Block Ciphers and Stream Ciphers: The State of the Art

Alex Biryukov

Katholieke Universiteit Leuven, Dept. ESAT/SCD-COSIC,
Kasteelpark Arenberg 10,
B–3001 Leuven-Heverlee, Belgium
abiryuko@esat.kuleuven.ac.be

Abstract. In these lecture notes we survey the state of the art in symmetric key encryption, in particular in the block ciphers and stream ciphers area. The areas of symmetric key encryption has been very active in the last five years due to growing interest from academic and industry research, standardization efforts like AES, NESSIE and CRYPTREC, as well as due to ease of government control over export of cryptography.

Keywords: Block ciphers, stream ciphers, cryptanalysis, design, AES, NESSIE, CRYPTREC, STORK, E-CRYPT.

1 Introduction

In these lecture notes we survey the state of the art of symmetric key encryption in the last five-six years, this is the time that passed since the previous such snapshot given in [72]. During this relatively short period of time several major developments have happened in this area. The first one would undoubtedly be the switch in 2001 by the US NIST [106] from the old 64-bit block 56-bit key cipher DES (Data Encryption Standard) [101] to a newly designed 128-bit block 128/192/256-bit key cipher AES (Advanced Encryption Standard) [103]. The choice of AES resulted from a three year open competition process [130], in which 15 submissions coming not only from North America but also from Europe and Asia were publicly evaluated for security, speed and compactness of implementation. As a result, Belgian cipher called Rijndael [40] has won the competition, and as of this writing stands unbroken in-spite of numerous attempts of analysis [100, 54, 47, 37, 4, 16, 48, 83].

In 1999-2000 several new cryptanalytic techniques were developed: slide attacks [24, 25], impossible differential attacks [10, 11, 76], boomerang attacks [128]. Considerable followup in the research literature shows that these are generic techniques applicable to a variety of constructions which in certain cases are more effective than the classic differential and linear techniques. In 2002 a new possible line of cryptanalysis came to light: an algebraic attack [37]. The research community is still divided on whether this technique actually works as described. However, it is applicable to a certain class of stream ciphers.

In the stream cipher area we may mention intensive research and progress in fast-correlation attacks [65, 30, 66, 95, 31] and BDD approach [78] for LFSR-based stream ciphers. New time-data-memeory tradeoffs [22]. Distinguishing attacks using linear masking and low diffusion [33]. Higher-order correlation and algebraic attacks [34, 36]. In the area of applications of stream ciphers we may mention adoption of a cipher Kasumi, which is a modification of a block-cipher MISTY, as complementary standard A5/3 for 3GPP cellular phones in addition to weak algorithms A5/1 and A5/2 that were used previously. There has been significant progress in cryptanalysis of industry standards A5, RC4 and E0 (Bluetooth).

Also worth mentioning in conjunction with symmetric key encryption is the area of side-channel and fault attacks, i.e. attacks on implementations of cryptographic primitives. The area has become very active in the last years fueled by practical attacks on many pre-existing implementations.

Another important development happened in the legal area and approximately at the same time when cipher Rijndael was chosen as the AES. In their meeting of 30 November-1 December 2000, the Wassenaar states (31 countries, including US, EU states, Japan and others), lifted the 64-bit limit for export controls on mass-market crypto software and hardware. Previously, for example in US only 40-bit ciphers could be exported. New US regulations [29] allowed for commercial export of encryption items with keys larger than 64-bit prior to review by Bureau of Industry and Security (BIS) and in some cases prior to notification (mainly for items with keys shorter than 64-bit).

The two initiatives for cryptographic primitives evaluation (including encryption) have been conducted in Europe (NESSIE) [104], and in Japan (CRYPTREC) [131]. These projects produced portfolios of primitives recommended for ISO standards (NESSIE) or E-government (CRYPTREC). A new Korean initiative is starting to gain momentum.

Since 2000 NIST has been running an effort for selection of modes of operation for block-ciphers [132].

In 2003 a roadmap project STORK [119] has been carried out by a team of researches from different EU countries. The project produced roadmaps for cryptography: research agenda, perspective future trends as well as lists of important open problems for the next 5-10 years. STORK has served as a launch pad for E-CRYPT – a new consortium of about 30 European universities and companies collaborating in the area of Cryptography and Watermarking. E-CRYPT is a five-year project which starts its work in November 2003.

2 Paying Tribute to DES

The Data Encryption Standard (DES) [101] has been around for more than 25 years. DES was a result of a call for primitives in 1974 which apparently didn't turn in many interesting candidates except for a predecessor of DES, Lucifer [117, 46] designed by IBM around 1971. It took another year for a joint IBM–NSA effort to turn Lucifer into DES. The structure of Lucifer was significantly altered and since the design rationale was never made public and the secret key size also went down from 128-bit to 56-bits this resulted in controversy, and distrust among the public.

However, in spite of all the controversy it is hard to underestimate the role of DES. DES was one of the first commercially developed (as opposed to government developed) ciphers whose structure was fully published. This effectively created a community of researchers who could analyse it and propose their own designs. This lead to a wave of public interest in cryptography, from which much of cryptography as we know it today was born.

In the two decades since its design three important attacks capable of breaking the cipher faster than exhaustive search have been discovered: differential cryptanalysis (1990) [18], linear cryptanalysis (1993) [85] and improved Davies' attack [9, 41]. An interesting twist is that differential cryptanalysis was known to the designers of DES and DES was constructed in particular to withstand [1] this powerful attack [32]. That is why DES design criteria were made secret. Many of these secrets became public with the development of the differential cryptanalysis and were later confirmed by the designers [114]. Both differential and linear attacks as well as Davies' attack are not of much threat to real-life applications since they require more than 2^{40} texts for analysis. For example: linear attack requires that 2^{43} **known plaintexts** would be encrypted under the same secret key. If the user changes the key every 2^{35} blocks the success probability of the attack would be negligible. Nevertheless linear attack was practically tested [86] and runs even slightly faster than theoretically predicted [67]. In the case of the differential attack 2^{47} **chosen plaintexts** are required, though the attack would still work if the data is coming from up to 2^{33} different keys. However the huge amount of **chosen** plaintext makes the attack impractical. In the case of Davies' attack the data requirement is 2^{50} **known plaintexts**, which is also clearly impractical.

Though the differential and linear attacks are hard to mount on DES they proved to be very powerful tools of cryptanalysis and many ciphers which were not designed to withstand these attacks have been broken, some even with practical attacks. See for example cipher FEAL [115, 98, 99]. In fact both attacks have been discovered while studying this cipher [17, 90], which was proposed as a more secure substitute for DES.

The currently most dangerous approach to cryptanalysis of DES remains exhaustive key search. It was clear from the very start that 56-bit key can be cryptanalysed in practical time using practical amount of resources. In 1977 a design for a key-search machine was proposed by Diffie-Hellman [42] with a cost of 20.000.000$ and ability to find a solution in a single day. Later Hellman proposed a chosen plaintext tradeoff approach, which would allow to build an

[1] Note that DES is strong but not optimal against linear cryptanalysis or improved Davies' attack, for example simple reordering of the S-boxes would make the cipher immune to these attacks without spoiling its strength against the differential attack [87]. This could indicate that designers of DES did not know about such attacks.

even cheaper machine, assuming that 2^{56} step precomputation is done once. In 1998 Electronic Frontier Foundation (EFF) has demonstrated a dedicated hardware machine which cost less than $250,000$ and could run through the full key-space in four days [45]. In a parallel development it has been shown that a network of tens of thousands PC's (a computational power available to a computer virus, for example) could do the same work in several weeks. It became clear to everyone that DES needs to be replaced. However at that time AES competition was already up and running.

So where is DES today? DES is not obsolete. Due to substantial cryptanalytic effort and no practical cryptanalytic attack, the structure of DES has gained public trust. There have been several proposals to remedy the short-key size problem plaguing the cipher.

– **Triple-DES.** Approach suggested by Diffie and Hellman [42]. Gains strength both against cryptanalytic attacks as well as against exhaustive search, speed is however 3 times slower than single DES.
– **Independent subkeys.** Proposed Berson [6]. Stops exhaustive search but not the cryptanalytic attacks, speed as for a single DES, but slower key-schedule.
– **Slow key-schedule.** Approaches by Quisquater et.al. [113] or Knudsen [71]. Exhaustive search is stopped by loosing key-agility of a cipher.
– **DESX.** Approach suggested by Rivest in 1984. Very effective against exhaustive search, but does not stop cryptanalytic attacks, allows to reuse old hardware; speed almost as for a single DES.
– **Key-dependent S-boxes.** Approach suggested by Biham-Biryukov [8]. Gains strength against exhaustive search, stops cryptanalytic attacks (with exception of related key) applies to software or to hardware which permits to load new S-boxes; speed as for a single DES.

As of today triple DES is still in wide use (especially in the banking community) and is part of NIST and ISO standards. The recommended usage mode is with three independently generated keys (i.e. 168-bit key total), for which the best attacks are the classical meet-in-the-middle attack with only 3 known plaintexts, 2^{56} words of memory and 2^{111} analysis steps; and the attack by Lucks [82] which requires 2^{108} time steps and 2^{45} known plaintexts. The attacks are clearly impractical. The two-key triple DES variant is not recommended for use due to dedicated meet-in-the-middle attack by Oorschot and Wiener [125] with complexity $2^{120-\log n}$ steps given $O(n)$ **known plaintexts** and memory. This attack is based on an earlier attack by Merkle and Hellman [93] which required 2^{56} **chosen plaintexts**, steps, and memory. The attacks are hard to mount in practice, but they are important certificational weakness. The DESX alternative is also in popular use due to simplicity and almost no speed loss. Thorough analysis of a generic construction is given in [69] and the best currently known attack is a slide attack [25] with complexity of n known plaintexts and $2^{121-\log n}$ analysis steps (for example: 2^{33} known plaintexts and memory and 2^{87} analysis steps).

3 AES-Rijndael

In the view of quickly aging standard DES on September 1997 NIST has issued a request for candidate nominations for the block-cipher that would become a new Advanced Encryption Standard. The minimal requirements were: 128-bit block size and support for 128/192/256 bit keys. An early draft of the call required also block sizes of 192 and 256 but this was dropped at a later stage. The ultimate goal of the competition was to design a cipher that would be as secure as triple-DES but which would be much faster. The process went in three stages: submission, evaluation-selection, choice of the finalist. Submissions were due by 15 May 1998, and candidate presentations took place at a public workshop on 20-22 August 1998. There were about 20 submissions, but only 15 satisfied the requirements. The second stage was evaluation and selection of the five finalists out of 15. The five finalists were announced in March 1999. These were: RC6 (RSA), MARS (IBM), Rijndael (Daemen-Rijmen), Twofish (Counterpane) and Serpent (Anderson-Biham-Knudsen). No security weaknesses were demonstrated for either of these ciphers. The first four were among the fastest submissions and Serpent was chosen due to its high security margin and reasonable performance. Since no objective criteria for security evaluation except for a resistance to all known attacks could be applied, and since all the five finalists were build to withstand any known attacks, the choice was a difficult matter. Such factors as elegance of description, simplicity of implementation on various platforms were taken into account. At the end of the second stage a poll of the audience was taken and it showed that Rijndael was public favorite (Rijndael:89 votes, Serpent:59, Twofish:31, RC6:23, MARS:13).

On October 2, 2000 Rijndael, has been proclaimed the winner of the AES competition. To cite NIST's decision:

"**Why did NIST select Rijndael to propose for the AES?**

When considered together, Rijndael's combination of security, performance, efficiency, ease of implementation and flexibility make it an appropriate selection for the AES.

Specifically, Rijndael appears to be consistently a very good performer in both hardware and software across a wide range of computing environments regardless of its use in feedback or non-feedback modes. Its key setup time is excellent, and its key agility is good. Rijndael's very low memory requirements make it very well suited for restricted-space environments, in which it also demonstrates excellent performance. Rijndael's operations are among the easiest to defend against power and timing attacks.

Additionally, it appears that some defense can be provided against such attacks without significantly impacting Rijndael's performance. Rijndael is designed with some flexibility in terms of block and key sizes, and the algorithm can accommodate alterations in the number of rounds, although these features would require further study and are not being considered at this time. Finally, Rijndael's internal round structure appears to have good potential to benefit from instruction-level parallelism.

What about the other four algorithms that were not selected?

In terms of security, NIST states in its report that "all five algorithms appear to have adequate security for the AES." NIST is not saying that there is anything "wrong" with any of the other four algorithms. However, when all of the analysis and comments were taken into consideration, the NIST team felt that Rijndael was the best selection for the AES.

Why did NIST select only one algorithm to propose for the AES?

...Briefly, NIST's AES selection team decided to select only one algorithm for several reasons. First, other FIPS-approved algorithms (e.g., Triple DES) offer a degree of systemic resiliency, should a problem arise with the AES. Second, multiple AES key sizes provide for increased levels of security. Third, a single algorithm AES will promote interoperability and decrease the complexity of implementations that will be built to comply with the AES specifications, hopefully promoting lower implementation costs than a multiple algorithm AES. Fourth, a single AES algorithm addresses vendors' concerns regarding potential intellectual property costs."

Frequently asked questions about AES and NIST's responses may be found here [105]. A new standard has been announced on November 26, 2001 under FIPS-197 "for use by U.S. Government organizations to protect sensitive, unclassified information". As it happened previously with DES it is expected that AES will become a de-facto world industry standard.

3.1 Summary of Properties of the AES

In this section we list the main features of the AES. AES is a substitution-permutation network (SPN) cipher with 128-bit block and allowing key sizes of 128/192/256 with 10/12/14 rounds respectively. As usual SPN it consists of layers of S-boxes (the same S-box is used in all positions and in all the rounds) which provide local diffusion and affine mappings provide global diffusion. The cipher uses S-boxes based on inversion function, which has provably optimal differential and linear properties [108] followed by an affine transform, to avoid interpolation attacks. The diffusion is an MDS-based matrix. As of today no security weakness has been demonstrated for AES for any of the key-sizes, so all security evaluations have been dealing with round reduced versions of the cipher. By design AES does not have differential or linear patterns that propagate more than four rounds, which probably indicates that the cipher is secure against these powerful attacks and some of their extensions already after 5-6 rounds. Designers studied application of a dedicated attack, so called "Square" attack (an attack of a multiset-type (see Section 4.1)), which gets its name from Rijndael's predecessor — Square [38]. The attack can break 6 rounds with $O(2^{32})$ known plaintexts, memory and 2^{72} analysis steps. The work factor can be further reduced to 2^{46} as shown in [47]. It is possible to add one more round for keys 192, 256 by just guessing one subkey and using weaknesses in the key-schedule [83]. The best attack found so far can break 7-rounds with 2^{32} chosen plaintexts and 2^{140} steps for 192, 256 and is claimed to be marginally faster than exhaustive search for 128-bit keys [54]. Studying structural elements of Rijndael an interesting property of the S-box was discovered, i.e. the output functions of the S-box are affine transforms of the same function [52]. This can help hardware designer but might be useful for the cryptanalysis as well. Along similar lines Barkan and Biham [4] have shown that due to the algebraic nature of the components AES possesses 240 isomorphic ciphers. In [21] this work is extended to show 61,200 isomorphic ciphers, by exploiting affine self-equivalence of the S-box (similar result would hold for any S-box based on a power function). Note that such alternative representations of a cipher may be used to combat side-channel attacks.

Regarding the speed, Rijndael is one of the fastest block-ciphers designed so far. For example in optimized software implementation it takes 22 cycles/byte on Pentium II, 23 cycles/byte on Pentium III, 24 cycles/byte on Xeon, 17 cycles/byte on Alfa. These numbers would vary significantly for different platforms and compilers.

The best source of additional information on AES would be the book written by its designers [40], and for a more recent security and speed comparison of AES with other modern ciphers see the deliverables D20 and D21 of the NESSIE project [133], available on-line.

4 Block Ciphers: Design and Cryptanalysis

In this section we review the state of the art in cryptanalysis and design of the block ciphers.

4.1 New Attacks

In the last 5-6 years several new methods of cryptanalysis have been developed. In 1999 an **impossible differential** attack [12] has been shown to break 31 out of 32 rounds of the cipher Skipjack [107], designed by the NSA and declassified in 1998. An attack based on similar principles was used by Knudsen to cryptanalyse 6-rounds of the cipher DEAL [76] which was one of his proposals for the AES competition. The attack using impossible differentials was shown to be a generic method of cryptanalysis [12] and was applied to improve on best attacks for such strong an long standing ciphers as IDEA [81] and Khufu [92], breaking round-reduced versions of these ciphers. One of the main ideas was a "miss-in-the-middle" technique for construction of impossible events inside ciphers. Another extension of differential cryptanalysis was shown in the same year 1999, by Wagner — **boomerang attack** and inside-out attack [128]. The attack breaks constructions in which there are perfect differential patterns propagating half-way through the cipher both from top and from the bottom, but there are no good trails that propagate through the full cipher. The attack was spectacularly demonstrated with a practical cryptanalysis of a cipher which was designed with provable security against conventional differential attack [126], as well as on round-reduced versions of several other ciphers. Further refinements of this technique have been found in papers on so called amplified boomerang and rectangular attacks [68, 14, 15]. Yet another attack which was developed in the same year (!) was a **slide attack** [24, 25]. The main feature of this attack is that it realizes a dream of cryptanalyst: if the cipher is vulnerable to such attack the complexity of attack is independent of the number of rounds of the cipher. Several ciphers or slight modifications of existing ciphers have been shown vulnerable to such attacks: for example Brown-Seberry variant of DES [28] (rotations in key-schedule are by 7 positions, instead of 1,2), DESX, arbitrary Feistel cipher with 4-round periodic key-schedule. In practice the attack seems easy to avoid breaking the similarity of the round transforms by applying round counters or different random constants in each round. Whether such simple changes are indeed sufficient is a matter of further research.

Another type of cryptanalytic attack which is currently receiving attention is the **multiset attack**. One of the main reasons is that these attacks are the best attacks for round-reduced versions of AES and exploit its byte-wise structure. The first such attack was discovered by Knudsen during analysis of the cipher Square [38] and was thus called "Square attack". Similar attack was used by Lucks [83] and called "saturation" attack. Later Biryukov and Shamir have shown an attack of similar type breaking arbitrary 3 round SPN network with secret components (the so called $SASAS$ scheme). Gilbert-Minier "collision" attack [54] on 7-rounds of Rijndael as well as Knudsen-Wagner [77] "integral" cryptanalysis of 5-rounds of MISTY1 also fall into the same class. The main feature is that unlike a differential attack in which the attacker studies the behavior of pairs of encryptions, in a multiset attack the attacker looks at a larger carefully chosen sets of encryptions, in which parts of the input text form a multiset. A multiset is different from a regular notion of a set, since it allows the same element to appear multiple times. The element of a multiset is thus a pair ($value, multiplicity$), where *value* is the value of the element and *multiplicity* counts the number of times this value appears in the multiset. The attacker then studies propagation of multisets through the cipher. The effect of the cipher on a multiset is in changing values of the elements but preserving some of the multiset properties like: multiplicity; or "integral" (i.e. sum of all the components); or causing a reduced set of values which would increase the probability of birthday-like events inside the cipher. This new type of attacks is a promising direction for further research.

4.2 A Few Words on the Design

The current state of the art in the field is that we know quite well how to construct ciphers secure, which at least look secure against the most powerful attacks, in particular against linear and differential attacks [109, 89, 126, 64, 39]. Whether such ciphers are secure against any attacks and what would be an optimal number of rounds for a cipher to be secure against all possible attacks is yet unknown. This is clearly demonstrated by the recent AES competition, where all the five finalists were in the category "no attack or weakness demonstrated". In this situation the choice would definitely go for the most simple and elegant design versus a complex and non-transparent one. Such choice is for the benefit of both the implementors, whose life is easier and thus implementation errors are less likely to occur and the researchers, who have a clean structure to analyse. It is clear that if AES will be successfully cryptanalysed the attack will have to be a "break through" which will raise state of the art in the field to a new level (similar to what has happened to differential and linear attacks on DES). Obviously a fashionable trend in design nowadays are AES-like ciphers, which means a shift of accent from Feistel-ciphers towards SPNs with algebraic components. A new twist are AES-like ciphers which are based solely on involutional components, like Khazad or Anubis. In these ciphers both the linear and the non-linear layers are involutions which simplifies hardware implementation. Some initial cryptanalysis of such construction is given in [19] but further research would be of much interest. Another popular design strategy is to base non-linear elements of a cipher on inversion or power functions in $GF(2^n)$. Such mappings have good non-linearity properties [108] as well as compact hardware representation.

4.3 On Algebraic Attacks

Recently a new line of attack on block an stream ciphers has been proposed, namely an algebraic attack. While the name is too generic (for example interpolation attacks may also be called algebraic attacks) it tries to capture the following distinction from the previous "statistical" approaches to cryptanalysis. The idea is to write a system of multivariate polynomial equations describing internal stages of encryption and to try to solve this system in case it is low degree, overdefined, or sparse for example by re-linearization or its derivative method [70, 35]. If such attack would be possible, it would likely be a conceptual attack on a class of cryptosystems which likely will not be repaired by increasing the number of rounds. In this respect situation would be similar to a trapdoor recovery attack on the public key-cryptosystem, proving that underlying problem is not hard. As a caveat, note that a problem of solving large systems of quadratic equations over a field is NP-hard. This however guarantees only asymptotic, worst-case hardness. It does not mean that solving a particular instance of the problem (for example the one generated by AES) is hard. What has been done so far is a construction of simple systems of multivariate equations (usually of degree 2) describing AES, Serpent, Camellia, Misty/Kasumi and other ciphers [37, 20] or providing such systems by embedding a cipher in a higher field [100]. The systems thus obtained are indeed very structured, low degree (typically quadratic), relatively small (thousands of equations with thousands of unknowns) and sparse, which is a result of popularity of algebraic components or memory size limitations on the S-boxes. However as of this writing no practical algorithm solving such systems has been demonstrated even on small but meaningful examples. Finding such a practical algorithm is an interesting topic for further research.

To summarize a section on block-ciphers: there area is reaching maturity; there are simple and effective design strategies to construct strong ciphers, practically secure against existing methods of attack; there are still many open problems to stimulate further research in the area.

5 Stream Ciphers

Stream ciphers differ from block ciphers in several aspects: they always contain a secret "state" (i.e. memory) which evolves with time during the encryption, they usually produce streams of bits rather than blocks. Thus the two main parts of a stream cipher are: state-transition function, which given an old state computes a new state, and a filter, which given the state produces the output of the stream cipher. The output of a stream cipher (i.e. a random-looking) stream of digits is typically XORed to the plaintexts resulting in a ciphertexts. Thus stream ciphers can be viewed as computational analogy of a one-time pad (OTP) cipher, replacing a long secret key by a short secret seed and pseudo-randomly generated stream of digits, computationally indistinguishable from a stream of random digits.

Prior to design of DES stream ciphers where ruling the world of encryption, either rotor machines (like Hagelin or Enigma), or secret military hardware-based designs using LFSR's all belonged to this class. Appearance of fast block ciphers has caused a shift of interest, due to convinience of use of block ciphers in various protocols, including a stream-like behavior which can be obtained via modes of operation in Counter, OFB or CBC, as well as due to a shift from hardware to software designs. This observation is supported by recent adoption of KASUMI [111] stream cipher as a 3GPP standard for encryption. KASUMI is in fact a strengthened version of block cipher MISTY1 [89] running in a Counter mode. Special properties of S-boxes of this cipher allow low-gate count implementations which traditionally has been the advantage of the stream ciphers.

Still in cases when there is need to encrypt large quantities of fast streaming data one would like to use a stream cipher. Popular trend in design of stream ciphers is to turn to block-wise stream ciphers (i.e. output is a block of bits, either a byte or 32-bits instead of a single bit) like RC4, SNOW 2.0, SCREAM, oriented towards fast software implementation. Stream ciphers which use parts of block-cipher like rounds intermixed with more traditional LFSR-like structure (MUGI, SCREAM).

One of the reasons why current state of the art in stream ciphers seems to be less stable than in block ciphers is due to great variety of constructions (LFSR-based: non-linear filters, non-linear feedback, irregular stepping function, irregular decimation/shrinking, block-based and other principles), compared to two basic models SPN and Feistel-cipher in the block cipher area.

5.1 Research Trends

There have been several interesting developments in the stream cipher area in the last 5 years. A concept of Hellman's time-memory tradeoff, has been applied and extended to the time-data-memory tradeoff for stream ciphers [22], which results in improved tradeoff compared to earlier tradeoffs [56, 2]. The Goldreich-Levin [55] one-way function hard-core bit construction has been enhanced into a more efficient pseudo-random number generator BMGL [59, 60, 94] with a proof of security. There has been considerable progress in the area of fast correlation attacks [65, 30, 66, 95, 31]. In practice such attacks would allow to break 100-bit LFSR if correlation is not too close to 1/2. A generic free binary decision diagrams (BDD) approach to LFSR-based stream cipher has been developed in [78]. Recently a discussion around "distinguishing" attacks on stream ciphers has arisen [61, 104]. New distinguishing attacks based on idea of linear masking have been proposed in [33]. Another important development is the high-order correlation attacks [34] based on correlations to low degree boolean functions and related to them algebraic attacks [36].

See [120] for a more detailed discussion on objectives and open problems of the stream cipher area. One of the goals of the newly formed consortium of European universities E-CRYPT would be to study new constructions in the area of stream ciphers.

5.2 On the Status of RC4 after Recent Attacks

RC4 is a popular stream cipher designed by Rivest for the RSA company in 1987, and whose disassembled source code was leaked to the Internet in 1994. RC4 is based on a state S which is a permutation of 256 bytes, the state-transition function makes a pseudo-random swap of two elements of the permutation. The output function outputs a a single byte (a byte of the permutation, at a pseudo-random index point). RC4 is a de-facto industry standard due to its high speed (7.3 cycles/byte on PIII) in software implementation and elegance of structure [2].

From the start a curious property was noticed by many researchers [3]: if one starts the indices by $i = a$, $j = a + 1$, and if $S[a + 1] = 1$, then the cipher has a very short cycle of size $256 \cdot 255$. Since in practice RC4 is initialized with $i = j = 0$, such state would be impossible to reach. In the surveyed period of time RC4 has received much attention from cryptographers [57, 97, 75, 51] but the cipher perfectly withstood most of the attacks. Though current attacks are very far from even demonstrating certificational weaknesses in the RC4 state-transition function, there has been considerable progress cryptanalysing the key-initialization procedure. For example, Mantin-Shamir [84] have shown that the second byte of the stream is biased towards 0 (probability 2^{-7}, instead of 2^{-8}). It was also demonstrated that a way in which frame resynch was used in the WEP protocol [110] was very weak. Namely, re-keying by mixing in a known IV leaked key-information even under a ciphertext-only attack. The attack has been demonstrated to work in practice [121]. With a proper key-initialization (for example if one drops the first 500 bits of the stream) there are no known key-recovery attacks on the stream generator. The situation with distinguishing attacks is more subtle. For more recent research see [96, 118].

[2] Though the key-agility is not very good: 2659 cycles/byte on PIII for 128-bit key, compare this with 504 cycles/byte for 128-bit key AES on the same machine [133].

[3] The "Finney property" by the name of the person who first published this discovery in a newsgroup "sci.crypt" in 1994.

5.3 On the Status of GSM Cipher after Recent Attacks

Over-the-air privacy of GSM telephone conversations is protected by A5 algorithm. This algorithm is in fact a triple of algorithms: A5/1, A5/2 and A5/3. The algorithms A5/1 and A5/2 were designed in 1989 and kept secret till 1994 when partial design was leaked (and cryptanalysed [1, 56]) and later in 1999 when the source code was reverse-engineered. The weaker A5/2 was immediately broken [27]. The stronger A5/1 (LFSR-based with majority clocking rule) also didn't last long [23]. The attacks on A5/1 were time-data-memory tradeoff attacks which could break the cipher given several seconds and up to a minute of known stream and analysis phase of few minutes, given a precomputation of $2^{42} - -2^{48}$ done once. Another effective attack is given in the paper by Biham-Dunkelman [13] and generic BDD-approach by Krause [78] also applies. An interesting observation is that even if the LFSR's are made longer the cipher does not become much more secure if one applies a different attack approach based on correlation attacks [44].

Following these developments a stronger cipher A5/3 (KASUMI) [111] based on MISTY1 [88, 89] has been added to the cipher suite. At the present moment there is no known weaknesses in this cipher in-spite of considerable research efforts around its predecessor MISTY1 [122, 123, 3, 79, 80, 77] and on KASUMI itself [26, 124]. Notice however that in the current standard protocol all three ciphers share a common secret key. Thus an attacker can request communication using the weakest alternative A5/2, recover the key in a ciphertext-only scenario, using weaknesses of the cipher and redundancy embedded into communication by error correcting codes. The attacker can then decrypt any further communications even encrypted under a strong A5/3 cipher [5].

5.4 On the Status of Bluetooth E0 Cipher after Recent Attacks

E0 (Bluetooth) is a stream cipher designed for short-range wireless LANs [116]. It is an LFSR-based cipher with four registers with total state of 128-bits. The recommended key size is 64-bits. Several attacks faster than exhaustive search over the state space (but not the key-space) have been proposed [63, 43, 50, 78]. The fastest attacks are the linear attack [58] with $O(2^{70})$ complexity of analysis and 2^{80} steps for precomputation and its potential improvement [49]. While these attacks indicate that the cipher is weak by modern standards it is still secure in practical applications.

6 On Side-Channel and Fault Attacks

The last 5-6 years have seen a surge in the amount of work done around side-channel attacks. This work is motivated by a simple discovery that encryption mechanisms leak side information in the form of varying time delays, power consumption or electromagnetic radiation. Another direction has been attacks by inducing faults into hardware. It is clear that such attacks are much more powerful than regular cryptanalytic attacks, since they gather information from inside the encryption process, which is not available for the analysis which is based only on mathematical description of a cipher. However study of such attacks in a general framework is hard since they are very implementation dependent. This type of attacks bears close similarity to hacking attacks, which could penetrate even systems guarded with perfect encryption primitives, but with weak protocols that are used around these primitives. Fault attacks would take this analogy further and correspond to active break-in attacks, in which the attacker is allowed to modify the source code of security primitives and observe the result. At the moment of this writing no implementation of cryptosystems has been demonstrated to be secure against these attacks. The industry currently is in a search for a tradeoff between the number of measurements required by the attack and the cost of the hardware implementation of the countermeasures.

7 NESSIE and CRYPTREC

Following the AES process two similar initiatives have been raised in EU (NESSIE) and in Japan (CRYPTREC).

7.1 NESSIE

The main objective of the NESSIE project was to put forward a portfolio of strong cryptographic primitives that has been obtained after an open call and been evaluated using a transparent and open process. The project was launched at the final stages of the AES competition and produced a call for a broad set of primitives providing confidentiality, data integrity, and authentication (rather than only encryption as in the AES effort). These primitives include block ciphers, stream ciphers, hash functions, MAC algorithms, digital signature schemes, and public-key encryption schemes. The project developed an evaluation methodology (both for security and performance evaluation) and a software toolbox to support the evaluation. The project goal was to widely disseminate the project results and to build consensus based on these results by using the appropriate fora (a project industry board, 5th Framework program, and various standardization bodies). A final objective was to maintain the strong position of European research while strengthening the position of European industry in cryptography. Note that unlike AES the NESSIE project provided recommendations for standardization bodies like ISO, but didn't have the standardization power itself.

In the area of block ciphers the project proposed MISTY1 for the legacy (64-bit block, 128-bit key) category, and AES and Camellia in the 128-bit block category. SHACAL-2, a 256-bit block, 512-bit key cipher based on a new hash function SHA-256 was recommended for the large-block category. In the area of stream ciphers no candidate managed to satisfy the high security requirements of the call (key length of at least 128 bits, internal memory of at least 128 bits), mainly due to certificational weaknesses related to distinguishing attacks faster than 2^{128} steps. The project has been finished and the result of the security and performance evaluation of the submitted primitives will be published as a book [133]. More information on the project may be found on the project web-site [104].

7.2 CRYPTREC

This project has been a Japanese e-government initiative [131]. Information technology Promotion Agency(IPA), sponsored by the Ministry of International Trade and Industry has been conducting the evaluation of cryptographic techniques. The purpose of this project was to list valid cryptographic techniques for the use of an electronic government whose infrastructure would be created by 2003.

A group of cryptographic techniques, which have been submitted to the formal call of "Call for Cryptographic Techniques" dated by June 13, 2000, have received detailed evaluation by assigned evaluators. Simultaneously, IPA was soliciting public analysis and comments. The CRYPTREC project was inviting submission of new primitives each year.

CRYPTREC has recommended the following primitives: in the area of 64-bit block ciphers — CIPHERUNICORN-E (NEC), Hierocrypt-L1 (Toshiba), MISTY1 (Mitsubishi), Triple DES with 3 keys (de facto standard). For the category of 128-bit keys: AES, Camellia (NTT), CIPHERUNICORN-A (NEC), Hierocrypt-3 (Toshiba), SC2000 (Fujitsu). In the area of stream ciphers: MUGI (Hitachi), MULTI-S01 (Hitachi), RC4 (with 128-bit key, de facto Internet standard), several pseudo-random generators based on SHA-1.

8 STORK and E-CRYPT

STORK was a thematic network funded within the Information Societies Technology (IST) Program of the European Commission's Fifth Framework Programme (FP5). It was one of the 25 roadmap projects within Key Action II with the objective to prepare the ground for research initiatives in the upcoming Sixth Framework Program (FP6). The STORK project established the framework for a European Network of Excellence in Cryptology, that would be the core of European research in the domain. The project was started on July 1, 2002 and lasted 12 months. STORK's main objectives were:

- "to produce a research roadmap for cryptologic research for FP6; critical goals and challenges facing the providers and users of cryptology;
- to define the main parties and relevant interests and stake-holders in the area of cryptology and its applications;
- to identify the gaps between the state of the art in cryptologic research and current and forthcoming requirements for cryptographic algorithms and techniques;
- to develop a shared agenda for research in cryptology;
- to lay the groundwork for a Network of Excellence in Cryptology, under the FP6;

E-CRYPT is a new network of excellence in FP6 which will span the next five years and is a broad consortium of about 30 partners (both from the academia and the industry) in the area of Cryptography and Watermarking. The network is divided into four "virtual labs" one of which will be devoted to symmetric key cryptography.

9 Conclusions

This paper surveyed the state of the art in symmetric key encryption. Since 1998 there has been considerable progress in cryptanalysis and design of symmetric ciphers. Old encryption standard DES was replaced by a new encryption standard AES, which was a result of open call and public evaluation. Important initiatives trying to bridge gaps between academy and industry: NESSIE and CRYPTREC have been carried out.

References

[1] R. Anderson and M. Roe, "A5," Technical report, 1994. `http://jya.com/crack-a5.htm`.

[2] S. Babbage, "Improved "exhaustive search" attacks on stream ciphers," in *ECOS 95 (European Convention on Security and Detection)*, no. 408 in IEE Conference Publication, May 1995.

[3] S. Babbage and L. Frisch, "On MISTY1 higher order differential cryptanalysis," in *International Conference on Information Security and Cryptology, ICISC 2000* (D. Won, ed.), vol. 2015 of *Lecture Notes in Computer Science*, pp. 22–36, Springer-Verlag, 2001.

[4] E. Barkan and E. Biham, "In how many ways can you write Rijndael?," in *Proceedings of Asiacrypt'02* (Y. Zheng, ed.), no. 2501 in Lecture Notes in Computer Science, pp. 160–175, Springer-Verlag, 2002. `NES/DOC/TEC/WP5/025`. Also in *Proceedings of the Third NESSIE Workshop*, 2002.

[5] E. Barkan, E. Biham, and N. Keller, "Instant ciphertext-only cryptanalysis of GSM encrypted communication," in *Advances in Cryptology – CRYPTO 2003* (D. Boneh, ed.), 2003.

[6] T. A. Berson, "Long key variants of DES," in *Advances in Cryptology – CRYPTO'82*, pp. 311–313, 1983.

[7] E. Biham, ed., *Advances in Cryptology – EUROCRYPT 2003*, Lecture Notes in Computer Science, Springer-Verlag, 2003.

[8] E. Biham and A. Biryukov, "How to strengthen DES using existing hardware," in *Advances in Cryptology – ASIACRYPT'94* (J. Pieprzyk and R. Safavi-Naini, eds.), vol. 917 of *Lecture Notes in Computer Science*, pp. 398–412, Springer-Verlag, 1995.

[9] E. Biham and A. Biryukov, "An Improvement of Davies' Attack on DES," *Journal of Cryptology*, vol. 10, no. 3, pp. 195–206, 1997.

[10] E. Biham, A. Biryukov, and A. Shamir, "Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials," in *Proceedings of Eurocrypt'99* (J. Stern, ed.), no. 1592 in Lecture Notes in Computer Science, pp. 12–23, Springer-Verlag, 1999.

[11] E. Biham, A. Biryukov, and A. Shamir, "Miss in the middle attacks on IDEA and Khufu," in Knudsen [73], pp. 124–138.

[12] E. Biham, A. Biryukov, and A. Shamir, "Miss in the middle attacks on IDEA, Khufu, and Khafre," in *Proceedings of Fast Software Encryption – FSE'99* (L. R. Knudsen, ed.), no. 1636 in Lecture Notes in Computer Science, pp. 124–138, Springer-Verlag, 1999.

[13] E. Biham and O. Dunkelman, "Cryptanalysis of the A5/1 GSM stream cipher," in *Progress in Cryptology – INDOCRYPT 2000* (B. K. Roy and E. Okamoto, eds.), vol. 1977 of *Lecture Notes in Computer Science*, pp. 43–51, Springer-Verlag, 2000.

[14] E. Biham, O. Dunkelman, and N. Keller, "The rectangle attack – rectangling the Serpent," in *Proceedings of Eurocrypt'01* (B. Pfitzmann, ed.), no. 2045 in Lecture Notes in Computer Science, pp. 340–357, Springer-Verlag, 2001.

[15] E. Biham, O. Dunkelman, and N. Keller, "New results on boomerang and rectangle attacks," in *Proceedings of Fast Software Encryption – FSE'02* (J. Daemen and V. Rijmen, eds.), no. 2365 in Lecture Notes in Computer Science, pp. 1–16, Springer-Verlag, 2002. `NES/DOC/TEC/WP5/018`.

[16] E. Biham and N. Keller, "Cryptanalysis of reduced variants of Rijndael," in *Proceedings of the Third AES Candidate Conference* [102].

[17] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," pp. 2–21, 1990.

[18] E. Biham and A. Shamir, *Differential Cryptanalysis of the Data Encryption Standard*. Springer-Verlag, 1993.

[19] A. Biryukov, "Analysis of involutional ciphers: KHAZAD and ANUBIS," in *Proceedings of Fast Software Encryption – FSE'03* (T. Johansson, ed.), p. 45.

[20] A. Biryukov and C. De Cannière, "Block ciphers and systems of quadratic equations," in *Fast Software Encryption, FSE 2003* (T. Johansson, ed.), to appear in *Lecture Notes in Computer Science*, Springer-Verlag, 2003.

[21] A. Biryukov, C. De Cannière, A. Braeken, and B. Preneel, "A toolbox for cryptanalysis: Linear and affine equivalence algorithms," in Biham [7].

[22] A. Biryukov and A. Shamir, "Cryptanalytic time/memory/data tradeoffs for stream ciphers," in *Proceedings of Asiacrypt'00* (T. Okamoto, ed.), no. 1976 in Lecture Notes in Computer Science, pp. 1–13, Springer-Verlag, 2000.

[23] A. Biryukov, A. Shamir, and D. Wagner, "Real time cryptanalysis of A5/1 on a PC," in *Proceedings of Fast Software Encryption – FSE'00* (B. Schneier, ed.), no. 1978 in Lecture Notes in Computer Science, pp. 1–18, Springer-Verlag, 2000.

[24] A. Biryukov and D. Wagner, "Slide attacks," in *Proceedings of Fast Software Encryption – FSE'99* (L. R. Knudsen, ed.), no. 1636 in Lecture Notes in Computer Science, pp. 245–259, Springer-Verlag, 1999.

[25] A. Biryukov and D. Wagner, "Advanced slide attacks," in Preneel [112], pp. 589–606.

[26] M. Blunden and A. Escott, "Related key attacks on reduced round KASUMI," in *Proceedings of Fast Software Encryption – FSE'01* (M. Matsui, ed.), Lecture Notes in Computer Science, pp. 277–285, Springer-Verlag, 2001.

[27] M. Briceno, I. Goldberg, and D. Wagner, "A pedagogical implementation of A5/1," Technical report, 1999. web publication, `http://www.scard.org/gsm/body.html`.

[28] L. Brown and J. Seberry, "Key scheduling in DES type cryptosystems," in *Auscrypt'90* (J. Seberry and J. Pieprzyk, eds.), vol. 453 of *Lecture Notes in Computer Science*, pp. 221–228, Springer-Verlag, 1990.

[29] Bureau of Industry and Security, “Commercial encryption export controls,” Technical report, U.S. Department of Commerce, `http://www.bxa.doc.gov/Encryption/Default.htm`, 2003.

[30] V. V. Chepyzhov, T. Johansson, and B. Smeets, “A simple algorithm for fast correlation attacks on stream ciphers,” in *Proceedings of Fast Software Encryption – FSE’00* (B. Schneier, ed.), no. 1978 in Lecture Notes in Computer Science, pp. 181–195, Springer-Verlag, 2000.

[31] P. Chose, A. Joux, and M. Mitton, “Fast correlation attacks: An algorithmic point of view,” in Knudsen [74], pp. 209–221.

[32] Coppersmith, “The Data Encryption Standard (DES) and its strength against attacks,” *IBM Journal of Research and Development.*, vol. 38, no. 3, pp. 243–250, 1994.

[33] D. Coppersmith, S. Halevi, and C. S. Jutla, “Cryptanalysis of stream ciphers with linear masking,” in *Proceedings of Crypto’02* (M. Yung, ed.), no. 2442 in Lecture Notes in Computer Science, pp. 515–532, Springer-Verlag, 2002. Also available at `http://eprint.iacr.org/2002/020/`.

[34] N. T. Courtois, “Higher order correlation attacks, XL algorithm, and cryptanalysis of Toyocrypt,” in *Proceedings of ICISC’02* (K. Kim, ed.), no. 2587 in Lecture Notes in Computer Science, Springer-Verlag, 2002. Also available at `http://eprint.iacr.org/2002/087/`.

[35] N. T. Courtois, A. Klimov, J. Patarin, and A. Shamir, “Efficient algorithms for solving overdefined systems of multivariate polynomial equations,” in Preneel [112], pp. 392–407.

[36] N. T. Courtois and W. Meier, “Algebraic attacks on stream ciphers with linear feedback,” in Biham [7], pp. 345–359.

[37] N. T. Courtois and J. Pieprzyk, “Cryptanalysis of block ciphers with overdefined systems of equations,” in *Advances in Cryptology – ASIACRYPT 2002* (Y. Zheng, ed.), vol. 2501 of *Lecture Notes in Computer Science*, pp. 267–287, Springer-Verlag, 2002. Earlier version available from `http://www.iacr.org`.

[38] J. Daemen, L. R. Knudsen, and V. Rijmen, “The block cipher Square,” in *Proceedings of Fast Software Encryption – FSE’97* (E. Biham, ed.), no. 1267 in Lecture Notes in Computer Science, pp. 149–165, Springer-Verlag, 1997.

[39] J. Daemen and V. Rijmen, “The wide trail design strategy,” in *Proceedings of Cryptography and Coding – CC’01* (B. Honary, ed.), no. 2260 in Lecture Notes in Computer Science, pp. 222–238, Springer-Verlag, 2001.

[40] J. Daemen and V. Rijmen, *The Design of Rijndael: AES — The Advanced Encryption Standard*. Springer-Verlag, 2002.

[41] D. W. Davies and S. Murphy, “Pairs and triplets of DES S-Boxes,” *Journal of Cryptology*, vol. 8, pp. 1–25, 1995.

[42] W. Diffie and M. Hellman, “Exhaustive cryptanalysis of the NBS data encryption standard,” *Computer*, vol. 10, no. 6, pp. 74–84, 1997.

[43] P. Ekdahl and T. Johansson, “Some results on correlations in the bluetooth stream generator,” in *10th Joint conference on communications and coding*, pp. 210–224, 2000.

[44] P. Ekdahl and T. Johansson, “Another attack on A5/1,” *IEEE Transactions on Information Theory*, vol. 49, pp. 1–7, 2003.

[45] Electronic Frontier Foundation (EFF), “DES cracker.” `http://www.eff.org/DEScracker/`, 1998.

[46] H. Feistel, “Cryptography and computer privacy,” *Scientific American*, vol. 228, pp. 15–23, May 1973.

[47] N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D. Wagner, and D. Whiting, "Improved cryptanalysis of Rijndael," in *Fast Software Encryption, FSE 2000* (B. Schneier, ed.), vol. 1978 of *Lecture Notes in Computer Science*, pp. 213–230, Springer-Verlag, 2001.

[48] N. Ferguson, R. Schroeppel, and D. Whiting, "A simple algebraic representation of Rijndael," in Vaudenay and Youssef [127], pp. 103–111.

[49] S. R. Fluhrer, "Improved key recovery of level 1 of the Bluetooth encryption system." Cryptology ePrint Archive: Report 2002/068, `http://eprint.iacr.org/2002/068/`.

[50] S. R. Fluhrer and S. Lucks, "Analysis of the E0 encryption system," in Vaudenay and Youssef [127], pp. 38–48.

[51] S. R. Fluhrer and D. A. McGrew, "Statistical analysis of the alleged RC4 stream cipher," in *Proceedings of Fast Software Encryption – FSE'00* (B. Schneier, ed.), no. 1978 in Lecture Notes in Computer Science, pp. 19–30, Springer-Verlag, 2000.

[52] J. Fuller and W. Millan, "On linear redundancy in S-boxes," in *Proceedings of Fast Software Encryption – FSE'03* (T. Johansson, ed.), no. 2887 in Lecture Notes in Computer Science, pp. 74–86, Springer-Verlag, 2003. Earlier version available at `http://eprint.iacr.org/2002/111/`.

[53] W. Fumy, ed., *Advances in Cryptology – EUROCRYPT'97*, vol. 1233 of *Lecture Notes in Computer Science*, Springer-Verlag, 1997.

[54] H. Gilbert and M. Minier, "A collision attack on seven rounds of Rijndael," in *Proceedings of the Third AES Candidate Conference* [102], pp. 230–241.

[55] O. Goldreich and L. A. Levin, "A hard core predicate for any one way function," in *Proceedings of Symposium on Theory of Computing – STOC'89*, pp. 25–32, ACM Press, 1989.

[56] J. D. Golic, "Cryptanalysis of alleged A5 stream cipher," in Fumy [53], pp. 239–255.

[57] J. D. Golic, "Linear statistical weakness of alleged RC4 keystream generator," in Fumy [53], pp. 226–238.

[58] J. D. Golic, V. Bagini, and G. Morgari, "Linear cryptanalysis of bluetooth stream cipher," in Knudsen [74], pp. 238–255.

[59] J. Håstad and M. Nāslund, "BMGL: Synchronous key-stream generator with provable security." Primitive submitted to NESSIE, Sept. 2000.

[60] J. Håstad and M. Nāslund, "Improved analysis of the BMGL keystream generator," in *Proceedings of the Second NESSIE Workshop*, 2001.

[61] P. Hawkes and G. G. Rose, "On the applicability of distinguishing attacks against stream ciphers," in *Proceedings of the Third NESSIE Workshop*, 2002.

[62] T. Helleseth, ed., *Advances in Cryptology – EUROCRYPT'93*, vol. 765 of *Lecture Notes in Computer Science*, Springer-Verlag, 1993.

[63] M. Hermelin and K. Nyberg, "Correlation properties of the Bluetooth combiner generator," in *International Conference on Information Security and Cryptology, ICISC 1999* (J. Song, ed.), vol. 1787 of *Lecture Notes in Computer Science*, pp. 17–29, Springer-Verlag, 2000.

[64] S. Hong, S. Lee, J. Lim, J. Sung, D. Cheon, and I. Cho, "Provable security against differential and linear cryptanalysis for the SPN structure," in *Proceedings of Fast Software Encryption – FSE'00* (B. Schneier, ed.), no. 1978 in Lecture Notes in Computer Science, pp. 273–283, Springer-Verlag, 2000.

[65] T. Johansson and F. Jönsson, "Improved fast correlation attacks on stream ciphers via convolution codes," in *Proceedings of Eurocrypt'99* (J. Stern, ed.), no. 1592 in Lecture Notes in Computer Science, pp. 347–362, Springer-Verlag, 1999.

[66] T. Johansson and F. Jönsson, "Fast correlation attacks through reconstruction of linear polynomials," in *Proceedings of Crypto'00* (M. Bellare, ed.), no. 1880 in Lecture Notes in Computer Science, pp. 300–315, Springer-Verlag, 2000.

[67] P. Junod, "On the complexity of Matsui's attack," in Vaudenay and Youssef [127], pp. 199–211.

[68] J. Kelsey, T. Kohno, and B. Schneier, "Amplified boomerang attacks against reduced-round MARS and Serpent," in *Proceedings of Fast Software Encryption – FSE'00* (B. Schneier, ed.), no. 1978 in Lecture Notes in Computer Science, pp. 75–93, Springer-Verlag, 2000.

[69] J. Kilian and P. Rogaway, "How to protect DES against exhaustive key search," in *Advances in Cryptology – CRYPTO'96* (N. Koblitz, ed.), vol. 1109 of *Lecture Notes in Computer Science*, pp. 252–267, Springer-Verlag, 1996.

[70] A. Kipnis and A. Shamir, "Cryptanalysis of the HFE public key cryptosystem," in *Proceedings of Crypto'99* (M. J. Wiener, ed.), no. 1666 in Lecture Notes in Computer Science, pp. 19–30, Springer-Verlag, 1999.

[71] L. R. Knudsen, "Practically secure Feistel cyphers," in *Fast Software Encryption, FSE'93* (R. J. Anderson, ed.), vol. 809 of *Lecture Notes in Computer Science*, pp. 211–221, Springer-Verlag, 1994.

[72] L. R. Knudsen, "Block ciphers - a survey," in *State of the Art in Applied Cryptography* (B. Preneel and V. Rijmen, eds.), no. 1528 in Lecture Notes in Computer Science, pp. 18–48, Springer-Verlag, 1998.

[73] L. R. Knudsen, ed., *Fast Software Encryption, FSE'99*, vol. 1636 of *Lecture Notes in Computer Science*, Springer-Verlag, 1999.

[74] L. R. Knudsen, ed., *Advances in Cryptology – EUROCRYPT 2002*, vol. 2332 of *Lecture Notes in Computer Science*, Springer-Verlag, 2002.

[75] L. R. Knudsen, W. Meier, B. Preneel, V. Rijmen, and S. Verdoolaege, "Analysis methods for (alleged) RC4," in *Advances in Cryptology – ASIACRYPT'98* (K. Ohta and D. Pei, eds.), vol. 1514 of *Lecture Notes in Computer Science*, pp. 327–341, Springer-Verlag, 1998.

[76] L. R. Knudsen, "DEAL - a 128-bit block cipher," Technical report 151, Dept. of Informatics, University of Bergen, Norway, 1998.

[77] L. R. Knudsen and D. Wagner, "Integral cryptanalysis (extended abstract)," in *Proceedings of Fast Software Encryption – FSE'02* (J. Daemen and V. Rijmen, eds.), no. 2365 in Lecture Notes in Computer Science, pp. 112–127, Springer-Verlag, 2002.

[78] M. Krause, "Bdd-based cryptanalysis of keystream generators," in Knudsen [74], pp. 222–237.

[79] U. Kühn, "Cryptanalysis of reduced-round MISTY," in *Proceedings of Eurocrypt'01* (B. Pfitzmann, ed.), no. 2045 in Lecture Notes in Computer Science, pp. 325–339, Springer-Verlag, 2001.

[80] U. Kühn, "Improved cryptanalysis of MISTY1," in *Proceedings of Fast Software Encryption – FSE'02* (J. Daemen and V. Rijmen, eds.), no. 2365 in Lecture Notes in Computer Science, pp. 61–75, Springer-Verlag, 2002. Also in *Proceedings of the Second NESSIE Workshop*, 2001.

[81] X. Lai and J. L. Massey, "A proposal for a new block encryption standard," in *Proceedings of Eurocrypt'90* (I. B. Damgard, ed.), no. 473 in Lecture Notes in Computer Science, pp. 389–404, Springer-Verlag, 1990.

[82] S. Lucks, "Attacking triple encryption," in *Fast Software Encryption, FSE'98* (S. Vaudenay, ed.), vol. 1372 of *Lecture Notes in Computer Science*, pp. 239–257, Springer-Verlag, 1998.

[83] S. Lucks, "Attacking seven rounds of Rijndael under 192-bit and 256-bit keys," in *Proceedings of the Third AES Candidate Conference* [102], pp. 215–229.

[84] I. Mantin and A. Shamir, "A practical attack on broadcast RC4," in *Proceedings of Fast Software Encryption – FSE'01* (M. Matsui, ed.), no. 2355 in Lecture Notes in Computer Science, pp. 152–164, Springer-Verlag, 2001.

[85] M. Matsui, "Linear cryptanalysis method for DES cipher," in Helleseth [62], pp. 386–397.

[86] M. Matsui, "The first experimental cryptanalysis of the data encryption standard," in *Advances in Cryptology – CRYPTO'94* (Y. Desmedt, ed.), vol. 839 of *Lecture Notes in Computer Science*, pp. 1–11, Springer-Verlag, 1994.

[87] M. Matsui, "On correlation between the order of S-boxes and the strength of DES," in *Proceedings of Eurocrypt'94* (A. De Santis, ed.), no. 950 in Lecture Notes in Computer Science, pp. 366–375, Springer-Verlag, 1995.

[88] M. Matsui, "Block encryption MISTY," *ISEC96-11*, 1996.

[89] M. Matsui, "Block encryption algorithm MISTY," in *Proceedings of Fast Software Encryption – FSE'97* (E. Biham, ed.), no. 1267 in Lecture Notes in Computer Science, pp. 64–74, Springer-Verlag, 1997.

[90] M. Matsui and A. Yamagishi, "A new method for known plaintext attack of FEAL cipher," in *Proceedings of Eurocrypt'92* (R. A. Rueppel, ed.), no. 658 in Lecture Notes in Computer Science, pp. 81–91, Springer-Verlag, 1992.

[91] A. Menezes and S. A. Vanstone, eds., *Advances in Cryptology – CRYPTO'90*, vol. 537 of *Lecture Notes in Computer Science*, Springer-Verlag, 1990.

[92] R. C. Merkle, "Fast software encryption functions," in Menezes and Vanstone [91], pp. 476–501.

[93] R. C. Merkle and M. E. Hellman, "On the security of multiple encryption," *Communications of the ACM*, vol. 24, 1981.

[94] B. Meyer, "About the NESSIE submission BMGL: Synchronous keystream generator with provable security," Public report, NESSIE, 2001. `NES/DOC/SAG/WP3/018`.

[95] M. J. Mihaljević, M. P. C. Fossorier, and H. Imai, "Fast correlation attack with list decoding and an application," in *Proceedings of Fast Software Encryption – FSE'01* (M. Matsui, ed.), no. 2355 in Lecture Notes in Computer Science, pp. 196–210, Springer-Verlag, 2001.

[96] I. Mironov, "(Not So) Random Shuffles of RC4," in Yung [129], pp. 304–319.

[97] S. Mister and S. E. Tavares, "Cryptanalysis of RC4-like ciphers," in *Selected Areas in Cryptography, SAC 98* (S. E. Tavares and H. Meijer, eds.), vol. 1556 of *Lecture Notes in Computer Science*, pp. 131–143, Springer-Verlag, 1998.

[98] S. Miyaguchi, "The FEAL-8 cryptosystem and a call for attack," in *Advances in Cryptology – CRYPTO'89* (G. Brassard, ed.), vol. 435 of *Lecture Notes in Computer Science*, pp. 624–627, Springer-Verlag, 1990.

[99] S. Miyaguchi, "The FEAL cipher family," in Menezes and Vanstone [91], pp. 627–638.

[100] S. Murphy and M. J. B. Robshaw, "Essential algebraic structure within the AES," in Yung [129], pp. 17–38.

[101] National Institute of Standards and Technology, "FIPS-46-3: Data Encryption Standard (DES)," May 1999. Available at `http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf`.

[102] National Institute of Standards and Technology, *Proceedings of the Third AES Candidate Conference*, Apr. 2000.

[103] National Institute of Standards and Technology, *Advanced Encryption Standard*. FIPS-197, NIST, Nov. 2001. Available at `http://csrc.nist.gov/encryption/`.

[104] NESSIE Project – New European Schemes for Signatures, Integrity and Encryption. http://cryptonessie.org.

[105] NIST, "ADVANCED ENCRYPTION STANDARD (AES) questions and answers." http://csrc.nist.gov/CryptoToolkit/aes/aesfact.html http://csrc.nist.gov/encryption/aes/.

[106] NIST, "National Institute of Standards and Technology (NIST)." http://www.nist.gov/.

[107] NIST, "Skipjack and KEA algorithm specification," Technical report, http://csrc.nist.gov/CryptoToolkit/skipjack/skipjack-kea.htm, 1998. Version 2.0.

[108] K. Nyberg, "Differentially uniform mappings for cryptography," in Helleseth [62], pp. 55–64.

[109] K. Nyberg and L. R. Knudsen, "Provable security against a differential attack," *Journal of Cryptology*, vol. 8, no. 1, pp. 27–38, 1995.

[110] L. of the IEEE CS, "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications," Technical report, 1999. IEEE Standard 802.11.

[111] G. O. Partners, "Specification of the 3GPP confidentiality and integrity algorithms: Kasumi algorithm specification – 3GPP TS 35.202," Technical report, http://www.3gpp.org/TB/Other/algorithms.htm, 2000.

[112] B. Preneel, ed., *Advances in Cryptology – EUROCRYPT 2000*, vol. 1807 of *Lecture Notes in Computer Science*, Springer-Verlag, 2000.

[113] J.-J. Quisquater, Y. Desmedt, and M. Davio, "The importance of "good" key scheduling schemes (how to make a secure DES scheme with ≤ 48 bit keys)," in *Advances in Cryptology – CRYPTO'85* (H. C. Williams, ed.), vol. 218 of *Lecture Notes in Computer Science*, pp. 537–542, Springer-Verlag, 1986.

[114] sci.crypt, "Subject: DES and differential cryptanalysis." unpublished, http://www.esat.kuleuven.ac.be/~abiryuko/coppersmith_letter.txt, 1992.

[115] A. Shimizu and S. Miyaguchi, "Fast data encipherment algorithm FEAL," in *Advances in Cryptology – EUROCRYPT'87* (D. Chaum and W. L. Price, eds.), vol. 304 of *Lecture Notes in Computer Science*, pp. 267–278, Springer-Verlag, 1988.

[116] B. SIG, "Bluetooth specification," Technical report, http://www.bluetooth.com. Version 1.0B.

[117] J. L. Smith, "The design of Lucifer: A cryptographic device for data communications," Technical report, IBM T.J. Watson Research Center, Yorktown Heights, N.Y., 10598, U.S.A., 1971.

[118] P. Souradyuti and B. Preneel, "Non-fortitous RC4 key stream generator," in *Progress in Cryptology – INDOCRYPT 2003* (T. Johansson and S. Maitra, eds.), pp. 318–325, 2003.

[119] STORK Strategic Roadmap for Crypto, "EU fifth framework programme (FP5) thematic project," Technical report, http://www.stork.eu.org/, 2003.

[120] STORK Strategic Roadmap for Crypto, "Public STORK documents," Technical report, http://www.stork.eu.org/documents.html, 2003.

[121] A. Stubblefield, J. Loannidis, and A. Rubin, "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP," Technical report, AT&T Labs, Florham park, NJ, 2001.

[122] M. Sugita, "Higher order differential attack on block cipher MISTY1, 2," Technical report ISEC98-4, IEICE, May 1998.

[123] H. Tanaka, K. Hisamatsu, and T. Kaneko, "Strength of MISTY1 without FL function for higher order differential attack," in *Proceedings of AAECC'99*

(M. Fossorier, H. Imai, S. Lin, and A. Poli, eds.), no. 1719 in Lecture Notes in Computer Science, pp. 221–230, Springer-Verlag, 1999.

[124] H. Tanaka, C. Ishii, and T. Kaneko, "On the strength of KASUMI without FL functions against higher order differential attack," in *Proceedings of ICISC'00* (D. Won, ed.), no. 2015 in Lecture Notes in Computer Science, pp. 14–21, Springer-Verlag, 2000.

[125] P. C. van Oorschot and M. J. Wiener, "A known plaintext attack on two-key triple encryption," in *Advances in Cryptology – EUROCRYPT'90* (I. Damgård, ed.), vol. 473 of *Lecture Notes in Computer Science*, pp. 318–325, Springer-Verlag, 1990.

[126] S. Vaudenay, "Provable security for block ciphers by decorrelation," in *STACS*, Lecture Notes in Computer Science, pp. 249–275, Springer-Verlag, 1998.

[127] S. Vaudenay and A. M. Youssef, eds., *Selected Areas in Cryptography, SAC 2001*, vol. 2259 of *Lecture Notes in Computer Science*, Springer-Verlag, 2001.

[128] D. Wagner, "The boomerang attack," in Knudsen [73], pp. 156–170.

[129] M. Yung, ed., *Advances in Cryptology – CRYPTO 2002*, vol. 2442 of *Lecture Notes in Computer Science*, Springer-Verlag, 2002.

[130] "Advanced encryption algorithm (AES) development effort," 1997–2000. `http://csrc.nist.gov/encryption/aes/`.

[131] "CRYPTREC project," 2000–2002. `http://www.ipa.go.jp/security/enc/CRYPTREC/`.

[132] "Modes of operation for symmetric key block ciphers," 2000–2002. `http://csrc.nist.gov/encryption/modes/`.

[133] "New European Schemes for Signatures, Integrity, and Encryption, deliverables of the NESSIE project," 2003. `https://www.cosic.esat.kuleuven.ac.be/nessie/deliverables/`.