Key-Alternating Ciphers in a Provable Setting: Encryption Using a Small Number of Public Permutations

(Extended Abstract*)

Andrey Bogdanov[1], Lars R. Knudsen[2], Gregor Leander[2],
Francois-Xavier Standaert[3], John Steinberger[4], and Elmar Tischhauser[1]

[1] KU Leuven and IBBT
{Andrey.Bogdanov,Elmar.Tischhauser}@esat.kuleuven.be
[2] Technical University of Denmark
{G.Leander,Knudsen}@mat.dtu.dk
[3] Université catholique de Louvain, UCL Crypto Group
fstandae@uclouvain.be
[4] Tsinghua University
jpsteinb@gmail.com

Abstract. This paper considers—for the first time—the concept of key-alternating ciphers in a provable security setting. Key-alternating ciphers can be seen as a generalization of a construction proposed by Even and Mansour in 1991. This construction builds a block cipher PX from an n-bit permutation P and two n-bit keys k_0 and k_1, setting $PX_{k_0,k_1}(x) = k_1 \oplus P(x \oplus k_0)$. Here we consider a (natural) extension of the Even-Mansour construction with t permutations $P_1, \ldots, P_t$ and $t+1$ keys, $k_0, \ldots, k_t$. We demonstrate in a formal model that such a cipher is secure in the sense that an attacker needs to make at least $2^{2n/3}$ queries to the underlying permutations to be able to distinguish the construction from random. We argue further that the bound is tight for $t = 2$ but there is a gap in the bounds for $t > 2$, which is left as an open and interesting problem. Additionally, in terms of statistical attacks, we show that the distribution of Fourier coefficients for the cipher over all keys is close to ideal. Lastly, we define a practical instance of the construction with $t = 2$ using AES referred to as AES^2. Any attack on AES^2 with complexity below 2^{85} will have to make use of AES with a fixed known key in a non-black box manner. However, we conjecture its security is 2^{128}.

Keywords: Block ciphers, provable security, Even-Mansour construction, AES.

1 Introduction

Block ciphers are one of the fundamental primitives in symmetric cryptography. Often called the work horses of cryptography, they form the backbone of today's

* Due to page limitations, several proofs are omitted in this proceedings version. A full version is available at [9].

D. Pointcheval and T. Johansson (Eds.): EUROCRYPT 2012, LNCS 7237, pp. 45–62, 2012.

secure communication. Therefore, their design has been an important research focus over the last 20 years, giving rise to different well-established strategies to prevent large classes of attacks. As typical examples, one can mention the practical security approach against linear and differential cryptanalysis [23], and the wide-trail strategy [15] that lead to the design of the AES Rijndael [14]. Another line of research is the so-called provable security approach against statistical attacks, that served as foundation for the block cipher MISTY [27, 28]. One can also mention the decorrelation theory [33] and the design of the ciphers C [1] and KFC [2]. At a high level, the three main design paradigms for block ciphers are Feistel structures such as DES, Lai-Massey ciphers such as IDEA [24], and key-alternating ciphers [12, 14, 15] for which the AES Rijndael is a prominent representative. State-of-the-art block ciphers are quite well understood and provide security against all known attacks. Though there has recently been remarkable progress in the cryptanalysis of AES [7], these results are far from being any threat for the use of AES in practice. Thus, from a practical point of view, block ciphers in general and key-alternating ciphers in particular can be seen as a success story.

Given the degree of confidence in properly designed key-alternating ciphers on the practical side (e.g. with AES approved for the encryption of secret and top secret data in the USA), it is even more surprising that there has been no provable setting developed so far for the design of key-alternating ciphers on the theoretical side. Nobody seems to have even formulated the problem of whether the key-alternating cipher makes sense from this point of view. Clearly, given the state of the art, proving AES secure in any strict sense is out of reach. However, by modeling the round functions as fixed public randomly chosen permutations, we are able to precisely formulate and—as we shall see—prove the soundness of the key-alternating cipher design. The cipher we are dealing with is depicted in Figure 2 and detailed in Section 2.

We note the difference of our setting to that of an idealized Feistel cipher, often called the Luby-Rackoff construction [26], or to that of similar results obtained for the Lai-Massey schemes [34]. In these former works, for each key it is assumed that the function used in the Feistel (resp. Lai-Massey) construction is chosen at random. Directly adopting this model to the case of a key-alternating cipher immediately results in an ideal cipher (even for one round). At the same time, in most key-alternating ciphers including AES, the key is the only part of the design to define the cipher permutation and all round permutations are fixed for the entire cipher, not varying from key to key. In other words, working along the lines of [26] does not elucidate how to mix the key into the state. It is exactly this point we deal with in the present paper, both at a high-level, i.e. in a provable setting, as well as at lower-levels, i.e. considering statistical attacks and as a guideline for actually designing ciphers.

Interestingly, another look at the construction and its properties arises from the question of how to design the key schedule of a block cipher. This has been an open problem in symmetric-key cryptography for decades. While some ciphers are based upon simple linear or nearly linear key schedules [8, 18], a number of others opt for heavier and often highly nonlinear key schedules, sometimes as complex as the round functions [3] or the cipher itself [31]. In the prominent case of AES, for instance, the key schedule is iterative, mainly linear, and provides relatively slow diffusion in the backward direction. It is precisely these properties that facilitated the related-key cryptanalysis of the full AES-192 and AES-256, e.g. [5,6] as well as the recent biclique cryptanalysis of all three full AES versions in the classical single-key model [7]. In general, these examples emphasize a relatively weak understanding of key scheduling algorithms, compared to the design of block cipher rounds. In this context, the results of this paper can be seen as a case for simple key schedules (or even no key scheduling at all). Hence, they provide new insights into the design of block ciphers.

1.1 Related Work

An exception from the above-mentioned lack of theoretical studies of key-alternating block ciphers is the Even-Mansour construction [16] depicted in Figure 1. This construction can be seen as a one-round variant of a key-alternating cipher. Informally, Even and Mansour proved that in order to have a reasonable success probability in decrypting an (unqueried) message, an attacker has to make roughly $2^{n/2}$ queries to the permutation P. In this setting, the attacker is given oracle access to P, its inverse, and to an encryption and decryption oracle. Later, Daemen [11] showed that this bound is actually tight. He presented a differential attack on the Even-Mansour scheme that allows to successfully recover the key with a good probability, after $2^{n/2}$ evaluations of both the permutation P and the encryption oracle.

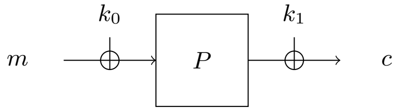


Fig. 1. The Even-Mansour construction

1.2 Our Contribution

Our contributions in this paper are twofold.

On the theoretical side (cf. Section 3), we provide the first treatment of the concept of key-alternating ciphers in a provable security setting. We prove below that, for any t-round version of the cipher with randomly drawn and fixed underlying permutations, $t \geq 2$, depicted in Figure 2, an attacker needs to make at least $2^{2n/3}$ queries before being able to distinguish the encryption oracle from a random permutation. Here n is the block size of the cipher. Furthermore, we provide a simple attack that shows that an attacker, by making $2^{\frac{t}{t+1}n}$ queries, is able to recover the secret key used in the decryption oracle. We do conjecture that this lower bound — being tight only for $t = 2$ — is the actual bound. We leave proving this as an important open question (see also Section 7). Note that in this setup, we necessarily only consider the query complexity of an attacker, ignoring the computational complexity. It seems unlikely that an attack with a comparable computational complexity exists. Such an attack would in particular imply an attack on e.g. AES-256 with a complexity of around 2^{120} operations.

On the practical side, we propose to actually use the construction of Figure 2. Given our theoretical results, the merit of this approach is the following: Any attack on a key-alternating cipher with complexity below $2^{2n/3}$ will have to make use of the round functions in a non-black box manner.

However, and we feel that it is important to make this point explicit even though it might be obvious, the theoretical result does not carry over to any efficient instance, as one must consider the round functions as black-boxes— i.e. objects which the adversary must query to evaluate—in order to meaningfully discuss the distinguishability of the cipher from a random permutation by an information-theoretic adversary.

This fact and the fact that, as mentioned above, the theoretical bounds are likely to be lower than the computational complexity of any attack, motivates us to study the security of our proposal with respect to such statistical attacks as linear cryptanalysis (see Section 5).

To capture the difference between the single-round Even-Mansour cipher and the multiple-round key-alternating construction with respect to linear cryptanalysis, we study the Fourier spectrum of the ciphers. We prove that once the fixed underlying permutations are close to average (which is the case for randomly drawn permutations with high probability), the distribution of Fourier coefficients for the key-alternating cipher over all keys for $t \geq 2$ gets close to that over all permutations — the natural reference point for any block cipher. At the same time, we demonstrate that this is not the case for the original Even-Mansour construction with $t = 1$ where the Fourier coefficients almost do not change from key to key. It seems therefore unlikely that linear attacks are able to break the multiple-round key-alternating cipher with $t \geq 2$.

Finally, as the crypto community likes targets and we anticipate that having a concrete proposal is a valuable stimulation for further research, we propose an actual cipher called AES^2 following the 2-round version of the general construction (see Section 6). Here we replace the random permutations by two instantiations of AES-128 with fixed known keys. Given the new AES instructions on recent Intel processors, AES^2 performs very competitively on those platforms, with as few as 2.65 cycles per byte required in the counter mode.

We conclude with a section dedicated to open questions and further work (Section 7), discussing how to possibly improve and extend the research we consider in the paper.

2 The Construction

The cipher we consider is an idealized model of a key-alternating cipher — the notion introduced under this name in [14, 15] in connection with the design of AES and used without being explicitly named even before that [12] in similar contexts. Such a cipher consists of round functions interleaved with xoring round keys to the current state. In our idealized model, the round functions are the public, randomly chosen permutations P_i and the key consists of $t+1$ independent round-keys are k_i. More precisely, let $P_1, \ldots, P_t$ be permutations from $\{0,1\}^n$ to $\{0,1\}^n$, $t \geq 1$. Let $k_0, \ldots, k_t \in \{0,1\}^n$ be keys. The block cipher $E = E_{k_0,\ldots,k_t} : \{0,1\}^n \to \{0,1\}^n$ we consider is defined by

$$E(x) = E_{k_0 \cdots k_t}(x) = P_t(\ldots P_2(P_1(x \oplus k_0) \oplus k_1) \ldots) \oplus k_t \tag{1}$$

for $x \in \{0,1\}^n$. The cipher is shown in Figure 2.

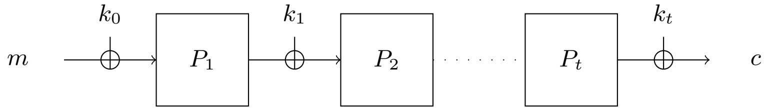


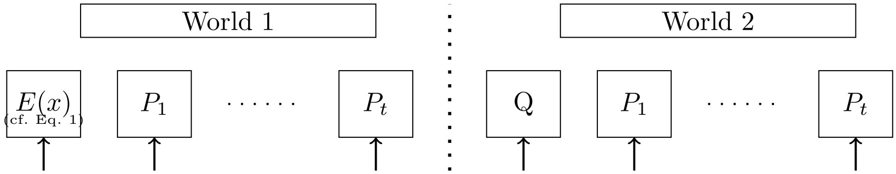
Fig. 2. A key-alternating cipher

3 Indistinguishability Analysis

Putting $N = 2^n$, we define the PRP security of E against an adversary A expecting a $(t+1)$-tuple of oracles as

$$\mathbf{Adv}^{\mathrm{PRP}}_{E,N,t}(A) = \Pr[k_0 \cdots k_t \leftarrow \{0,1\}^n; A^{E_{k_0 \cdots k_t}, P_1, \ldots, P_t} = 1] - \Pr[A^{Q, P_1, \ldots, P_t} = 1]$$

where in each experiment $Q, P_1, \ldots, P_t$ are independent and uniformly sampled random permutations. Here A can make inverse queries to each of its oracles. Thus, an attacker has to tell apart two worlds, depicted below.



We note that one *must* consider the permutations $P_1, \ldots, P_t$ as random (or pseudorandom) black-boxes—i.e. objects which the adversary must query to evaluate—in order to meaningfully discuss the distinguishability of $E_{k_0,\ldots,k_t}$ from a random permutation by an information-theoretic adversary.

We define

$$\mathbf{Adv}^{\mathrm{PRP}}_{E,N,t}(q) = \max_{A} \mathbf{Adv}^{\mathrm{PRP}}_{E}(A)$$

where the maximum is taken over all adversaries A making at most q queries. (We note the parameters n and t are elided from both of the notations $\mathbf{Adv}^{\mathrm{PRP}}_{E}(A)$ and $\mathbf{Adv}^{\mathrm{PRP}}_{E}(q)$; but it should be understood that $\mathbf{Adv}^{\mathrm{PRP}}_{E}(q)$ is a function n and t as well as of q.)

Our main security result is the following:

Theorem 1. *Let $N = 2^n$ and let $q = N^{\frac{t}{t+1}}/Z$ for some $Z \geq 1$. Then, for any $t \geq 1$, and assuming $q < N/100$, we have*

$$\boldsymbol{Adv}^{\mathrm{PRP}}_{E,N,t}(q) \leq \frac{4.3q^3t}{N^2} + \frac{t+1}{Z^t}.$$

For $t \geq 2$ the limiting term in the above bound is $4q^3t/N^2$, which caps q at around $N^{2/3}$. The following corollary is more telling.

Corollary 1. *Assume $t \geq 2$. Let $q = N^{\frac{2}{3}}/\lambda\sqrt[3]{t}$ for some $\lambda \geq 1$. Then, assuming $q < N/100$,*

$$\boldsymbol{Adv}^{\mathrm{PRP}}_{E,N,t}(q) \leq \frac{4.3}{\lambda^3} + \frac{t+1}{(\sqrt[3]{t}\lambda)^t}.$$

We also note that $q < N/100$ as long as $n \geq 20$; this condition is therefore compatible with practical parameters. We note that Corollary 1's security of $q \approx N^{\frac{2}{3}}$ is optimal for $t = 2$ (cf. Section 3.1) and suboptimal for $t > 2$, in which case we conjecture a security of $q \approx N^{\frac{t}{t+1}}$. Closing this gap might be obtained by a tightening of Proposition 2 below.

Theorem 1 is proved by a hybrid argument involving an intermediate game. In order to outline this hybrid argument we start by developing some new notation.

Note firstly that if E is defined as in (1) then, putting $P_0 = E^{-1}$, we have

$$P_0(P_t(\cdots P_1(\cdot \oplus k_0) \cdots) \oplus k_t) = id.$$

Applying P_0^{-1} to both sides and then substituting $P_0(\cdot)$ for the input, we find

$$P_t(\cdots P_2(P_1(P_0(\cdot) \oplus k_0) \oplus k_1) \cdots) \oplus k_t = id. \tag{2}$$

It is easy to see that, for fixed $k_0, \ldots, k_t$, randomly sampling $P_1, \ldots, P_t$, defining E as in (1) and giving an adversary access to the tuple of oracles $(E, P_1, \ldots, P_t)$ (and their inverses) is equivalent to sampling $P_0, \ldots, P_t$ uniformly at random from all $(t+1)$-tuples of permutations satisfying (2) and giving the adversary access to $(P_0^{-1}, P_1, \ldots, P_t)$ (and their inverses). Moreover, it is just a notational change to give the adversary access to $(P_0, P_1, \ldots, P_t)$, since the adversary is allowed inverse queries anyway (of course, the adversary is alerted to the fact that its first oracle is now P_0 and not P_0^{-1}).

We now formally implement the interface $(P_0, \ldots, P_t)$ via an oracle $O(N, t)$ taking $k_0, \ldots, k_t$ as implicit parameters. Rather than sampling $P_0, \ldots, P_t$ uniformly at random from those sequences satisfying (2) at the start of the experiment, $O(N, t)$ implements the permutations $P_0, \ldots, P_t$ by lazy sampling. More precisely, $P_0, \ldots, P_t$ are initially set to be undefined everywhere. When the adversary makes a query $P_i(x)$ or $P_i^{-1}(y)$, the adversary defines P_i at the relevant point using the following procedure, illustrated for the case of a forward query $P_i(x)$ (the case of a backward query is analogous):

- Let $\mathcal{P} = \mathcal{P}(P_0, \ldots, P_t)$ be the set of all $(t+1)$-tuples of permutations $(\overline{P}_0, \ldots, \overline{P}_t)$ such that $\overline{P}_i$ extends the currently defined portion of P_i, and such that

$$\overline{P}_t(\cdots \overline{P}_2(\overline{P}_1(\overline{P}_0(\cdot) \oplus k_0) \oplus k_1) \cdots \oplus k_{t-1}) \oplus k_t = id. \tag{3}$$

  Then $O(N,t)$ samples uniformly at random an element $(\overline{P}_0, \ldots, \overline{P}_t)$ from $\mathcal{P}$. The adversary sets $P_i(x) = \overline{P}_i(x)$ and returns this value.

After the above, the adversary "forgets" about $\overline{P}_0, \ldots, \overline{P}_t$, and samples these afresh at the next query. It is clear that this lazy sampling process gives the same distribution as sampling the tuple $(P_0, \ldots, P_t)$ at the start of the game. Thus, giving the adversary oracle access to $O(N,t)$ is equivalent to giving the adversary oracle access to $(E, P_1, \ldots, P_t)$, up to the cosmetic change that E is replaced by E^{-1}. We therefore have:

Proposition 1. *With $O(N,t)$ defined as above, we have:*

$$\boldsymbol{Adv}^{\mathrm{PRP}}_{E,N,t}(A) = \Pr[k_0 \cdots k_t \leftarrow \{0,1\}^n; A^{O(N,t)} = 1] - \Pr[A^{Q_0,Q_1,\ldots,Q_t} = 1]$$

where $Q_0, \ldots, Q_t$ are independent random permutations.

(We emphasize that $k_0, \ldots, k_t$ are implicit arguments to $O(N,t)$.)

Our hybrid will be an oracle $\tilde{O}(N,t)$ (also taking $k_0, \ldots, k_t$ as implicit inputs) that uses a slightly different lazy sampling procedure to define the permutations $P_0, \ldots, P_t$. Say that a sequence of partially defined permutations is *consistent* if $\mathcal{P}(P_0, \ldots, P_t) \neq \emptyset$, with $\mathcal{P}(\cdot)$ defined as in the description of $O(N,t)$ above. Initially, $\tilde{O}(N,t)$ also sets the permutations $P_0, \ldots, P_t$ to be undefined everywhere. Upon receiving (say) a forward query $P_i(x)$, $\tilde{O}(N,t)$ uses the following lazy sampling procedure to answer:

- Let $U \subseteq \{0,1\}^n$ be the set of values y such that defining $P_i(x) = y$ maintains the consistency of $P_0, \ldots, P_t$, besides maintaining the fact that P_i is a permutation. Then $\tilde{O}(N,t)$ samples a value y uniformly from U, sets $P_i(x) = y$, and returns y.

Inverse queries are lazy sampled the same way. While not immediately apparent, the above lazy sampling procedure produces a slightly *different* distribution of outputs than the first lazy sampling procedure.

Theorem 1 is an direct consequence of Proposition 1 and of the following two propositions.

Proposition 2. *Let $q < N/100$. With $O(N,t)$ and $\tilde{O}(N,t)$ defined as above,*

$$\Pr[k_0, \ldots, k_t \leftarrow \{0,1\}^n; A^{O(N,t)} = 1] - \Pr[k_0, \ldots, k_t \leftarrow \{0,1\}^n; A^{\tilde{O}(N,t)} = 1] \leq \frac{4.3q^3t}{N^2}$$

for every adversary A making at most q queries.

Proposition 3. *Let $q = N^{\frac{t}{t+1}}/Z$ for some $Z \geq 1$ be such that $q < N/3$. With $\tilde{O}(N,t)$ defined as above,*

$$\Pr[k_0,\ldots,k_t \leftarrow \{0,1\}^n; A^{\tilde{O}(N,t)} = 1] - \Pr[A^{Q_0,\ldots,Q_t} = 1] \leq \frac{t+1}{Z^{t+1}}.$$

for every adversary A making at most q queries, where $Q_0,\ldots,Q_t$ are independent random permutations.

Proposition 2 is the main technical hurdle in our proof. Its proof, however, is entirely combinatorial, given that we actually show this bound holds even when A sees the keys $k_0,\ldots,k_t$. The presence of keys is therefore actually irrelevant for this proposition[1]. We refer to the full version for more details and a proof of Proposition 2.

The proof of Proposition 3, on the other hand, is fairly accessible, and also contains those ingredients that have the most "cryptographic interest".

Proof (of Proposition 3.). We make the standard assumption that the adversary never makes a redundant query (querying $P_i^{\pm 1}(x)$ twice or querying, e.g., $P_i(x)$ after obtaining x as an answer to a query $P_i^{-1}(y)$).

We modify $\tilde{O}(N,t)$ to use a slightly different lazy sampling method, equivalent to $\tilde{O}(N,t)$'s original sampling method. In this new method, we also maintain a flag bad which is originally set to false.

$\tilde{O}(N,t)$'s new sampling method is as follows: when faced with a query $P_i(x)$, $\tilde{O}(N,t)$ samples a value y uniformly at random from the remaining range of $P_i(x)$, that is, uniformly at random from

$$\{0,1\}^n \backslash \{P_i(x') : x' \in \{0,1\}^n, P_i(x') \text{ is defined}\}.$$

$\tilde{O}(N,t)$ then checks if setting $P_i(x) = y$ would make $P_0,\ldots,P_t$ inconsistent; if so, it sets bad = true, and resumes its original sampling method for the rest of the game (including to answer the last query); otherwise, it sets $P_i(x) = y$, and returns y. Inverse queries are treated the same.

We can also define a value for the bad flag when the adversary has oracle access to the random permutations $(Q_0, Q_1, \ldots, Q_t)$. Originally, set bad = false and select random values $k_0,\ldots,k_t$. Set $Q_0,\ldots,Q_t$ to be undefined at all points, and use lazy sampling to define them by simulating the lazy sampling process for $P_0,\ldots,P_t$ up until bad = true; after bad = true, simply keep lazy sampling each permutation Q_i while ignoring bad as well as $k_0,\ldots,k_t$.

Obviously, the probability bad is set to true is equal in both worlds, and the two worlds behave identically up until bad = true. Thus (a standard argument shows that) the adversary's advantage is upper bounded by the probability that bad is set to true.

For simplicity, we upper bound the probability that bad becomes true when the adversary has oracle access to $Q_0,\ldots,Q_t$. In this case, note that it is equivalent

[1] We note that the bound of Proposition 2 is the bottleneck of Theorem 1. A potential improvement of Proposition 2 might exploit the fact that $k_0,\ldots,k_t$ aren't known to the adversary.

to set the bad flag by sampling the values $k_0, \ldots, k_t$ randomly at the end of the game, and then checking whether these values are inconsistent with the partially defined permutations $Q_0, \ldots, Q_t$. (To recall, $k_0, \ldots, k_t$ are inconsistent with $Q_0, \ldots, Q_t$ if there exist no permutations $\overline{Q}_0, \ldots, \overline{Q}_t$ such that

$$\overline{Q}_t(\cdots \overline{Q}_2(\overline{Q}_1(\overline{Q}_0(\cdot) \oplus k_0) \oplus k_1) \cdots \oplus k_{t-1}) \oplus k_t = id.)$$

Given the partially defined permutations $Q_0, \ldots, Q_t$ and values $k_0, \ldots, k_t$ a *contradictory path* is a sequence of values $(x_0, y_0), \ldots, (x_t, y_t)$ such that (i) $Q_i(x_i) = y_i$ for all i and (ii) $|\{i : y_i \oplus x_{i+1} = k_i, 0 \leq i \leq t\}| = t$, where we put $x_{t+1} = x_0$. Because $q < N/3$, one can show that $Q_0, \ldots, Q_t$ is consistent with $k_0, \ldots, k_t$ if and only if there exists no contradictory path (again, we have to refer to the full versions for details). Since each Q_i contains at most q defined input-output pairs (x_i, y_i) at the end of the game, there are at most q^{t+1} possible different sequences $((x_0, y_0), \ldots, (x_t, y_t))$ such that $Q(x_i) = y_i$ for $0 \leq i \leq t$. For each of these sequences, the probability that the random selection of $k_0, \ldots, k_t$ creates a contradictory path is upper bounded by $(t+1)N^{-t}$, since the condition $k_i = y_i \oplus x_{i+1}$ must be satisfied for all but one value of i, $0 \leq i \leq t$, and we can union bound over this value of i. Hence, by a union bound over the (at most) q^{t+1} possible different sequences, the probability that bad is set to true is at most $\frac{(t+1)q^{t+1}}{N^t} = \frac{t+1}{Z^t}$ as desired.

3.1 An Upper Bound

For any number of rounds t, there is an (non-adaptive) attack with a query complexity of roughly $t2^{\frac{t}{t+1}n}$, thus meeting the bound on the query complexity for $t = 2$. Note that this is not an attack in the practical sense, as the computational cost is higher than brute force. The idea of this attack is to actually construct (with high probability) a contradictory path for each possible key.

1. Make $2^{\frac{t}{t+1}n}$ queries to E and each of the oracles P_1 to P_t. Denote the set of queries to P_i by $\mathcal{P}_i$ and queries to E_k by $\mathcal{M}$.
2. For each key candidate $(k_0, k_1, \ldots, k_t)$ do:
   (a) Find all sequences of values $(x_1, \ldots, x_{t-1})$ such that $x_1 \in \mathcal{M}$ and $x_i \oplus k_{i-1} \in \mathcal{P}_i$, $\forall 1 \leq i \leq t$ and $P_i(x_i \oplus k_{i-1}) = x_{i+1}$, $\forall 1 \leq i \leq t-1$.
   (b) Check if $P_t(x_t \oplus k_{t-1}) \oplus k_t = E(x_1)$ for all these sequences.
   (c) If so, assume $(k_0, k_1, \ldots, k_t)$ is the correct value of the key;
   (d) otherwise, it is certainly the wrong value of the key.

To get a better reduction on key-candidates, a bit more than $t2^{\frac{t}{t+1}n}$ queries are sufficient.

4 Attacks

The bounds proved earlier are information-theoretic bounds which take into account only the number of queries of the random permutations made by an adversary. Of equal interest are attacks which take the computational complexity into account. In this section we consider only attacks in the single key-model. Note that, in the case where all round-keys are independent, related-key attacks exist trivially. However, the situation might be very different in the case where all round-keys are identical, see Section 7 for further discussion on this point.

4.1 Daemen's Attack for $t = 1$

For the original Even-Mansour construction (in our setting, this corresponds to $t = 1$), a differential attack has been published by Daemen [11] meeting the lower bound of $2^{n/2}$ evaluations of P proven by Even and Mansour. It can be described as follows:

1. Choose s plaintext pairs (m_i, m_i^*), $1 \leq i \leq s$, with $m_i \oplus m_i^* = \Delta$ for any nonzero constant Δ.
2. Get the encryptions (c_i, c_i^*) of the s pairs.
3. For $2^n/s$ values v:
   (a) Compute $w' := P(v) \oplus P(v \oplus \Delta)$.
   (b) If $w' = c_i \oplus c_i^*$ for some i: Output $k_0 := v \oplus m_1$ and $k_1 := c_1 \oplus P(m_1 \oplus k_0)$ and stop.

For a random permutation P, only very few values of v are expected to satisfy $P(v) + P(v + \Delta) = c_i \oplus c_i^*$. The wrong candidates can be easily filtered in step (3b) by testing them on a few additional encryptions. After encrypting s plaintext pairs, one has to perform about $2 \cdot 2^n/s$ evaluations of P. The expression $2(s + 2^n/s)$ is minimal for $s = 2^{n/2}$. In this case, the time complexity is $2^{n/2}$ with a storage requirement of $2^{n/2}$ plaintext pairs.

4.2 A Meet in the Middle Attack

There is a meet in the middle attack on the t-permutation construction which finds the keys in time and space $2^{tn/2}$ for $t > 1$. This is a straight-forward attack given here for the case $t = 2$:

1. From a pair of messages (m_1, m_2), compute and save in a sorted table, T, the values $P(m_1 \oplus k) \oplus P(m_2 \oplus k)$ for all possible 2^n values of k.
2. Get the encryptions c_1 and c_2 of m_1 respectively m_2.
3. For all 2^n possible values of k' compute $Q^{-1}(c_1 \oplus k') \oplus Q^{-1}(c_2 \oplus k')$ and look for a match in T.
4. Each match gives candidate values for the three keys, which are tested against additional encryptions.

5 Statistical Properties

A fundamental cryptographic property of a block cipher is its Fourier spectrum that completely defines the cipher via the Fourier transform and whose distribution is closely related to the resistance against linear cryptanalysis [10].

To support security claims, block cipher designs usually come with arguments why these Fourier coefficients cannot take values exploitable by an attacker. In most cases, however, formal proofs of these properties appear technically infeasible and designers limit themselves to demonstrating upper bounds on trail probabilities, that can be seen as summands to obtain the actual Fourier coefficients. This solution is usually denoted as the practical security approach for statistical cryptanalysis. Such an approach does not allow an accurate estimation of the data complexity of statistical attacks, that typically depends on numerous trails [25, 29].

As opposed to that, we analyze the construction of key alternating cipher following a provable security approach, by directly investigating its Fourier coefficients. In addition, we provide a more informative analysis than for standard block ciphers, as we study the distribution of the Fourier coefficients for the cipher over all keys, rather than bounding the mean value of this distribution. This is made possible by the use of fixed public permutations in our construction. More precisely, in a key-alternating cipher using $t \geq 2$ fixed public permutations, we study the distribution of the Fourier coefficients over all cipher keys. If these permutations are close to the average over all permutations, we show that this distribution turns out to be very close to that over all permutations, suggesting that the t-round key-alternating construction is theoretically sound from this perspective. This implies that it behaves well with respect to linear cryptanalysis.

On the contrary, the distribution of Fourier coefficients for a fixed point in the Fourier spectrum is nearly degenerated for the key-alternating cipher with $t = 1$ (the Even-Mansour cipher). This emphasizes the constructive effect of having 2 and more rounds in the key-alternating cipher.

5.1 Fourier Coefficients over All Permutations

Here we recall the definitions of Fourier coefficients and Fourier spectrum as well as the distribution of Fourier coefficients over all permutations. We also introduce some notations we will be using throughout the section.

Notations. The canonical scalar product of two vectors $a, b \in \{0,1\}^n$ is denoted by $a^T b$. We denote the normal distribution with mean μ and variance σ^2 as $\mathcal{N}(\mu, \sigma^2)$. By $X \sim_v \mathcal{D}$, we denote a random variable X following a distribution $\mathcal{D}$ taken over all values of v. The expectation of X with respect to v is denoted by $\mathbf{E}_v[X]$, its variance (with respect to v) by $\mathbf{Var}_v[X]$.

Fourier Coefficients and Fourier Spectrum. For a permutation $P : \{0,1\}^n \to \{0,1\}^n$, its *Fourier coefficient* at point (α, β) is defined as

$$W^P_{\alpha,\beta} \overset{\text{def}}{=} \sum_{x \in \{0,1\}^n} (-1)^{\alpha^T x + \beta^T P(x)}.$$

The collection of Fourier coefficients at all points $(\alpha, \beta) \in \{0,1\}^n \times \{0,1\}^n$ is called the *Fourier spectrum* of P. For a block cipher F, we denote the Fourier coefficient at point (α,β) as $W^F_{\alpha,\beta}[K]$ to emphasize its dependency on key K. If F is the t-round key-alternating cipher, this is denoted by $W^{P_1,\ldots,P_t}_{\alpha,\beta}[K]$.

The following characterisation for the distribution of Fourier coefficients in a Boolean permutation has been proven.

Fact 1 ([13, Corollary 4.3, Lemma 4.6]). *When $n \geq 5$, the distribution of the Fourier coefficient $W^P_{\alpha_0,\beta_0}$ with $\alpha_0, \beta_0 \neq 0$ over all n-bit permutations can be approximated by the following distribution up to continuity correction:*

$$W^P_{\alpha_0,\beta_0} \sim_P \mathcal{N}(0, 2^n). \tag{4}$$

The distribution of Fact 1 is the reference point throughout the section: A block cipher cannot have a better distribution of Fourier coefficients than that close to Fact 1.

5.2 Fourier Coefficients in the Single-Round Even-Mansour Cipher

Let F be the basic single-round Even-Mansour cipher, that is, a fixed public permutation P surrounded by two additions with keys k_0 and k_1, respectively (see Figure 1). If $W^P_{\beta_0,\beta_1}$ is the Fourier coefficient for the underlying permutation P at point (β_0, β_1), then the Fourier coefficient for the cipher at this point is

$$W^F_{\beta_0,\beta_1} = (-1)^{\beta_0^T k_0 \oplus \beta_1^T k_1} W^P_{\beta_0,\beta_1}.$$

Now consider the distribution of $W^F_{\beta_0,\beta_1}$ with $\beta_0 \neq 0$, $\beta_1 \neq 0$ taken over all keys (k_0, k_1). Its support contains exactly two points: $W^P_{\beta_0,\beta_1}$ and $-W^P_{\beta_0,\beta_1}$. Thus, the value of $W^F_{\beta_0,\beta_1}$ almost does not vary from key to key. This is crucially different from the reference point – the distribution over all permutations of Fact 1.

5.3 Fourier Coefficients in the t-Round Key-Alternating Cipher

Now we state the main result of this section. The proof is given omitted in this extended abstract and we refer to the full version.

Theorem 2. *Fix a point (β_0, β_t) with $\beta_0, \beta_t \neq 0$ in the Fourier spectrum of the t-round key-alternating n-bit block cipher with round permutations $P_1, \ldots, P_t$ for $t \geq 2$ and sufficiently high n. Then the distribution of the Fourier coefficient $W^{P_1,\ldots,P_t}_{\beta_0,\beta_t}$ at this point over all keys K is approximated by:*

$$W^{P_1,\ldots,P_t}_{\beta_0,\beta_t}[K] \sim_K \mathcal{N}\left(0, (1+\varepsilon)\left(\frac{2^n-1}{2^n}\right)^{t-1} 2^n\right), \tag{5}$$

assuming that the distributions over points of the Fourier spectra of the permutations P_i, $1 \leq i \leq t$, have variances satisfying

$$\mathop{\mathbf{Var}}_{(\beta_{i-1},\beta_i)}\left[W^{P_i}_{\beta_{i-1},\beta_i}\right] \geq 2^{n/2}, \tag{6}$$

and that for any given key K, the signs of the Fourier coefficients behave independently for different points. The deviation of the permutations P_i from the mean over all permutations Q_i is quantified by factor $(1+\varepsilon)$*:*

$$\begin{aligned} &\textstyle\sum_{(\beta_1,\ldots,\beta_{t-1})} \left(W^{P_1}_{\beta_0,\beta_1} \cdots W^{P_t}_{\beta_{t-1},\beta_t}\right)^2 \\ &= (1+\varepsilon)\cdot \mathbf{E}_{Q_1,\ldots,Q_t}\left[\textstyle\sum_{(\beta_1,\ldots,\beta_{t-1})} \left(W^{Q_1}_{\beta_0,\beta_1} \cdots W^{Q_t}_{\beta_{t-1},\beta_t}\right)^2\right]. \end{aligned} \tag{7}$$

Interestingly, the latter deviation ε from the mean in (7) is small for most choices of the P_i. For instance, in case $t=2$, it can be shown that over all permutations, mean and variance of each summand in (7) are 2^{2n} and 2^{4n+2}, respectively. The whole sum then approximately follows a normal distribution $\mathcal{N}(2^{3n}-2^{2n}, 2^{5n+2}-2^{4n+2})$. This means that for *randomly drawn permutations* P_1, P_2, the sum $\sum_{\beta_1}\left(W^{P_1}_{\beta_0,\beta_1}W^{P_2}_{\beta_1,\beta_2}\right)^2$ will be within d standard deviations from its mean with probability erf $\left(d/\sqrt{2}\right)$. Notably, this implies $\Pr(|\varepsilon| \le 2^{-n/2+3}) \approx 0.9999$, i.e. $|\varepsilon|$ only very rarely exceeds $2^{-n/2+3}$.

Theorem 2 gives the distribution over all keys of the Fourier coefficient $W^{P_1,\ldots,P_t}_{\beta_0,\beta_t}$ individually for each nontrivial point (β_0,β_t). Appropriate choices for the P_i should have distributions close to $\mathcal{N}(0,2^n)$ for each nontrivial point, not only for some of them. Conversely, the distribution of the Fourier coefficient at the (trivial) point $(\beta_0, 0)$ differs from (5) for any choice of the P_i, since it is constant over the keys.

Note also that the result of Theorem 2 does not require the underlying permutations to be different. Moreover, it does not require the permutations P_i to be randomly drawn from the set of all permutations, but holds for any fixed choice of permutations satisfying (6). To obtain a distribution close to ideal, however, the set of underlying permutations has to ensure a small deviation ε in (7). As argued above, drawing the underlying permutations at random from the set of all permutations is highly likely to result in a very small deviation ε from the average.

Summarising, the results of Theorem 2 suggest that once the small number of $t \ge 2$ underlying permutations are carefully chosen and fixed, the t-round key-alternating cipher for each secret key is likely to be statistically sound which rules out some crucial cryptanalytic distinguishers. More precisely, the distributions of the Fourier coefficients for the t-round key-alternating cipher over all keys become close to those over all permutations.

Note that, in contrast to the reference point, it is possible to identify large but efficiently representable subsets of keys where the distribution is again degenerated, as in the case for $t=1$. Examples of such sets are sets of keys where one fixes all keys k_1 up to k_{t-1}. For any point (β_0,β_1) the value of $W^{P_1,\ldots,P_t}_{\beta_0,\beta_t}$ takes on only two possible values - over all possible sub-keys k_0, k_t. However, it seems unlikely that this can be used in an attack.

6 Practical Constructions

In this section, we discuss possible practical realisations of the t-round key-alternating cipher.

A natural approach to building a practical cipher following the t-permutation construction is to base the t fixed permutations on a block cipher by fixing some keys. With $t = 1$, this corresponds to the original Even-Mansour construction, so the security level is limited to $2^{n/2}$ operations with n denoting the cipher's block length. With a 128-bit block cipher such as the AES, we therefore only obtain a security level of 2^{64} in terms of computational complexity, so it is advisable to choose $t > 1$.

In the following we describe a sample construction with $t = 2$, that is, we consider the 2-round key alternating construction with permutations P_1 and P_2 and the keys k_0, k_1, k_2.

6.1 AES^2: A Block Cipher Proposal Based on AES

The construction is defined by fixing two randomly chosen 128-bit AES-128 keys, which specifies the permutations P_1 and P_2. The key is comprised by three independently chosen 128-bit secret keys k_0, k_1, k_2.

Let AES$[k]$ denote the (10-round) AES-128 algorithm with the 128-bit key k and the 128-bit quantities π_1, π_2 be defined based on the first 256 bits of the binary digit expansion of $\pi = 3.1415\ldots$:

$$\pi_1 := \texttt{0x243f6a8885a308d313198a2e03707344} \quad \text{and}$$
$$\pi_2 := \texttt{0xa4093822299f31d0082efa98ec4e6c89}.$$

Then we denote the resulting 2-permutation construction by AES$^2[k_0, k_1, k_2]$. Its action on the 128-bit plaintext m is defined as:

$$\mathrm{AES}^2[k_0, k_1, k_2](m) := \mathrm{AES}[\pi_2](\mathrm{AES}[\pi_1](m \oplus k_0) \oplus k_1) \oplus k_2. \qquad (8)$$

Security. Any attack on AES^2 in the single secret-key model with complexity below 2^{85} will have to make use of AES with a fixed known key in a non-black box manner. On the other hand, we are aware of no attack with a computational complexity of less than 2^{128}. Moreover, if the distribution of Fourier coefficients for AES$[\pi_1]$ and AES$[\pi_2]$ meets the assumption of average behaviour, Theorem 2 suggests that the Fourier coefficients for AES^2 are distributed close to ideal which implies resistance against basic linear cryptanalysis and some of its variants. Intuitively, this construction can be seen to arguably transfer the security properties for AES with a single randomly fixed key to the entire cipher as a set of permutations. For AES^2, we explicitly do not claim any related-, known- or chosen-key security.

Performance. AES^2 can be implemented very efficiently in software on general-purpose processors. The two AES keys π_1 and π_2 are fixed and, therefore, the round keys for the two AES transformations can be precomputed, so there is no need to implement the key scheduling algorithm of AES. This ensures high key agility of AES^2.

On the Westmere architecture generation of Intel general-purpose processors, AES^2 can be implemented using the AES-NI instruction set [19]. As the AES round instructions are pipelined, we fully utilise the pipeline by processing four independent plaintext blocks in parallel implementing the basic electronic codebook mode (ECB) and counter mode (CTR). The performance of these implementations on recent processors is demonstrated and compared to two conventional implementations of AES-128 (i.e. without AES-NI instructions) – the bitsliced implementation of [21] and the OpenSSL 1.0.0e implementation based on lookup tables. All numbers are given in cycles per byte (cpb).

	Intel Xeon X5670	Intel Core i7 640M
	2.93 GHz, 12 MB L3 cache	2.8 GHz, 4 MB L3 cache
AES^2, AES-NI, ECB	2.54 cpb	2.69 cpb
AES^2, AES-NI, CTR	2.65 cpb	2.76 cpb
AES-128, AES-NI, ECB	1.18 cpb	1.25 cpb
AES-128, AES-NI, CTR	1.32 cpb	1.36 cpb
AES-128, bitsliced, CTR	7.08 cpb	7.84 cpb
AES-128, OpenSSL, CTR	15.73 cpb	16.76 cpb

It turns out that on both platforms, the performance of AES^2 is almost equal to half that of AES, indicating that the overhead is very low. Compared to the best implementations of the AES which are in widespread use now on standard platforms, AES^2 provides a performance improvement of almost factor three and higher with the AES-NI instruction set.

7 Conclusion, Open Problems and Future Work

In this paper we gave the first formal treatment of the key-alternating cipher in a provable setting. For two or more rounds an attacker needs to query the oracles at least $2^{2n/3}$ times for having a reasonable success probability. Furthermore, we studied the security of the construction with respect to statistical attacks, arguing that even for $t = 2$ linear attacks do not seem to be applicable. Finally we gave a concrete proposal mimicking the construction for $t = 2$. There are several lines of future work and open problems we like to mention.

On the theoretical side, it seems unlikely that the bounds given here are tight. Thus, improving them is an important open problem. We actually conjecture that the correct bound on the query complexity is roughly $2^{t/(t+1)n}$. As a first step, deriving bounds that increase with the number of rounds is a goal worth aiming for. Secondly, for now, we have to assume that all round keys are independent. For aesthetical reasons, but also from a practical point of view (see below) it would be nice to prove bounds for the case that all round keys are identical.

On the practical side, mainly for efficiency reasons but also due to resistance against related-key attacks, several variants for $t = 2$ are worth studying. First of all, since the security level is at most 2^n, due to the meet in the middle attack, one could be tempted to derive three n-bit keys k_0, k_1, and k_2 from one n-bit word. The simplest case here is to have all three keys identical. Taking P and Q different, we are not aware of any attack with computational complexity below 2^n. Furthermore, it seems reasonable to assume that such a construction provides some security against certain types of related-key attacks as well. The best attacks we are aware of in such a setting has birthday complexity $2^{n/2}$. See the full version for details.

Eventually, it is an interesting open problem to determine whether the results in this work can be used as directions for alternative block cipher designs, e.g. with minimum key scheduling algorithms. As a typical example, one could consider the possibility to generate public permutations from a variant of the AES, where the round keys would be replaced with simple constants. In general, such an approach could lead to efficient lightweight designs. Interestingly, it is also the direction taken, to a certain extent, by the recently proposed block cipher LED [20]. In its 64-bit version, this cipher just iterates blocks made of 4 rounds and the addition of the master key.

Another tempting way, in order to increase efficiency, is to choose $Q = P$. Similarly, it may be advantageous to have $Q = P^{-1}$, which has the further advantage that the decryption and encryption operations are similar, except for using the keys in reverse order. However, with $Q = P^{-1}$ there is an attack which finds the value of $k_0 \oplus k_2$ using $2^{n/2}$ queries and similar time. After $k_0 \oplus k_2$ is known the cipher is easily distinguishable from a random permutation. Also, with $Q = P$ but now assuming that $k_0 \oplus k_2$ is known, one finds the secret keys using $2^{n/2}$ queries and similar time.

Acknowledgements. Andrey Bogdanov is a postdoctoral fellow of the Fund for Scientific Research - Flanders (FWO). Francois-Xavier Standaert is associate researcher of the Belgian fund for scientific research (FNRS-F.R.S.). This work has been funded in parts by the ERC project 280141 (acronym CRASH). John Steinberger is supported by the National Basic Research Program of China Grant 2011CBA00300, 2011CBA00301, the National Natural Science Foundation of China Grant 61033001, 61061130540, 61073174, and by NSF grant 0994380.Elmar Tischhauser is a doctoral fellow of the Fund for Scientific Research - Flanders (FWO). This work is supported in part by the IAP Programme P6/26 BCRYPT of the Belgian State, by the European Commission under contract number ICT-2007-216676 ECRYPT NoE phase II, by KU Leuven-BOF (OT/08/027), and by the Research Council KU Leuven (GOA TENSE).

References

1. Baignères, T., Finiasz, M.: Dial C for Cipher. In: Biham, E., Youssef, A.M. (eds.) SAC 2006. LNCS, vol. 4356, pp. 76–95. Springer, Heidelberg (2007)
2. Baignères, T., Finiasz, M.: KFC - The Krazy Feistel Cipher. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 380–395. Springer, Heidelberg (2006)
3. Barreto, P.S.L.M., Rijmen, V.: The KHAZAD Legacy-Level Block Cipher. In: First open NESSIE Workshop, Leuven, Belgium, 15 pages (November 2000)
4. Bertoni, G., Daemen, J., Peeters, M., Van Assche, G.: Keccak sponge function family main document. Submission to NIST (Round 2) (2009)
5. Biryukov, A., Dunkelman, O., Keller, N., Khovratovich, D., Shamir, A.: Key Recovery Attacks of Practical Complexity on AES-256 Variants with up to 10 Rounds. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 299–319. Springer, Heidelberg (2010)
6. Biryukov, A., Khovratovich, D.: Related-Key Cryptanalysis of the Full AES-192 and AES-256. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 1–18. Springer, Heidelberg (2009)
7. Bogdanov, A., Khovratovich, D., Rechberger, C.: Biclique Cryptanalysis of the Full AES. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 344–371. Springer, Heidelberg (2011)
8. Bogdanov, A.A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C.: PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450–466. Springer, Heidelberg (2007)
9. Bogdanov, A., Knudsen, L.R., Leander, G., Standaert, F.-X., Steinberger, J., Tischhauser, E.: Key-Alternating Ciphers in a Provable Setting: Encryption Using A Small Number of Public Permutations. IACR Eprint Report 2012/035
10. Chabaud, F., Vaudenay, S.: Links between Differential and Linear Cryptanalysis. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 356–365. Springer, Heidelberg (1995)
11. Daemen, J.: Limitations of the Even-Mansour Construction. In: Matsumoto, T., Imai, H., Rivest, R.L. (eds.) ASIACRYPT 1991. LNCS, vol. 739, pp. 495–498. Springer, Heidelberg (1993)
12. Daemen, J., Govaerts, R., Vandewalle, J.: Correlation Matrices. In: Preneel, B. (ed.) FSE 1994. LNCS, vol. 1008, pp. 275–285. Springer, Heidelberg (1995)
13. Daemen, J., Rijmen, V.: Probability distributions of correlations and differentials in block ciphers. Journal on Mathematical Cryptology 1(3), 221–242 (2007)
14. Daemen, J., Rijmen, V.: The Design of Rijndael. Springer, Heidelberg (2002)
15. Daemen, J., Rijmen, V.: The Wide Trail Design Strategy. In: Honary, B. (ed.) Cryptography and Coding 2001. LNCS, vol. 2260, pp. 222–238. Springer, Heidelberg (2001)
16. Even, S., Mansour, Y.: A Construction of a Cipher from a Single Pseudorandom Permutation. J. Cryptology 10(3), 151–162 (1997)
17. Even, S., Mansour, Y.: A Construction of a Cipher From a Single Pseudorandom Permutation. In: Matsumoto, T., Imai, H., Rivest, R.L. (eds.) ASIACRYPT 1991. LNCS, vol. 739, pp. 210–224. Springer, Heidelberg (1993)
18. FIPS PUB 46-3: Data Encryption Standard (DES) (1999)
19. Gueron, S.: Intel Mobility Group, Israel Development Center, Israel: Intel Advanced Encryption Standard (AES) Instructions Set (2010), `http://software.intel.com/file/24917`

20. Guo, J., Peyrin, T., Poschmann, A., Robshaw, M.: The LED Block Cipher. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 326–341. Springer, Heidelberg (2011)
21. Käsper, E., Schwabe, P.: Faster and Timing-Attack Resistant AES-GCM. In: Clavier, C., Gaj, K. (eds.) CHES 2009. LNCS, vol. 5747, pp. 1–17. Springer, Heidelberg (2009)
22. Keliher, L., Meijer, H., Tavares, S.: Improving the Upper Bound on the Maximum Average Linear Hull Probability for Rijndael. In: Vaudenay, S., Youssef, A.M. (eds.) SAC 2001. LNCS, vol. 2259, pp. 112–128. Springer, Heidelberg (2001)
23. Knudsen, L.R.: Practically Secure Feistel Ciphers. In: Anderson, R. (ed.) FSE 1993. LNCS, vol. 809, pp. 211–221. Springer, Heidelberg (1994)
24. Lai, X., Massey, J.L.: A Proposal for a New Block Encryption Standard. In: Damgård, I.B. (ed.) EUROCRYPT 1990. LNCS, vol. 473, pp. 389–404. Springer, Heidelberg (1991)
25. Lai, X., Massey, J.L.: Markov Ciphers and Differential Cryptanalysis. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 17–38. Springer, Heidelberg (1991)
26. Luby, M., Rackoff, C.: How to Construct Pseudorandom Permutations from Pseudorandom Functions. SIAM J. Comput. 17(2), 373–386 (1988)
27. Matsui, M.: New Block Encryption Algorithm MISTY. In: Biham, E. (ed.) FSE 1997. LNCS, vol. 1267, pp. 54–68. Springer, Heidelberg (1997)
28. Matsui, M.: New Structure of Block Ciphers with Provable Security against Differential and Linear Cryptanalysis. In: Gollmann, D. (ed.) FSE 1996. LNCS, vol. 1039, pp. 205–218. Springer, Heidelberg (1996)
29. Nyberg, K.: Linear Approximation of Block Ciphers. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 439–444. Springer, Heidelberg (1995)
30. O'Connor, L.: Properties of Linear Approximation Tables. In: Preneel, B. (ed.) FSE 1994. LNCS, vol. 1008, pp. 131–136. Springer, Heidelberg (1995)
31. Rijmen, V., Daemen, J., Preneel, B.: Antoon Bosselaers and Erik De Win. The Cipher SHARK. In: Gollmann, D. (ed.) FSE 1996. LNCS, vol. 1039, pp. 99–111. Springer, Heidelberg (1996)
32. Spanos, A.: Probability Theory and Statistical Inference: Econometric Modeling with Observational Data. Cambridge University Press (1999)
33. Vaudenay, S.: Decorrelation: A Theory for Block Cipher Security. J. Cryptology 16(14), 249–286 (2003)
34. Vaudenay, S.: On the Lai-Massey Scheme. In: Lam, K.-Y., Okamoto, E., Xing, C. (eds.) ASIACRYPT 1999. LNCS, vol. 1716, pp. 8–19. Springer, Heidelberg (1999)