SCIENCE CHINA
Information Sciences

• **RESEARCH PAPER** •

Quantum Key-recovery Attack on Feistel Structures

DONG XiaoYang[1] & WANG Xiaoyun [1,2*]

[1]*Institute for Advanced Study, Tsinghua University, P. R. China;*
[2]*Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, P. R. China*
{*xiaoyangdong,xiaoyunwang*}*@tsinghua.edu.cn*

Received ; accepted

Abstract Post-quantum cryptography has attracted much attention from worldwide cryptologists. At Asiacrypt 2017, Leander and May combines Grover and Simon algorithms to quantumly break FX-based block ciphers. In this paper, we study the Feistel constructions with Grover and Simon algorithms and give some new quantum key-recovery attacks on different rounds of Feistel constructions. Our attacks requires $2^{nr/4-3n/4}$ quantum queries. When comparing with the quantum brute force search, the time complexity is reduced by a factor of $2^{0.75n}$. When comparing with the best classical attacks, the time complexity is reduced by a factor $2^{0.5n}$ without any memory cost.

Keywords Quantum-CPA, Key-recovery Attack, Feistel Structure, Simon, Grover

Citation Dong X Y, Wang X Y. Quantum Key-recovery Attack on Feistel Structures. Sci China Inf Sci, 2016, (): xxxxxx, doi: xxxxxxxxxxxxxx

1 Introduction

Due to the rapidly development of quantum computers, the security of classical cryptographic schemes are heavily challenged. The most severe and notable threat is Shor's algorithm [Sho97] that breaks RSA cryptosystem. Recently, researchers find that quantum computing not only impacts the public key cryptography, but also breaks many secret key schemes in polynomial time, such as Even-Mansour ciphers [EM93], Encrypted-CBC-MACs [KLLN16] and others. To study the security of many more classical and important cryptographic schemes against quantum attacks is urgently needed. At Asiacrypt 2017, NIST [TP17] reports the ongoing competition for post-quantum cryptographic algorithms, including signatures, encryptions and key-establishment. The ship for post-quantum crypto has sailed, cryptographic communities must get ready to welcome the post-quantum age.

In a quantum computer, the adversaries could make quantum queries on some superposition quantum states of the relevant cryptosystem, which is the so-called quantum-CPA setting [BZ13]. It is known that Grover's algorithm [Gro96] could speed up brute force search. Given an m-bit key, Grover's algorithm allows to recover the key using $\mathcal{O}(2^{m/2})$ quantum steps. It seems that doubling the key-length of one block cipher could achieve the same security against quantum attackers. However, Kuwakado and Morii [KM12b] identified a new family of quantum attacks on certain generic constructions of secret key schemes.

* Corresponding author (email: xiaoyunwang@tsinghua.edu.cn)

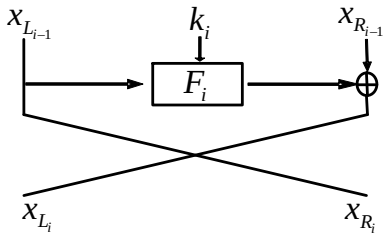

Figure 1 The ith round of the Feistel structure

They showed that the Even-Mansour ciphers could be broken in polynomial time by Simon algorithm [Sim97], which could find the period of a periodic function in polynomial time in a quantum computer. The following works by Kaplan *et al.* [KLLN16] revealed that many other secret key schemes could also be broken by Simon algorithm, such as CBC-MAC, PMAC, GMAC and some CAESAR candidates.

Feistel block ciphers [FNS75] are extremely important and extensively researched cryptographic schemes. It adopts an efficient Feistel network design. Historically, many block cipher standards such as DES, Triple-DES, MISTY1, Camellia and CAST-128 [Int10] are based on Feistel design. In a seminal work, Luby and Rackoff [LR88] proved that a three-round Feistel scheme is a secure pseudo-random permutation. However, Kuwakado and Morii [KM10] introduced a quantum distinguisher attack on 3-round Feistel ciphers, that could distinguish the cipher and a random permutation in polynomial time. In classical setting, Dinur *et al.* [DDKS15] gave a series of key-recovery attacks on 5 to 32-round Feistel ciphers. However, there are no key-recovery attacks on Feistel ciphers in quantum-CPA setting.

In this paper, we for the first time consider the quantum key-recovery attack on Feistel schemes. As shown in Figure 1, in the ith round of the Feistel structure, the n-bit blocks are divided into two equal parts $(x_{L_{i-1}}, x_{R_{i-1}})$, the $n/2$-bit subkeys k_i are wrapped into round function F_i. The output is (x_{L_i}, x_{R_i}). Similar to Dinur *et al.*'s [DDKS15] attacks, our attacks are also generic attacks that assumes the round functions in each round of the Feistel cipher to be not necessary identity and the round keys k_i are independent to each other. Hence, using Grover algorithm to brute force search all the subkeys k_i of an r-round Feistel cipher requires $2^{nr/4}$ quantum queries. In this paper, we combine Grover's algorithm and Simon algorithm to give a series quantum key-recovery attacks on different rounds of Feistel structures. Our attacks requires $2^{nr/4-3n/4}$ quantum queries, which reduces the time by a factor of $2^{0.75n}$ when comparing with the quantum brute force search. When compared with the best classical attacks, i.e. Dinur *et al.*'s attacks [DDKS15], our results reduce the time by a factor $2^{0.5n}$ without any memory cost. All the results are summarised in Table 1.

Table 1 Summary of Key-recovery Attacks on Feistel Schemes in Classical and Quantum-CPA Settings

	Dinur *et al.* [DDKS15]		Quantum-CPA Trivial Bound	Quantum-CPA of Ours
Rounds	Time	Memory	Time	
5	2^n	$2^{0.5n}$	$2^{1.25n}$	$2^{0.5n}$
7	$2^{1.5n}$	2^n	$2^{1.75n}$	2^n
8	$2^{1.75n}$	$2^{1.25n}$	2^{2n}	$2^{1.25n}$
15	$2^{3.5n}$	2^{2n}	$2^{3.75n}$	2^{3n}
31	$2^{7.5n}$	2^{4n}	$2^{7.75n}$	2^{7n}
32	$2^{7.75n}$	$2^{7.25n}$	2^{8n}	$2^{7.25n}$

2 Related Works

Our quantum attacks are based the two popular quantum algorithm, i.e. Simon algorithm [Sim97] and Grover algorithm [Gro96].

Simon's Problem. Given a boolen function f $\{0,1\}^n \to \{0,1\}^n$, that is known to be invariant under some n-bit XOR period a, find a. In other words, find a by given: $f(x) = f(y) \leftrightarrow x \oplus y \in \{0^n, a\}$.

The optimal time to solve the problem is $\mathcal{O}(2^{n/2})$. However, Simon [Sim97] gives a quantum algorithm that provides exponential speedup and only requires $\mathcal{O}(n)$ quantum queries to find a. The algorithm includes five quantum steps:

I. Initializing two n-bit quantum registers to state $|0\rangle^{\otimes n}|0\rangle^{\otimes n}$, one applies Hadamard transform to the first register to attain an equal superposition:

$$H^{\otimes n}|0\rangle|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|0\rangle. \tag{1}$$

II. A quantum query to the function f maps this to the state

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|f(x)\rangle$$

.

III. Measuring the second register, the first register collapses to the state:

$$\frac{1}{\sqrt{2}}(|z\rangle + |z \oplus a\rangle)$$

.

IV. Applying Hadamard transform to the first register, we get:

$$\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{y\cdot z}(1 + (-1)^{y\cdot a})|y\rangle$$

.

V. The vectors y such that $y \cdot a = 1$ have amplitude 0. Hence, measuring the state yields a value y that $y \cdot a = 0$.

Repeat $\mathcal{O}(n)$ times, one obtains a by solving a system of linear equations.

Kuwakado and Morii [KM12b] used Simon algorithm to break Even-Mansour construction [EM93]. For a given permutation P, the EM cipher is $Enc(x) = P(x + k_1) + k_2$. Classically, a EM cipher is secure up to $2^{n/2}$ queries, where n is the input size of P. However, using Simon algorithm [Sim97], Kuwakado and Morii [KM12a] gives a quantum key-recovery attack on EM ciphers with $\mathcal{O}(n)$ time complexity. They define the function $f(x) = Enc(x) \oplus P(x) = P(x \oplus k_1) \oplus P(x) \oplus k_2$. Obviously, it is a periodic function that satisfies $f(x \oplus k_1) = f(x)$.

Grover's Algorithm. The task is to find a marked element from a set X. We denote by $M \subseteq X$ the subset of marked elements. Classically, one solve the problem with time $|X|/|M|$. However, in a quantum computer, the problem is solve with high probability in time $\sqrt{|X|/|M|}$ using Grover's algorithm. The steps of the algorithm is as follows:

I. Initializing a n-bit register $|0\rangle^{\otimes n}$. One applies Hadamard transform to the first register to attain an equal superposition:

$$H^{\otimes n}|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle = |\varphi\rangle. \tag{2}$$

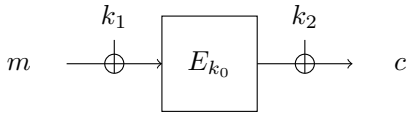

Figure 2 FX constructions

II. Construct an oracle $\mathcal{O}$: $|x\rangle \xrightarrow{\mathcal{O}} (-1)^{f(x)}|x\rangle$, where $f(x) = 1$ if x is the correct state, and $f(x) = 0$ otherwise.

III. Apply Grover iteration for $R \approx \frac{\pi}{4}\sqrt{2^n}$ times:

$$[(2|\varphi\rangle\langle\varphi| - I)\mathcal{O}]^R|\varphi\rangle \approx |x_0\rangle$$

IV. return x_0.

Later, Brassard *et al.* [BHMT00] generalized the Grover search as amplitude amplification.

Theorem 1. (Brassard, Hoyer, Mosca and Tapp [BHMT00]). Let $\mathcal{A}$ be any quantum algorithm on q qubits that uses no measurement. Let $\mathcal{B} : \mathbb{F}_2^q \to \{0, 1\}$ be a function that classifies outcomes of $\mathcal{A}$ as good or bad. Let $p > 0$ be the initial success probability that a measurement of $\mathcal{A}|0\rangle$ is good. Set $k = \lceil \frac{\pi}{4\theta} \rceil$, where θ is defined via $sin^2(\theta) = p$. Moreover, define the unitary operator $Q = -\mathcal{A}S_0\mathcal{A}^{-1}S_{\mathcal{B}}$, where the operator $S_{\mathcal{B}}$ changes the sign of the good state

$$|x\rangle \mapsto \begin{cases} -|x\rangle \text{ if } \mathcal{B}(x) = 1, \\ \ \ |x\rangle \text{ if } \mathcal{B}(x) = 0, \end{cases}$$

while S_0 changes the sign of the amplitude only for the zero state $|0\rangle$. Then after the computation of $Q^k\mathcal{A}|0\rangle$, a measurement yields good with probability a least $\max\{1\text{-}p, p\}$.

Assuming $|\varphi\rangle = \mathcal{A}|0\rangle$ is the initial vector, whose projections on the good and the bad subspace are denoted $|\varphi_1\rangle$ and $|\varphi_0\rangle$. The state $|\varphi\rangle = \mathcal{A}|0\rangle$ has angle θ with the bad subspace, where $sin^2(\theta) = p$. Each Q iteration increase the angle to 2θ. Hence, after $k \approx \frac{\pi}{4\theta}$, the angle roughly equals to $\pi/2$. Thus, the state after k iterations is almost orthogonal to the bad subspace. After measurement, it produces the good vector with high probability.

At Asiacrypt 2017, Leander and May [LM17] gave a quantum key-recovery attack on FX-construction shown in Figure 2: $Enc(x) = E_{k_0}(x + k_1) + k_2$. They introduce the function $f(k, x) = Enc(x) + E_k(x) = E_{k_0}(x + k_1) + k_2 + E_k(x)$. For the correct key guess $k = k_0$, we have $f(k, x) = f(k, x + k_1)$ for all x. However, for $k \neq k_0$, $f(k, \cdot)$ is not periodic. They combine Simon and Grover algorithm to attack FX ciphers (such as PRINCE [BCG+12], PRIDE [ADK+14], DESX) in the quantum-CPA model with complexity roughly 2^{32}.

3 Quantum Key-recovery Attacks on 5-Round Feistel Structures

Feistel structure is a very common way to build block ciphers. Here we give a 5-round quantum key-recovery attack on Feistel structure. As shown in Figure 3, F_i is the ith round function that absorbing independent round key k_i. Suppose the state size is n, then the length of k_i is $n/2$. Dinur *et al.* [DDKS15] recovers the full key $(k_1, k_2, k_3, k_4, k_5)$ of the 5-round Feistel cipher with 2^n classical queries on the cipher. In a quantum computer, one can use Grover search algorithm to find all the round keys with $2^{1.25n}$ quantum queries. So we have to construct a quantum algorithm that cost less time complexity than both 2^n and $2^{1.25n}$. Inspired by Leander and May's work [LM17], we combine Grover and Simon algorithm to find the round keys.

Kuwakado and Morii [KM10] introduced a quantum distinguish attack on 3-round Feistel scheme by using Simon algorithm. As shown in Figure 3, we place the 3-round distinguisher part in the dashed box.

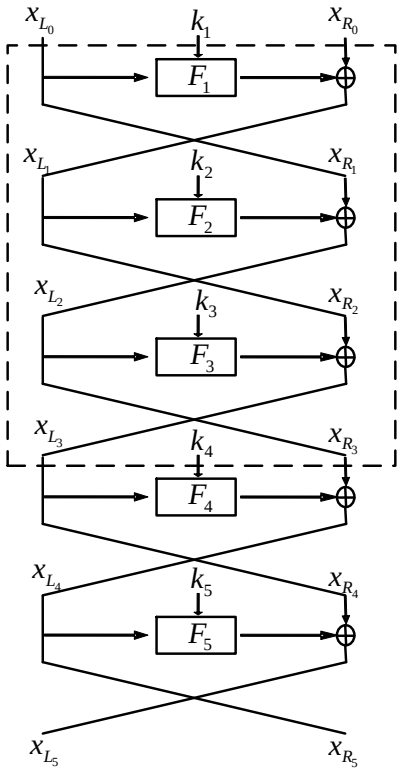

Figure 3 Quantum Key-recovery Attacks on 5-Round Feistel Structures

The following functions is defined:

$$f(b, x_{R_0}) = F_2(k_2, x_{R_0} \oplus F_1(k_1, \alpha_b)) = \alpha_b \oplus x_{R_3} = \alpha_b \oplus F_4(k_4, F_5(k_5, x_{R_5}) \oplus x_{L_5}) \oplus x_{R_5} \tag{3}$$

where $b \in \mathbb{F}_2$, $\alpha_b \in \mathbb{F}_2^{n/2}$ is arbitrary constant and $\alpha_0 \neq \alpha_1$, $(x_{L_5}||x_{R_5}) = Enc(\alpha_b||x_{R_0})$. It is easy to verify that $f(b, x_{R_0}) = f(b \oplus 1, x_{R_0} \oplus F_1(k_1, \alpha_0) \oplus F_1(k_1, \alpha_1))$. Therefore, with the right key guess (k_4, k_5), $f(b, x_{R_0}) = \alpha_b \oplus F_4(k_4, F_5(k_5, x_{R_5}) \oplus x_{L_5})$ has a nontrivial period $s = 1||F_1(k_1, \alpha_0) \oplus F_1(k_1, \alpha_1)$. However, if the guessed (k_4, k_5) is wrong, $f(b, x_{R_0})$ is a random function and not periodic with high probability.

Theorem 2. Let g: $\mathbb{F}_2^n \times \mathbb{F}_2^{n/2+1} \mapsto \mathbb{F}_2^{n/2}$ with

$$(k_4, k_5, y) \mapsto f(y) = f(b, x) = \alpha_b \oplus F_4(k_4, F_5(k_5, x_{R_5}) \oplus x_{L_5}) \oplus x_{R_5},$$

where α_0, α_1 are two arbitrary constants, $(x_{L_5}||x_{R_5}) = Enc(\alpha_b||x)$. Given quantum oracle to g and Enc, (k_4, k_5) and $F_1(k_1, \alpha_0) \oplus F_1(k_1, \alpha_1)$ could be computed with $n + (n+1)(n+2+2\sqrt{n/2+1})$ qubits and about $2^{n/2}$ quantum queries.

Under the right key guess k_4, k_5, $g(k_4, k_5, y) = g(k_4, k_5, y \oplus s)$. Let, h: $\mathbb{F}_2^n \times \mathbb{F}_2^{(n/2+1)^l} \mapsto \mathbb{F}_2^{(n/2)^l}$ with

$$(k_4, k_5, y_1, ..., y_l) \mapsto g(k_4, k_5, y_1)||...||g(k_4, k_5, y_l). \tag{4}$$

Let U_h be a quantum oracle that maps

$$|k_4, k_5, y_1, ..., y_l, \mathbf{0}, ..., \mathbf{0}\rangle \mapsto |k_4, k_5, y_1, ..., y_l, h(k_4, k_5, y_1, ..., y_l)\rangle. \tag{5}$$

We construct the following quantum algorithm $\mathcal{A}$.

1. Preparing the initial $(n + (n/2+1)l + nl/2)$-qubit state $|\mathbf{0}\rangle$.
2. Apply Hadamard $H^{\otimes n+(n/2+1)l}$ on the first $n + (n/2+1)l$ qubits resulting in
$$\sum_{k_4, k_5 \in \mathbb{F}_2^{n/2}, y_1, ..., y_l \in \mathbb{F}_2^{n/2+1}} |k_4, k_5\rangle |y_1\rangle ... |y_l\rangle |\mathbf{0}\rangle, \tag{6}$$
where we omit the amplitudes $2^{-(n+(n/2+1)l)/2}$.
3. Applying U_h to the above state, we get:
$$\sum_{k_4, k_5 \in \mathbb{F}_2^{n/2}, y_1, ..., y_l \in \mathbb{F}_2^{n/2+1}} |k_4, k_5\rangle |y_1\rangle ... |y_l\rangle |h(k_4, k_5, y_1, ..., y_l)\rangle. \tag{7}$$
4. Apply Hadamard to the qubits $|y_1\rangle ... |y_l\rangle$ of the above state, we get:
$$|\varphi\rangle = \sum_{k_4, k_5 \in \mathbb{F}_2^{n/2}, u_1, ..., u_l, y_1, ..., y_l \in \mathbb{F}_2^{n/2+1}} |k_4, k_5\rangle (-1)^{\langle u_1, y_1\rangle} |u_1\rangle ... (-1)^{\langle u_l, y_l\rangle} |u_l\rangle |h(k_4, k_5, y_1, ..., y_l)\rangle. \tag{8}$$

If the guessed k_4, k_5 is right, after measurement of $|\varphi\rangle$, the period s is orthogonal to all the $u_1, ..., u_l$. According to Lemma 4 of [LM17], choosing $l = 2(n/2 + 1 + \sqrt{n/2+1})$ is enough to compute a unique s .

Without measurement and considering the superposition $|\varphi\rangle$, assume that we had a classifier $\mathcal{B}$: $\mathbb{F}_2^{n+(n/2+1)l} \mapsto \{0, 1\}$, which partitions $|\varphi\rangle$ into a good subspace and a bad subspace: $|\varphi\rangle = |\varphi_1\rangle + |\varphi_0\rangle$, where $|\varphi_1\rangle$ and $|\varphi_0\rangle$ denotes the projection onto the good subspace and bad subspace, respectively. For the good one $|x\rangle$, $\mathcal{B}(x) = 1$.

In detail, we define $|\varphi_1\rangle$ as the sum of those basis states under the right key guessing of k_4, k_5. However, the correctness of k_4, k_5 could not be checked directly. The classifier $\mathcal{B}$ could compute the period s of $g(k_4, k_5, \cdot)$ by $k_4, k_5, u_1, ..., u_l$, and check if $g(k_4, k_5, y) = g(k_4, k_5, y \oplus s)$ for a given y.

Classifier $\mathcal{B}$. Define $\mathcal{B} : \mathbb{F}_2^{n+(n/2+1)l} \mapsto \{0, 1\}$ that maps $(k_4, k_5, u_1, ..., u_l) \mapsto \{0, 1\}$.

1. Let $\overline{U} = \langle u_1, ..., u_l \rangle$ be the linear span of all u_i. If $dim(\overline{U}) \neq n/2$, output 0. Else, use Lemma 4 of [LM17] to compute the unique period s.
2. Check $g(k_4, k_5, y) = g(k_4, k_5, y \oplus s)$ for a random given y. If the identity holds, output 1. Else output 0.

We classify a state $|k_4, k_5\rangle|u_1\rangle...|u_l\rangle$ is good iff $\mathcal{B}(k_4, k_5, u_1, ..., u_l) = 1$. If we measure $|\varphi\rangle$, it produces the good state with probability p.

$$\begin{aligned} p &= \Pr[|k_4, k_5\rangle|u_1\rangle...|u_l\rangle \text{ is good}] \\ &= \Pr\left|(k_4, k_5) \text{ is right}\right] \cdot \Pr[\mathcal{B}(k_4, k_5, u_1, ..., u_l) = 1|(k_4, k_5) \text{ is right}] \approx 2^{-n} \end{aligned} \tag{9}$$

Our classifier $\mathcal{B}$ defines a unitary operator $S_{\mathcal{B}}$ that conditionally change the sign of the quantum states:

$$|k_4, k_5\rangle|u_1\rangle...|u_l\rangle \mapsto \begin{cases} -|k_4, k_5\rangle|u_1\rangle...|u_l\rangle \text{ if } \mathcal{B}(k_4, k_5, u_1, ..., u_l) = 1, \\ \ \ |k_4, k_5\rangle|u_1\rangle...|u_l\rangle \text{ if } \mathcal{B}(k_4, k_5, u_1, ..., u_l) = 0. \end{cases} \tag{10}$$

The complete amplification process is realized by repeatedly for t times applying the unitary operator $Q = -\mathcal{A}S_0\mathcal{A}^{-1}S_{\mathcal{B}}$ to the state $|\varphi\rangle = \mathcal{A}|0\rangle$, i.e. $Q^t\mathcal{A}|0\rangle$.

Initially, the angle between $|\varphi\rangle = \mathcal{A}|0\rangle$ and the bad subspace $|\varphi_0\rangle$ is θ, where $sin^2(\theta) = p = \langle\varphi_1|\varphi_1\rangle$. When p is smaller enough, $\theta \approx arcsin(\sqrt{p}) \approx 2^{-\frac{n}{2}}$. According to Theorem 1, after $k = \lceil \frac{\pi}{4\theta} \rceil = \lceil \frac{\pi}{4\times 2^{-\frac{n}{2}}} \rceil$ Grover iterations Q, the angle between resulting state and the bad subspace is roughly $\pi/2$. The probability P_{good} that the measurement yields a good state is about $sin^2(\pi/2) = 1$.

The whole attack needs $(n + (n/2 + 1)l + nl/2) = n + (n + 1)(n + 2 + 2\sqrt{n/2 + 1})$ qubits. About $k = \lceil \frac{\pi}{4\times 2^{-\frac{n}{2}}} \rceil = 2^{n/2}$ quantum queries are required. Similarly, we can recover k_1, k_2 by placing the 3-round quantum distinguisher in the last three rounds, that means the decryption quantum oracle of the 5-round Feistel structure is required.

The quantum key-recovery attacks on 7/8/15/31/32-round Feistel structures are similar to the 5-round attack. The results are summarised in Table 1.

4 Conclusion

In this paper, we for the first time consider the quantum key-recovery attack against Feistel structures. Inspired by Leander and May's works, we combine Grover and Simon algorithm to construct the attack. Our attacks requires $2^{nr/4-3n/4}$ quantum queries. When comparing with the quantum brute force search, the time complexity is reduced by a factor of $2^{0.75n}$. When comparing with the best classical attacks, the time complexity is reduced by a factor $2^{0.5n}$ without any memory cost.

Conflict of interest The authors declare that they have no conflict of interest.

References

ADK+14 Martin R Albrecht, Benedikt Driessen, Elif Bilge Kavun, Gregor Leander, Christof Paar, and Tolga Yalcin. Block ciphers focus on the linear layer (feat. pride). pages 57–76, 2014.

BCG+12 Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R. Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, Peter Rombouts, Søren S. Thomsen, and Tolga Yalçin. PRINCE - A Low-Latency Block Cipher for Pervasive Computing Applications - Extended Abstract. In Xiaoyun Wang and Kazue Sako, editors, *ASIACRYPT 2012*, volume 7658 of *Lecture Notes in Computer Science*, pages 208–225. Springer, 2012.

BHMT00 Gilles Brassard, Peter Hoyer, Michele Mosca, and Alain Tapp. Quantum amplitude amplification and estimation. *arXiv: Quantum Physics*, 2000.

BZ13 Dan Boneh and Mark Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. pages 361–379, 2013.

DDKS15 Itai Dinur, Orr Dunkelman, Nathan Keller, and Adi Shamir. New attacks on feistel structures with improved memory complexities. In *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I*, pages 433–454, 2015.

EM93 Shimon Even and Yishay Mansour. *A construction of a cipher from a single pseudorandom permutation*, pages 210–224. Springer Berlin Heidelberg, Berlin, Heidelberg, 1993.

FNS75 H Feistel, W A Notz, and J L Smith. Some cryptographic techniques for machine-to-machine data communications. *Proceedings of the IEEE*, 63(11):1545–1554, 1975.

Gro96 Lov K Grover. A fast quantum mechanical algorithm for database search. *symposium on the theory of computing*, pages 212–219, 1996.

Int10 International Organization for Standardization(ISO). International Standard- ISO/IEC 18033-3, Information technology-Security techniques-Encryption algorithms -Part 3: Block ciphers. 2010.

KLLN16 Marc Kaplan, Gaetan Leurent, Anthony Leverrier, and Maria Nayaplasencia. Breaking symmetric cryptosystems using quantum period finding. *international cryptology conference*, 9815:207–237, 2016.

KM10 Hidenori Kuwakado and Masakatu Morii. Quantum distinguisher between the 3-round feistel cipher and the random permutation. *International symposium on information theory*, pages 2682–2685, 2010.

KM12a H. Kuwakado and M. Morii. Security on the quantum-type even-mansour cipher. In *2012 International Symposium on Information Theory and its Applications*, pages 312–316, Oct 2012.

KM12b Hidenori Kuwakado and Masakatu Morii. Security on the quantum-type even-mansour cipher. *International symposium on information theory and its applications*, pages 312–316, 2012.

LM17 Gregor Leander and Alexander May. Grover meets simon - quantumly attacking the fx-construction. In *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part II*, pages 161–178, 2017.

LR88 Michael G Luby and Charles Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM Journal on Computing*, 17(2):373–386, 1988.

Sho97 Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

Sim97 Daniel R. Simon. On the power of quantum computation. *SIAM Journal on Computing*, 26(5):1474–1483, 1997.

TP17 Tsuyoshi Takagi and Thomas Peyrin, editors. *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings*, volume 10624 of *Lecture Notes in Computer Science*. Springer, 2017.