frontiers | Frontiers in Physics

TYPE Original Research
PUBLISHED 18 October 2022
DOI 10.3389/fphy.2022.1028014

OPEN ACCESS

EDITED BY
Tianyu Ye,
Zhejiang Gongshang University, China

REVIEWED BY
Gang Xu,
North China University of Technology, China
Yefeng He,
Xi'an University of Posts and Telecommunications, China
Jun Zhu,
Guangxi Normal University, China

*CORRESPONDENCE
Gregor Leander,
gregor.leander@rub.de

SPECIALTY SECTION
This article was submitted to Quantum Engineering and Technology, a section of the journal Frontiers in Physics

RECEIVED 25 August 2022
ACCEPTED 20 September 2022
PUBLISHED 18 October 2022

CITATION
Cai B, Gao F and Leander G (2022), Quantum attacks on two-round even-mansour.
Front. Phys. 10:1028014.
doi: 10.3389/fphy.2022.1028014

Quantum attacks on two-round even-mansour

BinBin Cai[1,2], Fei Gao[1] and Gregor Leander[3]*

[1]State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, China, [2]Henan Key Laboratory of Network Cryptography Technology, Zhengzhou, China, [3]Ruhr University Bochum, Bochum, Germany

Even-Mansour is one of the most important constructions in symmetric cryptography, both from a theoretical and practical perspective. With the rapid development of quantum computing, the security of Even-Mansour construction in quantum setting needs to be considered. For one round Even-Mansour construction, it is well settled by classical and quantum attacks. While for the iterated scheme, the situation is much more complex. In this paper, we study the next case in line in detail and depth: quantum attacks against two rounds case. We first make an asymptotic comparison with existing classical and quantum attacks. Then we give concrete resource estimation for the proposed quantum attacks on round reduced LED cipher and AES[2]. The resource estimation allows to deduce the most efficient attacks based on the trade-off of the number of qubits and Toffoli depth.

KEYWORDS

even-mansour, grover algorithm, grover-meets-simon algorithm, offline simon algorithm, resource estimation

1 Introduction

The Even-Mansour (EM) construction [1] is a minimal block cipher that has been widely studied since its outstanding simplicity and provable classical security [1, 2]. It is made up of a n-bit public permutation P and two n-bit secret subkeys K_1 and K_2, *i.e.*, $E(x) = P(x \oplus K_1) \oplus K_2$, where n is the block size. When P is a public random permutation, EM construction has been proven to be indistinguishable from a random permutation when $D \cdot T = \Omega(2^n)$, where D and T are the number of queries to the encryption oracle $E(x)$ and permutation oracle P respectively. At EUROCRYPT 2012, Bogdanov *et al.* [3] studied EM construction into an r-round iterated EM scheme, which is defined as

$$E(x) = P_r(\cdots P_2(P_1(x \oplus K_1) \oplus K_2) \oplus K_3 \cdots \oplus K_r) \oplus K_{r+1},$$

where $P_1, \ldots, P_r$ are r independent permutations and $K_1, \ldots, K_{r+1}$ are $(r+1)$ n-bit subkeys. This construction was proven to be secure up to $2^{2n/3}$ queries against distinguishing attack for $r \geq 2$ [3] and subsequently improved to $2^{rn/(r+1)}$ queries [4, 5].

Recently, the security analysis of symmetric cryptography in quantum setting has also become a hot issue in cryptography research [6], in addition to quantum cryptography [7–10]. There are two different models for quantum cryptanalysis against symmetric cipher based on the notions for pseudorandom function security in quantum setting,

standard security and quantum security [11]. The standard security and quantum security are also denoted as Q1 model and Q2 model respectively by Kaplan *et al.* [12]. In Q1 model, the adversaries could only access the encryption oracle classically but process data with quantum operations. While in Q2 model, the adversaries could query the encryption oracle with quantum superpositions and process data with quantum operations.

In 2012, Kuwakado and Morri [13] proposed a quantum key-recovery attack against EM construction in Q2 model. Compared with the classical key-recovery attack, the quantum attack can attain exponential acceleration. In other words, the EM construction has been broken in Q2 model. Very recently, at EUROCRYPT 2022, Alagic *et al.* [14] proved a lower bound that $\approx 2^{n/3}$ queries are necessary for attacking EM construction in Q1 model. In 2014, Kaplan [15] gave the quantum meet-in-the-middle attack (QMITM attack) against iterated block ciphers in Q1 model. For two-round iterated EM (2EM) construction with two alternating subkeys and 2EM construction with independent subkeys, the attack requires the time and memory complexities of $\mathcal{O}(2^n)$ and $\Omega(2^n)$ quantum queries to permutation oracle to recover all subkeys. However, the QMITM attack which reduces key-recovery to claw finding problem [16] is a general attack that may not be as effective for 2EM constructions. Therefore, we aim at investigating more efficient quantum key-recovery attacks on 2EM constructions in this paper. The constructions we focused on are 2EM construction with identical subkeys, 2EM construction with two alternating subkeys and 2EM construction with independent subkeys which we refer as

$$\begin{aligned}
&\mathbf{2EM_1}: \quad E_1(x) = P_2(P_1(x \oplus K) \oplus K) \oplus K,\\
&\mathbf{2EM_2}: \quad E_2(x) = P_2(P_1(x \oplus K_1) \oplus K_2) \oplus K_1,\\
&\mathbf{2EM_3}: \quad E_3(x) = P_2(P_1(x \oplus K_1) \oplus K_2) \oplus K_3.
\end{aligned}$$

At FSE 2013, Nikolić *et al.* [17] proposed the first nontrivial classical attack on $2EM_1$ construction which requires the time complexity of $2^n \ln n/n$ with $2^n \ln n/n$ known plaintexts. Later, Dinur *et al.* [18] improved this attack to reduce the data complexity to $2^{\lambda n}$ known plaintexts, where $0 < \lambda < 1$. Meanwhile, they also presented an attack against $2EM_3$ construction with the time complexity of $\mathcal{O}(2^n\sqrt{\ln n/n})$ and $2^n\sqrt{\ln n/n}$ chosen plaintexts. However, the above attacks against $2EM_1$ construction are based on multi-collisions techniques, which require time and memory complexities close to 2^n. In 2016, Dinur *et al.* [19] presented an alternative attack on $2EM_1$ construction with linear algebra techniques. This attack requires a time complexity of $2^n/\lambda n$ and memory complexity of $2^{\lambda n}$, but with $2^n/\lambda n$ chosen plaintexts. Subsequently, Isobe *et al.* [20] introduced meet-in-the-middle techniques into the attack against $2EM_1$ construction which requires the time and memory complexities of $2^n \ln n/n$ with $2^n \ln n/n$ chosen plaintexts. Furthermore, they also described a low data-complexity and a time-optimized variant attacks. The low data-complexity attack requires the time and memory complexities of $2^n \ln n/n$ with $2^{\lambda n}$ chosen plaintexts. The time-optimized one requires the time complexity of $2^n\beta/n$ and memory complexity of $2^n/2^\beta$ with $2^n\beta/n$ chosen plaintexts, where $\log n \le \beta \lll n$. More recently, Leurent *et al.* [21] proposed three key-recovery attacks on $2EM_1$ construction which are related to the 3-XOR problem. The basic attack requires the time complexity of $2^n/n$ and memory complexity of $2^{2n/3}$ with $2^{2n/3}$ known plaintexts in a balanced case. The variant attack based on 3-SUM algorithm requires the time complexity of $2^n \ln^2 n/n^2$ and memory complexity of $2^{2n/3}$ with $2^{2n/3}$ known plaintexts, but it is unpractical for realistic block size. The low data-complexity attack requires the time complexity of $2^n/\lambda n$ and memory complexity of $2^{\lambda n}$ with λn known plaintexts.

Besides, there are also other quantum attacks against iterated EM construction such as the quantum slide attack on iterated EM construction with identical permutations and subkeys in Q2 model [12] and the quantum related-key attack against iterated EM cipher with identical permutations and independent subkeys in Q2 model [22]. However, these

TABLE 1 Comparison of previous quantum attacks and our attacks on $2EM_2$ and $2EM_3$ constructions, where "Data" represents encryption queries, "Queries" signifies calls to P_i, "Q-memory" and "C-memory" denote quantum memory and classical memory respectively.

Target	Model	Data	Queries	Time	Q-memory	C-memory	References
$2EM_2$	Q2	$\mathcal{O}(2^n)$	0	$\mathcal{O}(2^n)$	$\mathcal{O}(n)$	0	[23]
	Q1	$\mathcal{O}(1)$	$\Omega(2^n)$	$\mathcal{O}(2^n)$	$\mathcal{O}(n)$	$\mathcal{O}(2^n)$	[15]
	Q2	$\mathcal{O}(n \cdot 2^{n/2})$	$\mathcal{O}(n \cdot 2^{n/2})$	$\mathcal{O}(n^3 \cdot 2^{n/2})$	$\mathcal{O}(n^2)$	0	Section 3.2
	Q2	$\mathcal{O}(n)$	$\mathcal{O}(n \cdot 2^{n/2})$	$\mathcal{O}(n^3 \cdot 2^{n/2})$	$\mathcal{O}(n^2)$	$\mathcal{O}(n)$	Section 3.2
	Q1	$\mathcal{O}(2^{2n/3})$	$\mathcal{O}(n \cdot 2^{2n/3})$	$\mathcal{O}(n^3 \cdot 2^{2n/3})$	$\mathcal{O}(n^2)$	$\mathcal{O}(n)$	Section 3.2
$2EM_3$	Q2	$\mathcal{O}(2^{3n/2})$	0	$\mathcal{O}(2^{3n/2})$	$\mathcal{O}(n)$	0	[23]
	Q1	$\mathcal{O}(1)$	$\Omega(2^n)$	$\mathcal{O}(2^n)$	$\mathcal{O}(n)$	$\mathcal{O}(2^n)$	[15]
	Q2	$\mathcal{O}(n \cdot 2^{n/2})$	$\mathcal{O}(n \cdot 2^{n/2})$	$\mathcal{O}(n^3 \cdot 2^{n/2})$	$\mathcal{O}(n^2)$	0	Section 3.2
	Q2	$\mathcal{O}(n)$	$\mathcal{O}(n \cdot 2^{n/2})$	$\mathcal{O}(n^3 \cdot 2^{n/2})$	$\mathcal{O}(n^2)$	$\mathcal{O}(n)$	Section 3.2
	Q1	$\mathcal{O}(2^{2n/3})$	$\mathcal{O}(n \cdot 2^{2n/3})$	$\mathcal{O}(n^3 \cdot 2^{2n/3})$	$\mathcal{O}(n^2)$	$\mathcal{O}(n)$	Section 3.2

TABLE 2 Comparison of attacks against 2-step LED-64. Assume that one evaluation of the cipher as one complexity unit and the evaluation of one permutation costs 1/2 unit.

Data	Queries	Time	Memory	References
$2^{58.7}$	$2^{60.5}$	$2^{60.9}$	2^{60}	[17]
2^{45}	$2^{60.7}$	$2^{60.7}$	2^{60}	[18] ($\lambda = 0.7$)
2^{60}	2^{59}	$2^{60.6}$	2^{16}	[19] ($\lambda = 1/4$)
2^{60}	2^{60}	$2^{61.3}$	2^{60}	[20]
2^{8}	2^{62}	$2^{62.6}$	2^{62}	[20]
2^{61}	2^{57}	$2^{61.7}$	2^{58}	[20] ($\beta = 8$)
2^{42}	2^{43}	2^{58}	2^{42}	[21]
2^{42}	2^{43}	$2^{56.1}$	2^{42}	[21]
2^{4}	2^{60}	2^{61}	2^{16}	[21] ($\lambda = 1/4$)
2^{32}	0	2^{32}	2^{6} qubits	Section 3.1

TABLE 3 Comparison of quantum attacks against 2-step LED-128.

Model	Data	Queries	Time	Q-memory	C-memory	References
Q2	2^{64}	0	2^{64}	2^{7}	0	[23]
Q1	1	2^{64}	2^{64}	2^{7}	2^{64}	[15]
Q2	2^{39}	2^{39}	2^{50}	2^{12}	0	Section 3.2
Q2	2^{6}	2^{38}	2^{50}	2^{12}	2^{6}	Section 3.2
Q1	2^{47}	$2^{46.5}$	$2^{58.5}$	2^{12}	2^{6}	Section 3.2

quantum attacks are in Q2 model and only consider iterated EM construction with identical permutations.

Contributions. in this paper, we study quantum key-recovery attacks against 2EM constructions. The main contributions of this paper include the following two aspects.

First, we consider the security of two-round Even-Mansour constructions with independent permutations in quantum setting. Several quantum key-recovery attacks on 2EM constructions are proposed. For $2EM_1$ construction, the presented quantum key-recovery attack adopts Grover algorithm [23] directly. Compared with the classical attack with optimal query complexity (including the queries to cipher and permutation), *i.e.,* the observed by Leurent *et al.* [21], our attack reduces the query complexity by a factor of $2^{n/6}$. For $2EM_2$ and $2EM_3$ constructions, we consider Grover-meets-Simon algorithm [24] (GMS algorithm) and Offline Simon algorithm [25] (OS algorithm) on constructed functions. The proposed quantum attacks against $2EM_2$ and $2EM_3$ constructions require $\tilde{\mathcal{O}}(2^{2n/3})$ and $\tilde{\mathcal{O}}(2^{n/2})$ queries in Q1 and Q2 model, where $\tilde{\mathcal{O}}$ means ignoring logarithmic factors. In the case of $2EM_2$ construction, the query complexity of our attacks is less than Grover search by a factor of $2^{n/3}$ and $2^{n/2}$ in Q1 and Q2 model respectively. In the case of $2EM_3$ construction, the query complexity of our attacks is better than Grover search by a factor of $2^{5n/6}$ and 2^{n} in Q1 and Q2 model. When compared with the QMITM attack against $2EM_2$ and $2EM_3$ constructions, the query complexity of our attacks is reduced by a factor of $2^{n/3}$ and $2^{n/2}$ in Q1 and Q2 model.

TABLE 4 Comparison of attacks against AES^2.

Model	Data	Queries	Time	Q-memory	C-memory	References
/	2^{128}	2^{129}	$2^{129.6}$	0	2^{128}	[3]
/	$2^{125.4}$	$2^{126.8}$	$2^{126.8}$	0	$2^{125.4}$	[18]
Q2	2^{192}	0	2^{192}	$2^{8.6}$	0	[23]
Q1	1	2^{128}	2^{128}	$2^{8.6}$	2^{128}	[15]
Q2	2^{72}	2^{72}	2^{85}	2^{14}	0	Section 3.2
Q2	2^{7}	2^{71}	2^{85}	2^{14}	2^{7}	Section 3.2
Q1	2^{90}	2^{90}	2^{104}	2^{14}	2^{7}	Section 3.2

TABLE 5 Resource estimation for constructed functions of target ciphers, where #Toffoli/CNOT/NOT represents the number of Toffoli gates, CNOT gates and NOT gates respectively.

	Algorithm	Model	Target cipher	Toffoli depth	#Toffoli	#CNOT	#NOT	width
$f(i, x)$	GMS	Q2	2-step LED-128	304	7296	9280	1536	352
$f(i, x)$	OS	Q1&Q2	2-step LED-128	304	4864	6080	1024	208
$f(i, x)$	GMS	Q2	AES^2	22016	66032	328656	3264	1820
$f(i, x)$	OS	Q1&Q2	AES^2	22016	33016	164072	1632	910

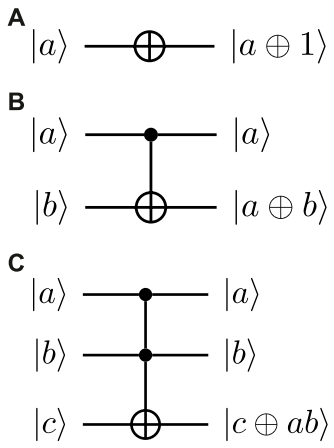

FIGURE 1
Quantum gates of **(A)** NOT gate, **(B)** CNOT gate and **(C)** Toffoli gate.

Besides, the classical memory complexity of our attacks can attain exponential acceleration compared with the QMITM attack on $2EM_2$ and $2EM_3$ constructions. It is worth noting that the presented quantum attacks could break $2EM_3$ construction with $\mathcal{O}(n \cdot 2^{n/2})$ queries in Q2 model, which is less than the classical indistinguishable bound for $2EM_3$ construction, *i.e.,* $2^{2n/3}$ queries. The comparison of previous quantum attacks and our attacks on $2EM_2$ and $2EM_3$ constructions is shown in Table 1.

Second, we apply the presented quantum attacks on 2-step LED-64, 2-step LED-128 and full AES^2. Then we design the quantum circuits for proposed attacks and give the corresponding resource estimation. According to the result of resource estimation, the cost imposed by the attacks based on GMS algorithm and attacks with OS algorithm in Q2 model is close. The extra overhead generated by the attacks based on GMS algorithm is mainly due to their more complex classifier oracles. Besides, the attacks based on OS algorithm in Q1 model cost more resources than corresponding attacks in Q2 model since the attacks in Q1 model require more iterations to search more bits exhaustively. Moreover, there is no doubt that the presented quantum attacks on 2-step LED-128 and AES^2 cost much less than the corresponding Grover attacks, except for the number of qubits.

Organization. The rest of the paper is organized as follows. In the next section, some essential preliminaries are introduced. The quantum attacks on 2EM constructions and their application to specific ciphers are presented in Sect. 3. In Sect. 4, we give the quantum resource estimation of the proposed quantum attacks on corresponding ciphers. Finally, a short conclusion is given in Sect. 5.

2 Preliminaries

In this section, some relevant preliminaries are given.

2.1 Quantum algorithms

2.1.1 Grover algorithm

Problem 1. (Grover [23]). Assume that there exists only one marked item x' in the N-scale unstructured datasets, the goal is to find x', *where* $N = 2^n$. *In other words, let* f: $\{0,1\}^n \rightarrow \{0, 1\}$ *be a function such that* $f(x) = 0$ *for all* $0 \leq x < 2^n$ *except* x', *for which* $f(x') = 1$, *find* x'.

To solve this problem, any deterministic classical algorithms need to make $\mathcal{O}(2^n)$ queries to $f(x)$. However, Grover algorithm can solve this problem with a probability close to 1 by performing Grover iteration about $\frac{\pi}{4}\sqrt{2^n}$ times. Therefore, the query complexity of Grover algorithm is $\mathcal{O}(\sqrt{2^n})$, which is a square speed-up compared to the classical counterpart. Furthermore, the generalization of Grover algorithm (*i.e.,* Quantum Amplitude Amplification, QAA) is given in the following theorem.

Theorem 1. (Brassard et al. [26]). Let $\mathcal{A}$ be any quantum algorithm performed on q qubits without *measurement. Let* $\mathcal{B}$: $\mathbb{F}_2^q \rightarrow \{0, 1\}$ *be a function that classifies the outcomes of* $\mathcal{A}$

as good or bad and $p > 0$ 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 as $\sin^2(\theta) = p$. Besides, define the unitary operator $Q = -\mathcal{A}S_0\mathcal{A}^{-1}S_{\mathcal{B}}$, where $S_{\mathcal{B}}$ changes the sign of the good state

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

while S_0 changes the sign of zero state $|0\rangle$ only. Finally, the measurement after the operation of $Q^k\mathcal{A}|0\rangle$ will obtain the good state with probability at least $\max\{1 - p, p\}$.

Step 1. Prepare the quantum state $|0^{\otimes n}\rangle$.
Step 2. Perform a Hadamard transform $H^{\otimes n}$ on the register:

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

Step 3. Construct the quantum oracle $O : |x\rangle \xrightarrow{O} (-1)^{f(x)}|x\rangle$, where $f(x) = 1$ if x is the marked item, otherwise $f(x) = 0$.
Step 4. Apply Grover iteration for R ($R \approx \frac{\pi}{4}\sqrt{2^n}$) times:

$$[(2|\psi\rangle\langle\psi| - I)O]^R|\psi\rangle \approx |x'\rangle.$$

Step 5. Measure the register and obtain x'.

Algorithm 1. Grover algorithm [23]

2.1.2 Simon algorithm

Problem 2. (Simon [27]). Let f: $\{0,1\}^n \to \{0,1\}^n$ be a function. Promise that there exists $s \in \{0,1\}^n$ such that for any $(x, y) \in \{0,1\}^n$, $[f(x) = f(y)] \Leftrightarrow [x \oplus y \in \{0^n, s\}]$ *is satisfied. The goal is to find the period s.*

By performing Simon algorithm, one can obtain a random vector y such that $y \cdot s = 0$. Therefore, $(n - 1)$ independent vectors orthogonal to period s can be obtained by repeating Simon algorithm for $\mathcal{O}(n)$ times. Then one can recover the period s with linear algebra classically. Thus, the query complexity of Simon algorithm is $\mathcal{O}(n)$.

According to EM construction, Kuwakado and Morri [13] introduce the function $f(x) = E(x) \oplus P(x) = P(x \oplus K_1) \oplus K_2 \oplus P(x)$. It is obvious that $f(x) = f(x \oplus K_1)$ and the period s is K_1. Hence, they can recover the subkey K_1 with Simon algorithm and then obtain the value of K_2 easily.

2.1.3 Grover-meets-simon algorithm

Problem 3. (Leander et al. [24]). Let f: $\{0,1\}^m \times \{0,1\}^n \to \{0,1\}^i$ be a function, where m is in $\mathcal{O}(n)$. There exists a unique $i_0 \in \{0,1\}^m$ such that for any $x \in \{0,1\}^n$, $f(i_0, x) = f(i_0, x \oplus s)$ is satisfied, where $s \in \{0,1\}^n$. The goal is to find the unique i_0 and the period s.

The problem can be solved by GMS algorithm which requires the query complexity of $\mathcal{O}(n \cdot 2^{m/2})$ and time complexity of $\mathcal{O}(n^3 \cdot 2^{m/2})$.

At Asiacrypt 2017, Leander and May [24] proposed GMS algorithm to attack the FX construction [28] that $Enc(x) = E_{K_0}(x \oplus K_1) \oplus K_2$. They consider the function $f(k, x) = Enc(x) \oplus E_k(x) = E_{K_0}(x \oplus K_1) \oplus K_2 \oplus E_k(x)$. Obviously, the function $f(k, x)$ is periodic with period K_1 for all x when $k = K_0$. Otherwise $f(k, x)$ is not periodic. In such a case, they design the following GMS algorithm to recover all subkeys of FX construction.

2.1.4 Offline Simon algorithm

Problem 4. (Bonnetain et al. [25]). Let f: $\{0,1\}^m \times \{0,1\}^n \to \{0,1\}^l$ and g: $\{0,1\}^n \to \{0,1\}^l$ be functions, where m is in $\mathcal{O}(n)$. There exists a unique $i_0 \in \{0,1\}^m$ such that for any $x \in \{0,1\}^n$, $f(i_0, x) \oplus g(x) = f(i_0, x \oplus s) \oplus g(x \oplus s)$ is satisfied, where $s \in \{0,1\}^n$. The goal is to find the unique i_0 and the period s.

Step 1. Prepare the quantum state $|0^{\otimes n}\rangle|0^{\otimes n}\rangle$.
Step 2. Apply a Hadamard transform $H^{\otimes n}$ to the first register:

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

Step 3. Apply a quantum query to the function f:

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

Step 4. Measure the second register and then the first register collapses to the state:

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

Step 5. Reapply a Hadamard transform $H^{\otimes n}$ to the first register:

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

Step 6. Measure the first register and obtain y.

Algorithm 2. Simon algorithm [27]

To solve this problem, we can adopt OS algorithm. The OS algorithm requires $\mathcal{O}(n)$ quantum queries to g, $\mathcal{O}(n \cdot 2^{m/2})$ quantum queries to f and the time complexity of $\mathcal{O}(n^3 \cdot 2^{m/2})$.

Furthermore, we can also solve this problem with OS algorithm in Q1 model if the function g can be only queried classically. Concretely, it is similar to executing OS algorithm in Q2 model except that the quantum state $|\psi_g\rangle$ in steps 2 and 6 now should be prepared by querying the whole codebook of g. Hence, it requires $\mathcal{O}(2^n)$ classical queries to g, $\mathcal{O}(n \cdot 2^{m/2})$ quantum queries to f and the time complexity of $\mathcal{O}(n^3 \cdot 2^{m/2})$.

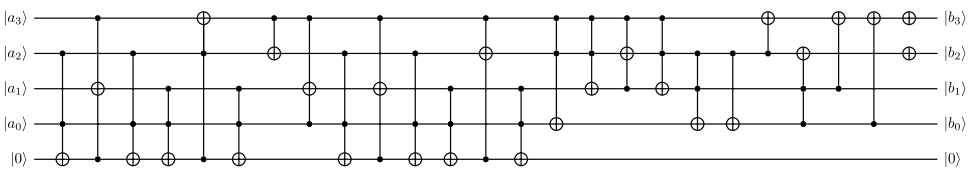

FIGURE 2
Quantum circuit of S-box used in SubCells: $|a\rangle|0\rangle \to |S(a)\rangle|0\rangle$, where $|a_3\rangle$ is the most significant qubit.

2.2 Target ciphers

Next, we introduce three ciphers that belong to $2EM_1$, $2EM_2$ and $2EM_3$ constructions respectively.

2.2.1 LED

At CHES 2011, Guo *et al.* [29] proposed a 64-bit resource-constrained block cipher named LED. The step function F_i of LED is a 4-round AES-like permutation where the addition of the subkeys is replaced with addition of constants. There are two primary variants of LED.**LED − 64** uses a 64-bit key in each step as a subkey and the number of steps is 8. It is clear that 2-step LED-64 belongs to $2EM_1$ construction.**LED − 128** divides a 128-bit key into $K_1\|K_2$ as the subkeys alternatively and the number of steps is 12. Obviously, 2-step LED-128 belongs to $2EM_2$ construction.

Algorithmic idea : apply Grover search over $i \in \{0,1\}^m$ and the classifier $\mathcal{B}$ identifies the periodicity of $f(i,\cdot)$ using Simon algorithm.
The quantum algorithm $\mathcal{A}$:
Step 1. Prepare the quantum state $|0^{\otimes m}\rangle|0^{\otimes \ell n}\rangle|0^{\otimes \ell l}\rangle$, where $\ell = \mathcal{O}(n)$.
Step 2. Apply Hadamard transforms $H^{\otimes(m+\ell n)}$ to the first $(m+\ell n)$ qubits:

$$\sum_{i\in\{0,1\}^m, x_1,\cdots x_\ell\in\{0,1\}^n} |i\rangle|x_1\rangle\cdots|x_\ell\rangle|0^{\otimes \ell l}\rangle,$$

where the amplitude is omitted for ease of exposition.
Step 3. Perform quantum querise to f for i and each x:

$$\sum_{i\in\{0,1\}^m, x_1,\cdots x_\ell\in\{0,1\}^n} |i\rangle|x_1\rangle\cdots|x_\ell\rangle|f(i,x_1)\,\|\cdots\|\,f(i,x_\ell)\rangle.$$

Step 4. Apply Hadamard transforms $H^{\otimes \ell n}$ to $|x_1\rangle\cdots|x_\ell\rangle$:

$$\sum_{i\in\{0,1\}^m, x_1,\cdots,x_\ell, u_1,\cdots,u_\ell\in\{0,1\}^n} |i\rangle(-1)^{u_1\cdot x_1}|u_1\rangle\cdots(-1)^{u_\ell\cdot x_\ell}|u_\ell\rangle|f(i,x_1)\,\|\cdots\|\,f(i,x_\ell)\rangle.$$

The classifier $\mathcal{B}$: $(i,u_1,\cdots,u_\ell)\in\{0,1\}^{m+\ell n}\to\{0,1\}$:
Test 1. If $\dim(\langle u_1,\cdots,u_\ell\rangle) \neq n-1$, output 0. Otherwise, use Lemma 2 of Ref. [24] to compute a candidate period $s'\in\{0,1\}^n$.
Test 2. For fixed i check whether $f(i,z)=f(i,z\oplus s')$ holds for some given z. If all identities hold, output 1. Otherwise, output 0.
Both Test 1 and Test 2 are satisfied, the classifier $\mathcal{B}$ outputs 1. Otherwise, output 0.

Algorithm 3. Grover-meets-Simon algorithm [24]

2.2.2 AES^2

AES^2 is a 128-bit cipher designed by Bogdanov et al. [3] at EUROCRYPT 2012. It belongs to $2EM_3$ construction, where each of the public permutations P_1 and P_2 is based on an invocation of full AES-128 with a pre-fix and publicly known key. The subkeys are composed of three independently chosen 128-bit secret subkeys K_1, K_2 and K_3.

3 Quantum attacks

In this section, several quantum key-recovery attacks on $2EM_1$, $2EM_2$ and $2EM_3$ constructions and the corresponding applications are given.

3.1 Quantum key-recovery Attack on $2EM_1$ construction

Based on $2EM_1$ construction, the function $E_1(x) = P_2(P_1(x\oplus K)\oplus K)\oplus K$ is obtained. In such a case, we adopt Grover algorithm on this function directly. Therefore, the query complexity and time complexity of this attack are both $\mathcal{O}(2^{n/2})$.

Step 1. Prepare the quantum state $\otimes^{cn}|0^{\otimes n}\rangle|0^{\otimes l}\rangle$, where c is a small constant.
Step 2. Perform Hadamard transforms $\otimes^{cn}H^{\otimes n}$ and cn quantum queries to g:

$$|\psi_g\rangle = \otimes^{cn}\left(\sum_{x\in\{0,1\}^n}|x\rangle|g(x)\rangle\right),$$

where the amplitude is ommitted for ease of exposition.
Step 3. Create the uniform superposition:

$$|\psi_g\rangle\otimes\sum_{i\in\{0,1\}^m}|i\rangle.$$

Step 4. Apply Grover iteration for $\mathcal{O}(2^{m/2})$ times, where the classifier in Grover iteration is to check whether $f(i,x)\oplus g(x)$ is periodic.
Step 5. Measure the register and obtain i_0.
Step 6. Apply Simon algorithm on $f(i_0,x)\oplus g(x)$ to obtain the period s.

Algorithm 4. Offline Simon algorithm [25]

3.1.1 The Application to 2-step LED-64

We can attack 2-step LED-64 by applying Grover algorithm on $E(x) = F_2(F_1(x\oplus K)\oplus K)\oplus K$ directly, where the block size is 64. Thus, the attack requires the query and time complexities of 2^{32}. The comparison of attacks against 2-step LED-64 is summarized in Table 2.

3.2 Quantum key-recovery Attacks on $2EM_2$ and $2EM_3$ constructions

For $2EM_2$ construction, we consider the function

$$\begin{aligned} f(i,x) &= E_2(x)\oplus P_2(P_1(x)\oplus i)\\ &= P_2(P_1(x\oplus K_1)\oplus K_2)\oplus K_1\oplus P_2(P_1(x)\oplus i).\end{aligned}$$

It is easily seen that $f(i, x)$ has the period K_1 when $i = K_2$ since

$$\begin{aligned} f(K_2, x\oplus K_1) &= P_2(P_1(x\oplus K_1\oplus K_1)\oplus K_2)\oplus K_1\oplus P_2(P_1(x\oplus K_1)\oplus K_2)\\ &= P_2(P_1(x)\oplus K_2)\oplus K_1\oplus P_2(P_1(x\oplus K_1)\oplus K_2)\\ &= f(K_2,x).\end{aligned}$$

Therefore, we can employ GMS algorithm on $f(i,x)$ to recover K_1 and K_2 which requires the query complexity of $\mathcal{O}(n\cdot 2^{n/2})$ and time complexity of $\mathcal{O}(n^3\cdot 2^{n/2})$.

Furthermore, the recovery of subkeys K_1 and K_2 can also be reduced to **Problem 4** by defining functions f: $\{0,1\}^n\times\{0,1\}^n\to\{0,1\}^n$ and g: $\{0,1\}^n\to\{0,1\}^n$ as

$$\begin{aligned} f(i,x) &= P_2(P_1(x)\oplus i),\\ g(x) &= E_2(x).\end{aligned}$$

Similarly, we can obtain that

$$f(K_2, x\oplus K_1)\oplus g(x\oplus K_1) = f(K_2,x)\oplus g(x)$$

when $i = K_2$. Then we can recover all subkeys with OS algorithm. In such a case, the quantum attack requires $\mathcal{O}(n)$ queries to $g(x)$, $\mathcal{O}(n\cdot 2^{n/2})$ queries to $f(i, x)$ and the time complexity of $\mathcal{O}(n^3\cdot 2^{n/2})$.

On the other hand, we can also solve this problem with OS algorithm in Q1 model if the cryptographic function $E_2(x)$

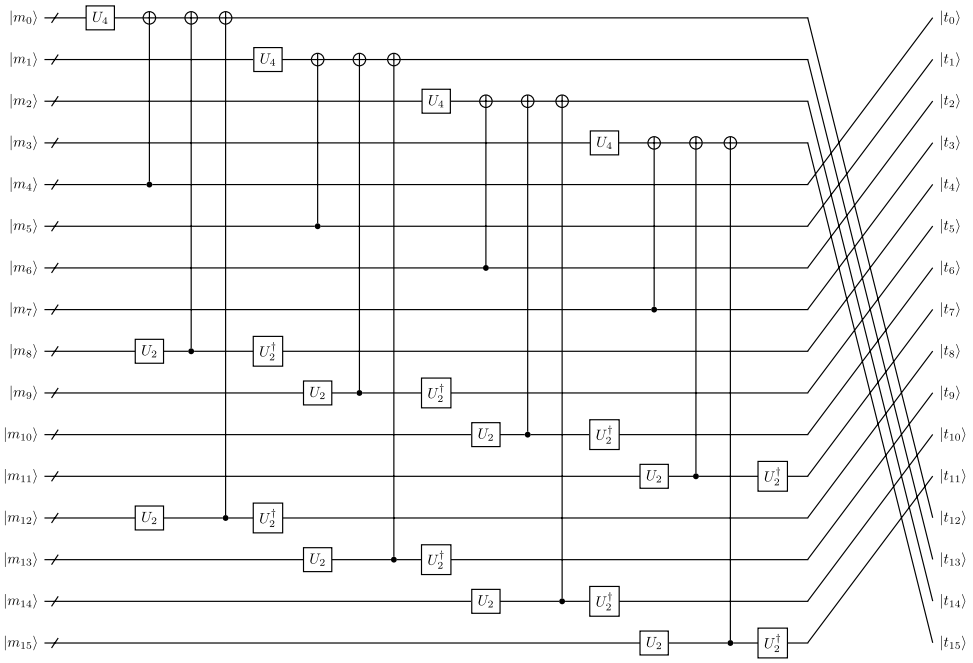

FIGURE 3
Quantum circuit of matrix A, where U_2 and U_4 are quantum circuits of operations 2 and 4 respectively. $U_2^\dagger$ represents the inverse quantum circuit of U_2. Each m_j and t_j contains four qubits, where $j = 0, 1, \ldots, 15$.

can be accessed only classically. Now the functions f: $\{0,1\}^{n+(n-u)} \times \{0,1\}^u \to \{0,1\}^n$ $(0 \le u \le n)$ and g: $\{0,1\}^u \to \{0,1\}^n$ are defined as

$$f(i\|j,x) = P_2(P_1(x\|j) \oplus i) \quad (j \in \{0,1\}^{n-u}),$$
$$g(x) = E_2(x\|0^{n-u}).$$

obviously, $f(K_2\|K_1^2, x) \oplus g(x)$ has the period K_1^1 when $i\|j = (K_2\|K_1^2, x \oplus K_1^1) \oplus g(x \oplus K_1^1)K_2\|K_1^2$ since

$$\begin{aligned} &f(K_2\|K_1^2, x \oplus K_1^1) \oplus g(x \oplus K_1^1) \\ &= P_2(P_1((x \oplus K_1^1)\|K_1^2) \oplus K_2) \oplus P_2(P_1((x \oplus K_1^1\|0^{n-u}) \oplus K_1) \oplus K_2) \oplus K_1 \\ &= P_2(P_1((x\|0^{n-u}) \oplus K_1) \oplus K_2) \oplus P_2(P_1(x\|K_1^2) \oplus K_2) \oplus K_1 \\ &= f(K_2\|K_1^2, x) \oplus g(x), \end{aligned}$$

where the subkey $K_1 = K_1^1\|K_1^2$ and $|K_1^1| = u$, $|K_1^2| = n - u$. Therefore, we can apply OS algorithm on above functions in Q1 model to recover subkeys K_1 and K_2. Then, the attack requires $\mathcal{O}(2^u)$ classical queries to $g(x)$, $\mathcal{O}(n \cdot 2^{(2n-u)/2})$ quantum queries to $f(i\|j, x)$ and the time complexity of $\mathcal{O}(n^3 \cdot 2^{(2n-u)/2})$. Specially, the number of classical queries to $g(x)$ and quantum queries to $f(i\|j, x)$ are balanced when $u = \frac{2n}{3}$.

The quantum key-recovery attack against $2EM_3$ construction is similar to the case of $2EM_2$ construction, except that the functions we considered here are

$$\begin{cases} f(i,x) = E_3(x) \oplus P_2(P_1(x) \oplus i), & \textbf{Problem 3} \\ f(i,x) = P_2(P_1(x) \oplus i),\ g(x) = E_3(x), & \textbf{Problem 4 in Q2 model} \\ f(i\|j,x) = P_2(P_1(x\|j) \oplus i),\ g(x) = E_3(x\|0^{n-u}), & \textbf{Problem 4 in Q1 model} \end{cases}.$$

Finally, we can easily obtain the value of K_3 with additional encryption after recovering subkeys K_1 and K_2. Hence, the query and time complexities of the quantum attacks on $2EM_3$ construction are the same as the case of $2EM_2$ construction.

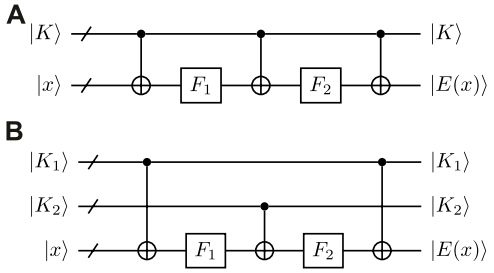

FIGURE 4
Quantum circuit of **(A)** 2-step LED-64 and **(B)** 2-step LED-128, here ancilla qubits are not represented.

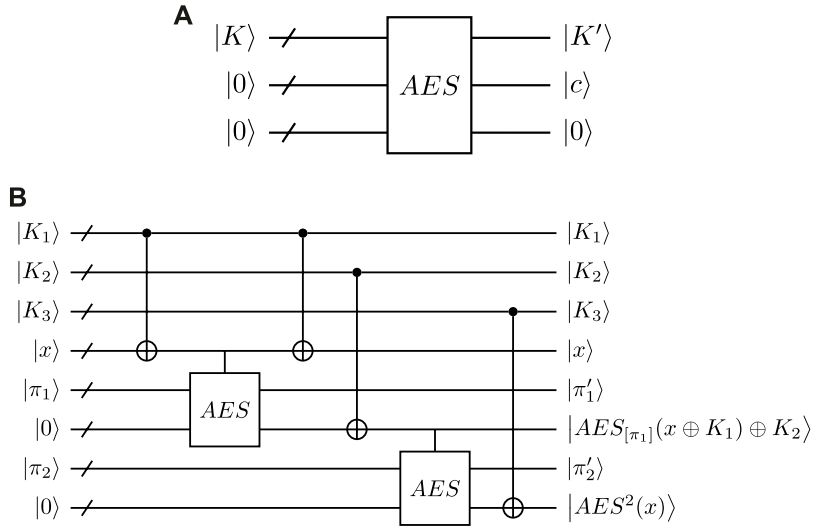

FIGURE 5
Quantum circuit of **(A)** AES, where the box of AES means the quantum circuit of AES-128 in Ref. [35], K' is the subkey of the 10th round in AES and c is the ciphertext; **(B)** AES^2, where the vertical line above the AES box indicates that 128 × 2 CNOT gates are performed instead of 128 × 2 NOT gates in the quantum circuit of AES-128. The ancilla qubits and unused outputs are not represented.

3.2.1 The applications to 2-step LED-128 and AES_2

According to the structure of 2-step LED-128, we can obtain the cryptographic function

$$E(x) = F_2(F_1(x \oplus K_1) \oplus K_2) \oplus K_1,$$

where $|K_1| = |K_2| = 64$. In order to attack 2-step LED-128, we consider the function

$$\begin{aligned} f(i,x) &= E(x) \oplus F_2(F_1(x) \oplus i) \\ &= F_2(F_1(x \oplus K_1) \oplus K_2) \oplus K_1 \oplus F_2(F_1(x) \oplus i) \end{aligned}$$

in **Problem 3**. Now, we can adopt GMS algorithm on $f(i, x)$ directly. Hence, this attack requires the query complexity of 2^{39} and time complexity of 2^{50}.

Furthermore, we can also utilize OS algorithm to recover K_1 and K_2 of 2-step LED-128. First, we define the functions

$$\begin{aligned} f(i,x) &= F_2(F_1(x) \oplus i), \\ g(x) &= E(x). \end{aligned}$$

Then the subkeys can be recovered with OS algorithm on $f(i, x)$ and $g(x)$. The quantum attack requires 2^6 quantum queries to $E(x)$, 2^{38} quantum queries to $f(i, x)$ and time complexity of 2^{50}. On the other hand, we can also consider functions

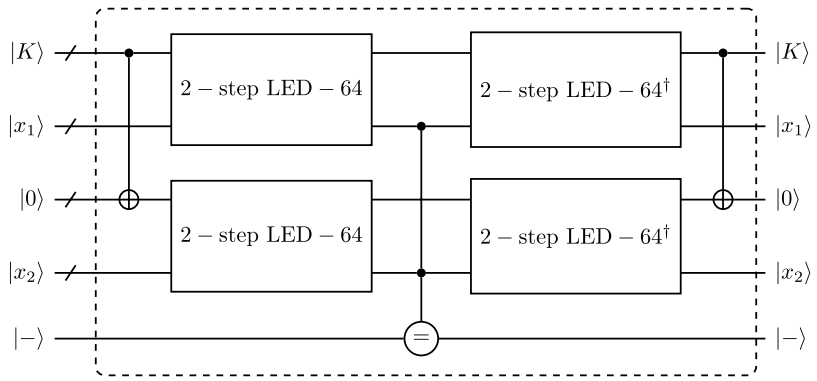

FIGURE 6
Grover oracle for 2-step LED-64.

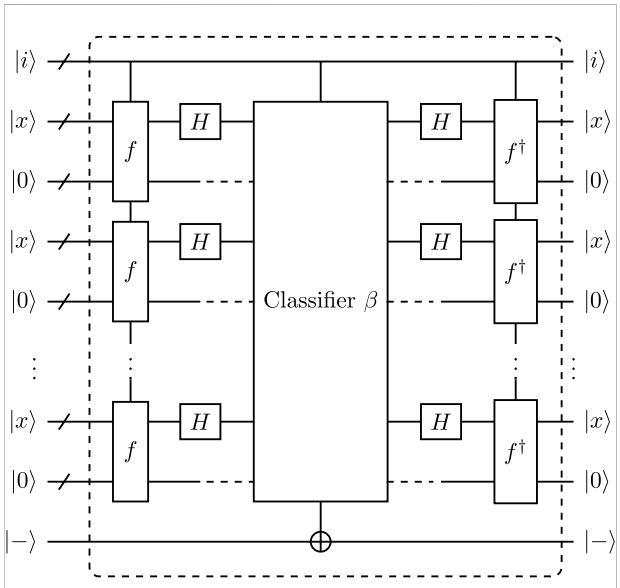

FIGURE 7
Iterative oracle for GMS algorithm, the quantum circuit for classifier β is given in Supplementary Figure S5 of Supplementary B.

$$f(i\|j,x) = F_2(F_1(x\|j) \oplus i),$$
$$g(x) = E(x\|0^{n-u})$$

and apply OS algorithm on $f(i\|j, x)$ and $g(x)$ in Q1 model when $E(x)$ can be queried only classically. In such a case, the quantum attack requires 2^{47} classical queries to $E(x)$, $2^{46.5}$ quantum queries to $f(i\|j, x)$ and time complexity of $2^{58.5}$ when $u = 47$. The comparison of quantum attacks against 2-step LED-128 is summarized in Table 3.

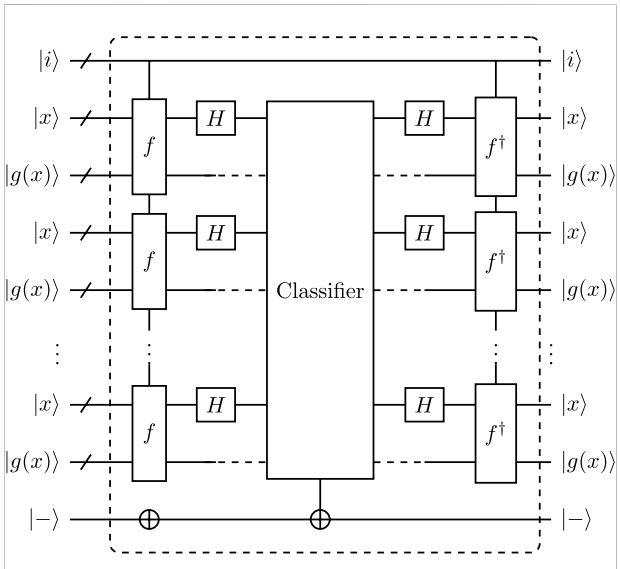

FIGURE 8
Iterative oracle for OS algorithm, the quantum circuit for classifier is provided in Supplementary Figure S6 of Supplementary B.

In order to attack AES_2, we need to construct functions in the case of $2EM_3$ construction described in Section 3.2 with block size 128. Thus, the subkeys of AES^2 can be recovered by GMS algorithm with the query complexity of 2^{72} and time complexity of 2^{85}. Furthermore, we can also attack AES^2 with OS algorithm in Q1 and Q2 model respectively. In Q1 model, the attack requires 2^{90} classical queries to $E(x)$, 2^{90} quantum queries to $f(i\|j, x)$ and the time complexity of 2^{104} when $u = 90$. In Q2 model, the attack requires 2^7 quantum queries to $E(x)$, 2^{71} queries to $f(i, x)$ and the time complexity of 2^{85}. The comparison of attacks against AES^2 is summarized in Table 4.

Tables 3 and 4 show that the quantum attacks we proposed in Q1 and Q2 models are more efficient than existing classical and quantum attacks in time complexity and query complexity when we consider queries of cryptographic function and public permutations, except that more qubits are needed.

4 Resource estimation

We first give some quantum gates that are used in quantum implementations of classical circuits in Figure 1. Note that the last qubit is target qubit and other qubits are control qubits in CNOT and Toffoli gates.

4.1 Resource estimation of target ciphers

Next, we give the quantum resource estimation of 2-step LED-64, 2-step LED-128 and AES^2 respectively.

4.1.1 Resource estimation of 2-step LED-64 and 2-step LED-128

The internal state of LED contains 64 bits, arranged in 16 nibbles. Each nibble represents an element from $GF(2^4)$ with the underlying polynomial for field multiplication given by $X^4 + X + 1$. The step function F_i of LED cipher is a 4-round AES-like permutation. Each of these four rounds consists of operations AddConstants, SubCells, ShiftRows and MixColumnsSerial.

AddConstants. The operation consists of XOR-ing of a 32-bit round constant to the internal state of LED. Thus, it can be realized by using 32 NOT gates in quantum circuit.

SubCells. LED cipher uses a 4-bit to 4-bit S-box of PRESENT [30], which is applied in parallel 16 times to the internal state of LED. According to Algorithm 3 of Ref. [31], the quantum circuit of the S-box is redesigned in Figure 2, which requires Toffoli depth 19, 19 Toffoli gates, 5 CNOT gates, 2 NOT gates and 5 qubits. Therefore, we can obtain the resource estimation of SubCells by multiplying the resources of the S-box by 16, except

TABLE 6 Resource estimation for iterative oracle of GMS algorithm and OS algorithm, where Clifford gate denotes the CNOT gate and Hadamard gate.

Algorithm	Model	Target cipher	Toffoli depth	#Toffoli	#Clifford	#NOT	width
GMS	Q2	2-step LED-128	62327	4759241	4516500	762376	25152
GMS	Q2	AES^2	12508008	83407802	368607419	3734666	365444
OS	Q1&Q2	2-step LED-128	4954	2887806	1966081	327809	26880
OS	Q1&Q2	AES^2	53626	31698174	105088001	1044737	270848

for the Toffoli depth since that these 16 S-boxes are applied in parallel.

ShiftRows. After the operation ShiftRows, the internal state is changed into a special permutation. Hence, we do not have to perform any operation for the quantum circuit of ShiftRows since it corresponds to a permutation of qubits. In this case, we only need to adjust the position of subsequent operations to ensure that the correct input wire is used.

MixColumnsSerial. The MixColumnsSerial performs four applications of matrix A, which is equivalent to matrix M:

$$(A)^4 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 4 & 1 & 2 & 2 \end{pmatrix}^4 = \begin{pmatrix} 4 & 1 & 2 & 2 \\ 8 & 6 & 5 & 6 \\ B & E & A & 9 \\ 2 & 2 & F & B \end{pmatrix} = M.$$

The first scheme of implementing MixColumnsSerial is to realize matrix A. In order to design the quantum circuit of matrix A, the quantum circuit of operations 2 and 4 in A should be considered first. It is easy to obtain that $2 \cdot (a_3, a_2, a_1, a_0) = (a_2, a_1, a_3 \oplus a_0, a_3)$ and $4 \cdot (a_3, a_2, a_1, a_0) = (a_1, a_3 \oplus a_0, a_3 \oplus a_2, a_2)$. Hence, the implementation of operations 2 and 4 cost 1 and 2 CNOT gates respectively. Now, we can design the quantum circuit of matrix A based on operations 2 and 4 in Figure 3.

According to Figure 3, we can derive that the quantum circuit of matrix A requires $(2 + 4 + 6 + 6) \times 4 = 72$ CNOT gates. Thus, the resource estimation for operation MixColumnsSerial is $72 \times 4 = 288$ CNOT gates.

The second scheme is to consider the matrix M directly. From SageMath [32], we can obtain the PLU decomposition

$$M = \begin{pmatrix} 4 & 1 & 2 & 2 \\ 8 & 6 & 5 & 6 \\ B & E & A & 9 \\ 2 & 2 & F & B \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 6 & 2 & 1 & 0 \\ 9 & 6 & 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 4 & 1 & 2 & 2 \\ 0 & 4 & 1 & 2 \\ 0 & 0 & 4 & 1 \\ 0 & 0 & 0 & 4 \end{pmatrix}.$$

Similarly, we can easily obtain that $6 \cdot (a_3, a_2, a_1, a_0) = (a_2 \oplus a_1, a_3 \oplus a_1 \oplus a_0, a_2 \oplus a_0, a_3 \oplus a_2)$ and $9 \cdot (a_3, a_2, a_1, a_0) = (a_0, a_3, a_2, a_1 \oplus a_0)$, which can be achieved with 5 and 1 CNOT gates respectively. Then, we can know that the matrix L and U require $4\times([(1 + 4 + 1) + (5 + 4 + 5) + (1 + 4 + 1)] + [(5 + 4 + 5) + (1 + 4 + 1)] + (1 + 4 + 1)) = 208$ and $4 \times ([2 + 4 + (1 + 4 + 1) + (1 + 4 + 1)] + [2 + 4 + (1 + 4 + 1)] + (2 + 4) + 2) = 152$ CNOT gates respectively. Therefore, the resource estimation for operation MixColumnsSerial is $208 + 152 = 360$ CNOT gates in second scheme. Comparing these two schemes, we adopt first one to implement the operation MixColumnsSerial since it requires fewer CNOT gates.

Taking all these into consideration, we can derive that the resource estimation of one round AES-like permutation costs Toffoli depth 19, 304 Toffoli gates, 368 CNOT gates, 64 NOT gates and 80 qubits. Then the quantum circuits of 2-step LED-64 and 2-step LED-128 are presented in Figure 4. In such a case, the quantum circuit of 2-step LED-64 requires Toffoli depth 152, 2432 Toffoli gates, 3136 CNOT gates, 512 NOT gates and 144 qubits. The quantum circuit of 2-step LED-128 costs Toffoli depth 152, 2432 Toffoli gates, 3136 CNOT gates, 512 NOT gates and 208 qubits.

TABLE 7 Resource estimation for proposed quantum attacks on target ciphers, where all figures are in log base 2. The values of u of OS algorithm in Q1 model for 2-step LED-128 and AES^2 are 47 and 90, respectively.

Algorithm	Model	Target cipher	Toffoli depth	#Toffoli	#Clifford	#NOT	width
GMS	Q2	2-step LED-128	47.6	53.8	53.8	51.2	14.6
GMS	Q2	AES^2	87.2	90.0	92.1	85.5	18.5
OS	Q2	2-step LED-128	43.9	53.1	52.6	50.0	14.7
OS	Q2	AES^2	79.4	88.6	90.3	83.6	18.0
OS	Q1	2-step LED-128	52.4	61.6	61.1	58.5	14.7
OS	Q1	AES^2	98.4	107.6	109.3	102.6	18.0

4.1.2 Resource estimation of AES²

The construction of AES² is defined by fixing two randomly chosen 128-bit AES-128 keys, which specify the permutations P_1 and P_2. The subkeys are comprised of three independently chosen 128-bit secret keys K_1, K_2 and K_3. Let AES[K] denotes the whole AES-128 encryption with the 128-bit key K. Hence, the encryption of AES² is defined as

$$\mathrm{AES}^2(x) = \mathrm{AES}[\pi_2](\mathrm{AES}[\pi_1](x \oplus K_1) \oplus K_2) \oplus K_3,$$

where two 128-bit keys π_1 and π_2 are defined based on the first 256 bits of the binary digit expansion of π. Recently, the implementation of AES quantum circuit received more and more attention [33–35]. Based on the fewer qubits principle, we take the quantum circuit of AES-128 from Ref. [35] for quntum circuit design of AES². As shown in Figure 5A, this quantum circuit costs Toffoli depth 11008, 16508 Toffoli gates, 81652 CNOT gates, 1072 NOT gates and 270 qubits. In Ref. [35], the XOR of a 128-bit plaintext in first round of AES-128 is considered as XOR-ing of a 128-bit constant, which is achieved by performing 128 NOT gates on the key of AES-128 first and then canceled by 128 NOT gates again. However, the 128-bit plaintext is a quantum superposition in our proposed quantum attacks. Hence, we need to adopt 128 × 2 CNOT gates instead of 128 × 2 NOT gates here. Therefore, the quantum circuit of AES-128 used in the quantum circuit design of AES² requires Toffoli depth 11008, 16508 Toffoli gates, 81908 CNOT gates, 816 NOT gates and 270 qubits. In such a case, we can easily design the quantum circuit of AES² in Figure 5B and obtain the resource estimation of AES² with Toffoli depth 22016, 33016 Toffoli gates, 164328 CNOT gates, 1632 NOT gates and 1038 qubits. Note that the ancilla qubits involved in first AES quantum circuit can be reused in second AES quantum circuit.

4.2 Resource estimation of Grover algorithm on 2-step LED-64

In order to adopt Grover algorithm on 2-step LED-64, we need to design the Grover oracle for 2-step LED-64 first. When designing the Grover oracle, the number of plaintext-ciphertext pairs required to recover the correct key uniquely should be considered. At EUROCRYPT 2020, Jaques *et al.* [34] stated that when the number of required plaintext-ciphertext pairs $\nu \geq \lceil \frac{m}{n} \rceil$, the probability of uniquely recovering the correct key is about $e^{-2^{m-\nu n}}$, where n and m are block size and key size for a block cipher respectively.

Hence, the number of required plaintext-ciphertext pairs for 2-step LED-64 should be $\nu \geq 1$ since $m = n = 64$. Then the probability of finding a unique key is around 0.37 for $\nu = 1$. For $\nu = 2$, the probability is about 0.99. Thus, we consider the case of $\nu = 2$ when designing the Grover oracle for 2-step LED-64. Therefore, the quantum circuit of the Grover oracle for 2-step LED-64 is illustrated in Figure 6, which requires Toffoli depth 317, 9981 Toffoli gates, 12672 CNOT gates, 2304 NOT gates and 383 qubits. In the quantum circuit of Grover oracle for 2-step LED-64, each comparison of n-bit known ciphertext and n-qubit output of 2-step LED-64 oracle requires Toffoli depth $2\lceil \log_2 n \rceil$, $2(n-1)$ Toffoli gates, $2n$ NOT gates and $(n-1)$ ancilla qubits.

In the process of Grover algorithm, $\lfloor \frac{\pi}{4} 2^{m/2} \rfloor$ iterations of Grover operator are performed. While estimating the resources, we only consider the cost incurred by Grover oracle. Since compared with the cost incurred by Grover oracle, the cost imposed by other operations in Grover operator is relatively small in terms of magnitude and can be ignored. In such a case, the resources of Grover oracle for 2-step LED-64 are multiplied by $\lfloor \frac{\pi}{4} 2^{m/2} \rfloor$ for estimating the resources of Grover algorithm on 2-step LED-64, which costs Toffoli depth $2^{40.0}$, $2^{44.9}$ Toffoli gates, $2^{45.3}$ CNOT gates, $2^{42.8}$ NOT gates and $2^{8.6}$ qubits. Note that the width is still the same as in Grover oracle since we assume that no parallelization is involved.

4.3 Resource estimation of proposed quantum attacks on 2-step LED-128 and AES²

The resource estimation of proposed quantum attacks on 2-step LED-128 and AES² can be considered in a similar way as Grover algorithm since that Grover algorithm, GMS algorithm and OS algorithm all need to perform an iterative operator. Thus, we should consider the resource estimation of iterative oracle for target ciphers first. Here, the resource estimation of constructed functions for target ciphers in proposed quantum attacks is given in Table 5 and the corresponding quantum circuits see Supplementary A.

Now, the quantum circuits of iterative oracle for GMS algorithm and OS algorithm are designed in Figure 7 and Figure 8 respectively.

In Figure 7, the classifier β for GMS algorithm contains Test 1 and Test 2 (see also Supplementary Figure S5 of Supplementary B). When both two test conditions are satisfied, the phase of target qubit will be flipped. Test 1 of classifier β. The Test 1 of classifier β includes the checking of dim $(\langle u_1, \ldots, u_\ell \rangle)$ and the calculation of candidate period s'. The first phase includes the computation of triangular basis and the rank checking of triangular basis. Based on Algorithm 4 of Ref. [36], we can obtain that the computation of triangular basis requires Toffoli depth $\ell(4 + \lceil \log_2 n \rceil) + \sum_{i=2}^{n} (4 + \lceil \log_2 (n - i + 1) \rceil)$, $\ell n^2 + \ell n$ Toffoli gates and $\ell + n(n+1)/2 + n(n-1)$ ancilla qubits, where the value of ℓ is $2(n + \sqrt{n})$ [24]. For the rank checking of triangular basis, it requires Toffoli depth $2\lceil \log_2 n \rceil$, $2(n-1)$ Toffoli gates, $2n$ NOT gates and $(n-1)$ ancilla qubits. The second phase is the calculation of the candidate period. Bonnetain *et al.* [36] showed that the realizing of computing orthogonal vectors (*i.e.,* Algorithm 5 in Ref. [36]) costs Toffoli depth $n(n-1)$, $n(n-1)$ Toffoli gates, n CNOT gates and n ancilla

qubits. However, there is a mistake that the Toffoli depth and Toffoli gates should be $n(n-1)/2$. Thus, we can obtain that the resource estimation for Test 1 of classifier β requires Toffoli depth $\ell(4+\lceil\log_2 n\rceil)+\sum_{i=2}^{n}(4+\lceil\log_2(n-i+1)\rceil)+2\lceil\log_2 n\rceil+n(n-1)/2$, $\ell n^2+\ell n+2(n-1)+n(n-1)/2$ Toffoli gates, n CNOT gates, $2n$ NOT gates and $\ell+n(n+1)/2+n(n-1)+n$ ancilla qubits by combining all these terms. Note that there are $(n-1)$ ancilla qubits missing since the ancilla qubits in the process of rank checking can be reused in the computation of orthogonal vectors. In this case, we only need $\max\{n-1, n\}$ ancilla qubits in these two processes. Test 2 of classifier β. The quantum circuit of Test 2 of classifier β for 2-step LED-128 is given in Supplementary Figure S7 of Supplementary B, which costs

$$\begin{cases} \text{Toffoli depth} \quad 147\times(76\times 4+2\log_2 64+49)+5=53660 & \\ 147\times[1216\times 8+2\times(64-1)+49]+13=1455754 & \text{Toffoli gates}\\ 147\times(1472\times 8+64\times 10+1)=1825299 & \text{CNOT gates},\\ 147\times(256\times 8+64\times 2)+8=319880 & \text{NOT gates}\\ 64\times 2+63+6+8+1=206 & \text{qubits}\end{cases}$$

since $t=1,2,\ldots,147$ (i.e., $\frac{3n+n\ell}{n}$) [24] in Supplementary Figure S7. Here $|i\rangle$ and the candidate period $|s'\rangle$ are not included in the qubits. The quantum circuit of Test 2 of classifier β for AES^2 is provided in Supplementary Figure S8 of Supplementary B, which requires

$$\begin{cases} \text{Toffoli depth} \quad 282\times(11008\times 4+2\log_2 128+64)+7=12439027 & \\ 282\times[16508\times 8+2\times(128-1)+64]+15=37331739 & \text{Toffoli gates}\\ 282\times(81908\times 8+128\times 10+1)=185145690 & \text{CNOT gates},\\ 282\times(816\times 8+128\times 2)+10=1913098 & \text{NOT gates}\\ 128\times 10+127+9+7+1=1424 & \text{qubits}\end{cases}$$

where $t=1,2,\ldots,282$ in Supplementary Figure S8. Here $|i\rangle$ and $|s'\rangle$ are not included in the qubits.

Hence, the classifier β for 2-step LED-128 costs

$$\begin{cases} \text{Toffoli depth} \quad 2\times(2007+6+2016)+53660+1=61719 & \\ 2\times(599040+63+2016)+1455754+1=2657993 & \text{Toffoli gates}\\ 2\times 64+1825299+1=1825428 & \text{CNOT gates},\\ 2\times 64+319880=320008 & \text{NOT gates}\\ 6256+64+206+1+1=6528 & \text{qubits}\end{cases}$$

where $|u_1\rangle, |u_2\rangle, \cdots, |u_\ell\rangle$ and $|i\rangle$ are not included in the qubits. The classifier β for AES^2 costs

$$\begin{cases} \text{Toffoli depth} \quad 2\times(4339+7+8128)+12439027+1=12463976 & \\ 2\times(4606848+127+8128)+37331739+1=46561946 & \text{Toffoli gates}\\ 2\times 128+185145690+1=185145947 & \text{CNOT gates}.\\ 2\times 128+1913098=1913354 & \text{NOT gates}\\ 24791+128+1424+1+1=26345 & \text{qubits}\end{cases}$$

Altogether, the resource estimation for iterative oracle of GMS algorithm is summarized in Table 6.

In Supplementary Figure S6 of Supplementary B, the classifier oracle of OS algorithm consists of the computation of triangular basis and rank checking. Therefore, the classifier oracle costs Toffoli depth $2\star[cn\star(4+\lceil\log_2 n\rceil)+\sum_{i=2}^{n}(4+\lceil\log_2(n-i+1)\rceil)+\lceil\log_2 n\rceil]$, $2\star[cn\star n^2+cn\star n+(n-1)]$ Toffoli gates, 1 CNOT gates, $2n+1$ NOT gates and $cn+n(n+1)/2+n(n-1)+(n-1)+1$ ancilla qubits, where $cn\simeq 2.5n$ [25]. Then, the corresponding resource estimation for iterative oracle of OS algorithm is listed in Table 6. Here, the resource estimation for iterative oracle of OS algorithm in Q1 model is same as the case of OS algorithm in Q2 model, except that the width in Q1 model should consider extra $(n-u)$ qubits.

Similarly, $\lceil\frac{\pi}{4}2^{n/2}\rceil$ iterations for the iterative operator of proposed quantum attacks are required. Here, we only consider the cost incurred by the iterative oracle and assume that the iterative oracle is applied in serial. Hence, the resources (except the number of qubits) in Table 6 are multiplied by $\lceil\frac{\pi}{4}2^{n/2}\rceil$ for estimating the resources of mounting presented quantum attacks on 2-step LED-128 and AES^2. The resource estimation is summarized in Table 7. From Table 7, it is obvious that the proposed quantum attacks based on GMS algorithm cost more than ones with OS algorithm in Q2 model. The main reason for this is caused by Test 2 of classifier β in GMS algorithm, which needs to check whether $f(i,z)=f(i,z\oplus s')$ for fixed i, the given t pairs of z and thus requires more resources. Note that the cost incurred by proposed quantum attacks with OS algorithm in Q1 model is more than the ones in Q2 model because guessing the value of j requires another $2^{(n-u)/2}$ iterations. Moreover, we also give the resource estimation for Grover algorithm on 2-step LED-128 and AES^2 in Supplementary C. Compared with the proposed quantum attacks on 2-step LED-128 and AES^2, the corresponding Grover algorithm costs much more since the Grover algorithm requires more iterations, except for the width.

Besides, it is worth noting that the resource estimation for OS algorithm in Q1 model should also consider the cost of preparing the quantum state $|\psi_g\rangle=\otimes^{cn}(\sum_{x\in\{0,1\}^n}|x\rangle|g(x)\rangle)$ with quantum read-only memory (QROM). According to Theorem 2 of Ref. [37], we can obtain that the transform

$$\sum_{x\in\{0,1\}^u}|x\rangle|0\rangle\mapsto\sum_{x\in\{0,1\}^u}|x\rangle|g(x)\rangle$$

costs Toffoli depth $\lceil 2^u/\omega\rceil+n(\omega-1)$, $\lceil 2^u/\omega\rceil+n(\omega-1)$ Toffoli gates and $n(\omega-1)+\lceil\log(2^u/\omega)\rceil)$ ancilla qubits, where ω is a power of 2 such that $1<\omega<2^u$. Therefore, the preparing of the quantum state $|\psi_g\rangle$ in OS algorithm for 2-step LED-128 requires Toffoli depth 2^{46}, $2^{53.3}$ Toffoli gates and $2^{14.1}$ ancilla qubits when $\omega=2$. The preparing of the quantum state $|\psi_g\rangle$ in OS algorithm for AES^2 costs Toffoli depth 2^{88}, $2^{96.3}$ Toffoli gates and $2^{17.2}$ ancilla qubits when $\omega=4$. In such a case, we can easily prepare the quantum state $|\psi_g\rangle$ under the resources of the iteration in OS algorithm. Therefore, the cost incurred by preparing the quantum state $|\psi_g\rangle$ of OS algorithm in Q1 model can be ignored. Similarly, the cost imposed by recovering the period K_1 of GMS and OS algorithms can also be ignored since it is relatively small in terms of magnitude compared with the iteration in GMS and OS algorithms.

5 Conclusion

In this study, we consider the security of two-round Even-Mansour constructions in quantum setting. Compared with the

classical attack with optimal query complexity, the presented quantum key-recovery attack on $2EM_1$ construction reduces the query complexity by a factor of $2^{n/6}$. For $2EM_2$ and $2EM_3$ constructions, we design quantum key-recovery attacks in Q1 and Q2 model respectively. The comparison in Table 2 shows that our attacks are more efficient than Grover search and QMITM attack no matter in Q1 or Q2 model. Furthermore, we also give the applications of proposed quantum attacks and analyze the corresponding resource estimation.

Data availability statement

The original contributions presented in the study are included in the article/Supplementary Material, further inquiries can be directed to the corresponding author.

Author contributions

These authors contributed equally to this work.

Funding

This work was supported by National Natural Science Foundation of China (Grant Numbers 61972048, 61976024), Henan Key Laboratory of Network Cryptography Technology (LNCT2021-A10), BUPT Excellent Ph.D. Students Foundation (Grant Number CX2019207) and China Scholarship Council (Grant Number 202006470082).

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

Supplementary material

The Supplementary Material for this article can be found online at: https://www.frontiersin.org/articles/10.3389/fphy.2022.1028014/full#supplementary-material

References

1. Even S, Mansour Y. A construction of a cipher from a single pseudorandom permutation. *J Cryptology* (1997) 10(3):151–61. doi:10.1007/s001459900025

2. Orr D, Keller N, Shamir A. Minimalism in cryptography: The even-mansour scheme revisited. In: D Pointcheval T Johansson, editors. *Advances in cryptology - EUROCRYPT 2012 - 31st annual international conference on the theory and applications of cryptographic techniques*. Cambridge, UK: Springer (2012). p. 336–54. April 15-19, 2012. Proceedings, volume 7237 of Lecture Notes in Computer Science.

3. Bogdanov A, Knudsen LR, Leander G, Standaert F-X, Steinberger JP, Tischhauser E. Key-alternating ciphers in a provable setting: Encryption using a small number of public permutations - (extended abstract). In: D Pointcheval T Johansson, editors. *Advances in cryptology - EUROCRYPT 2012 - 31st annual international conference on the theory and applications of cryptographic techniques*. Cambridge, UK: Springer (2012). p. 45–62. April 15-19, 2012. Proceedings, volume 7237 of Lecture Notes in Computer Science.

4. Lampe R, Patarin J, Seurin Y. An asymptotically tight security analysis of the iterated even-mansour cipher. In: X Wang K Sako, editors. *Advances in cryptology - ASIACRYPT 2012 - 18th international conference on the theory and application of cryptology and information security*. Beijing, China: Springer (2012). p. 278–95. December 2-6, 2012. Proceedings, volume 7658 of Lecture Notes in Computer Science.

5. Chen S, Steinberger JP. Tight security bounds for key-alternating ciphers. In: PQ Nguyen E Oswald, editors. *Advances in cryptology - EUROCRYPT 2014 - 33rd annual international conference on the theory and applications of cryptographic techniques*. Copenhagen, Denmark: Springer (2014). p. 327–50. May 11-15, 2014. Proceedings, volume 8441 of Lecture Notes in Computer Science.

6. Jordan SP, Liu Y-K. Quantum cryptanalysis: Shor, grover, and beyond. *IEEE Secur Priv* (2018) 16(5):14–21. doi:10.1109/msp.2018.3761719

7. Bennett CH, Brassard G. *Quantum cryptography: Public key distribution and coin tossing* (2020). *arXiv preprint arXiv:2003.06557*.

8. Deng FG, Long GL. Bidirectional quantum key distribution protocol with practical faint laser pulses. *Phys Rev A* (2004) 70(1):012311. doi:10.1103/PhysRevA.70.012311

9. Ye T-Y, Li H-K, Hu J-L. Semi-quantum key distribution with single photons in both polarization and spatial-mode degrees of freedom. *Int J Theor Phys (Dordr)* (2020) 59(9):2807–15. doi:10.1007/s10773-020-04540-y

10. Ye T-Y, Geng M-J, Xu T-J, Chen Y. Efficient semiquantum key distribution based on single photons in both polarization and spatial-mode degrees of freedom. *Quan Inf Process* (2022) 21(4):123–1. doi:10.1007/s11128-022-03457-1

11. Zhandry M. How to construct quantum random functions. In: *53rd annual IEEE symposium on foundations of computer science*. New Brunswick, NJ, USA: FOCSIEEE Computer Society (2012). p. 679–87. October 20-23, 2012.

12. Kaplan M, Leurent G, Anthony L, Naya-Plasencia M. Breaking symmetric cryptosystems using quantum period finding. In: M Robshaw J Katz, editors. *Advances in cryptology - CRYPTO 2016 - 36th annual international cryptology conference*. Santa Barbara, CA, USA: Springer (2016). p. 207–37. August 14-18, 2016, Proceedings, Part II, volume 9815 of Lecture Notes in Computer Science.

13. 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: IEEE (2012). p. 312–6. October 28-31, 2012.

14. Alagic G, Chen B, Katz J, Majenz C. Post-quantum security of the even-mansour cipher. In: *Orr dunkelman and stefan DziembowskiAdvances in cryptology - EUROCRYPT 2022 - 41st annual international conference on the theory and applications of cryptographic techniques*. Trondheim, Norway: Springer (2022). p. 458–87. May 30 - June 3, 2022, Proceedings, Part III, volume 13277 of Lecture Notes in Computer Science.

15. Kaplan M. Quantum attacks against iterated block ciphers. *CoRR abs* (2014) 1410–34.

16. Brassard G, Høyer P, Tapp A. Quantum cryptanalysis of hash and claw-free functions. In: CL Lucchesi AV Moura, editors. *Latin '98: Theoretical informatics, third Latin American symposium*. Campinas, Brazil: Springer (1998). p. 163–9. April, 20-24, 1998, Proceedings, volume 1380 of Lecture Notes in Computer Science.

17. Nikolic I, Wang L, Wu S. Cryptanalysis of round-reduced LED. *IACR Cryptol Eprint Arch* (2015) 429.

18. Dinur I, Orr D, Keller N, Shamir A. Key recovery attacks on 3-round even-mansour, 8-step led-128, and full AES2. In: K Sako P Sarkar, editors. *Advances in cryptology - ASIACRYPT 2013 - 19th international Conference on the Theory and Application of Cryptology and information security*. Bengaluru, India: Springer (2013). p. 337–56. December 1-5, 2013, Proceedings, Part I, volume 8269 of Lecture Notes in Computer Science.

19. Dinur I, Orr D, Keller N, Shamir A. Key recovery attacks on iterated even-mansour encryption schemes. *J Cryptol* (2016) 29(4):697–728. doi:10.1007/s00145-015-9207-3

20. Isobe T, Shibutani K. New key recovery attacks on minimal two-round even-mansour ciphers. In: T Takagi T Peyrin, editors. *Advances in cryptology - ASIACRYPT 2017 - 23rd international Conference on the Theory and Applications of Cryptology and information security*. Hong Kong, China: Springer (2017). p. 244–63. December 3-7, 2017, Proceedings, Part I, volume 10624 of Lecture Notes in Computer Science.

21. Leurent G, Sibleyras F. Low-memory attacks against two-round even-mansour using the 3-xor problem. In: S Barbara, editor. *Alexandra boldyreva and daniele MicciancioAdvances in cryptology - CRYPTO 2019 - 39th annual international cryptology conference*. CA, USA: Springer (2019). p. 210–35. August 18-22, 2019, Proceedings, Part II, volume 11693 of Lecture Notes in Computer Science.

22. Hosoyamada A, Aoki K. On quantum related-key attacks on iterated even-mansour ciphers. *IEICE Trans Fundamentals* (2019) 102(1):27–34. doi:10.1587/transfun.e102.a.27

23. Grover LK. A fast quantum mechanical algorithm for database search. In: GL Miller, editor. *Proceedings of the twenty-eighth annual ACM symposium on the theory of computing*. Philadelphia, Pennsylvania, USA: ACM (1996). p. 212–9. May 22-24, 1996.

24. Leander G, May A. Grover meets simon - quantumly attacking the fx-construction. In: T Takagi T Peyrin, editors. *Advances in cryptology - ASIACRYPT 2017 - 23rd international Conference on the Theory and Applications of Cryptology and information security*. Hong Kong, China: Springer (2017). p. 161–78. December 3-7, 2017, Proceedings, Part II, volume 10625 of Lecture Notes in Computer Science.

25. Bonnetain X, Hosoyamada A, Naya-Plasencia M, Sasaki Y, Schrottenloher A. Quantum attacks without superposition queries: The offline simon's algorithm. In: SD Galbraith S Moriai, editors. *Advances in cryptology - ASIACRYPT 2019 - 25th international Conference on the Theory and Application of Cryptology and information security*. Kobe, Japan: Springer (2019). p. 552–83. December 8-12, 2019, Proceedings, Part I, volume 11921 of Lecture Notes in Computer Science.

26. Brassard G, Hoyer P, Mosca M, Tapp A. Quantum amplitude amplification and estimation. *Contemp Math* (2002) 305:53–74. doi:10.1090/conm/305/05215

27. Simon DR. On the power of quantum computation. *SIAM J Comput* (1997) 26(5):1474–83. doi:10.1137/s0097539796298637

28. Kilian J, Rogaway P. How to protect DES against exhaustive key search. In: K Neal, editor. *Advances in cryptology - CRYPTO '96, 16th annual international cryptology conference*. Santa Barbara, California, USA: Springer (1996). p. 252–67. August 18-22, 1996, Proceedings, volume 1109 of Lecture Notes in Computer Science.

29. Guo J, Peyrin T, Poschmann A, Matthew JB. Robshaw. The LED block cipher. In: *Bart preneel and tsuyoshi TakagiCryptographic hardware and embedded systems - CHES 2011 - 13th international workshop*. Nara, Japan: Springer (2011). p. 326–41. September 28 - October 1, 2011, Proceedings, volume 6917 of Lecture Notes in Computer Science.

30. Bogdanov A, Knudsen LR, Leander G, Paar C, Poschmann A, Matthew J, et al. Present: An ultra-lightweight block cipher. In: *Pascal paillier and ingrid VerbauwhedeCryptographic hardware and embedded systems - CHES 2007, 9th international workshop*. Vienna, Austria: Springer (2007). p. 450–66. September 10-13, 2007, Proceedings, volume 4727 of Lecture Notes in Computer Science.

31. Rahman M, Paul G. Grover on present: Quantum resource estimation. In: *IACR cryptol. ePrint arch.* (2021). p. 1655.

32. Stein W. *Sage mathematics software* (2007). Available at: http://www.sagemath//org.

33. Zou J, Wei Z, Sun S, Liu X, Wu W. Quantum circuit implementations of AES with fewer qubits. In: S Moriai H Wang, editors. *Advances in cryptology - ASIACRYPT 2020 - 26th international Conference on the Theory and Application of Cryptology and information security, daejeon*. South Korea: Springer (2020). p. 697–726. December 7-11, 2020, Proceedings, Part II, volume 12492 of Lecture Notes in Computer Science.

34. Jaques S, Naehrig M, Roetteler M, Virdia F. Implementing grover oracles for quantum key search on AES and lowmc. In: A Canteaut Y Ishai, editors. *Advances in cryptology - EUROCRYPT 2020 - 39th annual international conference on the theory and applications of cryptographic techniques*. Zagreb, Croatia: Springer (2020). p. 280–310. May 10-14, 2020, Proceedings, Part II, volume 12106 of Lecture Notes in Computer Science.

35. Li ZQ, Cai BB, Sun HW, Liu HL, Wan LC, Qin SJ, et al. Novel quantum circuit implementation of advanced encryption standard with low costs. *Sci China Phys Mech Astron* (2022) 65(9):290311–6. doi:10.1007/s11433-022-1921-y

36. Bonnetain X, Jaques S. Quantum period finding against symmetric primitives in practice. *IACR Trans Cryptogr Hardw Embed Syst* (2022) 2022(1):1–27. doi:10.46586/tches.v2022.i1.1-27

37. Berry DW, Craig G, Motta M, McClean JR, Ryan B. Qubitization of arbitrary basis quantum chemistry leveraging sparsity and low rank factorization. *Quantum* (2019) 3:208. doi:10.22331/q-2019-12-02-208