XOR of PRPs in a Quantum World

Bart Mennink[1,2](✉) and Alan Szepieniec[3]

[1] Digital Security Group, Radboud University, Nijmegen, The Netherlands
b.mennink@cs.ru.nl
[2] CWI, Amsterdam, The Netherlands
[3] imec-COSIC KU Leuven, Leuven, Belgium
alan.szepieniec@esat.kuleuven.be

Abstract. In the classical world, the XOR of pseudorandom permutations $E_{k_1} \oplus \cdots \oplus E_{k_r}$ for $r \geq 2$ is a well-established way to design a pseudorandom function with "optimal" security: security up to approximately $\min\{|K|, |X|\}$ queries, where K and X are the key and state space of the block cipher E. We investigate security of this construction against adversaries who have access to quantum computers. We first present a key recovery attack in $|K|^{r/(r+1)}$ complexity. The attack relies on a clever application of a claw-finding algorithm and testifies of a significant gap with the classical setting where 2 pseudorandom permutations already yield optimal security. Next, we perform a quantum security analysis of the construction, and prove that it achieves security up to $\min\{|K|^{1/2}/r, |X|\}$ queries. The analysis relies on a generic characterization of classical and quantum distinguishers and a universal transformation of classical security proofs to the quantum setting that is of general interest.

Keywords: XOR of pseudorandom permutations · Classical · Quantum · Claw-finding · Proof transformation

1 Introduction

PRP to PRF Conversion. Block ciphers are omnipresent in cryptographic literature, and their security is usually measured in the degree to which they approximate a pseudorandom permutation (PRP). However, in many cases, one prefers to reason with pseudorandom functions instead. A simple example of this is the counter mode encryption. Using a block cipher $E : K \times X \to X$, counter mode encrypts a message $M = M_1 \cdots M_\ell \in X^\ell$ as

$$C_i = E_k(\text{ctr} + i) \oplus M_i \text{ for } i = 1, \ldots, \ell, \tag{1}$$

for a carefully selected counter ctr. If E_k behaves like a random permutation, it is straightforward to observe a bias: an adversary that keeps all message blocks the same will never see colliding ciphertext blocks. However, if we consider E_k to behave like a random function, the ciphertext will always be perfectly random,

T. Lange and T. Takagi (Eds.): PQCrypto 2017, LNCS 10346, pp. 367–383, 2017.
DOI: 10.1007/978-3-319-59879-6_21

and distinguishing counter mode from random reduces to distinguishing E_k from a random function. The trick to view a PRP as a PRF is called the "PRP-PRF-switch," and it finds myriad applications in existing symmetric key security proofs (e.g., [3,10,18,22,26,36,40,41,46]).

The PRP-PRF-switch only guarantees tight birthday bound security: security up to $\min\{|K|, |X|^{1/2}\}$ queries [7,8,20,23]. The same bound applies to counter mode. Suppose we *replace* E_k with $E_{k_1} \oplus E_{k_2}$ for two secret keys k_1, k_2 (this is in fact a simplified case of the CENC mode by Iwata [24,25]):

$$C_i = E_{k_1}(\text{ctr} + i) \oplus E_{k_2}(\text{ctr} + i) \oplus M_i \text{ for } i = 1, \ldots, \ell. \quad (2)$$

In a steady line of research set out in '99 [6,16,33,39,43,44],[1] Patarin finally proved in 2010 [44] that $E_{k_1} \oplus E_{k_2}$ behaves like a random function up to query complexity $\min\{|K|, |X|\}$, well beyond the classical $\min\{|K|, |X|^{1/2}\}$ birthday level of the PRP-PRF-switch. This result almost immediately implies security up to about $\min\{|K|, |X|\}$ queries for this case of CENC, and more generally demonstrates well the relevance of beyond birthday level security of the PRP to PRF conversion.

Quantum Security. Computers exploiting the physical properties of quantum particles seem to promise dramatic speedups for certain problems. The growing branch of *post-quantum cryptography* [9] focuses chiefly on public key cryptosystems and aims to offer immunity to Shor's quantum algorithm for integer factorization and discrete logarithms [50]. Within this branch it is tacitly assumed that symmetric cryptographic primitives remain largely unaffected by the advent of quantum computers: a doubling of the key length will suffice to protect against Grover's search algorithm [19]. Among other things we show that this tacit assumption is false: it is possible to outperform Grover in certain circumstances even without achieving the exponential speedup promised by Shor.

For modes that operate *on top of* symmetric cryptographic primitives, various attacks have been mounted recently [2,28,30,31], but all explicitly require the attack *and the cryptographic algorithm itself* to be run on a quantum computer. In our estimation this model is uninteresting because it requires sophisticated users in order to be relevant; as opposed to offering simple users protection against sophisticated attacks.

The current reality is that secret keys are stored in classical hardware and are hence incapable of sustaining quantum superposition or entanglement. Consequently, while the attacker may have classical query access to keyed primitives, there can be *no quantum interaction with secret key material.* Nevertheless, the attacker *is* allowed to evaluate offline and in quantum superposition any publicly known circuit, such as block ciphers—as long as it provides its own guess, in superposition or not, at the secret key.

[1] This list omits research on the XOR of *public* permutations [37,39].

PRP-PRF-Conversion in Quantum Computers. Recently, Zhandry [54] considered the PRP-PRF-switch in case the adversary has quantum access to the secret key material, and he proves tight $|X|^{1/3}$ security. His analysis builds upon two of his earlier observations from [53]. Zhandry likewise considered transitions from QPRGs to QPRFs in [53] and QPRPFs to QPRPs [55]. To our knowledge, this work is the first to generically study the XOR of multiple PRPs in a quantum setting, online *or* offline.

We first present a quantum key recovery attack against the XOR of r PRPs in $|K|^{r/(r+1)}$ complexity. This attack is performed *without* quantum interaction with secret key material, and as such, it stands in sharp contrast with the state of the art in the classical world where optimal $\min\{|K|, |X|\}$ security is achieved already for $r = 2$. The attack internally runs the quantum claw-finding algorithm of Tani [52] in a sophisticated way to recover the key of the r PRPs.[2] In order to eliminate false positives, the algorithm incorporates a threshold τ. We prove that, if the PRPs are perfect permutations, for $\tau = O(r)$ the number of false positives is 0 with high probability. In case the PRP is instantiated with an off-the-shelf block cipher (such as AES), a slightly higher threshold may be required.

As a second contribution, we present a quantum security analysis of the XOR of r PRPs, and prove that the construction achieves security up to around $\min\{|K|^{1/2}/r, |X|\}$ queries by a quantum distinguisher with only classical access to the keyed primitives. At the core of the security proof lies a fresh perspective on (i) how to formalize classical and quantum distinguishers, (ii) how classical proofs compare with quantum proofs, and (iii) how classical proofs can be *used* in a quantum setting. The observations show particularly that a large part of classical security reductionist proofs can be lifted to the quantum setting almost verbatim: for our result on the XOR of PRPs we immediately rely on a classical security proof by Patarin [43,44], but the techniques carry over to a broader spectrum of existing security proofs. For example, the techniques can be used *in turn* to argue quantum security of counter mode of Eq. (1), CENC of Eq. (2), and many more schemes whose security analysis is in the standard model [1,4,5,18, 22,26,29,32,34,41,46,47,49].[3] We remark that Hallgren et al. [21] and Song [51] already considered how to lift classical security proofs to the quantum world. However, their focus was on adversaries with quantum interaction to the secret key material, making the conditions stricter and the lifting harder to verify. We focus on the setting where the secret key material is stored in classical hardware, and our lifting conditions are easily verified.

Admittedly, the gap between our attack and our security bound is not tight. Informally, this gap is caused by a specific step in the analysis that upper bounds the success probability of guessing the secrets key of the r PRPs by r times the

[2] An earlier, yet unrelated and less profound, application of claw finding to cascaded encryption appeared by Kaplan [27].

[3] The lifting does not apply to ideal-model proofs, such as the ones used for sponge functions [3,40], Even-Mansour constructions [11,14], and some tweakable block cipher designs [17,38], which is because in ideal-model proofs the adversary has quantum query access to idealized primitives.

success probability of guessing one of the keys (the step is in fact more technical, cf., Eq. (13) in the proof of Theorem 2). While this step is conventional in classical security proofs as it gives a fairly insignificant loss; for distinguishers that can make quantum evaluations the loss is more severe. In Sect. 6 we discuss various paths towards potentially resolving this step.

2 Preliminaries

For two sets X, Y, by $\mathsf{Func}(X, Y)$ we denote the set of all functions from X to Y and by $\mathsf{Perm}(X)$ the set of all permutations on X. We denote by $x \xleftarrow{\$} X$ the uniformly random drawing of an element x from X. For a positive natural number $r \geq 1$, $\binom{X}{r}$ denotes the set of unordered subsets of X of size r with no duplicates. For two bit strings x and y of equal length, $x \oplus y$ denotes their bitwise exclusive OR (XOR). For two integers $m \geq n \geq 1$, we denote by $m^{\underline{n}} = m(m-1)\cdots(m-n+1) = \frac{m!}{(m-n)!}$ the falling factorial power.

2.1 Security Notions

PRP Security. A block cipher $E : K \times X \to X$ is a family of permutations $E(k, \cdot)$ indexed by a key $k \in K$. Its security is measured by considering a distinguisher $\mathcal{D}$ that has forward query access to either $E_k(\cdot) := E(k, \cdot)$ for a randomly drawn key $k \xleftarrow{\$} K$, or to a random permutation $\pi \xleftarrow{\$} \mathsf{Perm}(X)$. Its goal is to distinguish both worlds, and after its interaction it outputs 0 or 1, referring to the guessed oracle.

Definition 1 (PRP Security). *Let $E : K \times X \to X$ be a block cipher. The PRP (pseudorandom permutation) advantage of a distinguisher $\mathcal{D}$ is defined as*

$$\mathsf{Adv}_E^{\mathrm{prp}}(\mathcal{D}) = \left|\mathbf{P}\left(\mathcal{D}^{E_k} = 1\right) - \mathbf{P}\left(\mathcal{D}^{\pi} = 1\right)\right|,$$

where the probabilities are taken over $k \xleftarrow{\$} K$, $\pi \xleftarrow{\$} \mathsf{Perm}(X)$, and the randomness of $\mathcal{D}$.

For a set of distinguishers $\mathbb{D}$, we define

$$\mathsf{Adv}_E^{\mathrm{prp}}(\mathbb{D}) = \sup_{\mathcal{D} \in \mathbb{D}} \mathsf{Adv}_E^{\mathrm{prp}}(\mathcal{D}).$$

The set of distinguishers $\mathbb{D}$ is typically parameterized by certain complexity parameters, and contains the set of all distinguishers that are bounded by these complexities. In Sect. 3 we elaborate on distinguishers and their complexities.

We remark that block ciphers are often considered in a slightly stronger security model, namely SPRP (strong pseudorandom permutation) security, where the distinguisher can query its oracle in forward as well as in inverse direction. However, for the analysis in this work, SPRP security is inconsequential. We need only consider the weak security notion, PRP security.

PRF Security. Let $F : K \times X \to Y$ be a family of functions $F(k, \cdot)$ from $X \to Y$ indexed by a key $k \in K$. Its security as a family of random functions is defined similarly as the SPRP security, with the difference that distinguisher $\mathcal{D}$ now has oracle access to either $F_k(\cdot) := F(k, \cdot)$ for a randomly drawn key $k \xleftarrow{\$} K$, or to a random function $\rho \xleftarrow{\$} \mathsf{Func}(X, Y)$.

Definition 2 (PRF Security). *Let $F : K \times X \to Y$ be a family of functions. The PRF (pseudorandom function) advantage of a distinguisher $\mathcal{D}$ is defined as*

$$\mathsf{Adv}_F^{\mathrm{prf}}(\mathcal{D}) = \left|\mathbf{P}\left(\mathcal{D}^{F_k} = 1\right) - \mathbf{P}\left(\mathcal{D}^{\rho} = 1\right)\right|,$$

where the probabilities are taken over $k \xleftarrow{\$} K$, $\rho \xleftarrow{\$} \mathsf{Func}(X, Y)$, and the randomness of $\mathcal{D}$.

As before, for a set of distinguishers $\mathbb{D}$, we define

$$\mathsf{Adv}_F^{\mathrm{prf}}(\mathbb{D}) = \sup_{\mathcal{D} \in \mathbb{D}} \mathsf{Adv}_F^{\mathrm{prf}}(\mathcal{D}).$$

We remark that in above definition, the key set can be anything. Typically, K is a set of bit strings, but in this work we will also apply the analysis to the case where K is a set of functions. For example, consider $F : \mathsf{Perm}(X) \times X \to X$, defined as $F(\pi, x) = \pi(x) \oplus x$. This definition of F is a family of functions indexed by "key" π and for every key it represents a Davies-Meyer-like random function. The probabilities in the PRF security advantage are in this case taken over $\pi \xleftarrow{\$} \mathsf{Perm}(X)$ and $\rho \xleftarrow{\$} \mathsf{Func}(X, X)$.

2.2 XOR of PRPs

Let $E : K \times X \to X$ be a block cipher, and let $r \geq 1$ be a positive natural number. The "XOR of r permutations" is the function $F_r : K^r \times X \to X$ defined as

$$F_r(\mathbf{k}, x) = E_{k_1}(x) \oplus \cdots \oplus E_{k_r}(x) =: z, \tag{3}$$

where $\mathbf{k} = (k_1, \ldots, k_r)$. The function F_r is visually depicted in Fig. 1.

The terminology is a bit misleading for $r = 1$ (there is no such thing as the "XOR of 1 permutation"), but we have opted this naming for the sake of generality. The case of $r = 1$ is in fact the "PRP-to-PRF-switch" [7,8,20,23].

2.3 Idealized XOR of PRPs

We also consider an idealized version of F_r that is not based on an underlying block cipher, but is instead keyed via r random permutations. In more detail, for a positive natural number $r \geq 1$ we define $F_r^{\mathrm{id}} : \mathsf{Perm}(X)^r \times X \to X$ as

$$F_r^{\mathrm{id}}(\boldsymbol{\pi}, x) = \pi_1(x) \oplus \cdots \oplus \pi_r(x) =: z, \tag{4}$$

where $\boldsymbol{\pi} = (\pi_1, \ldots, \pi_r)$.

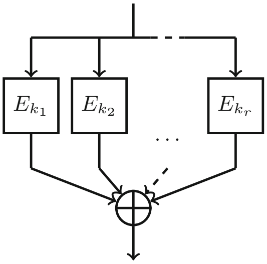

Fig. 1. XOR of r permutations.

2.4 Quantum Claw-Finding

The claw-finding problem centers around the following goal: given two functions $f : X \to Z$ and $g : Y \to Z$, determine whether a tuple $(x, y) \in X \times Y$ such that $f(x) = g(y)$ exists, and find this "claw." Quantum algorithms for solving the claw-problem are usually a function of $M = |X|$ and $N = |Y|$, and we denote the problem by $\mathsf{claw}(M, N)$. We follow the work of Tani [52], that uses quantum walks to solve the problem and that builds upon a list of earlier results on quantum claw-finding [12,13,35,56]. Tani describes an optimal algorithm for discovering a claw in the following number of evaluations of f and g:

$$\mathcal{Q}(\mathsf{claw}(M,N)) = \begin{cases} O\left((M \cdot N)^{1/3}\right) \text{ if } N \le M < N^2, \\ O\left(M^{1/2}\right) \text{ if } M \ge N^2. \end{cases} \tag{5}$$

We remark that Tani [52] derives this algorithm as a special case of a generalized problem that aims at deriving p evaluations of f and q evaluations of g that satisfy a pre-described relation R. More formally, denote by $\mathsf{relation}_{p,q,R}(M, N)$ the problem of discovering a tuple $(x_1, \dots, x_p, y_1, \dots, y_q) \in X^p \times Y^q$ such that $(f(x_1), \dots, f(x_p), g(y_1), \dots, g(y_q)) \in R$.[4] Tani's relation-finding algorithm solves the problem in the following number of evaluations of f and g:

$$\mathcal{Q}(\mathsf{relation}_{p,q,R}(M,N)) = \begin{cases} O\left((M^p \cdot N^q)^{1/(p+q+1)}\right) \text{ if } N \le M < N^{1+1/p}, \\ O\left(M^{p/(p+1)}\right) \text{ if } M \ge N^{1+1/p}. \end{cases} \tag{6}$$

Note that $\mathsf{claw}(M, N)$ is equivalent to $\mathsf{relation}_{1,1,R}(M, N)$ if we define R as the equality relation.

3 Modeling Quantum Distinguishers

Consider a security measurement $\mathsf{Adv}(\cdot)$ (*e.g.*, $\mathsf{Adv}_E^{\mathrm{prp}}(\cdot)$ or $\mathsf{Adv}_F^{\mathrm{prf}}(\cdot)$). For a family of distinguishers $\mathbb{D}$, we define

$$\mathsf{Adv}(\mathbb{D}) = \sup_{\mathcal{D} \in \mathbb{D}} \mathsf{Adv}(\mathcal{D}).$$

[4] Tani [52] uses a slightly different naming: (p, q)-$\mathsf{subset}(M, N)$.

The complexity of a distinguisher is typically bounded in two parameters: data or *online* complexity $q \geq 0$, and time or *offline* complexity $t \geq 0$.[5] Data complexity measures the number of oracle queries the distinguisher can make to its oracle. Time complexity bounds the number of other activities that $\mathcal{D}$ can do, and it can use its time for anything it wants: making coffee, solving sudokus, or, on a more serious note, making evaluations of underlying unkeyed primitives. For example, if we consider the XOR of PRPs of (3) and a distinguisher that tries to separate F_r from a random function ρ in terms of Definition 2, the online complexity measures the number of queries to the oracle $\mathcal{O} \in \{F_r, \rho\}$. As F_r internally uses a block cipher E, which is a known construction, the distinguisher can evaluate E offline. These evaluations are counted by the offline complexity.

Note the small abuse of terminology here: *time complexity* refers to the number of *time steps* that are available to the distinguisher, while *offline complexity* refers to the number of *evaluations of* E that the distinguisher can make offline. This abuse retains generality, as these numbers only differ by a small constant factor. For example, assume that one evaluation of E always takes at least t_E time. We simply rescale to $t_E = 1$ and assume that the time spent on other computations is negligible in this number. This makes the time and offline complexity equivalent.

We have so far bounded the distinguisher to data and time complexities q and t. Another distinction can be made depending on the *type of access* the distinguisher has to its oracle: quantum, printed as $\hat{q}$ or $\hat{t}$ (with hat), or classical, printed as q or t (without hat). In more detail, we will adopt the following notations:

- $\mathbb{D}(q, t)$ is the set of all distinguishers that can make q classical oracle queries and t classical offline evaluations,
- $\mathbb{D}(q, \hat{t})$ is the set of all distinguishers that can make q classical oracle queries and t quantum offline evaluations,
- $\mathbb{D}(\hat{q}, \hat{t})$ is the set of all distinguishers that can make q quantum oracle queries and t quantum offline evaluations.

There is little point in considering the remaining set $\mathbb{D}(\hat{q}, t)$, where the distinguisher can make quantum oracle queries but only classical offline evaluations.

Note how the difference between $\mathbb{D}(\hat{q}, \hat{t})$ and $\mathbb{D}(q, \hat{t})$ effectively pinpoints the difference between quantum adversaries with quantum access or with classical access to the oracle. The former set includes in particular distinguishers based on Simon's or Shor's quantum algorithms and that require quantum oracle access; whereas the latter set covers distinguishers based on Grover's algorithm and that therefore require only classical oracle access. In this work we do not consider the former set, and instead restrict our focus on quantum adversaries which only have classical oracle access to the keyed primitives. This models the scenario where the secret key is stored in classical memory but where the adversary employs a quantum computer to perform its attack.

[5] Throughout this work, we ignore a third measurement, memory, and assume that the distinguisher has sufficient memory available at all times.

We will consider a final set of distinguishers:

- $\mathbb{D}(q, \infty)$, the set of all distinguishers that can make q classical oracle queries and that have *unbounded computational power*.

Note that by definition, we have for any $q, t \geq 0$ (see also Fig. 2):

$$\mathbb{D}(q, t) \subseteq \mathbb{D}(q, \hat{t}) \subseteq \mathbb{D}(q, \infty). \tag{7}$$

Both $\mathbb{D}(q, t)$ and $\mathbb{D}(q, \infty)$ appear in non-quantum literature frequently. As a matter of fact, a customary way to perform classical standard-model security analysis goes along the following lines (see, e.g., [1,4,5,18,22,26,29,32,34,41, 46,47,49] for just a few examples): consider a scheme $\mathcal{S}$ that internally uses a primitive $\mathcal{P}$, where the key k to the scheme is fed to the primitive. Consider a distinguisher with complexities (q, t). As a first step, we replace $\mathcal{P}_k$ by its ideal equivalent $\mathcal{I}$. This step "costs" us the standard-model security of $\mathcal{P}_k$ against a distinguisher with complexities $(O(q), O(t))$ (the exact complexities depend on the number of times $\mathcal{S}$ invokes $\mathcal{P}$ per evaluation). What is left is the scheme $\mathcal{S}$ *keyed* by ideal secret primitive $\mathcal{I}$, and the only way for a distinguisher to gain any information about the construction is through queries to the construction. Therefore, the distinguisher is given unlimited computational power, and security is solely measured by the number of queries to the online oracle: the scheme is evaluated against a distinguisher with complexities (q, ∞). More formally, we thus obtain:

$$\mathsf{Adv}_{\mathcal{S}^{\mathcal{P}_k}}(\mathbb{D}(q, t)) \leq \mathsf{Adv}_{\mathcal{P}_k}(\mathbb{D}(O(q), O(t))) + \mathsf{Adv}_{\mathcal{S}^{\mathcal{I}}}(\mathbb{D}(q, \infty)),$$

where the corresponding security notions depend on the type of scheme $\mathcal{S}$ and type of primitive $\mathcal{P}$, and are omitted from the equation. The security of the primitive $\mathcal{P}_k$ is often not evaluated further, it for instance corresponds to the PRP security of AES. The other two advantage terms, on the other hand, *are* considered.

Equation (7) confirms that many non-quantum research on distinguishers with unbounded computational power directly covers distinguishers that can make quantum offline evaluations. We will use this observation in Sect. 5, but the observation has many more applications. As a matter of fact, virtually any standard-model security proof can be lifted to quantum security up to reasonable assumptions, including recently introduced authenticated encryption schemes [1, 4,22,26,41,46,47] and MAC functions [5,18,34]. The approach does not apply to security proofs that are a priori ideal-model, such as the analyses of sponge functions [40], Even-Mansour [11,14], and others. This is mostly due to the fact that in ideal-model security analyses, both the construction and the primitive are idealized and accessible by the distinguishers through queries: q stands for queries to the construction and t queries to the primitive, and the distinguishers have unbounded time complexity. Once evaluated in a quantum setting, part of the queries—namely the primitive queries—should be considered quantum.

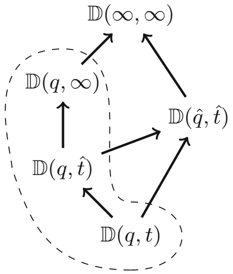

Fig. 2. Adversaries categorized by computational power and type of oracle access. An arrow represents inclusion, *i.e.*, $A \rightarrow B$ represents $A \subseteq B$.

4 Quantum Key-Recovery Attack

We present a generic attack to recover the key of F_r of Sect. 2.2. The key recovery is performed by translating the problem to a $\mathsf{relation}_{p,q,R}$ problem in the terminology of Sect. 2.4, where an evaluation of $F_r(\mathbf{k}, x)$ is used to build the functions f and g and to recover the key $\mathbf{k}$. However, various technicalities occur in this approach, most importantly as there may, for one test value x, be multiple keys $\mathbf{k} \neq \mathbf{k}'$ that fulfill the relation. These technicalities are resolved via the use of a *threshold* τ, which indicates the number of test values to be considered. The threshold τ provides a trade-off between accuracy (of the key guessing) and complexity (of the attack). We first state the definition of colliding key sets for a block cipher in Sect. 4.1. The generic attack is then given in Sect. 4.2.

Without loss of generality, it is fair to consider F_r only for keys $\mathbf{k}$ such that $k_i \neq k_j$ for all $i \neq j$. Indeed, if two keys collide, the corresponding keyed block ciphers cancel each other out and we are effectively considering a scheme based on $r-2$ permutations which is less secure. Furthermore, note that if $\sigma : \{1, \dots, r\} \rightarrow \{1, \dots, r\}$ is a permutation and $\mathbf{k}' = (k_{\sigma(1)}, \dots, k_{\sigma(r)})$, then

$$F_r(\mathbf{k}, \cdot) = F_r(\mathbf{k}', \cdot).$$

In other words, for any key $\mathbf{k}$, there are $r!$ elements of K^r (including $\mathbf{k}$) giving the exact same function F_r. As such, in our attack we will simply view keys as *unordered sets* from $\binom{K}{r}$ rather than *ordered lists* from K^r, or formally, $F_r : \binom{K}{r} \times X \rightarrow X$.

4.1 Colliding Key Sets

The success of the generic attack depends on the probability that there exist colliding key sets for the block cipher. Although it is written in terminology of F_r of Sect. 2.2, it is merely a standalone combinatorial statement.

Definition 3. *Let $E : K \times X \rightarrow X$ be a block cipher. Let $r \geq 1$ and $\tau \geq 1$ be two positive natural numbers. We define by $\mathsf{collkeyset}_E(r, \tau)$ the probability that* *there exist two distinct key sets* $\mathbf{k}, \mathbf{k}' \in \binom{K}{r}$ *such that*

$$F_r(\mathbf{k}, 1) \| \cdots \| F_r(\mathbf{k}, \tau) = F_r(\mathbf{k}', 1) \| \cdots \| F_r(\mathbf{k}', \tau),$$

where F_r *is defined in Sect.* 2.2.

If E is an ideal cipher, *i.e.*, if $E \xleftarrow{\$} \mathsf{Block}(K, X)$, the probability $\mathsf{collkeyset}_E(r, \tau)$ can be straightforwardly computed.

Lemma 1. *If* $E \xleftarrow{\$} \mathsf{Block}(K, X)$, *then*

$$\mathsf{collkeyset}_E(r, \tau) \le \binom{|K|}{r}^2 / |X|^{\underline{\tau}}. \tag{8}$$

For $\alpha := \lceil \log_{|X|}(|K|) \rceil$, *assuming that* $(2\alpha)^2 r \le |X|$,

$$\mathsf{collkeyset}_E(r, 2\alpha r + 1) \le \frac{4}{|X| - 2\alpha r}. \tag{9}$$

Proof. Pick any two distinct sets $\mathbf{k}, \mathbf{k}' \in \binom{K}{r}$, at most $\binom{|K|}{r}\left(\binom{|K|}{r} - 1\right) \le \binom{|K|}{r}^2$ choices. As $\mathbf{k}$ and $\mathbf{k}'$ both consist of r distinct elements and are no permutation of each other (by definition of $\binom{K}{r}$), $\mathbf{k}$ contains at least one element that does not occur in the rest of $\mathbf{k}$ or in $\mathbf{k}'$. W.l.o.g., $k_1 \notin \{k_2, \ldots, k_r, k'_1, \ldots, k'_r\}$.

The probability that

$$\forall\, i = 1, \ldots, \tau \;:\; E_{k_1}(i) = \Big(E_{k_2}(i) \oplus \cdots \oplus E_{k_r}(i)\Big) \oplus \Big(E_{k'_1}(i) \oplus \cdots \oplus E_{k'_r}(i)\Big) \tag{10}$$

is at most $\frac{(|X|-\tau)!}{|X|!} = 1/|X|^{\underline{\tau}}$. This completes the proof of (8).

Remains to prove (9). Using that $(m - n + 1)^n \le m^{\underline{n}} \le m^n$, we get from (8):

$$\begin{aligned}
\mathsf{collkeyset}_E(r, 2\alpha r + 1) &\le \binom{|K|}{r}^2 / |X|^{\underline{2\alpha r + 1}} = \frac{(|K|^{\underline{r}})^2}{(r!)^2 \cdot |X|^{\underline{2\alpha r + 1}}} \\
&\le \frac{|K|^{2r}}{(r!)^2 \cdot (|X| - 2\alpha r)^{2\alpha r}} \cdot \frac{1}{|X| - 2\alpha r} \\
&= \frac{|K|^{2r}}{(r!)^2 \cdot |X|^{2\alpha r} \cdot \left(1 - \frac{2\alpha r}{|X|}\right)^{2\alpha r}} \cdot \frac{1}{|X| - 2\alpha r} \\
&\le \frac{1}{(r!)^2 \cdot \left(1 - \frac{2\alpha r}{|X|}\right)^{2\alpha r}} \cdot \frac{1}{|X| - 2\alpha r},
\end{aligned} \tag{11}$$

where the last step holds as $\alpha \ge \log_{|X|}(|K|)$.

Note that

$$\left(1 - \frac{2\alpha r}{|X|}\right)^{\alpha} \ge 1 - \frac{2\alpha^2 r}{|X|} \ge \frac{1}{2},$$

where the first step holds as $(1-x)^y \geq 1-xy$ and the second step by assumption that $(2\alpha)^2 r \leq |X|$. We thus obtain for (11):

$$\mathsf{collkeyset}_E(r, 2\alpha r+1) \leq \left(\frac{2^r}{r!}\right)^2 \cdot \frac{1}{|X|-2\alpha r} \leq \frac{4}{|X|-2\alpha r},$$

which completes the proof of (9). □

4.2 Generic Attack

Theorem 1. *Let $E : K \times X \to X$ be a block cipher, and let $r \geq 1$ be a positive natural number. Consider F_r of Sect. 2.2. Let $\tau \geq 1$ be a positive natural number. There exists a distinguisher $\mathcal{D} \in \mathbb{D}(\tau, \hat{t})$ with $t = O\left(\tau \cdot |K|^{r/(r+1)}\right)$ that recovers the key of F_r with success probability at least $1 - \mathsf{collkeyset}_E(r, \tau)$.*

Proof. Let $\mathbf{k} = (k_1, \ldots, k_r) \in \binom{K}{r}$ be the secret key to F_r, *i.e.*,

$$F_r(\mathbf{k}, x) = E_{k_1}(x) \oplus \cdots \oplus E_{k_r}(x).$$

As a first step, the distinguisher queries $F_r(\mathbf{k}, i) = z_i$ for $i = 1, \ldots, \tau$. Then, define the following two functions:

$$\begin{aligned} &f : K \to X^\tau, && g : K \to X^\tau,\\ &f(l) = E_l(1) \| \cdots \| E_l(\tau), && g(m) = \big(E_m(1) \oplus z_1\big) \| \cdots \| \big(E_m(\tau) \oplus z_\tau\big). \end{aligned}$$

Next, evaluate the quantum relation-finding algorithm of Sect. 2.4 for parameters $p = r-1$, $q = 1$, and R as the relation that all elements of the tuple XOR to 0:[6]

$$R = \{(a_1, \ldots, a_r) \mid a_1 \oplus \cdots \oplus a_r = 0\}.$$

The relation-finding algorithm makes

$$O\left(\tau \cdot |K|^{r/(r+1)}\right)$$

evaluations of E (the factor τ corresponds to the number of evaluations of E per evaluation of f and g).

Note that by construction, there is at least one set of candidate keys for the algorithm: $\mathbf{k}$. If this is the only set of candidate keys, then the algorithm will output the correct key and $\mathcal{D}$ succeeds. On the other hand, there exist more than two sets of solutions with probability at most $\mathsf{collkeyset}_E(r, \tau)$. Therefore, the attack succeeds with probability at least $1 - \mathsf{collkeyset}_E(r, \tau)$. □

From Theorem 1 and Lemma 1 we obtain the following corollary.

[6] The attack can be simplified by putting $z_1 \| \cdots \| z_\tau$ inside relation R and considering $p = r$ and $q = 0$. We follow current approach for intuitiveness.

Corollary 1. *Let $E : K \times X \to X$ be an ideal cipher, and let $r \geq 1$ be a positive natural number. Consider F_r of Sect. 2.2. Put $\alpha = \lceil \log_{|X|}(|K|) \rceil$, assume that $(2\alpha)^2 r \leq |X|$, and let $\tau = 2\alpha r + 1$. There exists a distinguisher $\mathcal{D} \in \mathbb{D}(\tau, \hat{t})$ with $t = O\left(\tau \cdot |K|^{r/(r+1)}\right) = O\left(|K|^{r/(r+1)}\right)$ that recovers the key of F_r with success probability at least $1 - \frac{4}{|X|-2\alpha r}$.*

The estimation of offline complexity presents an asymptotic relation as a function of $|K|$ only. In addition to absorbing τ, the big O notation hides various constant factors that depend on r, deriving from the underlying quantum search algorithm.

5 Quantum Security Analysis

For our quantum security analysis of F_r we recall a classical result on its idealized counterpart F_r^{id} due to Patarin for $r = 2$ [43,44] and its generalization to $r \geq 3$ by Mennink and Preneel [39]:

Lemma 2. *Let $r \geq 2$ be integral. For $q \leq |X|/67$, we have*

$$\mathsf{Adv}^{\mathrm{prf}}_{F_r^{\mathrm{id}}}(\mathbb{D}(q, \infty)) = \frac{q}{|X|}.$$

The analysis in [39,43,44] is performed to cover information-theoretic distinguishers. It considers deterministic distinguishers which query their oracle (either F_r^{id} or ρ) q times adaptively, and which are computationally unbounded.

Using Lemma 2, we can derive the following upper bound on the success probability of a quantum distinguisher (from $\mathbb{D}(q, \hat{t})$) in distinguishing F_r for random keys $\mathbf{k} = (k_1, \ldots, k_r) \xleftarrow{\$} K^r$ from a random function ρ.

Theorem 2. *Let $E : K \times X \to X$ be a block cipher, and let $r \geq 2$ be integral. For $q \leq |X|/67$, we have*

$$\mathsf{Adv}^{\mathrm{prf}}_{F_r}(\mathbb{D}(q, \hat{t})) \leq r \cdot \mathsf{Adv}^{\mathrm{prp}}_{E}(\mathbb{D}(q, \hat{t})) + \frac{q}{|X|}.$$

Proof. Let $\mathbf{k} = (k_1, \ldots, k_r) \xleftarrow{\$} K^r$, $\boldsymbol{\pi} = (\pi_1, \ldots, \pi_r) \xleftarrow{\$} \mathsf{Perm}(X)^r$, and $\rho \xleftarrow{\$} \mathsf{Func}(X, X)$. Consider any distinguisher $\mathcal{D} \in \mathbb{D}(q, \hat{t})$. We have

$$\begin{aligned} \mathsf{Adv}^{\mathrm{prf}}_{F_r}(\mathcal{D}) &= \left|\mathbf{P}\left(\mathcal{D}^{F_{r,\mathbf{k}}} = 1\right) - \mathbf{P}\left(\mathcal{D}^{\rho} = 1\right)\right| \\ &\leq \left|\mathbf{P}\left(\mathcal{D}^{F_{r,\mathbf{k}}} = 1\right) - \mathbf{P}\left(\mathcal{D}^{F^{\mathrm{id}}_{r,\boldsymbol{\pi}}} = 1\right)\right| + \mathsf{Adv}^{\mathrm{prf}}_{F_r^{\mathrm{id}}}(\mathcal{D}). \end{aligned} \tag{12}$$

The first term of (12) satisfies

$$\begin{aligned} \left|\mathbf{P}\left(\mathcal{D}^{F_{r,\mathbf{k}}} = 1\right) - \mathbf{P}\left(\mathcal{D}^{F^{\mathrm{id}}_{r,\boldsymbol{\pi}}} = 1\right)\right| &\leq \sum_{i=1}^{r} \left|\mathbf{P}\left(\mathcal{E}^{E_{k_i}} = 1\right) - \mathbf{P}\left(\mathcal{E}^{\pi_i} = 1\right)\right| \\ &\leq r \cdot \mathsf{Adv}^{\mathrm{prp}}_{E}(\mathcal{E}), \end{aligned} \tag{13}$$

for some distinguisher $\mathcal{E}$ with online complexity q and offline complexity at most $\hat{t}$. Clearly,

$$\mathsf{Adv}_E^{\mathrm{prp}}(\mathcal{E}) \leq \sup_{\mathcal{E}\in\mathbb{D}(q,\hat{t})} \mathsf{Adv}_E^{\mathrm{prp}}(\mathcal{E}) \leq \mathsf{Adv}_E^{\mathrm{prp}}(\mathbb{D}(q,\hat{t})).$$

Using Lemma 2, the second term of (12) satisfies

$$\mathsf{Adv}_{F_r^{\mathrm{id}}}^{\mathrm{prf}}(\mathcal{D}) \leq \sup_{\mathcal{D}\in\mathbb{D}(q,\hat{t})} \mathsf{Adv}_{F_r^{\mathrm{id}}}^{\mathrm{prf}}(\mathcal{D}) \leq \sup_{\mathcal{D}\in\mathbb{D}(q,\infty)} \mathsf{Adv}_{F_r^{\mathrm{id}}}^{\mathrm{prf}}(\mathcal{D}) = \mathsf{Adv}_{F_r^{\mathrm{id}}}^{\mathrm{prf}}(\mathbb{D}(q,\infty)) \leq \frac{q}{|X|}.$$

We have hence obtained

$$\mathsf{Adv}_{F_r}^{\mathrm{prf}}(\mathcal{D}) \leq r \cdot \mathsf{Adv}_E^{\mathrm{prp}}(\mathbb{D}(q,\hat{t})) + \frac{q}{|X|}.$$

As the derivation holds for any $\mathcal{D} \in \mathbb{D}(q,\hat{t})$, this completes the proof. □

The step that facilitates the application of Lemma 2 is mainly due to our formalization of distinguishers in Sect. 3. It is interesting to see that the classical world equivalent of Theorem 2 would read

$$\mathsf{Adv}_{F_r}^{\mathrm{prf}}(\mathbb{D}(q,t)) \leq r \cdot \mathsf{Adv}_E^{\mathrm{prp}}(\mathbb{D}(q,t)) + \frac{q}{|X|},$$

and the security analysis is fairly identical. The reduction in the proof of Theorem 2 therewith clearly demonstrates that the analysis directly generalizes to many other proofs in symmetric key cryptography and it is therefore of independent interest. Rather than writing the direct security proof, we could have equally well departed from the techniques of Hallgren et al. [21] and Song [51]. However, as pointed out in Sect. 1, these techniques are stronger and more involved by design, and we believe that for our case a direct proof is easier to grasp.

The question as to what level of PRP security a block cipher E offers is beyond the scope of this work; it strongly depends on the strength of E against cryptanalysis. For example, in the classical setting, assuming that E is a strong enough cipher, we have $\mathsf{Adv}_E^{\mathrm{prp}}(\mathbb{D}(q,t)) \approx \frac{q}{|K|}$. If the distinguisher can make quantum offline evaluations, we know that, due to Grover's algorithm, $\mathsf{Adv}_E^{\mathrm{prp}}(\mathbb{D}(q,\hat{t})) = \Omega\left(\frac{q}{|K|^{1/2}}\right)$. Assuming that E is strong enough and Grover's algorithm describes the best possible attack on E, Theorem 2 gives security of F_r as long as the complexity satisfies $q \ll \min\{|K|^{1/2}/r, |X|\}$. Using a block cipher with a key twice the state size, *e.g.*, AES-256, one obtains optimal security.

6 Discussion

Theorem 2 suggests that F_r achieves security up to $\min\{|K|^{1/2}/r, |X|\}$ queries, provided that Grover's algorithm is the best way of breaking the underlying block cipher. On the other hand, the attack of Sect. 4 only reaches $|K|^{r/(r+1)}$, indicating a gap between the best attack and best security bound. The tightness appears to be lost in Eq. (13) of the proof of Theorem 2, which upper bounds the advantage of guessing a key $\mathbf{k} \in K^r$ by the advantage of guessing one of its elements $k_i \in K$. While this step is a conventional and reasonably harmless proof technique in countless works on non-quantum symmetric key security, for analysis against quantum distinguishers this step entails a significant loss.

Recall that the bound of Lemma 2 holds for any $r \geq 2$. Now, consider F_r, and assume that the adversary is able to recover $r-2$ keys. This effectively reduces F_r to F_2, which, as suggested by Lemma 2, should not have an influence on the bound. Instead, if one recovers $r-1$ out of r keys, the lemma cannot be applied, and the problem of breaking F_r reduces to the problem of recovering $r-1$ keys. In other words, intuition tells that security up to at least $\min\{|K|^{(r-1)/r}, |X|\}$ could be attainable. Well hidden in this intuition are, however, various conceptual difficulties. Most importantly, it requires the formalization of "block ciphers being secure conditioned on the absence of key recovery." Additionally, it requires a mechanism to verify whether a distinguisher has recovered a key of $E_{k_1} \oplus \cdots \oplus E_{k_r}$, without having access to $E_{k_1}, \ldots, E_{k_r}$ separately.

Acknowledgments. This work was supported in part by the Research Council KU Leuven: GOA TENSE (GOA/11/007). In addition, this work was supported by the European Commission through the Horizon 2020 research and innovation programme under grant agreement No H2020-ICT-2014-645622 PQCRYPTO and grant agreement No H2020-MSCA-ITN-2014-643161 ECRYPT-NET. Bart Mennink is supported by a postdoctoral fellowship from the Netherlands Organisation for Scientific Research (NWO) under Veni grant 016.Veni.173.017. Alan Szepieniec is supported by a Ph.D. Fellowship from the Institute for the Promotion of Innovation through Science and Technology in Flanders (VLAIO, formerly IWT). The authors would like to thank Stacey Jeffery and the anonymous reviewers of PQCrypto 2017 for their useful suggestions.

References

1. Abed, F., Forler, C., List, E., Lucks, S., Wenzel, J.: RIV for robust authenticated encryption. In: Peyrin [45], pp. 23–42
2. Anand, M.V., Targhi, E.E., Tabia, G.N., Unruh, D.: Post-quantum security of the CBC, CFB, OFB, CTR, and XTS modes of operation. In: Takagi, T. (ed.) PQCrypto 2016. LNCS, vol. 9606, pp. 44–63. Springer, Cham (2016). doi:10.1007/978-3-319-29360-8_4
3. Andreeva, E., Bilgin, B., Bogdanov, A., Luykx, A., Mennink, B., Mouha, N., Yasuda, K.: APE: authenticated permutation-based encryption for lightweight cryptography. In: Cid and Rechberger [15], pp. 168–186
4. Andreeva, E., Bogdanov, A., Luykx, A., Mennink, B., Tischhauser, E., Yasuda, K.: Parallelizable and authenticated online ciphers. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013. LNCS, vol. 8269, pp. 424–443. Springer, Heidelberg (2013). doi:10.1007/978-3-642-42033-7_22
5. Andreeva, E., Daemen, J., Mennink, B., Van Assche, G.: Security of keyed sponge constructions using a modular proof approach. In: Leander, G. (ed.) FSE 2015. LNCS, vol. 9054, pp. 364–384. Springer, Heidelberg (2015). doi:10.1007/978-3-662-48116-5_18

6. Bellare, M., Impagliazzo, R.: A tool for obtaining tighter security analyses of pseudorandom function based constructions, with applications to PRP to PRF conversion. Cryptology ePrint Archive, Report 1999/024 (1999)
7. Bellare, M., Kilian, J., Rogaway, P.: The security of cipher block chaining. In: Desmedt, Y.G. (ed.) CRYPTO 1994. LNCS, vol. 839, pp. 341–358. Springer, Heidelberg (1994). doi:10.1007/3-540-48658-5_32
8. Bellare, M., Rogaway, P.: The security of triple encryption and a framework for code-based game-playing proofs. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 409–426. Springer, Heidelberg (2006). doi:10.1007/11761679_25
9. Bernstein, D.J., Buchmann, J., Dahmen, E. (eds.): Post-Quantum Cryptography. Springer Science & Business Media, Heidelberg (2009)
10. Bhaumik, R., Nandi, M.: OleF: an inverse-free online cipher. IACR Trans. Symmetric Cryptol. **1**(2), 30–51 (2016)
11. 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. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 45–62. Springer, Heidelberg (2012). doi:10.1007/978-3-642-29011-4_5
12. Brassard, G., Høyer, P., Tapp, A.: Quantum cryptanalysis of hash and claw-free functions. In: Lucchesi, C.L., Moura, A.V. (eds.) LATIN 1998. LNCS, vol. 1380, pp. 163–169. Springer, Heidelberg (1998). doi:10.1007/BFb0054319
13. Buhrman, H., Dürr, C., Heiligman, M., Høyer, P., Magniez, F., Santha, M., de Wolf, R.: Quantum algorithms for element distinctness. SIAM J. Comput. **34**(6), 1324–1330 (2005)
14. Chen, S., Steinberger, J.P.: Tight security bounds for key-alternating ciphers. In: Nguyen and Oswald [42], pp. 327–350
15. Cid, C., Rechberger, C. (eds.): FSE 2014. LNCS, vol. 8540. Springer, Heidelberg (2015)
16. Cogliati, B., Lampe, R., Patarin, J.: The indistinguishability of the XOR of k permutations. In: Cid and Rechberger [15], pp. 285–302
17. Cogliati, B., Lampe, R., Seurin, Y.: Tweaking even-mansour ciphers. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9215, pp. 189–208. Springer, Heidelberg (2015). doi:10.1007/978-3-662-47989-6_9
18. Cogliati, B., Seurin, Y.: EWCDM: an efficient, beyond-birthday secure, nonce-misuse resistant MAC. In: Robshaw and Katz [48], pp. 121–149
19. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Miller, G.L. (ed.) Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, 22–24 May 1996, pp. 212–219. ACM (1996)
20. Hall, C., Wagner, D., Kelsey, J., Schneier, B.: Building PRFs from PRPs. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 370–389. Springer, Heidelberg (1998). doi:10.1007/BFb0055742
21. Hallgren, S., Smith, A., Song, F.: Classical cryptographic protocols in a quantum world. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 411–428. Springer, Heidelberg (2011). doi:10.1007/978-3-642-22792-9_23
22. Hoang, V.T., Krovetz, T., Rogaway, P.: Robust authenticated-encryption AEZ and the problem that it solves. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9056, pp. 15–44. Springer, Heidelberg (2015). doi:10.1007/978-3-662-46800-5_2

23. Impagliazzo, R., Rudich, S.: Limits on the provable consequences of one-way permutations. In: Goldwasser, S. (ed.) CRYPTO 1988. LNCS, vol. 403, pp. 8–26. Springer, New York (1990). doi:10.1007/0-387-34799-2_2
24. Iwata, T.: New blockcipher modes of operation with beyond the birthday bound security. In: Robshaw, M. (ed.) FSE 2006. LNCS, vol. 4047, pp. 310–327. Springer, Heidelberg (2006). doi:10.1007/11799313_20
25. Iwata, T., Mennink, B., Vizr, D.: CENC is optimally secure. Cryptology ePrint Archive, Report 2016/1087 (2016)
26. Iwata, T., Minematsu, K., Guo, J., Morioka, S.: CLOC: authenticated encryption for short input. In: Cid and Rechberger [15], pp. 149–167
27. Kaplan, M.: Quantum attacks against iterated block ciphers. CoRR abs/1410.1434 (2014)
28. Kaplan, M., Leurent, G., Leverrier, A., Naya-Plasencia, M.: Breaking symmetric cryptosystems using quantum period finding. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. LNCS, vol. 9815, pp. 207–237. Springer, Heidelberg (2016). doi:10.1007/978-3-662-53008-5_8
29. Krovetz, T., Rogaway, P.: The software performance of authenticated-encryption modes. In: Joux, A. (ed.) FSE 2011. LNCS, vol. 6733, pp. 306–327. Springer, Heidelberg (2011). doi:10.1007/978-3-642-21702-9_18
30. Kuwakado, H., Morii, M.: Quantum distinguisher between the 3-round Feistel cipher and the random permutation. In: Proceedings of IEEE International Symposium on Information Theory, ISIT 2010, 13–18 June 2010, Austin, Texas, USA, pp. 2682–2685. IEEE (2010)
31. Kuwakado, H., Morii, M.: Security on the quantum-type Even-Mansour cipher. In: Proceedings of the International Symposium on Information Theory and its Applications, ISITA 2012, Honolulu, HI, USA, 28–31 October 2012, pp. 312–316. IEEE (2012)
32. Landecker, W., Shrimpton, T., Terashima, R.S.: Tweakable blockciphers with beyond birthday-bound security. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 14–30. Springer, Heidelberg (2012). doi:10.1007/978-3-642-32009-5_2
33. Lucks, S.: The sum of PRPs is a secure PRF. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 470–484. Springer, Heidelberg (2000). doi:10.1007/3-540-45539-6_34
34. Luykx, A., Preneel, B., Tischhauser, E., Yasuda, K.: A MAC mode for lightweight block ciphers. In: Peyrin [45], pp. 43–59
35. Magniez, F., Santha, M., Szegedy, M.: Quantum algorithms for the triangle problem. SIAM J. Comput. **37**(2), 413–424 (2007)
36. Malozemoff, A.J., Katz, J., Green, M.D.: Automated analysis and synthesis of block-cipher modes of operation. In: IEEE 27th Computer Security Foundations Symposium, CSF 2014, Vienna, Austria, 19–22 July 2014, pp. 140–152. IEEE Computer Society (2014)
37. Mandal, A., Patarin, J., Nachef, V.: Indifferentiability beyond the birthday bound for the XOR of two public random permutations. In: Gong, G., Gupta, K.C. (eds.) INDOCRYPT 2010. LNCS, vol. 6498, pp. 69–81. Springer, Heidelberg (2010). doi:10.1007/978-3-642-17401-8_6
38. Mennink, B.: XPX: generalized tweakable even-mansour with improved security guarantees. In: Robshaw and Katz [48], pp. 64–94

39. Mennink, B., Preneel, B.: On the XOR of multiple random permutations. In: Malkin, T., Kolesnikov, V., Lewko, A.B., Polychronakis, M. (eds.) ACNS 2015. LNCS, vol. 9092, pp. 619–634. Springer, Cham (2015). doi:10.1007/978-3-319-28166-7_30
40. Mennink, B., Reyhanitabar, R., Vizár, D.: Security of full-state keyed sponge and duplex: applications to authenticated encryption. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015. LNCS, vol. 9453, pp. 465–489. Springer, Heidelberg (2015). doi:10.1007/978-3-662-48800-3_19
41. Minematsu, K.: Parallelizable rate-1 authenticated encryption from pseudorandom functions. In: Nguyen and Oswald [42], pp. 275–292
42. Nguyen, P.Q., Oswald, E. (eds.): EUROCRYPT 2014. LNCS, vol. 8441. Springer, Heidelberg (2014)
43. Patarin, J.: A proof of security in $O(2^n)$ for the XOR of two random permutations. In: Safavi-Naini, R. (ed.) ICITS 2008. LNCS, vol. 5155, pp. 232–248. Springer, Heidelberg (2008). doi:10.1007/978-3-540-85093-9_22
44. Patarin, J.: Introduction to mirror theory: analysis of systems of linear equalities and linear non equalities for cryptography. Cryptology ePrint Archive, Report 2010/287 (2010)
45. Peyrin, T. (ed.): FSE 2016. LNCS, vol. 9783. Springer, Heidelberg (2016)
46. Peyrin, T., Seurin, Y.: Counter-in-tweak: authenticated encryption modes for tweakable block ciphers. In: Robshaw and Katz [48], pp. 33–63
47. Reyhanitabar, R., Vaudenay, S., Vizár, D.: Authenticated encryption with variable stretch. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016. LNCS, vol. 10031, pp. 396–425. Springer, Heidelberg (2016). doi:10.1007/978-3-662-53887-6_15
48. Robshaw, M., Katz, J. (eds.): CRYPTO 2016. LNCS, vol. 9814. Springer, Heidelberg (2016)
49. Rogaway, P.: Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC. In: Lee, P.J. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 16–31. Springer, Heidelberg (2004). doi:10.1007/978-3-540-30539-2_2
50. Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: 35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 20–22 November 1994, pp. 124–134. IEEE Computer Society (1994)
51. Song, F.: A note on quantum security for post-quantum cryptography. In: Mosca, M. (ed.) PQCrypto 2014. LNCS, vol. 8772, pp. 246–265. Springer, Cham (2014). doi:10.1007/978-3-319-11659-4_15
52. Tani, S.: Claw finding algorithms using quantum walk. Theor. Comput. Sci. **410**(50), 5285–5297 (2009)
53. Zhandry, M.: How to construct quantum random functions. In: 53rd Annual IEEE Symposium on Foundations of Computer Science, FOCS 2012, New Brunswick, NJ, USA, 20–23 October 2012, pp. 679–687. IEEE Computer Society (2012)
54. Zhandry, M.: A note on the quantum collision and set equality problems. Quant. Inf. Comput. **15**(7&8), 557–567 (2015)
55. Zhandry, M.: A note on quantum-secure PRPs. Cryptology ePrint Archive, Report 2016/1076 (2016)
56. Zhang, S.: Promised and distributed quantum search. In: Wang, L. (ed.) COCOON 2005. LNCS, vol. 3595, pp. 430–439. Springer, Heidelberg (2005). doi:10.1007/11533719_44