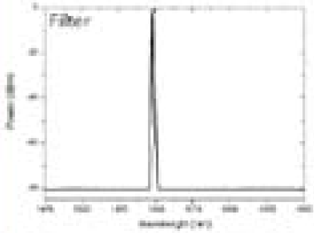
Recent experimental studies (reported at QCrypt, Paris, Sept 14)

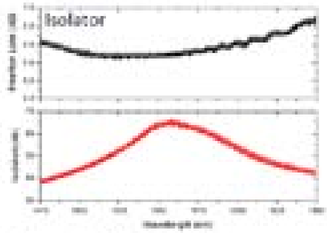
- CV QKD : Khan et al, Erlangen, Paris Telecom Tech & SecureNet
- "two-way" QKD : Sajeed et al, IQC & IdQuantique
- "one-way" QKD : considered here

ISBN 979-10-92620-04-7

Shutting out the Trojan Horse

- 150dB Isolation provided by spectral filtering and optical isolator(s)





- 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@crl.toshiba.co.uk

ISBN 979-10-92620-04-7

A certifiable QKD Relay Node Network

Nino Walenta, Battelle

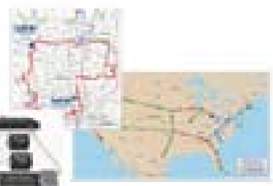
Besides the obvious benefits and strengths of quantum key distribution (QKD) of securely distributing cryptographic keys [1], the widespread adoption of commercial QKD systems has mainly been hindered by their range, limited to a few hundred kilometers, and their intrinsic point-to-point connectivity. 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 16/3/2014

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)

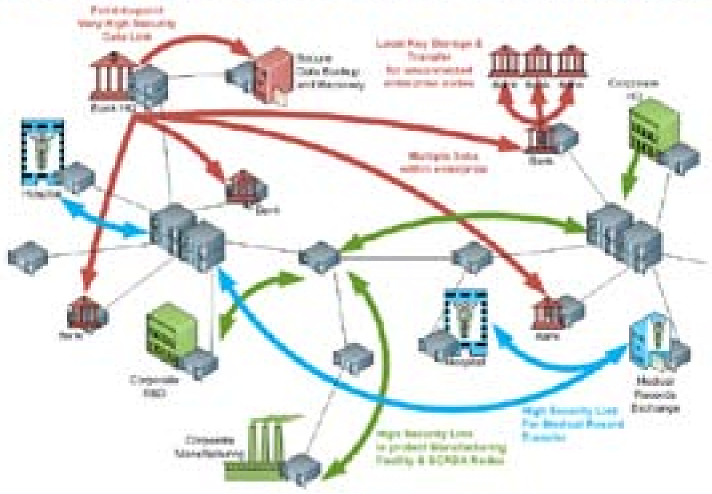
Our solution: A QKD Trusted Node network

- **A single design to handle both short comings**

3 16/3/2014

ISBN 979-10-92620-04-7

The QKD Trusted Node Architecture

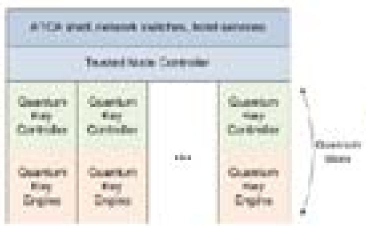


4

IDQ

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

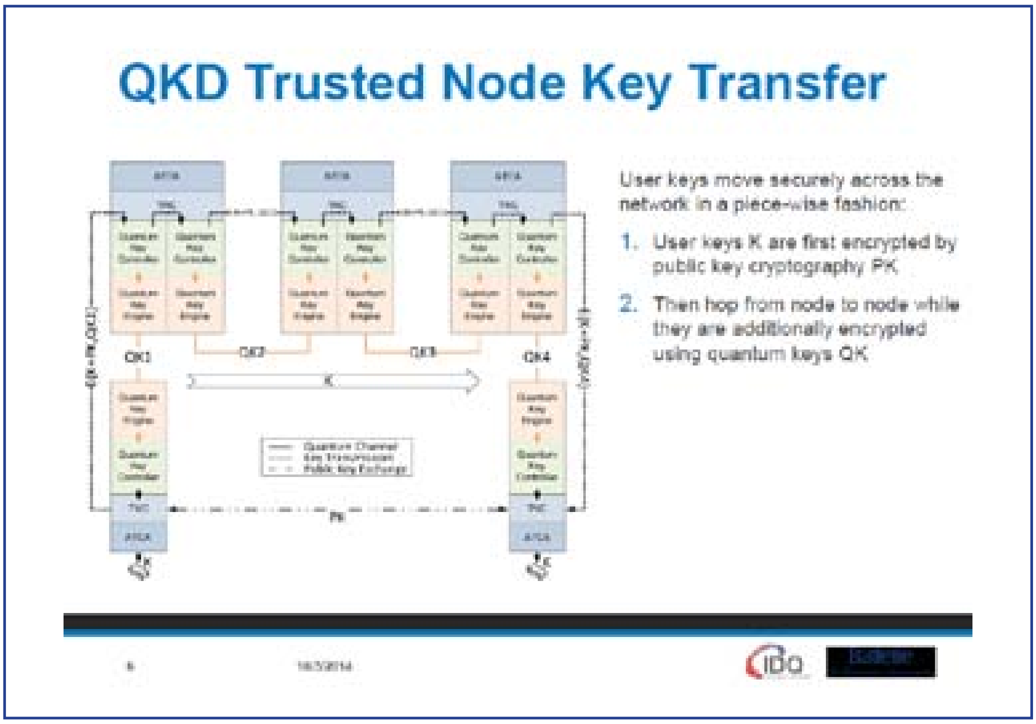


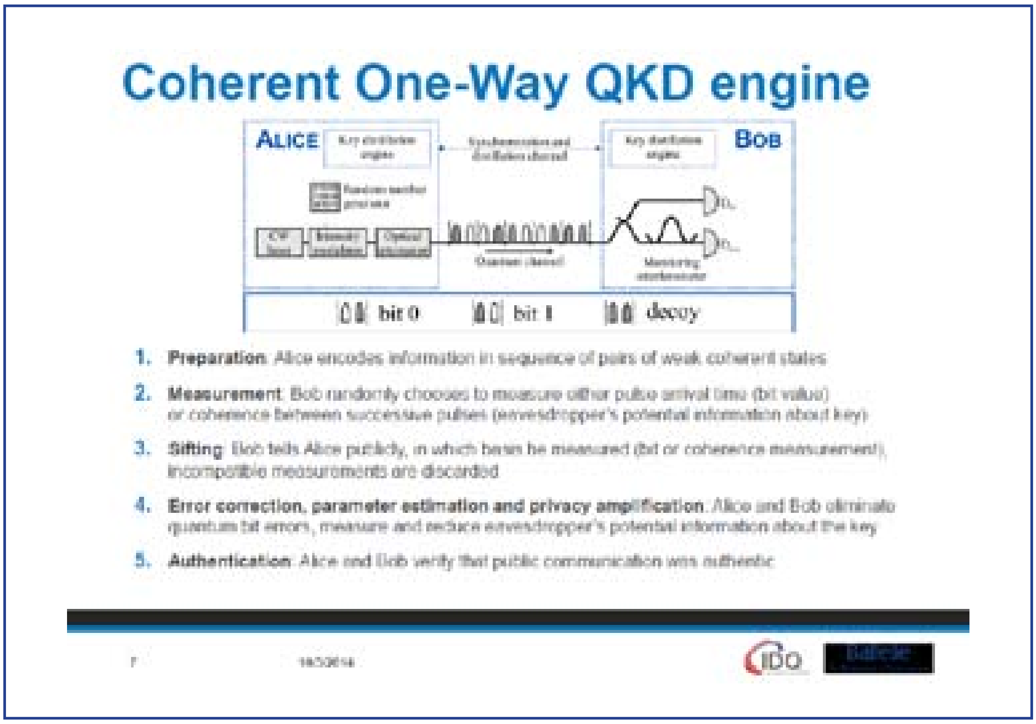
- Redundant node controller in a single node
  - Manages node discovery and provides route tables for quantum network
  - Manages and routes key transactions
- Fault tolerant dynamic path finding algorithm
  - Routing balances security and quality of service
  - Finds least cost path across the QKD network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

5

IDQ

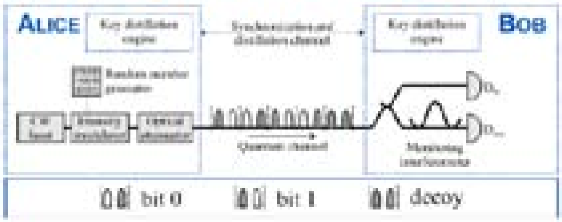
ISBN 979-10-92620-04-7





ISBN 979-10-92620-04-7

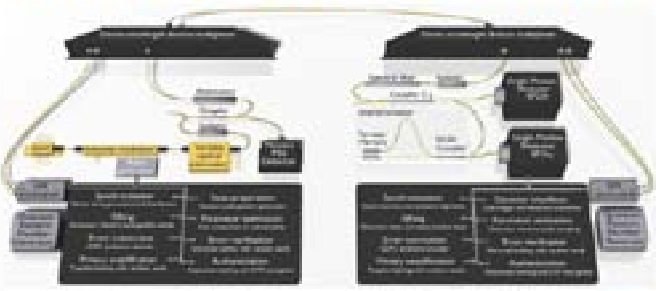
Coherent One-Way QKD engine



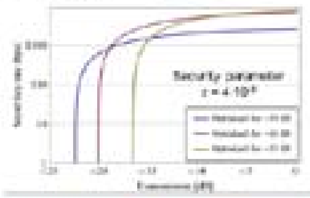
Characteristics

- 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

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



ISBN 979-10-92620-04-7

IT security standards

NIST
National Institute of Standards and Technology

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

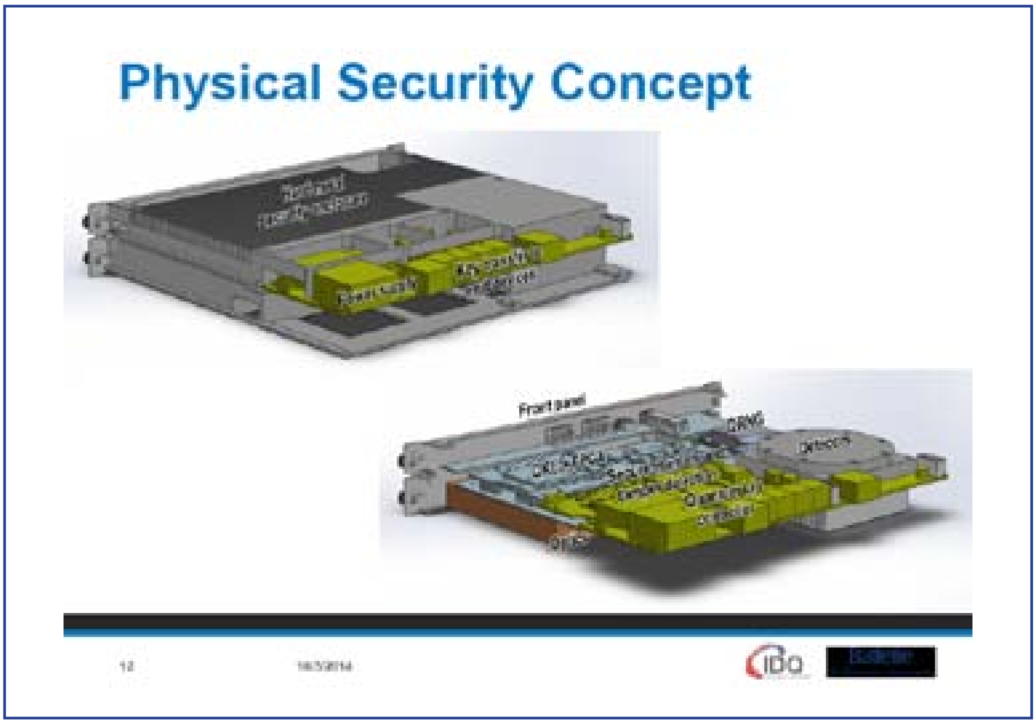
No existing standards include QKD as an approved key distribution method

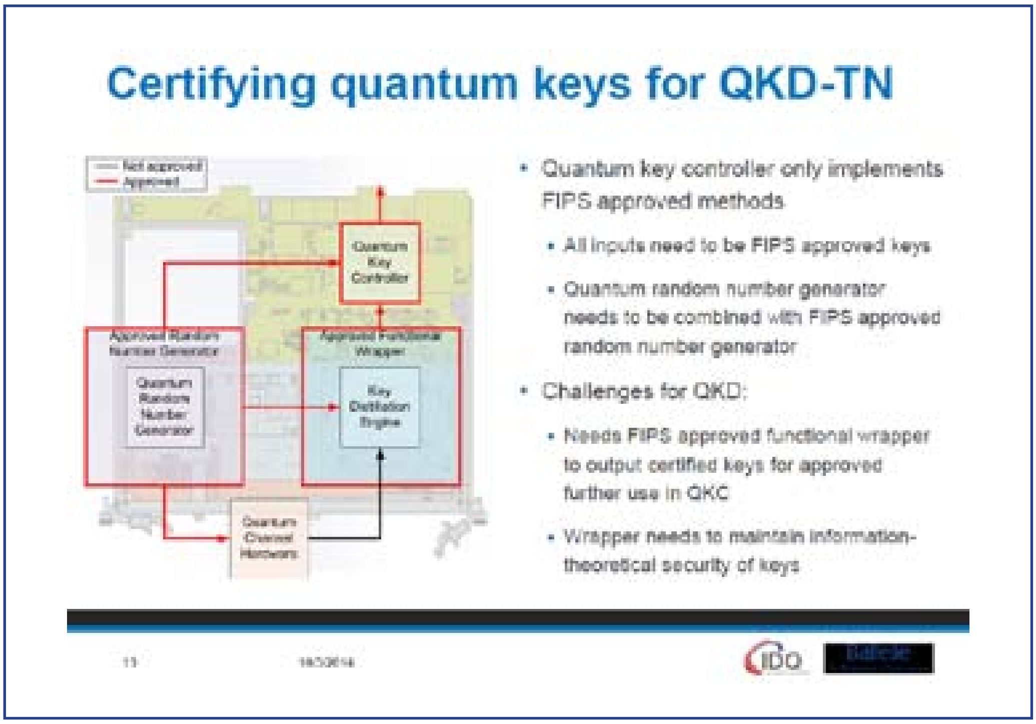
10 16/3/2014 IDQ

FIPS Security requirements

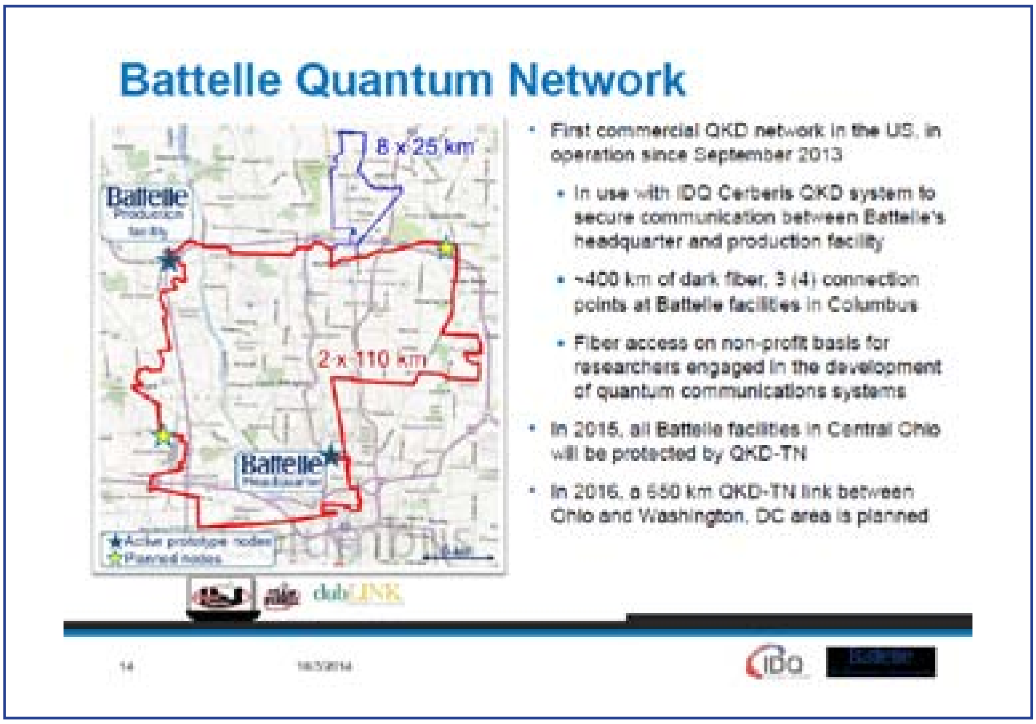
	Security Level 1	Security Level 2	Security Level 3	Security Level 4
Roles, Services, and Authentication	Logical separation of roles and services.	Role-based or identity-based authentication.	Identity-based operator authentication.	
Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware 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 key input/output in plaintext form.		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.

11 16/3/2014 IDQ

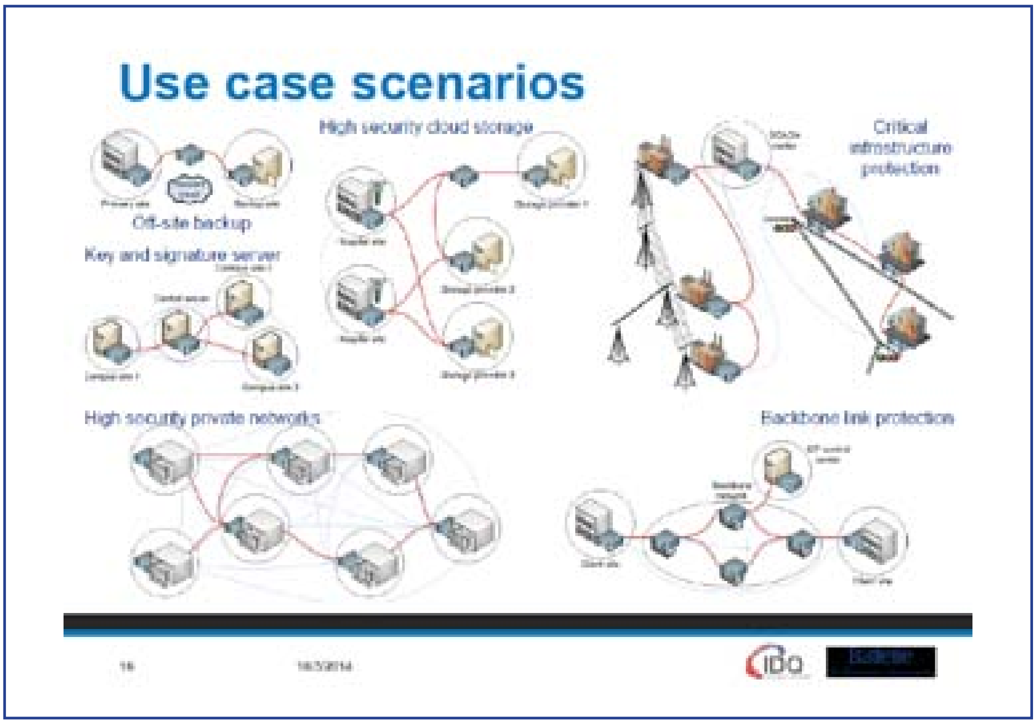


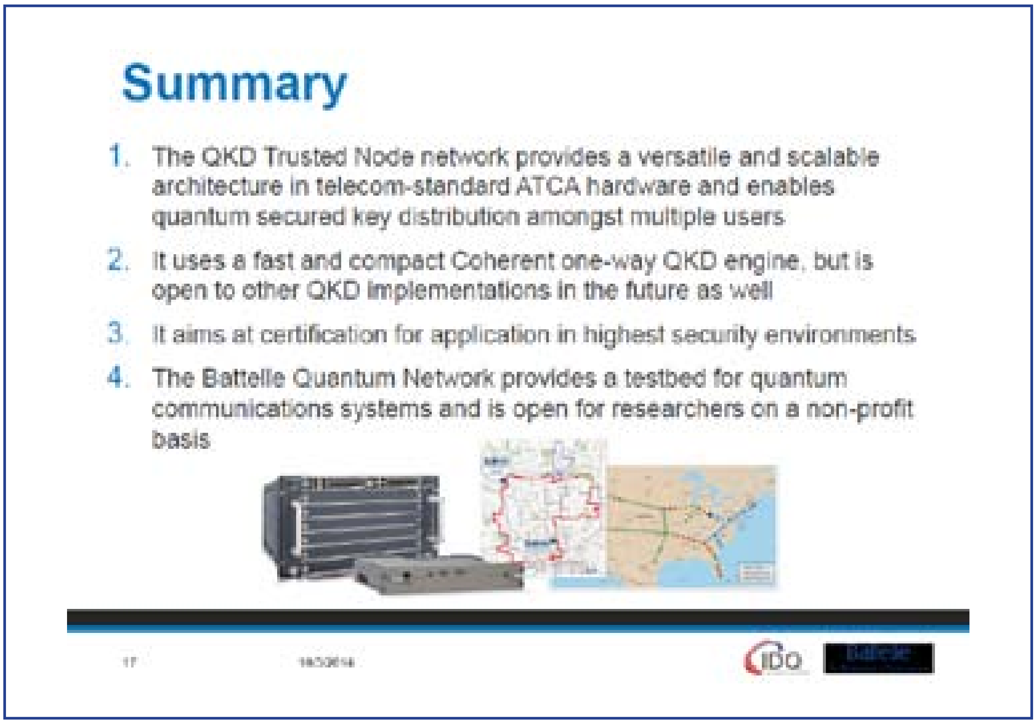


ISBN 979-10-92620-04-7



ISBN 979-10-92620-04-7





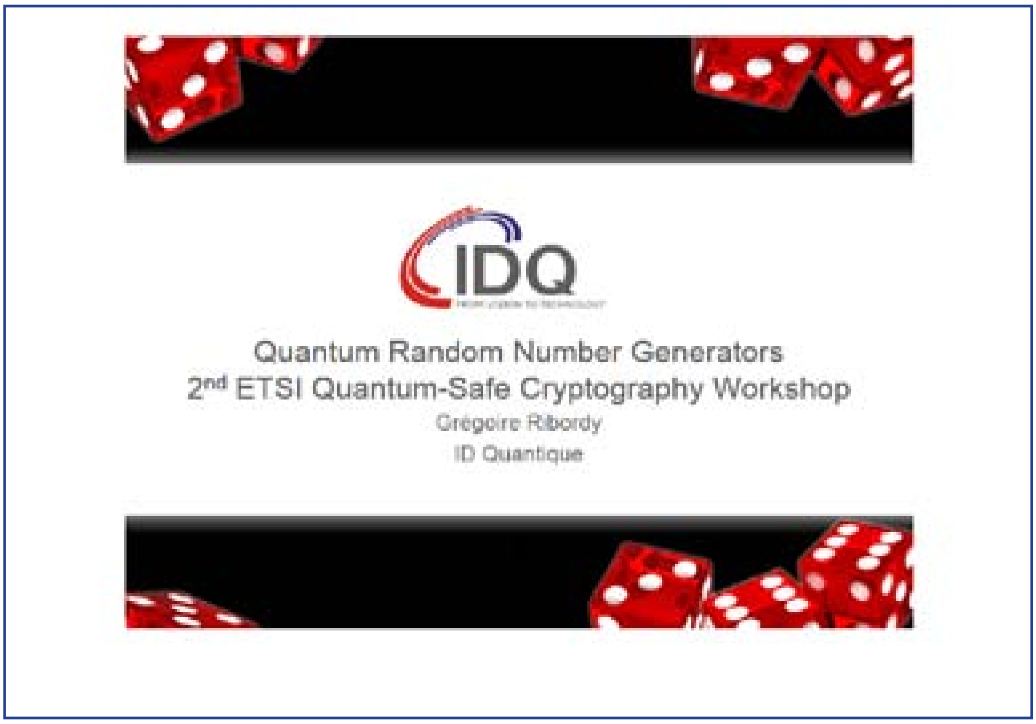
ISBN 979-10-92620-04-7

Presentations

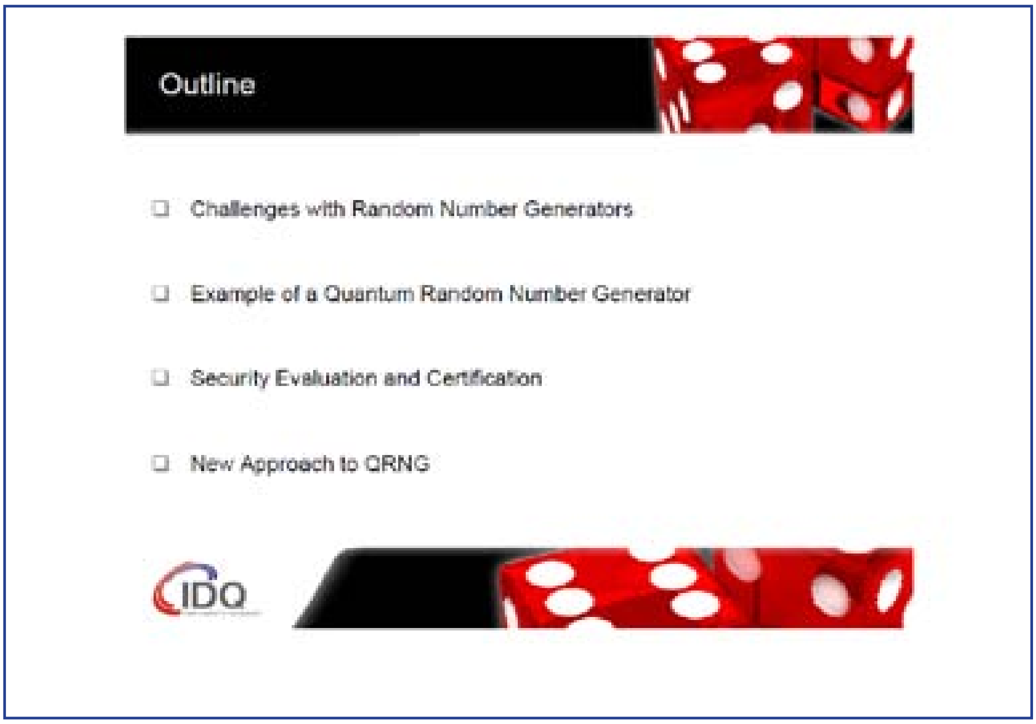
SESSION 5
INDUSTRY

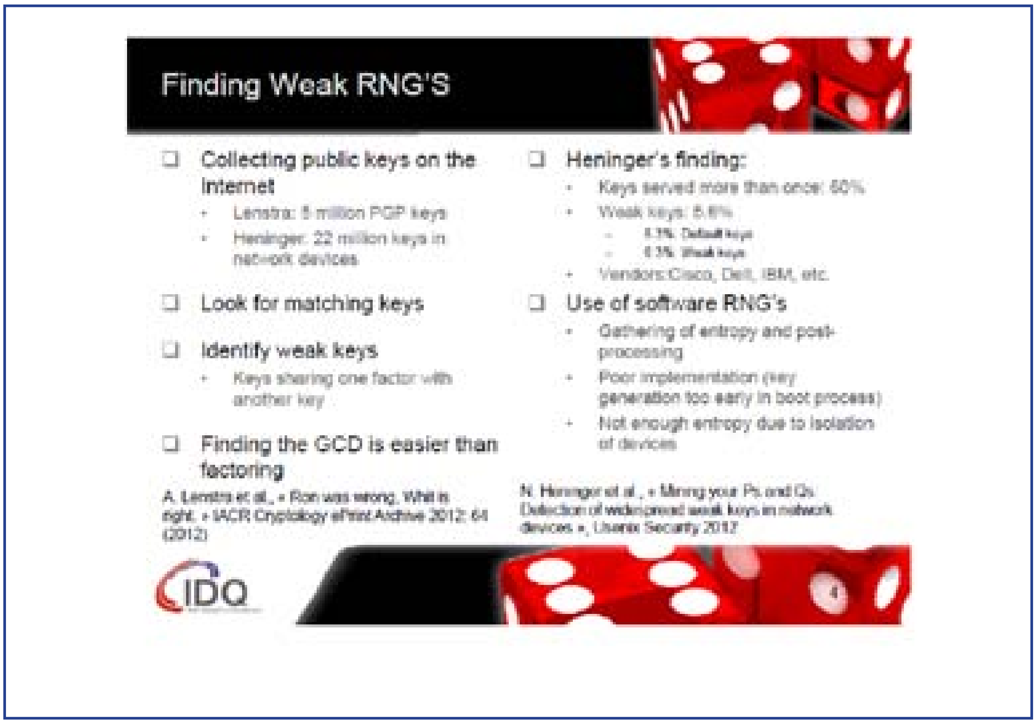
Quantum Random Number Generator

Grégoire Ribordy, IDQ

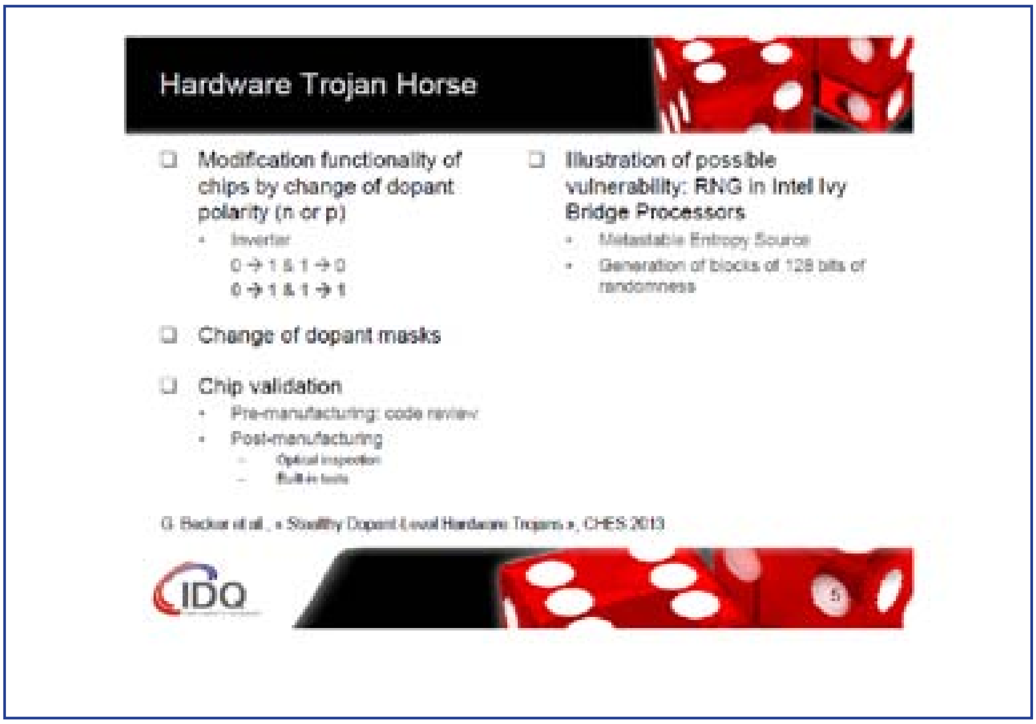


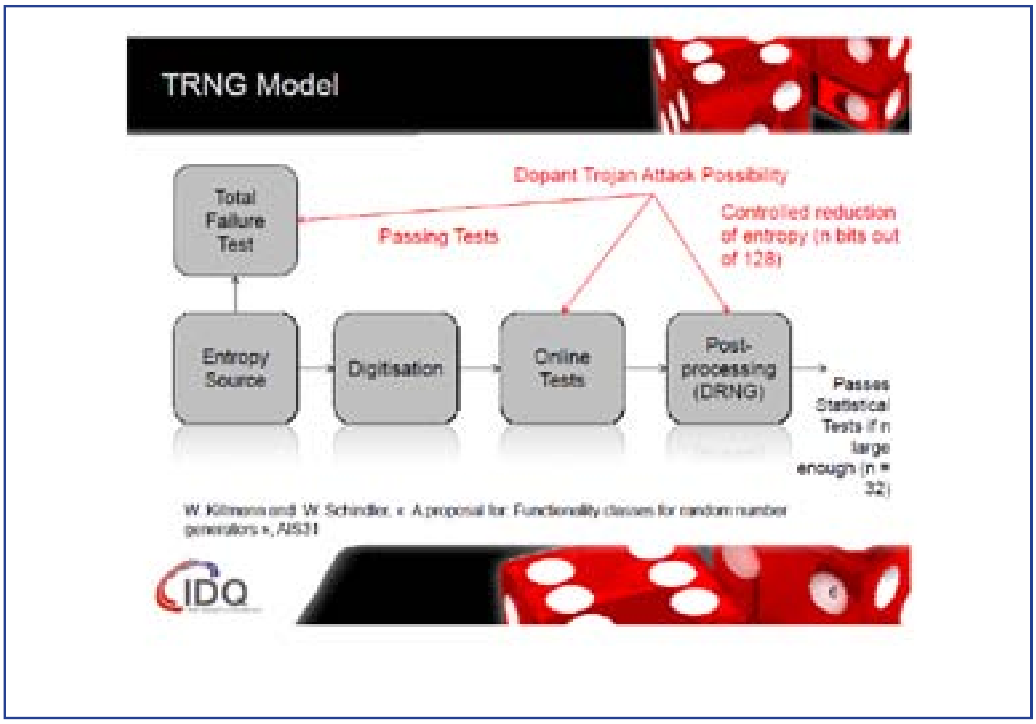
ISBN 979-10-92620-04-7



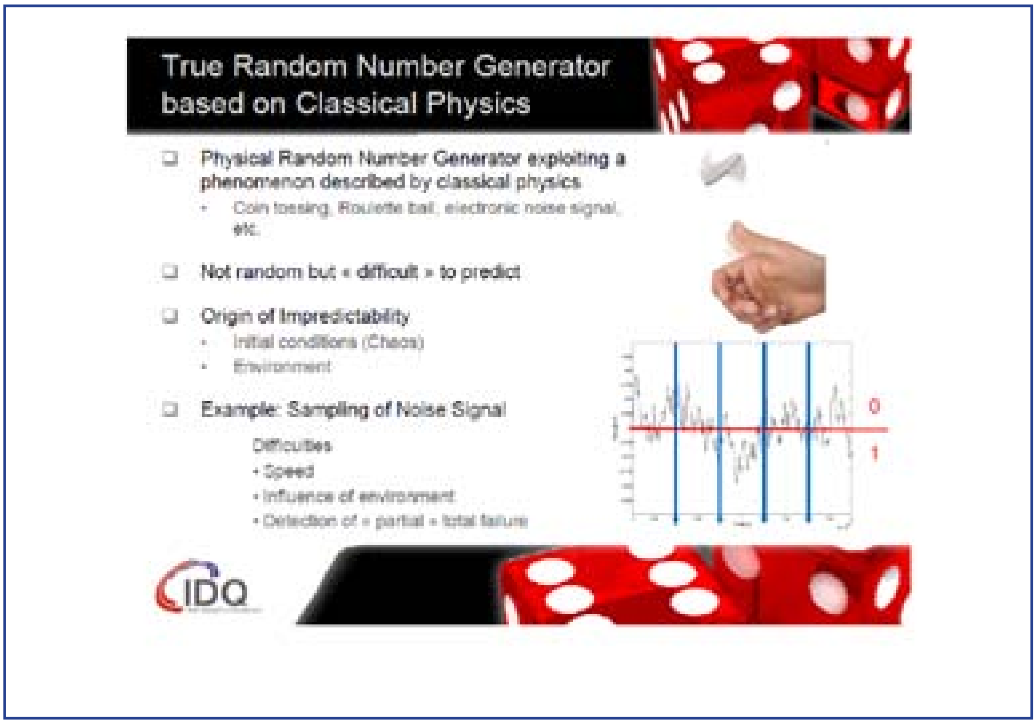


ISBN 979-10-92620-04-7

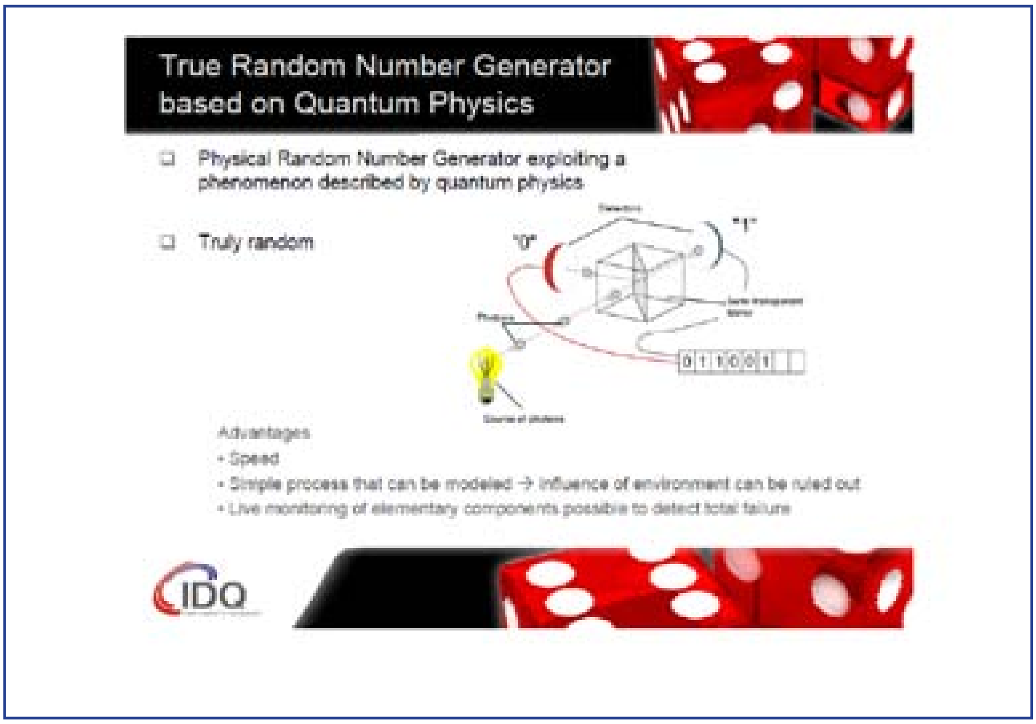




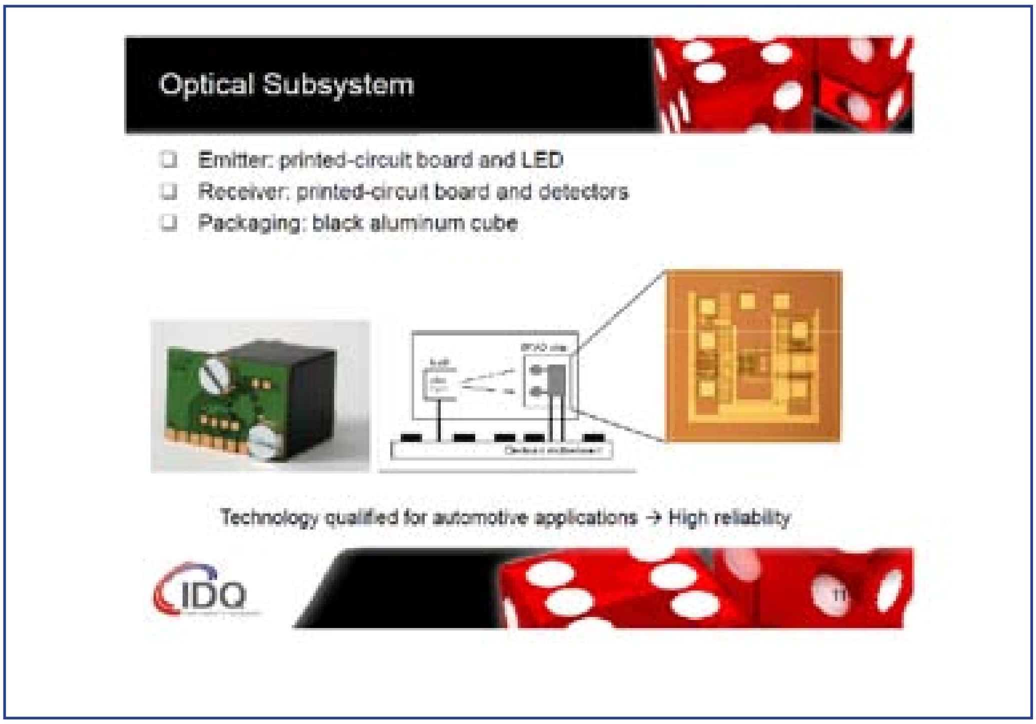
ISBN 979-10-92620-04-7



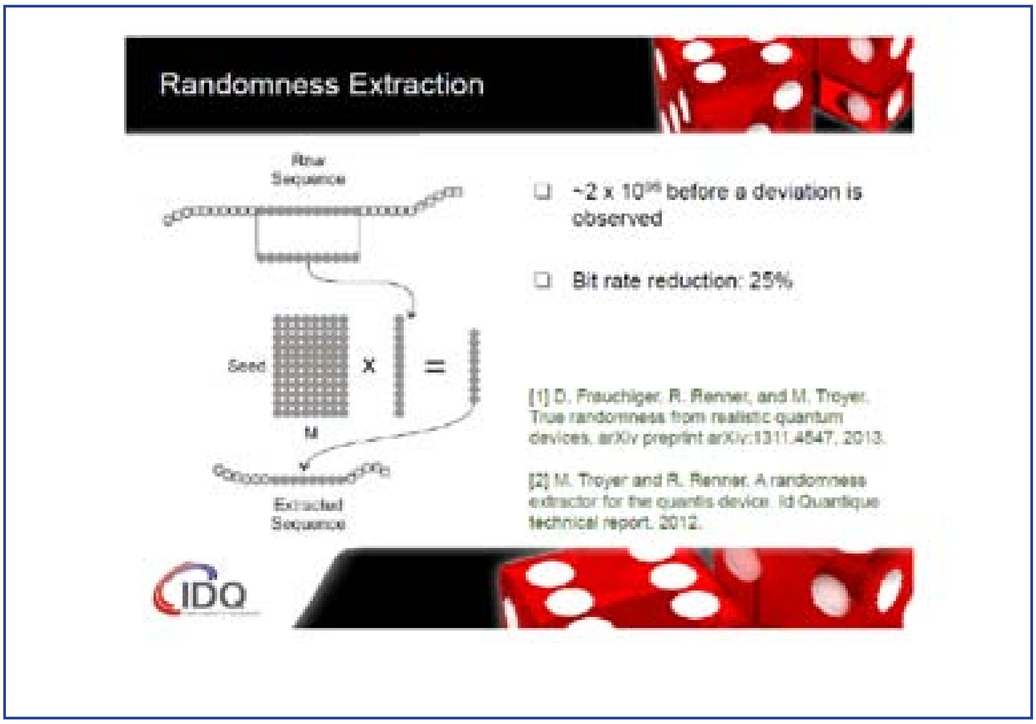
ISBN 979-10-92620-04-7



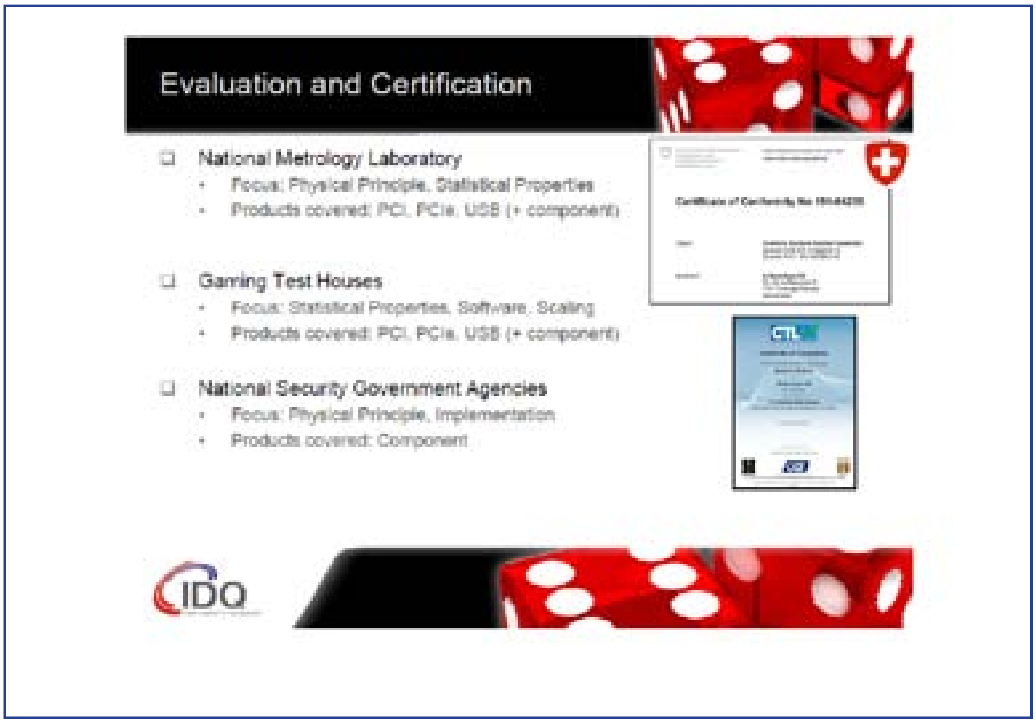
ISBN 979-10-92620-04-7

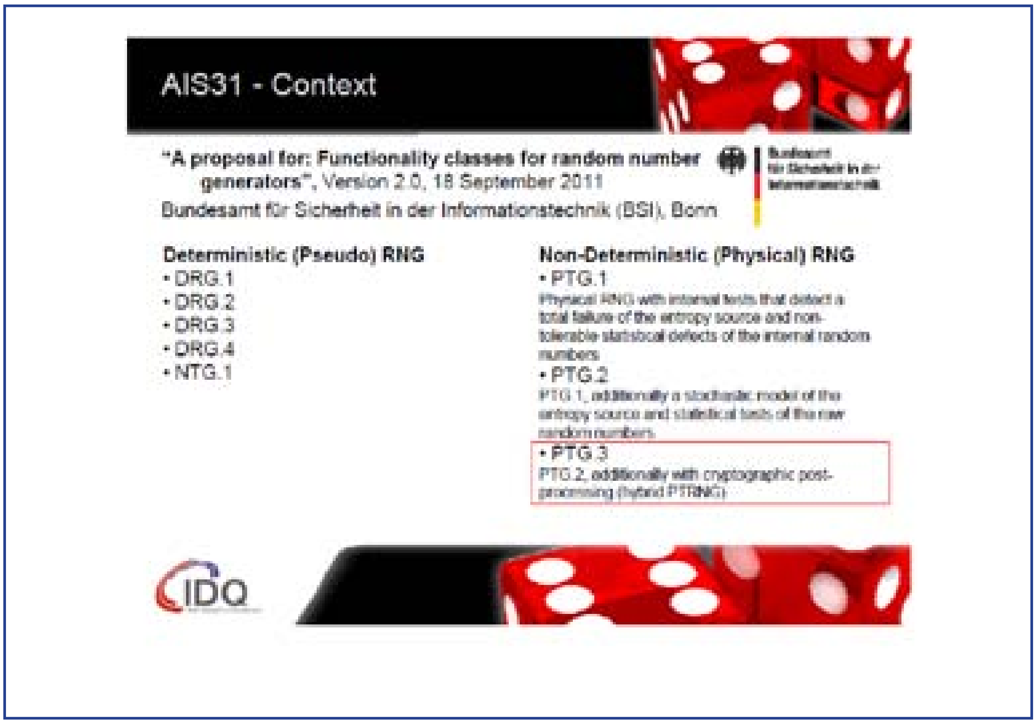


ISBN 979-10-92620-04-7

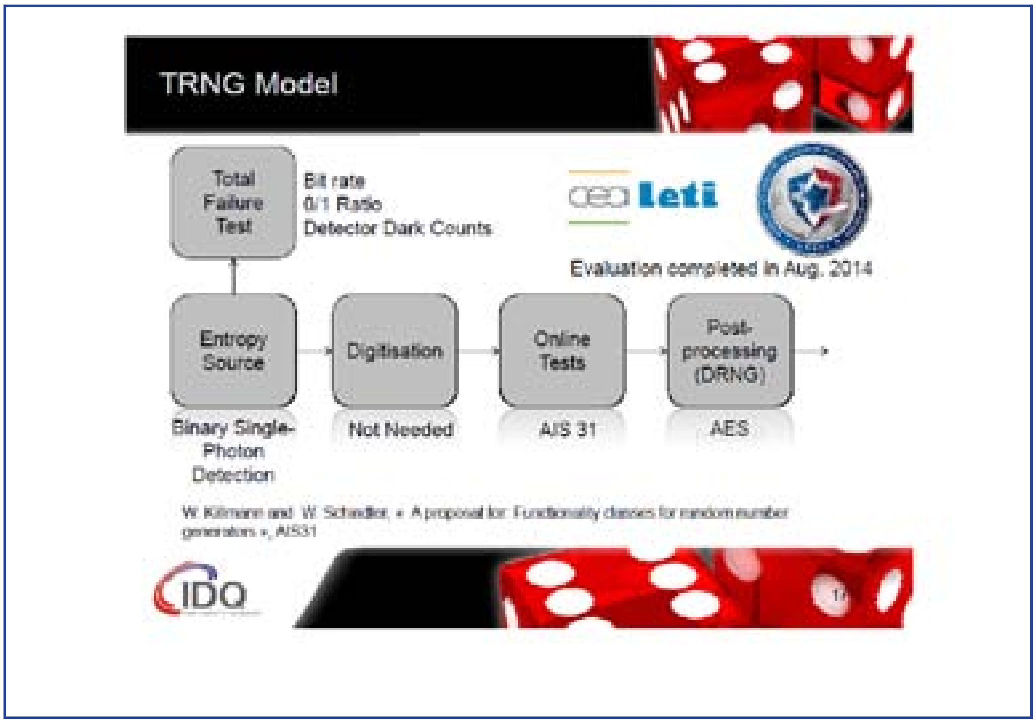


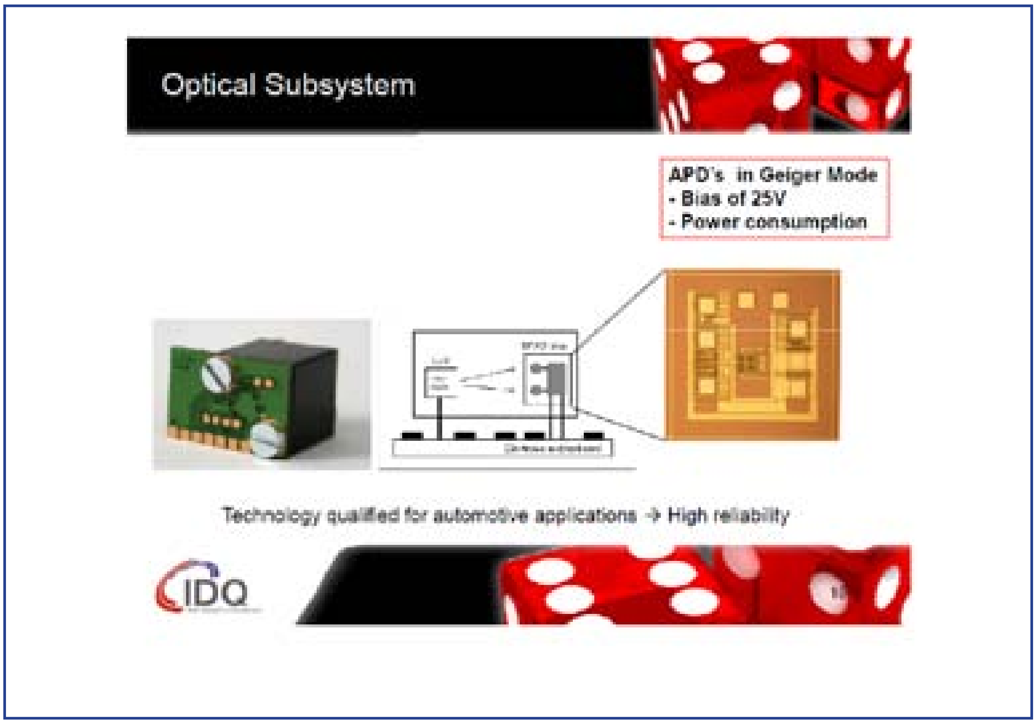
ISBN 979-10-92620-04-7



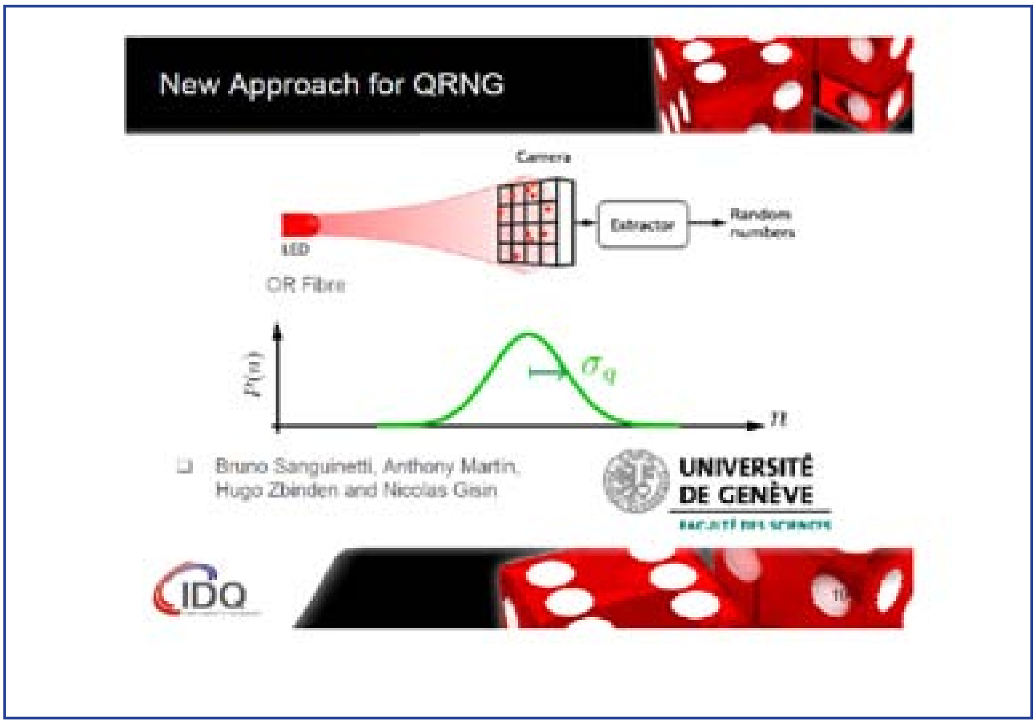


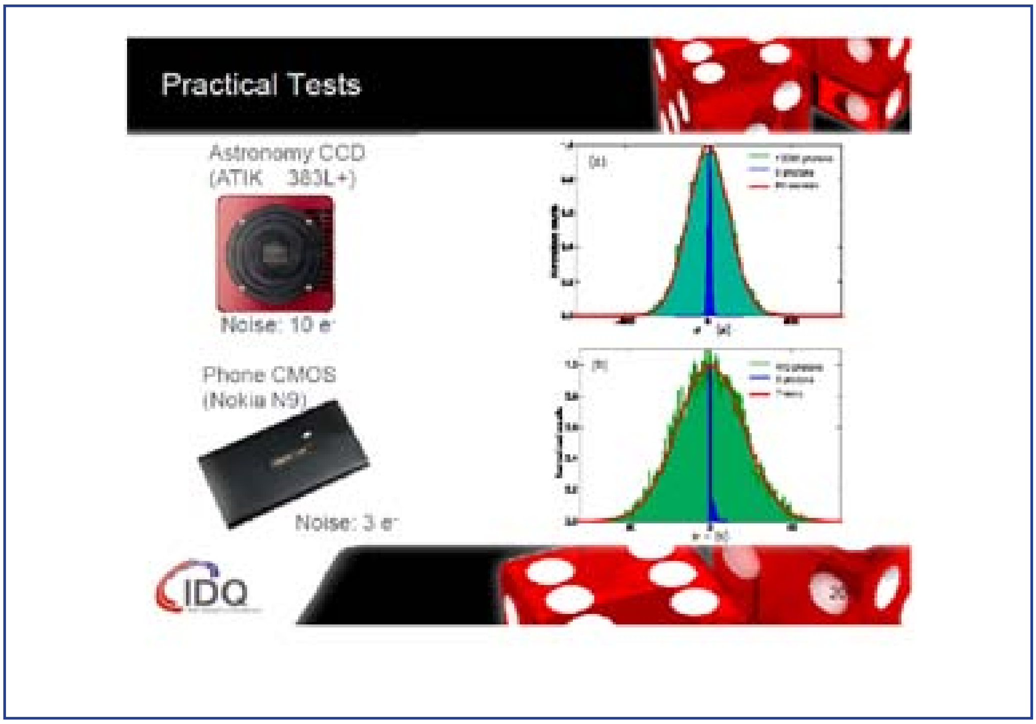
ISBN 979-10-92620-04-7



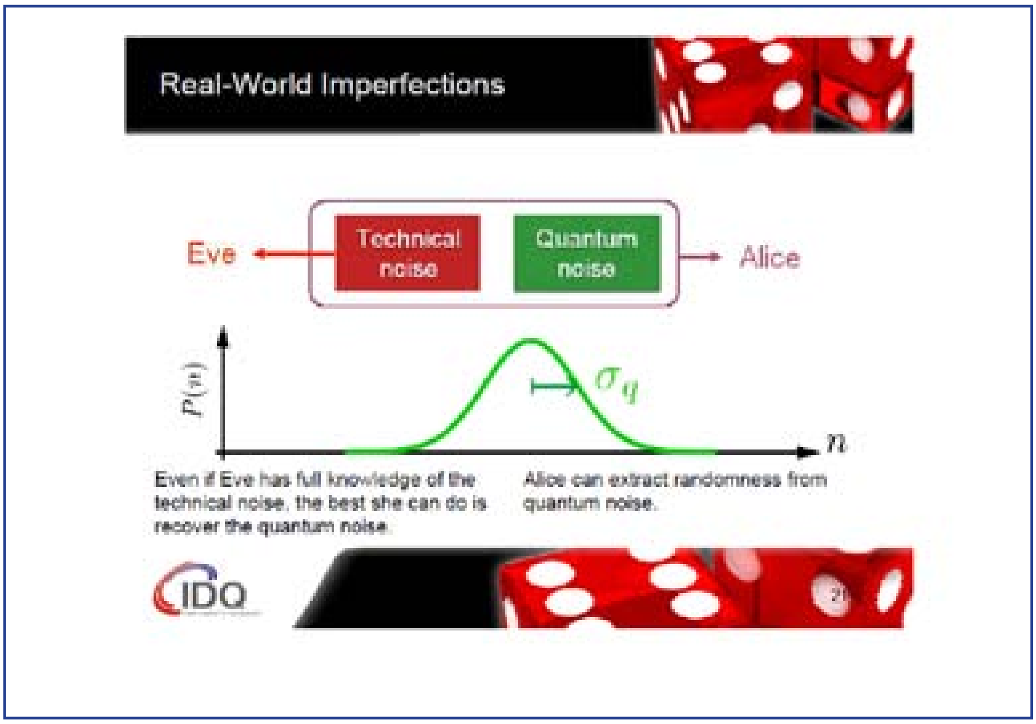


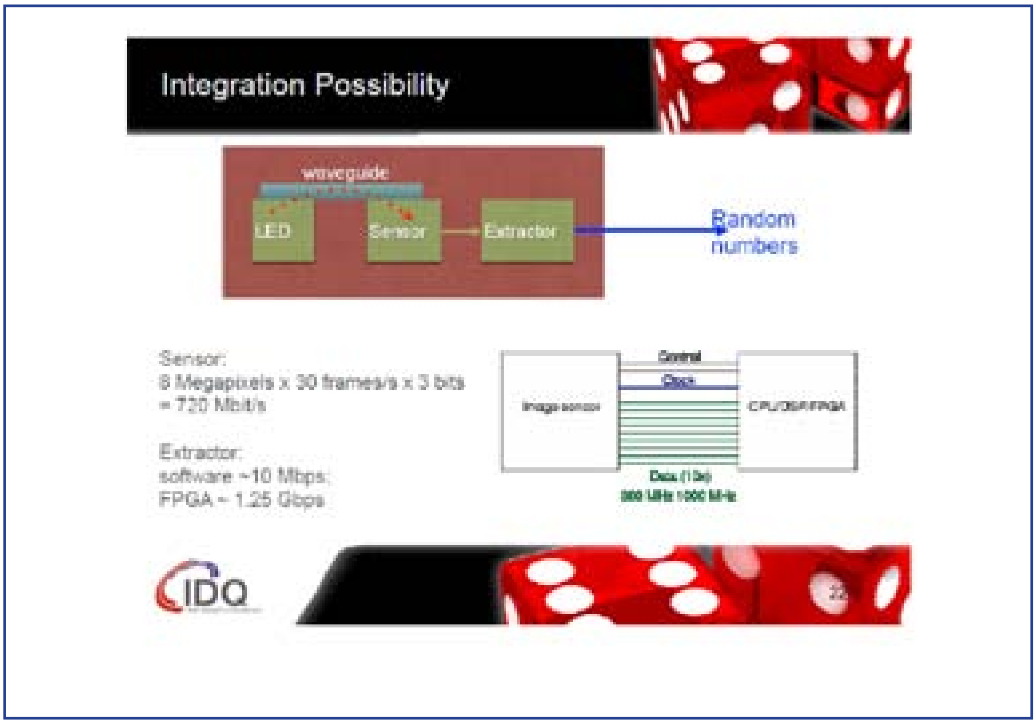
ISBN 979-10-92620-04-7



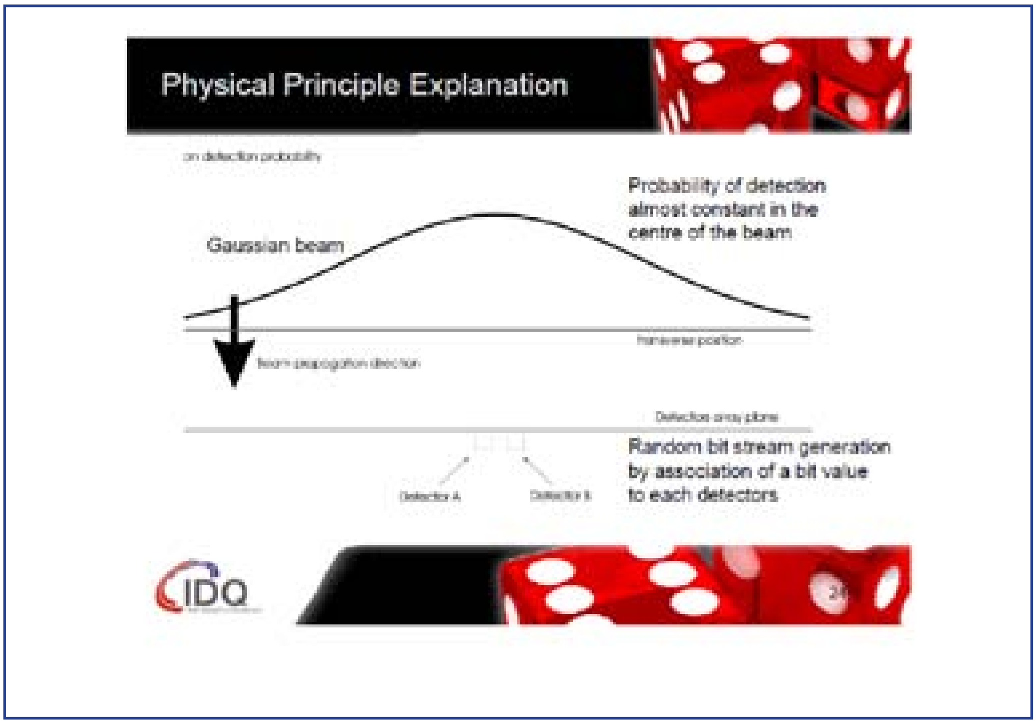


ISBN 979-10-92620-04-7


Real-World Imperfections
Eve
Technical noise
Quantum noise
Alice
P(n)
σq
n
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.
IDQ
21


Integration Possibility
waveguide
LED
Sensor
Extractor
Random numbers
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
CPU/DSP/FPGA
IDQ
22

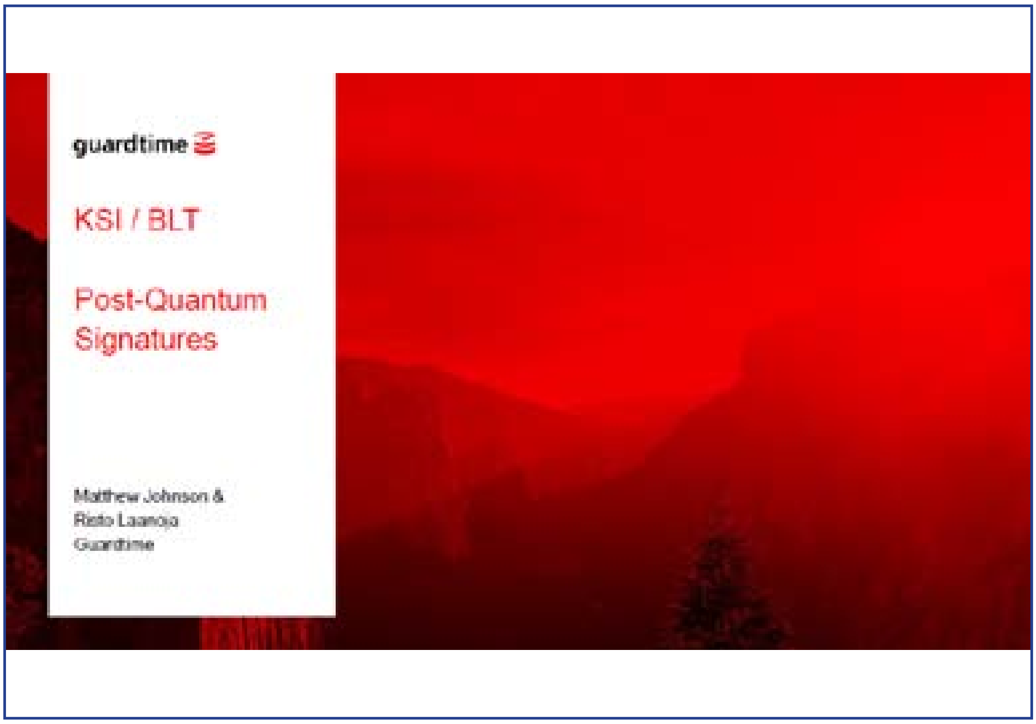

Thank you for you attention
7th Winter school on practical quantum communications
January 2015
In Les Diablerets, Switzerland
– Whitfield Diffie
– Nicolas Gisin
– Dr. Colin P Williams, D-Wave,
– Sandu Popescu
– Eleni Diamanti
New – Track on Security Evaluation and Certification
Website: http://www.idquantique.com/instrumentation/training.html
Contact: info@idquantique.com or gregoire.ribordy@idquantique.com
IDQ


Physical Principle Explanation
Probability of detection almost constant in the centre of the beam
Gaussian beam
Random bit stream generation by association of a bit value to each detectors
IDQ

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 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 (~ 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 consuption 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.



ISBN 979-10-92620-04-7

guardtime

Estonia: a 100% Digital Society Built Post-Internet

NATO Cybersecurity Center of Excellence
Tallinn Estonia

- 100% Electronic Health Records
- 99.6% 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:

2

guardtime

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 an exabyte 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.

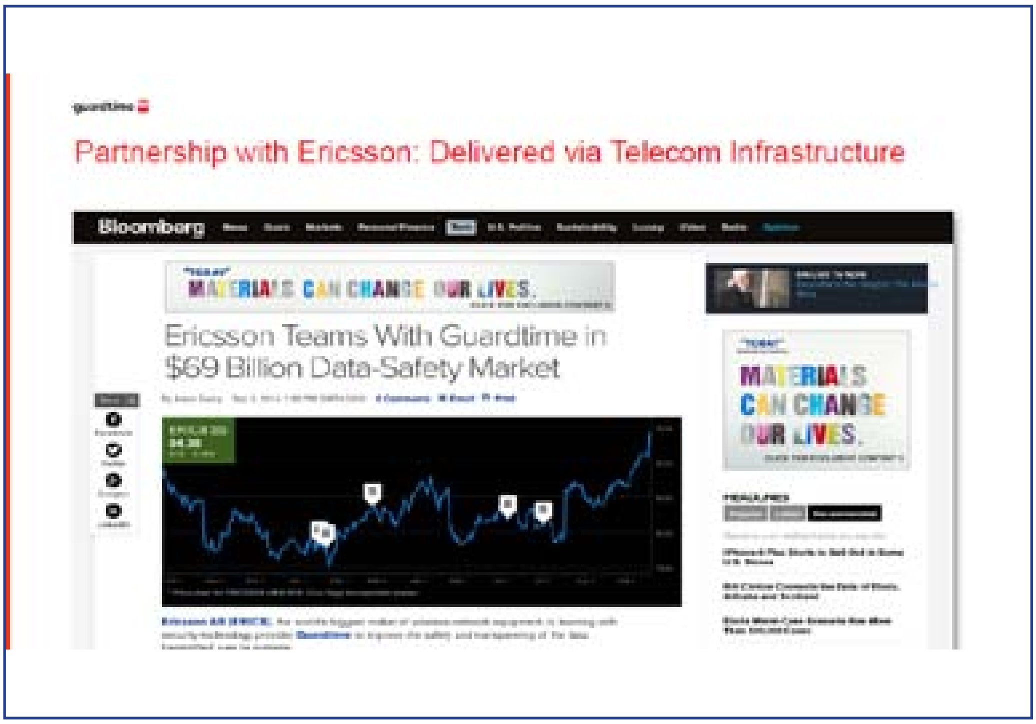
Indefinite Expiry: The signatures should not have an operational lifetime.

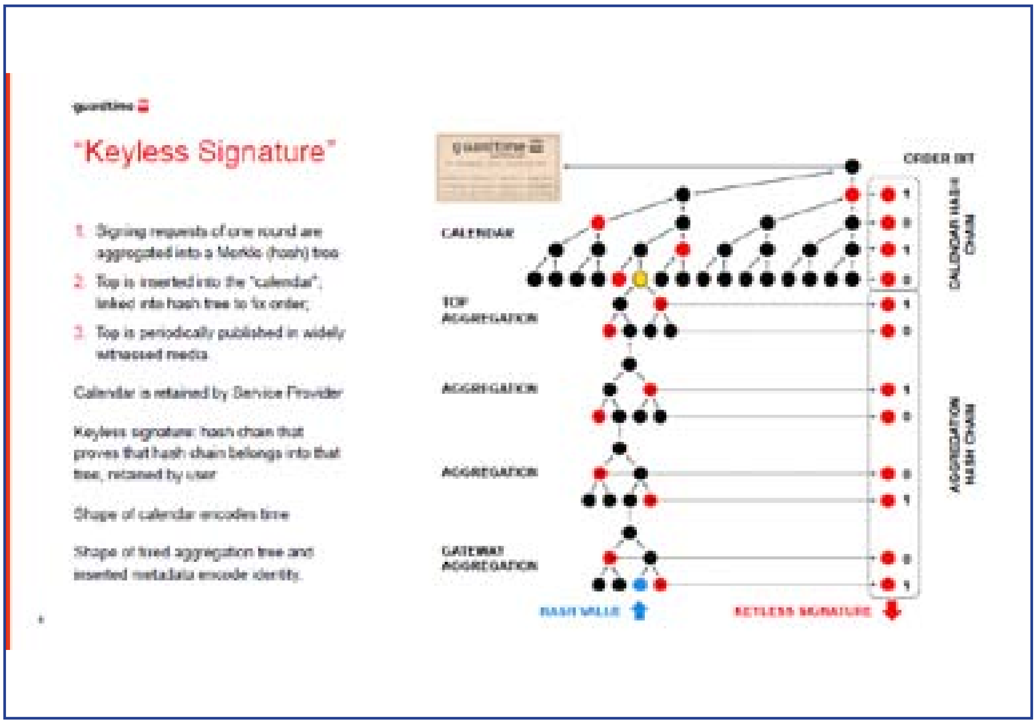
Telecom Grade: The system should be able to deliver 99.999% availability.

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

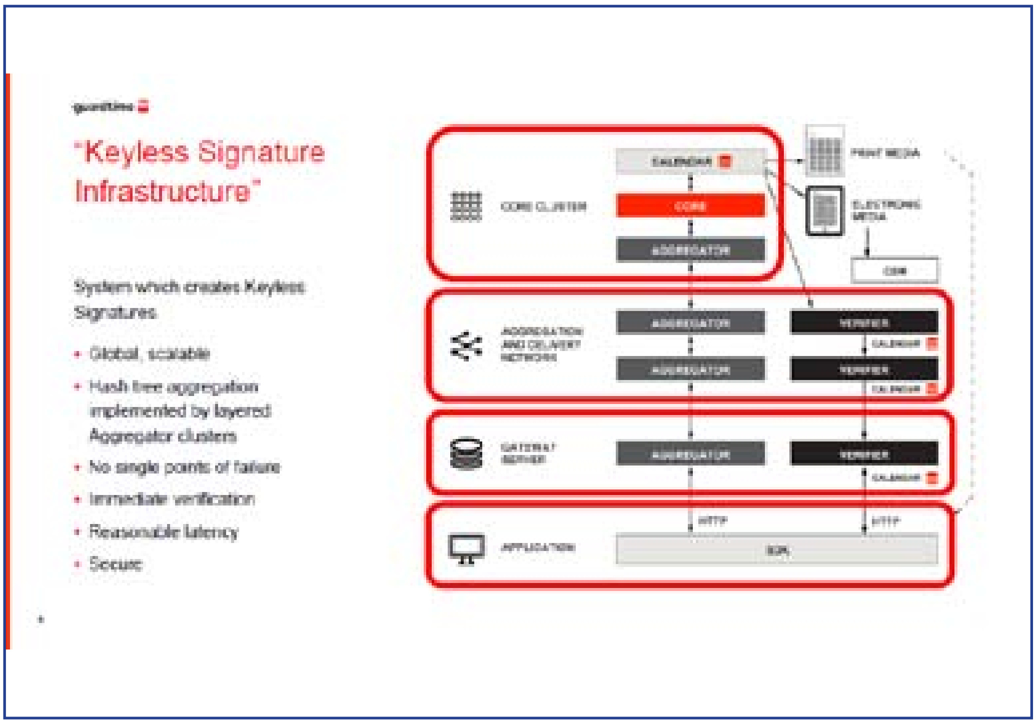
Post-Quantum: The system should be work assuming functioning quantum computers i.e. it cannot rely on traditional asymmetric key cryptography.

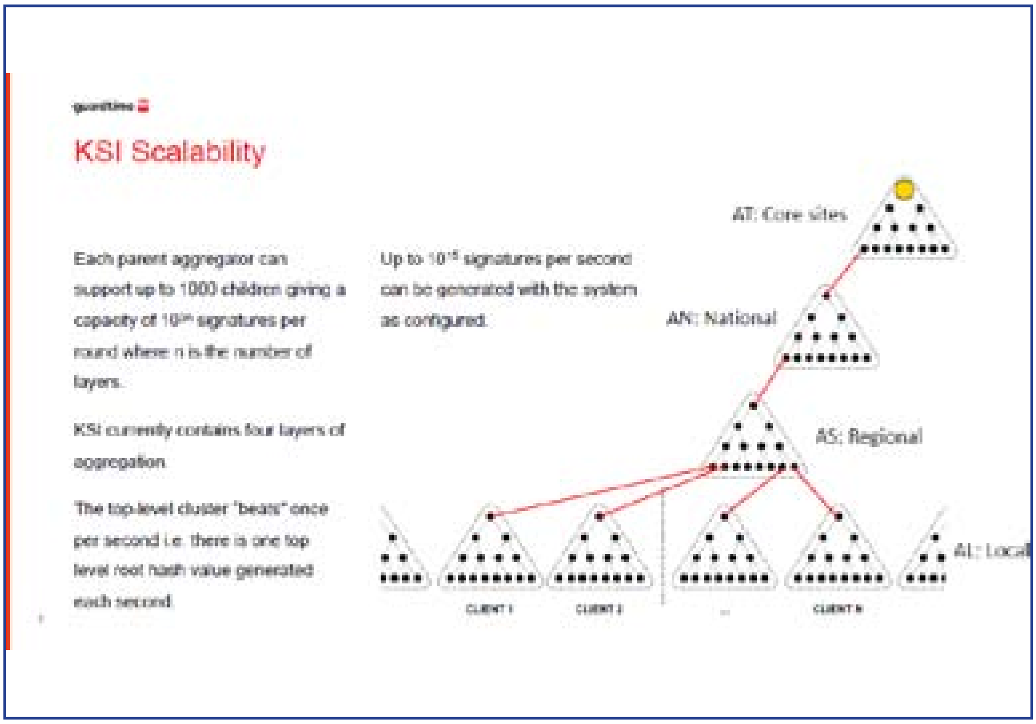
8





ISBN 979-10-92620-04-7





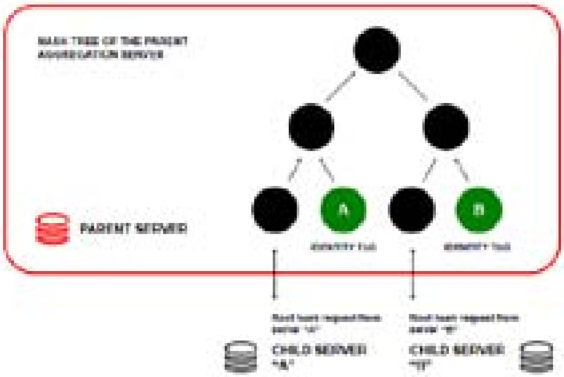
ISBN 979-10-92620-04-7

guardtime

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.



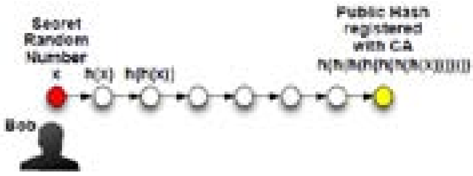
guardtime

Introducing BLT: One way hash chains

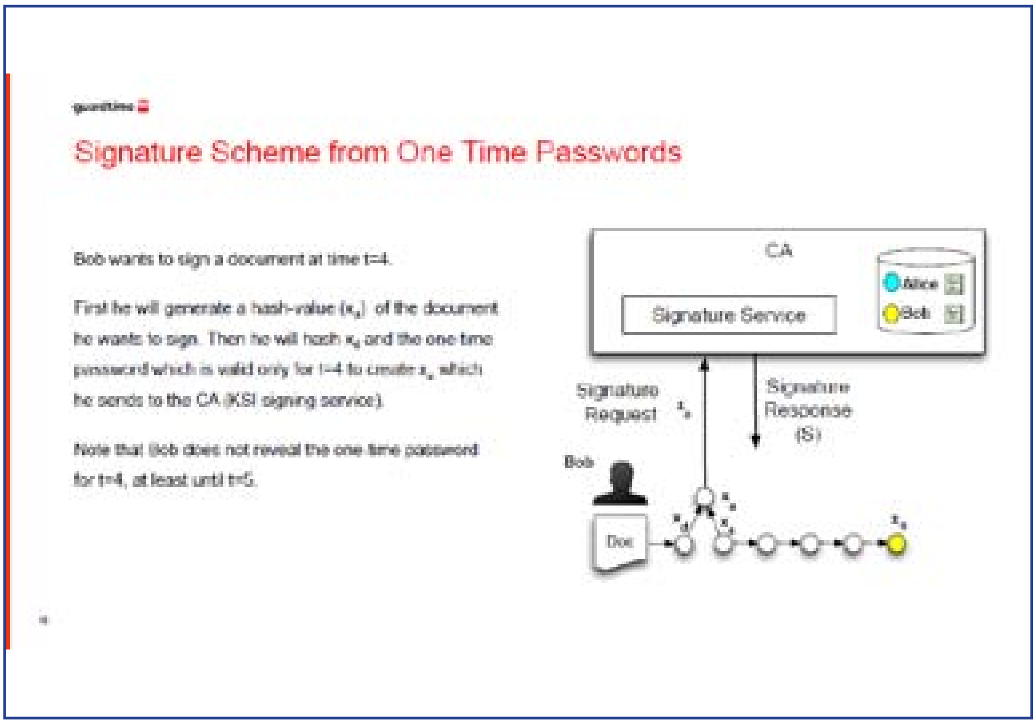
Bob first generates a secret random number and generates a hash value of that number, then generates a hash value of that and repeats creating a chain of hash-values (Lamport one-time passwords).

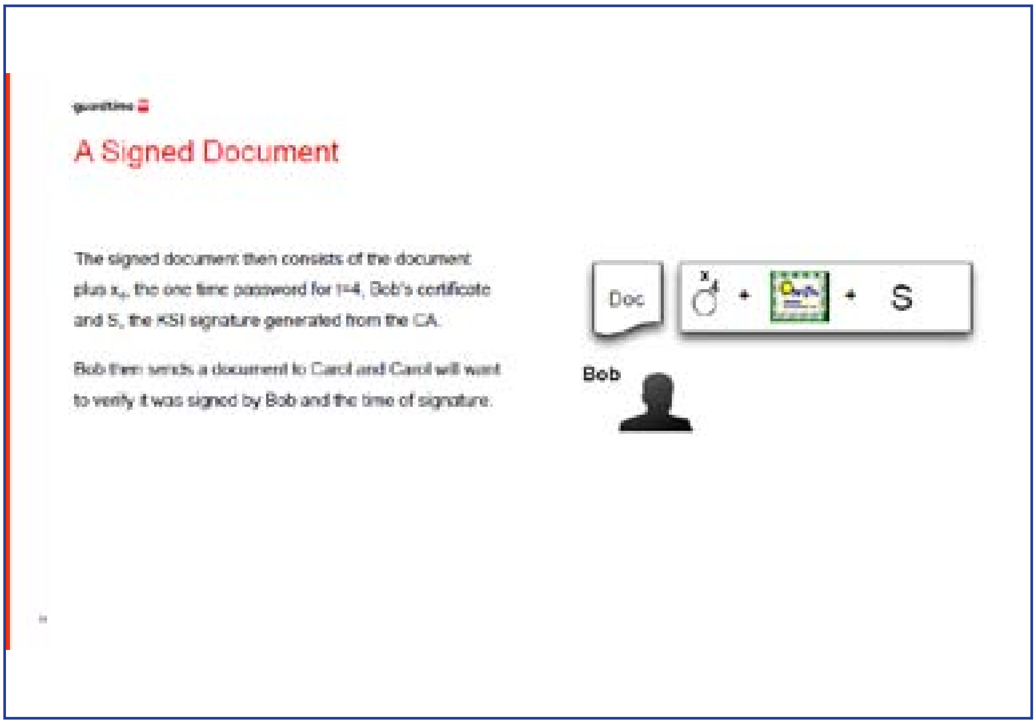
The last hash value in the chain is then registered with a CA after Bob's identity is verified.

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.



ISBN 979-10-92620-04-7

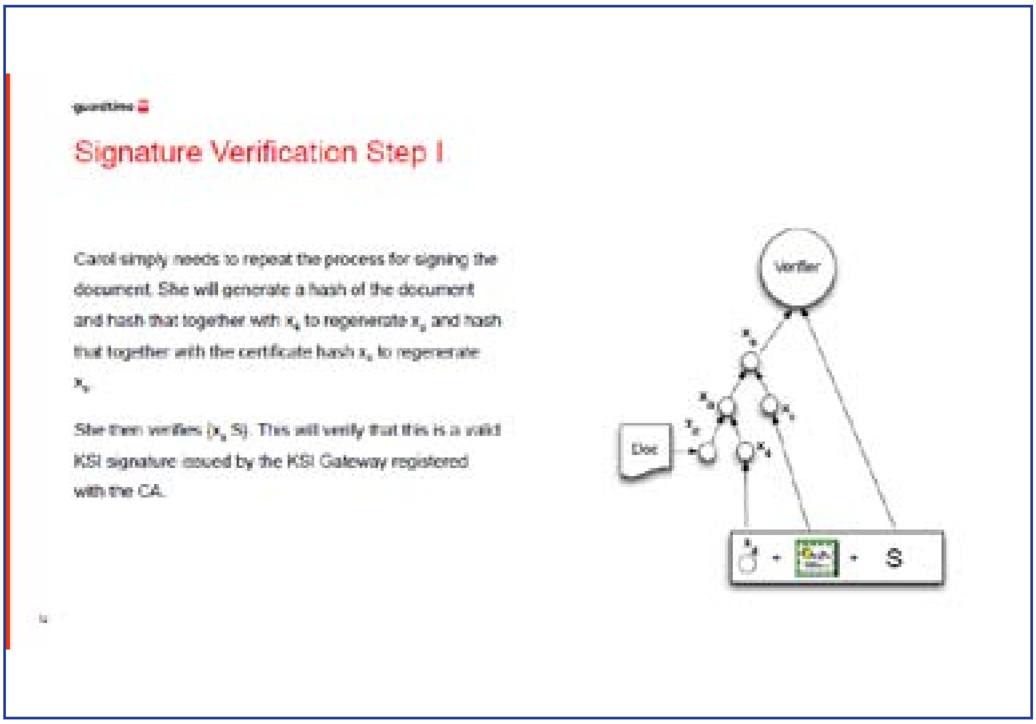


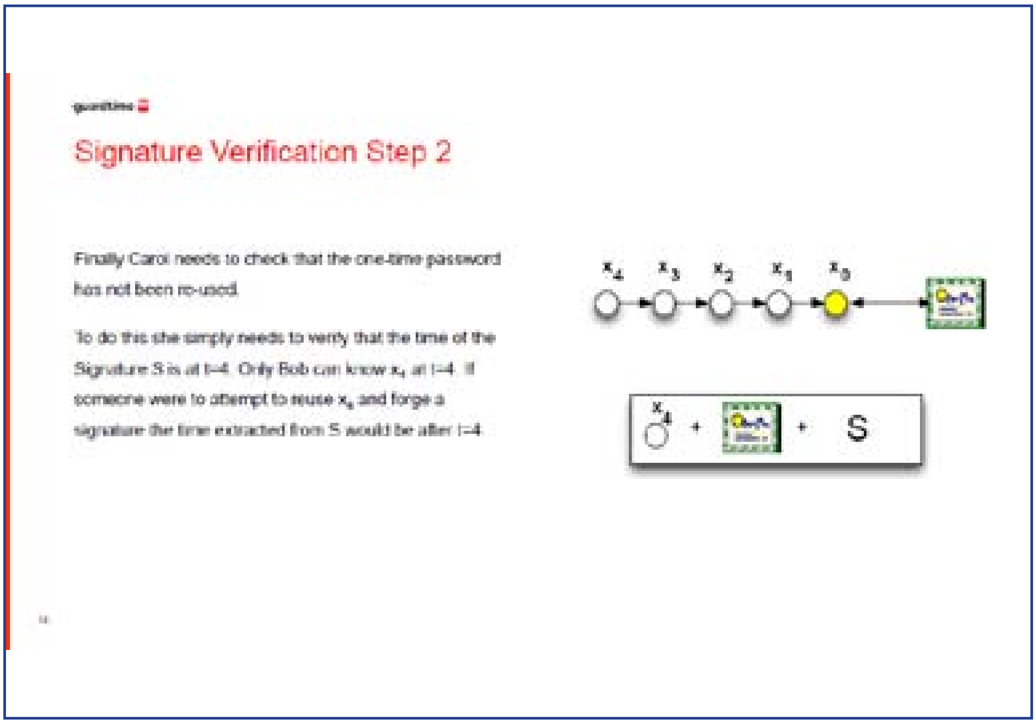


ISBN 979-10-92620-04-7

Presentations

SESSION 5
INDUSTRY





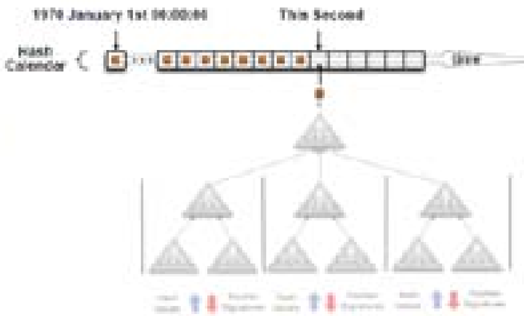
ISBN 979-10-92620-04-7

guardtime

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.



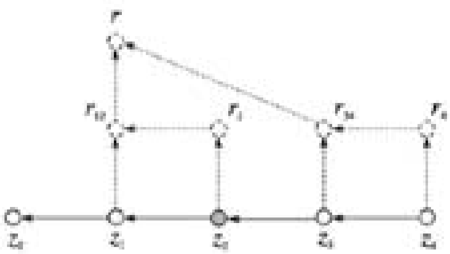
guardtime

Optimizations

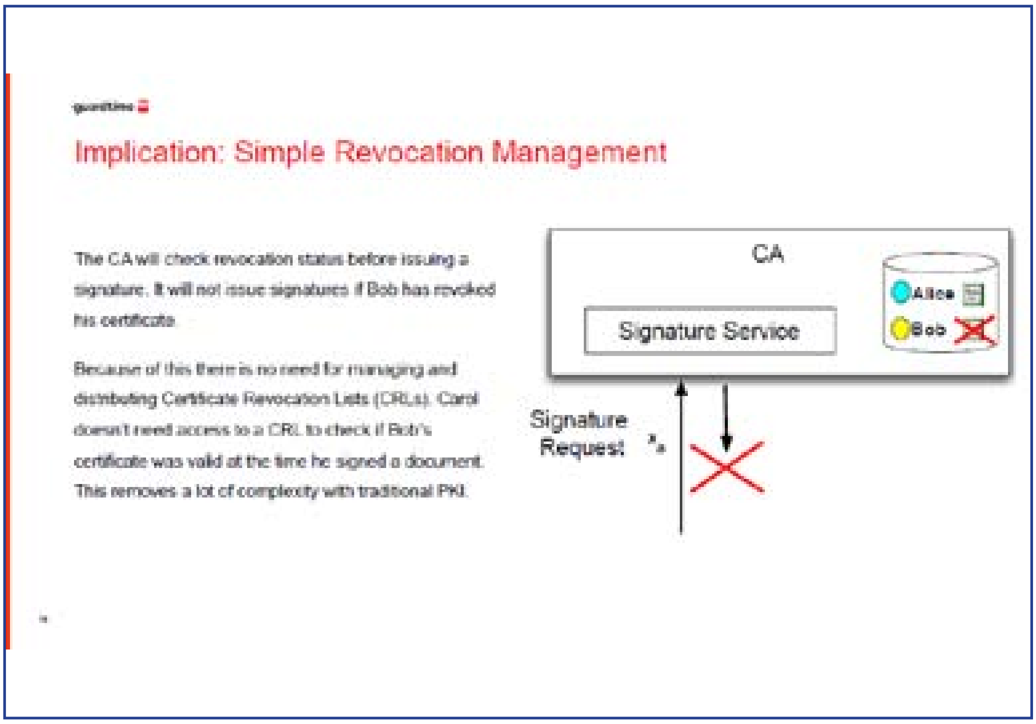
Signature verification complexity $O(t)$ is not acceptable.

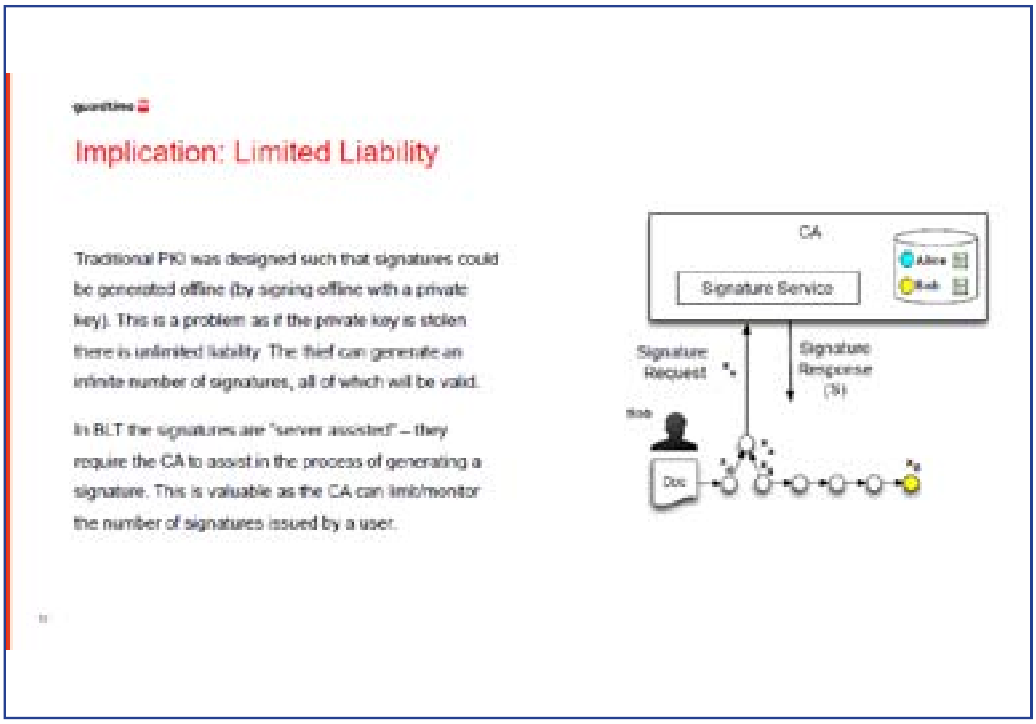
Hash-tree built on top of one-time password chain allows to create compact proofs, reducing verification time to: $O(\log(t))$.

Jakobsson's pebbles reduce chain+tree storage to $O(\log^2(t))$ and next password generation to $O(\log^2(t))$.



ISBN 979-10-92620-04-7





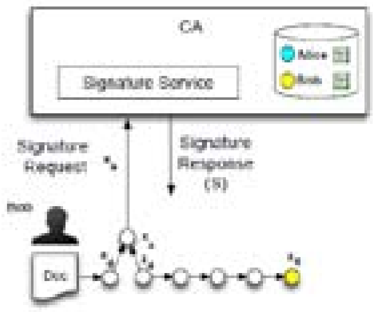
ISBN 979-10-92620-04-7

guardtime

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_4 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_4 before t=4.



guardtime

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-timestamp after the time-stamping keys are rotated (typically 5 years).

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

ISBN 979-10-92620-04-7

guardtime

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)

guardtime

Summary

	PKI (RSA)	KSI (BLT)
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

ISBN 979-10-92620-04-7


guardtime
B L T
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/2014/696

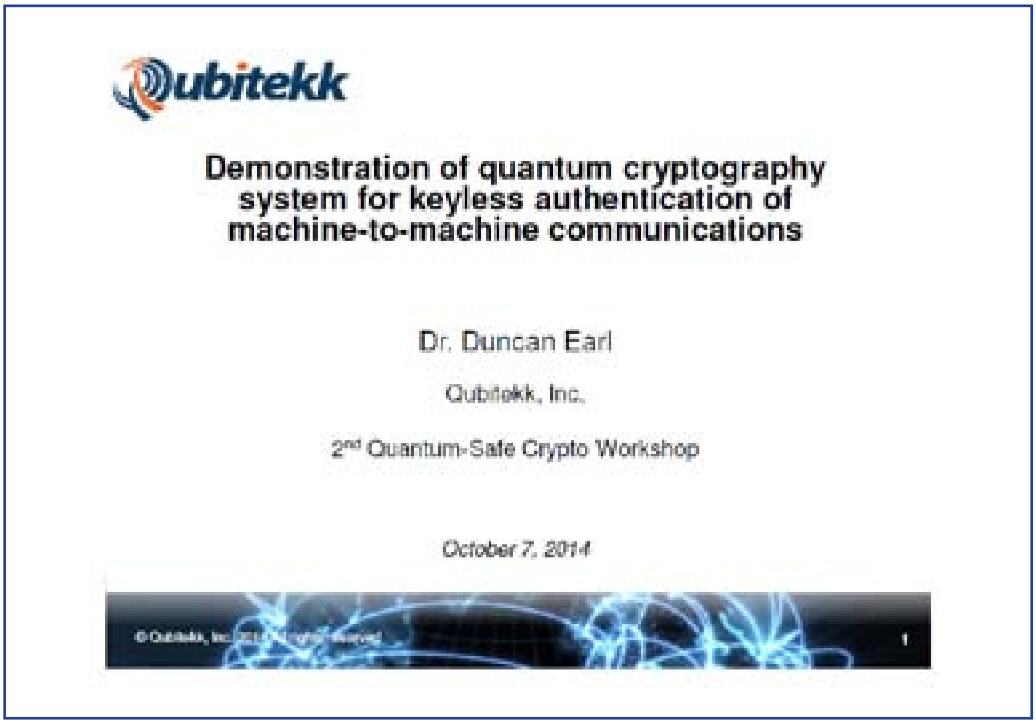
Presentations

SESSION 5
INDUSTRY

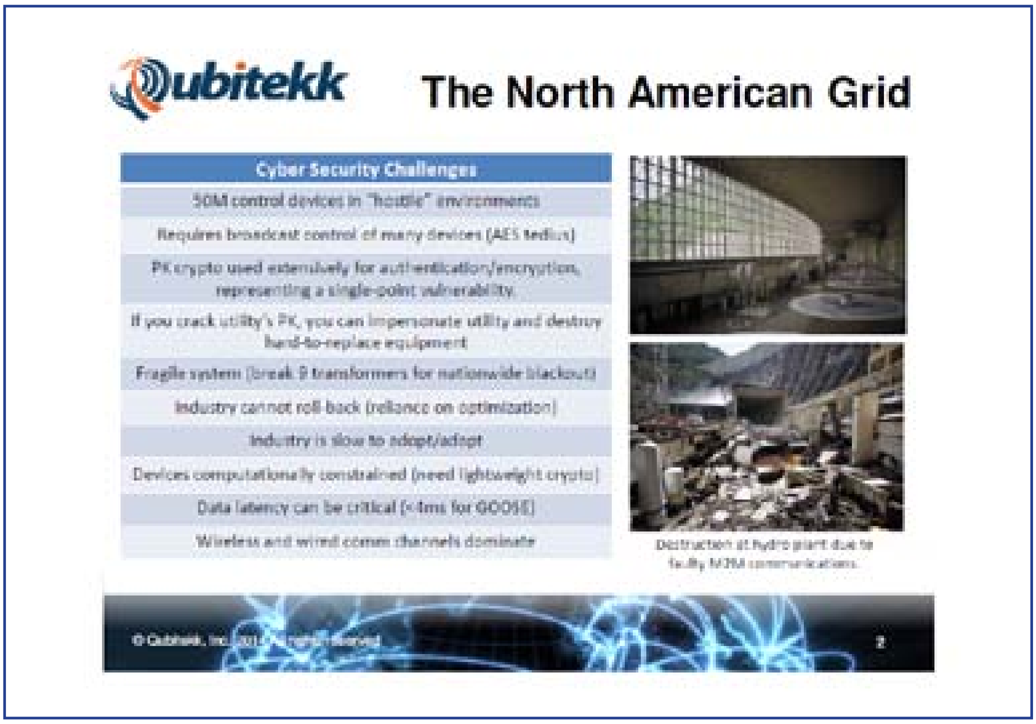
Demonstration of quantum cryptography system for keyless authentication of machichine-to-machine communications

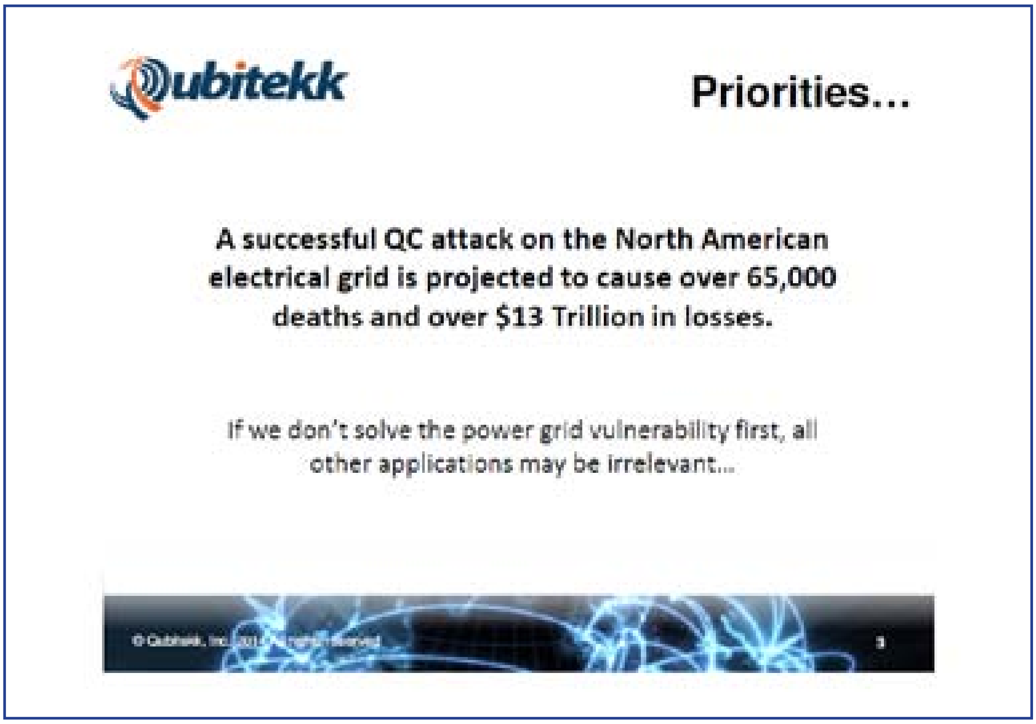
Duncan Earl, Qubitekk Inc.

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.

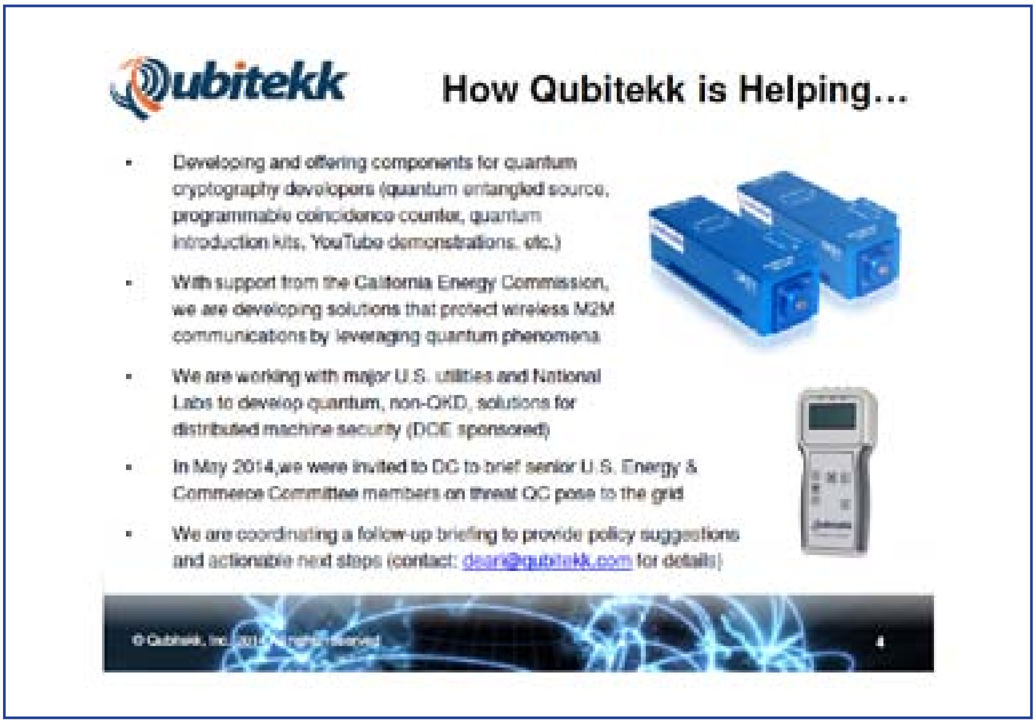


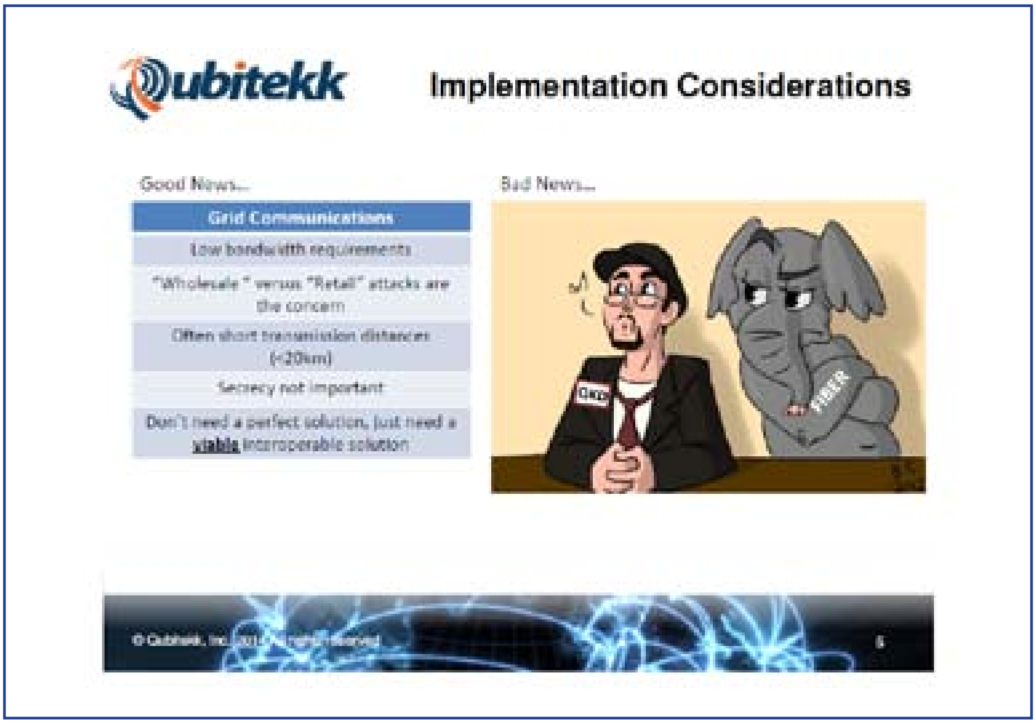
ISBN 979-10-92620-04-7



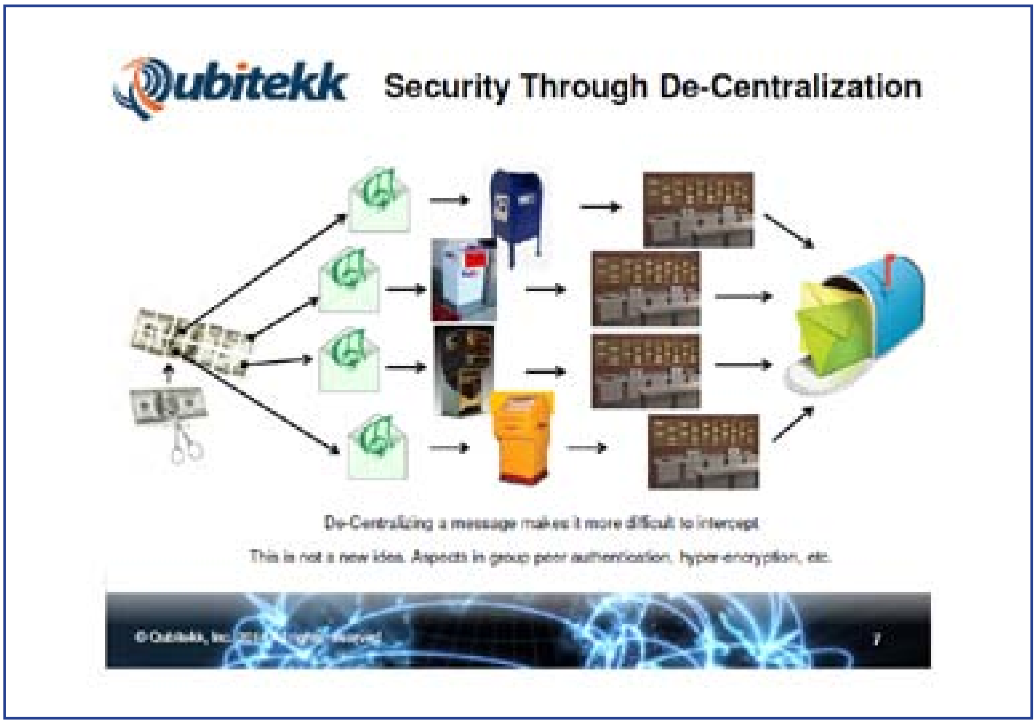


ISBN 979-10-92620-04-7

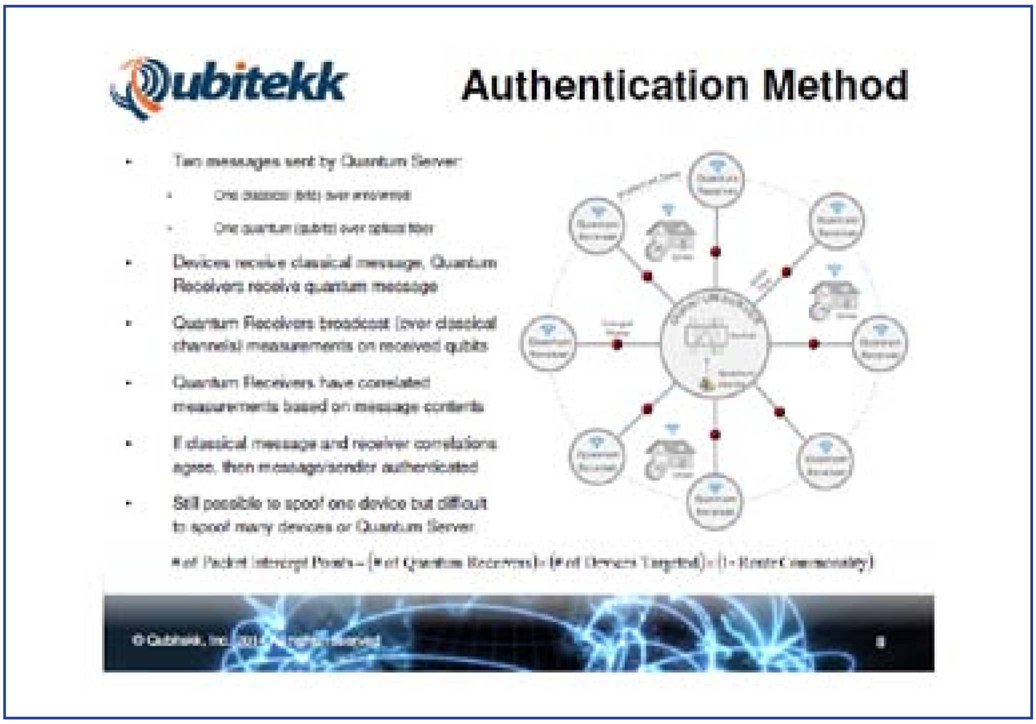


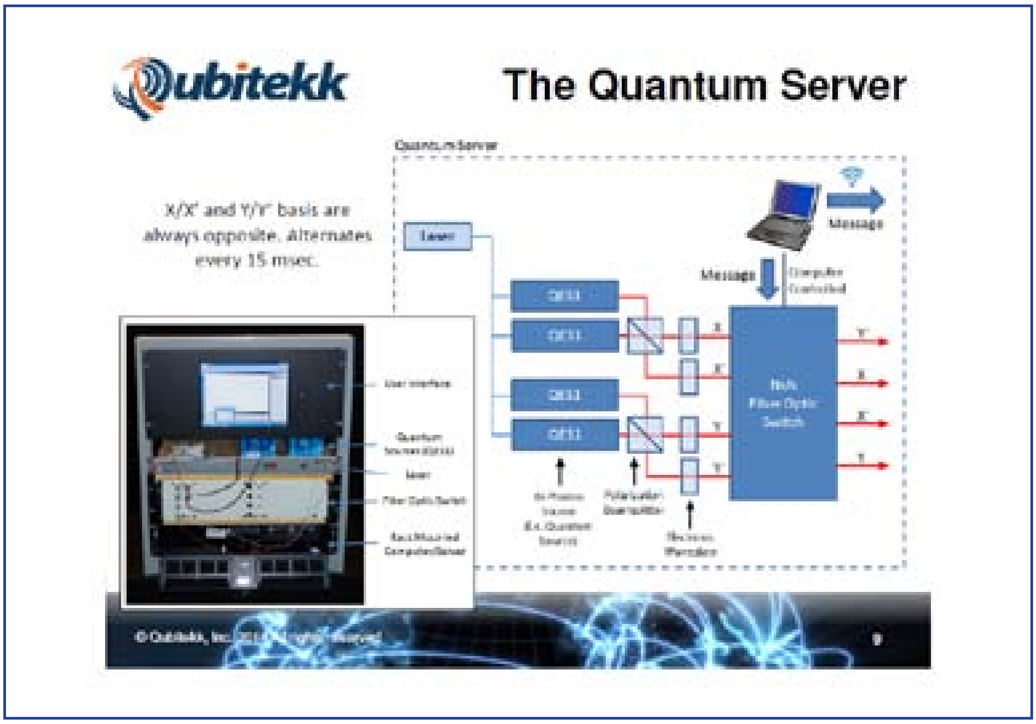


ISBN 979-10-92620-04-7

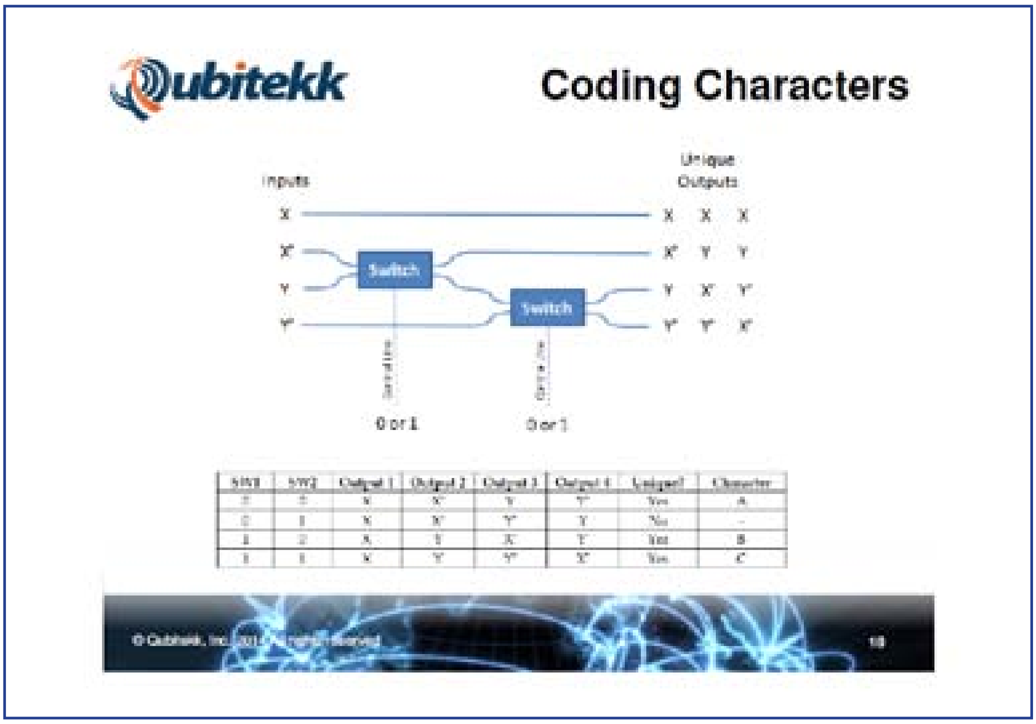


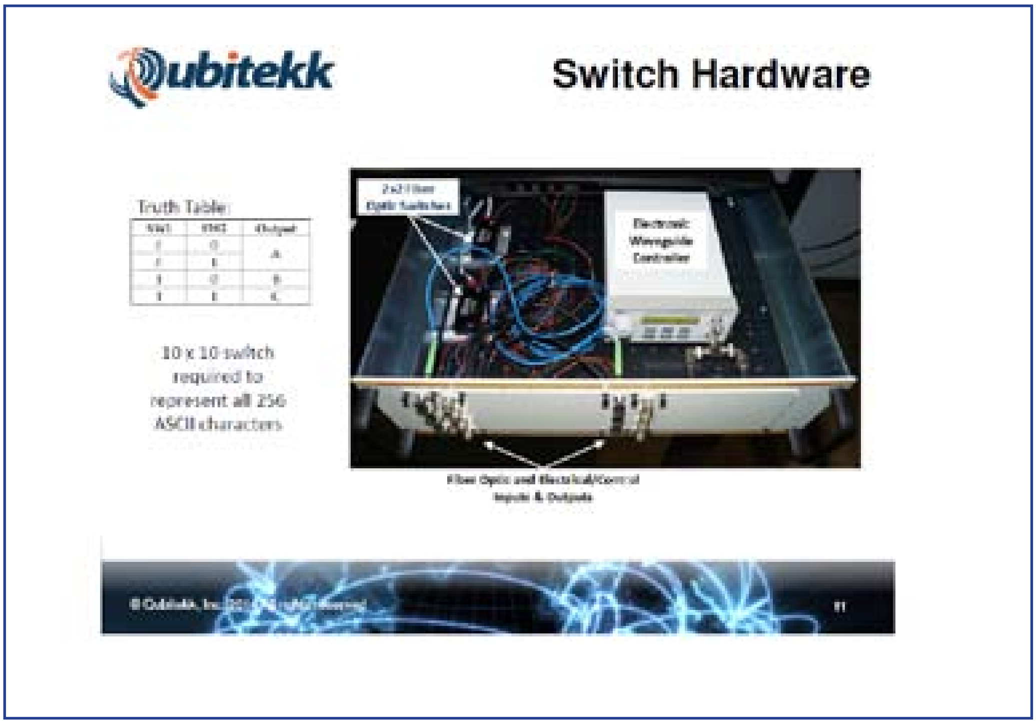
ISBN 979-10-92620-04-7





ISBN 979-10-92620-04-7

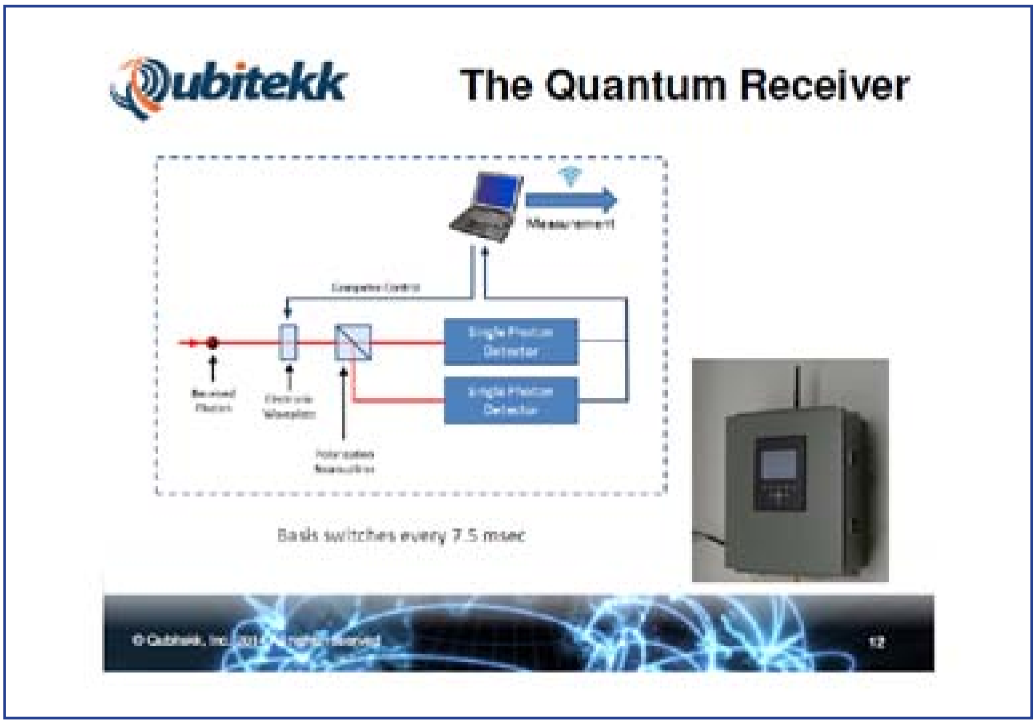


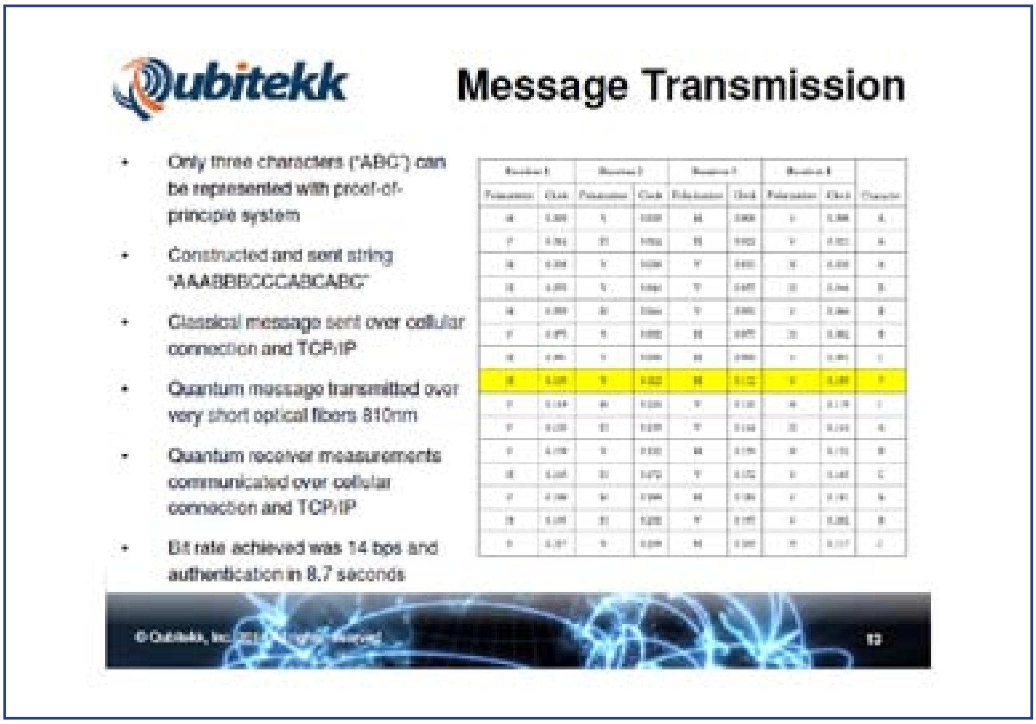


ISBN 979-10-92620-04-7

Presentations

SESSION 5
INDUSTRY





ISBN 979-10-92620-04-7

Qubitekk

Summary

- Proof-of-principle demonstration successful but very simplified (required polarization pre-correction, global triggering/timing, etc.) and used slow connections
- Multiple photon value measurements (per basis selection) had to be made and post-sifted to compensate for low detector efficiency (~52%)
- Message needed to be repeated to gain confidence
- System did securely authenticate messages without requiring secret key or assume computational complexity
- Bit rates can be improved to 27 kbps with minor changes
- At 27 kbps, 80 bit messages can be authenticated in less than 4 msec (meets data latency targets)
- Approach is a new way to apply quantum phenomena to message authentication
- For larger numbers of Quantum Receivers, one fiber can remain inside Quantum Server . This makes the Quantum Server "Alice" and some random Quantum Receiver "Bob" and traditional QKD can be performed between the two for tamper detection.

 14

Qubitekk

Contact Us

Contact Info:

Duncan Earl
Phone: 865-599-5233
dearl@qubitekk.com
www.qubitekk.com

 15

ISBN 979-10-92620-04-7

Testing Quantum Crypto

Vadim Makarov, Institute for Quantum Computing, University of Waterloo

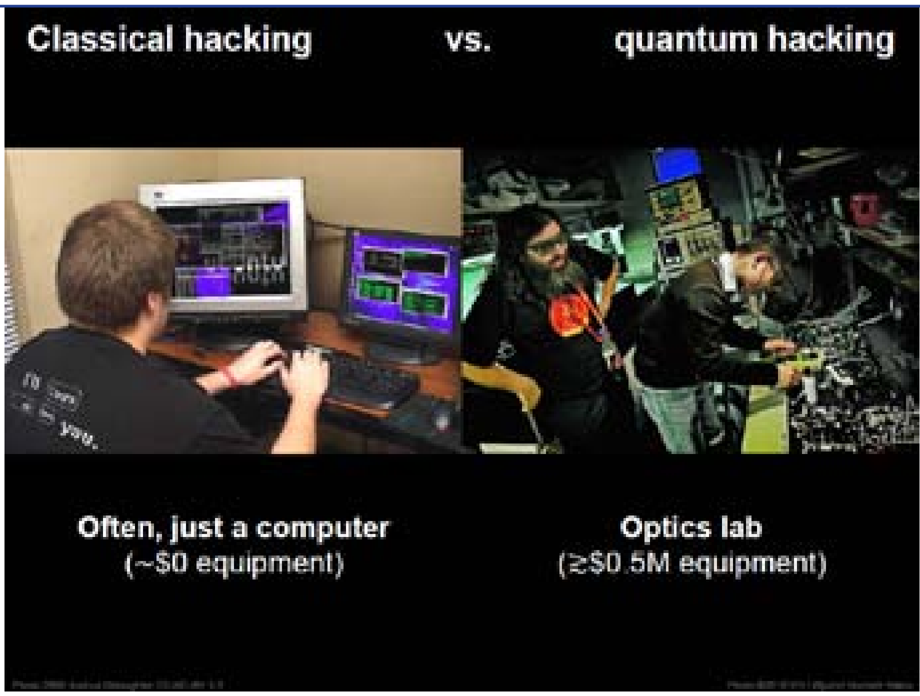
Cryptography:	classical	vs. quantum
Based on...	Unproven mathematical assumptions	Laws of physics
Convenient to implement?	Yes	No
Forward secure?	No	Yes
Authenticate via PKI?	Yes	Yes
Loopholes in implementations?	Yes	

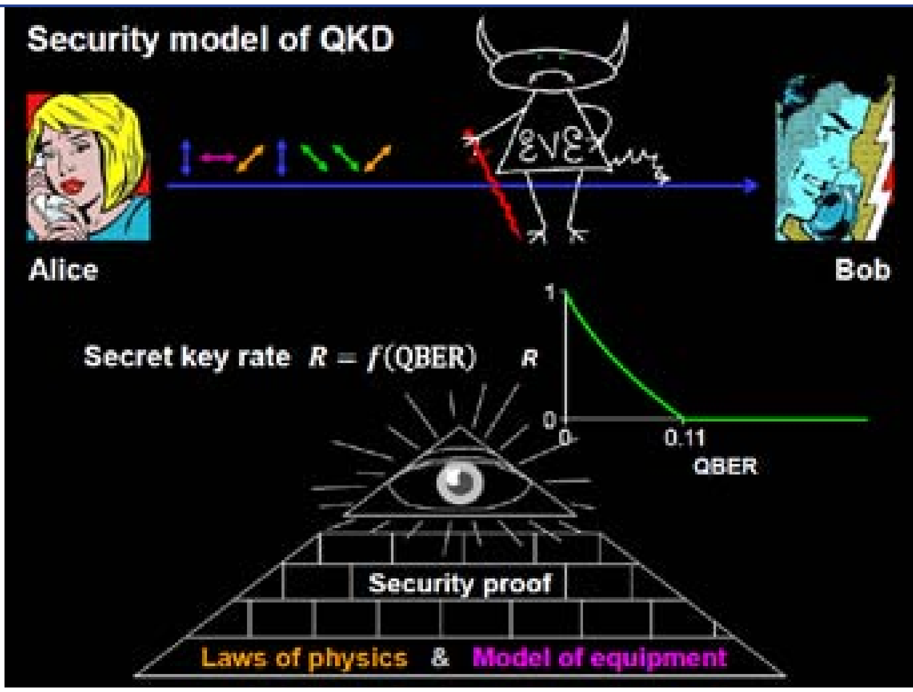
ISBN 979-10-92620-04-7

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*

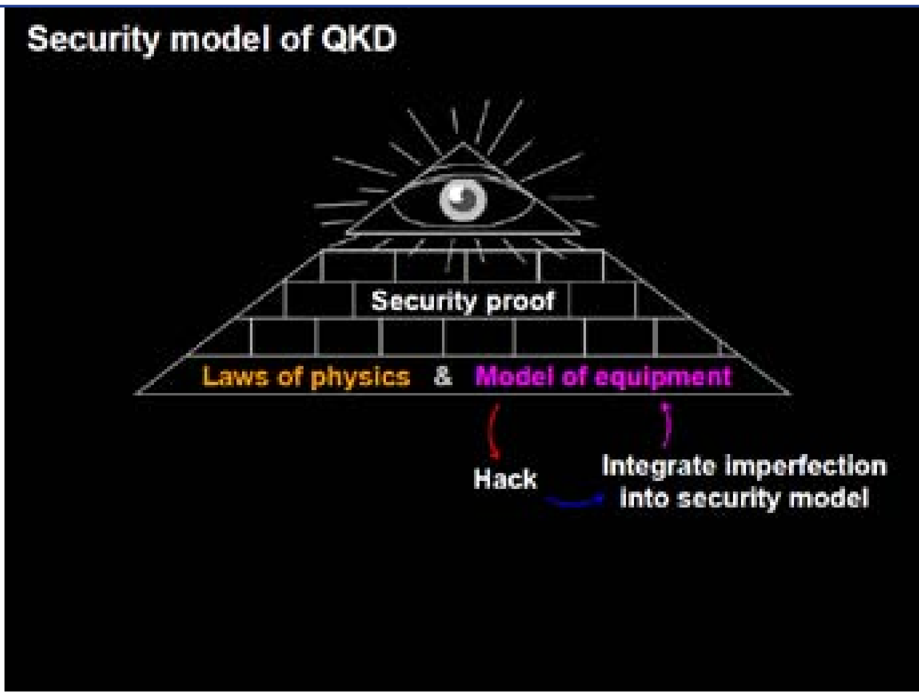
* Single exception: A. Lamas-Linares & C. Kurtsiefer, Opt. Express 15, 9388 (2007)

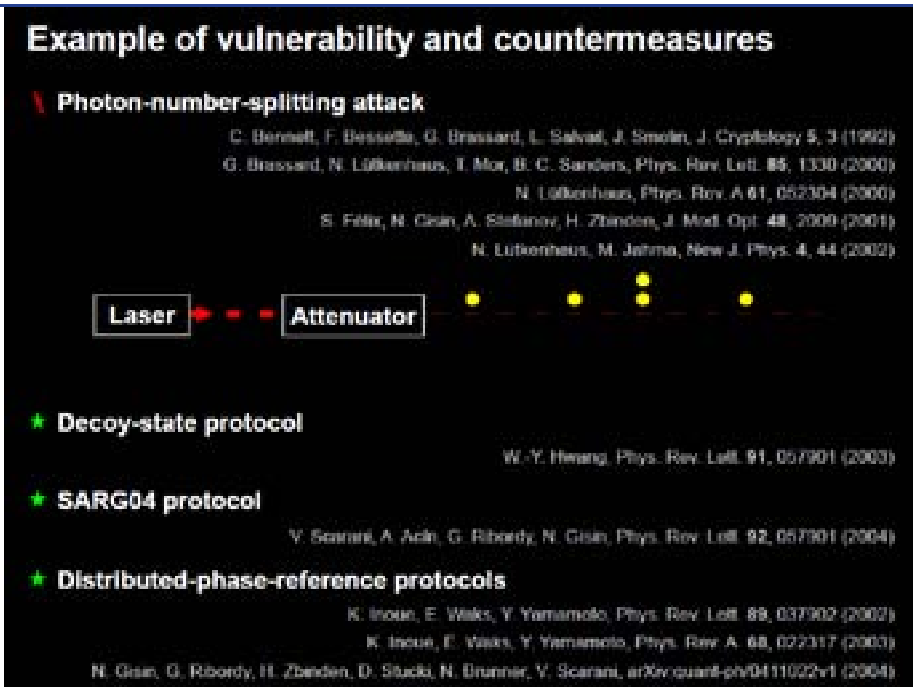
ISBN 979-10-92620-04-7





ISBN 979-10-92620-04-7





ISBN 979-10-92620-04-7

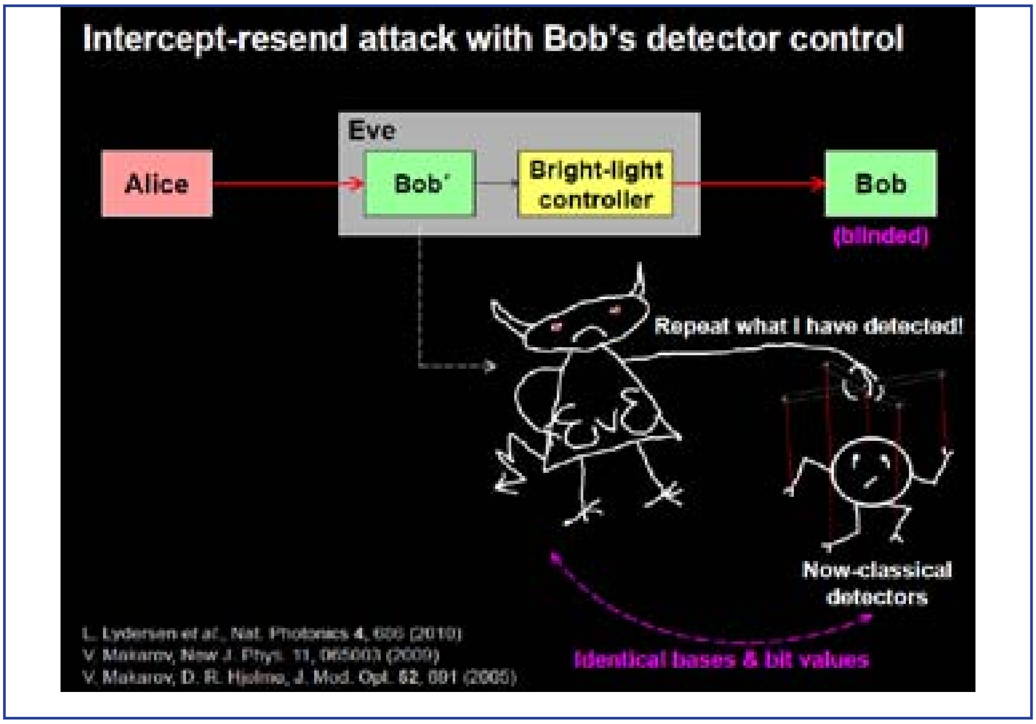
Attack	Target component	Tested system
Pulse energy calibration S. Sajeed *et al.*, presentation at QCrypt (2014)	classical watchdog detector	ID Quantique
Trojan-horse I. Khan *et al.*, presentation at QCrypt (2014)	phase modulator in Alice	SeQureNet
Trojan-horse N. Jain *et al.*, arXiv 1406.5813	phase modulator in Bob	ID Quantique*
Detector saturation H. Qin, R. Kumar, R. Alléaume, presentation at QCrypt (2013)	homodyne detector	SeQureNet
Shot-noise calibration P. Jouguet, S. Kunz-Jacques, E. Diamanti, Phys. Rev. A 87, 062313 (2013)	classical sync detector	SeQureNet
Wavelength-selected PNS M.-S. Jiang, S.-H. Sun, C.-Y. Li, L.-M. Liang, Phys. Rev. A 86, 032310 (2012)	intensity modulator	(theory)
Multi-wavelength H.-W. Li *et al.*, Phys. Rev. A 84, 062308 (2011)	beamsplitter	research syst.
Deadtime H. Weier *et al.*, New J. Phys. 13, 073024 (2011)	single-photon detector	research syst.
Channel calibration N. Jain *et al.*, Phys. Rev. Lett. 107, 110501 (2011)	single-photon detector	ID Quantique
Faraday-mirror S.-H. Sun, M.-S. Jiang, L.-M. Liang, Phys. Rev. A 83, 062331 (2011)	Faraday mirror	(theory)
Detector control I. Gerhardt *et al.*, Nat. Commun. 2, 349 (2011); L. Lydersen *et al.*, Nat. Photonics 4, 686 (2010)	single-photon detector	ID Quantique, MagiQ, research syst.
Phase-remapping F. Xu, B. Qi, H.-K. Lo, New J. Phys. 12, 113026 (2010)	phase modulator in Alice	ID Quantique*
Time-shift Y. Zhao *et al.*, Phys. Rev. A 78, 042333 (2008)	single-photon detector	ID Quantique

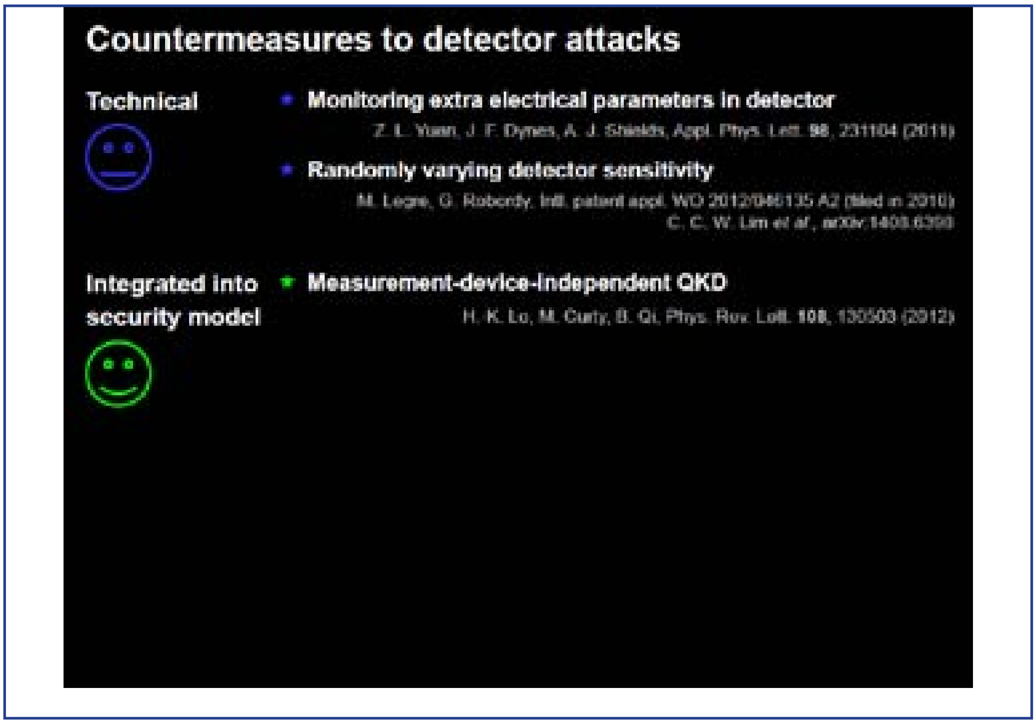
* Attack did not break security of the tested system, but may be applicable to a different implementation

Attack	Target component	Tested system
Pulse energy calibration S. Sajeed *et al.*, presentation at QCrypt (2014)	classical watchdog detector	ID Quantique
Trojan-horse I. Khan *et al.*, presentation at QCrypt (2014)	phase modulator in Alice	SeQureNet
Trojan-horse N. Jain *et al.*, arXiv 1406.5813	phase modulator in Bob	ID Quantique*
Detector saturation H. Qin, R. Kumar, R. Alléaume, presentation at QCrypt (2013)	homodyne detector	SeQureNet
Shot-noise calibration P. Jouguet, S. Kunz-Jacques, E. Diamanti, Phys. Rev. A 87, 062313 (2013)	classical sync detector	SeQureNet
Wavelength-selected PNS M.-S. Jiang, S.-H. Sun, C.-Y. Li, L.-M. Liang, Phys. Rev. A 86, 032310 (2012)	intensity modulator	(theory)
Multi-wavelength H.-W. Li *et al.*, Phys. Rev. A 84, 062308 (2011)	beamsplitter	research syst.
Deadtime H. Weier *et al.*, New J. Phys. 13, 073024 (2011)	single-photon detector	research syst.
Channel calibration N. Jain *et al.*, Phys. Rev. Lett. 107, 110501 (2011)	single-photon detector	ID Quantique
Faraday-mirror S.-H. Sun, M.-S. Jiang, L.-M. Liang, Phys. Rev. A 83, 062331 (2011)	Faraday mirror	(theory)
Detector control I. Gerhardt *et al.*, Nat. Commun. 2, 349 (2011); L. Lydersen *et al.*, Nat. Photonics 4, 686 (2010)	single-photon detector	ID Quantique, MagiQ, research syst.
Phase-remapping F. Xu, B. Qi, H.-K. Lo, New J. Phys. 12, 113026 (2010)	phase modulator in Alice	ID Quantique*
Time-shift Y. Zhao *et al.*, Phys. Rev. A 78, 042333 (2008)	single-photon detector	ID Quantique

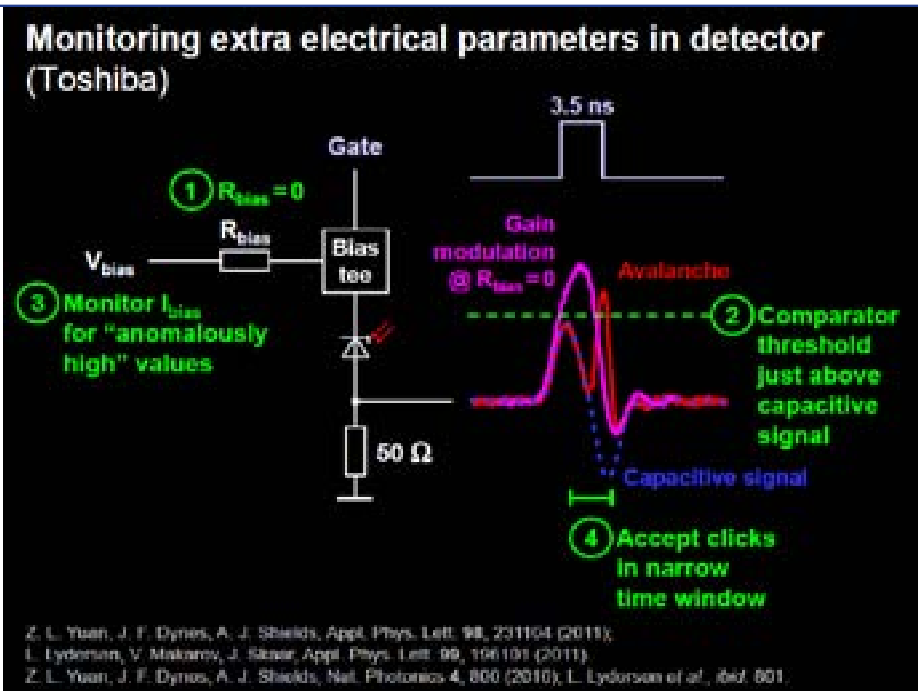
* Attack did not break security of the tested system, but may be applicable to a different implementation

ISBN 979-10-92620-04-7





ISBN 979-10-92620-04-7



I: Can we test your detector?

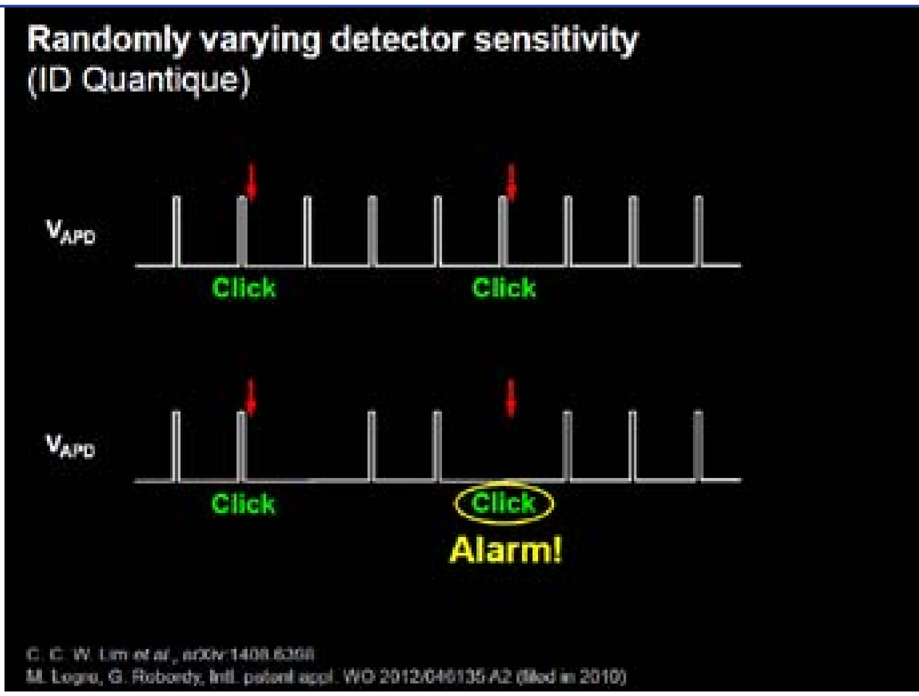
Toshiba: No.

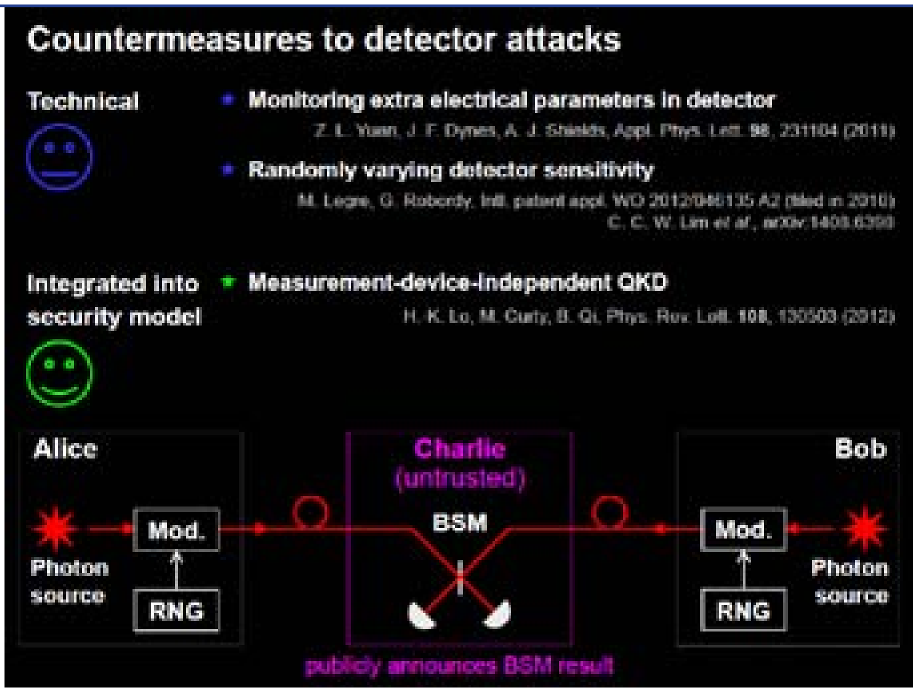
I: Why not?

Toshiba: Still no.

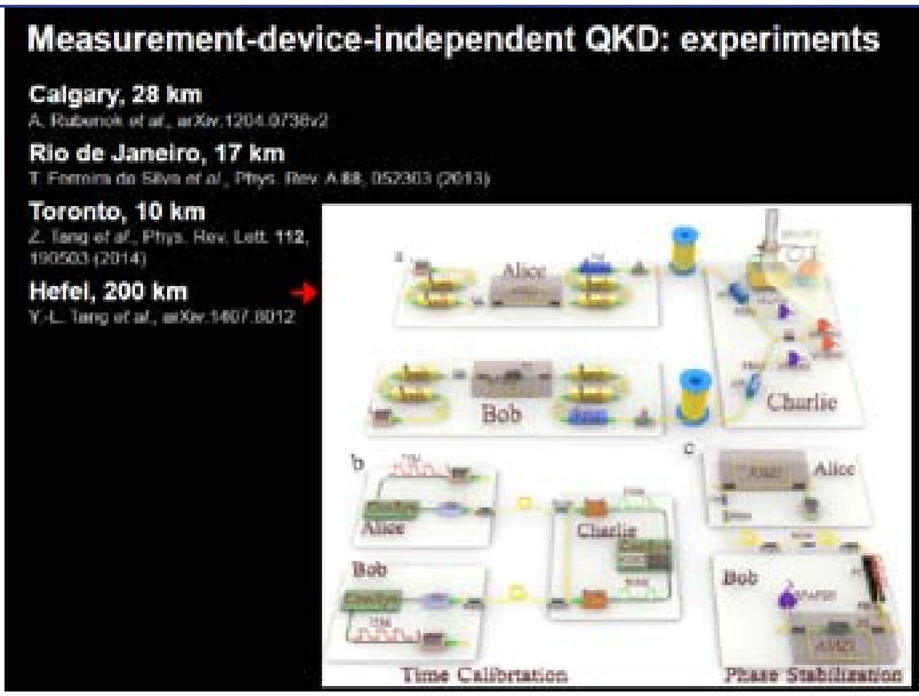
Chinese way: build a copy and hack it.

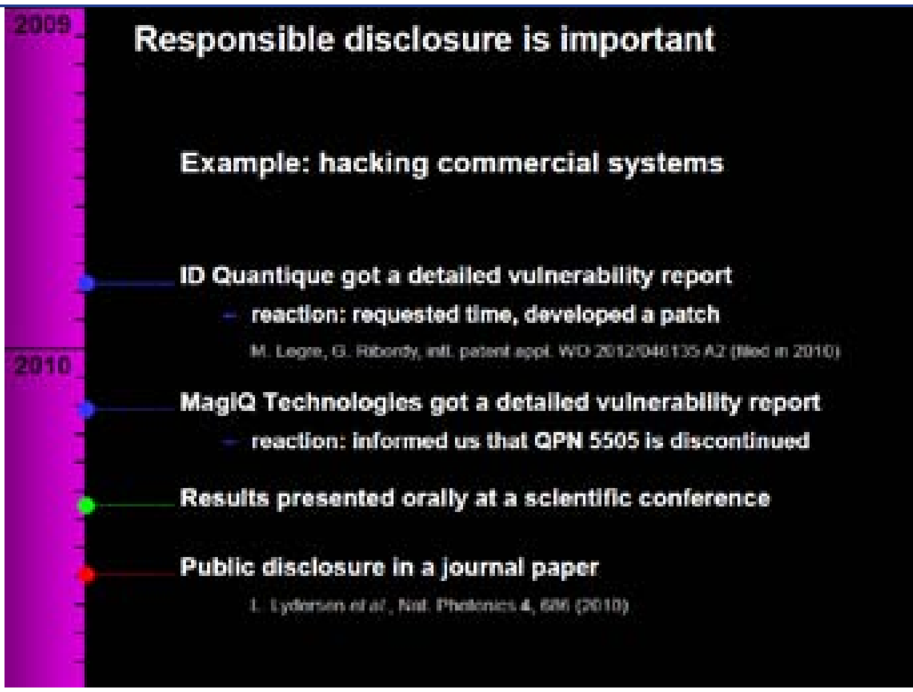
M.-S. Jiang *et al.*, Phys. Rev. A 88, 062335 (2013)

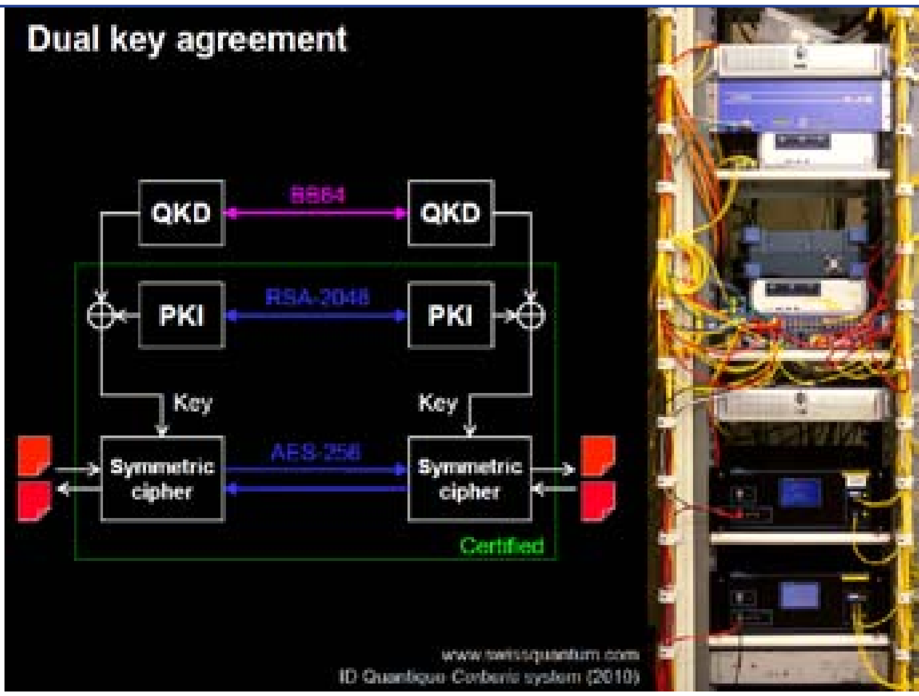




ISBN 979-10-92620-04-7


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
Alice
Bob
Charlie
Time Calibration
Phase Stabilization


2009
2010
Responsible disclosure is important
Example: hacking commercial systems
ID Quantique got a detailed vulnerability report
– reaction: requested time, developed a patch
M. Legre, G. Ribordy, intl. patent appl. WO 2012/046135 A2 (filed in 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)



ISBN 979-10-92620-04-7

Codes for security against computationally unbounded adversaries

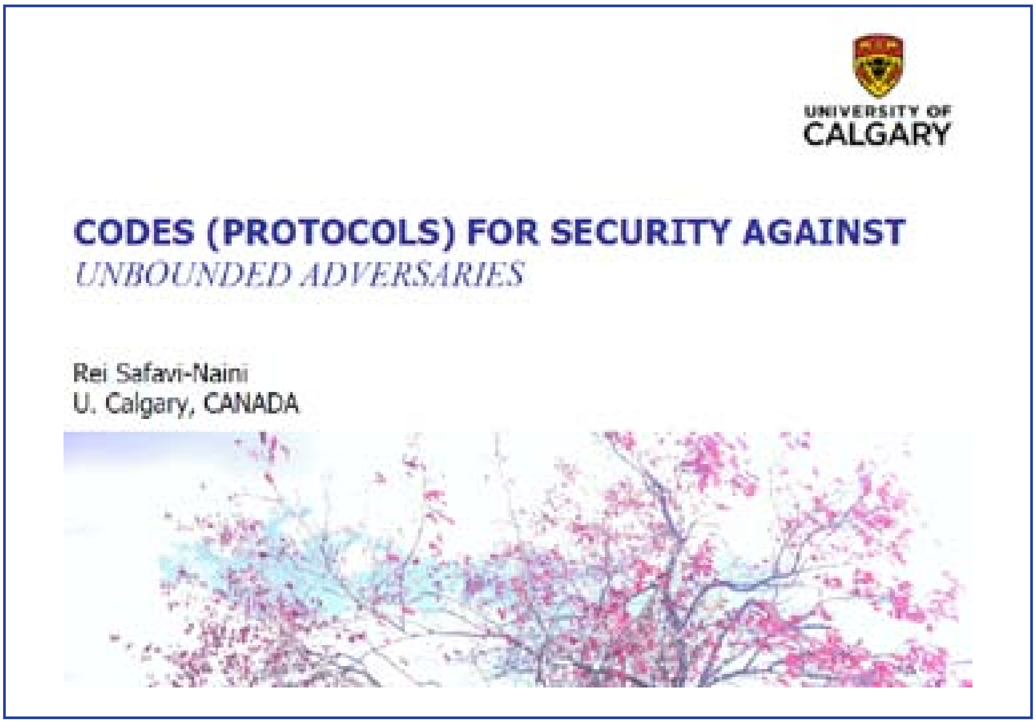
Rei Safavi-Naini, University of Calgary

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.

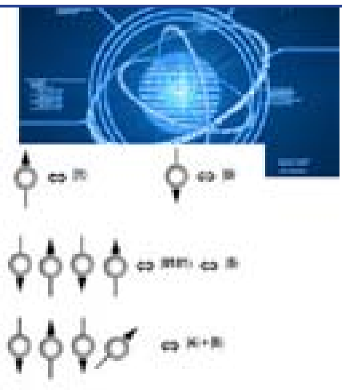
[1] http://www.nucrypt.net/noise-based-physical-layer-encryption.html



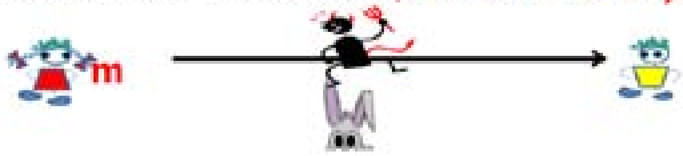
ISBN 979-10-92620-04-7

It is year 2030....

Q-computers are up and running....



Alice wants to send a private message to Bob.



Alice & Bob's options..

Quantum cryptography

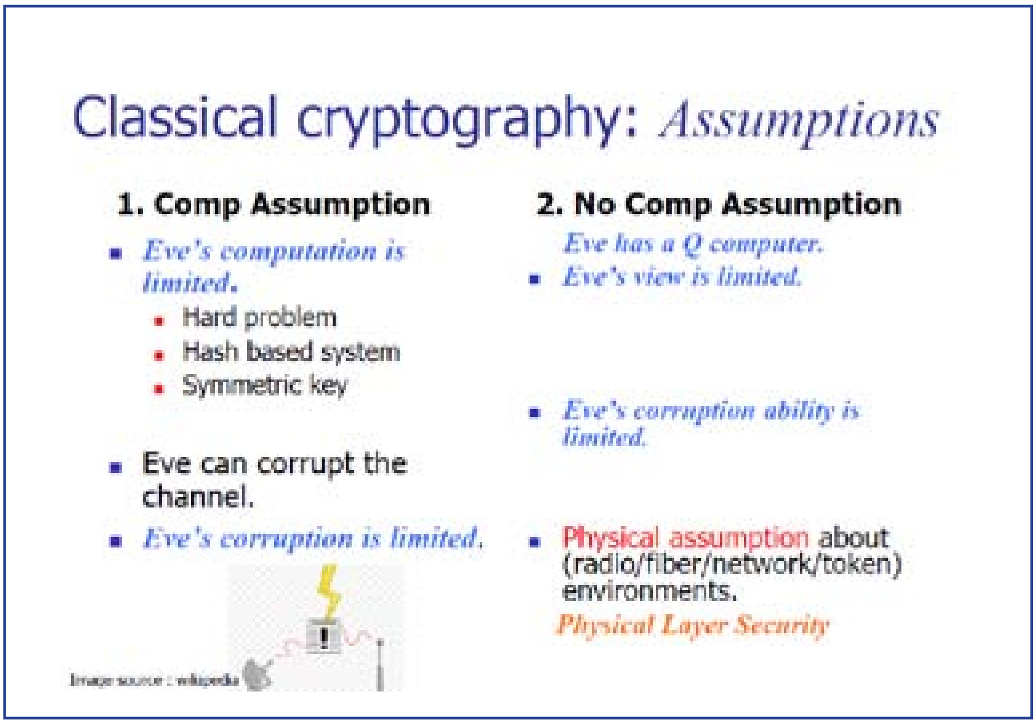
1. Qubits
   - *Physical (quantum) assumption*
   - Implementation challenges
     - Side-channels
     - Trojan horse attack

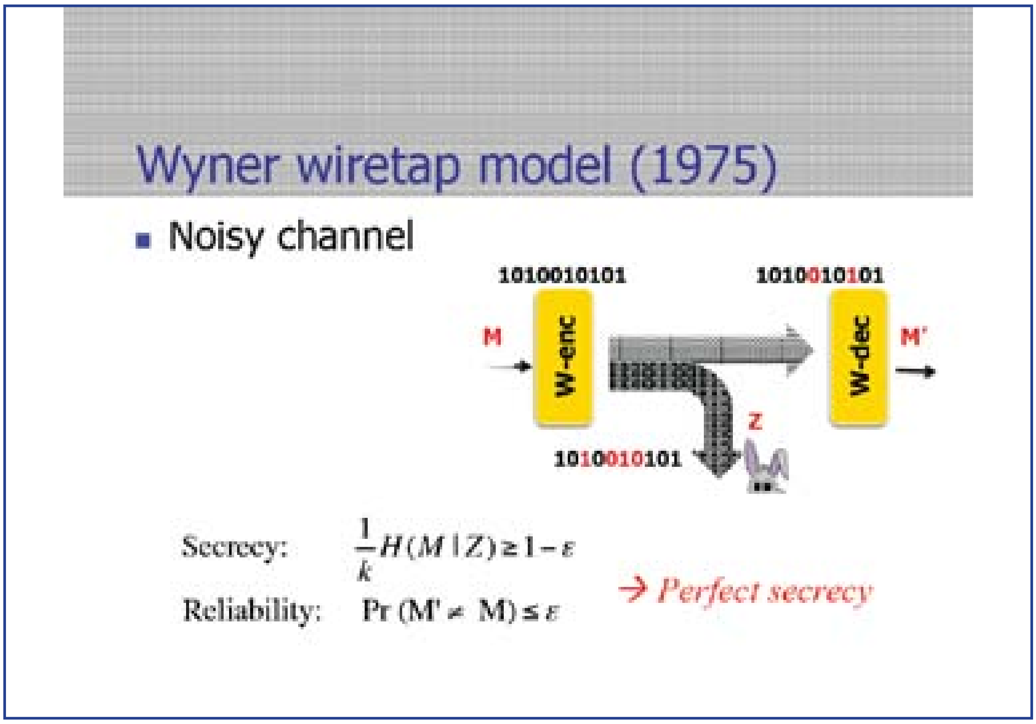
   →Estimating adversary

Classical cryptography

1. Computational assumption
2. No computational assumption

ISBN 979-10-92620-04-7

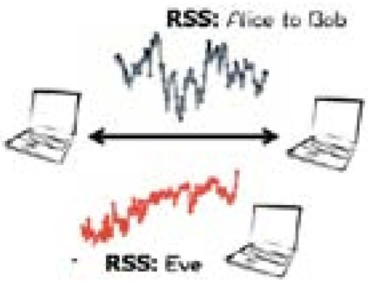




ISBN 979-10-92620-04-7

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 comes 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"

NuCrypt

ISBN 979-10-92620-04-7

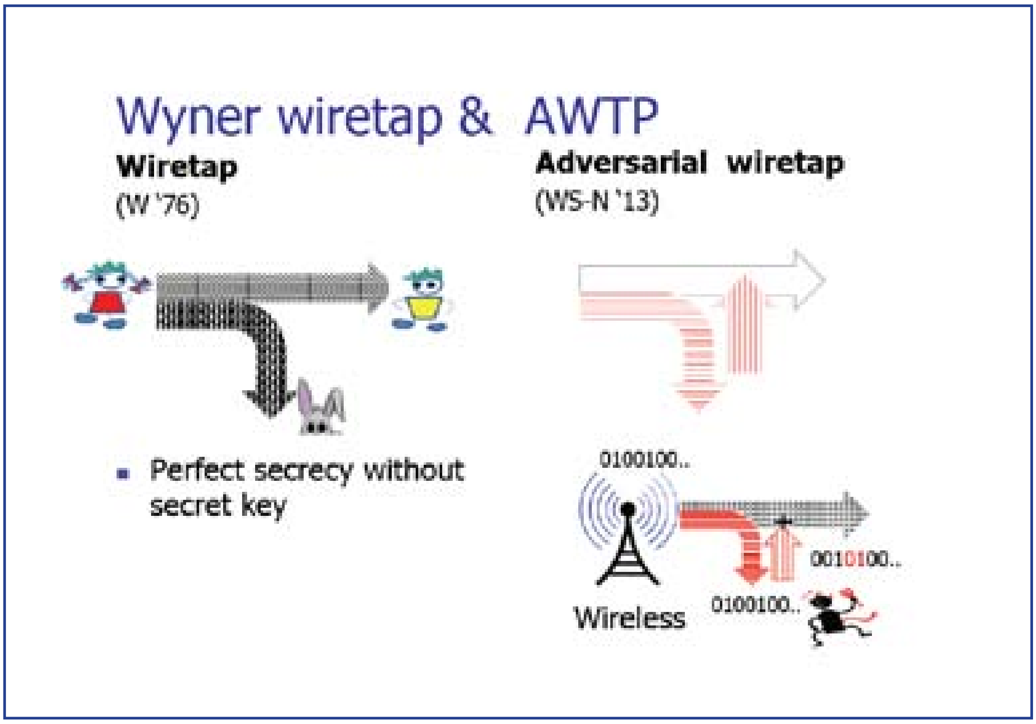
Summary: *Post-quantum Crypto*

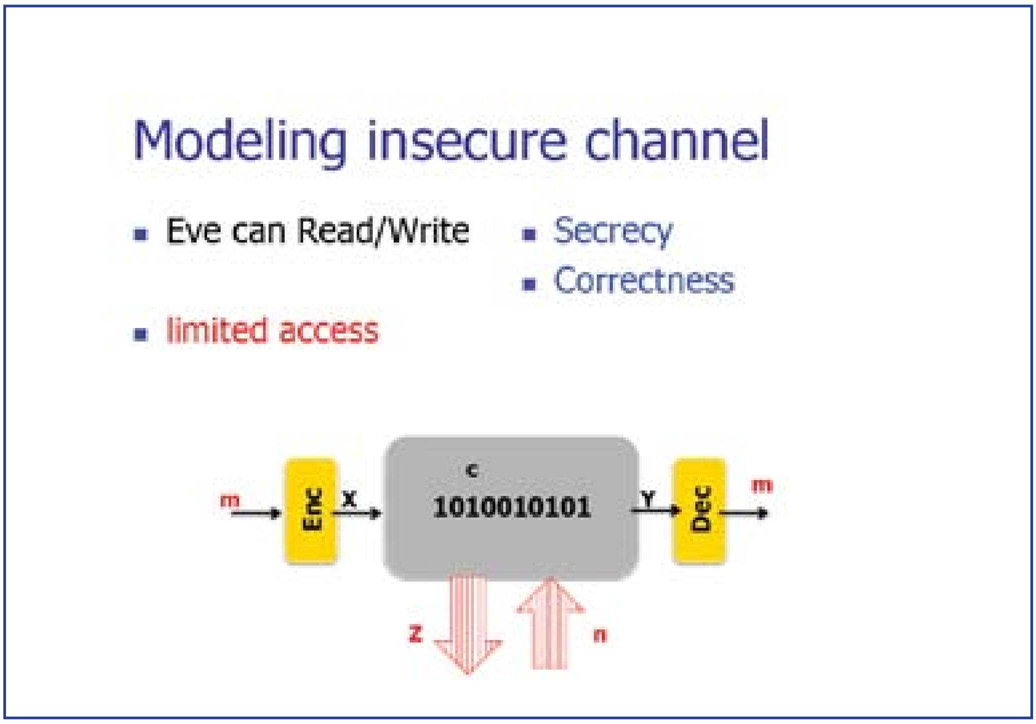
	Q-Crypto	Classical			
		PhyLayer	Hash	Symm	Hard Prob
Assum	Phys	Phys	Comp	Comp	Comp
Proof/Reduc	Yes	Yes	No	No	Yes

Rest of the talk

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

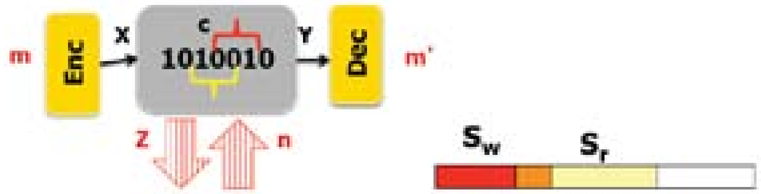
ISBN 979-10-92620-04-7


Wyner wiretap & AWTP
Wiretap
(W '76)
Adversarial wiretap
(WS-N '13)
Perfect secrecy without secret key
0100100..
0010100..
Wireless
0100100..


Modeling insecure channel
Eve can Read/Write
Secrecy
Correctness
limited access
m
Enc
X
c
1010010101
Y
Dec
m
z
n

Adversarial wiretap

Private & Reliable communication



- Encoder:
  Enc: M × R ⟶ Σ^N
- Decoder:
  Dec: Σ^N ⟶ M

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

$$SD(V_A(m_1,r);V_A(m_1,r)) \le \varepsilon$$

$$\Pr(M' \ne M) \le \delta$$

$$SD(X;Y) = \sum_{v} |\Pr(X = v) - \Pr(y = v)|$$

AWTP: *Efficiency*

- Information rate of a code

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

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

- Encoding/Decoding complexity

ISBN 979-10-92620-04-7

Rate bound & Capacity

- Bound

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

- 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

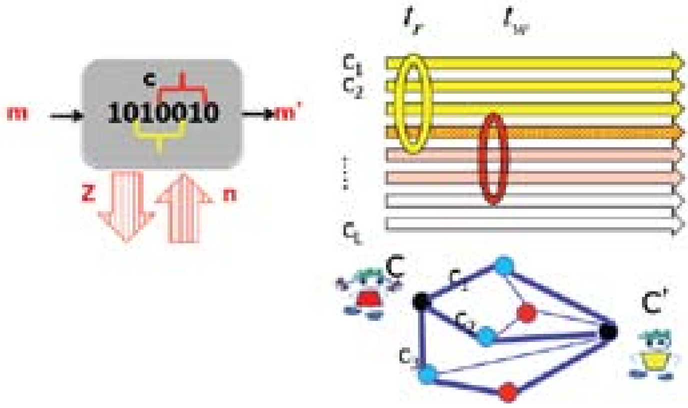
$$\text{AWTPenc} = FRS(SESenc(AMD(m) \| [0]_g) \| [r]_{u\rho,L})$$

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

ISBN 979-10-92620-04-7

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

ISBN 979-10-92620-04-7

Related publications

- Wang, Safavi-Naini,, *Adversarial wiretap with Public Discussions*, CNS 2014
- Ahmad, 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 (0, δ)-Secure Message Transmission against Generalized Adversary* AFRICACRYPT 2012
- Safavi-Naini, Tuhin & Wang, *A General Construction for 1-round δ-RMT and (0-δ)-SMT*, ACNS 2012.
- Tuhin, Safavi-Naini, *Optimal One Round Almost Perfectly Secure Message Transmission*, FC'11
- 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?*

ISBN 979-10-92620-04-7

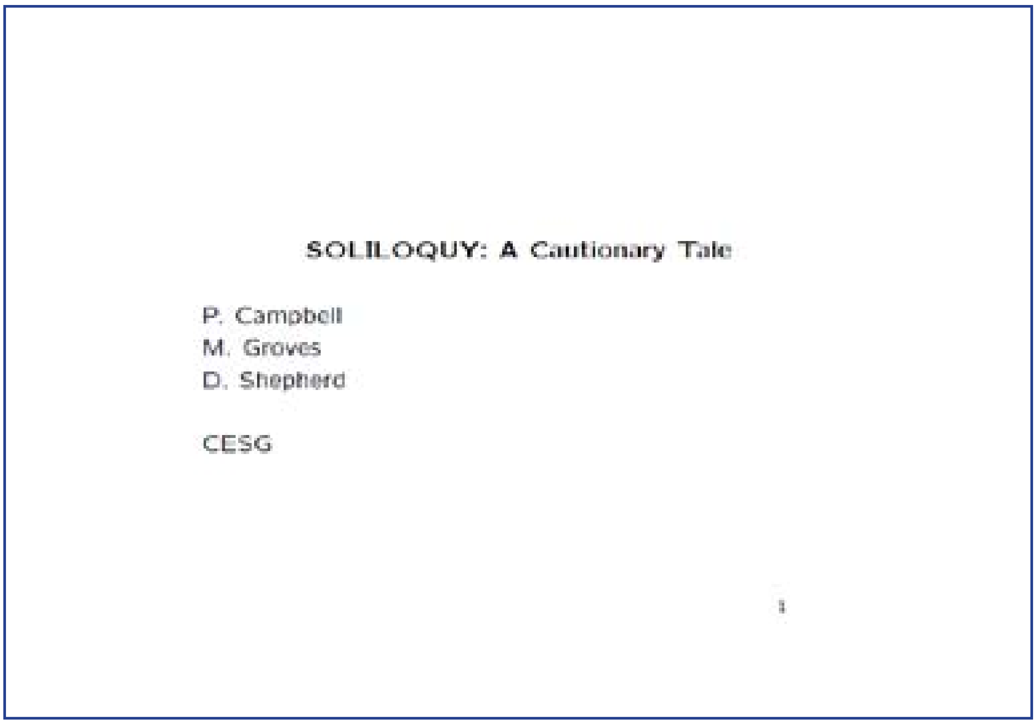
SOLILOQUY: A Cautionary Tale

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.



ISBN 979-10-92620-04-7

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

ISBN 979-10-92620-04-7

Some mathematical background

Let n be a prime and ζ a primitve 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 $\alpha = \sum_{i=1}^{n} a_i \zeta^i \in \mathcal{O}$.

For primes $p \equiv 1 \bmod n$ 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 $Gal(K/\mathbb{Q}) \approx (\mathbb{Z}/n\mathbb{Z})^\times$. They have a simple two-element representation $\mathcal{P} = p\mathcal{O} + (\zeta - c_i)\mathcal{O}$, where the c_i are n^{th} roots of unity in $GF(p)$.

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

4

Public and private keys

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

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 $c \not\equiv 1 \bmod p$. Conjugate to get into the required form $\alpha\mathcal{O} = p\mathcal{O} + (\zeta - c)\mathcal{O}$.

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

5

ISBN 979-10-92620-04-7

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:

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

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

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

6

SOLILOQUY as a GGH-type lattice scheme

Private / public lattice basis matrices with $H = HNF(C)$:

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

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

ISBN 979-10-92620-04-7

ISBN 979-10-92620-04-7

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 $u_1, \ldots, u_{r-1}$ 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 $\log(\omega) = (\log(|\sigma_0(\omega)|), \ldots, \log(|\sigma_{r-1}(\omega)|))$ 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 $F : \mathbb{Z} \times \mathbb{R}^r \to \mathbb{R}^r$, such that $F(k, v) = F(k', v')$ iff $(k, v) \equiv (k', v') \bmod \Lambda_\alpha$.

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

ISBN 979-10-92620-04-7

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

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

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 superpositon 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 $E_n(\rho) := Ball_{n,\rho} \cdot B^{-1}$ in the sense that that it fits within an ellipsoid $E_n(\rho+\varepsilon)$ and covers all the integer points in $E_n(\rho-\varepsilon)$.

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

14

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

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

$$\mathbf{u} = \theta_B(\mathbf{v}) := \lceil q \cdot \mathbf{v} \cdot B \cdot O \rfloor.$$

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

15

ISBN 979-10-92620-04-7

Our (simple) quantum fingerprint generator computes

$$|k,v\rangle\,|0\rangle \mapsto \frac{1}{\sqrt{\lceil l \rceil}} \sum_{x=0}^{\lceil l \rceil - 1} |k,v\rangle \left|\theta_{B(k,v)}(\phi(x))\right\rangle$$

The pure state

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

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

The coherent randomised version is:

$$\left|\psi'_{(k,v)}\right\rangle := \frac{\sum_R \sum_{\mathrm{w}} \sum_{x=0}^{\lceil l \rceil - 1} |R\rangle\,|\mathrm{w}\rangle \left|\theta_{R,\mathrm{w},B(k,v)}(\phi(x))\right\rangle}{\sqrt{\#_R \cdot \#_{\mathrm{w}} \cdot \lceil l \rceil}}$$

16

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

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

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

ISBN 979-10-92620-04-7

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 suggesed using multiple Gaussian sampling.

19

ISBN 979-10-92620-04-7

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.

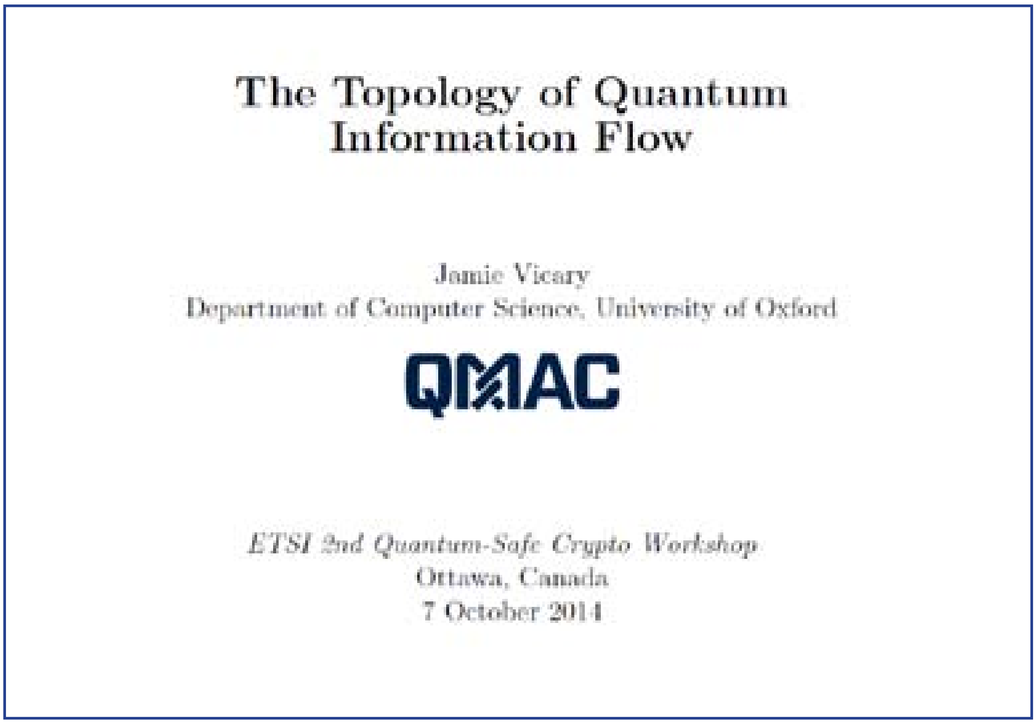
29

ISBN 979-10-92620-04-7

The topolofy 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.



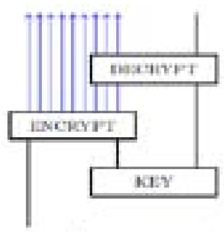
ISBN 979-10-92620-04-7

Introduction

There is a deep analogy between encryption and teleportation:

Introduction

There is a deep analogy between encryption and teleportation:

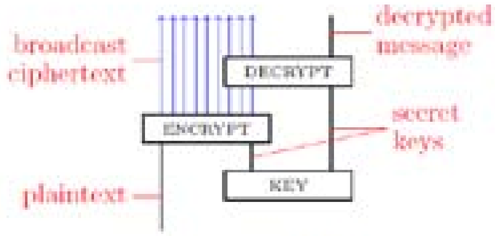


Encrypted communication

ISBN 979-10-92620-04-7

Introduction

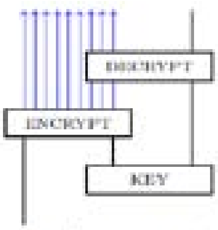
There is a deep analogy between encryption and teleportation:



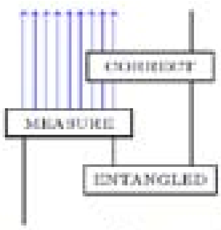
Encrypted communication

Introduction

There is a deep analogy between encryption and teleportation:



Encrypted communication

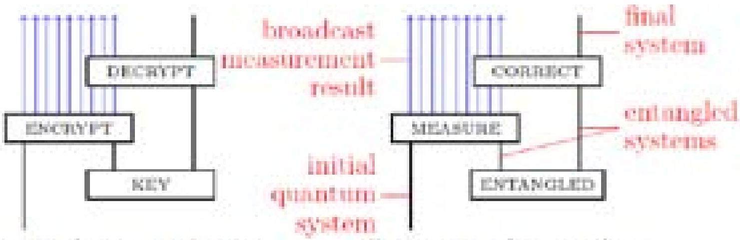


Quantum teleportation

ISBN 979-10-92620-04-7

Introduction

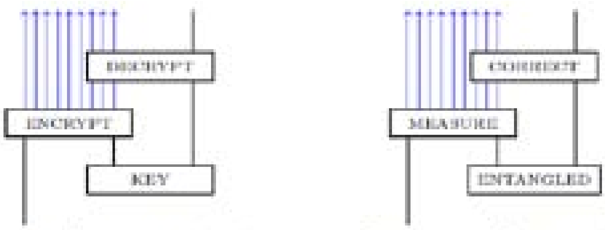
There is a deep analogy between encryption and teleportation:



Encrypted communication Quantum teleportation

Introduction

There is a deep analogy between encryption and teleportation:

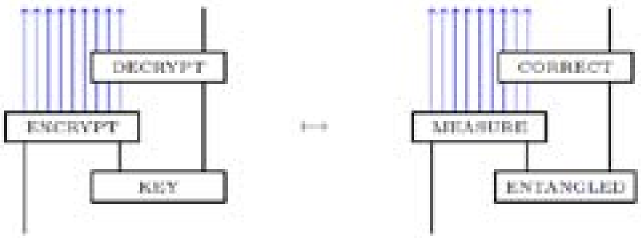


Encrypted communication Quantum teleportation

ISBN 979-10-92620-04-7

Introduction

There is a deep analogy between encryption and teleportation:



Encrypted communication   Quantum teleportation

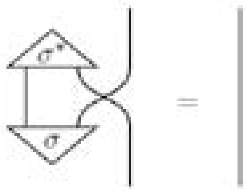
New idea. We can make this precise using topological mathematics.

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

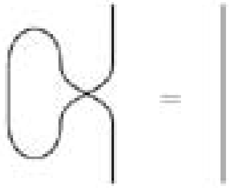
Consider the following equation, where σ is a bipartite state preparation and σ^* is the corresponding bipartite postselection:



ISBN 979-10-92620-04-7

Strings and correlation

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



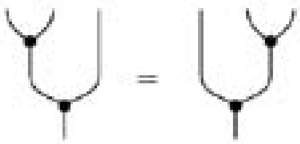
We change notation and use **topological strings**.

We can investigate consequences of this equation in different settings.

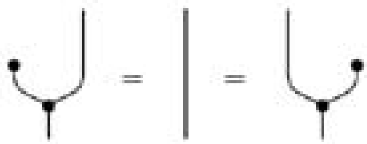
- **Quantum theory.**
  The state σ is *maximally entangled*: $|\sigma\rangle = |00\rangle + |11\rangle$
- **Classical computation.**
  The state σ is *perfectly correlated*: $\sigma = \{00\} \cup \{11\}$.

Surfaces and logic

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

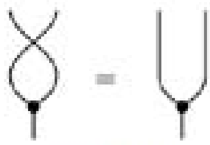


Associativity



Unit

Frobenius law

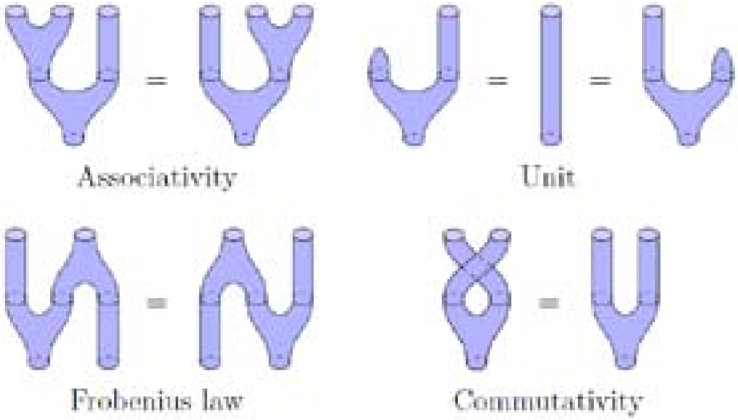


Commutativity

ISBN 979-10-92620-04-7

Surfaces and logic

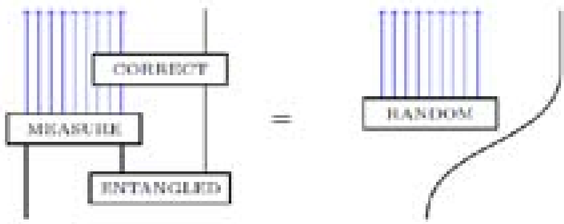
We now think about basic properties of copying, comparing and deleting classical information:



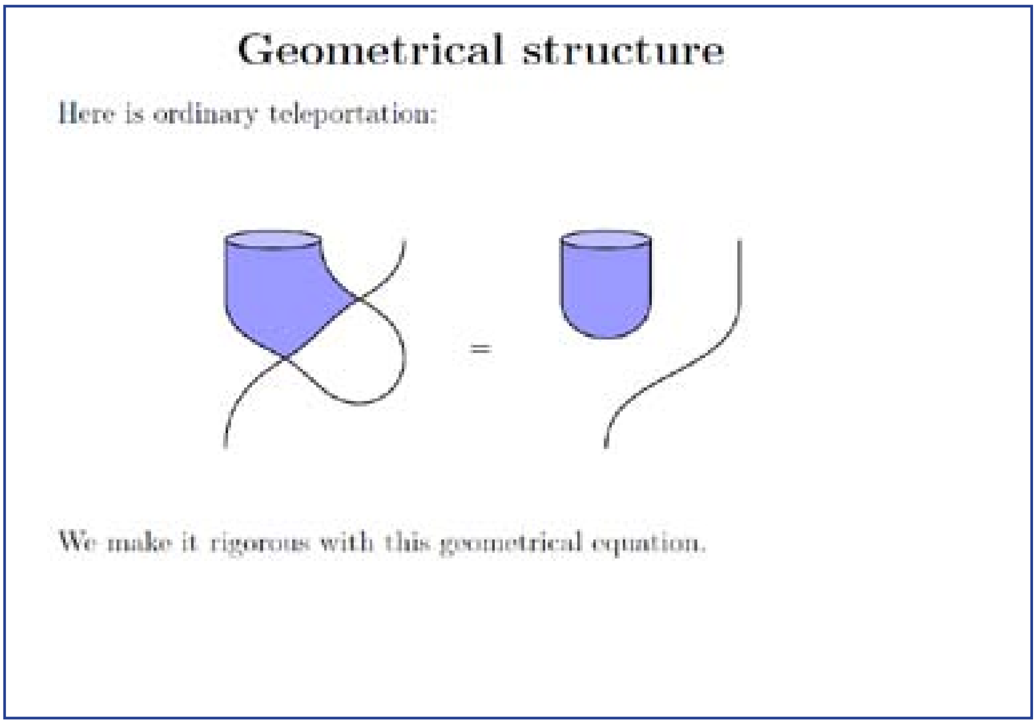
These are the laws obeyed by surfaces up to deformation!
So we change notation and use **topological surfaces**.

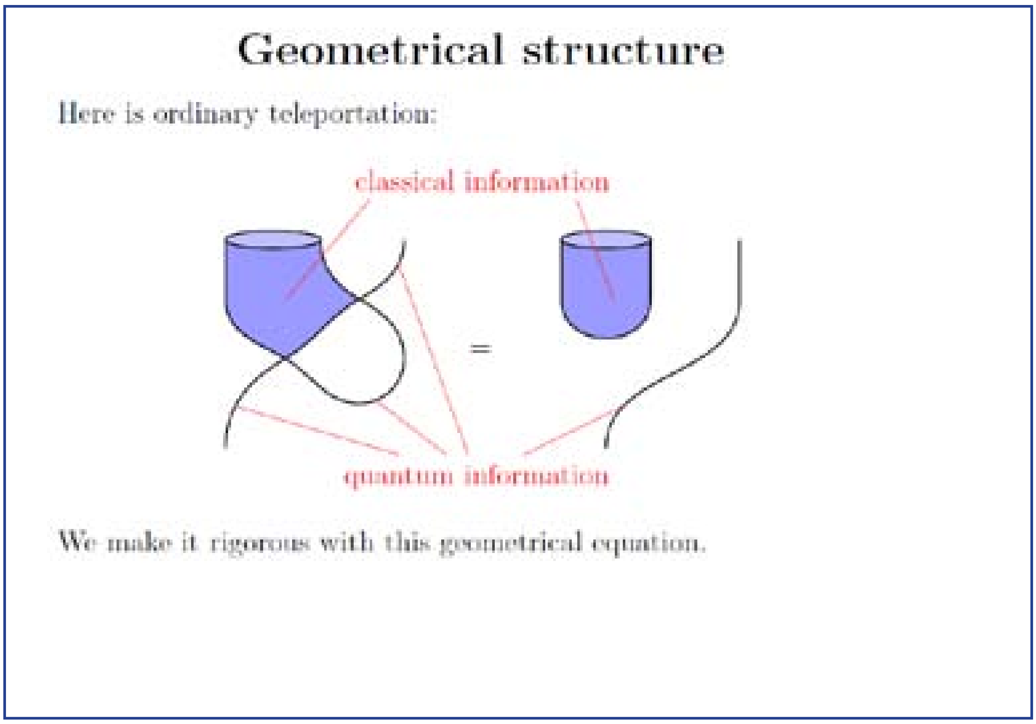
Geometrical structure

Here is ordinary teleportation:



ISBN 979-10-92620-04-7

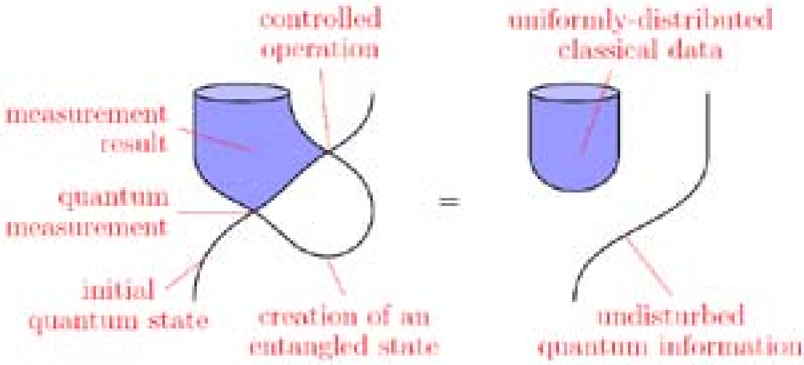




ISBN 979-10-92620-04-7

Geometrical structure

Here is ordinary teleportation:

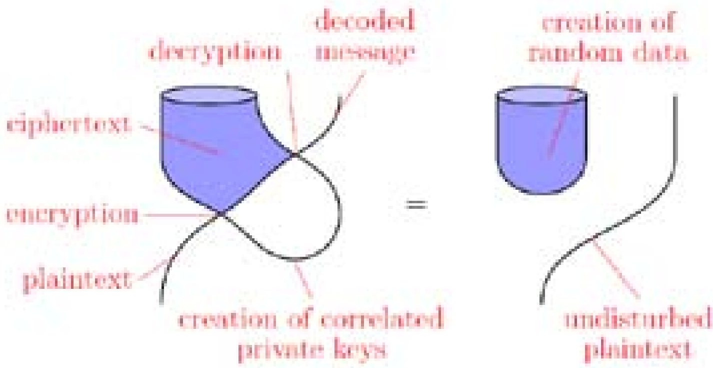


We make it rigorous with this geometrical equation.

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.

ISBN 979-10-92620-04-7

So what?

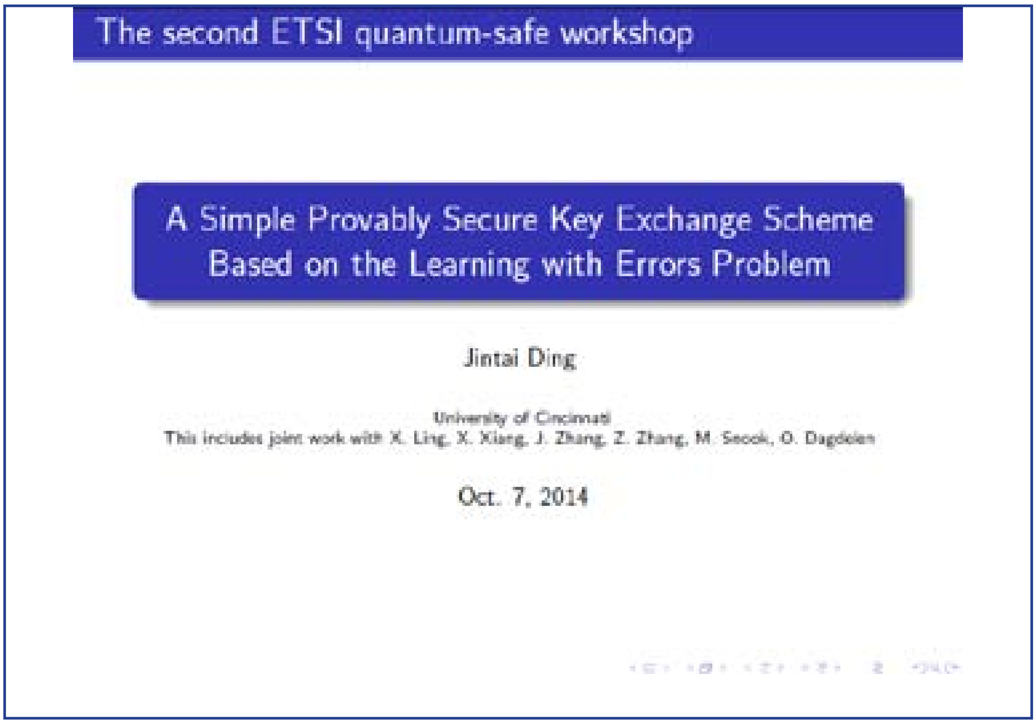
- Allows us to reason logically about cryptographic primitives in both quantum and classical computation.
- Provides a formal foundation for computational support tools.
- Gives a unified setting to consider integrated classical and quantum phenomena—for example, QKD+OTP.
- Addresses fascinating conceptual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

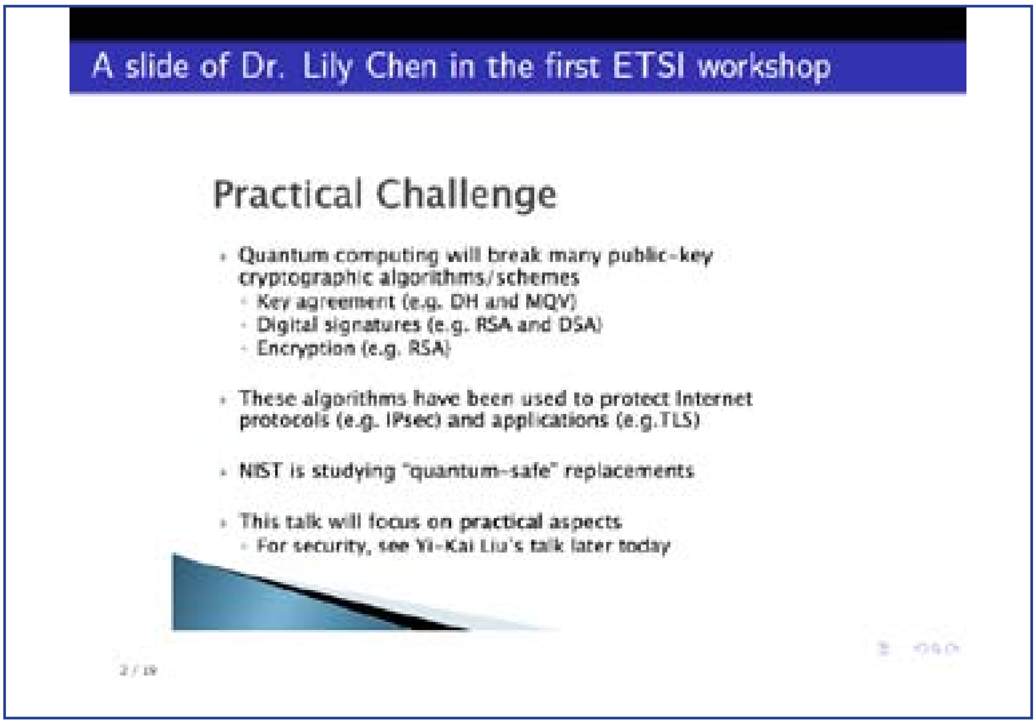
Thank you!

ISBN 979-10-92620-04-7

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

Jintai Ding, University of Cincinnati





ISBN 979-10-92620-04-7

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.

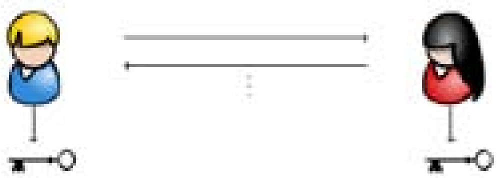
  In practice, public key encryption is only used to transmit random keys. (The key is only determined by one party)

- 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

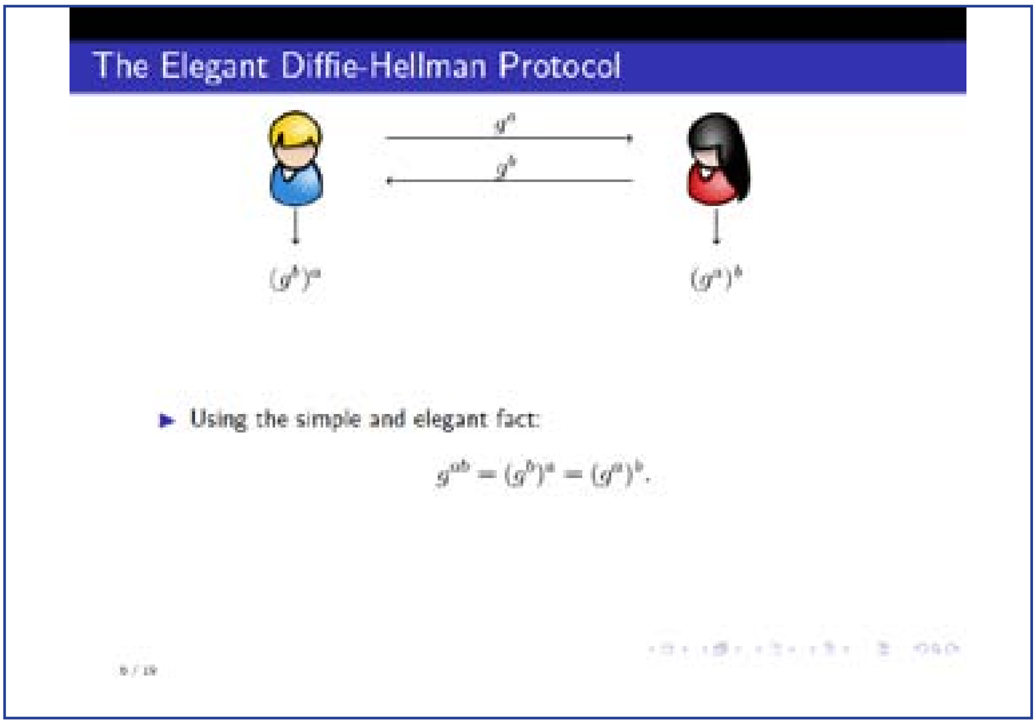
What's Key Exchange

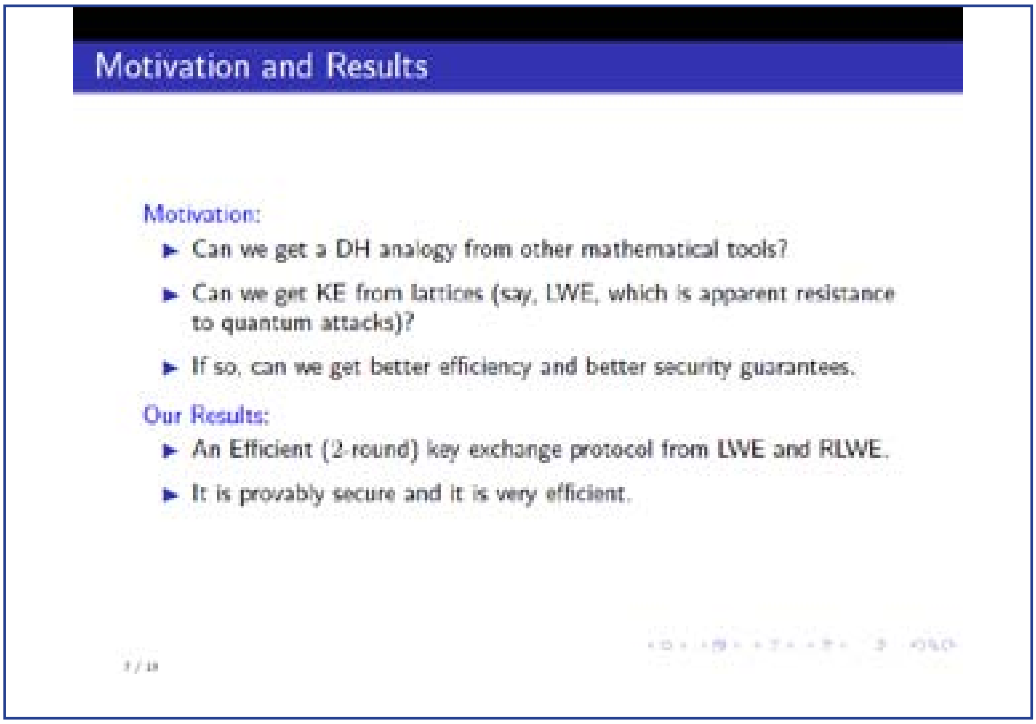


- Two parties get a shared secret key over an unsecure channel.

5 / 19

ISBN 979-10-92620-04-7





ISBN 979-10-92620-04-7

Learning with Errors (LWE) [Oded Regev 2005]

Goal: distinguishing "noisy inner products" from uniform.

$\mathbf{a}_1 \leftarrow \mathbb{Z}_q^n;$	$b_1 = \langle \mathbf{a}_1, \mathbf{s} \rangle + e_1 \mod q$
$\mathbf{a}_2 \leftarrow \mathbb{Z}_q^n;$	$b_2 = \langle \mathbf{a}_2, \mathbf{s} \rangle + e_2 \mod q$
$\vdots$	
$\mathbf{a}_m \leftarrow \mathbb{Z}_q^n;$	$b_m = \langle \mathbf{a}_m, \mathbf{s} \rangle + e_m \mod q$

$\mathbf{a}_1 \leftarrow \mathbb{Z}_q^n;$	$b_1 \leftarrow \mathbb{Z}_q$
$\mathbf{a}_2 \leftarrow \mathbb{Z}_q^n;$	$b_2 \leftarrow \mathbb{Z}_q$
$\vdots$	
$\mathbf{a}_m \leftarrow \mathbb{Z}_q^n;$	$b_m \leftarrow \mathbb{Z}_q$

In a matrix form

$$(\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e}) \approx_c (\mathbf{A}, \mathbf{b})$$

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

8 / 19

Provable security

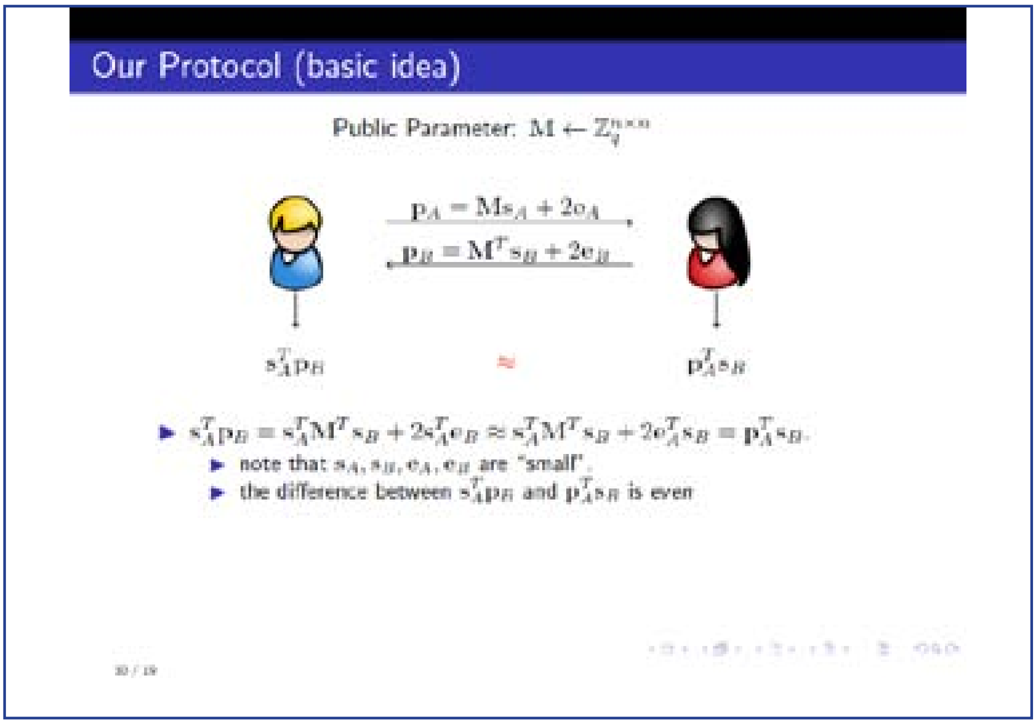
Theorem (Informal)[Reg'05]

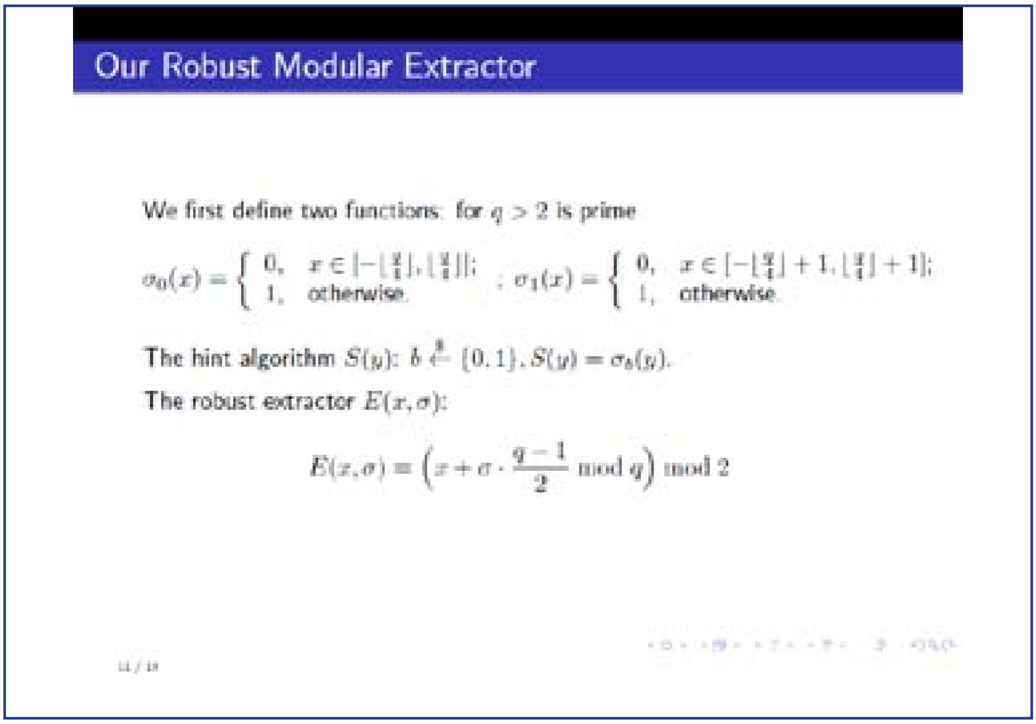
Let χ be a discrete Gaussian distribution with parameter $0 < \alpha < 1$, s.t. $\alpha q \geq 2\sqrt{n}$. If there exists a polynomial time algorithm solves LWE problem, then there exists a quantum algorithm solves (n/α)-SVP problems for all n-dimension lattices.

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

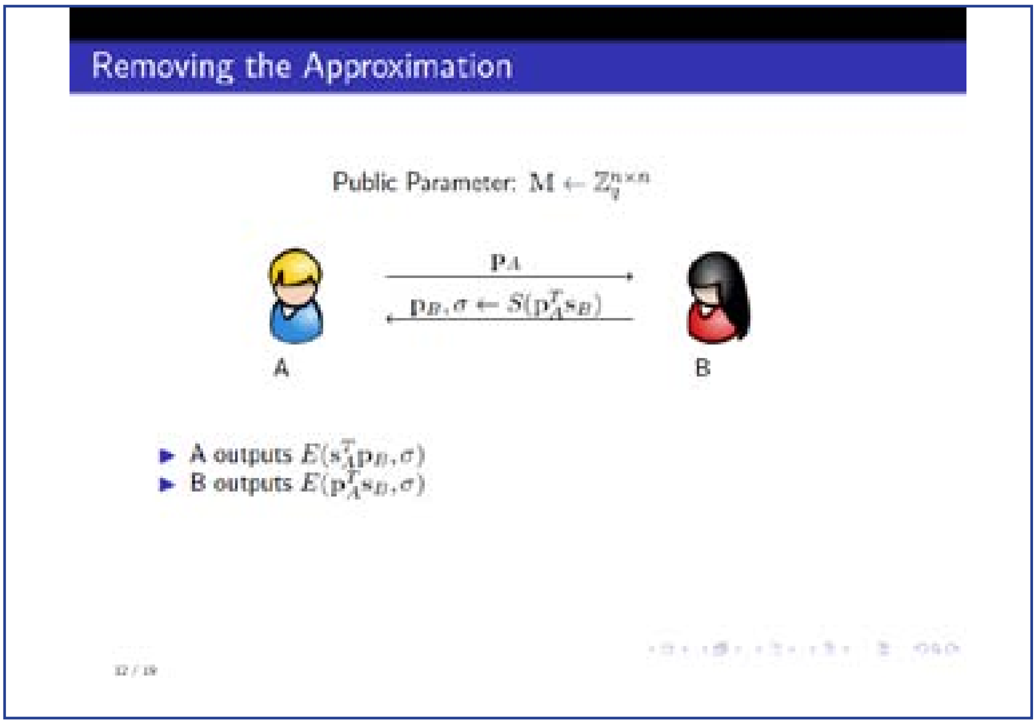
9 / 19

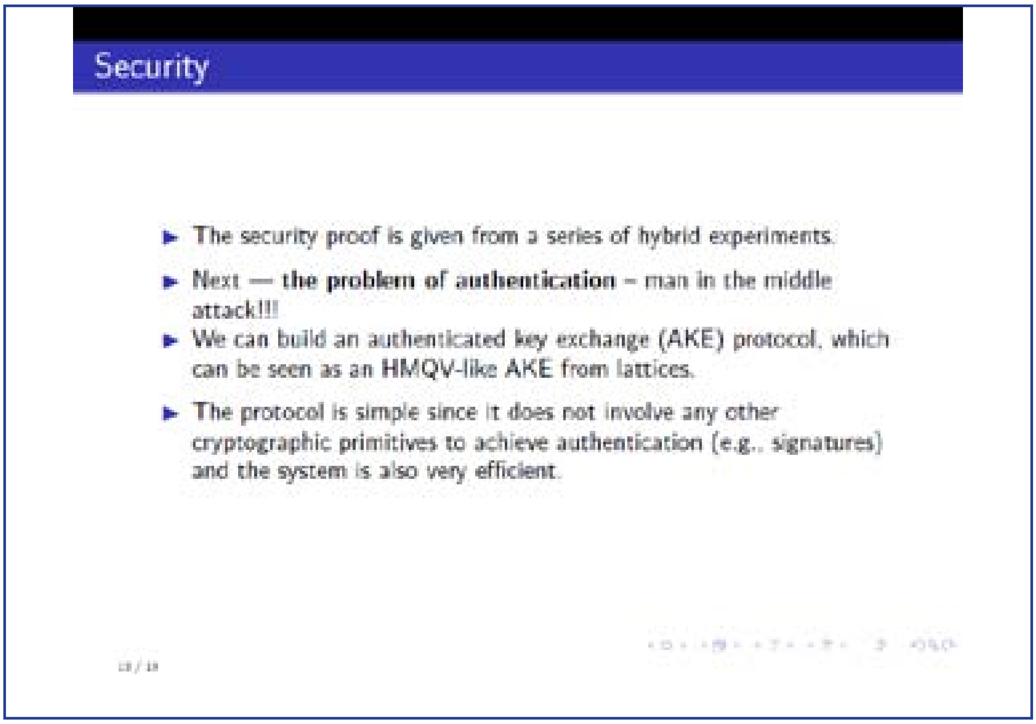
ISBN 979-10-92620-04-7





ISBN 979-10-92620-04-7





ISBN 979-10-92620-04-7

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 $s_i, e_i \leftarrow_r \chi_\alpha$

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

→ x_i →

Party j

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

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

← y_j, w_j ←

Party i

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

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

AKE from ring-LWE

Intuition for Security:

1. We can prove the security of the system
2. We can prove the forward security of the system
3. We did preliminary implementation and it is very efficient.
4. Parameters for implementation.

Parameters	n	Security (expt.)	α	γ	$\log \frac{\gamma}{\alpha}$	$\log q$ (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

ISBN 979-10-92620-04-7

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

16 / 19

AKE from ring-LWE

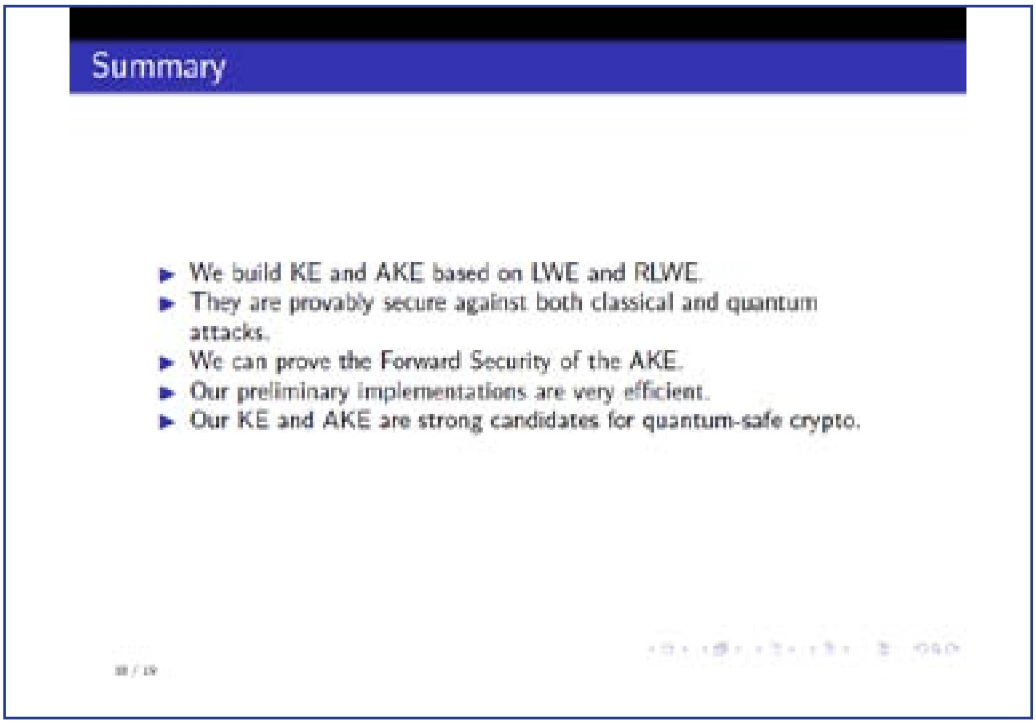
Timings:

Parameters	Initiation	Response	Finish
I	3.22 ms (0.02 ms)	8.50 ms (4.69 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.

17 / 19



ISBN 979-10-92620-04-7

Quantum-Safe-Crypto Workshop

ETSI World Class Standards

IISBN 979-10-92620-02-3

Editors: Michele Mosca
Gaby Lenhart
Mark Pecen