Resistance Against Iterated Attacks by Decorrelation Revisited

Aslı Bay[⋆], Atefeh Mashatan[⋆⋆], and Serge Vaudenay

EPFL, Switzerland
{asli.bay, atefeh.mashatan, serge.vaudenay}@epfl.ch

Abstract. Iterated attacks are comprised of iterating adversaries who can make d plaintext queries, in each iteration to compute a bit, and are trying to distinguish between a random cipher C and the ideal random cipher C^* based on all bits. In EUROCRYPT '99, Vaudenay showed that a $2d$-decorrelated cipher resists to iterated attacks of order d when iterations make almost no common queries. Then, he first asked what the necessary conditions are for a cipher to resist a non-adaptive iterated attack of order d. Secondly, he speculated that repeating a plaintext query in different iterations does not provide any advantage to a non-adaptive distinguisher. We close here these two long-standing open problems.

We show that, in order to resist non-adaptive iterated attacks of order d, decorrelation of order $2d-1$ is not sufficient. We do this by providing a counterexample consisting of a cipher decorrelated to the order $2d-1$ and a successful non-adaptive iterated attack of order d against it.

Moreover, we prove that the aforementioned claim is wrong by showing that a higher probability of having a common query between different iterations can translate to a high advantage of the adversary in distinguishing C from C^*. We provide a counterintuitive example consisting of a cipher decorrelated to the order $2d$ which can be broken by an iterated attack of order 1 having a high probability of common queries.

1 Introduction

Unlike asymmetric cryptography, in which the security of a cryptosystem is provably reduced to a mathematical problem and guaranteed by an intractability assumption, the focus in symmetric cryptography is often statistical cryptanalysis and, in the absence of a successful attack, a cryptosystem is believed to be secure. For instance, once the crypto community has spent enough time for scrutinizing a block cipher and has

[⋆] This work was supported in part by the European Commission through the ICT program under contract ICT-2007-216646 ECRYPT II.

[⋆⋆] This work was supported by the National Competence Center in Research on Mobile Information and Communication Systems (NCCR-MICS), a center of the SNF under grant number 5005-67322.

found no successful attacks against its full round version, the block cipher is believed to be secure. However, a different approach against block cipher cryptanalysis was pioneered by Nyberg [Nyb91] where she formalizes the notion of strength against differential cryptanalysis. Her work is followed by Chabaud and Vaudenay [CV94] formalizing the notion of strength against linear cryptanalysis.

Decorrelation Theory, introduced by Vaudenay [Vau99b,Vau03], encapsulates the techniques that guarantee the *provable* resistance of block ciphers against a wide range of statistical cryptanalysis, including the seminal differential and linear attacks, as well as their variants, for example the boomerang attack, truncated differential attacks, and impossible differential attacks. The beauty of this theory is that it can even guarantee resistance against some not-yet-discovered attacks that meet a certain broad criteria in the model presented by Luby and Rackoff [LR85,LR86]. They prove the security of Feistel schemes by assuming that the round function is random. However, their approach needs a very long secret key and is not suitable in practice. Carter and Wegman [CW79,CW81], on the other hand, use derandomization techniques for sampling pairwise independent numbers, which has inspired the notion of decorrelation in that it measures the pseudorandomness with smaller keys and examines its effects against the adversaries.

It is worth mentioning that *perfect* decorrelation of order d is equivalent to *d-wise independence* [Lub86]. Moreover, decorrelation of order d is also referred to as *almost* d-wise independence [NN90,AGM02]. Furthermore, the concept of decorrelation is somewhat related to the notion of pseudorandom functions and pseudorandom permutations except that we do not limit the time-complexity of the distinguisher, but only the number of queries are restricted.

The adversaries considered here can query d plaintexts and receive their corresponding ciphertexts, but are unlimited in terms of computational power. When these plaintext/ciphertext pairs are chosen randomly and independently from each other, we are dealing with d-limited *non-adaptive* adversaries, as opposed to d-limited *adaptive* adversaries. These adversaries give rise to distinguishers of order d, whether adaptive or otherwise, who are trying to distinguish between a random cipher C and the ideal random cipher C^*.

Several block ciphers have been proposed whose security is proven by decorrelation techniques, see for example DFC [PV98], NUT (n-Universal Transformation) families of block ciphers [Vau03]. Using similar techniques, Baignères and Finiasz propose two provably secure block ciphers to use in practice called the block cipher C [BF06a] and KFC [BF06b]. Decorrelation Theory has been used in other results as well, see for instance [Vau98b,Vau00,Vau99a,Vau99b,Vau98a,BV05].

Vaudenay [Vau03] shows how differential and linear attacks fit in the d-limited adversarial model by introducing *iterated* attacks, which are simply constructed by iterating a d-limited distinguisher (see Fig. 1). Linear and differential cryptanalysis can be formulated as non-adaptive iterated attacks of order 1 and order 2, respectively, and the boomerang attack is an adaptive (chosen plaintext and ciphertext) iterated attack of order 4. Moreover, he computes a bound on the advantage of the d-limited adversaries by decorrelation techniques in the Luby-Rackoff model. This result is expressed in the following theorem. Let C denote a random cipher, i.e., the encryption based on a key which is modeled by a random variable, and C^* be the ideal random cipher, i.e., a uniformly distributed permutation. Moreover, $[C]^d$ is the d-wise distribution matrix of C (see Definition 3) and $\|\cdot\|_\infty$ is a matrix-norm (see Definition 4).

Theorem 1. *[Vau03] Let C be a cipher on a message space of cardinality M such that $\|[C]^{2d} - [C^*]^{2d}\|_\infty \leq \varepsilon$, for some given $d \leq M/2$, where C^* is the ideal random cipher. Let us consider a non-adaptive iterated distinguisher of order d between C and C^* with n iterations. We assume that a set of d plaintexts is generated in each iteration in an independent way and following the same distribution. Moreover, we define δ as the probability that two sets drawn with this distribution have a nonempty intersection. Then, we bound the advantage of the adversary as* $\mathrm{Adv}_{\mathcal{A}_{\mathsf{NAI}(d)}} \leq 5\sqrt[3]{\left(2\delta + \frac{5d^2}{2M} + \frac{3\varepsilon}{2}\right)n^2} + n\varepsilon$.

In this paper, we focus on the above result and address an open problem and disprove a claim that arise from Theorem 1. This theorem shows that, in order to resist a non-adaptive iterated attack of order d with seldom common queries, it is *sufficient* for a cipher to have the decorrelation of order $2d$. However, whether or not this is a necessary condition has not been addressed. Moreover, the bound given in the theorem can be interpreted to imply that, perhaps, a high probability δ of having a common query increases the bound of the attack. Despite this hint, Vaudenay in his EUROCRYPT '99 paper [Vau99b] speculates that having the same query to the oracle does not provide any advantage, but whether or not this is true has been left open. We will settle both of these open questions.

Firstly, we show that the decorrelation of order $2d-1$ is not sufficient. We do this by proposing a counterexample consisting of a 3-round Feistel cipher which is decorrelated to the order $2d-1$ and, *yet*, we are able to mount a successful non-adaptive iterated distinguisher of order d against it. Secondly, we propose another set of counterexamples where a higher probability of having common queries surprisingly increases the advantage of the distinguisher. In particular, we show that there is an iterated distinguisher of order 1 on a $2d$-decorrelated cipher when the probability of having at least one query in common in any two iterations is high, which is counterintuitive. The rest of this paper is organized as follows. Section 2 summarizes some background. We dedicate Section 3 to our main contribution and address the aforementioned open problems.

2 Preliminaries

In this paper, F denotes a random function (or equivalently a function set up with a random key) from $\mathcal{M}_1$ to $\mathcal{M}_2$ and F^* denotes the ideal random function from $\mathcal{M}_1$ to $\mathcal{M}_2$, that is, a function drawn uniformly at random among all $|\mathcal{M}_2|^{|\mathcal{M}_1|}$ functions on the given sets. Similarly, C denotes a random cipher (or equivalently, the encryption function set up with a random key) over $\mathcal{M}_1$ and C^* denotes the ideal random cipher over $\mathcal{M}_1$, that is, a permutation drawn uniformly at random among all $|\mathcal{M}_1|!$ permutations. We use the following standard notations: $|S|$ denotes the cardinality of the set S; $\mathcal{M}^d$ is the set of all sequences of d tuples over the set $\mathcal{M}$; $\mathsf{GF}(q)$ is the finite field with q elements; $\mathsf{GF}(q)[x]$ is the set of polynomials defined over $\mathsf{GF}(q)$; $\mathbb{E}(X)$ denotes the expected value of the random variable X; $V(X)$ is the variance of the random variable X; and $\mathsf{gcd}(p(x), q(x))$ denotes the greatest common divisor of $p(x)$ and $q(x)$.

We consider the *Luby-Rackoff model* [LR85] in which an adversary $\mathcal{A}$ is unbounded in terms of *computational power*. It is bounded to d number of plaintext/ciphertext queries to an oracle Ω implementing a random function. The goal of the adversary $\mathcal{A}$ is to guess whether this function is drawn following the distribution of F (resp. C) or of F^* (resp. C^*). When queries are chosen randomly and at once, such an adversary is exactly a d-limited *non-adaptive* distinguisher. However, when queries are chosen depending on the answers to the previous queries, it is referred to as a d-limited *adaptive* distinguisher. In both distinguishers, the measure of success of $\mathcal{A}$ is computed by means of the *advantage* of the adversary.

Definition 2. *Let F_0 and F_1 be two random functions. The* advantage *of an adversary $\mathcal{A}$ distinguishing F_0 from F_1 is defined by* $\mathrm{Adv}_{\mathcal{A}}(F_0, F_1) = \big|\Pr[\mathcal{A}(F_0) = 1] - \Pr[\mathcal{A}(F_1) = 1]\big|$.

Another measure is the *best advantage* of the distinguisher which is formulated as $\mathrm{BestAdv}_{\zeta}(F_0, F_1) = \max_{\mathcal{A} \in \zeta} \mathrm{Adv}_{\mathcal{A}}$. Here, the maximum is taken over adversaries in a class ζ. For instance, ζ can consist of all non-adaptive or all adaptive d-limited distinguishers, denoted by $\mathsf{NA}(d)$ and $\mathsf{A}(d)$, respectively, between F_0 and F_1 depending on $\mathcal{A}$ being non-adaptive or adaptive.

Vaudenay also relates d-limited distinguishers with the two milestones of block cipher cryptanalysis, namely differential and linear cryptanalyses. These attacks are in fact members of a set of attacks called *iterated attacks* which includes many statistical attacks against block ciphers. Iterated attacks are basically constructed by iterating non-adaptive d-limited distinguishers and they are called non-adaptive iterated distinguishers of order d. We denote this distinguisher and its advantage by $\mathcal{A}_{\mathsf{NAI}(d)}$ and $\mathrm{Adv}_{\mathcal{A}_{\mathsf{NAI}(d)}}$, respectively. Briefly, a function $\mathcal{T}$ produces the binary outcome T_i of the d-limited distinguisher at iteration i. Another function $\mathcal{A}cc$ produces the final outcome based on $(T_1, \ldots, T_n)$. The advantage of this Linear and differential cryptanalyses can be given as examples for non-adaptive iterated attacks of order 1 and 2, respectively. Boomerang attack is an adaptive iterated attack of order 4 (with chosen plaintexts and ciphertexts). Figure 1 gives a generic non-adaptive iterated distinguisher of order d with chosen plaintexts. We note that when referring to the advantage of an adversary in the rest of the paper, what we really mean is the best advantage.

```
Parameters: a complexity $n$, a distribution on $X$, a test $\mathcal{T}$, a set $\mathcal{A}cc$
Oracle: an oracle $\Omega$ implementing a permutation $c$
for $i = 1$ to $n$ do
  pick $x = (x_1, \ldots, x_d)$ at random
  get $y = (c(x_1), \ldots, c(x_d))$
  set $T_i = 0$ or $1$ such that $T_i = \mathcal{T}(x, y)$
end for
if $(T_1, \ldots, T_n) \in \mathcal{A}cc$ then
  output 1
else
  output 0
end if
```

Fig. 1. A generic non-adaptive iterated distinguisher of order d

The *d-wise distribution matrix* of a random function is defined next.

Definition 3. *[Vau03] Let F be a random function from $\mathcal{M}_1$ to $\mathcal{M}_2$. The d-wise* distribution matrix *$[F]^d$ of F is a $|\mathcal{M}_1|^d \times |\mathcal{M}_2|^d$-matrix which is defined by $[F]^d_{(x_1,\ldots,x_d),(y_1,\ldots,y_d)} = \Pr_F[F(x_1) = y_1, \ldots, F(x_d) = y_d]$, where $x = (x_1, \ldots, x_d) \in \mathcal{M}_1^d$ and $y = (y_1, \ldots, y_d) \in \mathcal{M}_2^d$.*

Afterwards, the *decorrelation of order d of a random function F* is computed by finding the distance $\mathcal{D}([F]^d, [F^*]^d)$ between its d-wise distribution matrix and the d-wise distribution matrix of the ideal random function F^*. The definition of $\mathcal{D}$ indeed depends on whether the used distinguisher is adaptive or not. Moreover, if $\mathcal{D}([F]^d, [F^*]^d) = 0$, then F is a *perfect* d-decorrelated function. During the paper, we use a d-decorrelated function and a function decorrelated to the order d, interchangeably.

Definition 4. *Let $M \in \mathbb{R}^{|\mathcal{M}_1|^d \times |\mathcal{M}_2|^d}$ be a matrix. Then, two matrix-norms are defined by $\|M\|_\infty = \max_{x_1,\ldots,x_d} \sum_{y_1,\ldots,y_d} |M_{(x_1,\ldots,x_d),(y_1,\ldots,y_d)}|$ and $\|M\|_A = \max_{x_1} \sum_{y_1} \cdots \max_{x_d} \sum_{y_d} |M_{(x_1,\ldots,x_d),(y_1,\ldots,y_d)}|$.*

Next, the advantage of the best distinguisher is computed.

Theorem 5 (Theorems 10 and 11 in [Vau03]). *Let F and F^* be a random function and the ideal random function, respectively. The respective advantages of the best d-limited non-adaptive and adaptive distinguishers, $\mathcal{A}_{\mathsf{NA}(d)}$ and $\mathcal{A}_{\mathsf{A}(d)}$, are $\mathrm{Adv}_{\mathcal{A}_{\mathsf{NA}(d)}}(F, F^*) = \frac{1}{2}\|[F]^d - [F^*]^d\|_\infty$ and $\mathrm{Adv}_{\mathcal{A}_{\mathsf{A}(d)}}(F, F^*) = \frac{1}{2}\|[F]^d - [F^*]^d\|_A$.*

Theorem 1 provides a bound for the advantage of a distinguisher against random permutations. We provide the following theorem for the case of random functions with a better bound for the advantage.

Theorem 6. *Let F be a random function from $\mathcal{M}_1$ to $\mathcal{M}_2$, where $d \leq |\mathcal{M}_1|/2$ and $|\mathcal{M}_2| = N$. Assume that F is decorrelated to the order $2d$ by $\|[F]^{2d} - [F^*]^{2d}\|_\infty \leq \varepsilon$, where F^* is the ideal random function. We consider a non-adaptive iterated distinguisher of order d between F and F^* with n iterations. We assume that a set of d plaintexts is generated in each iteration in an independent way and following the same distribution. Moreover, we define δ as the probability that two sets drawn with this distribution have a nonempty intersection. Then, we bound the advantage of the adversary as*

$$\mathrm{Adv}_{\mathcal{A}_{\mathsf{NAI}(d)}} \leq 5\sqrt[3]{\left(2\delta + \frac{3\varepsilon}{2}\right)n^2} + n\varepsilon.$$

The proof of this theorem can be found in Appendix A.

Theorem 7 (Theorem 21 in [Vau03] for $k = r = 3$). *Let F_1, F_2, and F_3 be three independent random functions over $\mathcal{M}_1$ such that $\|[F_i]^d - [F^*]^d\|_A \leq \varepsilon$ for $i \in \{1, 2, 3\}$, where F^* is the ideal random function. Consider a 3-round Feistel cipher C on $\mathcal{M}_1^2$ as in Fig. 2 having F_i's as a round function in round i and the ideal cipher C^*. Then, we have $\|[C]^d - [C^*]^d\|_A \leq 3\varepsilon + 2d^2/\sqrt{M}$, where $M = |\mathcal{M}_1|^2$.*

The following results are useful for the rest of the paper.

Definition 8. *The trace $\mathsf{Tr}(\beta)$ of an element $\beta \in \mathsf{GF}(2^k)$, is defined as $\mathsf{Tr}(\beta) = \beta + \beta^2 + \cdots + \beta^{2^{k-1}}$.*

Note that it is well known that the trace is linear and the trace of an element of $\mathsf{GF}(2^k)$ is either 0 or 1.

Lemma 9. *Hoeffding's bound [Hoe62]: Let X_1, $X_2, \ldots,$ X_n be independent random variables and $0 \leq X_i \leq 1$, for $i \in \{1, \ldots, n\}$. Define $\bar{X} = \frac{1}{n}\sum_{i=0}^{n} X_i$ and let $\mu = \mathbb{E}(\bar{X})$. Then, for ε, $0 \leq \varepsilon \leq 1 - \mu$, we have $\Pr[\bar{X} \geq \mathbb{E}(\bar{X}) + \varepsilon] \leq e^{-2n\varepsilon^2}$and $\Pr[\bar{X} \leq \mathbb{E}(\bar{X}) - \varepsilon] \leq e^{-2n\varepsilon^2}$. In addition, two-sided Hoeffding's bound is stated by $\Pr[|\bar{X} - \mathbb{E}(\bar{X})| \geq \varepsilon] \leq 2e^{-2n\varepsilon^2}$.*

3 Addressing the Two Open Problems

We deal with two open problems in Decorrelation Theory. In [Vau03], Vaudenay proposes Theorem 1 proving that the decorrelation of order $2d$ is *sufficient* for a cipher in order to resist a non-adaptive iterated attack of order d. We show here that the decorrelation of order $2d - 1$ is not sufficient by providing a counterexample. Secondly, the same theorem can be interpreted to imply that probability of having common queries increases the bound of the attack. To see the effect of this probability, we provide another counterexample showing that when this probability is high, the advantage of the distinguisher can be high.

We now provide a three round Feistel scheme C to be used in the following two subsections. This cipher C consists of three perfect κ-decorrelated functions F_1, F_2, and F_3 on $\mathcal{M}_1 = \mathsf{GF}(q)$. Each F_i is defined by $F_i(x) = a^i_{\kappa-1}x^{\kappa-1} + a^i_{\kappa-2}x^{\kappa-2} + \cdots + a^i_0$ over a finite field $\mathsf{GF}(q)$, where $(a^i_{\kappa-1}, a^i_{\kappa-2}, \ldots, a^i_0)$ is distributed uniformly at random over $\mathsf{GF}(q)^\kappa$, for $i \in \{1, 2, 3\}$. According to Theorem 7, we have $\|[C]^\kappa - [C^*]^\kappa\|_A \leq 2\kappa^2/q$.

3.1 Decorrelation of Order $2d - 1$ is NOT Sufficient

In this section, we are going to propose a counterexample on a 3-round Feistel cipher decorrelated to the order $2d - 1$. We are going to provide

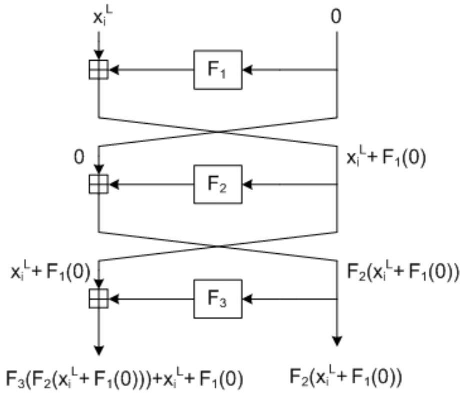

Fig. 2. The structure of the distinguisher for the 3-round Feistel cipher used in subsections 3.1 and 3.2

a successful non-adaptive iterated distinguisher of order d against this cipher showing that the decorrelation of order $2d-1$ is not enough to resist a non-adaptive iterated distinguisher of order d.

In our counterexample, we distinguish C for $\kappa = 2d-1$. We show that C is not resistant to our non-adaptive iterated distinguisher of order d while $\|[C]^{2d-1} - [C^*]^{2d-1}\|_A \leq 2(2d-1)^2/q$. First of all, we start with explaining the input distribution that adversary uses. Let $(x_1, x_2, \ldots, x_d)$ be the input tuple and $(y_1, y_2, \ldots, y_d)$ be the output tuple such that $C(x_i) = y_i$, where $1 \leq i \leq d$. We will pick plaintexts with specific properties. Every plaintext x_i can be written as $x_i = x_i^L \| x_i^R$, where x_i^L and x_i^R, both in $\mathsf{GF}(q)$, are left and right halves of x_i. For each i, we let $x_i^R = 0$, i.e., $x_i = x_i^L \| 0$. Moreover, we choose a random c_1 and plaintexts $(x_1^L, x_2^L, \ldots, x_d^L)$ satisfying $\prod_{i=1}^d x_i^L = c_0$ and

$$\sum_{i_1 \leq d} x_{i_1}^L = c_{d-1}, \sum_{i_1 < i_2 \leq d} x_{i_1}^L x_{i_2}^L = c_{d-2}, \ldots, \sum_{i_1 < \cdots < i_{d-1} \leq d} x_{i_1}^L x_{i_2}^L \cdots x_{i_{d-1}}^L = c_1,$$

where all c_i's, except c_1, are previously chosen constants and x_i^L's are pairwise distinct. The left half is chosen by the algorithm is Fig. 3.

Given d and $c_0, c_2, \ldots, c_{d-1} \in \mathsf{GF}(q)$, this algorithm first constructs $h(x)$, where $h(x) = x^d - c_{d-1}x^{d-1} + \cdots + (-1)^{d-2}c_2x^2 + (-1)^d c_0$. It picks a random c_1 from $\mathsf{GF}(q)$ to construct $g(x)$ which is defined as $g(x) = h(x) + (-1)^{d-1}c_1 x$. It checks if $g(x)$ divides $x^q - x$ in order to be sure that all roots are in $\mathsf{GF}(q)$. Afterwards, it verifies that all roots are distinct. For this reason, it verifies that $g(x)$ and its derivative $g'(x)$ have no common divisors. Once these two conditions are satisfied, the algorithm outputs the roots of the polynomial g and gets the desired plaintext tuple.

The number of iterations in the algorithm to get the desired plaintext tuple is approximately $q^d/\binom{q}{d} \leq d!$, that is, one over the probability that a random monic polynomial of degree d has d distinct roots in $\mathsf{GF}(q)$. To be more precise, since there are q possible irreducible factors of degree 1 in $\mathsf{GF}(q)[x]$, we compute their d possible combinations in $\binom{q}{d}$ ways to construct polynomials of degree d and we divide it by the number of total monic polynomials of degree d which is q^d.

```
Input: $d, c_0, c_2, \ldots, c_{d-1}$, $q$
Output: $(x_1, \ldots, x_d)$
construct $h(x) = x^d - c_{d-1}x^{d-1} + \cdots + (-1)^{d-2}c_2x^2 + (-1)^d c_0$
repeat
    pick $c_1 \in \mathsf{GF}(q)$ at random and construct $g(x) = h(x) + (-1)^{d-1}c_1 x$
until $x^q \equiv x \mod g(x)$ and $\mathsf{gcd}(g(x), g'(x)) = 1$
find the roots $(x_1, \ldots, x_d)$ of $g(x)$ by using a factorization algorithm for polynomials
return $(x_1, \ldots, x_d)$
```

Fig. 3. The algorithm to generate the left half of the plaintext tuples

Consider the encryption of each round when x_i's are satisfying the above properties. After the first round, we have $0 \| (x_i^L + F_1(0))$. Then, the output of the second round encryption is $(x_i^L + F_1(0)) \| F_2(x_i^L + F_1(0))$. Finally, the corresponding ciphertext y_i will be $y_i = y_i^L \| y_i^R = (F_3(F_2(x_i^L + F_1(0))) + x_i^L + F_1(0)) \| F_2(x_i^L + F_1(0))$. However, we will only be interested in the right part of the ciphertext, i.e., y_i^R, which can be seen as the output of a random polynomial function of degree at most $2d-2$. More explicitly, since $y_i^R = F_2(x_i^L + F_1(0))$, we can write y_i^R as a function of x_i^L such that $F(x_i^L) = F_2(x_i^L + a_0^1)$. Obviously, each coefficient of the polynomial F is a function of coefficients of F_2 and the constant coefficient of F_1, namely $f_i(a_0^1, a_{2d-2}^2, \ldots, a_0^2)$. Since the coefficients of F depend on the coefficients of random functions F_1 and F_2, F is also a random function.

Since we use the input distribution defined above, we can get some fixed bits by interpolating the right part of the output of the cipher, which is exactly the function F mentioned previously. In more detail, in every iteration we interpolate a polynomial r, which will appear in Equation 1. We expect that for the ideal random function F^* the constant coefficient of the polynomial r would be random, but for F it would be fixed. We prove this in Lemma 10. After formally writing this argument, by defining the test function $\mathcal{T}$ and the acceptance set $\mathcal{A}cc$, we can distinguish the cipher from the ideal random cipher with only two iterations.

The distinguisher has d plaintext-ciphertext pairs in each iteration and F is a polynomial. Moreover, we know d points on F and we can use the underdetermined interpolation technique to determine F. We write F such that $F(x) = a_{2d-2}x^{2d-2} + a_{2d-3}x^{2d-3} + \cdots + a_0$ over $\mathsf{GF}(q)$, then we can determine F by

$$F(x) = r(x) + s(x)g(x). \tag{1}$$

Here, r is a unique polynomial of degree at most $d-1$ which interpolates d given points, s is a polynomial of degree at most $d-2$ over $\mathsf{GF}(q)$ and g is a polynomial of degree d with the x_i^L's as its roots $g(x) = (x-x_1^L)\cdots(x-x_d^L)$. Let $r(x) = r_{d-1}x^{d-1}+\cdots+r_0$, $g(x) = x^d - c_{d-1}x^{d-1} + \cdots + (-1)^{d-1}c_1 + (-1)^d c_0$, and $s(x) = s_{d-2}x^{d-2}+\cdots+s_0$, where $r_i, c_j, s_k \in \mathsf{GF}(q)$, $0 \leq i,j \leq d-1$, and $0 \leq k \leq d-2$. We note that $g(x)$ can be written as $g(x) = h(x) + (-1)^{d-1}c_1 x$, where h is a fixed polynomial of degree d with zero coefficient for the term x.

Our aim is to get some fixed bits related to the function F in each iteration to have a distinguisher. The following lemma shows that, when the input distribution is picked as above, the constant coefficient r_0 of polynomial r is fixed in each iteration.

Lemma 10. *Let F be the polynomial of degree at most $2d-2$ over $\mathsf{GF}(q)$ as defined above. Let $x_1^L, \ldots, x_d^L \in \mathsf{GF}(q)$ be the left half of the plaintexts following the distribution above and $F(x_i^L) = y_i^R$, $0 \leq i \leq d$. Then, the constant coefficient r_0 of the polynomial r, which is obtained by the Lagrange interpolation of the given d points, is fixed in each iteration.*

Proof. We write $g(x) = h(x) + (-1)^{d-1}c_1 x$ for $(x_1^L, \ldots, x_d^L)$ and for some $c_1 \in \mathsf{GF}(q)$, where h is a fixed polynomial. Therefore, $F(x) = r(x) + s(x)g(x) = r(x) + s(x)(h(x) + (-1)^{d-1}c_1 x)$ as in Equation 1. Moreover, $F(x) = r'(x) + s'(x)g'(x) = r'(x) + s'(x)(h(x) + (-1)^{d-1}c_1' x)$, for some $c_1' \in \mathsf{GF}(q)$. Hence,

$$\begin{aligned}
&(r(x) + s(x)(h(x) + (-1)^{d-1}c_1 x)) - (r'(x) + s'(x)(h(x) + (-1)^{d-1}c_1' x)) \\
&= \underbrace{r(x) - r'(x) + ((-1)^{d-1}(c_1 s(x) - c_1' s'(x)))x}_{\text{Polynomial 1}} + \underbrace{(s(x) - s'(x))h(x) = 0}_{\text{Polynomial 2}} \\
&\Rightarrow s(x) = s'(x).
\end{aligned}$$

Polynomial 1 has degree at most $d-1$ and Polynomial 2 has at least degree d (the degree of h), unless $s(x) = s'(x)$. Therefore, in order to have zero on the left side of the equation, $s(x) - s'(x)$ has to be zero. This shows that the polynomial s is a fixed polynomial, i.e., independent from the plaintext tuple that is queried. Therefore, we can write F as $F(x) = r(x) + s(x)(h(x) + (-1)^{d-1}c_1 x)$, for fixed polynomials s and h and for some $c_1 \in \mathsf{GF}(q)$. Hence, when $x = 0$, we have $F(0) = r(0) + s(0)h(0)$ which implies that $r_0 = a_0 - s_0 h_0$ is always fixed. □

We can now deduce that r_0 is always fixed and independent from the plaintext tuple due to the choice of plaintext tuple.

Now, we use Lemma 10 to construct a distinguisher between C and C^*. We denote the derived value of r_0 as a function $f((x_1, \ldots, x_d), (y_1, \ldots, y_d))$. Let D be a subset of distinguished values of $\mathsf{GF}(q)$ with a given cardinality q/μ, where $\mu > 1$ is a positive divisor of q. Define the test function as

$$\mathcal{T}((x_1, \ldots, x_d), (y_1, \ldots, y_d)) = \begin{cases} 1, & \text{if } f((x_1, \ldots, x_d), (y_1, \ldots, y_d)) \in D, \\ 0, & \text{otherwise,} \end{cases}$$

and the acceptance set as

$$\mathcal{A}cc[t_1, \ldots, t_n] = \begin{cases} 1, & \text{if } (t_1, \ldots, t_n) \neq (0, \ldots, 0), \\ 0, & \text{otherwise.} \end{cases}$$

All iterations will reply the same answer for the function F and a random answer for F^*. Let p (resp. p^*) be the probability that the distinguisher outputs 1 when it is fed with F (resp. F^*). Hence, according to the acceptance set defined above, we get $p = \frac{1}{\mu}$ and $p^* = 1 - (1 - \frac{1}{\mu})^n$. If we consider $n = 2$, two iterations only, then the advantage of the distinguisher will be $|p - p^*| = |\frac{1}{\mu} - (1 - (1 - \frac{1}{\mu})^2)| = \frac{1}{\mu}(1 - \frac{1}{\mu})$ which is high. By this way, we can distinguish the cipher C from the ideal random cipher C^* by distinguishing the function F defining the right part of the output of the cipher C from the ideal random function F^*.

3.2 Assuming a Low δ is NECESSARY

Theorem 1 shows that if a cipher is decorrelated to the order $2d$, then it resists to an iterated attack of order d. Moreover, it is speculated that a high probability δ of having a common query does not provide any advantage to the adversary. However, we give a counterintuitive example showing that there is an iterated distinguisher of order 1 on a $2d$-decorrelated cipher when the probability of having at least one query in common in any two iterations is high. This shows that Theorem 1 is not universal and has a limit since δ may increase the bound of the distinguisher.

In our distinguisher, we use C depicted in Fig. 2 for $\kappa = 2d$ and $q = 2^k$. Note that Theorem 7 implies that $\|[C]^{2d} - [C^*]^{2d}\|_A \le 8d^2/2^k$. We are going to prove that the random cipher C defined above is not resisting the iterated attack of order 1 when the set of plaintexts of adversary's choice is small. Let S be a set of plaintexts $S = \{x_1, x_2, \ldots, x_{2d+2}\}$, where $x_i = x_i^L \| x_i^R$, x_L and x_R are left and right halves of x_i, respectively. These sets of plaintexts satisfy $x_i^R = 0$ and $\sum_{i=1}^{2d+2} \left(x_i^L\right)^j = 0$, $1 \le j \le 2d-1$ and all x_i^L's are pairwise distinct elements of $\mathsf{GF}(2^k)$. The algorithm to generate the left part of the plaintexts in S is provided in Fig. 4.

This algorithm finds $p(x) = x^{2d+2} + ax^2 + bx + c$ with distinct roots in $\mathsf{GF}(2^k)$, where $a, b, c \in \mathsf{GF}(2^k)$. Note that $p(x)$ has roots of the form $\sum_{i=1}^{2d+2} \left(x_i^L\right)^j = 0$, $1 \le j \le 2d-1$. This is proved in Appendix B for the case $n = 2d+2$. The expected number of iterations in the algorithm can be computed heuristically as $2^{k(2d+2)}/\binom{2^k}{2d+2} \le (2d+2)!$, that is, one over the probability that a random monic polynomial of degree $2d+2$ has $2d+2$ distinct roots in $\mathsf{GF}(2^k)$. Since there are 2^k possible irreducible factors of degree 1 in $\mathsf{GF}(2^k)[x]$, we compute their $2d+2$ possible combinations $\binom{2^k}{2d+2}$ to construct polynomials of degree $2d+2$ and we divide it by the total number of monic polynomials of degree $2d+2$ which is $2^{k(2d+2)}$. In each iteration, we pick one element of S at random. Since the adversary's choice of input set has $2d+2$ elements, we have $\delta = 1/(2d+2)$.

```
Input: $k$, $d$
Output: $(x_1, \ldots, x_{2d+2})$
repeat
    pick $a, b, c \in \mathsf{GF}(2^k)$ at random and construct $p(x) = x^{2d+2} + ax^2 + bx + c$
until $x^{2^k} \equiv x \mod p(x)$ and $\mathsf{gcd}(p(x), p'(x)) = 1$
find the roots $(x_1, \ldots, x_{2d+2})$ of $p(x)$ by using a factorization algorithm for polynomials
return $(x_1, \ldots, x_{2d+2})$
```

Fig. 4. The algorithm to generate the left half of the plaintexts in S

Like in the first counterexample, in order to distinguish this cipher C from the ideal random cipher C^*, we are going to take advantage of the right half of the output of the cipher. For this, at first we will show how to define the right part of the cipher to be a random function. When plaintexts x_i's are satisfying the above properties, we have $y_i = y_i^L \| y_i^R =$

$(F_3(F_2(x_i^L + F_1(0))) + x_i^L + F_1(0)) \| F_2(x_i^L + F_1(0)))$. We only use the right part of the ciphertext which can be seen as an output of a random polynomial of degree at most $2d-1$. In detail, since $y_i^R = F_2(x_i^L + F_1(0))$, y_i^R can be written as a function of x_i^L such that $F(x_i^L) = F_2(x_i^L + a_0^1)$. Obviously, each coefficient of the polynomial function F is a function of the coefficients of F_2 and the constant coefficient of F_1, namely $f(a_0^1, a_{2d-1}^2, \ldots, a_0^2)$. The fact that the coefficients of F are depending on the coefficients of random functions implies that F is also a random function. We then denote the function F as $F(x) = a_{2d-1}x^{2d-1} + a_{2d-2}x^{2d-2} + \cdots + a_0$ over $\mathsf{GF}(q)$.

The trick is that we distinguish the right half of the output of C which is in fact the polynomial F mentioned above. To explain how the distinguisher works briefly, when we consider that the plaintext space has the special form mentioned before, the right half of the cipher C which defines a polynomial F can be distinguished by using the trace. This is because, by the following Lemma, the sum of the trace of all elements in the set S behaves differently in this polynomial function F than in the ideal random function F^* allowing us to distinguish C from C^*. Now, we will propose this distinguishing property of the polynomial function F.

Lemma 11. *Let F be a random function and S be the input set defined as above. For $x_i = x_i^L \| 0 \in S$, $1 \le i \le 2d+2$, we have $\sum_{i=1}^{2d+2} \mathsf{Tr}(F(x_i^L)) = 0$.*

Proof. Since $\sum_{i=1}^{2d+2} (x_i^L)^j = 0$, $1 \le j \le 2d-1$, we have

$$\sum_{i=1}^{2d+2} \mathsf{Tr}(F(x_i^L)) = \sum_{i=1}^{2d+2} \mathsf{Tr}(a_{2d-1}(x_i^L)^{2d-1} + a_{2d-2}(x_i^L)^{2d-2} + \cdots + a_0) =$$

$$\mathsf{Tr}\Big(a_{2d-1}\sum_{i=1}^{2d+2}(x_i^L)^{2d-1}\Big) + \mathsf{Tr}\Big(a_{2d-2}\sum_{i=1}^{2d+2}(x_i^L)^{2d-2}\Big) + \cdots + \mathsf{Tr}\Big(a_0\sum_{i=1}^{2d+2}(x_i^L)^0\Big).$$

Which is equal to 0 due the linearity of trace, the characteristic of this field being 2, and $\mathsf{Tr}(0) = 0$. □

We emphasize that Lemma 11 implies that there is an *even* number of $F(x_i^L)$'s which have $\mathsf{Tr}(F(x_i^L)) = 1$ since $\sum_{i=1}^{2d+2} \mathsf{Tr}(F(x_i^L)) = 0$. We use this property of F to distinguish the cipher C from the ideal random cipher C^*. In fact, like in the first counterexample, we distinguish the function F which is equivalent to distinguishing C.

Now, we explicitly explain how the iterated distinguisher of order 1 with n iterations works, where the input is distributed independently and identically over the set S. We us the property of the polynomial function F which is stated in Lemma 11 in a way that in each iteration, we pick a plaintext x from S at random and compute the trace of $F(x^L)$, i.e., $t = \mathsf{Tr}(F(x^L))$ since $F(x^L) = y^R$. Then, we compute the average $\bar{T} = \frac{1}{n}(t_1 + \cdots + t_n)$, where t_i is the output of iteration i. We decide whether the oracle implements F (equivalently C) or F^* (equivalently C^*) by simply checking that the average value $\bar{T}$ is in the specified set K which is determined according to the expected values of both $\bar{T}$ and $\bar{T}^*$.

Lemma 12. *Assume that the plaintext set S has the above property. Then, depending on S, the expected value of $\bar{T}$ takes any value from the set $S_1 = \{2m/(2d+2) |\ 0 \leq m \leq d+1\}$, and the expected value of $\bar{T}^*$ takes any value from the set $S_2 = \{m/(2d+2) | 0 \leq m \leq 2d+2\}$.*

Proof. Assume that there are $2m$ number of x_i's in S such that $F(x_i^L)$'s have $\mathsf{Tr}(F(x_i^L)) = 1$ (from Lemma 11). Then, the number of x_i's satisfying $\mathsf{Tr}(F(x_i^L)) = 1$ in n iterations is expected to be $n(2m)/(2d+2)$, where $0 \leq m \leq d+1$. Therefore, the expected value of $\bar{T}$ will be $2m/(2d+2)$, where $0 \leq m \leq d+1$. In a similar way, we can find the expected value of $\mathbb{E}(\bar{T}^*)$ for the ideal random function F^*. □

Now, using Lemma 12, we define the acceptance set as

$$\mathcal{A}cc[t_1, \ldots, t_n] = \begin{cases} 1, & \text{if } \bar{T} \in K = \bigcup_{m=0}^{d+1} \left(\frac{2m}{2d+2} - \varepsilon, \frac{2m}{2d+2} + \varepsilon \right), \\ 0, & \text{otherwise.} \end{cases}$$

Typically, $\varepsilon = 1/(4d+4)$. Let p (resp. p^*) be the probability that the distinguisher outputs 1 when it is fed with F (resp. F^*). The following lemma states the bounds for both p and p^*.

Lemma 13. *We have $p \geq 1 - 2e^{-2n\varepsilon^2}$ and $p^* \leq \frac{1}{2} + e^{-2n\varepsilon^2}$.*

Proof. For the function F, according to the acceptance set defined previously, p is expressed by $p = \sum_{x \in S_1} \Pr[\mathbb{E}(\bar{T}) = x] \Pr[\bar{T} \in K | \mathbb{E}(\bar{T}) = x]$.

Since $\Pr[\bar{T} \in K | \mathbb{E}(\bar{T}) = x] \geq 1 - 2e^{-2n\varepsilon^2}$ by Hoeffding's bound from Lemma 9, we have $p \geq 1 - 2e^{-2n\varepsilon^2}$. Similarly, p^* is computed as $p^* = \sum_{x \in S_2} \Pr[\mathbb{E}(\bar{T}^*) = x] \Pr[\bar{T}^* \in K | \mathbb{E}(\bar{T}^*) = x]$. The computation of p^* is not straightforward, hence, we first compute the probability that each expected value of $\bar{T}^*$ from S_2 occurs with probability $\Pr[\mathbb{E}(\bar{T}^*) = x] = \binom{2d+2}{x(2d+2)} 2^{-(2d+2)}$. In detail, we are picking $x(2d+2)$ places for 1's among $2d+2$ possible places and dividing the total number of possible choices which is 2^{2d+2}. Furthermore, the probabilities $\Pr[\bar{T}^* \in K | \mathbb{E}(\bar{T}^*) = x]$ are different according to the expected value of different $\bar{T}^*$. More explicitly, when $\mathbb{E}(\bar{T}^*) = 2m/(2d+2)$ for $0 \leq m \leq d+1$, we have $\Pr[\bar{T}^* \in K | \mathbb{E}(\bar{T}^*) =$

$x] \leq 1$. Similarly, when $\mathbb{E}(\bar{T}^*) = (2m'+1)/(2d+2)$, $0 \leq m' \leq d$, we get $\Pr[\bar{T}^* \in K | \mathbb{E}(\bar{T}^*) = x] \leq 2e^{-2n\varepsilon^2}$ by Hoeffding's bound (Lemma 9). Then, p^* can be computed as

$$\begin{aligned}
p^* = & \sum_{x \in \{2m/(2d+2) | 0 \leq m \leq d+1\}} \Pr[\mathbb{E}(\bar{T}^*) = x] \Pr[\bar{T}^* \in K | \mathbb{E}(\bar{T}^*) = x] \\
& + \sum_{x \in \{(2m'+1)/(2d+2) | 0 \leq m' \leq d\}} \Pr[\mathbb{E}(\bar{T}^*) = x] \Pr[\bar{T}^* \in K | \mathbb{E}(\bar{T}^*) = x] \\
& \leq \sum_{x \in \{2m/(2d+2) | 0 \leq m \leq d+1\}} \binom{2d+2}{x(2d+2)} 2^{-(2d+2)} \\
& + \sum_{x \in \{(2m'+1)/(2d+2) | 0 \leq m' \leq d\}} \binom{2d+2}{x(2d+2)} 2^{-(2d+2)} 2e^{-2n\varepsilon^2}.
\end{aligned}$$

Note that the sum of even and odd indices of binomial coefficients are $\sum_{i \geq 0} \binom{n}{2i} = 2^{n-1}$ and $\sum_{i \geq 0} \binom{n}{2i+1} = 2^{n-1}$, respectively. Hence, we have

$$\sum_{x \in \{2m/(2d+2) | 0 \leq m \leq d+1\}} \binom{2d+2}{x(2d+2)} 2^{-(2d+2)} = \frac{1}{2}.$$

Then, we get

$$\sum_{x \in \{(2m'+1)/(2d+2) | 0 \leq m' \leq d\}} \binom{2d+2}{x(2d+2)} 2^{-(2d+2)} 2e^{-2n\varepsilon^2} \leq \frac{1}{2} 2e^{-2n\varepsilon^2} = e^{-2n\varepsilon^2}.$$

Therefore, we get $p^* \leq \frac{1}{2} + e^{-2n\varepsilon^2}$. □

Finally, the advantage of the distinguisher is computed as

$$|p - p^*| \geq \left| \left(1 - 2e^{-2n\varepsilon^2}\right) - \left(\frac{1}{2} + e^{-2n\varepsilon^2}\right) \right| = \left| \frac{1}{2} - 3e^{-2n\varepsilon^2} \right|.$$

When the distinguisher has a large number of iterations, we have $|p - p^*| \approx 1/2$ which is quite high. This way we manage to distinguish the cipher C from the ideal random cipher C^*. Hence, *in specific situations*, having common queries *can* increase the advantage. Essentially, if the images of $2d+2$ points sum to zero, by taking $\varepsilon = 1/(4d+4)$ and $n \approx \Omega(d^2)$ we obtain an efficient iterated distinguisher of order 1. This could be used to transform Integral/Square/Saturation attacks to this kind of distinguisher (with a squared number of inputs).

As a final remark, in Decorrelation Theory, Vaudenay considers block ciphers in the context of deterministic symmetric key encryption. Therefore, for some input distribution, the probability δ that two iterations have at least one query in common can be high. However, if we consider symmetric-key probabilistic encryption, then δ will always be small. This is because, in this scheme, the oracle picks the random coins, and even if the same plaintext is picked by the adversary, the random coins picked by the oracle for two plaintexts would be different which causes two different inputs to the encryption. This implies that high δ is not a threat when we consider the probabilistic encryption.

4 Conclusion and Future Work

We settled an open problem and disproved a claim, both of which are raised by the EUROCRYPT '99 work of Vaudenay in Decorrelation Theory. In particular, we proved that in order for a cipher C to resist a non-adaptive iterated attack of order d, it is not sufficient to have a decorrelation of order $2d-1$. We showed this by providing a cipher decorrelated to the order $2d-1$ and a successful non-adaptive iterated attack against it which has order d. Hence, we concluded that the minimal order of decorrelation to ensure resistance is $2d$. Furthermore, we illustrated that when the probability of having a common query between different iterations increases, the advantage of the distinguisher *can* increase.

Our counterexamples comprise of non-adaptive distinguishers. One could also investigate whether or not a similar result holds for the case of adaptive adversaries. Moreover, the adversaries we consider make plaintext queries and receive the corresponding ciphertexts. A different adversarial model can also be considered where the adversary can make ciphertext queries together with plaintext queries.

References

[AGM02] Noga Alon, Oded Goldreich, and Yishay Mansour. Almost k-wise independence versus k-wise independence. *Electronic Colloquium on Computational Complexity (ECCC)*, 9(048), 2002.

[BF06a] Thomas Baignères and Matthieu Finiasz. Dial C for Cipher. In Eli Biham and Amr M. Youssef, editors, *Selected Areas in Cryptography*, volume 4356 of *Lecture Notes in Computer Science*, pages 76–95. Springer, 2006.

[BF06b] Thomas Baignères and Matthieu Finiasz. KFC - The Krazy Feistel Cipher. In Xuejia Lai and Kefei Chen, editors, *ASIACRYPT*, volume 4284 of *Lecture Notes in Computer Science*. Springer, 2006.

[BV05] Thomas Baignères and Serge Vaudenay. Proving the Security of AES Substitution-Permutation Network. In Bart Preneel and Stafford E. Tavares, editors, *Selected Areas in Cryptography*, volume 3897 of *Lecture Notes in Computer Science*, pages 65–81. Springer, 2005.

[CV94] Florent Chabaud and Serge Vaudenay. Links Between Differential and Linear Cryptoanalysis. In Alfredo De Santis, editor, *EUROCRYPT*, volume 950 of *Lecture Notes in Computer Science*, pages 356–365. Springer, 1994.

[CW79] Larry Carter and Mark N. Wegman. Universal Classes of Hash Functions. *Journal of Computer and System Sciences*, 18(2):143–154, 1979.

[CW81] Larry Carter and Mark N. Wegman. New Hash Functions and Their Use in Authentication and Set Equality. *Journal of Computer and System Sciences*, 22(3):265–279, 1981.

[Hoe62] Wassily Hoeffding. Probability Inequalities For Sums Of Bounded Random Variables, 1962.

[LR85] Michael Luby and Charles Rackoff. How to Construct Pseudo-Random Permutations from Pseudo-Random Functions (Abstract). In Hugh C. Williams, editor, *CRYPTO*, volume 218 of *Lecture Notes in Computer Science*, page 447. Springer, 1985.

[LR86] Michael Luby and Charles Rackoff. Pseudo-random Permutation Generators and Cryptographic Composition. In Juris Hartmanis, editor, *STOC*, pages 356–363. ACM, 1986.

[Lub86] Michael Luby. A Simple Parallel Alogarithm for the Maxial Independent Set Problem. *SIAM J. Comput.*, 15(4):1036–1053, 1986.

[NN90] Joseph Naor and Moni Naor. Small-bias probability spaces: Efficient constructions and applications. In Harriet Ortiz, editor, *STOC*, pages 213–223. ACM, 1990.

[Nyb91] Kaisa Nyberg. Perfect Nonlinear S-Boxes. In Donald W. Davies, editor, *EUROCRYPT*, volume 547 of *Lecture Notes in Computer Science*, pages 378–386. Springer, 1991.

[PV98] Guillaume Poupard and Serge Vaudenay. Decorrelated Fast Cipher: An AES Candidate Well Suited for Low Cost Smart Card applications. In Jean-Jacques Quisquater and Bruce Schneier, editors, *CARDIS*, volume 1820 of *Lecture Notes in Computer Science*, pages 254–264. Springer, 1998.

[Vau98a] Serge Vaudenay. Feistel Ciphers with L_2-Decorrelation. In Stafford E. Tavares and Henk Meijer, editors, *Selected Areas in Cryptography*, volume 1556 of *Lecture Notes in Computer Science*, pages 1–14. Springer, 1998.

[Vau98b] Serge Vaudenay. Provable Security for Block Ciphers by Decorrelation. In Michel Morvan, Christoph Meinel, and Daniel Krob, editors, *STACS*, volume 1373 of *Lecture Notes in Computer Science*, pages 249–275. Springer, 1998.

[Vau99a] Serge Vaudenay. On Probable Security for Conventional Cryptography. In JooSeok Song, editor, *ICISC*, volume 1787 of *Lecture Notes in Computer Science*, pages 1–16. Springer, 1999.

[Vau99b] Serge Vaudenay. Resistance Against General Iterated Attacks. In Jacques Stern, editor, *EUROCRYPT*, volume 1592 of *Lecture Notes in Computer Science*, pages 255–271. Springer, 1999.

[Vau00] Serge Vaudenay. Adaptive-Attack Norm for Decorrelation and Super-Pseudorandomness. In Howard M. Heys and Carlisle M. Adams, editors, *Selected Areas in Cryptography*, volume 1758 of *Lecture Notes in Computer Science*, pages 49–61. Springer, 2000.

[Vau03] Serge Vaudenay. Decorrelation: A Theory for Block Cipher Security. *J. Cryptology*, 16(4):249–286, 2003.

A The Proof of Theorem 6

This proof is exactly the same as the proof of Theorem 1 [Vau03] except for the computation of $V(T(F^*))$ which results in a tighter bound for the distinguisher. Given $F = f$ (resp. $F^* = f$), let $T(f)$ be the probability that test function $\mathcal{T}$ outputs 1 when $(X, f(X))$ is its input, i.e., $T(f) = \mathbb{E}_X(\mathcal{T}(X, f(X)))$. Let p (resp. p^*) be the probability that the distinguisher outputs 1, i.e., $p = \mathsf{Pr}_F[(T_1(F), \ldots, T_n(F)) \in \mathcal{A}cc]$, where $\mathcal{A}cc$ is the acceptance set and $T_i(F)$ (resp. $T_i(F^*)$) is the output of iteration i.

Since $T_i(F)$'s are all independent with the same expected value $T(F)$ which only depends on F, we get

$$p = \mathbb{E}_F\left(\sum_{(t_1,\ldots,t_n)\in\mathcal{A}cc} T(F)^{t_1+\cdots+t_n}(1-T(F))^{n-(t_1+\cdots+t_n)}\right).$$

Then, p can be rewritten as $p = \sum_{i=0}^{n} a_i \mathbb{E}_F(T(F)^i(1-T(F))^{n-i})$ for some integers a_i such that $0 \le a_i \le \binom{n}{i}$. Therefore, the advantage $|p - p^*|$ is maximal when all a_i's are either 0 or $\binom{n}{i}$ depending on the distributions $T(F)$ and $T(F^*)$. This implies that the acceptance set of the best distinguisher is of the form $\mathcal{A}cc = \{(t_1, \ldots, t_n) | \sum_{i=1}^{n} t_i \in \mathcal{B}\}$ for some set $\mathcal{B} \subseteq \{0, \ldots, n\}$. Therefore, we have $p = \mathbb{E}_F(s(T(F)))$ where $s(x) = \sum_{x\in\mathcal{B}} \binom{n}{i} x^i(1-x)^{n-i}$.

Recall that $|s(T(F)) - s(T(F^*))| \le 2n|T(F) - T(F^*)|$. In addition, we have $|\mathbb{E}_F(T(F)) - \mathbb{E}_{F^*}(T(F^*))| \le \varepsilon/2$, $|\mathbb{E}_F(T^2(F)) - \mathbb{E}_{F^*}(T^2(F^*))| \le \varepsilon/2$ and $|V(T(F)) - V(T(F^*))| \le 3\varepsilon/2$. Then, the advantage of the distinguisher is $|p - p^*| = |\mathbb{E}(T(F)) - \mathbb{E}(T(F^*))| \le \mathbb{E}(|T(F) - T(F^*)|)$. By applying Tchebichev's inequality for both $T(F)$ and $T(F^*)$ which is $\Pr[|T(F) - \mathbb{E}(T(F))| > \lambda] \le V(T(F))/\lambda^2$ for any $\lambda > 0$ (same for $T(F^*)$), we get

$$|p - p^*| \le 5\Big(\big(2V(T(F^*)) + \frac{3\varepsilon}{2}\big)n^2\Big)^{\frac{1}{3}} + n\varepsilon, \tag{2}$$

when $\lambda = \left(\frac{2V(T(F^*)) + \frac{3\epsilon}{2}}{n}\right)^{\frac{1}{3}}$. Up to this point, the proof was the same with the proof of Theorem 1. However, the bound for $V(T(F^*))$ is different from the bound for $V(T(C^*))$, where C^* is the ideal random cipher. We get $V(T(F^*))$ to be equal to $\sum_{(x,y),(x',y')\in\mathcal{T}} \Pr[X = x] \Pr[X = x']\Big(\Pr_{F^*}[(x,x') \xrightarrow{F^*} (y,y')] - \Pr_{F^*}[x \xrightarrow{F^*} y] \Pr_{F^*}[x' \xrightarrow{F^*} y']\Big)$.

In order to bound this sum, we divide pairs (x, x') into two groups of pairs such that the first group has no common queries, i.e., $\forall i, j\ x_i \ne x'_j$, but the second one has. As a remark, we assume that the adversary does not pick the same query in a single iteration, i.e., $x_i \neq x_j$, when $i \neq j$. Since all x_i are distinct in $x = (x_1, \dots, x_d)$, then $[F^*]^d_{(x_1,\dots,x_d),(y_1,\dots,y_d)} = \prod_{i=1}^d \Pr[F^*(x_i) = y_i] = N^{-d}$. When inputs x and x' have no common queries, then $[F^*]^{2d}_{(x_1,\dots,x_d,x'_1,\dots,x'_d),(y_1,\dots,y_d,y'_1,\dots,y'_d)} = \prod_{i=1}^d \Pr[F^*(x_i) = y_i] \prod_{i=1}^d \Pr[F^*(x'_i)= y'_i]= N^{-2d}$. Therefore, when input tuples x and x' have no common queries, the sum will be 0. Otherwise, when the plaintext tuples x and x' have common queries with probability δ, then the sum over all these plaintext tuples will be less than δ. Hence, we have $V(T(F^*)) \leq \delta$. When we substitute δ for $V(T(F^*))$ in Inequality 2, we get $|p - p^*| \leq 5\sqrt[3]{\left(2\delta + \frac{3\varepsilon}{2}\right)n^2} + n\varepsilon$.

B A Required Lemma for Subsection 3.2

Lemma 14. *Let f be a polynomial of the form $f(x) = x^n + a_1x^{n-1} + a_2x^{n-1} + \cdots + a_{n-2}x^2 + a_{n-1}x + a_n$ over $\mathsf{GF}(2^k)$ and $x_1, x_2, \dots, x_n$ be its roots. If $a_1 = a_2 = \cdots = a_{n-3} = 0$, then its roots satisfy $s_k = \sum_{i=1}^n x_i^j = 0$, where $1 \leq j \leq n-3$ and $n \geq 4$.*

Proof. First, we recall the *Newton formulas*. Let f be a polynomial of the form $f(x) = x^n + a_1x^{n-1} + a_2x^{n-1} + \cdots + a_{n-2}x^2 + a_{n-1}x + a_n$ with the roots $x_1, x_2, \dots, x_n$ so that $f(x) = (x - x_1)(x - x_2)\cdots(x - x_n)$ over a ring R. Then, we define the elementary symmetric functions of the roots as $\sum_{1\leq i\leq n} x_i = -a_1, \sum_{1\leq i<j\leq n} x_ix_j = a_2, \sum_{1\leq i<j<k\leq n} x_ix_jx_k = -a_3, \dots,$ and $x_1x_2\cdots x_n = (-1)^n a_n$.

In addition, k^{th} power sums of the roots is defined as $s_k = \sum_{1\leq i\leq n} x_i^k$. Then, *Newton formulas* give recursion relations between a_i's and s_i's as $s_1 + a_1 = 0, s_2 + a_1s_1 + 2a_2 = 0, \dots, s_n + a_1s_{n-1} + a_2s_{n-2} + \cdots + na_n = 0, s_{n+1} + a_1s_{n-1} + a_2s_{n-2} + \cdots + s_1a_n = 0$.

Note that Newton formulas are valid over finite fields. Now, if we assume that $a_1 = a_2 = \cdots = a_{n-3} = 0$, then according to the Newton formulas given above we will show that $s_k = 0$ for $1 \leq k \leq n-3$. Since $s_1 + a_1 = 0$ and $a_1 = 0$, we have $s_1 = 0$. By induction, assume that $s_1 = s_2 = \cdots = s_{k-1} = 0$ and $a_1 = a_2 = \cdots = a_k = 0$, then we have $s_k = -(a_1s_{k-1} + a_2s_{k-2} + \cdots + ka_k) = 0$. Therefore, the polynomial $f(x) = x^n + a_{n-2}x^2 + a_{n-1}x + a_n$ satisfies $s_k = \sum_{i=1}^n x_i^j = 0$, where $1 \leq j \leq n-3$ and $n \geq 4$. □