Which eSTREAM ciphers have been broken?

Daniel J. Bernstein *

Department of Mathematics, Statistics, and Computer Science (M/C 249)
The University of Illinois at Chicago
Chicago, IL 60607–7045
snuffle6@box.cr.yp.to

Abstract. This paper summarizes the impact of known attacks on the stream ciphers submitted to eSTREAM. This paper focuses on "software phase 3" ciphers and "hardware phase 3" ciphers, but it also discusses the eSTREAM submissions that did not advance to phase 3.

1 Introduction

This paper looks back at three years of cryptanalysis of the stream ciphers submitted to eSTREAM, the ECRYPT Stream Cipher Project. Which ciphers have been broken? Which ciphers have survived cryptanalysis?

Section 3 summarizes the status of the "software phase 3" ciphers (CryptMT, Dragon, HC, LEX, NLS, Rabbit, Salsa20, SOSEMANUK). Section 4 summarizes the status of the "hardware phase 3" ciphers (DECIM, Edon80, F-FCSR, Grain, MICKEY, Moustique, Pomaranch, Trivium). Section 5 summarizes the status of ciphers that did not advance to phase 3 of eSTREAM (ABC, Achterbahn, DICING, Frogbit, Fubuki, Hermes, MAG, Mir, Phelix, Polar Bear, ProVEST, Py, SFINKS, SSS, TPy, TSC, WG, YAMB, and ZK-Crypt).

If a cipher has multiple versions, the versions are listed in the same section but are otherwise treated as separate ciphers. For example, CryptMT v1, CryptMT v2, and CryptMT v3 appear separately in my table of attacks in Section 3. Note that eSTREAM's "phase 3" ciphers are usually the newest versions of ciphers—for example, CryptMT v3 is a phase 3 cipher, while CryptMT v1 and CryptMT v2 are not.

Occasionally—especially in Section 5—there are disputes as to whether a cipher is actually broken. Section 2 discusses what it means for a cipher to be secure.

I also have a web page `http://cr.yp.to/streamciphers/attacks.html` that includes non-eSTREAM ciphers. I intend to keep the web page up to date after the end of eSTREAM, both for eSTREAM ciphers and for non-eSTREAM ciphers.

* Permanent ID of this document: `83331cc746de71bc71540a0f372acbf6`. Date of this document: 2008.02.21. This work was supported by the National Science Foundation under grant ITR–0716498.

1.1 Will all the unbroken ciphers stay unbroken?

Some of the eSTREAM submissions were published earlier than others—for example, Rabbit first appeared at FSE 2003, while HC-128 first appeared in June 2006—but all of the submissions have undergone considerable scrutiny by cryptanalysts.

Maybe the cryptanalysts have missed something. Maybe better attacks will be developed. Possible future attacks on eSTREAM submissions will inevitably by the subject of speculation: "every previous RC4-style cipher is insecure, so HC can't possibly be secure"; "surely LEX will be broken by algebraic attacks"; "SOSEMANUK is too complicated for any cryptanalysts to have really looked at it"; "anything as simple as Trivium will inevitably be broken"; etc. But this sort of speculation strikes me as increasingly silly if nobody is able to turn the speculation into a working attack! This paper classifies ciphers according to the expense of *known* attacks.

2 What does security mean?

This paper uses the standard definition of cipher security: a cipher is not secure ("not a PRF," say the theoreticians) if its output, given a uniform random key, is distinguishable from a uniform random string. This section discusses the definition in more detail.

2.1 Is a definition necessary?

In most cases, the definition of security doesn't matter. A typical cipher attack is acknowledged by the designer and leads to the designer withdrawing the cipher proposal. Once a cipher has been withdrawn, the cipher is avoided by practically all users, and the cipher's actual security becomes a purely academic question.

There have, however, been several cases where the designer disputes the attack, saying that the attack doesn't actually break the cipher. Sometimes the dispute is about whether the attack performs as specified, but sometimes the dispute is about whether the specified performance constitutes a break. In the latter cases it becomes important for the attacker, and for the designer, to understand what security means.

2.2 Doesn't an attack have to recover the key?

No. Attacks are not required to, and often do not, recover the key. Example: Wu and Preneel showed that, out of 2^{23} carefully selected nonces for Py, about 2^7 produce identical output streams, leaking a tremendous amout of information about the corresponding plaintexts. This attack does not recover the Py key, but it distinguishes the cipher output from uniform.

As another example, consider the cipher C that expands a key k and nonce n into the keystream $C(k, n) = \text{Hermes8F}(\text{MD5}(k), n)$. Given a few bytes of

$C(k, 0)$, the Babbage–Cid–Pramstaller–Raddum attack on Hermes8F quickly computes MD5(k) and therefore reveals $C(k, 1)$, $C(k, 2)$, etc. This attack does not recover k, but it nevertheless distinguishes the cipher output from uniform; C is not secure. Drawing a line between Hermes8F and C, on the grounds that Hermes8F allows key recovery while C (as far as we know) does not, would be foolish.

2.3 Doesn't an attack have to do more than distinguish from uniform?

Novice cryptographers often criticize the standard definition and claim that a distinguisher is merely a "theoretical" or "certificational" attack. This criticism is fundamentally misplaced. The simple fact is that, at least for some plaintext distributions, a distinguisher allows the attacker to check his guesses for the plaintext, blatantly violating the privacy that encryption is meant to ensure.

Example: A user sends his stockbroker one encrypted message each day. On special days, the plaintext says "BUY SHARES TODAY"; on other days, to foil traffic analysis, the plaintext contains random garbage that the receiver will throw away. In other words, on special days, the ciphertext xor "BUY SHARES TODAY" is exactly the cipher keystream; on other days, the ciphertext xor "BUY SHARES TODAY" is random garbage. A distinguishing attack tells us whether a string is keystream or random garbage, so it tells us which days are special—at least with better probability than the attacker would otherwise have had.

2.4 What if an attack needs many bytes of keystream?

Many ciphers require users to change keys after a limited amount of data. For example, LEX users are required to use a key k for at most 2^{32} nonces n, and to use a pair (k, n) for at most 2^9 output blocks. Switching keys fairly frequently is an annoyance for cryptographic protocol designers and implementors but isn't terribly expensive for the end user; as a designer I try to avoid such small limits but I certainly can't argue (and I haven't heard anyone else argue) that these limits make ciphers unusable.

Of course, if the user accepts only 32-bit nonces and stops generating data after 2^9 output blocks, then there are only 2^{41} output blocks that the attacker can ever see. The attacker's job is to distinguish those 2^{41} output blocks from uniform. "Attacks" that require more data simply don't work.

Sometimes cipher designers have responded to attacks by pointing to specified limits—or specifying new limits—on the amount of data generated from a key. In these cases, I have noted those limits in my tables, and focused entirely on the security of output generated within those limits.

2.5 What if an attack needs expensive computations?

Words such as "distinguishable" and "secure" are implicitly parametrized by limits on the amount of computation that can be carried out by the attacker.

The best generic attack, the attack that a competent attacker will use if he doesn't know any better attack against a particular cipher, is a parallel brute-force search for the key. Brute force can be run for a fraction as much time; its chance of success drops linearly with the time spent. Brute force can also find the keys for many different users in only marginally more time than finding the key for 1 user. See my paper [27] for further discussion of the power of a parallel brute-force key-searching machine.

Other attacks are pointless unless they are better than a parallel brute-force search. An attack machine that costs as much as P parallel brute-force key-searching circuits, that runs for T times as long as a key test, and that targets U keys, each key having K bits, must succeed with probability more than (approximately) $PTU/2^K$; otherwise an attacker will prefer brute force. A surprisingly large number of the "attacks" in the cryptographic literature flunk this simple requirement.

Some attacks are faster than brute force but still completely infeasible. The cost of brute force grows exponentially with K, the number of key bits, and for moderately large K is far beyond the resources available to an attacker. For example, a brute-force search for a 256-bit SOSEMANUK key is inconceivable. The Ahmadi–Eghlidos–Khazaei attack on SOSEMANUK is a billion times faster, taking only 2^{226} simple operations, but is still far beyond any computation that will ever be carried out. This attack did not stop SOSEMANUK from entering phase 3 of eSTREAM.

The minimum acceptable security level is a matter of debate. It is clear that eSTREAM officially allows 80-bit keys, at least for hardware ciphers; obviously some cryptographers think that $K = 80$ makes brute force infeasible. It is not clear whether eSTREAM will allow lower security levels. The recent Grain v1 attack by De Cannière, Kucuk, and Preneel at SASC 2008 is twice as fast as a brute-force search for the 80-bit key; is Grain therefore considered broken? If 2^{79} is not considered a break, what about 2^{78}, or 2^{75}, or 2^{64}? If 2^{75} is considered a break, what about 2^{80} key tests for another cipher where each key test is a hundred times faster?

I predict that future cryptographers will consider $K = 80$ a silly historical mistake and will consider $K = 128$ uncomfortably risky. However, I realize that this viewpoint is not yet universal, so I have used "broken" only for attacks faster than 2^{64} key tests.

2.6 What about side channels?

Cipher security is defined by the cipher output. Side-channel leaks from the cipher computation are not contemplated; their dependence on implementation details makes them qualitatively different from output-only attacks.

Of course, side-channel leaks are a serious real-world problem, as illustrated by the Osvik–Shamir–Tromer theft of AES keys from a Linux disk-encryption device via cache-timing side-channel attacks. Eliminating side-channel leaks can drastically increase costs to the cryptographic user. However, cost issues are outside the scope of this paper.

3 Software phase 3

The eSTREAM committee's "Short report on the end of the second phase" says "While our focus [for software] is on ciphers with 128-bit keys, we have retained companion versions that support 256-bit keys."

The following table shows the cost of the best attacks known against 128-bit "software phase 3" ciphers; against 256-bit versions of those ciphers; and against previous versions of those ciphers. "B-bit security" means that a known attack has comparable cost to 2^B key tests.

Security conjecture	Key size	Cipher
256-bit security	256 bits	CryptMT v1
256-bit security	256 bits	CryptMT v2
256-bit security	256 bits	CryptMT v3
256-bit security	256 bits	Dragon limited to 2^{64} bits per key
256-bit security	256 bits	HC-256
249-bit security	256 bits	Salsa20/8
256-bit security	256 bits	Salsa20/12
256-bit security	256 bits	Salsa20/20
226-bit security	256 bits	SOSEMANUK
128-bit security	128 bits	CryptMT v1
128-bit security	128 bits	CryptMT v2
128-bit security	128 bits	CryptMT v3
128-bit security	128 bits	Dragon limited to 2^{64} bits per key
128-bit security	128 bits	HC-128
128-bit security	128 bits	HC-256
128-bit security	128 bits	LEX v1 limited to 2^{46} bits per key
128-bit security	128 bits	LEX v2 limited to 2^{46} bits per key
withdrawn?	128 bits	NLS v1
128-bit security	128 bits	NLS v2 limited to 2^{64} bits per key
128-bit security	128 bits	Rabbit
128-bit security	128 bits	Salsa20/8
128-bit security	128 bits	Salsa20/12
128-bit security	128 bits	Salsa20/20
128-bit security	128 bits	SOSEMANUK

The rest of this section discusses each of these ciphers in detail.

3.1 CryptMT

2005.04 [112] Matsumoto, Hagita, Nishimura, Saito proposed CryptMT v1; see also 2005.12 [113] Matsumoto, Saito, Nishimura, Hagita for design notes. 2006.01 [114] Matsumoto, Saito, Nishimura, Hagita proposed CryptMT v2. 2007.01 [115] Matsumoto, Saito, Nishimura, Hagita proposed CryptMT v3. Attacks:

- Brute force.

Non-attacks:

- 2005.11 [103] Khazaei, Shakour claimed an attack but later withdrew the claim.

The eSTREAM committee's "Short Report on the End of the Second Phase" announced CryptMT v3 as a "software phase 3" cipher.

3.2 Dragon

2005.04 [42] Chen, Henricksen, Millan, Fuller, Simpson, Dawson, Lee, Moon proposed Dragon. Attacks:

- Dragon modified to output many more words of keystream: 2005.09 [56] Englund, Maximov stated an attack; 2007.01 [45] Cho, Pieprzyk streamlined the attack; 2008.02 Cho further streamlined the attack. 2005.10 [53] Dawson, Henricksen, Millan, Simpson responded that the Dragon-256 documentation had already recommended generating no more than 2^{64} bits per key, making the attack impossible.
- Dragon as specified: Brute force.

The eSTREAM committee's "Short Report on the End of the Second Phase" announced Dragon as a "software phase 3" cipher.

3.3 HC

2005.04 [157] Wu proposed HC-256. 2006.06 Wu proposed HC-128. Attacks:

- HC-128: Brute force.
- HC-256: Brute force.

The eSTREAM committee's "Short Report on the End of the Second Phase" announced "HC-128 (HC-256)" as a "software phase 3" cipher.

3.4 LEX

2005.04 [34] Biryukov proposed LEX v1. 2006.03 [35] Biryukov proposed LEX v2. Attacks:

- LEX v1: 2005.09 [161] Wu, Preneel stated "If a key is used with about 2^{61} random IVs, and 20,000 keystream bytes are generated from each IV, then the key could be recovered easily." In response, designer withdrew LEX v1, despite commenting that the attack does not have better price-performance ratio than brute force.
- LEX v2 modified to output many more words of keystream: 2007.01 [55] Englund, Hell, Johansson pointed out that N LEX nonces, each used for B blocks, have probability approximately $BN^2/2^{128}$ of producing identical keystreams modulo shifts.

- LEX v2 as specified (N limited to 2^{32} and B limited to 2^9): Brute force. The Englund–Hell–Johansson collisions have chance approximately $1/2^{55}$.

Non-attacks:

- 2006.08 [155] Wang, Wang, Wang claimed an attack but later withdrew the claim.

The eSTREAM committee's "Short Report on the End of the Second Phase" announced LEX as a "software phase 3" cipher.

3.5 NLS

2005.04 [135] Rose, Hawkes, Paddon, de Vries proposed NLS v1. 2006.03 [77] Hawkes, Paddon, Rose, de Vries proposed NLS v2. Attacks:

- NLS v1: 2006.01 [43] Cho, Pieprzyk stated an attack. The designers appear to have withdrawn NLS v1 in response, although the record does not make this clear. See also 2006.08 [121] McDonald, Hawkes.
- NLS v2 modified to output many more words of keystream: 2006.09 [44] Cho, Pieprzyk stated that "NLSv2 is distinguishable from a random stream cipher after observing around 2^{74} keystream words." This distinguisher has only about one chance in a billion of succeeding within 2^{64} bytes.
- NLS v2 as specified: Brute force.

The eSTREAM committee's "Short Report on the End of the Second Phase" announced "NLS v2" as a "software phase 3" cipher. The NLS specification had also proposed an optional authenticator, but the eSTREAM committee wrote "Poor performance of the authentication component means that we no longer consider this feature in eSTREAM."

3.6 Rabbit

2005.04 [37] Boesgaard, Vesterager, Christensen, Zenner proposed Rabbit for eSTREAM, after first proposing it at FSE 2003. Attacks:

- Brute force.

Non-attacks:

- 2006.12 [9] [10] Aumasson stated a completely undetectable "bias" of Rabbit.

The eSTREAM committee's "Short Report on the End of the Second Phase" announced Rabbit as a "software phase 3" cipher.

3.7 Salsa20

2005.04 [26] Bernstein proposed Salsa20/20. 2006.02 [29] Bernstein proposed reduced-round ciphers Salsa20/8 and Salsa20/12. Smaller numbers of rounds have also been considered as cryptanalytic targets. Attacks:

- 256-bit Salsa20/5: 2005.10 [48] Crowley reported a 2^{165}-operation attack. 2006.12 [57] Fischer, Meier, Berbain, Biasse, Robshaw reported a much faster attack, clearly breaking Salsa20/5.
- 256-bit Salsa20/6: 2006.12 [57] Fischer, Meier, Berbain, Biasse, Robshaw reported a 2^{177}-operation attack. 2007.01 [144] Tsunoo, Saito, Kubo, Suzaki, Nakashima reported a much faster attack, clearly breaking Salsa20/6.
- 256-bit Salsa20/7: 2007.01 [144] Tsunoo, Saito, Kubo, Suzaki, Nakashima reported a 2^{184}-operation attack. 2007.12 [11] [12] Aumasson, Fischer, Khazaei, Meier, Rechberger reported a 2^{153}-operation attack.
- 256-bit Salsa20/8: 2007.12 [11] [12] Aumasson, Fischer, Khazaei, Meier, Rechberger reported a 2^{249}-operation attack.
- 256-bit Salsa20/9 and above: Brute force.
- 128-bit Salsa20/8 and above: Brute force.

Non-attacks:

- 2005.09 [108] Li, 2005.10 [109] Li claimed distinguishing attacks against any number of rounds of Salsa20. 2005.09 [28] Bernstein showed that the attacks don't work.

The eSTREAM committee's "Short Report on the End of the Second Phase" announced Salsa20 as a "software phase 3" cipher.

3.8 SOSEMANUK

2005.04 [22] Berbain, Billet, Canteaut, Courtois, Gilbert, Goubin, Gouget, Granboulan, Lauradoux, Minier, Pornin, Sibert proposed SOSEMANUK. Attacks:

- 2005.12 [1] Ahmadi, Eghlidos, Khazaei stated an attack on SOSEMANUK taking "2^{226} basic operations"; see also 2006.01 [145] Tsunoo, Saito, Shigeri, Suzaki, Ahmadi, Eghlidos, Khazaei. Authors responded that SOSEMANUK never claimed more than a 128-bit security level.

The eSTREAM committee's "Short Report on the End of the Second Phase" announced SOSEMANUK as a "software phase 3" cipher.

4 Hardware phase 3

The eSTREAM committee's "Short report on the end of the second phase" says "While our focus [for hardware] is on ciphers with 80-bit keys, we have retained companion versions that support 128-bit keys."

The following table shows the cost of the best attacks known against 80-bit and 96-bit "hardware phase 3" ciphers; against previous versions of those ciphers; and against 128-bit versions of those ciphers. "B-bit security" means that a known attack has comparable cost to 2^B key tests.

Security conjecture	Key size	Cipher
128-bit security	128 bits	DECIM-128
withdrawn	128 bits	F-FCSR-8
128-bit security	128 bits	F-FCSR-H
128-bit security	128 bits	F-FCSR-16
128-bit security	128 bits	Grain-128
128-bit security	128 bits	MICKEY-128 v1
128-bit security	128 bits	MICKEY-128 v2
withdrawn	128 bits	Pomaranch (CJCSG) v1
withdrawn	128 bits	Pomaranch v2
128-bit security	128 bits	Pomaranch v3 limited to 2^{64} bits per key
withdrawn	96 bits	Mosquito
90-bit security	96 bits	Moustique
withdrawn	80 bits	DECIM v1
80-bit security	80 bits	DECIM v2
80-bit security	80 bits	Edon80 limited to 2^{64} bits per key
withdrawn	80 bits	F-FCSR-8
80-bit security	80 bits	F-FCSR-H
80-bit security	80 bits	F-FCSR-16
withdrawn	80 bits	Grain v0
79-bit security	80 bits	Grain v1
80-bit security	80 bits	MICKEY v1
80-bit security	80 bits	MICKEY v2
withdrawn	80 bits	Pomaranch (CJCSG) v1
withdrawn	80 bits	Pomaranch v2
80-bit security	80 bits	Pomaranch v3 limited to 2^{64} bits per key
80-bit security	80 bits	Trivium

The rest of this section discusses each of these ciphers in detail.

4.1 DECIM

2005.04 [20] Berbain, Billet, Canteaut, Courtois, Debraize, Gilbert, Goubin, Gouget, Granboulan, Lauradoux, Minier, Pornin, Sibert proposed DECIM v1. 2006.01 [21] Berbain, Billet, Canteaut, Courtois, Debraize, Gilbert, Goubin, Gouget, Granboulan, Lauradoux, Minier, Pornin, Sibert proposed DECIM v2 and DECIM-128. Attacks:

- DECIM v1: 2005.07 [160] Wu, Preneel broke DECIM v1. In response, the designers withdrew DECIM v1: "H. Wu and B. Preneel showed two serious flaws in the stream cipher DECIM."
- DECIM v2: Brute force.
- DECIM-128: Brute force.

The eSTREAM committee's "Short Report on the End of the Second Phase" announced "DECIM v2 (-128)" as a "hardware phase 3" cipher.

4.2 Edon80

2005.04 [63] Gligoroski, Markovski, Kocarev, Gusev proposed Edon80. Attacks:

- Edon80 as originally specified: 2007.09 [83] Hell, Johansson stated an attack against Edon80 using "2^{69} simple operations." The designers disputed the attack, saying that each "simple operation" is more expensive than 2^{11} key tests. This dispute has not been resolved. (The paper does not give a clear statement of what the "simple operations" are.)
- Edon80 modified to produce 2^{64} keystream bits: Brute force.

Non-attacks:

- 2005.06 [85] Hong commented on the period of Edon80. I don't see any attacks stated here. See also 2005.07 [64] Gligoroski, Markovski, Kocarev, Gusev; 2006.01 [62] Gligoroski, Markovski, Knapskog.
- 2007.01 [150] [151] Vojvoda, Sys, Jokay commented on the quasigroups used in Edon80.
- 2007.09 [36] Bjørstad commented on the Edon80 S-box.

The eSTREAM committee's "Short Report on the End of the Second Phase" announced "Edon-80" as a "hardware phase 3" cipher.

4.3 F-FCSR

2005.04 [25] Berger, Arnault, Lauradoux proposed F-FCSR-8. 2005.10 [6] [7] Arnault, Berger, Lauradoux proposed F-FCSR-H and F-FCSR-16; see also 2007.01 [8] Arnault, Berger, Minier. Attacks:

- F-FCSR-8: 2005.07 [94] Jaulmes, Muller broke F-FCSR-8. In response, the designers withdrew F-FCSR-8: "These attacks pointed out three weaknesses on the algorithms. The first one is a bottleneck effect due to a big mistake in our design."
- F-FCSR-H: Brute force.
- F-FCSR-16: Brute force.

Non-attacks:

- 2008.02 Fischer, Meier, Stegemann discussed F-FCSR.
- 2008.02 Pousse, Minier discussed F-FCSR.

The eSTREAM committee's "Short Report on the End of the Second Phase" announced "F-FCSR-H (-16)" as a "hardware phase 3" cipher.

4.4 Grain

2005.04 [84] Hell, Johansson, Meier proposed Grain v0. They later proposed Grain v1. Hell, Johansson, Maximov, Meier proposed Grain-128. Attacks:

- Grain v0: 2005.10 [101] Khazaei, Hassanzadeh, Kiaei stated an attack on Grain v0. 2006.01 [24] Berbain, Gilbert, Maximov stated an attack on Grain v0. In response, the designers withdrew Grain v0: "We have now specified a tweaked version by changing the output function. ... The old version ... is not to be considered."
- Grain v1: 2008.02 De Cannière, Kucuk, Preneel stated an attack speeding up brute force "by a factor two." See 2006.07 [104] Kucuk for preliminary work.
- Grain-128 with initialization reduced to 180 out of 256 iterations: 2008.02 Fischer, Khazaei, Meier stated an attack 16 times faster than brute force.
- Grain-128 as specified: Brute force.

Non-attacks:

- 2008.02 De Cannière, Kucuk, Preneel stated various "related-key attacks" on Grain v1.

4.5 MICKEY

2005.04 [16] Babbage, Dodd proposed MICKEY v1. 2005.04 [17] Babbage, Dodd proposed MICKEY-128 v1. Babbage, Dodd later proposed MICKEY v2 and MICKEY-128 v2. Attacks:

- MICKEY v1: Brute force.
- MICKEY-128 v1: Brute force.
- MICKEY v2: Brute force.
- MICKEY-128 v2: Brute force.

Non-attacks:

- 2005.08 [86] Hong, Kim asked how much entropy is lost by the MICKEY state update. I see no reason to believe that this type of loss will produce an attack.
- Hong commented that MICKEY (like most ciphers) allows "BSW sampling." This doesn't change the price-performance ratio of an attack, but it means that the attacker can build a ridiculously insanely large attack machine rather than merely an insanely large attack machine.

The eSTREAM committee's "Short Report on the End of the Second Phase" announced both "MICKEY v2" and "MICKEY-128 v2" as "hardware phase 3" ciphers.

4.6 Mosquito and Moustique

2005.04 [51] Daemen, Kitsos proposed Mosquito. Daemen, Kitsos later proposed Moustique, also known as Mosquito v2. Attacks:

- Mosquito: 2006 Joux, Muller stated attacks on Mosquito. In response, the designers withdrew Mosquito.
- Moustique: 2008.02 Kaesper, Rijmen, Bjoerstad, Rechberer, Robshaw, and Sekar stated an attack on Moustique about 4 times faster than brute force. In the corresponding talk at SASC 2008 they announced that a refinement of the attack would be "about 50 times faster" than brute force.

The eSTREAM committee's "Short Report on the End of the Second Phase" announced "MOUSTIQUE" as a "hardware phase 3" cipher.

The original eSTREAM submission requirements said "A key length of 80 bits must be accommodated"; but I haven't found a specification of how 80-bit keys are used in Mosquito and Moustique. Of course, one could simply append 16 constant bits to an 80-bit key, but would the resulting cipher have 80-bit security, 74-bit security, or something in between? Perhaps the situation here is analogous to the SOSEMANUK situation, where the maximum key size K allowed by the designers does not provide K bits of security, but the key size required by eSTREAM is still safe.

4.7 Pomaranch

2005.04 [93] Jansen, Kolosha proposed Pomaranch (CJCSG) v1. 2005.10 [91] Jansen, Kholosha, 2005.10 [92] Jansen, Kholosha, 2006.01 [80] Helleseth, Jansen, Kholosha, 2006.02 [90] Jansen, Helleseth, Kholosha proposed Pomaranch v2. Jansen, Helleseth, Kholosha later proposed Pomaranch v3. Attacks:

- Pomaranch v1: 2005.09 [46] Cid, Gilbert, Johansson stated an attack. 2005.10 [99] Khazaei stated an attack. 2005.12 [74] Hasanzadeh, Khazaei, Kholosha stated an attack. Pomaranch v1 was withdrawn by the designers.
- Pomaranch v2: 2006 SAC Hell, Johansson stated an attack. Pomaranch v2 was withdrawn by the designers.
- Pomaranch v3 modified to output many more words of keystream: 2007.01 [54] Englund, Hell, Johansson stated an attack.
- Pomaranch v3: Brute force.

The eSTREAM committee's "Short Report on the End of the Second Phase" announced Pomaranch v3 as a "hardware phase 3" cipher.

4.8 Trivium

2005.04 [40] Cannière, Preneel proposed Trivium; see also 2006.01 [41] Cannière, Preneel. Attacks:

- Trivium reduced to Bivium: 2006.03 [133] Raddum stated an attack. 2007.04 [120] McDonald, Charnes, Pieprzyk stated another attack. 2008.02 Eibach, Pilz, Steck stated another attack.
- Trivium with a reduced initialization stage: 2007.01 [148] Turan, Kara stated an attack on 288 initialization steps. 2007.10 [149] Vielhaber stated an attack on 576 initialization steps. 2008.02 Fischer, Khazaei, Meier stated an attack on 672 initialization steps twice as fast as brute force.
- Trivium as specified: Brute force.

Non-attacks:

- 2005.09 [100] Khazaei, Hassanzadeh stated a guess-and-determine attack slower than brute force.
- 2007.01 [118] Maximov, Biryukov, 2007.01 [119] Maximov, Biryukov stated a streamlined guess-and-determine attack slower than brute force.
- 2007.01 [13] Babbage reviewed attack strategies.

The eSTREAM committee's "Short Report on the End of the Second Phase" announced Trivium as a "hardware phase 3" cipher.

5 Other eSTREAM submissions

The following table shows the cost of the best attacks known against non-"phase 3" ciphers in eSTREAM. "B-bit security" means that a known attack has comparable cost to 2^B key tests.

Security conjecture	Key size	Cipher
withdrawn	256 bits	DICING v0
withdrawn	256 bits	DICING v1
256-bit security	256 bits	DICING v2
256-bit security	256 bits	Fubuki
withdrawn	256 bits	MAG v0
unclear	256 bits	MAG v1/v2
broken	256 bits	MAG v3
256-bit security	256 bits	Phelix
withdrawn	256 bits	Py
withdrawn	256 bits	Py6
withdrawn	256 bits	Pypy
256-bit security	256 bits	TPy limited to 2^{64} bytes per key
256-bit security	256 bits	TPy6 limited to 2^{64} bytes per key
256-bit security	256 bits	TPypy
unclear	256 bits	YAMB
withdrawn	128 bits	ABC v1
withdrawn	128 bits	ABC v2
broken	128 bits	ABC v3
128-bit security	128 bits	Achterbahn-128 limited to 2^{44} bits per key
broken	128 bits	Frogbit
withdrawn	128 bits	Mir-1
withdrawn	128 bits	Polar Bear v1
128-bit security	128 bits	Polar Bear v2
100-bit security	128 bits	ProVEST-4
100-bit security	128 bits	ProVEST-16
100-bit security	128 bits	ProVEST-32
withdrawn	128 bits	SSS
withdrawn	128 bits	WG v1
128-bit security	128 bits	WG v2 limited to 2^{45} bits per key
withdrawn	128 bits	ZK-Crypt v1
128-bit security	128 bits	ZK-Crypt v2
128-bit security	128 bits	ZK-Crypt v3
withdrawn	80 bits	Achterbahn v1
withdrawn	80 bits	Achterbahn v2
80-bit security	80 bits	Achterbahn-80 limited to 2^{44} bits per key
80-bit security	80 bits	Hermes8
withdrawn	80 bits	Hermes8F
withdrawn	80 bits	SFINKS
withdrawn	80 bits	TSC-3

The rest of this section discusses each of these ciphers in detail.

5.1 ABC

2005.04 [5] Anashin, Bogdanov, Kizhvatov, Kumar proposed ABC v1. 2005.07 [2] Anashin, Bogdanov, Kizhvatov proposed ABC v2; see also 2005.11 [3] Anashin, Bogdanov, Kizhvatov and 2006.01 [4] Anashin, Bogdanov, Kizhvatov. The designers later proposed ABC v3. Attacks:

- 2005.07 [23] Berbain, Gilbert stated an attack on ABC v1. 2005.07 [98] Khazaei stated another attack on ABC v1. In response, the designers withdrew ABC v1: "We sent the ECRYPT stream cipher project committee an update. ... We would like the cryptographical community to regard the updated version of ABC as the basic one."
- 2006.02 [162] Wu, Preneel stated an attack on ABC v2. In response, the designers withdrew ABC v2: "We would like to thank the authors for the nice attack."
- 2006.08 [167] Zhang, Li, Wang stated an attack on ABC v3: "We show that, there are at least $2^{103.71}$ weak keys among 2^{128} random primary keys, and for each weak key, the expanded key can be recovered with about $2^{33.6}$ keystream words and $2^{50.56}$ operations." 2007 Wu, Preneel stated a speedup of the attack; the speedup has only about 2^{96} weak keys but detects a weak key from about 2^{20} bytes of output and recovers the key from about 2^{32} bytes of output. There has been no response from the designers but there has also been no dispute.

Non-attacks:

- 2005.09 [102] Khazaei, Kiaei claimed an attack on ABC v1 and ABC v2 but later withdrew the claim.

The eSTREAM committee's "Short Report on the End of the Second Phase" eliminated ABC from phase 3: "There are security problems. ... All three versions of ABC have been attacked and the design approach appears to be flawed."

5.2 Achterbahn

2005.04 [58] Gammel, Göttfert, Kniffler proposed Achterbahn v1. 2005.10 [59] Gammel, Göttfert, Kniffler, 2006.01 [60] Gammel, Göttfert, Kniffler proposed Achterbahn v2. The designers later proposed Achterbahn-80 and Achterbahn-128; see 2007.01 [61] Gammel, Gottfert, Kniffler. In their talk at SASC 2007, the designers proposed limiting Achterbahn-80 to 2^{52} bits of keystream, and limiting Achterbahn-128 to 2^{56} bits of keystream. 2007.05 [66] Göttfert, Gammel proposed limiting Achterbahn-80 and Achterbahn-128 to 2^{44} bits of keystream. Attacks:

- Achterbahn v1: 2005.09 [95] Johansson, Meier, Muller stated an attack on Achterbahn v1. In response, the designers withdrew Achterbahn v1.
- Achterbahn v2: 2006.05 [81] Hell, Johansson stated an attack on Achterbahn v2. In response, the designers withdrew Achterbahn v2.
- Achterbahn-80 as originally specified: 2006.11 [82] Hell, Johansson stated an attack. 2006.11 [132] [127] Naya-Plasencia stated an improved attack. In response, the designers imposed a keystream limit on Achterbahn-80.
- Achterbahn-80 limited to 2^{52} bits of keystream: 2007.02 [126] Naya-Plasencia stated an attack. In response, the designers imposed a smaller keystream limit on Achterbahn-80.
- Achterbahn-80 limited to 2^{44} bits of keystream: Brute force.
- Achterbahn-128 as originally specified: 2006.11 [82] Hell, Johansson stated an attack. 2006.11 [132] [127] Naya-Plasencia stated an improved attack. In response, the designers imposed a keystream limit on Achterbahn-128.
- Achterbahn-128 limited to 2^{56} keystream bits: 2007.02 [126] Naya-Plasencia stated an attack. In response, the designers imposed a smaller keystream limit on Achterbahn-128.
- Achterbahn-128 limited to 2^{44} keystream bits: Brute force.

The eSTREAM committee's "Short Report on the End of the Second Phase" eliminated Achterbahn from phase 3 as a result of the attacks listed above

I dispute the effectiveness of the stated attacks. The attack machines need a tremendous amount of storage and are slower than brute-force key-search machines of the same size. There is clearly some possibility of parallelizing the attacks, but it is not clear that the results would be better than brute force. This dispute might seem purely academic—the attacked forms of Achterbahn have been withdrawn—but incorrect evaluation of attack costs continues to be an embarrassment for the community.

5.3 DICING

2005.04 [107] Li proposed DICING v0 and, almost immediately, DICING v1; two different specifications (and software) were submitted to eSTREAM. 2006.01 [110] Li proposed DICING v2. Attacks:

- DICING v0: 2005.07 [131] Piret stated an attack. In response, the designer withdrew DICING v0: "The attacks is nice and the cryptanalysis is helpful."
- DICING v1: Brute force.
- DICING v2: Brute force.

The eSTREAM committee's "Short Report on the End of the Second Phase" eliminated DICING from phase 3 for performance reasons.

5.4 Frogbit

2005.04 [123] Moreau proposed Frogbit. Attacks:

- 2006.01 [138] [137] Saarinen stated an attack on Frogbit. 2006.01 [146] [147] Turan, Doganaksoy, Calik independently stated an attack on Frogbit. No response from the designer, but also no dispute.

Frogbit was eliminated by the eSTREAM committee at the end of phase 1 without comment.

5.5 Fubuki

2005.04 [112] Matsumoto, Mariko, Nishimura, Saito proposed Fubuki. Attacks:

- Brute force.

Fubuki was eliminated by the eSTREAM committee at the end of phase 1 without comment.

5.6 Hermes8

2005.04 [97] Kaiser proposed Hermes8. Kaiser later proposed Hermes8F. Attacks:

- 2006.08 [14] [15] Babbage, Cid, Pramstaller, Raddum broke Hermes8F. In response, the designer withdrew Hermes8F.

The eSTREAM committee's "Short Report on the End of the Second Phase" eliminated Hermes8 from phase 3 with the following statement: "There are two versions of Hermes8 currently under consideration: Hermes8 (as submitted originally to eSTREAM), and the faster Hermes8F. Hermes8F is subject to a devastating cryptanalytic attack [1]. This attack does not seem to extend directly to Hermes8; however, the paper does identify serious flaws in the design principles of the Hermes8 family as a whole."

5.7 MAG

2005.04 [152] Vuckovac proposed MAG v0 ("Provisional C++ version initially submitted to the ECRYPT"). The designer later proposed MAG v1 ("different from C++ version"). The designer later proposed MAG v2. The designer later proposed MAG v3. See 2005.10 [153] Vuckovac, 2006.01 [154] Vuckovac. Attacks:

- MAG v0: 2005.07 [105] Künzli, Meier broke MAG: "We present a very simple distinguishing attack ... requiring only 129 successive bytes of known keystream, computation and memory are negligible." Author's response was fairly incoherent but appeared to admit that the attack works: "DA shows how MAG secure stream can be differentiated from a random stream ... it appears that the next unknown byte can be predicted with 1/2 probability."
- MAG v1: Unresolved dispute. The standard presumption is that MAG v1, like MAG v0, is distinguishable at very low cost, but the designer disputes this.

- MAG v2: Unresolved dispute. The standard presumption is that MAG v2, like MAG v0, is distinguishable at very low cost, but the designer disputes this.
- MAG v3: Extremely fast; very briefly attracted attention. Distinguishable at very low cost; I posted distinguishing code to the eSTREAM forum in 2007.02.

MAG was eliminated by the eSTREAM committee at the end of phase 1 without comment.

5.8 Mir-1

2005.04 [117] Maximov proposed Mir-1. Attacks:

- 2006.01 [143] Tsunoo, Saito, Kubo, Shigeri stated an attack on Mir-1. No response from the designer but also no dispute.

Mir-1 was eliminated by the eSTREAM committee at the end of phase 1 without comment.

5.9 Phelix

2005.04 [156] Whiting, Schneier, Lucks, Muller proposed Phelix. Attacks:

- Brute force.

Non-attacks:

- 2006.10 [139] Salehani, Ahmadi claimed an attack but later withdrew the claim.
- 2006.11 [165] Wu, Preneel pointed out attacks against senders who are unable to count $1, 2, 3, \ldots$ and who do not follow the Phelix specification.

The eSTREAM committee's "Short Report on the End of the Second Phase" eliminated Phelix from phase 3 because of the Wu–Preneel attack. I was, and I remain, astonished at this action. Attacks against senders who are unable to count $1, 2, 3, \ldots$ should not eliminate an attractive option for senders who *are* able to count $1, 2, 3, \ldots$!

The committee statement acknowledged a debate regarding the Wu–Preneel attack but gave two arguments in favor of eliminating Phelix:

- The first argument was that the Wu–Preneel attack disproves a claim made by the Phelix designers. I agree that the Phelix designers made a silly claim; so what? The claim has nothing to do with security.
- The second argument was as follows: "We believe that the attack does constitute a genuine threat against real life systems using Phelix. It does seem plausible that an attacker would be able to mount an attack against such a system, reusing nonces, and that recovering the key would be a serious outcome. Attackers are not usually bound by usage rules." Here the

committee is confusing the *attacker* with the legitimate *sender*. The simple fact is that, when the legitimate sender and receiver use Phelix as specified, the Wu–Preneel attack doesn't work. If an attacker repeats a nonce, the attacker's packet is simply discarded.

Perhaps Phelix would not have been among the final eSTREAM selections, but perhaps it *would* have been. Having it eliminated for frivolous reasons didn't help eSTREAM's credibility.

The bottom line is that users considering Phelix can simply follow the Phelix specification and disregard the Wu–Preneel attack.

5.10 Polar Bear

2005.04 [76] Håstad, Näslund proposed Polar Bear v1. They later proposed Polar Bear v2. Attacks:

- John Mattsson stated an attack on Polar Bear v1. 2005.12 [75] Hasanzadeh, Shakour, Khazaei stated an improved attack on Polar Bear v1. The designers withdrew Polar Bear v1. 2006.01 [116] Mattsson discussed the attack in more detail.
- Polar Bear v2: Brute force.

The eSTREAM committee's "Short Report on the End of the Second Phase" eliminated Polar Bear from phase 3 for performance reasons.

5.11 ProVEST

2005.04 [128] O'Neil, Gittins, Landman proposed ProVEST-4, ProVEST-16, and ProVEST-32. Attacks:

- 2007.01 [96] Joux, Reinhard stated an attack on ProVEST. This attack is slower than brute-force search on a machine of the same size. However, my current impression is that a refined attack, parallelizing the Joux-Reinhard attack and reducing its memory requirements, recovers an F-bit key using time approximately $2^{F/2+4}$ on a machine of size $2^{F/4}$. In particular, a 128-bit ProVEST key can be found in time comparable to a 100-bit brute-force search.

The eSTREAM committee's "Short Report on the End of the Second Phase" eliminated VEST from phase 3 with the following statement: "A paper due to Joux and Reinhard [5] describes an attack against the submitted version of VEST. This practical attack allows the recovery of internal state and means that the cipher cannot be advanced to the next phase of eSTREAM." The committee erred in emphasizing "recovery of internal state"—every cipher leaks information about its internal state!—but everyone appears to agree that ProVEST does not meet the desired 128-bit security level.

5.12 Py and TPy

2005.04 [31] Biham, Seberry proposed Py and Py6. 2006.03 [32] Biham, Seberry proposed Pypy. 2007.01 [33] Biham, Seberry proposed TPy, TPypy, and TPy6. Attacks:

- Py modified to generate many more bytes of keystream: 2005.12 [130] Paul, Preneel, Sekar stated that the first 24 bytes of Py output for $2^{83.82}$ nonces are quickly distinguishable from uniform. 2006.01 [49] Crowley reduced $2^{83.82}$ nonces to 2^{73} nonces. The designers responded that Py must not be used for more than 2^{64} bytes per key.
- Py (and Py6 and PyPy) as specified: 2006.08 [163] Wu, Preneel, 2006.09 [164] Wu, Preneel stated (among other things) that, out of 2^{23} carefully selected nonces, about 2^7 produce the same Py output stream. They stated similar attacks on Py6 and PyPy. 2006.12 [88] [89] Isobe, Ohigashi, Kuwakado, Morii stated improved attacks, as did 2007.01 [166] Wu, Preneel. In response, the designers withdrew Py, Py6, and PyPy.
- TPy: Brute force.
- TPypy: Brute force.
- TPy6: Brute force.

Non-attacks:

- 2007.03 [129] Paul, Preneel stated an attack slower than brute force. See also 2007.03 [140] Sekar, Paul, Preneel; 2007.06 [141] Sekar, Paul, Preneel; 2007.11 [142] Sekar, Paul, Preneel.

The eSTREAM committee's "Short Report on the End of the Second Phase" eliminated Py etc. from phase 3: "Py and its variants demonstrate a promising approach that might offer exceptional performance. Unfortunately, however, there is sufficient analysis [4, 6, 9] to suggest that the submitted versions of the cipher demonstrate a weakness in the design."

5.13 SFINKS

2005.04 [38] Braeken, Lano, Mentens, Preneel, Verbauwhede proposed SFINKS. Attacks:

- 2006.01 [47] Courtois stated an attack on SFINKS. There does not appear to have been a response from the designers.

The eSTREAM committee's "Short Report on the End of the Second Phase" said that SFINKS had already been archived at the end of phase 1. However, the eSTREAM "End of Phase 1" document had actually announced that SFINKS would be a "hardware phase 2" cipher. There has been no explanation for the discrepancy.

I dispute the effectiveness of the stated attacks. SFINKS is analogous to Achterbahn in this respect. See Section 5.2 for further comments.

5.14 SSS

2005.04 [136] Rose, Hawkes, Paddon, de Vries proposed SSS. Attacks:

- 2005.06 [52] Daemen, Lano, Preneel broke SSS. The designers withdrew the cipher: "A neat attack, thanks. I confess that trying a self-synchronous stream cipher was a departure from anything that we really knew how to do . . . "

SSS was eliminated by the eSTREAM committee at the end of phase 1 without comment.

5.15 TRBDK3 YAEA

2005.04 [39] Brigham proposed TRBDK3 YAEA. The cipher was eliminated by the eSTREAM committee at the end of phase 1 without comment. I am not aware of any security evaluation of the cipher.

5.16 TSC

2005.04 [87] Hong, Lee, Yeom, Han, Chee proposed TSC-3. 2006.01 [122] Moon, Kwon, Han, Lee, Ryu, Lee, Yeom, Chee proposed TSC-4. Attacks:

- 2005.06 [124] Muller, Peyrin broke TSC-3. The designers withdrew TSC-3: "I have quickly read through the paper and believe the attacks to be valid."
- 2007 Zhang, Wang stated an attack that recognizes TSC-4 output using 2^{40} chosen IVs. The attack works for only 1 out of every 2^8 keys, but it's still better than brute force.

Non-attacks:

- 2006.12 [57] Fischer, Meier, Berbain, Biasse, Robshaw studied TSC-4.

The eSTREAM committee's "Short Report on the End of the Second Phase" eliminated TSC-4 from phase 3: "While no weaknesses have been reported in this version of the cipher, previous versions were broken in a range of attacks. Since there is little supporting security analysis of this cipher, the reliability of the underlying construction might be open to some question. With regards to performance, the available metrics do not suggest that TSC-4 would offer particularly compact hardware advantages over the AES or over other designs submitted to eSTREAM. Since this is the main focus of Profile II, we have decided not to advance the cipher."

5.17 WG

2005.04 [65] Gong, Nawaz proposed WG v1. 2005.07 [125] Nawaz, Gong proposed WG v2. Attacks:

- 2005.07 [159] Wu, Preneel broke WG version 1. Authors withdrew the cipher: "We admit that 22 clock cycles for key/IV setup phased as suggested by us in the original WG paper was too optimistic. ... We therefore recommend the key/IV setup phase of the WG cipher to be 88 clock cycles. No design changes are required."
- 2007.01 [134] Ronjom, Helleseth stated an attack on WG version 2 using $2^{45.2}$ keystream bits and $2^{45.2}$ simple operations after a precomputation of complexity 2^{62}. However, the WG specification limits the keystream to 2^{45} bits.

The eSTREAM committee's "Short Report on the End of the Second Phase" eliminated WG from phase 3 with the following statement: "No attacks have been reported against WG (P2). However, since the linear complexity of the keystream is around 2^{45}, the cipher is fully compromised after only a slight relaxation of the restriction that no more than 2^{45} bits be generated from a single key/IV pair. At the same time, the information we have to hand on hardware implementation suggests that WG (P2) will be larger than we would like."

5.18 YAMB

2005.04 [50] Lebedev et al. proposed YAMB. Attacks:

- 2005.06 [158] Wu, Preneel stated an attack on YAMB. Several months later, 2006.03 [106] Lebedev, Starodubtzev, Volchkov disputed the attack. This dispute has not been resolved.

The eSTREAM committee's "Short Report on the End of the Second Phase" said that YAMB had already been archived at the end of phase 1. However, the eSTREAM "End of Phase 1" document had actually announced that YAMB would be a "software phase 2" and "hardware phase 2" cipher. There has been no explanation for the discrepancy.

5.19 ZK-Crypt

2005.04 [71] Gressel, Granot, Vago proposed ZK-Crypt v1. 2006.02 [69] Gressel, Dunkelman, Granot, Vago proposed ZK-Crypt v2 and later ZK-Crypt v3. See 2008.02 [70] Gressel, Dunkelman, Hecht; 2008.02 [79] Hecht, Gressel, Granot; 2008.02 [78] Hecht, Bard, Gressel; 2008.02 [67] Gressel, Bard, Dunkelman, Hecht, Granot; 2008.02 [18] Bard, Gressel, Hecht; 2008.02 [72] Gressel, Hecht, Granot; 2008.02 [68] Gressel, Bard, Dunkelman, Hecht, Granot; 2008.02 [73] Gressel, Hecht, Rivkin, Granot. Attacks:

- ZK-Crypt v1: 2005.10 [111] Lubkin, Ryabko appeared to state that ZK-Crypt output is compressible by a standard move-to-front-plus-Huffman algorithm. The designers questioned the Lubkin–Ryabko result. 2006.03 [30] Bernstein confirmed and simplified the result. In the meantime, 2006.01 [138] [137] Saarinen stated that ZK-Crypt output flunks a simple IV-diffusion test;

2006.01 [146] [146] Turan, Doganaksoy, Calik independently stated that ZK-Crypt output flunks another IV test. In response, the designers withdrew ZK-Crypt v1.

- ZK-Crypt v2: Brute force.
- ZK-Crypt v3: Brute force.

The eSTREAM committee's "Short Report on the End of the Second Phase" eliminated ZK-Crypt from phase 3 with the following statement: "Zk-Crypt has poor documentation. This is a great obstacle to anyone trying to attempt cryptanalysis. In particular, within a limited timeframe, anyone looking over the set of eSTREAM submissions with a view to attempting cryptanalysis on one of them, will almost certainly pick an algorithm that can be understood more readily. We suspect that there has been little independent security analysis of Zk-Crypt and, with the documentation to hand, we would expect this to continue in the third phase. We feel that Zk-Crypt cannot be advanced to the next phase."

References

1. Hadi Ahmadi, Taraneh Eghlidos, Shahram Khazaei, *Improved Guess and Determine Attack on SOSEMANUK*, eSTREAM report 2005/085 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.8.
2. Vladimir Anashin, Andrey Bogdanov, Ilya Kizhvatov, *Increasing the ABC Stream Cipher Period*, eSTREAM report 2005/050 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.1.
3. Vladimir Anashin, Andrey Bogdanov, Ilya Kizhvatov, *ABC Is Safe And Sound*, eSTREAM report 2005/079 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.1.
4. Vladimir Anashin, Andrey Bogdanov, Ilya Kizhvatov, *Security and Implementation Properties of ABC v.2*, eSTREAM report 2006/026 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.1.
5. Vladimir Anashin, Andrey Bogdanov, Ilya Kizhvatov, Sandeep Kumar, *ABC : A New Fast Flexible Stream Cipher*, eSTREAM report 2005/001 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.1.
6. François Arnault, Thierry Berger, Cédric Lauradoux, *Preventing weaknesses on F-FCSR in IV mode and tradeoff attack on F-FCSR 8*, eSTREAM report 2005/075 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.3.
7. François Arnault, Thierry Berger, Cédric Lauradoux, *Update on F-FCSR Stream Cipher*, eSTREAM report 2006/025 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.3.
8. Francois Arnault, Thierry P. Berger, Marine Minier, *On the security of FCSR-based pseudorandom generators*, in Workshop Record of SASC 2007: The State of the Art of Stream Ciphers, eSTREAM report 2007/022 (2007). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.3.
9. Jean-Philippe Aumasson, *On a bias of Rabbit*, eSTREAM report 2006/058 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.6.
10. Jean-Philippe Aumasson, *On a bias of Rabbit*, in Workshop Record of SASC 2007: The State of the Art of Stream Ciphers, eSTREAM report 2007/033 (2007). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.6.
11. Jean-Philippe Aumasson, Simon Fischer, Shahram Khazaei, Willi Meier, Christian Rechberger, *New features of Latin dances: analysis of Salsa, ChaCha, and Rumba* (2007). URL: `http://eprint.iacr.org/2007/472`. Citations in this document: §3.7, §3.7.
12. Jean-Philippe Aumasson, Simon Fischer, Shahram Khazaei, Willi Meier, Christian Rechberger, *New features of Latin dances: analysis of Salsa, ChaCha, and Rumba*, FSE 2008 (2007). Citations in this document: §3.7, §3.7.
13. Steve Babbage, *Some thoughts on Trivium*, in Workshop Record of SASC 2007: The State of the Art of Stream Ciphers, eSTREAM report 2007/007 (2007). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.8.
14. Steve Babbage, Carlos Cid, Norbert Pramstaller, Havard Raddum, *Cryptanalysis of Hermes8F*, eSTREAM report 2006/048 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.6.

15. Steve Babbage, Carlos Cid, Norbert Pramstaller, Havard Raddum, *Cryptanalysis of Hermes8F*, in Workshop Record of SASC 2007: The State of the Art of Stream Ciphers, eSTREAM report 2007/009 (2007). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.6.
16. Steve Babbage, Matthew Dodd, *The stream cipher MICKEY (version 1)*, eSTREAM report 2005/015 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.5.
17. Steve Babbage, Matthew Dodd, *The stream cipher MICKEY-128 (version 1)*, eSTREAM report 2005/016 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.5.
18. Gregory Bard, Carmi Gressel, Avi Hecht, *Security Analysis of the ZK-Crypt III Stream Cipher and Data Authenticator Against Algebraic Cryptanalytic, Differential & Correlation Attacks*, eSTREAM report 2008/006 (2008). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.19.
19. Rana Barua, Tanja Lange (editors), *Progress in Cryptology—INDOCRYPT 2006, 7th International Conference on Cryptology in India, Kolkata, India, December 11–13, 2006, Proceedings*, Lecture Notes in Computer Science, 4329, Springer, 2006. ISBN 3–540–49767–6. See [57].
20. Come Berbain, Olivier Billet, Anne Canteaut, Nicolas Courtois, Blandine Debraize, Henri Gilbert, Louis Goubin, Aline Gouget, Louis Granboulan, Cédric Lauradoux, Marine Minier, Thomas Pornin, Hervé Sibert, *Decim - A New Stream Cipher for Hardware Applications*, eSTREAM report 2005/004 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.1.
21. Come Berbain, Olivier Billet, Anne Canteaut, Nicolas Courtois, Blandine Debraize, Henri Gilbert, Louis Goubin, Aline Gouget, Louis Granboulan, Cédric Lauradoux, Marine Minier, Thomas Pornin, Hervé Sibert, *DECIM v2*, eSTREAM report 2006/004 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.1.
22. Come Berbain, Olivier Billet, Anne Canteaut, Nicolas Courtois, Henri Gilbert, Louis Goubin, Aline Gouget, Louis Granboulan, Cédric Lauradoux, Marine Minier, Thomas Pornin, Hervé Sibert, *Sosemanuk, a fast software-oriented stream cipher*, eSTREAM report 2005/027 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.8.
23. Côme Berbain, Henri Gilbert, *Cryptanalysis of ABC*, eSTREAM report 2005/048 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.1.
24. Côme Berbain, Henri Gilbert, Alexander Maximov, *Cryptanalysis of Grain*, eSTREAM report 2006/019 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.4.
25. Thierry Berger, François Arnault, Cédric Lauradoux, *F-FCSR*, eSTREAM report 2005/008 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.3.
26. Daniel J. Bernstein, *Salsa20*, eSTREAM report 2005/025 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.7.
27. Daniel J. Bernstein, *Understanding brute force*, eSTREAM report 2005/036 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §2.5.

28. Daniel J. Bernstein, *Disproof of Li An-Ping's claims regarding Salsa20*, eSTREAM report 2005/058 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.7.
29. Daniel J. Bernstein, *Salsa20/8 and Salsa20/12*, eSTREAM report 2006/007 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.7.
30. Daniel J. Bernstein, *Does ZK-Crypt version 1 flunk a repetition test?*, eSTREAM report 2006/033 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.19.
31. Eli Biham, Jennifer Seberry, *Py (Roo) : A Fast and Secure Stream Cipher Using Rolling Arrays*, eSTREAM report 2005/023 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.12.
32. Eli Biham, Jennifer Seberry, *Pypy: Another Version of Py*, eSTREAM report 2006/038 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.12.
33. Eli Biham, Jennifer Seberry, *Tweaking the IV Setup of the Py Family of Stream Ciphers – The Ciphers TPy, TPypy, and TPy6*, eSTREAM report 2007/038 (2007). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.12.
34. Alex Biryukov, *A new 128 bit key stream cipher : LEX*, eSTREAM report 2005/013 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.4.
35. Alex Biryukov, *The Tweak for LEX-128, LEX-192, LEX-256*, eSTREAM report 2006/037 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.4.
36. Tor E. Bjørstad, *A note on the Edon80 S-box*, eSTREAM report 2007/043 (2007). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.2.
37. Martin Boesgaard, Mette Vesterager, Thomas Christensen, Erik Zenner, *The Stream Cipher Rabbit*, eSTREAM report 2005/024 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.6.
38. An Braeken, Joseph Lano, Nele Mentens, Bart Preneel, Ingrid Verbauwhede, *SFINKS : A Synchronous Stream Cipher for Restricted Hardware Environments*, eSTREAM report 2005/026 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.13.
39. Timothy Brigham, *TRBDK3 YAEA - High Security, Synchronous Stream Cypher Implementable in Hardware and Software*, eSTREAM report 2005/029 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.15.
40. Christophe De Cannière, Bart Preneel, *Trivium - A Stream Cipher Construction Inspired by Block Cipher Design Principles*, eSTREAM report 2005/030 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.8.
41. Christophe De Cannière, Bart Preneel, *Trivium - A Stream Cipher Construction Inspired by Block Cipher Design Principle*, eSTREAM report 2006/021 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.8.
42. Kevin Chen, Matt Henricksen, William Millan, Joanne Fuller, Leonie Simpson, Ed Dawson, Hoonjae Lee, Sangjae Moon, *Dragon: A Fast Word Based Stream Cipher*, eSTREAM report 2005/006 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.2.

43. Joo Yeon Cho, Josef Pieprzyk, *Linear Distinguishing Attack on NLS*, eSTREAM report 2006/018 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.5.
44. Joo Yeon Cho, Josef Pieprzyk, *Crossword Puzzle Attack on NLSv2*, eSTREAM report 2006/051 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.5.
45. Joo Yeon Cho, Josef Pieprzyk, *An Improved Distinguisher for Dragon*, eSTREAM report 2007/002 (2007). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.2.
46. Carlos Cid, Henri Gilbert, Thomas Johansson, *Cryptanalysis of Pomaranch*, eSTREAM report 2005/060 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.7.
47. Nicolas Courtois, *Cryptanalysis of Sfinks*, eSTREAM report 2006/002 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.13.
48. Paul Crowley, *Truncated differential cryptanalysis of five rounds of Salsa20*, eSTREAM report 2005/073 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.7.
49. Paul Crowley, *Improved cryptanalysis of Py*, eSTREAM report 2006/010 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.12.
50. LAN Crypto, *LAN Crypto Submission to the ECRYPT Stream Cipher Project.*, eSTREAM report 2005/034 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.18.
51. Joan Daemen, Paris Kitsos, *Submission to ECRYPT call for stream ciphers: the self-synchronizing stream cipher Mosquito*, eSTREAM report 2005/018 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.6.
52. Joan Daemen, Joseph Lano, Bart Preneel, *Chosen Ciphertext Attack on SSS*, eSTREAM report 2005/044 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.14.
53. Ed Dawson, Matt Henricksen, Willam Millan, Leonie Simpson, *The Dragon Is Alive and Well*, eSTREAM report 2005/069 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.2.
54. Hakan Englund, Martin Hell, Thomas Johansson, *Two General Attacks on Pomaranch-like Keystream Generators*, eSTREAM report 2007/001 (2007). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.7.
55. Hakan Englund, Martin Hell, Thomas Johansson, *A Note on Distinguishing Attacks*, in Workshop Record of SASC 2007: The State of the Art of Stream Ciphers, eSTREAM report 2007/013 (2007). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.4.
56. Hakan Englund, Alexander Maximov, *Attack the Dragon*, eSTREAM report 2005/062 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.2.
57. Simon Fischer, Willi Meier, Côme Berbain, Jean-François Biasse, Matthew J. B. Robshaw, *Non-randomness in eSTREAM candidates Salsa20 and TSC-4*, in [19] (2006), 2–16. Citations in this document: §3.7, §3.7, §5.16.
58. Berndt Gammel, Rainer Göttfert, Oliver Kniffler, *The Achterbahn Stream Cipher*, eSTREAM report 2005/002 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.2.

59. Berndt Gammel, Rainer Gottfert, Oliver Kniffler, *Improved Boolean Combining Functions for Achterbahn*, eSTREAM report 2005/072 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.2.
60. Berndt M. Gammel, Rainer Göttfert, Oliver Kniffler, *Status of Achterbahn and Tweaks*, eSTREAM report 2006/027 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.2.
61. Berndt Gammel, Rainer Gottfert, Oliver Kniffler, *Achterbahn- 128/80: Design and Analysis*, in Workshop Record of SASC 2007: The State of the Art of Stream Ciphers, eSTREAM report 2007/020 (2007). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.2.
62. Danilo Gligoroski, Smile Markovski, Svein Johan Knapskog, *On periods of Edon-*$(2m; 2k)$ *Family of Stream Ciphers*, eSTREAM report 2006/022 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.2.
63. Danilo Gligoroski, Smile Markovski, Ljupco Kocarev, Marjan Gusev, *Edon80*, eSTREAM report 2005/007 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.2.
64. Danilo Gligoroski, Smile Markovski, Ljupco Kocarev, Marjan Gusev, *Understanding Periods in Edon80*, eSTREAM report 2005/054 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.2.
65. Guang Gong, Yassir Nawaz, *The WG Stream Cipher*, eSTREAM report 2005/033 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.17.
66. Rainer Göttfert, Berndt M. Gammel, *On the frame length of Achterbahn-128/80*, eSTREAM report 2007/041 (2007). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.2.
67. Carmi Gressel, Gregory Bard, Orr Dunkelman, Avi Hecht, Ran Granot, *ZK-Crypt Dual Track FB Circuit & Concept Drawings*, eSTREAM report 2008/005 (2008). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.19.
68. Carmi Gressel, Gregory Bard, Orr Dunkelman, Avi Hecht, Ran Granot, *The A to Z GUIDE to the ZK-Crypt*, eSTREAM report 2008/008 (2008). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.19.
69. Carmi Gressel, Orr Dunkelman, Ran Granot, Gabi Vago, *Enhanced ZK-Crypt*, eSTREAM report 2006/031 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.19.
70. Carmi Gressel, Orr Dunkelman, Avi Hecht, *Understanding the ZK-Crypts – Ciphers for (almost) all Reasons*, eSTREAM report 2008/002 (2008). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.19.
71. Carmi Gressel, Ran Granot, Gabi Vago, *ZK-Crypt*, eSTREAM report 2005/035 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.19.
72. Carmi Gressel, Avi Hecht, Ran Granot, *What the Host Sees in the ZK-Crypt*, eSTREAM report 2008/007 (2008). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.19.
73. Carmi Gressel, Avi Hecht, Michael Rivkin, Ran Granot, *The ZK-Crypt Noise Generator Design Parameter Emulator*, eSTREAM report 2008/009 (2008). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.19.

74. Mahdi Hasanzadeh, Shahram Khazaei, Alexander Kholosha, *On IV Setup of Pomaranch*, eSTREAM report 2005/082 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.7.
75. Mahdi Hasanzadeh, Elham Shakour, Shahram Khazaei, *Improved Cryptanalysis of Polar Bear*, eSTREAM report 2005/084 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.10.
76. Johan Håstad, Mats Näslund, *The Stream Cipher Polar Bear*, eSTREAM report 2005/021 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.10.
77. Philip Hawkes, Michael Paddon, Gregory G. Rose, Miriam Wiggers de Vries, *Primitive Specification for NLSv2*, eSTREAM report 2006/036 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.5.
78. Avi Hecht, Gregory Bard, Carmi Gressel, *An Expanded ZK-Crypt III Security Analysis*, eSTREAM report 2008/004 (2008). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.19.
79. Avi Hecht, Carmi Gressel, Ran Granot, *The ZK-Crypt III Algorithmic Specification*, eSTREAM report 2008/003 (2008). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.19.
80. Tor Helleseth, Cees J.A. Jansen, Alexander Kholosha, *Pomaranch - Design and Analysis of a Family of Stream Ciphers*, eSTREAM report 2006/008 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.7.
81. Martin Hell, Thomas Johansson, *Cryptanalysis of Achterbahn-Version 2*, eSTREAM report 2006/042 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.2.
82. Martin Hell, Thomas Johansson, *Cryptanalysis of Achterbahn-128/80*, eSTREAM report 2006/054 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.2, §5.2.
83. Martin Hell, Thomas Johansson, *A Key Recovery Attack on Edon80*, eSTREAM report 2007/044 (2007). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.2.
84. Martin Hell, Thomas Johansson, Willi Meier, *Grain - A Stream Cipher for Constrained Environments*, eSTREAM report 2005/010 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.4.
85. Jin Hong, *Remarks on the Period of Edon80*, eSTREAM report 2005/041 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.2.
86. Jin Hong, Woo-Hwan Kim, *TMD-Tradeoff and State Entropy Loss Considerations of Streamcipher MICKEY*, eSTREAM report 2005/055 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.5.
87. Jin Hong, Dong Hoon Lee, Yongjin Yeom, Daewan Han, Seongtaek Chee, *T-function Based Stream Cipher TSC-3*, eSTREAM report 2005/031 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.16.
88. Takanori Isobe, Toshihiro Ohigashi, Hidenori Kuwakado, Masakatu Morii, *How to Break Py and Pypy by a Chosen-IV Attack*, eSTREAM report 2006/060 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.12.

89. Takanori Isobe, Toshihiro Ohigashi, Hidenori Kuwakado, Masakatu Morii, *How to Break Py and Pypy by a Chosen-IV Attack*, in Workshop Record of SASC 2007: The State of the Art of Stream Ciphers, eSTREAM report 2007/035 (2007). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.12.
90. Cees J.A. Jansen, Tor Helleseth, Alexander Kholosha, *Cascade Jump Controlled Sequence Generator and Pomaranch Stream Cipher (Version 2)*, eSTREAM report 2006/006 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.7.
91. Cees Jansen, Alexander Kholosha, *Countering the Correlation Attack on Pomaranch*, eSTREAM report 2005/070 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.7.
92. Cees Jansen, Alexander Kholosha, *Pomaranch is Sound and Healthy*, eSTREAM report 2005/074 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.7.
93. Cees Jansen, Alexander Kolosha, *Cascade Jump Controlled Sequence Generator (CJCSG)*, eSTREAM report 2005/022 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.7.
94. Eliane Jaulmes, Frédéric Muller, *Cryptanalysis of ECRYPT Candidates F-FCSR-8 and F-FCSR-H*, eSTREAM report 2005/046 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.3.
95. Thomas Johansson, Willi Meier, Frédéric Muller, *Cryptanalysis of Achterbahn*, eSTREAM report 2005/064 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.2.
96. Antoine Joux, Jean-Rene Reinhard, *Overtaking VEST*, in Workshop Record of SASC 2007: The State of the Art of Stream Ciphers, eSTREAM report 2007/021 (2007). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.11.
97. Ulrich Kaiser, *Hermes-8*, eSTREAM report 2005/012 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.6.
98. Shahram Khazaei, *Divide and Conquer Attack on ABC Stream Cipher*, eSTREAM report 2005/052 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.1.
99. Shahram Khazaei, *Cryptanalysis of Pomaranch (CJCSG)*, eSTREAM report 2005/065 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.7.
100. Shahram Khazaei, Mehdi Hassanzadeh, *Linear Sequential Circuit Approximation of the TRIVIUM Stream Cipher*, eSTREAM report 2005/063 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.8.
101. Shahram Khazaei, Mehdi Hassanzadeh, Mohammad Kiaei, *Distinguishing Attack on Grain*, eSTREAM report 2005/071 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.4.
102. Shahram Khazaei, Mohammad Kiaei, *Distinguishing Attack on the ABC v.1 and v.2*, eSTREAM report 2005/061 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.1.
103. Shahram Khazaei, Elham Shakour, *Distinguishing Attack on CryptMT*, eSTREAM report 2005/080 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.1.

104. Ozgul Kucuk, *Slide Resynchronization Attack on the Initialization of Grain 1.0*, eSTREAM report 2006/044 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.4.
105. Simon Künzli, Willi Meier, *Distinguishing Attack on MAG*, eSTREAM report 2005/053 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.7.
106. Anatoly Lebedev, Sergey Starodubtzev, Alexey Volchkov, *Real Distinguishing of Yamb Output and a True Random Sequence*, eSTREAM report 2006/035 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.18.
107. An-Ping Li, *A New Stream Cipher: Dicing*, eSTREAM report 2005/005 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.3.
108. An-Ping Li, *Linear approximating for the Cipher Salsa20*, eSTREAM report 2005/056 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.7.
109. An-Ping Li, *Linear approximating for the Cipher Salsa20 (II)*, eSTREAM report 2005/067 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.7.
110. An-Ping Li, *A New Version of the Cipher DICING*, eSTREAM report 2006/003 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.3.
111. Alexey Lubkin, Boris Ryabko, *The distinguishing attack on ZK-Crypt cipher*, eSTREAM report 2005/076 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.19.
112. Makoto Matsumoto, Mariko Hagita, Takuji Nishimura, Mutsuo Saito, *Mersenne Twister and Fubuki Stream/Block Cipher*, eSTREAM report 2005/003 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.1, §5.5.
113. Makoto Matsumoto, Mutsuo Saito, Takuji Nishimura, Mariko Hagita, *Cryptanalysis of CryptMT: Effect of Huge Prime Period and Multiplicative Filter*, eSTREAM report 2005/083 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.1.
114. Makoto Matsumoto, Mutsuo Saito, Takuji Nishimura, Mariko Hagita, *CryptMT version 2.0 : A Large State Generator with Faster Initialization*, eSTREAM report 2006/023 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.1.
115. Makoto Matsumoto, Mutsuo Saito, Takuji Nishimura, Mariko Hagita, *CryptMT Stream Cipher Version 3*, in Workshop Record of SASC 2007: The State of the Art of Stream Ciphers, eSTREAM report 2007/028 (2007). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.1.
116. John Mattsson, *A Guess-and-Determine Attack on the Stream Cipher Polar Bear*, eSTREAM report 2006/017 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.10.
117. Alexander Maximov, *A New Stream Cipher Mir-1*, eSTREAM report 2005/017 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.8.
118. Alexander Maximov, Alex Biryukov, *Two Trivial Attacks on Trivium*, eSTREAM report 2007/003 (2007). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.8.

119. Alexander Maximov, Alex Biryukov, *Two Trivial Attacks on Trivium*, in Workshop Record of SASC 2007: The State of the Art of Stream Ciphers, eSTREAM report 2007/006 (2007). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.8.
120. Cameron McDonald, Chris Charnes, Josef Pieprzyk, *Attacking Bivium with MiniSat*, eSTREAM report 2007/040 (2007). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.8.
121. Cameron McDonald, Philip Hawkes, *On Exploiting Adjacent Bits in NLS*, eSTREAM report 2006/047 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.5.
122. Dukjae Moon, Daesung Kwon, Daewan Han, Jooyoung Lee, Gwon Ho Ryu, Dong Wook Lee, Yongjin Yeom, Seongtaek Chee, *T-function based streamcipher TSC-4*, eSTREAM report 2006/024 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.16.
123. Thierry Moreau, *The Frogbit Cipher, a Data Integrity Algorithm*, eSTREAM report 2005/009 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.4.
124. Frédéric Muller, Thomas Peyrin, *Linear Cryptanalysis of TSC Stream Ciphers - Applications to the ECRYPT proposal TSC-3*, eSTREAM report 2005/042 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.16.
125. Yassir Nawaz, Guang Gong, *Preventing Chosen IV Attack on WG Cipher by Increasing the Length of Key/IV Setup*, eSTREAM report 2005/047 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.17.
126. Maria Naya-Plasencia, *Cryptanalysis of Achterbahn-128/80 with a new keystream limitation*, eSTREAM report 2007/004 (2007). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.2, §5.2.
127. Maria Naya-Plasencia, *Cryptanalysis of Achterbahn-128/80*, in Workshop Record of SASC 2007: The State of the Art of Stream Ciphers, eSTREAM report 2007/019 (2007). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.2, §5.2.
128. Sean O'Neil, Benjamin Gittins, Howard Landman, *VEST - Hardware-Dedicated Stream Ciphers*, eSTREAM report 2005/032 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.11.
129. Souradyuti Paul, Bart Preneel, *On the (In)security of Stream Ciphers Based on Arrays and Modular Addition*, eSTREAM report 2007/036 (2007). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.12.
130. Souradyuti Paul, Bart Preneel, Gautham Sekar, *Distinguishing Attacks on the Stream Cipher Py*, eSTREAM report 2005/081 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.12.
131. Gilles Piret, *Practical Attacks on one Version of DICING*, eSTREAM report 2005/051 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.3.
132. Maria Naya Plasencia, *Cryptanalysis of Achterbahn-128/80*, eSTREAM report 2006/055 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.2, §5.2.
133. Havard Raddum, *Cryptanalytic Results on Trivium*, eSTREAM report 2006/039 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.8.

134. Sondre Ronjom, Tor Helleseth, *Attacking the Filter Generator over $GF(2^m)$*, in Workshop Record of SASC 2007: The State of the Art of Stream Ciphers, eSTREAM report 2007/011 (2007). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.17.
135. Gregory Rose, Philip Hawkes, Michael Paddon, Miriam Wiggers de Vries, *Primitive Specification for NLS*, eSTREAM report 2005/019 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.5.
136. Gregory Rose, Philip Hawkes, Michael Paddon, Miriam Wiggers de Vries, *Primitive Specification for SSS*, eSTREAM report 2005/028 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.14.
137. Markku-Juhani O. Saarinen, *Chosen-IV Statistical Attacks on eSTREAM Stream Ciphers*, eSTREAM report 2006/005 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.4, §5.19.
138. Markku-Juhani O. Saarinen, *Chosen-IV Statistical Attacks on eSTREAM Stream Ciphers*, eSTREAM report 2006/013 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.4, §5.19.
139. Yaser Esmaeili Salehani, Hadi Ahmadi, *A Chosen-key Distinguishing Attack on Phelix*, eSTREAM report 2006/053 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.9.
140. Gautham Sekar, Souradyuti Paul, Bart Preneel, *Weaknesses in the Pseudorandom Bit Generation Algorithms of the Stream Ciphers TPypy and TPy*, eSTREAM report 2007/037 (2007). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.12.
141. Gautham Sekar, Souradyuti Paul, Bart Preneel, *New Weaknesses in the Keystream Generation Algorithms of the Stream Ciphers TPy and Py* (2007). URL: `http://eprint.iacr.org/2007/230`. Citations in this document: §5.12.
142. Gautham Sekar, Souradyuti Paul, Bart Preneel, *New attacks on the stream cipher TPy6 and design of new ciphers the TPy6-A and the TPy6-B* (2007). URL: `http://eprint.iacr.org/2007/436`. Citations in this document: §5.12.
143. Yukiyasu Tsunoo, Teruo Saito, Hiroyasu Kubo, Maki Shigeri, *Cryptanalysis of Mir-1, a T-function Based Stream Cipher*, eSTREAM report 2006/020 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.8.
144. Yukiyasu Tsunoo, Teruo Saito, Hiroyasu Kubo, Tomoyasu Suzaki, Hiroki Nakashima, *Differential Cryptanalysis of Salsa20/8*, in Workshop Record of SASC 2007: The State of the Art of Stream Ciphers, eSTREAM report 2007/010 (2007). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.7, §3.7.
145. Yukiyasu Tsunoo, Teruo Saito, Maki Shigeri, Tomoyasu Suzaki, Hadi Ahmadi, Taraneh Eghlidos, Shahram Khazaei, *Evaluation of SOSEMANUK With Regard to Guess-and-Determine Attacks*, eSTREAM report 2006/009 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.8.
146. Meltem Sonmez Turan, Ali Doganaksoy, Cagdas Calik, *Statistical Analysis of Synchronous Stream Ciphers*, eSTREAM report 2006/012 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.4, §5.19, §5.19.

147. Meltem Sonmez Turan, Ali Doganaksoy, Cagdas Calik, *Detailed Statistical Analysis of Synchronous Stream Ciphers*, eSTREAM report 2006/043 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.4.
148. Meltem Sonmez Turan, Orhun Kara, *Linear Approximations for 2- round Trivium*, in Workshop Record of SASC 2007: The State of the Art of Stream Ciphers, eSTREAM report 2007/008 (2007). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.8.
149. Michael Vielhaber, *Breaking ONE.FIVIUM by AIDA an Algebraic IV Differential Attack* (2007). URL: `http://eprint.iacr.org/2007/413`. Citations in this document: §4.8.
150. Milan Vojvoda, Marek Sys, Matus Jokay, *A Note on Algebraic Properties of Quasigroups in Edon80*, eSTREAM report 2007/005 (2007). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.2.
151. Milan Vojvoda, Marek Sys, Matus Jokay, *A Note on Algebraic Properties of Quasigroups in Edon80*, in Workshop Record of SASC 2007: The State of the Art of Stream Ciphers, eSTREAM report 2007/032 (2007). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.2.
152. Rade Vuckovac, *MAG My Array Generator (a new strategy for random number generation)*, eSTREAM report 2005/014 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.7.
153. Rade Vuckovac, *MAG alternating methods notes*, eSTREAM report 2005/068 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.7.
154. Rade Vuckovac, *MAG Cipher Design Notes*, eSTREAM report 2006/001 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.7.
155. Xiaoyun Wang, Meiqin Wang, Shaohui Wang, *Efficient Attack on the Stream Cipher LEX*, eSTREAM report 2006/045 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.4.
156. Doug Whiting, Bruce Schneier, Stephan Lucks, Frédéric Muller, *Phelix - Fast Encryption and Authentication in a Single Cryptographic Primitive*, eSTREAM report 2005/020 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.9.
157. Hongjun Wu, *Stream Cipher HC-256*, eSTREAM report 2005/011 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.3.
158. Hongjun Wu, Bart Preneel, *Distinguishing Attack on Stream Cipher Yamb*, eSTREAM report 2005/043 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.18.
159. Hongjun Wu, Bart Preneel, *Chosen IV Attack on Stream Cipher WG*, eSTREAM report 2005/045 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.17.
160. Hongjun Wu, Bart Preneel, *Cryptanalysis of Stream Cipher DECIM*, eSTREAM report 2005/049 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §4.1.
161. Hongjun Wu, Bart Preneel, *Attacking the IV Setup of Stream Cipher LEX*, eSTREAM report 2005/059 (2005). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §3.4.

162. Hongjun Wu, Bart Preneel, *Cryptanalysis of ABC v2*, eSTREAM report 2006/029 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.1.
163. Hongjun Wu, Bart Preneel, *Attacking the IV Setup of Py and Pypy*, eSTREAM report 2006/050 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.12.
164. Hongjun Wu, Bart Preneel, *Key Recovery Attack on Py and Pypy with Chosen IVs*, eSTREAM report 2006/052 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.12.
165. Hongjun Wu, Bart Preneel, *Differential-Linear Attacks against the Stream Cipher Phelix*, eSTREAM report 2006/056 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.9.
166. Hongjun Wu, Bart Preneel, *Differential Cryptanalysis of the Stream Ciphers Py, Py6 and Pypy*, in Workshop Record of SASC 2007: The State of the Art of Stream Ciphers, eSTREAM report 2007/034 (2007). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.12.
167. Haina Zhang, Lin Li, Xiaoyun Wang, *Fast Correlation Attack on Stream Cipher ABC v3*, eSTREAM report 2006/049 (2006). URL: `http://www.ecrypt.eu.org/stream/papers.html`. Citations in this document: §5.1.