Quantum Key Recovery Attacks on 4-round Iterated Even-Mansour with Two Keys

Ravi Anand[1], Shibam Ghosh[2], Takanori Isobe[3], and Rentaro Shiba[4,5]

[1] Indrapastha Institute of Information Technology Delhi, Delhi, India
ravi.anand@iiit.ac.in
[2] Computer Science Department, University of Haifa, Haifa, Israel
sghosh03@campus.haifa.ac.il
[3] University of Hyogo, Kobe, Japan
takanori.isobe@ai.u-hyogo.ac.jp
[4] Mitsubishi Electric Corporation, Kamakura, Japan
[5] Nagoya University, Nagoya, Japan
shiba.rentaro.k7@s.mail.nagoya-u.ac.jp

Abstract. In this paper, we propose quantum key recovery attacks on 4-round iterated Even-Mansour (IEM) with a key schedule that applies two keys alternately. We first show that a conditional periodic function such that one of the secret keys appears as a period conditionally can be constructed using the encryption function and internal permutations. By applying the offline Simon's algorithm to this function, we construct a key recovery attack with a complexity of $O(\sqrt{N}\log N)$ for $N = 2^n$, where n is the block size and one secret key size. Using quantum queries, this attack outperforms the generic quantum attack, *i.e.*, Grover's search which takes the time complexity of $O(N)$. Moreover, we propose the quantum version of the multibridge attack proposed by Dinur *et al.* in ASIACRYPT 2014 to analyze the 4-round IEM. As a result, we show that the quantum multibridge attack can achieve the optimal complexity of $O(N)$ even if we have only $O(1)$ data without quantum queries, while the classical attack requires $O(N)$ data to achieve the same time complexity. Furthermore, we show that the quantum multibridge attack slightly outperforms Grover's search when considering the quantum circuit depth for these attacks.

Keywords: Cryptanalysis, quantum attack, multibridge attack, iterated Even-Mansour

1 Introduction

The Even-Mansour (EM) scheme [13] is a well-known approach for constructing a block cipher E from a public pseudo-random permutation $P : \{0,1\}^n \mapsto \{0,1\}^n$ and two n-bit keys $\mathsf{K}_0, \mathsf{K}_1$. The Even-Mansour (EM) cipher $E : \{0,1\}^{2n} \times \{0,1\}^n \mapsto \{0,1\}^n$ is defined as:

$$E_{\mathsf{K}_0,\mathsf{K}_1}(x) = P(x \oplus \mathsf{K}_0) \oplus \mathsf{K}_1$$

The EM cipher has been studied intensively due to its simplicity and security has been discussed in both classical and quantum settings.

The structure obtained by iterating an EM scheme is called an Iterated Even-Mansour (IEM) scheme, which is also referred to as an abstraction of many concrete block ciphers. Given r permutations $P_1, \ldots, P_r : \{0,1\}^n \mapsto \{0,1\}^n$, and the secret key $\mathsf{K} = \mathsf{K}_0 || \mathsf{K}_1 || \cdots || \mathsf{K}_r \in \{0,1\}^{(r+1)n}$, the r-round IEM cipher is defined as follows:

$$E_{\mathsf{K}}(x) = P_r(P_{r-1}(\cdots P_1(x \oplus \mathsf{K}_0) \cdots)) \oplus \mathsf{K}_r. \tag{1}$$

Analyzing the security of the IEM ciphers is useful for deriving lower bounds on the number of queries and the computational cost required for the attacks since its internal permutations correspond to the round functions of concrete block ciphers and are assumed to be random. Moreover, the security of IEM ciphers varies depending on the number of permutations used and the key schedule, making it very useful for determining the foundational constructions of block ciphers.

To date, various security analyses have been proposed for several variants of EM and IEM ciphers. In [8], Chen and Steinberger analyzed the tight security bound of Eq. (1) and proved that it is $2^{\frac{r}{r+1}n}$. In [11], Dinur *et al.* proposed the *multibridge attack* for recovering the secret key of the 4-round variants of the IEM ciphers with two independent n-bit keys. They showed that the secret key of 4-round 2-key IEM ciphers can be recovered with the optimal complexity of $N = 2^n$, and the trade-off curve of $DT = N^2$ can be obtained by applying the multibridge attack. [9,12].

In the case of quantum security, Kuwakado and Morii [21] was the first to show that a 1-round 2-key EM cipher can be attacked using Simon's algorithm with the time complexity of $O(\log N)$ in the Q2 model. The same paper also shows that the keys of this scheme can be recovered with time complexity of $O(N^{1/3})$ and a qRAM of size $O(N^{1/3})$ by applying a quantum collision search algorithm [6] in the Q1 model. Leander and May [22] described a method to combine the quantum algorithms of Simon and Grover, termed Grover-meets-Simon (GMS), and it can be applied to the analysis of FX constructions. In [2], the offline Simon's algorithm was proposed. The offline Simon's algorithm is a variant of GMS where the quantum state the attacker wants to evaluate is prepared at the beginning of the algorithm. The authors showed that the offline Simon's algorithm can recover the keys of 1-round 2-key EM with $O(N^{1/3} \log N)$ time complexity and $O(\log N)$ quantum memory.

1.1 Motivation

As mentioned above, the quantum security of EM has been intensively studied. On the other hand, for IEM schemes, although several studies on the quantum security are conducted [18,7,3,26], it is insufficient because of the large number of variants. Specifically, for the 4-round IEM with two keys (*i.e.*, $2n$-bit secret key), which was analyzed classically by Dinur *et al.* [11], the efficient key recovery

attacks using quantum algorithms have not been proposed, despite the fact that the similar construction is used as the basis of several block ciphers such as LED-128 [17] PRINCE v2 [4] and QARMA v2 [1]. Thus, in this paper, we analyze the quantum key recovery security of this construction. For simplicity, we refer to this IEM cipher as 4-IEM in the rest of the paper. We will briefly describe the construction of 4-IEM in Section 2.1.

1.2 Our Contribution

Our aim in this paper is to analyze the security of 4-IEM, which uses four permutations P_1, P_2, P_3, P_4 and the $2n$-bit master key $\mathsf{K} = \mathsf{K}_0||\mathsf{K}_1$ with the alternating key schedule. In the rest of the paper, we denote the classical and quantum data complexities and the classical and quantum time complexities as D_C, D_Q, T_C, and T_Q, respectively. Here, the quantum data complexity D_Q indicates the number of quantum queries.

In this paper, we propose efficient quantum attacks on 4-IEM. One of our attacks is based on the offline Simon's algorithm [2], a quantum search algorithm that employs Simon's algorithm as a subroutine. We show that the conditional periodic function can be constructed by exploiting the construction of 4-IEM. Since this function has a period that becomes the true value of one of the secret keys under the condition that the guess of another key value is correct, we can search two keys by using the offline Simon's algorithm [2] with quantum queries. As a result, we show that two keys of 4-IEM can be identified with the complexity of $T_Q = \sqrt{N} \log N$ and $D_Q = \log N$. Moreover, we show that this attack can be converted to the quantum attack in the Q1 model under the assumption that the attacker can make a superposition of all possible plaintext and ciphertext pairs by only classical queries, *i.e.*, the attacker can have the full codebook. Although this requires $D_C = N$ classical queries and matches the quantum time complexity of Grover's search, some advantages might be gained in some settings since the number of quantum computations can be reduced. We also show the application of the offline Simon's algorithm based attack to LED-128 [17].

Furthermore, we also propose a quantum adaptation of the multibridge attack presented in [11] dubbed the quantum multibridge attack to 4-IEM in the Q1 model. We show how to incorporate quantum computations to enhance the efficiency of the classical multibridge attack. As a result, we show that the quantum multibridge attack can achieve the complexity of $T_Q = N$ even if $D_C = 1$, and the time complexity is independent of the data complexity, while the classical one requires $D_C = N$ data to achieve $T_C = N$. This complexity matches Grover's search. However, considering the depth of quantum circuits, the time complexity of the quantum multibridge attack becomes $T_Q = N/2$ when we consider the complexity of Grover's search as $T_Q = N$, since the quantum multibridge attack requires only $O(1)$ evaluations for full-round encryptions. Table 1 summarizes the results of our study.

Paper Organization The rest of the paper is structured as follows: Section 2 briefly describes 4-IEM, basis of quantum computation and algorithms, and the

Table 1: Comparison of the optimal complexities. (The time quantum complexity of the quantum multibridge attack is relative to Grover's algorithm when considering the depth of the quantum circuit.)

Method	Setting	Classical Data (D_C)	Classical Time (T_C)	Quantum Data (D_Q)	Quantum Time (T_Q)	Trade-off	Reference
Multibridge	Classical	N	N	-	-	$DT = N^2$	[11]
Grover (Generic)	Q1 / Q2	1	-	-	N	-	[16]
Offline Simon's	Q2	-	-	$\log N$	$\sqrt{N}\log N$	-	Section 3
Offline Simon's with full codebook	Q1	N	N	-	$\sqrt{N}\log N$	-	Section 3
Quantum Multibridge	Q1	1	-	-	$N/2$	-	Section 4

previous attack against 4-IEM. In Section 3, we show a quantum attack on 4-IEM using the offline Simon's algorithm. In Section 4, we propose the quantum multibridge attack. After that, we conclude the paper in Section 5.

2 Preliminaries

2.1 Iterated Even-Mansour Schemes with Two Keys

In this paper, we focus on the 4-IEM cipher that uses two independent n-bit keys K_0 and K_1, i.e., a $2n$-bit master key $\mathsf{K} = \mathsf{K}_0||\mathsf{K}_1$. The two keys K_0 and K_1 are XOR-ed alternately as shown in Fig. 1.

$$E_{\mathsf{K}}(x) = P_4(P_3(P_2(P_1(x \oplus \mathsf{K}_0) \oplus \mathsf{K}_1) \oplus \mathsf{K}_0) \oplus \mathsf{K}_1) \oplus \mathsf{K}_0.$$

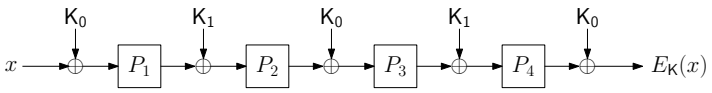

Fig. 1: 4-round IEM with alternating two keys (4-IEM)

This type of key schedule is used for some block cipher instances, such as LED-128, PRINCE v2 and QARMA v2.

2.2 Basis of Quantum Computation

We assume that the readers have some basic knowledge of quantum computation. For more details, see [23]. In the following, we will give brief explanations about quantum adversary models, some quantum algorithms, and qRAM.

Quantum Adversary Models Quantum attacks are performed by an attacker who possesses a quantum computer and utilizes quantum computation. In [25], Zhandry shows that there are two quantum adversary models, depending on the capabilities of the adversary.

Q1 model The adversary can perform offline quantum computation and online classical queries.

Q2 model The adversary can perform offline quantum computation and quantum superposition queries.

The Q1 model is considered more realistic than the Q2 model. Despite their lack of apparent practicality, attacks obtained in the Q2 model are of particular interest as they are powerful attacks, often with very low cost.

Quantum Amplitude Amplification (QAA) Quantum amplitude amplification (QAA) was introduced by Brassard, Høyer and Tapp [5], which will be used in the attacks described in this paper. QAA is a quantum search algorithm, and it can be viewed as a generalized version of Grover's algorithm [16].

Theorem 1 ([5]). *Let $\chi : \{0,1\}^n \to \{0,1\}$ be a boolean function, and $G = \{x|\chi(x) = 1\}$ be a set of good elements and $B = \{x|\chi(x) = 0\}$ be a set of bad elements. Assume $\mathcal{A}$ is a quantum algorithm on n qubits, without measurement, that applied to an initial zero state produces the superposition: $\mathcal{A}|0\rangle = \sum_{x\in G} \alpha_x |x\rangle + \sum_{y\in B} \alpha_y |y\rangle$. Let $a = \sum_{x\in G} |\alpha_x|^2 > 0$ be the probability of obtaining a good element x if we measure $\mathcal{A}|0\rangle$. Furthermore, let the unitary operators $\mathcal{S}_\chi$ and $\mathcal{S}_0$ be defined as follows:*

$$\mathcal{S}_\chi : |x\rangle \mapsto \begin{cases} -|x\rangle & \text{if } x \in G \\ |x\rangle & \text{if } x \in B \end{cases}, \mathcal{S}_0 : |x\rangle \mapsto \begin{cases} -|x\rangle & \text{if } x = 0 \\ |x\rangle & \text{otherwise} \end{cases}$$

Define $\mathbf{Q} = -\mathcal{A}\mathcal{S}_0\mathcal{A}^{-1}\mathcal{S}_\chi$ and set $m = \lfloor \frac{\pi}{4\theta_a} \rfloor$, where $\theta_a \in [0, \pi/2]$ is the constant defined by $\sin^2\theta_a = a$. Then, if we compute $\mathbf{Q}^m\mathcal{A}|0\rangle$ and measure the system, the result is a good element with probability at least $\max(1-a, a)$.

We represent the operation $\mathbf{Q} = -\mathcal{A}\mathcal{S}_0\mathcal{A}^{-1}\mathcal{S}_\chi$ in two phases. The algorithm $\mathcal{A}$ is called the SETUP phase, and $\mathcal{S}_\chi$ is called the FLIP phase. Thus, the whole procedure is denoted as

$$\mathsf{QAA}(\mathsf{SETUP}, \mathsf{FLIP}) = \mathsf{QAA}(\mathcal{A}, \mathcal{S}_\chi),$$

which is equivalent to $\mathbf{Q}^m\mathcal{A}$. Grover's algorithm is the special case when $H^{\otimes n}$ is used as $\mathcal{A}$. In this paper, whenever we use QAA, we give a proper description of the SETUP and FLIP phases. Besides, we set the iteration number m to $1/\sqrt{a}$ where a good element can be measured with an overwhelming probability.

Simon's Algorithm Simon's algorithm [24] is a quantum algorithm for finding hidden Boolean period in a function. Simon's algorithm aims to solve the following problem.

Problem 1. Given a function $f : \{0,1\}^n \mapsto \{0,1\}^n$, find $\mathsf{S} \in \{0,1\}^n \setminus \{0\}^n$ such that $f(x) = f(x \oplus \mathsf{S})$.

Simon's algorithm finds S in $O(\log N)$, where solving this problem with classical oracle access to f requires $N^{1/2}$ queries to f.

For several cryptographic constructions, Simon's algorithm may obtain the secret key directly as the period S or obtain effective secret information for attacks. The subroutine for Simon's algorithm is as follows:

1. Prepare $n+1$ qubits. Consider the first n qubits as the first register and the last 1 qubit as the second register:$|0\rangle^{\otimes n} |0\rangle$
2. Apply $H^{\otimes n}$ to the first register: $\sum_{x\in\{0,1\}^n} |x\rangle |0\rangle$
3. Make a quantum query to f: $\sum_{x\in\{0,1\}^n} |x\rangle |f(x)\rangle$
4. Measure the second register and the state of the second register is collapsed to a constant a: $\sum_{x\in\{0,1\}^n|f(x)=a} |x\rangle |a\rangle$
5. Apply H to the first register: $\sum_{y\in\{0,1\}^n} \sum_{x\in\{0,1\}^n|f(x)=a} (-1)^{x\cdot y} |y\rangle |a\rangle$
6. Measure the first register to get a value of y.

We omitted the normalized values of superpositions for simplicity. We repeat the subroutine above $O(\log N)$ times to get a set of values $Y = \{y : y \cdot \mathsf{S} = 0\}$. By using the set, we can find S from this Y if the system Y is not full rank.

Grover-Meets-Simon Grover-Meets-Simon (GMS) algorithm [22], was proposed as a combination of Grover algorithm and Simon algorithm. The core idea of GMS is to check periodic property as a condition inside Grover algorithm. This was proposed to analyze FX schemes in the Q2 model. FX schemes [19,20] are defined as $\mathsf{FX}_{\mathsf{K},\mathsf{K}_{\rm in},\mathsf{K}_{\rm out}}(x) = E_{\mathsf{K}}(x \oplus \mathsf{K}_{\rm in}) \oplus \mathsf{K}_{\rm out}$ where E_{K} is a secure block cipher. GMS consists of an outer loop of Grover's algorithm and an inner subroutine of Simon's algorithm. We describe the core algorithm with the following function:

$$f(\mathsf{K}, x) = \mathsf{FX}_{\mathsf{K},\mathsf{K}_{\rm in},\mathsf{K}_{\rm out}(x)} \oplus E_{\mathsf{K}}(x) = E_{\mathsf{K}}(x \oplus \mathsf{K}_{\rm in}) \oplus \mathsf{K}_{\rm out} \oplus E_{\mathsf{K}}(x)$$

Note that, only if K is the correct key, $f(\mathsf{K}, \cdot)$ is periodic as $f(\mathsf{K}, x) = f(\mathsf{K}, x \oplus \mathsf{K}_{\rm in})$ with period $\mathsf{K}_{\rm in}$. Thus, one can use Grover search over K with the periodicity of $f(\mathsf{K}, \cdot)$ as a testing condition inside Grover iteration.

The Offline Simon's Algorithm The offline Simon's algorithm [2] is a variant of the GMS. Unlike GMS, we first make a superposition as a database by making queries of the target constructions. In the superposition, all the possible inputs and corresponding outputs of the target algorithm are included. The superposition can also be created from offline queries, and it allows for the elimination of superposition queries. Thus, the offline Simon's algorithm can be used also in the $Q1$ model.

qRAM The quantum random access memory (qRAM) is a quantum operator that represents the behavior of classical RAM. Assume that there is a data array $\{x_1, x_2 \cdots x_M\}$, where M is the number of elements. Then, the qRAM is an efficient implementation achieving the following unitary:

$$|i\rangle |y\rangle \rightarrow |i\rangle |y \oplus x_i\rangle$$

where x_i is an element stored in the position of address i in qRAM. We define this operation as qRAM Read. This operation can be performed with a superposition of all addresses.

2.3 Multibridge Attack

Dinur *et al.* [11] proposed the multibridge attack on 4-IEM cipher and showed that the master key of this cipher can be recovered with the complexity of D_C=T_C=N. Similar to the dissection technique, this method dissects the cipher into four parts that are processed separately. However, unlike dissection, the parts are not sequential but instead nested. After that, like the splice-and-cut technique, it connects or bridges two outer parts and two inner parts based on the intermediate encryption values of the cipher. Finally, the attack exploits a self-similarity property of the cipher to connect another pair of intermediate encryption values using another bridge. In the multibridge attack, the attacker assumed that the relation shown in Fig. 2 holds for a fixed constant Δ. The attack works as follows:

1. At first, query D_C plaintexts x to the encryption oracle E_{K} and compute $d(x) = x \oplus E_{\mathsf{K}}(x)$. For each x, store $(d(x), x)$ in a table L_1.
2. For each of the N/D_C arbitrary values of Δ:
   (a) Let the value after P_1 be α. For each of the N possible values of α:
      i. Assume that the value before P_4 is $\alpha \oplus \Delta$. Compute $P_1^{-1}(\alpha) \oplus P_4(\alpha \oplus \Delta)$ and search for matches with this values of $d(x)$ in L_1 (This is the first *bridge*, denoted in red in Fig. 2 that connects intermediate values, after P_1 and before P_4, respectively).
      ii. For each match, obtain x_j and compute $\hat{\mathsf{K}}_0 = x_j \oplus P_1^{-1}(\alpha)$ as a possible value of K_0 and store $\hat{\mathsf{K}}_0$ in L_2, next to α.
   (b) Let the value before P_2 be β. For each of the N possible values of β:
      i. From the self-similarity of the cipher, the value after P_3 is $\beta \oplus \Delta$. Compute $\hat{\mathsf{K}}_0 = P_2(\beta) \oplus P_3^{-1}(\beta \oplus \Delta)$ and search for matches in L_2 (This is the second *bridge*, denoted in blue in Fig. 2 that connects intermediate values, before P_2 and after P_3, respectively).
      ii. For each match, obtain α and calculate $\hat{\mathsf{K}}_1 = \alpha \oplus \beta$ as a possible value of K_1.
      iii. Test the suggested key pair $(\hat{\mathsf{K}}_0, \hat{\mathsf{K}}_1)$ by trial encryptions, and if it succeeds, return it.

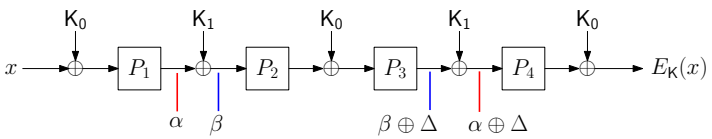

Fig. 2: Multibridge attack on 4-IEM

In this attack, the attacker tries to independently guess K_0 and K_1 for N/D_C constants Δ. Each key is guessed from an intermediate value which takes N possible values. Thus, the data complexity of the attack is D_C and the time complexity of attack is $T_C = (N/D_C)(N + N) \approx N^2/D_C$. The complexity is optimal when $D_C = T_C = N$.

3 Quantum Key Recovery Attack on 4-IEM

In this section, we introduce a quantum key recovery attack on 4-IEM that leverages the offline Simon's algorithm. This algorithm can be utilized within the Q1 model for certain cryptographic constructions, as it enables the elimination of quantum queries in Grover-Meets-Simon (GMS) algorithm by utilizing a superposition created through offline queries. However, for our initial attack on 4-IEM, we are unable to reduce the number of queries below N. Consequently, we primarily focus on the scenario where the attacker generates the initial superposition via quantum queries, referred to as the Q2 model. We employ the offline Simon's algorithm in our attack, ensuring its applicability within the Q1 model, as will be demonstrated later in this section.

For our first attack, consider the following two functions F and G constructed from 4-IEM encryption and internal permutations and their inverses as

$$F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n, F(\kappa, x) = P_3(P_2(x) \oplus \kappa),$$
$$G : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n, G(\kappa, x) = P_4^{-1}(E_{\mathsf{K}}(P_1^{-1}(x) \oplus \kappa) \oplus \kappa).$$

G includes an offline computation of E_{K}. Furthermore, for simplicity we write $F(\kappa, \cdot) = f_\kappa(\cdot)$ and $G(\kappa, \cdot) = g_\kappa(\cdot)$ in the parametrized form with respect to the parameter $\kappa \in \{0,1\}^n$. Note that, when $\kappa = \mathsf{K}_0$, *i.e.*, κ is a right value, we can rewrite g_{K_0} as

$$\begin{aligned} g_{\mathsf{K}_0}(x) &= P_4^{-1}(E_{\mathsf{K}}(P_1^{-1}(x) \oplus \mathsf{K}_0) \oplus \mathsf{K}_0) \\ &= P_4^{-1}(P_4(P_3(P_2(P_1(P_1^{-1}(x) \oplus \mathsf{K}_0 \oplus \mathsf{K}_0) \oplus \mathsf{K}_1) \oplus \mathsf{K}_0) \oplus \mathsf{K}_1) \oplus \mathsf{K}_0 \oplus \mathsf{K}_0) \\ &= P_3(P_2(x \oplus \mathsf{K}_1) \oplus \mathsf{K}_0) \oplus \mathsf{K}_1 \end{aligned}$$

Thus, if we set $\kappa = \mathsf{K}_0$, we get

$$f_{\mathsf{K}_0}(x) \oplus g_{\mathsf{K}_0}(x) = P_3(P_2(x) \oplus \mathsf{K}_0) \oplus P_3(P_2(x \oplus \mathsf{K}_1) \oplus \mathsf{K}_0) \oplus \mathsf{K}_1.$$

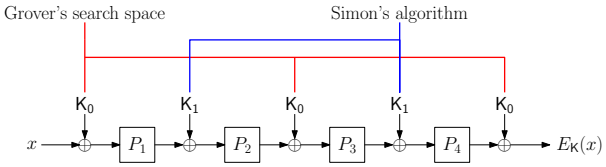

Fig. 3: Application of GMS to 4-IEM

This implies that, for the correct value of $\kappa = \mathsf{K}_0$, $(F \oplus G)(\mathsf{K}_0, x) = f_{\mathsf{K}_0} \oplus g_{\mathsf{K}_0}(x)$ is a periodic function with period K_1. Thus, we can apply Grover-meets-Simon(GMS) [22] or the offline Simon's algorithm [2] as shown in Fig. 3.

In our algorithm, the attacker is required to query both of the plaintexts and K_0 because the starting point of this algorithm is the value after P_1. In the Q2 model, the attacker is assumed to perform quantum queries. Therefore, the attacker can query to the plaintexts space and K_0 space. The attack procedure is as follows:

1. For a small constant $c\,(\geq 1)$, we start from the following superposition:

$$\bigotimes^{cn} \left(\sum_{x \in \{0,1\}^n} |x\rangle \, |g_\kappa(x)\rangle \right) \otimes \sum_{\kappa \in \{0,1\}^n} |\kappa\rangle$$

2. Using cn superposition queries to f, the following superposition state can be obtained:

$$\bigotimes^{cn} \left(\sum_{x \in \{0,1\}^n} |x\rangle \, |f_\kappa \oplus g_\kappa(x)\rangle \right) \otimes \sum_{\kappa \in \{0,1\}^n} |\kappa\rangle$$

3. After applying $(H^{\otimes n} \otimes I_n)^{cn}$, we have:

$$\left(\sum_{x_1, u_1} (-1)^{u_1 \cdot x_1} \, |u_1\rangle \, |(f_\kappa \oplus g_\kappa)(x_1)\rangle \right) \otimes \cdots \otimes \left(\sum_{x_{cn}, u_{cn}} (-1)^{u_{cn} \cdot x_{cn}} \, |u_{cn}\rangle \, |(f_\kappa \oplus g_\kappa)(x_{cn})\rangle \right) \otimes \sum_{\kappa \in \{0,1\}^n} |\kappa\rangle \, .$$

4. Define the following Boolean function H_{GMS} and a FLIP operator $\mathcal{S}_{H_{GMS}}$ over the domain of κ:

$$H_{GMS}(\kappa) = \begin{cases} 1, \text{ if } f_\kappa \oplus g_\kappa \text{ is periodic} \\ 0, \text{ otherwise} \end{cases} , \mathcal{S}_{H_{GMS}} : |\kappa\rangle = \begin{cases} -|\kappa\rangle, \text{ if } H_{GMS}(\kappa) = 1 \\ |\kappa\rangle, \text{ if } H_{GMS}(\kappa) = 0. \end{cases}$$

The quantum subroutine of H_{GMS} performs Simon's algorithm to check if $(f_\kappa \oplus g_\kappa)$ is periodic or not. In H_{GMS}, the dimension d of the vector space spanned by $u_1, \ldots, u_{cn}$ is computed.

If $d < n$, $f_\kappa \oplus g_\kappa$ is periodic for the input κ and H_{GMS} returns 1, otherwise $f_\kappa \oplus g_\kappa$ is not periodic for the input and $H_{GMS}(\kappa)$ returns 0. The FLIP operator $\mathcal{S}_{H_{GMS}}$ flips the phase if $H_{GMS} = 1$. After constructing this function, amplify the amplitude of $|\kappa\rangle$ such that $f_\kappa \oplus g_\kappa$ is periodic.

5. After identifying the K_0, fix $\kappa = \mathsf{K}_0$ and apply single Simon's algorithm to $f_{\mathsf{K}_0} \oplus g_{\mathsf{K}_0}$. As K_0 is assumed to be known in this step, the simple application of Simon's algorithm can identify K_1.

Complexity Analysis This quantum attack starts with making a superposition cn of all possible plaintext and ciphertext pairs. Here, we assume that the superposition is created by quantum queries. Therefore, the (quantum) data complexity is $D_Q = \log N$. The time complexity corresponds to the cost for quantum computation of the offline Simon's algorithm. Thus, the offline quantum computation for identifying K_0 and K_1 takes the time complexity of $T_Q = \sqrt{N} \log N$.

The Q1 Attack with Full Codebook

Now we discuss an attack on 4-IEM in the Q1 model. As we use the offline Simon's algorithm, we start the algorithm by creating a superposition of all possible plaintexts and ciphertexts. If the attacker can collect all possible plaintexts and ciphertexts by classical queries, the quantum attack without quantum queries is also possible. In this setting, the attacker first creates a superposition over N plaintext and ciphertexts pairs by only classical queries. We use the method proposed in [2] to create the superposition. The procedure is as follows:

1. Start with two n qubit registers: $|0\rangle^{\otimes n} |0\rangle^{\otimes n}$.
2. Apply $H^{\otimes}$ to the first register: $\sum_{x \in \{0,1\}^n} |x\rangle |0\rangle$.
3. For each $y \in \{0,1\}^n$, query y to E_K classically. Write $E_\mathsf{K}(y)$ in the second register if the first contains the value y: $\sum_{x \in \{0,1\}^n} |x\rangle |E_\mathsf{K}(x)\rangle$.

The output superposition can be viewed as a quantum keyed oracle, but it exists offline. Therefore, if the attacker can construct this superposition, s.he executes the quantum attack based on the offline Simon's algorithm without superposition queries. In this setting, N classical queries are required in the online phase. On the other hand, the time complexity is the same as the Q2 model, *i.e.*, $T_Q = \sqrt{N} \log N$.

In [14], the authors assumed that quantum computers require a lot of execution of error corrections, which degrades the performance. Under the assumption of [14], modern classical computers are faster per operation than quantum computers. Therefore, we can say that N times classical queries are faster than N times Grover's iterations following the assumption. Thus, in this setting, our quantum attack based on the offline Simon's algorithm may outperform Grover's search.

Application to LED-128

LED-128 is a variant of a lightweight block cipher family LED [17], which takes a 64-bit plaintext and a 128-bit secret key as the input. LED-128 employs the IEM with two alternating keys as the underlying construction. LED-128 iterates the *step*, which consists of XORing half of the secret key and application of the public permutation consisting of the 4-round AES-like round function. The full LED-128 has total 12 steps.

The best know attack in classical setting against the LED-128 is the application of the attack against the 3-round IEM proposed in [10], which can attack up to 8-step LED-128. However, for the 4-step LED-128, Dinur et al. show that direct application of the multibridge attack is the most efficient attack in the classical setting with the complexity $D_C = T_C = 2^{64}$.

Our quantum attack can be applied to attack on 4-step LED-128 directly. Our attack in the Q2 model requires $T_Q = \sqrt{N} \log N$ with $D_Q = \log N$ quantum data. Thus, applying this attack to 4-round LED-128 requires $T_Q = 2^{32} \cdot 2^6 = 2^{38}$ with $D_Q = 64 = 2^6$ quantum data. In the Q1 model, considering that the attacker has a full codebook, the data complexity becomes $D_C = 2^{64}$ and time complexity remain the same, i.e., $T_Q = 2^{32} \cdot 2^6 = 2^{38}$.

4 The Quantum Multibridge Attack

In this section, we propose the quantum multibridge attack, which can be applied to recover two keys of 4-IEM without quantum queries. In this attack, we first make D_C classical queries to get QAA to find two intermediate values and a constant, which forms a bridge between them. The procedure of our attack is as follows:

1. Make offline queries of D_C plaintexts and create a list of queried data and the values calculated from the response and store the list in a qRAM.
2. Amplify N/D_C possible values of Δ
   (a) Create a superposition over D_C candidates for K_0 based on the list created in the first step.
   (b) Create a superposition over D_C candidates of key pair $(\mathsf{K}_0, \mathsf{K}_1)$ based on the list of candidates for K_0.
   (c) Run a quantum search algorithm to identify a right key pair $(\mathsf{K}_0, \mathsf{K}_1)$.
   (d) Test $(\mathsf{K}_0, \mathsf{K}_1)$ by a trial encryption.

The first step is in the online phase, and the other steps are offline. In the following, we explain the detailed procedure of our attack.

The Attack Procedure. Similarly to the original multibridge attack, our attack begins by initializing variables, as depicted in Fig. 2. The *online* phase involves querying plaintexts x and obtaining their corresponding ciphertexts $E_{\mathsf{K}}(x)$. By calculating $d(x) = x \oplus E_{\mathsf{K}}(x)$ for each plaintext, we prepare a list L such that $L(d(x)) = (d(x), x)$ and store it in the qRAM, where x is a plaintext indexed by

$d(x)$. In the offline phase, we search Δ from N/D_C possible values by using QAA in the actual algorithm. However, for simplicity, we describe the procedure of the offline phase for a fixed Δ. The procedure of the offline phase of the quantum multibridge attack under a fixed Δ is as follows:

1. Iterate the following procedure D_C times:
   (a) we apply the first QAA, namely $\mathcal{F}_1 = \mathsf{QAA}(\mathcal{A}_1, \mathcal{S}_1)$.
      i. The SETUP phase $\mathcal{A}_1 = H^{\otimes n}$. In other words, this is Grover's algorithm.
      ii. To define the FLIP phase $\mathcal{S}_1$, we consider the function f, defined over all possible values of $\alpha \in \{0,1\}^n$ as $f_\Delta(\alpha) = P_1^{-1}(\alpha) \oplus P_4(\alpha \oplus \Delta)$. Furthermore, we define the following Boolean function based on f:

$$F_\Delta(\alpha) = \begin{cases} 1 & \text{if } f_\Delta(\alpha) \text{ has a match in } L \\ 0 & \text{otherwise .} \end{cases}$$

In other words, F_Δ validates if there is a x such that $f_\Delta(\alpha) = d(x)$ and $(d(x), x) \in L$, as shown in Fig. 4.

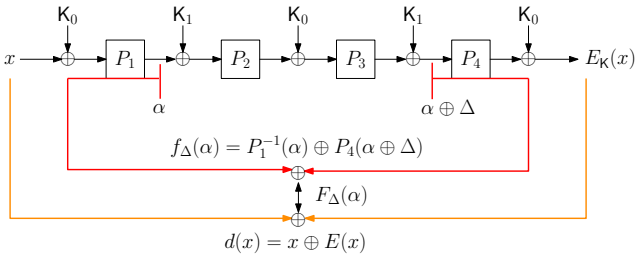

Fig. 4: Validation of **STEP 1**

The FLIP phase consists of the unitary $\mathcal{S}_1 = \mathcal{S}_{F_\Delta}$ which flips the phase of $|\alpha\rangle$ if $F_\Delta(\alpha) = 1$. Note that, $\mathcal{S}_{F_\Delta}$ can be implemented with two calls to O_{F_Δ}, which is a quantum offline circuit for computing F_Δ.
We start with a superposition of

$$|\psi_0\rangle = \sum_{\alpha \in \{0,1\}^n} |\alpha\rangle .$$

Run QAA where $\mathcal{Q} = -\mathcal{A}_1 \mathcal{S}_0 \mathcal{A}_1^{-1} \mathcal{S}_1$ Then, we have

$$|\psi_0\rangle \xrightarrow{\mathsf{QAA}} |\psi_1\rangle = \sum_{\alpha \in \{0,1\}^n | F_\Delta(\alpha)=1} |\alpha\rangle .$$

(b) In this step, apply qRAM Read to $|\psi_1\rangle$ to create a superposition of all possible K_0. We read values of x indexed by $d(x) = f_\Delta(\alpha)$ from L. The operation is as follows:

$$|\psi_1\rangle \xrightarrow{\text{Compute } f_\Delta(\alpha) \text{ and } P_1^{-1}(\alpha)} \sum_{\alpha\in\{0,1\}^n | F_\Delta(\alpha)=1} |\alpha\rangle\,|f_\Delta(\alpha)\rangle\,\left|P_1^{-1}(\alpha)\right\rangle$$
$$\xrightarrow{\text{qRAM Read}} \sum_{\alpha\in\{0,1\}^n | F_\Delta(\alpha)=1} |\alpha\rangle\,|f_\Delta(\alpha) = d(x)\rangle\,\left|P_1^{-1}(\alpha)\oplus x\right\rangle$$

Measure α and $P_1^{-1}(\alpha)\oplus x$ and store them next to the corresponding $d(x)$ in L.

2. Now we apply another QAA, namely $\mathcal{F}_2 = \mathsf{QAA}(\mathcal{A}_2, \mathcal{S}_2)$.

(a) We start with the description of $\mathcal{A}_2$. The algorithm $\mathcal{A}_2$ is $\mathcal{A}_2 = \mathsf{QAA}(\mathcal{A}_3, \mathcal{S}_3)$ where $\mathcal{A}_3$ is $H^{\otimes n}$. To define $\mathcal{S}_3$, consider the function $g_\Delta(\beta) = P_2(\beta) \oplus P_3^{-1}(\beta \oplus \Delta)$ defined over all possible values of $\beta \in \{0,1\}^n$ and corresponding Boolean function:

$$G_\Delta(\beta) = \begin{cases} 1, & \text{if there is } P_1^{-1}(\alpha)\oplus x \in L \text{ s.t. } g_\Delta(\beta) = P_1^{-1}(\alpha)\oplus x \\ 0, & \text{otherwise .} \end{cases}$$

Thus, $G_\Delta(\beta) = 1$ if and only if there is $P_1^{-1}(\alpha)\oplus x$ such that $P_1^{-1}(\alpha)\oplus x = g_\Delta(\beta)$, as shown in Fig. 5, which is exactly the multibridge property we need.

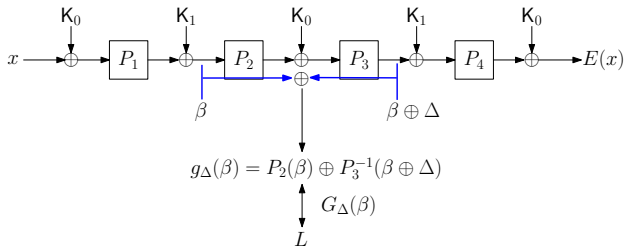

Fig. 5: Validation of **STEP 2**

Thus, the FLIP phase consists of the unitary $\mathcal{S}_3 = \mathcal{S}_{G_\Delta}$ which flips the phase of $|\beta\rangle$ if $G_\Delta(\beta) = 1$. Note that, $\mathcal{S}_{G_\Delta}$ can be implemented with two calls to O_{G_Δ}, which is a quantum offline circuit for computing G_Δ.
We start with the following initial state:

$$|\psi_2\rangle = \sum_{\beta\in\{0,1\}^n} |\beta\rangle\,.$$

We run QAA with $\mathbf{Q} = -\mathcal{A}_3\mathcal{S}_0\mathcal{A}_3^{-1}\mathcal{S}_3$ and we have:

$$|\psi_2\rangle \xrightarrow{\mathsf{QAA}} \sum_{\beta\in\{0,1\}^n | G_\Delta(\beta)=1} |\beta\rangle$$

By computing $|g_\Delta(\beta)\rangle$ and reading the values of α such that stored with $P_1^{-1}(\alpha) \oplus x$ where $|g_\Delta(\beta)\rangle = P_1^{-1}(\alpha) \oplus x$, from L, we can obtain the following superposition.

$$|\psi_3\rangle = \sum_{\{\alpha\in\{0,1\}^n | F_\Delta(\alpha)=1\}} \sum_{\{\beta\in\{0,1\}^n | G_\Delta(\beta)=1\}} |g_\Delta(\beta)\rangle\,|\alpha\oplus\beta\rangle\,.$$

Let $\mathcal{K}$ be a set that contains all key pairs generated from a pair of (α, β) for a Δ. Then, $|\psi_3\rangle$ can be expressed as

$$|\psi_3\rangle = \sum_{\hat{\mathsf{K}}_0||\hat{\mathsf{K}}_1\in\mathcal{K}} \left|\hat{\mathsf{K}}_0\right\rangle\left|\hat{\mathsf{K}}_1\right\rangle = \sum_{\hat{\mathsf{K}}=\hat{\mathsf{K}}_0||\hat{\mathsf{K}}_1\in\mathcal{K}} \left|\hat{\mathsf{K}}\right\rangle$$

where $\hat{\mathsf{K}}_0$ and $\hat{\mathsf{K}}_1$ are the candidates for K_0 and K_1, respectively.

(b) Finally, we define $\mathcal{S}_2$. This operator simply flips the phase of $\left|\hat{\mathsf{K}}\right\rangle$ if $\hat{\mathsf{K}}$ is a valid key and we check this by trial encryptions over a small set of plaintext-ciphertext pairs $\mathcal{M} = \{(m_i, c_i)|0 \le i < s\}$, where s is a small constant[6]. Define the following Boolean function:

$$H_\Delta(\hat{\mathsf{K}}) = \begin{cases} 1 & \text{if } E_{\mathsf{K}}(m_i) = c_i, \forall (m_i, c_i) \in \mathcal{M} \\ 0 & \text{otherwise.} \end{cases}$$

E_{K} is the quantum circuit of 4-IEM which uses $\mathsf{K} = \hat{\mathsf{K}}_0||\hat{\mathsf{K}}_1$ as the secret key. Note that, with a guessed key pair, it is possible to prepare such a circuit offline. Now define a unitary operator $\mathcal{S}_3 = \mathcal{S}_H$ which flips the sign if $H_\Delta(\hat{\mathsf{K}}) = 1$.
Thus, we run QAA with $\mathbf{Q} = -\mathcal{A}_2\mathcal{S}_0\mathcal{A}_2^{-1}\mathcal{S}_3$ with initial state $|\psi_3\rangle$ and perform a final measuring of the whole state.

Complexity Analysis

The online phase requires D_C online classical queries and D_C simple computations to compute $d(x)$. In the following, we analyze the complexity of each offline steps.

STEP 1. This is an offline phase. In this step we apply $\mathcal{F}_1 = \mathsf{QAA}(\mathcal{A}_1, \mathcal{S}_1)$ which is a simple Grover's algorithm for creating a superposition state of D_C solutions

[6] In [15], this number is sufficient if it satisfies $s > \lceil 2k/n \rceil$, where k is the secret key size. Thus, it is small enough that it does not affect the time complexity.

from a uniform superposition state. Since, there are D_C numbers of α such that $x_{f_\Delta(\alpha)} \in L$, the superposition after applying $\mathcal{S}_1 = \mathcal{S}_{F_\Delta}$ is as follows:

$$\mathcal{S}_1 |\psi_0\rangle = \sqrt{(N - D_C)/N} \sum_{\substack{\alpha \in \{0,1\}^n \\ |F_\Delta(\alpha)=0}} |\alpha\rangle - \sqrt{D_C/N} \sum_{\substack{\alpha \in \{0,1\}^n \\ |F_\Delta(\alpha)=1}} |\alpha\rangle$$

Therefore, the number of iterations is $\sqrt{N/D_C}$. We iterate this QAA operation D_C times to store all D_C solutions to L. Thus, the complexity of this step is $\sqrt{N/D_C} \times D_C = \sqrt{ND_C}$.

STEP 2. Similar to the **STEP 1**, the SETUP phase of $\mathcal{F}_2 = \mathsf{QAA}(\mathcal{A}_2, \mathcal{S}_2)$, namely $\mathcal{A}_2$ is a simple Grover's algorithm for creating a superposition state of D_C solutions from a uniform superposition state. Since, there are D_C numbers of β such that $G_\Delta(\beta) = 1$, application of $\mathcal{S}_3 = \mathcal{S}_{G_\Delta}$ is as follows:

$$S_3 |\psi_2\rangle = \sqrt{(N - D_C)/N} \sum_{\substack{\beta \in \{0,1\}^n \\ |G_\Delta(\beta)=0}} |\beta\rangle - \sqrt{D_C/N} \sum_{\substack{\beta \in \{0,1\}^n \\ |G_\Delta(\beta)=1}} |\beta\rangle$$

Thus, the number of iterations is $\sqrt{N/D_C}$, which is the complexity of the SETUP phase of $\mathcal{F}_2$. Finally, in the FLIP phase, if we apply $\mathcal{S}_2 = \mathcal{S}_H$ to $|\psi_3\rangle$, then the superposition state is as follows:

$$\mathcal{S}_2 |\psi_3\rangle = \sum_{\hat{\mathsf{K}} \in \mathcal{K}} \left|\hat{\mathsf{K}}\right\rangle = \sqrt{(D_C - 1)/D_C} \sum_{\hat{\mathsf{K}} | H(\hat{\mathsf{K}})=0} \left|\hat{\mathsf{K}}\right\rangle - \sqrt{1/D_C} \sum_{\hat{\mathsf{K}} | H(\hat{\mathsf{K}})=1} \left|\hat{\mathsf{K}}\right\rangle$$

As the number of possible key pairs is D, $\mathcal{F}_2$ requires $\sqrt{D}$ iterations. The operations from creating $|\psi_3\rangle$ to identifying a right key pair is a sequential execution of $\mathcal{A}_2$ and $\mathcal{S}_2$. Thus, the cost of this sequence requires $\sqrt{N/D_C} \times \sqrt{D_C} = \sqrt{N}$.

Overall Complexity. We also search for the right value of Δ by QAA. Since the search space of Δ is N/D_C, the search cost is $\sqrt{N/D_C}$. In summary, the overall complexity is as follows:

$$T_Q = D_C + \sqrt{N/D_C}(\sqrt{ND_C} + \sqrt{N}) = D_C + N \approx N$$

The optimal complexity is $T_Q = N$, and the time complexity of the quantum version of the multibridge attack is independent of the amount of data. Therefore, $D_C = 1$ is sufficient and no qRAM is required to achieve the optimal time complexity.

Comparison with Grover's Search. Although this attack does not outperform Grover's search, the quantum multibridge attack does not need exponential times evaluations for full round encryption of 4-IEM. In the quantum multibridge attack, the quantum search operations are executed for quantum oracles consisting of

XOR of two permutations. We can assume each execution of these functions takes about 1/4 of a full round encryption time. Therefore, when we consider the complexity of Grover's search as N, the time complexity of the quantum multibridge attack when $D_C = 1$ becomes:

$$T_Q = 1 + \sqrt{N}(\sqrt{N}/4 + \sqrt{N}/4) \approx N/2.$$

Thus, the multibridge attack slightly outperforms Grover's search when considering the depth of the quantum circuit.

5 Conclusion

In this paper, we propose quantum key recovery attacks against 4-IEM, which was analyzed classically by Dinur *et al.* [11] We show that our attack based on the offline Simon's algorithm is highly efficient when the attacker can make superposition queries, *i.e.*, in the Q2 model. Besides, we show that this attack can be used in the Q1 model, under the assumption that the attacker can create the full codebook using classical queries. Moreover, we propose a quantum version of the multibridge attack [11]. The result shows that the quantum version can achieve $T_Q = N$ even if $D_C = 1$, while the classical one requires $D_C = N$ to achieve the time complexity of $T_C = N$. Furthermore, we show that the quantum multibridge attack slightly more efficient than Grover's search, when considering the depth of the quantum circuit. Specifically, the result shows that the time complexity of the quantum multibridge attack becomes $T_Q = N/2$, when we consider the time complexity of Grover's search as $T_Q = N$.

References

1. Avanzi, R., Banik, S., Dunkelman, O., Eichlseder, M., Ghosh, S., Nageler, M., Regazzoni, F.: The tweakable block cipher family qarmav2. IACR Cryptol. ePrint Arch. p. 929 (2023)
2. Bonnetain, X., Hosoyamada, A., Naya-Plasencia, M., Sasaki, Y., Schrottenloher, A.: Quantum attacks without superposition queries: The offline simon's algorithm. In: ASIACRYPT (1). Lecture Notes in Computer Science, vol. 11921, pp. 552–583. Springer (2019)
3. Bonnetain, X., Schrottenloher, A., Sibleyras, F.: Beyond quadratic speedups in quantum attacks on symmetric schemes. In: EUROCRYPT (3). Lecture Notes in Computer Science, vol. 13277, pp. 315–344. Springer (2022)
4. Bozilov, D., Eichlseder, M., Knezevic, M., Lambin, B., Leander, G., Moos, T., Nikov, V., Rasoolzadeh, S., Todo, Y., Wiemer, F.: Princev2 - more security for (almost) no overhead. In: SAC. Lecture Notes in Computer Science, vol. 12804, pp. 483–511. Springer (2020)
5. Brassard, G., Hoyer, P., Mosca, M., Tapp, A.: Quantum amplitude amplification and estimation. Contemporary Mathematics **305**, 53–74 (2002)
6. Brassard, G., Hoyer, P., Tapp, A.: Quantum algorithm for the collision problem. arXiv preprint quant-ph/9705002 (1997)

7. Cai, B., Gao, F., Leander, G.: Quantum attacks on two-round even-mansour. Frontiers in Physics **10**, 1028014 (2022)
8. Chen, S., Steinberger, J.P.: Tight security bounds for key-alternating ciphers. In: EUROCRYPT. Lecture Notes in Computer Science, vol. 8441, pp. 327–350. Springer (2014)
9. Cogliati, B., Seurin, Y.: Beyond-birthday-bound security for tweakable even-mansour ciphers with linear tweak and key mixing. In: ASIACRYPT (2). Lecture Notes in Computer Science, vol. 9453, pp. 134–158. Springer (2015)
10. Dinur, I., Dunkelman, O., Keller, N., Shamir, A.: Key recovery attacks on 3-round even-mansour, 8-step led-128, and full AES2. In: ASIACRYPT (1). Lecture Notes in Computer Science, vol. 8269, pp. 337–356. Springer (2013)
11. Dinur, I., Dunkelman, O., Keller, N., Shamir, A.: Cryptanalysis of iterated even-mansour schemes with two keys. In: ASIACRYPT (1). Lecture Notes in Computer Science, vol. 8873, pp. 439–457. Springer (2014)
12. Dutta, A.: Minimizing the two-round tweakable even-mansour cipher. In: ASIACRYPT (1). Lecture Notes in Computer Science, vol. 12491, pp. 601–629. Springer (2020)
13. Even, S., Mansour, Y.: A construction of a cipher from a single pseudorandom permutation. J. Cryptol. **10**(3), 151–162 (1997)
14. Gidney, C., Ekerå, M.: How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. Quantum **5**, 433 (2021)
15. Grassl, M., Langenberg, B., Roetteler, M., Steinwandt, R.: Applying grover's algorithm to AES: quantum resource estimates. In: PQCrypto. Lecture Notes in Computer Science, vol. 9606, pp. 29–43. Springer (2016)
16. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: STOC. pp. 212–219. ACM (1996)
17. Guo, J., Peyrin, T., Poschmann, A., Robshaw, M.J.B.: The LED block cipher. In: CHES. Lecture Notes in Computer Science, vol. 6917, pp. 326–341. Springer (2011)
18. Hosoyamada, A., Aoki, K.: On quantum related-key attacks on iterated even-mansour ciphers. In: IWSEC. Lecture Notes in Computer Science, vol. 10418, pp. 3–18. Springer (2017)
19. Kilian, J., Rogaway, P.: How to protect des against exhaustive key search. In: Advances in Cryptology—CRYPTO'96: 16th Annual International Cryptology Conference Santa Barbara, California, USA August 18–22, 1996 Proceedings 16. pp. 252–267. Springer (1996)
20. Kilian, J., Rogaway, P.: How to protect des against exhaustive key search (an analysis of desx). Journal of Cryptology **14**, 17–35 (2001)
21. Kuwakado, H., Morii, M.: Security on the quantum-type even-mansour cipher. In: ISITA. pp. 312–316. IEEE (2012)
22. Leander, G., May, A.: Grover meets simon - quantumly attacking the fx-construction. In: ASIACRYPT (2). Lecture Notes in Computer Science, vol. 10625, pp. 161–178. Springer (2017)
23. Nielsen, M.A., Chuang, I.L.: Quantum computation and quantum information, vol. 2. Cambridge university press Cambridge (2001)
24. Simon, D.R.: On the power of quantum computation. In: FOCS. pp. 116–123. IEEE Computer Society (1994)
25. Zhandry, M.: How to construct quantum random functions. In: FOCS. pp. 679–687. IEEE Computer Society (2012)
26. Zhang, P., Luo, Y.: Quantum key recovery attacks on tweakable even–mansour ciphers. Quantum Information Processing **22**(9), 336 (2023)