Quantum Information & Computation
ISSN 1533-7146 Volume 25 (2025) pp.421–437
©Cerebration Science Publishing

Article

Tight Analysis of Grover-Meets-Simon and Alg-PolyQ2 Attacks via Formalizing Quantum Rank-Solving under Deferred Measurement

Qiqing Xia [1,2,3], Qianru Zhu [1,2,3], Huiqin Xie [4] and Li Yang [1,2,3,*]

[1] Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100085, China; xiaqiqing@iie.ac.cn (Q.X.); zqr971023@163.com (Q.Z.)
[2] State Key Laboratory of Cyberspace Security Defense, Beijing 100085, China
[3] School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
[4] Beijing Electronic Science and Technology Institute, Beijing 100070, China; xiehuiqindky@163.com
* Corresponding author: yangli@iie.ac.cn

Received date: 24 July 2025; Accepted date: 18 August 2025; Published online: 25 September 2025

Abstract: The combination of quantum algorithms is one promising approach to attacking symmetric cryptography. In this paper, we study in detail the Grover-meets-Simon and Alg-PolyQ2 algorithms under deferred measurement, which combine the ideas of Grover's and Simon's algorithms and are applicable to attacking the FX construction. By converting intermediate measurements into unitary operations deferred to the end of the quantum circuit, both quantum algorithms involve a quantum rank-solving problem. To address it, we first provide a formal analysis of the generalized quantum Gauss–Jordan elimination and characterize the resulting quantum state after the corresponding unitary operations, which serves as a subroutine in these two algorithms. Subsequently, we derive the tight bounds of the attack success probability of these two algorithms based on the initial amplitude, offering a novel perspective that confirms their effectiveness. Furthermore, our research perspective provides an idea for analyzing the attack success probability for some quantum algorithms integrating Grover's algorithm without considering quantum input length, and contributes to a deeper understanding of these attacks' underlying mechanisms under the deferred measurement principle.

Keywords: Grover-meets-Simon; Alg-PolyQ2; deferred measurement; quantum rank-solving; formal analysis; success probability

1. Introduction

The development of large-scale quantum computers will have a significant impact on the security of many cryptographic schemes currently in use [1]. In particular, the introduction of Shor's algorithm [2,3] can solve factorization and discrete logarithm problems in polynomial time. Since almost all current public key schemes are built on the assumption of these computationally difficult problems, this will have a devastating impact on asymmetric cryptographic schemes. This situation has triggered a new line of research, namely post-quantum cryptography, which aims to develop new cryptographic primitives in the hope of resisting attackers equipped with quantum computers. NIST has proposed the post-quantum asymmetric scheme project [4–7] to standardize several quantum-resistant public-key cryptographic algorithms. It is crucial to start the transition to quantum-resistant cryptography before quantum computers are truly available. Fully exploring the potential of quantum algorithms to attack cryptographic schemes and effectively assessing the quantum security of existing schemes under quantum computing will help better design cryptographic algorithms to resist attacks from future quantum computers.

However, the situation for symmetric cryptographic schemes is less clear: universal attacks define the security of ideal symmetric primitives and will achieve a quadratic speed-up through Grover's algorithm [8,9], implying that in a post-quantum world, doubling the key length can restore equivalent ideal security. For nearly 20 years, it was believed that Grover's algorithm was the only advantage attackers had when attacking symmetric cryptography using

DOI: 10.2478/qic-2025-0024

quantum computers. Although the community seems to think that this solution [10,11] has solved the problem, knowledge about practical attacks is still very limited. At present, the impact of many quantum attacks on symmetric cryptography remains unclear, and potential threats need to be explored. The National Academy of Sciences report on the rise of quantum computing [12] also pointed out that there may be some currently unknown clever quantum attacks, such as Simon's algorithm. Indeed, cryptographers have made significant progress against quantum attackers using superposition queries, which can break many symmetric key schemes in polynomial time.

Quantum algorithms have become a central focus in the field of symmetric cryptanalysis. Grover's algorithm is one of the most widely applied algorithms in this field, as it can speed up the search efficiency in an unstructured database of size 2^n, reducing the complexity of exhaustive search attacks from $\mathcal{O}(2^n)$ to $\mathcal{O}(\sqrt{2^n})$. Then, Brassard et al. generalized Grover's algorithm and developed the famous quantum amplitude amplification (QAA) algorithm [13]. Compared with Grover's algorithm, the QAA algorithm extends the preparation of the initial state from the n Hadamard gates to any quantum algorithm $\mathcal{A}$, thus expanding the application range. Based on Grover's algorithm, Brassard et al. [14] proposed a quantum collision search algorithm (BHT algorithm) for the 2-to-1 function over a domain of size 2^n, which can find a set of collisions with high probability through $\mathcal{O}(2^{\frac{n}{3}})$ queries. Ambainis [15] extends this result to arbitrary functions, showing that $\mathcal{O}(2^{\frac{2n}{3}})$ queries suffice to find a set of collisions. Furthermore, Aaronson and Shi [16] established a lower bound of $\mathcal{O}(2^{\frac{n}{3}})$ for the BHT algorithm, which is lower than the original optimal lower bound. Zhandry [17] proved that the probability of finding a collision after performing q queries is at most $\frac{q^3}{2^n}$. Additionally, Hosoyamada et al. [18] explored multiple collisions and proposed a new quantum algorithm that, for l-collisions with small l, gets collisions in $2^{\frac{n\times(3^{l-1}-1)}{2\times 3^{l-1}}}$ queries. Apart from Grover's algorithm, Simon's algorithm [19] is also the current research focus in symmetric cryptanalysis. Kuwakado and Morii [20] proved that Simon's algorithm can distinguish a three-round Feistel structure from a random permutation using the parallelism of quantum computation—an impossible task for classical computers. Similarly, many quantum cryptanalysis works [21–23] are carried out based on the periodicity-finding feature of Simon's algorithm. These include attacks on working modes such as CBC-MAC, PMAC, GMAC, GCM, OCB, and constructions like LRW, etc. Many common quantum attack methods [24–27] are also built upon or inspired by Simon's algorithm.

In recent years, a significant focus of research has been the development of new quantum attack algorithms targeting cryptographic schemes. One popular approach involves combining different quantum algorithms to achieve more efficient attacks, such as Grover-meets-Kuperberg algorithm [28], Bernstein–Vazirani-meets-Grover algorithm [29], etc. The Grover-meets-Simon algorithm proposed by Leander and May [30] is the most widely applied among them, where Grover's algorithm serves as the outer structure and Simon's algorithm as the inner structure. The period identified by Simon's algorithm is used as the decision condition of Grover's search. The introduction of the Grover-meets-Simon has enabled its application to search for two keys in function structures that can be modeled as periodic functions [31–33]. Building on this idea, Bonnetain [34] proposed two improved combinations of Grover's algorithm and Simon's algorithm under the Q1 model (attackers perform offline quantum computations but make only classical online queries) and Q2 model (attackers can make superposition queries to a quantum oracle), where the one in the Q2 model is called Alg-PolyQ2 algorithm. This Alg-PolyQ2 algorithm leverages a combination of online queries and offline computation to achieve an exponential reduction in quantum query complexity.

Despite the promising structure of these combined quantum algorithms, the actual attack success probability and the required number of iterations, especially under practical constraints such as deferred measurement, remain insufficiently characterized. This motivates our work: to analyze in detail how the internal structure of these algorithms affects their success probability under deferred measurement, and to derive tight bounds on the attack success probability and the required number of iterations. Through this analysis, we aim to better understand the real-world effectiveness of such combined quantum attacks, going beyond asymptotic query complexity and providing quantitative insight into their feasibility.

Our contributions In this paper, we mainly study the Grover-meets-Simon and Alg-PolyQ2 algorithms in detail under deferred measurement. We analyze the generalized success probability of these two algorithms in detail from a novel perspective based on the initial amplitude, thereby confirming their effectiveness. To the best of our knowledge, such a detailed analysis has not been done before. In more detail, our main contributions are as follows:

- Since both algorithms involve the rank-solving problem of a system of linear equations, we provide a formal analysis of the generalized quantum Gauss-Jordan elimination. Through the formal description, we discuss the situation (quantum state form) of obtaining the reduced row echelon form matrix based on this method, demonstrate the necessity of auxiliary qubits, and provide its formal proof. Based on the deferred measurement principle to solve the rank, we further analyze the rank-solving process and

provide the number of matrices with rank-$(n-1)$ in both n-dimensional and $(n-1)$-dimensional linear spaces, respectively, along with the corresponding proofs. This is the first time to consider in detail the formal analysis of quantum Gauss–Jordan elimination as a subroutine to solve the rank in the parallel Simon's algorithms under deferred measurement.

- We provide a tight analysis of the Grover-meets-Simon and Alg-PolyQ2 algorithms under deferred measurement in detail. Specifically, considering that when Simon's algorithm is used as the internal structure, the key space will collapse if the intermediate measurements are made. Therefore, combined with the deferred measurement principle, we examine the challenges arising from deferring all measurements in Simon's algorithm to the end of the entire computation during the iteration process. Based on the oscillation amplitude of the initial state, the tight bounds of the generalized success probability and the optimal number of iterations of the Grover-meets-Simon algorithm are analyzed in detail. Similarly, we also provide a tight analysis of the Alg-PolyQ2 algorithm to demonstrate its effectiveness as a quantum attack. This paper provides a novel perspective for assessing the practical effectiveness of quantum algorithms—one that does not rely on assumptions about quantum input length, such as the number of parallel instances of Simon's algorithm and the choice of plaintext pairs in the classifier of the Grover-meets-Simon algorithm.

Outline The rest of the paper is organized as follows: Section 2 introduces the relevant knowledge of quantum circuit models and quantum algorithms; Section 3 provides a formal analysis of the generalized quantum Gauss-Jordan elimination; Section 4 provides a tight analysis of the Grover-meets-Simon and Alg-PolyQ2 algorithms under deferred measurement via formalizing quantum rank-solving; Section 5 discusses some future research directions; Section 6 summarizes this paper.

2. Preliminaries

In this section, we introduce some concepts of quantum computation and review Simon's and Grover's algorithms.

2.1. Quantum Circuit Model

A circuit consisting of a series of quantum gates applied to a group of qubits is called a quantum circuit, which can be used to describe the change of quantum state in Hilbert space. Each quantum logic gate can be represented by a unitary matrix. These unitary operators in Hilbert space are all invertible, and it may be necessary to use enough auxiliary qubits to achieve the required goal. A single qubit has two quantum ground states $|0\rangle$, $|1\rangle$. If the quantum state $|\varphi\rangle$ can be linearly represented by $|0\rangle$, $|1\rangle$, then this state is called a superposition state $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$. Among them, the probability amplitudes α and β are complex numbers, and $|\alpha|^2 + |\beta|^2 = 1$. When an n-qubit is given, the computational basis has 2^n vectors. After applying a series of quantum gates to the initial state, the original superposition state changes. Finally, the system is measured and some n-qubit vectors are obtained on the computational basis to get the desired result.

Quantum computing takes advantage of parallel computing by utilizing quantum phenomena such as quantum superposition and entanglement, allowing multiple computable states to be processed simultaneously, thereby improving efficiency and speed. The unique capabilities of quantum computers enable them to surpass classical computers in certain computing tasks.

Principle of quantum parallel computing. Assume $f(x) : \{0,1\}^n \to \{0,1\}^m$, the mapping of this function in the quantum setting can be used as an oracle $U_f : |x,y\rangle \to |x, y \oplus f(x)\rangle$. When the initial state $|0\rangle^{\otimes n}|0\rangle^{\otimes m}$ is input, $H^{\otimes n}|0\rangle^{\otimes n}|0\rangle^{\otimes m} \xrightarrow{U_f} \frac{1}{\sqrt{2^n}}\sum_x |x\rangle|f(x)\rangle$, which can calculate all values of this function f. This oracle U_f is widely used in various quantum algorithms.

In addition, the following two important principles regarding quantum circuits are very practical. For detailed proof, refer to [35].

Principle of deferred measurement. Measurements can always be moved from the intermediate stage of a quantum circuit to the end of the circuit. Any measurement that occurs inside a quantum circuit can be deferred to the end of the circuit.

Principle of implicit measurement. Any unmeasured qubit at the end of a quantum circuit can be assumed to be measured.

2.2. Parallel Simon's Algorithm

Simon's algorithm [19] aims to solve the periodic problem of hidden subgroups, which can be described as follows:

Simon's Problem with promise: suppose there is a quantum oracle to a function $f\colon \{0,1\}^n \to \{0,1\}^m$ such that $\exists\, s \in \{0,1\}^n, \forall\, x \in \{0,1\}^n, f(x) = f(x \oplus s)$. The goal is to find the period s.

An individual Simon's algorithm can be performed by the following steps, with the corresponding quantum circuit shown in Figure 1.

1. Prepare the initial state $|0\rangle_I^{\otimes n}|0\rangle_{II}^{\otimes m}$ and perform the Hadamard transform $H^{\otimes n}$ on the first register. The following quantum states can be obtained:
$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle_I |0\rangle_{II}.$$
2. Perform a quantum query on the function f, mapping to the following quantum state:
$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle_I |f(x)\rangle_{II}.$$
3. Perform the Hadamard transform $H^{\otimes n}$ on the first register, and the following quantum state can be obtained:
$$\frac{1}{2^n} \sum_{y\in\{0,1\}^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} |y\rangle_I |f(x)\rangle_{II}.$$
Suppose there is some $s \neq 0$, for each y, then $|y, f(x)\rangle = |y, f(x \oplus s)\rangle$, and the amplitude of this configuration is:
$$\alpha(x,y) = \frac{1}{2^n}[(-1)^{x\cdot y} + (-1)^{(x\oplus s)\cdot y}] = \frac{1}{2^n}(-1)^{x\cdot y}[(1 + (-1)^{s\cdot y}]. \tag{1}$$
Let X_1 be an $((n-1)$-dimensional subspace of $\mathbb{F}_2^n$, and divide $\mathbb{F}_2^n$ into coset X_1 and $X_1 + s, s \in \mathbb{F}_2^n \backslash X_1$. In this setting, we assume $x \in X_1$.
4. Measure the first register, and it will collapse to a value that satisfies $y \cdot s = 0$.

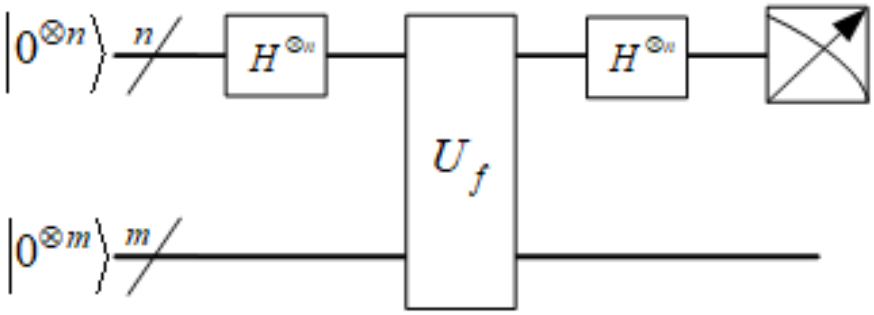

Figure 1. Quantum circuit of Simon's algorithm.

When $y \cdot s = 1$, the amplitude of $\alpha(x,y)$ is 0. Hence, we can only get the vector y orthogonal to period s. The parallel Simon's algorithms under deferred measurement only need $\mathcal{O}(n)$ oracle queries, $n-1$ linearly independent values of y are obtained with high probability, then s can be obtained by solving the following linear equations:

$$\begin{cases} y_1 \cdot s = 0 \\ y_2 \cdot s = 0 \\ \quad \vdots \\ y_n \cdot s = 0. \end{cases} \tag{2}$$

Simon's algorithm is a probabilistic algorithm, and the promise of Simon's problem is not always fully satisfied in cryptanalysis. We introduce a theorem to quantify the relationship between the number of parallel instances of Simon's algorithm and the success probability. The proof can be found in [23]:

Theorem 1. *Given $f:\{0,1\}^n \to \{0,1\}^m$ and s as an actual period of f, $\exists\, t \in \{0,1\}^n \backslash \{0,s\}$ such that the input $x \in \{0,1\}^n$ satisfies $f(x \oplus t) = f(x)$. Define*

$$\varepsilon(f) = \max_{t \in \{0,1\}^n \backslash \{0,s\}} Pr_x[f(x) = f(x \oplus t)]. \tag{3}$$

If $\varepsilon(f) \leq p_0 < 1$, after performing l instances of Simon's algorithm in parallel, the success probability of outputting the actual period s is at least $1 - 2^n(\frac{1+p_0}{2})^l$. Choosing $l \geq 3n/(1-p_0)$, $\varepsilon(f)$ is far enough away from 1.

2.3. Generalized Grover's Algorithm

Grover's algorithm [8,9] aims to quickly search for r marked solution elements in an unstructured database of size N, which can achieve a quadratic speedup compared to the time complexity of classical exhaustive algorithms. It can be described as follows:

Grover's problem: given a search space N whose elements are represented on $n = \log_2 N$ qubits, suppose there is a quantum oracle to a function f: $\{0,1\}^n \to \{0,1\}$ such that $x \in N, f(x) = 1$. The goal is to find these r marked solution elements.

Amplitude amplification is a natural generalization of the original Grover's algorithm. The result of amplitude amplification is described in the following theorem [13], with the corresponding quantum circuit shown in Figure 2.

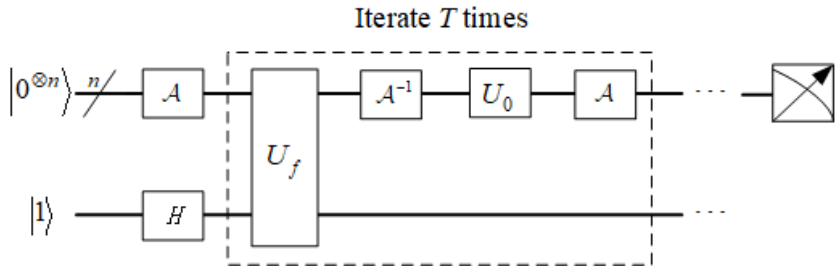

Figure 2. Quantum circuit of generalized Grover's algorithm.

Here, $\mathcal{A}$ is the Hadamard transform $H^{\otimes n}$ in the original Grover's algorithm.

Theorem 2. *Let $\mathcal{A}$ be any quantum algorithm without measurement, and let f: $\{0,1\}^n \to \{0,1\}$ be a Boolean function that distinguishes between good and bad states from the output of the algorithm $\mathcal{A}$. Let $p > 0$ be the initial success probability of $\mathcal{A}|0\rangle$. We define $\mathcal{Q} = -\mathcal{A}U_0\mathcal{A}^{-1}U_f$, where $U_0 = 2|0\rangle^{\otimes n}\langle 0|^{\otimes n} - I$, U_f is performed:*

$$U_f|x\rangle = \begin{cases} -|x\rangle, & if \;\; f(x) = 1 \\ |x\rangle, & if \;\; f(x) = 0, \end{cases}$$

if the state is good, then the phase is reversed.

After T iterations $\mathcal{Q}^T\mathcal{A}|0\rangle$, the outcome is good with probability at least max $\{p, 1-p\}$ under deferred measurement, where $T = \lfloor \frac{\pi}{4\theta} \rfloor$ and $sin^2(\theta) = p$.

3. Formal Analysis of Generalized Quantum Gauss-Jordan Elimination

Quantum Gauss-Jordan elimination (QGJE) was first proposed by Do et al. [36] to solve the linear system of n equations on n variables $AX = b, a_{ij} \in A$, with the goal of achieving a speedup over classical computing techniques. However, no formal proof has been provided yet. In this section, we provide a formal analysis of the generalized QGJE, in particular the existence of a full rank or rank-$(n-1)$ check in a quantum oracle of cryptographic algorithms. The following are the formal steps to perform it. For detailed quantum gate operations of the generalized QGJE, please refer to [37,38].

Formal description of the generalized QGJE. Given a quantum coefficient matrix $|A\rangle_{m\otimes n} = \sum_i \alpha_i |A_i\rangle_{m\otimes n}$ of linear systems of equations, there exists a unitary operator U_{QGJE} such that $\sum_i \alpha_i |A_i\rangle|0\rangle^{\otimes num} \xrightarrow{U_{\text{QGJE}}} \sum_i \alpha_i |A_i'\rangle|\varepsilon_i\rangle$, where $|A_i'\rangle$ is the reduced row echelon form (RREF) matrix corresponding to different $|A_i\rangle$, and $|\varepsilon_i\rangle$ corresponding to each superposition component are auxiliary qubits after applying the generalized QGJE.

Quantum Gauss-Jordan Elimination (QGJE) [36]
Step 1: First, find out the first non-zero $|a_{i,1}\rangle \neq 0$ using Grover's Search algorithm.
Step 2: If successful, take the first leading $|1\rangle$ in the first position as $|a_{1,1}\rangle$, otherwise change to the next column and repeat step 1.
Step 3: Eliminate all other elements $|a_{2,1}\rangle, \cdots, |a_{n,1}\rangle$ in the first column.
Step 4: Change n to $n-1$, control if still $n > 0$, repeat step 1.
Step 5 In backward eliminate all $|a_{n-1,n}\rangle, \cdots, |a_{1,n}\rangle$.
Step 6: Check if $n > 0$, change n to $n-1$, and repeat step 5.

Remark 1. *The QGJE is chosen because it is a generalized quantum extension of the classical Gauss-Jordan elimination, which serves as the foundational algorithm for rank-solving problems. The algorithm proposed by Bonnetain and Jaques is specifically tailored to determine the full-rank property of certain structured matrices derived from symmetric cryptographic primitives and its core technique still relies on Gauss-Jordan elimination to transform the matrix into an upper triangular form. The quantum algorithms proposed by Xia et al. are universal and can compute both the rank and the general solution of arbitrary quantum linear systems with a single measurement. Therefore, for the detailed steps of quantum rank-solving, please refer to [37,38].*

In brief, if the rank is required through deferred measurement, then these auxiliary qubits $|\varepsilon\rangle = \sum_i |\varepsilon_i\rangle$ can contain the solution of the rank corresponding to $\sum_i \alpha_i A_i$. The rank of a linear system of equations is solved without any intermediate measurement that would cause superposition state collapse. The specific operation is as follows: the pivot $|a'_{ii}\rangle, i \leq \min\{m,n\}$ in $|A'_i\rangle$ is used as the control qubit of the CNOT gate, XORed to these all-zero auxiliary qubit inputs, and finally the rank is obtained by measuring these auxiliary qubits after the operation.

In formal description of the generalized QGJE, auxiliary qubits $|0\rangle^{\otimes num}$ are necessary to complete the generalized QGJE. Next, we provide a lemma to prove its necessity.

Lemma 1. *There exists a unitary operation U_{QGJE} such that $U_{\mathrm{QGJE}}(|A\rangle|0\rangle^{\otimes num}) = |A'\rangle|\varepsilon\rangle$. Then it always holds that $num > 0$.*

Proof. Consider the first non-zero element $|a_{k,j}\rangle$ in the column as a pivot and an element $|a_{i,j}\rangle (i > k)$ of its column. In the generalized QGJE, these two elements not only serve as control qubits but must also be transformed as target qubits during the elimination process.

Assume for contradiction that there exists a unitary operator U without auxiliary qubits such that $U|00\rangle = |00\rangle, U|01\rangle = |10\rangle, U|10\rangle = |10\rangle, U|11\rangle = |11\rangle$. From this, we can find that

$$\begin{cases} U|01\rangle = |10\rangle \\ U|10\rangle = |10\rangle \end{cases} \Rightarrow \begin{cases} U(0,0,1,0)^T = (0,1,0,0)^T \ \ (i) \\ U(0,1,0,0)^T = (0,1,0,0)^T \ \ (ii). \end{cases}$$

If we do $(i) - (ii)$, we get $U(0,-1,1,0)^T = (0,0,0,0)^T$, violating unitarity since U^{-1} cannot recover the original state, contradicts! There is no inverse operator such that $U^{-1}(0,0,0,0)^T = (0,-1,1,0)^T$. As a result, there exists no such unitary operator U. Thus, the assumption does not hold.

It can be seen that auxiliary qubits are necessary to store the values of data qubits to control the transformation. □

Lemma 1 demonstrates the necessity of auxiliary qubits in the generalized QGJE. This naturally raises an important question: we need to consider whether the auxiliary qubits can be disentangled. Next, we provide a theorem to state the issue and show the form of the quantum state after the generalized QGJE.

Theorem 3. *There is no operator $U = U' \cdot U_{\mathrm{QGJE}}$ such that*

$$\sum_i \alpha_i |A_i\rangle|0\rangle^{\otimes num} \xrightarrow{U} (\sum_j \beta_j |B_j\rangle) \otimes (\sum_k \gamma_k |c_k\rangle),$$

where B_j is the same RREF matrix corresponding to multiple different A_i. The coefficient β_j is the probability amplitude associated with $|B_j\rangle$ and γ_k is the probability amplitude associated with $|c_k\rangle$, where $|c_k\rangle$ are different auxiliary states for different k.

Proof. This means that the auxiliary qubits cannot be disentangle with other registers and thus $\sum_i \alpha_i |A_i\rangle|0\rangle^{\otimes num} \xrightarrow{U_{\mathrm{QGJE}}} \sum_i \alpha_i |A'_i\rangle|\varepsilon_i\rangle$.

Next, we use the method of contradiction. Suppose that there is an operator U such that $\sum_i \alpha_i|A_i\rangle|0\rangle^{\otimes num} \longrightarrow (\sum_j \beta_j|B_j\rangle) \otimes (\sum_k \gamma_k|c_k\rangle)$. We divide U into the product of two unitary operators U_{QGJE} and U'.

$$\begin{aligned} U_{\mathrm{QGJE}}\left(\sum_i \alpha_i|A_i\rangle \otimes |0\rangle^{\otimes num}\right) &= \sum_i \alpha_i\left(|A_i'\rangle \otimes |\varepsilon_i\rangle\right) \\ &\xrightarrow{U'} \left(\sum_j \beta_j|B_j\rangle\right) \otimes \left(\sum_k \gamma_k|c_k\rangle\right) \\ &= \sum_{j,k} \beta_j\gamma_k\Big(|B_j\rangle \otimes |c_k\rangle\Big). \end{aligned} \tag{4}$$

While the RREF of a matrix is unique, the reduction process may not be, which results in different auxiliary states. Multiple different A_i may correspond to the same RREF matrix B_j. Hence, $j \leq i$ always holds. The original problem can be reduced to whether the auxiliary states added during the operation can be disentangled through U'. If both $\sum_j = 1$ and $\sum_k = 1$, then the space containing $\sum_i \alpha_i(|A_i'\rangle \otimes |\varepsilon_i\rangle)$ has the same dimension as that of $\sum_{j,k} \beta_j\gamma_k|B_j \otimes c_k\rangle$ since U' is a unitary operator and they are both one-dimensional, which contradicts the fact that multiple $|A_i\rangle$ map to the same $|B_j\rangle$. Thus, it is evident that the case satisfying both $\sum_j = 1$ and $\sum_k = 1$ clearly cannot hold. There may exist the following cases:

Case 1: $\sum_j = 1$ and $\sum_k \neq 1$.

Since auxiliary qubits record the information of $|A_i\rangle$, it is generally the case that $|\varepsilon_i\rangle \neq |\varepsilon_{i'}\rangle$ when $i \neq i'$. However, due to $\sum_j = 1$, all different $|A_i\rangle$ correspond to the same RREF matrix $|B_1\rangle$, which is clearly not the case.

Case 2: $\sum_j \neq 1$ and $\sum_k = 1$.

According to Formula (4), when $k = 1$, that is, auxiliary qubits are disentangled and can return to all-zero states $|0\rangle^{\otimes num}$. Thus, we can get that $\sum_i \alpha_i|A_i\rangle \xrightarrow{U} \sum_j \beta_j|B_j\rangle$. Different matrices may get the same RREF matrix after the generalized QGJE, that is $|\{A_i\}| > |\{B_j\}|$. Suppose that $|B_1\rangle$ is the RREF matrix corresponding to $|A_{11}\rangle$, $|A_{12}\rangle$. And $|B_2\rangle$ is the RREF matrix corresponding to $|A_{21}\rangle$, $|A_{22}\rangle$. There are superposition states $\frac{1}{\sqrt{2}}|A_{11}\rangle + \frac{1}{\sqrt{2}}|A_{21}\rangle$ and $\frac{1}{\sqrt{2}}|A_{12}\rangle + \frac{1}{\sqrt{2}}|A_{22}\rangle$. We get that

$$U(\frac{1}{\sqrt{2}}|A_{11}\rangle + \frac{1}{\sqrt{2}}|A_{21}\rangle) = U(\frac{1}{\sqrt{2}}|A_{12}\rangle + \frac{1}{\sqrt{2}}|A_{22}\rangle) = \frac{1}{\sqrt{2}}|B_1\rangle + \frac{1}{\sqrt{2}}|B_2\rangle. \tag{5}$$

Consider the invertibility of the unitary operator U, $U^{-1}(\frac{1}{\sqrt{2}}|B_1\rangle + \frac{1}{\sqrt{2}}|B_2\rangle)$ must have only unique preimage. Contradicting with the above Formula (5), this case does not hold.

Case 3: $\sum_j \neq 1$ and $\sum_k \neq 1$.

In this case, suppose that there are k_1 original matrices $|A_{i_1}\rangle$ corresponding to the same RREF matrix $|B_1\rangle$ and there are k_2 original matrices $|A_{i_2}\rangle$ corresponding to the same RREF matrix $|B_2\rangle$. Since the inputs are distinct and unitary operators are invertible, we have

$$\begin{cases} U_{\mathrm{QGJE}}(|A_{i_1} \otimes 0^{num}\rangle) = |B_1 \otimes \varepsilon_{i_1}\rangle, & i_1 \in \{1, 2, \cdots k_1\} \\ U_{\mathrm{QGJE}}(|A_{i_2} \otimes 0^{num}\rangle) = |B_2 \otimes \varepsilon_{i_2}\rangle, & i_2 \in \{1, 2, \cdots k_2\}. \end{cases} \tag{6}$$

According to Formula (6), the number of original matrices corresponding to different RREF matrices may be different. Hence, there is no such unitary operation U' that $\sum_i \alpha_i\left(|A_i'\rangle \otimes |\varepsilon_i\rangle\right) \xrightarrow{U'} \sum_{j,k} \beta_j\gamma_k\Big(|B_j\rangle \otimes |c_k\rangle\Big)$.

Besides, if $\sum_i \alpha_i|A_i\rangle|0\rangle^{\otimes num} \xrightarrow{U} (\sum_j \beta_j|B_j\rangle) \otimes (\sum_k \gamma_k|c_k\rangle)$ holds, then there is always a unitary transformation that changes auxiliary qubits $\sum_k \gamma_k|c_k\rangle$ into all-zero states. As in case 2, this case does not hold. In summary, there is no unitary transformation U', equivalent to this theorem, which does not hold. Thus, the generalized QGJE can only realize $\sum_i \alpha_i|A_i\rangle|0\rangle^{\otimes num} \xrightarrow{U_{\mathrm{QGJE}}} \sum_i \alpha_i|A_i'\rangle|\varepsilon_i\rangle$. □

According to the above analysis, we provide a formal description and analysis of the generalized QGJE, demonstrating that it can serve as a subroutine for determining whether a matrix is of full rank or rank-$(n-1)$ in the quantum setting (see Remark 1).

In particular, since the registers of multiple instances of Simon's algorithm form a tensor product, the resulting matrix is randomly generated. If Simon's promise holds—i.e., there exists a hidden period, and then the rank of the resulting matrix is at most $n-1$. In the following, we consider these cases and express them as a lemma.

Lemma 2. *Let l, n be integers such that $l \geq n$, and consider matrices over the binary field $\mathbb{F}_2$. Then, the number of $l \times n$ matrices with rank-$(n-1)$ is given by $N_{\mathbb{F}_2^n}(n-1) = (2^n - 1)\prod_{i=0}^{n-2}(2^l - 2^i)$ over $\mathbb{F}_2^n$ and $N_{\mathbb{F}_2^{n-1}}(n-1) = \prod_{i=0}^{n-2}(2^l - 2^i)$ over $\mathbb{F}_2^{n-1}$.*

Proof. Let us consider the set of all $l \times n$ matrices over $\mathbb{F}_2$ whose rank is exactly $n-1$. The idea is to count the number of such matrices using a combinatorial argument based on matrix factorizations and properties of linear independence over finite fields. A matrix $A \in \mathbb{F}_2^{l\times n}$ has rank-$(n-1)$ if and only if:

- The row space of A has dimension $n-1$ (i.e., $n-1$ linearly independent rows);
- The column space of A has dimension $n-1$ (i.e., $n-1$ linearly independent columns).

Every rank-$(n-1)$ matrix A can be written as a product $A = UV$, where:

- $U \in \mathbb{F}_2^{l\times(n-1)}$ is a full-rank matrix (its columns span a rank-$(n-1)$ subspace of $\mathbb{F}_2^l$);
- $V \in \mathbb{F}_2^{(n-1)\times n}$ is a full-rank matrix (its rows span a rank-$(n-1)$ subspace of $\mathbb{F}_2^n$).

Tight Bounds and Approximation
Let $P = \prod_{i=0}^{n-2}(2^l - 2^i) = 2^{\sum_{i=0}^{n-2} i} \cdot \prod_{i=0}^{n-2}(2^{l-i} - 1)$, $Q = \prod_{i=0}^{n-2}(2^{l-i} - 1)$, and thus $P = 2^{\frac{(n-2)(n-1)}{2}} \cdot Q$.
Lower Bound: Since $2^{l-i} - 1 \geq 2^{l-i-1}$ for $l - i \geq 1$, we have

$$Q \geq \prod_{i=0}^{n-2} 2^{l-i-1} = 2^{\sum_{i=0}^{n-2}(l-i-1)} = 2^{(n-1)(l-1) - \frac{(n-2)(n-1)}{2}},$$

$$P \geq 2^{\frac{(n-2)(n-1)}{2}} \cdot 2^{(n-1)(l-1) - \frac{(n-2)(n-1)}{2}} = 2^{(n-1)(l-1)}.$$

Upper Bound: Since $2^{l-i} - 1 \leq 2^{l-i}$, we have

$$Q \leq \prod_{i=0}^{n-2} 2^{l-i} = 2^{\sum_{i=0}^{n-2}(l-i)} = 2^{(n-1)l - \frac{(n-2)(n-1)}{2}},$$

$$P \leq 2^{\frac{(n-2)(n-1)}{2}} \cdot 2^{(n-1)l - \frac{(n-2)(n-1)}{2}} = 2^{(n-1)l}.$$

Summary of Bounds: $2^{(n-1)(l-1)} \leq P \leq 2^{(n-1)l}$.
Asymptotic Approximation: For large $l \gg n$, the terms $2^{-(l-i)}$ become negligible. Rewrite P as

$$P = 2^{(n-1)l} \prod_{i=0}^{n-2}\left(1 - 2^{-(l-i)}\right).$$

Taking the logarithm: $\ln P = (n-1)l \cdot \ln 2 + \sum_{i=0}^{n-2} \ln\left(1 - 2^{-(l-i)}\right)$. For $l \gg n$, $2^{-(l-i)} \approx 0$, so $\ln\left(1 - 2^{-(l-i)}\right) \approx -2^{-(l-i)}$. Thus,

$$\sum_{i=0}^{n-2} \ln\left(1 - 2^{-(l-i)}\right) \approx -\sum_{i=0}^{n-2} 2^{-(l-i)} = -2^{-l}(2^{n-1} - 1).$$

Exponentiating: $P \approx 2^{(n-1)l} \exp\left(-2^{-(l-n+1)}\right) \approx 2^{(n-1)l}\left(1 - 2^{-(l-n+1)}\right)$.
Final Results

- **Tight Bounds:**

$$2^{(n-1)(l-1)} \leq \prod_{i=0}^{n-2}(2^l - 2^i) \leq 2^{(n-1)l}. \tag{7}$$

- **Approximation (for $l \gg n$):**

$$\prod_{i=0}^{n-2}(2^l - 2^i) \approx 2^{(n-1)l}\left(1 - 2^{-(l-n+1)}\right). \tag{8}$$

However, this factorization is not unique because different pairs (U, V) can give rise to the same matrix A. Specifically, for any invertible matrix $T \in \mathrm{GL}_{n-1}(\mathbb{F}_2)$, we have $A = UV = (UT)(T^{-1}V)$, and both UT and $T^{-1}V$ are still full-rank. Therefore, to avoid overcounting, we divide by the number of invertible $(n-1) \times (n-1)$ matrices over $\mathbb{F}_2$. We proceed as follows:

1. First, we count the number of full-rank $(n-1)$-dimensional column spaces over $\mathbb{F}_2^l$. This is the number of ordered sets of $(n-1)$ linearly independent column vectors over $\mathbb{F}_2^l$, which is $\prod_{i=0}^{n-2}(2^l - 2^i)$.
2. Next, we proceed to count the number of full-rank $(n-1)$-dimensional row spaces over $\mathbb{F}_2^n$, which is $\prod_{i=0}^{n-2}(2^n - 2^i)$.
3. Finally, we divide by the number of invertible $(n-1) \times (n-1)$ matrices over $\mathbb{F}_2$, which is $|\mathrm{GL}_{n-1}(\mathbb{F}_2)| = \prod_{i=0}^{n-2}(2^{n-1} - 2^i)$.

Combining all the above parts, we can obtain: $N_{\mathbb{F}_2^n}(n-1) = \prod_{i=0}^{n-2} \frac{(2^l - 2^i)(2^n - 2^i)}{2^{n-1} - 2^i} = (2^n - 1)\prod_{i=0}^{n-2}(2^l - 2^i)$.

Consider the set of all $l \times n$ matrices over $\mathbb{F}_2$ whose rank is exactly $n-1$, and it is equivalent to a full-rank matrix associated with a homogeneous system of linear equations, i.e., the number of ordered sets of $(n-1)$ linearly independent column vectors over $\mathbb{F}_2^l$, which is $N_{\mathbb{F}_2^{n-1}}(n-1) = \prod_{i=0}^{n-2}(2^l - 2^i)$. □

For subsequent calculations, we provide the tight bound and approximation on this value of $\prod_{i=0}^{n-2}(2^l - 2^i)$, as summarized in **Tight Bounds and Approximation**.

4. Tight Analysis of Grover-Meets-Simon and Alg-PolyQ2 under Deferred Measurement

In this section, we analyze and discuss the generalized success probability of the Grover-meets-Simon and Alg-PolyQ2 algorithms without relying on assumptions about quantum input length under deferred measurement. Both quantum algorithms can be applicable to the FX construction $Enc(k, x) = E(k, x \oplus k_1) \oplus k_2$ shown in Figure 3, where $k \in \{0,1\}^m$, $k_1, k_2 \in \{0,1\}^n$. The key k_2 is independent of the keys k, k_1. Once the keys k and k_1 are recovered, the key k_2 can be naturally derived. Hence, the attack goal is to focus on recovering the keys k, k_1.

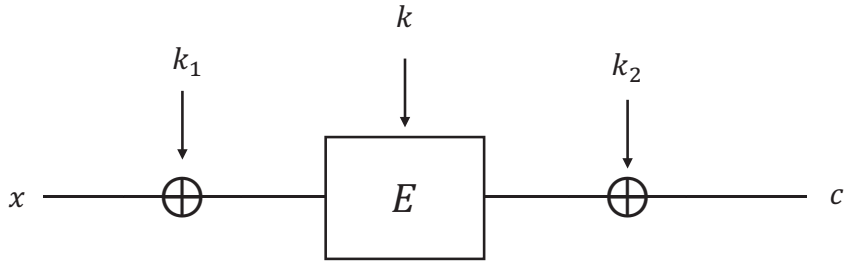

Figure 3. FX-construction.

Previous works. In the Grover-meets-Simon algorithm [30], assuming that the periodic function has been sampled uniformly at random, the success probability is shown to be at least $\frac{2}{5}$, using $m + 4n(n + \sqrt{n})$ qubits and $2^{\frac{m}{2}}\mathcal{O}(m+n)$ oracle queries; in the Alg-PolyQ2 algorithm [34], it shows that the error produced in each iteration of this algorithm, i.e., the function has a period but does not return the actual period, is bounded by the maximum on the index i of $p^{(i)} \leq 2^{(n+1)}((1+p_0)/2)^l$ only using $\mathcal{O}(n)$ oracle queries, where l is the number of parallel Simon's algorithms and p_0 is the upper bound of $\epsilon(f)$ in Theorem 1.

Our work. Our work begins with a formal analysis of the generalized quantum Gauss–Jordan elimination method for the rank problem in Section 3. From a novel perspective that does not rely on assumptions about quantum input length, we provide a tight analysis of the generalized success probability and the optimal number of iterations for the Grover-meets-Simon and Alg-PolyQ2 algorithms, based on the amplitudes of their initial states. The results demonstrate that both algorithms are effective quantum attacks, with generalized success probabilities close to 1.

4.1. Generalized Success Probability of Grover-Meets-Simon

Leander and May [30] proposed a key-recovery attack leveraging a combination of Grover's algorithm and Simon's algorithm. The method embeds Simon's algorithm within the iterations of Grover's search, using Simon's

algorithm as the internal decision function and Grover's algorithm as the outer search procedure. They also provided a relatively loose success probability of $\frac{2}{5}$ by choosing a specific quantum input length, such as the number of parallel instances of Simon's algorithm. In this subsection, we provide the generalized success probability and the optimal number of iterations of the Grover-meets-Simon algorithm, along with their proofs.

Indeed, the Grover-meets-Simon algorithm is the generalized Grover's algorithm shown in Figure 2, where $\mathcal{A}$ is $l(\geq n)$ parallel Simon's algorithms, U_f is used to determine whether the rank is $n-1$ by applying the generalized QGJE, and U_0 changes the phase of the amplitude only for the zero state.

Let $f : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^n$ be a function such that $f(k',x) = Enc(k',x) + E(k',x)$. It is evident that $f(k',x)$ has the period $s = k_1$ when $k' = k$. Applying algorithm $\mathcal{A}$ on $|0\rangle^{\otimes m+2nl}$, the initial input state of Grover-meets-Simon algorithm is

$$|\varphi\rangle = \frac{1}{\sqrt{2^m}}(\frac{1}{2^n})^l \sum_{\substack{k'\in\mathbb{F}_2^m \\ x_1,\cdots,x_l\in\mathbb{F}_2^n \\ y_1,\cdots,y_l\in\mathbb{F}_2^n}} (-1)^{x_1\cdot y_1}\cdots(-1)^{x_l\cdot y_l}|y_1,y_2\cdots,y_l\rangle|f(k',x_1),\cdots,f(k',x_l)\rangle|k'\rangle. \tag{9}$$

Next, we analyze the initial state $|\varphi\rangle$ in detail. The key space $\sum_{k'\in\mathbb{F}_2^n}|k'\rangle$ to be searched is entangled with the superposition state of the matrices $\sum_{y_1,\cdots,y_l\in\mathbb{F}_2^n}|y_1,\cdots,y_l\rangle$ generated in parallel multiple Simon's registers. Suppose that $Y_1 = \{(y_1,y_2,\cdots,y_l) \in \mathbb{F}_2^{nl} | y_i \perp s, s \neq 0\}$ and $Y_2 = \{(y_1,y_2,\cdots,y_l) \in \mathbb{F}_2^{nl} | y_i \in F_2^n\}$. When $|k'\rangle$ is the correct key $|k\rangle$, the row vector $|y_i\rangle(i \in 1,2\cdots l)$ of the corresponding matrix $|y_1,y_2,\cdots,y_l\rangle$ satisfies that $y_i \in Y_1$. Otherwise, the row vector $|y_i\rangle(i \in 1,2\cdots l)$ only satisfies $y_i \in Y_2$. If we consider the intermediate measurement in the original Simon's algorithm, the key space $\sum_{k'\in\mathbb{F}_2^n}|k'\rangle$ will collapse so that we cannot search for the correct key $|k\rangle$. Therefore, we can measure only at the end of the algorithm according to the principle of deferred measurement.

In addition, when $l = \mathcal{O}(n)$, Simon's algorithms are executed in parallel, the linear systems of equations generated are different from the linear systems of equations generated by a single Simon's algorithm running $\mathcal{O}(n)$ times. After $\mathcal{O}(n)$ Simon's algorithms via measurement, we can obtain a determined classical matrix. Whereas as the number of parallel instances increases, the dimension of the span $\dim(\text{span}((y_1,y_2,\cdots,y_l))) = n-1$ can be obtained with a high probability [23], enabling recovery of the period s. However, without intermediate measurement after $\mathcal{O}(n)$ Simon's algorithms in parallel, the resulting superposition state of matrices $\sum_{y_1,y_2,\cdots,y_l\in\mathbb{F}_2^n}|y_1,y_2,\cdots,y_l\rangle$ would contain all matrices generated by a row vector y that satisfies the promise. That is, the matrix components with rank less than $n-1$ will inevitably be present in the superposition. For example, one of the components of the superposition state is $|y_1,y_1\cdots y_1\rangle$, that is, all row vectors are the same and $\dim((y_1,y_1\cdots y_1)) = 1$. Therefore, under this deferred measurement setting, one must not only search for the correct key $|k\rangle$, but also identify and extract the appropriate components $|y_1,y_2,\cdots,y_l\rangle$ by applying the generalized QGJE.

Consider that if k is the correct key, then the function $f(k,x)$ has a non-zero period s such that $f(k,x) = f(k,x\oplus s)$. To simplify the representation, we define a set X_1 that is the $n-1$ dimensional subspace of $\mathbb{F}_2^n$ and divide $\mathbb{F}_2^n$ into cosets X_1 and X_1+s. We suppose that the ground states can be combined to obtain the following result by applying parallel Simon's algorithms:

$$(\frac{1}{2^{n-1}})^l \sum_{\substack{x\in X_1 \\ y_1,\cdots,y_l\in\mathbb{F}_2^n, y\perp s}} (-1)^{x_1\cdot y_1}\cdots(-1)^{x_l\cdot y_l}|y_1,y_2,\cdots,y_l\rangle|f(k',x_1),\cdots,f(k',x_l)\rangle. \tag{10}$$

Suppose that k is the correct key for the function $f(k',x)$. If $k' = k$, the period s is not 0; if $k' \neq k$, the function $f(k',x)$ has no period. Then the initial state can be further written as

$$\begin{aligned}|\varphi\rangle = &\frac{1}{\sqrt{2^m}}(\frac{1}{2^n})^l \sum_{\substack{k'\in\mathbb{F}_2^m, k'\neq k \\ x_1,\cdots,x_l\in\mathbb{F}_2^n \\ y_1,\cdots,y_l\in\mathbb{F}_2^n}} (-1)^{x_1\cdot y_1}\cdots(-1)^{x_l\cdot y_l}|y_1,y_2,\cdots,y_l\rangle|f(k',x_1),\cdots,f(k',x_l)\rangle|k'\rangle \\ &+ \frac{1}{\sqrt{2^m}}(\frac{1}{2^{n-1}})^l \sum_{\substack{x_1,\cdots,x_l\in X_1 \\ y_1,\cdots,y_l\perp s, s\neq 0}} (-1)^{x_1\cdot y_1}\cdots(-1)^{x_l\cdot y_l}|y_1,y_2\cdots,y_l\rangle|f(k,x_1),\cdots,f(k,x_l)\rangle|k\rangle. \end{aligned} \tag{11}$$

In the Grover-meets-Simon algorithm, the above process is equivalent to moving all the measurements of the parallel Simon's algorithms during the iteration process to the end of the entire algorithm, satisfying the principle of deferred measurement.

Here, the quantum classifier U_f is defined as follows:

$$U_f : \mathbb{F}_2^m \times (\mathbb{F}_2^n)^l \to \{0,1\} \ \ with \ \ (k', y_1, \cdots, y_l) \to \{0,1\}.$$

(1) If $\dim(y_1, y_2, \cdots, y_l) \neq n-1$, the output will be 0. Otherwise compute a basis of $|y_1, y_2, \cdots, y_l\rangle$ by applying the generalized QGJE and the unique vector $k_1' \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}$ orthogonal to y.

(2) Check $(k', k_1') \stackrel{?}{=} (k, k_1)$ for arbitrary provided plaintext pairs $(m_i, m_i') \in_R \mathbb{F}_2^n$. If all identities hold, the output will be 1, otherwise it will be 0.

Therefore, the operator U_f can be defined like:

$$|\varphi'\rangle \to \begin{cases} -|\varphi'\rangle, \ \ if \ \ U_f|\varphi'\rangle = 1 \\ \ \ |\varphi'\rangle, \ \ if \ \ U_f|\varphi'\rangle = 0, \end{cases} \tag{12}$$

where $|\varphi'\rangle$ is the component of the superposition state $|\varphi\rangle$.

From Formula (11), we know that the initial state of the Grover-meets-Simon algorithm is not a uniform superposition and there is an amplitude of oscillation due to the entanglement between the key space $|k'\rangle$ and Simon's registers $|y_1, \cdots, y_l\rangle$. Specifically, amplitudes for $k' = k$ (correct key) scale as $1/2^{(m+2(n-1)l)/2}$, while others scale as $1/2^{(m+2nl)/2}$, creating an oscillating imbalance.

In [39], Biron et al. discussed the maximum success probability and the optimal number of iterations of Grover's algorithm in an arbitrary initial state. They depend only on the standard deviation of the initial amplitude distributions of the marked or unmarked states. Hence, we can provide a tight bound of the generalized success probability of the Grover-meets-Simon algorithm based on the initial amplitude from a novel perspective without considering quantum input length.

Biron et al. [39] obtained first-order linear difference equations for the time evolution of the amplitudes of r marked states and $N-r$ unmarked states and solved them exactly. The results of the maximum success probability and the optimal number of iterations are summarized in the following theorem.

Theorem 4 ([39]). *Suppose that the number of correct solutions is r and the size of the database searched is N. When $r/N \ll 1$, the optimal number of iterations T of the search and the success probability of these marked states in the measurement at time t at the end satisfy*

$$T = -\frac{1}{2}\frac{\overline{k(0)}}{\overline{l(0)}} + \frac{\pi}{4}\sqrt{N/r} - \frac{\pi}{24}\sqrt{r/N} + \mathcal{O}(r/N),$$
$$P(t) = P_{max} - (N-r)|\overline{l(0)}|^2, P_{max} = 1 - (N-r)\sigma_l^2,$$

where $\overline{k(0)}$ represents the average of the initial amplitude of the marked states (i.e., correct solutions), $\overline{l(0)}$ represents the average of the initial amplitude of the unmarked states, σ_l^2 is the variance of the initial amplitude of the unmarked states, and P_{max} is a time-independent quantity that serves as a tight bound on the success probability.

As shown in Formula (11), when k' is the correct key k, the matrices generated by them contain cases with rank less than or equal to $n-1$. We can calculate the number of marked correct solutions r (matrices with rank-$(n-1)$) according to Lemma 2. For l parallel instances of Simon's algorithm, the size of the overall state space is $2^{2(n-1)l}$.

Then, we discuss the initial success probability based on the initial amplitudes. According to the calculation method of the maximum success probability in [39,40], we can get that the maximum success probability in the initial state is $P_{max} = 1 - (N-r)\sigma_l^2$, where the variance $\sigma_l^2 = \frac{1}{N-r}\sum_{i=1}^{N-r}|l_i(0) - \overline{l(0)}|^2 = \frac{1}{N-r}\sum_i (l_i(0))^2 - (\frac{1}{N-r}\sum_i l_i(0))^2$. From Formula (11), we can know that

$$l_i(0)^2 = \begin{cases} \frac{1}{2^m}(\frac{1}{2^{2nl}}), \ \ k' \neq k \\ \frac{1}{2^m}(\frac{1}{2^{2(n-1)l}}), \ \ k' = k. \end{cases}$$

Note that $k' = k$ but $\dim(\mathrm{span}(y_1, y_2, \cdots, y_l)) < n-1$ are unmarked states. In unmarked states, when $k' \neq k$, the number is $(2^m - 1)2^{2nl}$ and when $k' = k$, the number is $2^{2(n-1)l} - r$. Hence, we can get

$$\sum_i (l_i(0))^2 = \frac{(2^m-1)2^{2nl}}{2^m 2^{2nl}} + \frac{2^{2(n-1)l}-r}{2^m 2^{2(n-1)l)}} = 1 - \frac{r}{2^m 2^{2(n-1)l)}}. \tag{13}$$

Then, we show $\sum_i l_i(0) = \sum_{k'=k,\dim(\mathrm{span}(y_1,\cdots,y_l))<n-1} l_i(0) + \sum_{k'\neq k} l_i(0)$, where

$$\sum_{\substack{k'=k \\ \dim(\mathrm{span}(y_1,\cdots,y_l))<n-1}} l_i(0) = \frac{1}{\sqrt{2^m}}(\frac{1}{2^{n-1}})^l \sum_{\substack{x_1,\cdots,x_l\in X_1 \\ \dim(\mathrm{span}(y_1,\cdots,y_l))<n-1}} (-1)^{x_1\cdot y_1}\cdots(-1)^{x_l\cdot y_l}$$

and

$$\sum_{k'\neq k} l_i(0) = \frac{1}{\sqrt{2^m}}(\frac{1}{2^{n-1}})^l \sum_{\substack{x_1,\cdots,x_l\in \mathbb{F}_2^n \\ y_1,\cdots,y_l\in \mathbb{F}_2^n}} (-1)^{x_1\cdot y_1}\cdots(-1)^{x_l\cdot y_l}.$$

When computing the value of $\sum_i l_i(0)$, we need to get the value of $\sum_{\substack{x_1,\cdots,x_l\in \mathbb{F}_2^n \\ y_1,\cdots,y_l\in \mathbb{F}_2^n}} (-1)^{x_1\cdot y_1}\cdots(-1)^{x_l\cdot y_l}$. According to theorem in [35], we know that

$$\sum_{x\in\mathbb{F}_2^n}(-1)^{x\cdot y} = \sum_{x\in X_1}(-1)^{x\cdot y} + \sum_{x\oplus s\in\mathbb{F}_2^n/X_1}(-1)^{(x\oplus s)\cdot y} = \begin{cases} 0, & y\neq 0 \\ 2^n, & y=0. \end{cases}$$

Because of $y\perp s$, we can get $\sum_{x\in\mathbb{F}_2^n}(-1)^{x\cdot y} = 2\sum_{x\in X_1}(-1)^{x\cdot y}$. Thus, we can get

$$\sum_{x\in X_1}(-1)^{x\cdot y} = \begin{cases} 0, & y\neq 0 \\ 2^{n-1}, & y=0. \end{cases} \tag{14}$$

According to the implementation of U_f , we know that $x\in X_1$, only when $y_1, y_2, \cdots, y_l$ are all 0, the value of $\sum_{k'=k,\dim(\mathrm{span}(y_1,\cdots,y_l))<n-1} l_i(0) \neq 0$; otherwise, it is 0. Likewise, $\sum_{k'\neq k} l_i(0)$ is the same. According to Formula (14), $\sum_{k'=k,\dim(\mathrm{span}(y_1,\cdots,y_l))<n-1} l_i(0) = \frac{2^{(n-1)l}}{\sqrt{2^m}2^{(n-1)l}}$ and $\sum_{k'\neq k} l_i(0) = \frac{(2^m-1)2^{nl}}{\sqrt{2^m}2^{nl}}$. Hence,

$$(\frac{1}{N-r}\sum_i l_i(0))^2 = (\frac{1}{N-r}(\frac{(2^m-1)2^{nl}}{\sqrt{2^m}2^{nl}} + \frac{2^{(n-1)l}}{\sqrt{2^m}2^{(n-1)l}}))^2 = \frac{2^m}{(N-r)^2}. \tag{15}$$

By calculation, we can get the time-independent quantity $P_{\max}$ and the initial success probability $P(0)$ based on the initial amplitudes as follows:

$$P_{max} = 1-(N-r)\sigma_l^2 = \frac{r}{2^m 2^{2(n-1)l}} + \frac{2^m}{N-r}, \tag{16}$$

$$P(0) = P_{max} - (N-r)|\overline{l(0)}|^2 = \frac{r}{2^m 2^{2(n-1)l}}. \tag{17}$$

Remark 2. *When* $\dim(\mathrm{span}(y_1,\cdots,y_l)) = n-1$, *the vector* $(y_1,\cdots,y_l)$ *is not the all-zero vector. It follows from Formula (14) that* $\sum_{k'=k,\dim(\mathrm{span}(y_1,\cdots,y_l))=n-1} k_i(0) = 0$, *and thus the initial average amplitude of the marked states* $\overline{k(0)} = 0$. *Therefore, the optimal number* $T = \lfloor \frac{\pi}{4}\sqrt{N/r} \rfloor$ *of iterations has nothing to do with the initial state.*

The size of the database searched is $N = (2^m-1)2^{2nl} + 2^{2(n-1)l}$. The number of marked correct solutions is $r = 2^{(n-1)l}P = \Omega(2^{(n-1)(2l-1)})$, where the scaling behavior of P is given in Formula (7). According to Theorem 4, we can compute the optimal number of iterations as follows:

$$T = \lfloor \frac{\pi}{4}\sqrt{N/r} \rfloor \sim \mathcal{O}(\sqrt{N/r}) = \mathcal{O}(2^{\frac{m+n+2l}{2}}). \tag{18}$$

The initial angle $\theta = \arcsin(\sqrt{P(0)}) \approx \sqrt{P(0)}$ for small values of $P(0)$, where $P(0) = \frac{r}{2^m 2^{2(n-1)l}}$. Each iteration of Grover's algorithm increases the angle by 2θ, reaching $(2T+1)\theta$ after T iterations. Therefore, the generalized success probability is

$$p_{success} = \sin^2((2T+1)\theta) \approx \Theta(1). \tag{19}$$

Therefore, we can obtain $(k, y_1, \cdots, y_l)$ with the probability of $\Theta(1)$, where $\dim(\mathrm{span}(y_1, \cdots, y_l)) = n-1$, thereby recovering the keys k, k_1.

When considering the amplitude of the initial state, the initial amplitude is not a uniform superposition state, and there is an oscillation in the amplitude. After analyzing the Grover-meets-Simon algorithm in detail, we know that the Grover-meets-Simon algorithm is an effective algorithm to obtain the correct key with the generalized success probability close to 1 under deferred measurement when moving the measurement of all parallel Simon's algorithms during the iterative process to the end of the entire algorithm. Specifically, we provide a generalized success probability of the Grover-meets-Simon algorithm, which is independent of the length of the key of the block cipher and the number of parallel Simon's algorithms. The advantage of the above analysis is that the generalized success probability in any different cases can be calculated without relying on assumptions about the number of plaintext pairs in the classifier or the number of parallel Simon's algorithms.

4.2. Generalized Success Probability of Alg-PolyQ2

Bonnetain et al. [34] proposed a new algorithm that also uses a combination of Grover's algorithm and Simon's algorithm for solving the asymmetric search problem of a period. This method can also be applied to the FX construction and can exponentially reduce query complexity. However, they do not provide a tight analysis of the generalized success probability of this algorithm.

Asymmetric Search of a Period. There are two functions $F : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^n$ and $g : \{0,1\}^n \to \{0,1\}^n$. F is a family of functions and can be written $F(i,\cdot) = f_i()$. There exists a unique $i_0 \in \{0,1\}^m$ such that $\forall x \in \{0,1\}^n, f_{i_0}(x) \oplus g(x) = f_{i_0}(x \oplus s) \oplus g(x \oplus s)$.

In the FX construction shown in Figure 3, $g = Enc(i,x)$ is a secret key function that the adversary can query online to evaluate it, while $f_i(x) = E(i,x)$ is a function that the adversary can evaluate it offline. Then, the function $f_i \oplus g$ has a period k_1 if $i = k$, whereas it does not have any period if $i \neq k$. Therefore, we can guess whether i is equal to the key k by testing whether $f_i \oplus g$ has a period. The index i can be tested in superposition due to quantum queries to F and g. Thus, the uniform superposition over indices is created as follows: $\sum_{i\in\{0,1\}^m} |i\rangle \otimes |\psi_g\rangle$, where $|\psi_g\rangle = \bigotimes^{l} \left(\sum_{x\in\{0,1\}^n} |x\rangle|g(x)\rangle \right)$.

Similar to the Grover-meets-Simon algorithm, the Alg-PolyQ2 algorithm is also a generalized Grover's algorithm shown in Figure 2, where $\mathcal{A}$ is $l(\geq n)$ parallel Simon's algorithms for solving the asymmetric search of a period, U_f is used to determine whether the rank is n by applying the generalized QGJE, and U_0 changes the phase of the amplitude only for the zero state. Applying $\mathcal{A} \otimes I_1$ on $|0\rangle^{\otimes m+2nl+1}$, the initial input state of Alg-PolyQ2 algorithm is

$$|\varphi\rangle = \frac{1}{\sqrt{2^m}} \left(\frac{1}{2^n}\right)^l \sum_{\substack{i\in\{0,1\}^m \\ x_1,\ldots,x_l\in\mathbb{F}_2^n \\ y_1,\ldots,y_l\in\mathbb{F}_2^n}} |i\rangle \, (-1)^{x_1\cdot y_1} \cdots (-1)^{x_l\cdot y_l} \, |y_1,\ldots,y_l\rangle \otimes |(f_i\oplus g)(x_1),\ldots,(f_i\oplus g)(x_l)\rangle \, |b\rangle. \tag{20}$$

Suppose that k is the correct key for the function $(f_i \oplus g)(x)$. If $i = k$, the period s is not 0; if $i \neq k$, there may be values that are not actual non-zero periods t. For $b \in \{0,1\}$, compute $|b \oplus 1\rangle$ if $\dim(\mathrm{span}(y_1, \cdots, y_l)) < n$; otherwise $|b\rangle$ if $\dim(\mathrm{span}(y_1, \cdots, y_l)) = n$. Then the initial state can be further written as

$$|\varphi\rangle = \alpha \left(\sum_{\substack{i\in\mathbb{F}_2^m, i\neq k \\ x_1,\cdots,x_l\in\mathbb{F}_2^n \\ y_1,\cdots,y_l\in\mathbb{F}_2^n}} (-1)^{x_1\cdot y_1} \cdots (-1)^{x_l\cdot y_l} |y_1,\cdots,y_l\rangle |(f_i\oplus g)(x_1),\cdots,(f_i\oplus g)(x_l)\rangle |i\rangle |b\rangle \right)$$
$$+ \beta \left(\sum_{\substack{x_1,\cdots,x_l\in X_1 \\ y_1,\cdots,y_l \perp s, s\neq 0}} (-1)^{x_1\cdot y_1} \cdots (-1)^{x_l\cdot y_l} |y_1,\cdots,y_l\rangle |(f_i\oplus g)(x_1),\cdots,(f_i\oplus g)(x_l)\rangle |k\rangle |b\oplus 1\rangle \right), \tag{21}$$

where $\alpha = \frac{1}{\sqrt{2^m}} (\frac{1}{2^n})^l$ and $\beta = \frac{1}{\sqrt{2^m}} (\frac{1}{2^{n-1}})^l$.

In the Alg-PolyQ2 algorithm, the above process also satisfies the principle of deferred measurement.

Here, the quantum oracle U_f is defined as follows:

$$U_f : i \in \mathbb{F}_2^m \to \{0,1\}.$$

Once we have the superposition $|\psi_g\rangle$ and given a quantum oracle access to U_f, we can know if $f_i \oplus g$ has a period or not without making new queries to g by the test oracle. This test oracle is a subroutine of the quantum oracle U_f. Next, the test oracle can be defined as follows:

$$|i\rangle|\psi_g\rangle|b\rangle \xrightarrow{\textbf{test}} \begin{cases} |i\rangle|\psi_g\rangle|b\rangle, & if\ (f_i \oplus g) \text{ has no period} \\ |i\rangle|\psi_g\rangle|b \oplus 1\rangle, & if\ (f_i \oplus g) \text{ has a period.} \end{cases}$$

If we obtain $|b \oplus 1\rangle$ for $b \in \{0,1\}$, the output will be 1. Otherwise, the output will be 0. Therefore, the unitary operator U_f can be defined as in Formula (12). Note that even if $f_i \oplus g$ has no period, it is not necessarily equal to $|i\rangle|\psi_g\rangle|b\rangle$ and Formula (3) holds when $i \neq k$ are almost random according to Theorem 1. However, we expect that $\textbf{test}|i\rangle|\psi_g\rangle|b\rangle = |i\rangle|\psi_g\rangle|b\rangle + |\delta\rangle$ holds for small error $|\delta\rangle$.

Next, we provide a tight analysis of the generalized success probability of the Alg-PolyQ2 algorithm. According to the above analysis, $\textbf{test}|k\rangle|\psi_g\rangle|b\rangle = |k\rangle|\psi_g\rangle|b \oplus 1\rangle$ always holds when $i = k$, showing that there must be a non-zero period in the case. Thus, $\dim(\text{span}(y_1, y_2, \cdots, y_l)) < n$ always holds when $i = k$ and $(k, y_1, y_2, \cdots, y_l)$ are marked states only in the case; all other states are unmarked states.

It follows from Formula (21) that there must be a non-zero period when $i = k$. As a result of executing the parallel Simon's algorithms, the quantum states in the overall state space are marked states. Consequently, we have $r = 2^{2(n-1)l}$. From the perspective of the time evolution of the amplitude of the initial state, similar to the initial success probability analysis in the Grover-meets-Simon algorithm, the sum of the initial probability of the unmarked states is $\sum_i (l_i(0))^2 = 1 - \frac{1}{2^m}$ and the sum of their initial amplitude is $\sum_{i \neq k} l_i(0) = \frac{(2^m-1)2^{nl}}{\sqrt{2^m 2^{nl}}}$. Thus, according to the definitions in Formulas (16) and (17), we obtain $P(0) = \frac{1}{2^m}$. This verifies that this algorithm essentially applies Grover's algorithm only on the index i. After an optimal number of iterations $T = \mathcal{O}(\sqrt{N/r}) = \mathcal{O}(2^{\frac{m+2l}{2}})$, the key k can be recovered with the probability of $\Theta(1)$. We will further interpret the results using joint and conditional probabilities in the following discussion.

Let this event $i = k$ be represented as A and this event $\dim(\text{span}(y_1, y_2, \cdots, y_l)) = n$ as B. We divide the discussion into three points as follows:

1. The event $(i = k) \cap (\dim(\text{span}(y_1, y_2, \cdots, y_l)) < n)$ by applying Grover's search can be represented as $A \cap \overline{B}$ and its probability is $Pr[A \cap \overline{B}] = \Theta(1)$ according to the above analysis. Due to the property of conditional probability $Pr[A \cap \overline{B}] = Pr[\overline{B}|A] \cdot Pr[A]$, then $Pr[\overline{B}|A] = Pr[A] = \Theta(1)$. This again illustrates that Grover's algorithm, as a subroutine of Alg-PolyQ2, is essentially just a search for index i with the probability of $\Theta(1)$.
2. The initial state can be written as $\sum_{i \neq k} \alpha_i |i\rangle|\psi_g\rangle|b\rangle + \sum_{i=k} \beta_i |i\rangle|\psi_g\rangle|b\rangle$, it changes to $\sum_{i \neq k} \alpha_i |i\rangle|\psi_g\rangle|b\rangle + \sum_{i=k} \beta_i |i\rangle|\psi_g\rangle|b \oplus 1\rangle$ after applying the test oracle. Due to $Pr[\overline{B}|A] = \Theta(1)$ at point 1, then $Pr[B|A] \approx 0$, showing that when $i = k$, $f_i \oplus g$ have a non-zero period with the probability of $\Theta(1)$.
3. The event $(i \neq k) \cap (\dim(\text{span}(y_1, y_2, \cdots, y_l)) < n)$ by applying Grover's search can be represented as $\overline{A} \cap \overline{B}$ and its probability is $Pr[\overline{A} \cap \overline{B}] = Pr[\overline{B}|\overline{A}] \cdot Pr[\overline{A}]$. According to Lemma 1 in [34], $||\delta||^2 = Pr[\overline{B}|\overline{A}] \leq 2^{n+1}(\frac{1+p_0}{2})^l$, it follows that the probability of returning the incorrect period is far enough away from 1 by choosing $l \geq 3n/(1-p_0)$ according to Theorem 1. Due to $Pr[A] = \Theta(1)$ at point 1, hence $Pr[\overline{A} \cap \overline{B}] \approx 0$. Similarly, $Pr[\overline{A} \cap B] \approx 0$. Thus, $Pr[\overline{A} \cap (B \cup \overline{B})] \approx 0$. This shows that the event $i \neq k$ independent of this event that $\dim(\text{span}(y_1, y_2, \cdots, y_l))$ returns a certain answer.

The above analysis indicates that k can be searched and $f_i \oplus g$ have a non-zero period with the probability of $\Theta(1)$ when $i = k$; otherwise $(y_1, y_2, \cdots, y_l)$ are almost random and return incorrect answers when $i \neq k$. However, the ultimate goal of applying the Alg-PolyQ2 algorithm to the FX construction is to recover not only the key k but also the key k_1. This algorithm indicates that, once k has been obtained, if the hidden shift is still required, one instance of Simon's algorithm may be applied to obtain k_1.

Let this event $\dim(\text{span}(y_1, y_2, \cdots, y_l)) = n - 1$ as $\overline{B_1}$ and the event $\dim(\text{span}(y_1, y_2, \cdots, y_l)) < n - 1$ as $\overline{B_2}$ ($\overline{B} = \overline{B_1} \cup \overline{B_2}$). Then $Pr[\overline{B}|A] = Pr[\overline{B_1}|A] + Pr[\overline{B_2}|A]$, where $Pr[\overline{B_1}|A] \geq 1 - 2^n(\frac{1+p_0}{2})^l$ and $Pr[\overline{B_2}|A] \leq 2^n(\frac{1+p_0}{2})^l$ according to Theorem 1. This shows that the Alg-PolyQ2 is an effective algorithm that can solve the keys k, k_1 with the probability of $\Theta(1)$.

5. Discussion

When analyzing quantum algorithms related to cryptanalysis, it is crucial to evaluate their practical effectiveness in real-world quantum computing environments. While theoretical constructions often assume idealized quantum systems, practical quantum computing must cope with issues such as the complexity of quantum measurements. These practical issues are particularly prominent when considering combinations of different quantum algorithms—for example, when other quantum algorithms are embedded in Grover's algorithm or when integrating multiple quantum subroutines into a composite algorithm.

We emphasize the role of measurement in such combinatorial algorithms. The interaction between Grover's amplitude amplification and other quantum components introduces subtle constraints and design considerations. Specifically, we analyze existing algorithms, including the Grover-meets-Simon algorithm and the Alg-PolyQ2 algorithm, from the perspective of initial state success probability under deferred measurement. This provides a unified approach to understanding how to defer intermediate measurements, which is particularly important for preserving quantum superpositions between algorithmic modules. Our analysis highlights that deferred measurement is an important principle in quantum algorithm design.

This research inspires two promising directions. First, inspired by our analysis of the combination of Grover's and Simon's algorithms from a novel perspective, we believe that further investigation of the effectiveness of other quantum cryptanalysis techniques is warranted. Many classical cryptanalysis strategies (e.g., differential and linear cryptanalysis) have been partially applied to the quantum realm, but a comprehensive evaluation of them remains incomplete. By leveraging insights from deferred measurement and algorithm decomposition, we can better understand which classical strategies are amenable to efficient quantum implementations to analyze the security of key alternation ciphers against quantum-CPA attacks (quantum chosen-plaintext attack, where the adversary has superposition access to the encryption oracle). Second, our discussion of rank problems and linear algebraic structures focuses on quantum Gauss-Jordan elimination. Future research could revisit the basic assumptions behind the classical methods and explore whether similar algorithmic primitives can be constructed or optimized in a quantum setting. A deeper understanding of the structure and algebraic foundations of these problems will help develop more efficient and general quantum solvers.

6. Conclusion

In this paper, we mainly study the Grover-meets-Simon and Alg-PolyQ2 Attacks via formalizing quantum rank-solving under deferred measurement in detail. First, we provide a formal analysis of the generalized quantum Gauss-Jordan elimination for the rank problem. In the formal description under deferred measurement, we discuss the situation of obtaining the reduced row echelon form matrix based on this method, including the form of the resulting quantum state and entanglement characteristics. Then, we apply it as a subroutine to the Grover-meets-Simon algorithm and the Alg-PolyQ2 algorithm, achieving full quantum treatment and ensuring its theoretical feasibility in a quantum environment.

In these two original algorithms, each Grover's iteration involves the rank-solving process. The core of these two algorithms lies in the relationship between the two keys, that is, the periodic relationship. The output of multiple Simon's registers is a superposition state of the matrix in the non-measurement state. If the measurement operation in Simon's algorithm is considered, the search space will change due to collapse, which will affect the search of Grover's algorithm. Based on the formal analysis of the generalized quantum Gauss-Jordan elimination, only the parallel Simon's algorithms are considered, and their measurement can be postponed to the end according to the principle of deferred measurement. From a novel perspective without relying on assumptions about quantum input length, we analyze the tight bounds of the generalized success probability and the optimal number of iterations of the Grover-meets-Simon algorithm and the Alg-PolyQ2 algorithm in detail based on the initial state amplitude, showing that they are effective attack algorithms with the generalized success probability close to 1.

Author Contributions

The first author Qiqing Xia proposed the original idea, completed the work and wrote the manuscript. The second author Qianru Zhu contributed to part of the methodology. The third author Huiqin Xie provided the financial support. The fourth author Li Yang contributed to the review and supervision of the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding

This work was supported by the Beijing Natural Science Foundation (Grant No. 4234084).

Conflicts of Interest Statement
The authors declare that there is no conflict of interest.

Data Availability Statement
All data generated during the study are included in the article.

References

1. Shao, C.; Li, Y.; Li, H. Quantum algorithm design: techniques and applications. *J. Syst. Sci. Complex*. **2019**, *32*, 375–452.
2. Shor, P.W. Algorithms for quantum computation: discrete logarithms and factoring. *Proc. 35th Annu. Symp. Found. Comput. Sci*. **1994**, 124–134.
3. Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev*. **1999**, *41*, 303–332.
4. Alagic, G.; Alperin-Sheriff, J.; Apon, D.; Cooper, D.; Dang, Q.; Liu, Y.-K.; Miller, C.; Moody, D.; Peralta, R.; et al. Status report on the first round of the NIST post-quantum cryptography standardization process. **2019**.
5. Alagic, G.; Alperin-Sheriff, J.; Apon, D.; Cooper, D.; Dang, Q.; Kelsey, J.; Liu, Y.-K.; Miller, C.; Moody, D.; Peralta, R.; et al. Status report on the second round of the NIST post-quantum cryptography standardization process. *US Dept. Commerce, NIST* **2020**, *2*, 69.
6. Alagic, G.; Apon, D.; Cooper, D.; Dang, Q.; Dang, T.; Kelsey, J.; Lichtinger, J.; Liu, Y.-K.; Miller, C.; et al. Status report on the third round of the NIST post-quantum cryptography standardization process. **2022**.
7. Alagic, G.; Bros, M.; Ciadoux, P.; Cooper, D.; Dang, Q.; Dang, T.; Kelsey, J.; Lichtinger, J.; Liu, Y.-K.; Miller, C.; et al. Status report on the fourth round of the NIST post-quantum cryptography standardization process. *NIST, Gaithersburg, MD, USA* **2025**.
8. Grover, L.K. A fast quantum mechanical algorithm for database search. *Proc. 28th Annu. ACM Symp. Theory Comput*. **1996**, 212–219.
9. Grover, L.K. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett*. **1997**, *79*, 325.
10. Bernstein, D.J.; et al. Introduction to post-quantum cryptography. *Post-Quantum Cryptogr*. **2009**, *1*, 1–10.
11. Diffie, W.; Hellman, M.E. New directions in cryptography. *Democratizing Cryptography* **2022**, 365–390.
12. Horowitz, M.; Grumbling, E. Quantum computing: progress and prospects. **2019**.
13. Brassard, G.; Hoyer, P.; Mosca, M.; Tapp, A. Quantum amplitude amplification and estimation. *Contemp. Math*. **2002**, *305*, 53–74.
14. Brassard, G.; Høyer, P.; Tapp, A. Quantum cryptanalysis of hash and claw-free functions. *Latin Am. Symp. Theor. Inform*. **1998**, 163–169.
15. Ambainis, A. Quantum walk algorithm for element distinctness. *SIAM J. Comput*. **2007**, *37*, 210–239.
16. Aaronson, S.; Shi, Y. Quantum lower bounds for the collision and the element distinctness problems. *J. ACM* **2004**, *51*, 595–605.
17. Zhandry, M. A note on the quantum collision and set equality problems. *arXiv preprint* arXiv:1312.1027 **2013**.
18. Hosoyamada, A.; Sasaki, Y.; Xagawa, K. Quantum multicollision-finding algorithm. *Int. Conf. Theory Appl. Cryptology Inf. Secur*. **2017**, 179–210.
19. Simon, D.R. On the power of quantum computation. *SIAM J. Comput*. **1997**, *26*, 1474–1483.
20. Kuwakado, H.; Morii, M. Quantum distinguisher between the 3-round Feistel cipher and the random permutation. *Proc. IEEE Int. Symp. Inf. Theory*, **2010**, 2682–2685.
21. Kuwakado, H.; Morii, M. Security on the quantum-type Even-Mansour cipher. *Proc. Int. Symp. Inf. Theory and Its Applications*, **2012**, 312–316.
22. Santoli, T.; Schaffner, C. Using Simon's algorithm to attack symmetric-key cryptographic primitives. *Quantum Inf. Comput*., **2017**, *17*, 65–78.
23. Kaplan, M.; Leurent, G.; Leverrier, A.; Naya-Plasencia, M. Breaking symmetric cryptosystems using quantum period finding. *Advances in Cryptology—CRYPTO*, **2016**, 207–237.
24. Ito, G.; Hosoyamada, A.; Matsumoto, R.; Sasaki, Y.; Iwata, T. Quantum chosen-ciphertext attacks against Feistel ciphers. *Cryptographers' Track at the RSA Conf*., **2019**, 391–411.
25. Xie, H.; Yang, L. Quantum miss-in-the-middle attack. *arXiv preprint arXiv:1812.08499*, **2018**.
26. Roetteler, M.; Steinwandt, R. A note on quantum related-key attacks. *Inf. Process. Lett*., **2015**, *115*, 40–44.
27. Bonnetain, X.; Naya-Plasencia, M.; Schrottenloher, A. On quantum slide attacks. *Sel. Areas Cryptogr*., **2020**, 492–519.

28. Bonnetain, X.; Naya-Plasencia, M. Hidden shift quantum cryptanalysis and implications. *Advances in Cryptology—ASIACRYPT*, **2018**, 560–592.
29. Zhou, B.-M.; Yuan, Z. Quantum key-recovery attack on Feistel constructions: Bernstein–Vazirani meet Grover algorithm. *Quantum Inf. Process.*, **2021**, *20*, 1–14.
30. Leander, G.; May, A. Grover meets Simon—Quantumly attacking the FX-construction. *Advances in Cryptology—ASIACRYPT*, **2017**, 161–178.
31. Dong, X.; Li, Z.; Wang, X. Quantum cryptanalysis on some generalized Feistel schemes. *Sci. China Inf. Sci.*, **2019**, *62*, 1–12.
32. Dong, X.; Wang, X. Quantum key-recovery attack on Feistel structures. *Sci. China Inf. Sci.*, **2018**, *61*, 1–7.
33. Shinagawa, K.; Iwata, T. Quantum attacks on sum of Even-Mansour pseudorandom functions. *Inf. Process. Lett.*, **2022**, *173*, 106172.
34. Bonnetain, X.; Hosoyamada, A.; Naya-Plasencia, M.; Sasaki, Y.; Schrottenloher, A. Quantum attacks without superposition queries: the offline Simon's algorithm. *Advances in Cryptology—ASIACRYPT*, **2019**, 552–583.
35. Nielsen, M.A.; Chuang, I. Quantum computation and quantum information. *Am. Assoc. Phys. Teachers*, **2002**.
36. Diep, D.N.; Giang, D.H. Quantum Gauss-Jordan elimination. *arXiv preprint quant-ph/0511062*, **2005**.
37. Bonnetain, X.; Jaques, S. Quantum period finding against symmetric primitives in practice. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, **2022**, 1–27.
38. Xia, Q.; Zhu, Q.; Xie, H.; Yang, L. Algorithm for solving quantum linear systems of equations with coherent superposition and extended applications. *Comput. J.*, **2025**, *68*, 520–538.
39. Biron, D.; Biham, O.; Biham, E.; Grassl, M.; Lidar, D.A. Generalized Grover search algorithm for arbitrary initial amplitude distribution. *Lect. Notes Comput. Sci.*, **1999**, 140–147.
40. Biham, E.; Biham, O.; Biron, D.; Grassl, M.; Lidar, D.A. Grover's quantum search algorithm for an arbitrary initial amplitude distribution. *Phys. Rev. A*, **1999**, *60*, 2742.