Cryptanalysis against Symmetric-Key Schemes with Online Classical Queries and Offline Quantum Computations

Akinori Hosoyamada[1] and Yu Sasaki[1]

NTT Secure Platform Laboratories,
3-9-11, Midori-cho Musashino-shi, Tokyo 180-8585, Japan.
{hosoyamada.akinori,sasaki.yu}@lab.ntt.co.jp

Abstract. In this paper, quantum attacks against symmetric-key schemes are presented in which adversaries only make classical queries but use quantum computers for offline computations. Our attacks are not as efficient as polynomial-time attacks making quantum superposition queries, while our attacks use the realistic model and overwhelmingly improve the classical attacks. Our attacks convert a type of classical meet-in-the-middle attacks into quantum ones. The attack cost depends on the number of available qubits and the way to realize the quantum hardware. The tradeoff between data complexity D and time complexity T against the problem of cardinality N is $D^2 \cdot T^2 = N$ and $D \cdot T^6 = N^3$ in the best and worst case scenarios to the adversary respectively, while the classic attack requires $D \cdot T = N$. This improvement is meaningful from an engineering aspect because several existing schemes claim beyond-birthday-bound security for T by limiting the maximum D to be below $2^{n/2}$ according to the classical tradeoff $D \cdot T = N$. Those schemes are broken if quantum offline computations are performed by adversaries. The attack can be applied to many schemes such as a tweakable block-cipher construction *TDR*, a dedicated MAC scheme *Chaskey*, an on-line authenticated encryption scheme *McOE-X*, a hash function based MAC H^2-*MAC* and a permutation based MAC *keyed-sponge*. The idea is then applied to the FX-construction to discover new tradeoffs in the classical query model.

keywords: post-quantum cryptography, classical query model, meet-in-the-middle, tradeoff, Chaskey, TDR, keyed sponge, KMAC, FX

1 Introduction

Recent advancement of the development of quantum computers arises a lot of security concerns in cryptography. It is well-known that the problem of factoring can be solved much faster with quantum computers than classical computers. Thus security of the RSA cryptosystem significantly drops against quantum computers. The similar issue occurs in many other cryptosystem and security against quantum computers, often called post-quantum security, is of great interest in the current cryptographic community.

Algorithmic speed-up using quantum computers can be applied to symmetric-key schemes as well. For example, Grover's seminal result [Gro96] enables to recover the k-bit key K only with $O(2^{k/2})$ quantum computations. It also enables to find preimages of n-bit output cryptographic hash function H only with $O(2^{n/2})$ quantum computations. Moreover, Brassard *et al.* [BHT97] showed the algorithm to generate collision of H only with $O(2^{n/3})$ quantum computations[1].

Besides the above improvements on generic attacks, quantum attacks against a particular modes, constructions and primitives have been studied. Kuwakado and Morii proposed a distinguishing attack against 3-round Feistel cipher [KM10] and a key recovery attack against Even-Mansour construction [KM12]. Kaplan *et al.* proposed forgery attacks on various CBC-like MACs [KLLN16a] and proposed differential cryptanalysis in the quantum setting [KLLN16b]. Liu and Liu pointed out that existential forgery attacks in [KLLN16a] can be universal forgery attacks [LL17b] and proposed key recovery attacks against full keyed-sponge construction [LL17a]. Most of the attacks assume that all communications are done in superposition, and the attacker is allowed to make superposition queries. Although the assumption of quantum queries is unrealistic, the attacks work only with $O(n)$ queries and computational complexities where n is the size of the function output, say the size of the ciphertext block or the tag length.

Those attacks revealed the fact that security against quantum computations in symmetric-key schemes heavily depends on the construction. For example, Even-Mansour construction can be attacked in polynomial-time in the quantum query model while block-ciphers require $O(2^{k/2})$ quantum computations even with quantum queries. Similarly, CBC-like MACs can be attacked in polynomial-time in the quantum query model while HMAC requires $O(2^{k/2})$ quantum computations even with quantum queries. Those facts encourage the researchers to classify various constructions into classes with different post-quantum security. Indeed, the recent standardization activity for lightweight cryptosystems conducted by NIST [MBTM17] explicitly mentions that the post-quantum security is taken into account during the selection process.

While the polynomial-time attacks in quantum query model is efficient, the model that requires all the users to implement quantum computers and data in the network is communicated in the form of superposition is unrealistic. This motivates us to investigate the security of symmetric-key schemes against attackers who make queries only in the same manner as the classic attackers but can perform offline computations by using quantum computers. Many generic attacks e.g. key recovery attack with Grover's algorithm, work in this model, while only a limited number of results are known for particular symmetric-key schemes. An example in this direction is again the key recovery attack against Even-Mansour construction [KM12], which recovers the key only with $O(2^{n/3})$ classical queries and $O(2^{n/3})$ quantum computations. Because post-quantum security depends on the construction, more investigation is necessary.

[1] While several concerns have been pointed out recently [Ber09,BB17], those works surely took important roles to the progress of this research topic in early stage.

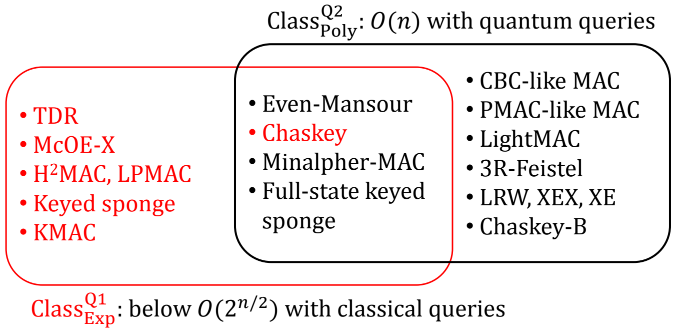

Fig. 1. Classification of Problems Attacked in Quantum Adversaries

Our Contributions. We present quantum attacks against symmetric-key schemes in which adversaries make queries only in the classical manner but use quantum computers for offline computations.

We first observe that many of previous quantum attacks can be classified into two classes; polynomial-time complexity in the quantum query model and exponential-time complexity (but significantly improves classical attacks) in the classical query model. We call the former class $\mathtt{Class}^{\mathtt{Q2}}_{\mathtt{Poly}}$ and the latter class $\mathtt{Class}^{\mathtt{Q1}}_{\mathtt{Exp}}$. Most of the previous work focused on $\mathtt{Class}^{\mathtt{Q2}}_{\mathtt{Poly}}$, yet [KM12] showed that attacks in $\mathtt{Class}^{\mathtt{Q2}}_{\mathtt{Poly}}$ may also belong to $\mathtt{Class}^{\mathtt{Q1}}_{\mathtt{Exp}}$. The current community pays much attention to $\mathtt{Class}^{\mathtt{Q2}}_{\mathtt{Poly}}$, while $\mathtt{Class}^{\mathtt{Q1}}_{\mathtt{Exp}}$ receives less attention. This motivates us to search for attacks in $\mathtt{Class}^{\mathtt{Q1}}_{\mathtt{Exp}}$ because classical query model is more realistic. We will show many problems that belong to $\mathtt{Class}^{\mathtt{Q1}}_{\mathtt{Exp}}$ but not to $\mathtt{Class}^{\mathtt{Q2}}_{\mathtt{Poly}}$. If researchers only focus on $\mathtt{Class}^{\mathtt{Q2}}_{\mathtt{Poly}}$, those problems will be overlooked. The two classes and problems in each class are shown in Fig. 1.

Our attack converts a type of the classical meet-in-the-middle (MitM) attacks into quantum ones. In details, if the classical MitM attacks make D online queries and T offline computations such that $D \cdot T = N$, we replace the classical offline computations with quantum ones, while the classical online queries stay unchanged. Hence, we call the attack *online-offline MitM attack*.[2]

There are two issues about the evaluation of the cost of quantum computations. 1) Grover and Rudolph [GR04] pointed out that the equivalence between having Q quantum memory and Q quantum processors, which may affect the best choice of the quantum computations for offline computations. 2) Bernstein [Ber09] argued that quantum hardware architecture significantly impacts to the cost of the quantum computation. In this paper, the attacks are evaluated by taking into account those observations. As a result, the classical tradeoff of

[2] Kaplan [Kap14] proposed another type of quantum MitM attack against multiple encryptions. It computes both independent parts of MitM offline, thus is very different from ours.

$D \cdot T = N$ can be improved to $D^2 \cdot T^2 = N$, $D^{3/2} \cdot T^2 = N$ or $D \cdot T^6 = N^3$, depending on the assumption of the models.

This improvement is meaningful because several existing schemes claim beyond-birthday-bound (BBB) security for T by limiting the maximum D to be below $2^{n/2}$ by following the classical tradeoff of $D \cdot T = N$. Those schemes are broken by our attacks. For example, both of a tweakable block-cipher (TBC) construction *tweak dependent rekey (TDR)* proposed by Minematsu [Min09] and a dedicated MAC scheme *Chaskey* [Mou15,MMH+14] are AES-based 128-bit output schemes. TDR and Chaskey claim 86-bit security and 80-bit security for T by limiting the maximum D to be 2^{42} and 2^{48}, respectively. Our attacks can break those schemes with $T = D = 2^{32}$ using 2^{32} qubits or with $D = 2^{57}, T = 2^{42}$ using only $128 \cdot c$ qubits where c is a small constant. Our attacks have more applications such as an on-line authenticated encryption scheme *McOE-X* [FFL12], a hash based MAC *H^2-MAC* [Yas09], a permutation based MAC *keyed-sponge* [BDPA08] and thus *KMAC* [NIS16] standardized by NIST.

We also discuss similar tradeoff in the classical query model for the quantum attacks against the FX-construction proposed by Leander and May [LM17], in which [LM17] only analyzed the quantum query model. The attack is further extended to 2-key variants of LRW, XE, and XEX TBC constructions.

Paper Outline. The remaining part of this paper is organized as follows. Section 2 introduces quantum attack models and previous work. Section 3 gives general description of the quantum online-offline MitM attacks. Section 4 applies our attack to various schemes. Section 5 discusses the attack against the FX construction. Section 6 finally concludes the paper.

2 Preliminaries

We explain the models to evaluate cost of quantum computations in Sect. 2.1. We then summarize the cost of quantum multi-target preimage search in Sect. 2.2. Previous quantum attacks are reviewed in Sect. 2.3 and their drawbacks and unexplored topics are explained in Sect. 2.4.

2.1 Attack Models for Quantum Computations

Cost of Quantum Computation. There are two important quantities to evaluate the cost of quantum computation, *time* complexity and number of *qubits*.

The complexity of qubits is measured by the quantum register size of a quantum computer. Although memory is cheaper than processor in the classical setting, they are physically equivalent in the quantum setting. As pointed out by Grover and Rudolph [GR04], executing an algorithm using Q quantum memory and parallelly processing Q threads of 1-qubit processor are equally difficult.

As for time complexity, Bernstein [Ber09] pointed out that the way of realizing quantum hardware significantly impacts to running time of algorithms. We consider the following two models by following the terminology in [Ber09].

Free communication model. A quantum hardware can operate elementary quantum gates, e.g. Toffoli gates, on arbitrary pair of qubits. Thus the time complexity is equal to that of the well-known quantum circuit model.

Realistic communication model. Qubits in a quantum hardware are arranged in a square, and elementary operations can only be applied to the pair of qubits within a constant distance.

When the size of the qubits is only polynomial to the size of the problem to solve, restrictions from the hardware architecture has negligible impact in the evaluation of asymptotic time complexity. For example, suppose that a quantum hardware in realistic communication model with $O(n)$-qubits is available to solve the problem of size $O(2^n)$. Then, it can emulate a quantum hardware in free communication model with $O(n)$-qubits, only with time overhead of $O(n)$ (see [BBG$^+$13] for details).

Query Model. In the classical setting, an adversary is given an oracle that is usually a black box to her and the oracle runs a keyed operation such as encryption, decryption, or MAC. There are two quantum attack models that naturally extends the classical one, which are called *Q1 model* and *Q2 model* in [KLLN16b].

Q1 model: The adversary is allowed to make *classical* online queries, similarly as in the classical settings.

Q2 model: The adversary is allowed to make *quantum superposition* online queries. That is, oracles allow queries in quantum superposition states and return the results as quantum superposition states.

Q2 model implicitly requires that all the data on the network must be communicated as quantum superposition states, which is unrealistic.

2.2 Quantum Multi-target Preimage Search

Basics. Grover's algorithm [Gro96] is a quantum algorithm for unstructured database search problem, which is mathematically modeled as follows:

Problem 2.1. Let $f : \{0,1\}^n \to \{0,1\}$ be a binary function on the set of n-bit strings. The problem is to find an element $x \in \{0,1\}^n$ such that $f(x) = 1$.

Given f as a quantum circuit or a quantum oracle, and with the promise $|f^{-1}(1)| = 1$, the original algorithm [Gro96] solves this problem with $O(2^{n/2})$ evaluations of f. The algorithm was later generalized by Boyer *et al.* [BBHT98] to solve the problem without promise, and it can solve the problem with $O\left(\sqrt{2^n/\ell}\right)$ evaluations of f, here $\ell = |f^{-1}(1)|$. Hereafter, we also call this generalized one Grover's algorithm.

Proposition 2.1 ([BBHT98] Theorem 3). *Let $\ell = |f^{-1}(1)|$. There is a quantum algorithm that can solve Problem 2.1 with an expected number of $O(\sqrt{2^n/\ell})$ evaluations of f. If $\ell = 0$, then this algorithm will never abort.*

Quantum Multi-target Preimage Search. Let us consider to solve the following problem using quantum algorithms.

Problem 2.2. Fix a parameter $t < n/2$. Let $H : \{0,1\}^n \to \{0,1\}^n$ be a random function, and $L \subseteq \{0,1\}^n$ be a subset of size 2^t that is chosen uniformly at random. Given the list L and allowed to quantum oracle access to H, find $x \in \{0,1\}^n$ such that $H(x) \in L$.

Naive Algorithm. Naive way to solve the above problem is to apply Grover's algorithm as follows. Let us consider free communication model. First, we sort the list L. This requires $O(t2^t)$ classical computation. Let $f : \{0,1\}^n \to \{0,1\}$ be a function such that $f(x) = 1$ if and only if $H(x) \in L$. Since H is a random function and L is chosen randomly, $|f^{-1}(1)| \approx |L| = 2^t$. Thus, using Grover's algorithm, we can find $x \in \{0,1\}^n$ such that $f(x) = 1$, which is equivalent to $H(x) \in L$, with $O(2^{(n-t)/2})$ evaluation of f. One evaluation of f requires $O(1)$ evaluations of H, and a search in the list L, which can be done in time $O(t)$. Therefore the total computational time is $O(t2^{(n-t)/2})$. We need $O(2^t)$ qubits because L should be embedded to the quantum circuit of f. Eventually we obtain the following proposition.

Proposition 2.2. *In free communication model, there is a quantum algorithm that can solve Problem 2.2 in time $\tilde{O}(2^{(n-t)/2})$, using $O(2^t)$ qubits.*

Combination of Grover's Algorithm with Parallel Rho Method. At SAC 2017, Banegas and Bernstein [BB17] presented a parallelized quantum multi-target preimage search that combines Grover's algorithm with a parallel rho method [VOW94]. The paper has two results, which takes into account the ways of realizing quantum hardware.

One result is that, in free communication model, there exists a quantum algorithm that solves Problem 2.1 in time $\tilde{O}(\sqrt{2^n/p2^t})$ using $\tilde{O}(p)$ qubits, where $p \geq 2^t$. Another result is that, in realistic communication model, there exists a quantum algorithm that solves Problem 2.1 in time $\tilde{O}(\sqrt{2^n/p2^{t/2}})$ using $\tilde{O}(p)$ qubits, where $p \geq 2^t$.

This paper assumes that the number of qubits available is at most the size of L, which is 2^t. Setting $p = 2^t$, their results are summarized as follows.

Proposition 2.3 ([BB17]). *In free communication model, there exists a quantum algorithm that solves Problem 2.1 in time $\tilde{O}(\sqrt{2^n/2^{2t}})$, using $\tilde{O}(2^t)$ qubits. In realistic communication model, there exists a quantum algorithm that solves Problem 2.1 in time $\tilde{O}(\sqrt{2^n/2^{3t/2}})$, using $\tilde{O}(2^t)$ qubits.*

Algorithm with Small Number of Qubits. Even if the number of available qubits is limited to polynomial in n, we can use the algorithm from Asiacrypt 2017 by Chailoux *et al.* [CNPS17]. Note that as discussed in Section 2.1, quantum hardware architecture does not impact to its complexity.

Proposition 2.4 ([CNPS17], Theorem 3). *Assume that $t < \frac{3n}{7}$ holds. Then, there exists a quantum algorithm that can solve Problem 2.2 in time $\tilde{O}(2^{n/2-t/6})$, using $O(n)$ qubits and $\tilde{O}(2^{t/3})$ classical memory.*

2.3 Previous Quantum Attacks

Previous Quantum Attacks in Polynomial Time. Recently there has been many works on polynomial-time quantum attacks against symmetric-key schemes [Bon17,HA17,KM10,KM12,KLLN16a,KLLN16b,LL17b]. Those obtain *exponential speed-up* compared to classical attacks, while those work only in Q2 model to adopt Simon's algorithm [Sim97]. In short, Simon's algorithm can find the secret period of a periodic function $f : \{0,1\}^n \to \{0,1\}^n$ with time complexity of polynomial in n. The strategy of those attacks is to make a periodic function with a period that contains secret information. Then the secret is recovered by using Simon's algorithm.

Previous Quantum Attacks with Classical Online Queries. To avoid relying on strong but unrealistic Q2 model, several previous researches discussed quantum attacks in Q1 model, i.e. adversaries only can make classical queries [KM12,KLLN16b,Kap14,MS17]. This kind of attacks have been less focused compared to the attacks in Q2 model. In particular, the seminal work by Kuwakado and Morii against the Even-Mansour construction presented a key recovery attack in Q1 model as well as Q2 model [KM12]. Their attack in Q1 model requires $O(2^{n/3})$ classical online queries, $O(2^{n/3})$ quantum offline computations and $O(2^{n/3})$ qubits of memory.

2.4 Unexplored Topics and Drawbacks of Previous Work

As discussed above, many of the previous work can be classified into two classes; polynomial-time complexity in Q2 model, $\mathtt{Class}^{\mathtt{Q2}}_{\mathtt{Poly}}$, and exponential-time complexity (but significantly improves classical attacks) in Q1 model, $\mathtt{Class}^{\mathtt{Q1}}_{\mathtt{Exp}}$. Most of the previous work focused on $\mathtt{Class}^{\mathtt{Q2}}_{\mathtt{Poly}}$, yet Kuwakado and Morii [KM12] showed that attacks in $\mathtt{Class}^{\mathtt{Q2}}_{\mathtt{Poly}}$ may also belong to $\mathtt{Class}^{\mathtt{Q1}}_{\mathtt{Exp}}$. This motivates us to search for attacks in $\mathtt{Class}^{\mathtt{Q1}}_{\mathtt{Exp}}$ because Q1 model is more realistic. We will show may problems that belong to $\mathtt{Class}^{\mathtt{Q1}}_{\mathtt{Exp}}$ but not to $\mathtt{Class}^{\mathtt{Q2}}_{\mathtt{Poly}}$. If researchers only focus on $\mathtt{Class}^{\mathtt{Q2}}_{\mathtt{Poly}}$, those problems will be overlooked.

Another observation is that the attack in [KM12] in $\mathtt{Class}^{\mathtt{Q1}}_{\mathtt{Exp}}$ may not be optimal if the observations in [GR04] about the equivalence of quantum memory and processor and in [Ber09] about the cost in realistic hardware architecture are considered. Indeed, the attack in [KM12] requires $O(2^{n/3})$ classical queries and $O(2^{n/3})$ qubits to achieve $O(2^{n/3})$ time complexity, while the parallel execution of Grover's algorithm using $O(2^{n/3})$ qubits only require $O(1)$ query to achieve $O(2^{n/3})$ time complexity. This motivates us to optimize the attack by taking into account recent observations about the complexity.

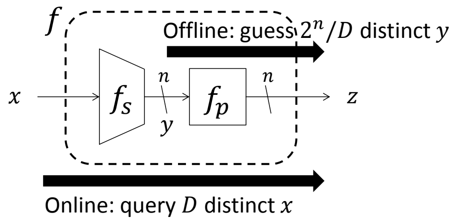

Fig. 2. General Settings for Online-Offline MitM

3 General Framework

In this section, we present a general framework of the quantum online-offline MitM attack in Q1 (classical query) model. We review the classical online-offline MitM attack in Sect 3.1. We then introduce quantum online-offline MitM attack in Q1 model in Sect 3.2. The impact of new tradeoffs is discussed in Sect. 3.3.

3.1 Classical Online-Offline MitM Attack

Let $f : \{0,1\}^* \mapsto \{0,1\}^n$ be a secret function with n-bit output and suppose that f is the composition of a secret function with n-bit output $f_s : \{0,1\}^* \mapsto \{0,1\}^n$ followed by an n-bit to n-bit public function $f_p : \{0,1\}^n \mapsto \{0,1\}^n$, namely $f = f_p \circ f_s$ as illustrated in Fig. 2. Here, the input, the internal state and the output are denoted by x, y and z, respectively.

The online-offline MitM attack is a type of the MitM attack, in which the adversary first makes D online queries to collect D output values with randomized n-bit internal state, and then makes $2^n/D$ random guesses of the internal state and computes f_p offline. The match of the n-bit output suggests the correct value of the n-bit internal state. To be more precise, the attack is described in Algorithm 1 in an algorithmic form.

Algorithm 1 Classical Online-Offline MitM Attack

Classical Online Queries

for $i \leftarrow 1, 2, \ldots, D$ **do**
  Choose distinct input x_i.
  Query x_i to f, and store the corresponding z_i in the classical memory L.
end for

Classical Offline Computations

for $j \leftarrow 1, 2, \ldots, \frac{2^n}{D}$ **do**
  Guess internal state value y^j
  Compute $z_j \leftarrow f_p(y_j)$ offline and check a match between z_j and L.
end for

The number of possible pairs from online and offline phases is 2^n, thus a match of the n-bit value is expected with a reasonably high probability. The classical online-offline MitM attack provides the tradeoff of

$$D \cdot T = N, \tag{1}$$

where D and T are balanced when $D = T = N^{1/2}$.

3.2 Quantum Online-Offline MitM Attack

We now introduce the quantum online-offline MitM attack in Q1 model. Queries can only be made in the classical manner. Hence, the online phase in Algorithm 1 stays unchanged, and we replace the offline phase performing classical computations with quantum ones.

Insufficiency of Applying Multi-target Preimage Search. The simplest way is applying the naive multi-target preimage search in section 2.2 instead of the random guess in Algorithm 1. When D targets are available in the quantum list, as in Proposition 2.1, the multi-target preimage search runs with $T = O(\sqrt{N/D})$ quantum computations. Hence, the tradeoff becomes $D{\cdot}T^2 = N$, in which T and D are balanced when $T = D = N^{1/3}$. This achieves a good improvement over the classical setting. However, this method has the crucial drawback; $D = N^{1/3}$ qubits are exploited only for storing the data. If we apply Grover's algorithm (for key search) in parallel with $N^{1/3}$ qubits, the offline phase for $D = 1$ can finish in $O(N^{1/3})$, which is better than applying the multi-target preimage search in terms of the low data complexity. This discussion shows that it is insufficient to simply replace the classical offline phase with a quantum algorithm using qubits only for storing the data.

Case Analysis Depending on Quantum Hardware. Let Q be the number of qubits available to the attacker. We will use each of Q qubits to process quantum operations rather than to store the data. Here, the computational cost of quantum algorithms relies on Q. Hence we do the case analysis; the first case assumes that Q can be an exponential size, while the second case assumes that Q only can be a limited size. The first case analyzes the future that is more advantageous to the attacker, while the second case is more challenging to her.

Bernstein [Ber09], and also Banegas and Bernstein [BBG$^+$13], pointed out that the hardware architecture, i.e. how to positioning qubits in quantum hardware, significantly impacts to the computational cost of quantum algorithms. As discussed in Sect 2.1, we consider the free and realistic communication models. The former allows any qubit to interact with any other qubit. The latter assumes that each qubits is arranged in a square and the range to interact is limited. The gap between two models is big when Q is an exponential size. While for a sufficiently small Q, say polynomial in $\log N$, the way of realizing hardware does not significantly effect on the time complexity. In summary, we analyze the following three cases.

1. Q is exponential (more advantageous to the attacker).
   (a) free communication model
   (b) realistic communication model
2. Q is not exponential (more challenging to the attacker).

In the following case analysis, we assume that the classical online queries collect D targets and those are stored in the classical memory M.

Tradeoff for Case 1a. It assumes that Q qubits are available in the free-communication model, where $O(Q) \geq D$. Banegas and Bernstein [BBG+13] showed that the computational cost T of the multi-target preimage search in the free communication model is

$$T = \tilde{O}\Big(\sqrt{\frac{N}{Q \cdot D}}\Big).$$

By setting $Q = D$, the tradeoff for Case 1a becomes

$$D^2 \cdot T^2 = N, \tag{2}$$

where D and T are balanced when $D = T = N^{1/4}$. Q and M are also $N^{1/4}$.

Tradeoff for Case 1b. It assumes that Q qubits are available in the realistic-communication model, where $O(Q) \geq D$. Banegas and Bernstein [BBG+13] showed that the computational cost T of the multi-target preimage search in the realistic communication model is

$$T = \tilde{O}\Big(\sqrt{\frac{N}{Q \cdot D^{1/2}}}\Big).$$

By setting $Q = D$, the tradeoff for Case 1b becomes

$$D^{3/2} \cdot T^2 = N, \tag{3}$$

where D and T are balanced when $D = T = Q = M = N^{2/7}$.

Tradeoff for Case 2. It assumes that $Q = O(\log N)$ qubits are available in the free communication model. Chailloux *et al.* [CNPS17] showed that T of the multi-target preimage search with $O(\log N)$ qubits is

$$T = \tilde{O}\Big(\frac{N^{1/2}}{D^{1/6}}\Big)$$

for $D < N^{3/7}$, using $D^{1/3}$ classical memory. The tradeoff for $D < N^{3/7}$ in Case 2 becomes

$$D \cdot T^6 = N^3, \tag{4}$$

where D and T are balanced when $D = T = N^{3/7}$. Note that $T = N^{3/7}$ even with $D > N^{3/7}$. The number of qubits $Q = O(\log N)$ is sufficiently small when N in practical functions are considered. For example, $N = 2^{128}$, $D = 2^{42}$, and $Q = 128 \cdot c$ for a small constant c in an example discussed in Sect. 4.

Table 1. Tradeoff of Online-Offline MitM Attack in Various Models

reference	Sect. 3.1	Case 1a	Case 1b	Case 2
query model	classic	classic	classic	classic
num of qubits	0	$O(D)$	$O(D)$	$O(\log N)$
comm model	-	free	realistic	free
algorithm	Algorithm 1	[BBG+13]	[BBG+13]	[CNPS17]
tradeoff	$D \cdot T = N$	$D^2 \cdot T^2 = N$	$D^{3/2} \cdot T^2 = N$	$D \cdot T^6 = N^3$
$\min\{D, T\}$	$N^{1/2}$	$N^{1/4}$	$N^{2/7}$	$N^{3/7}$

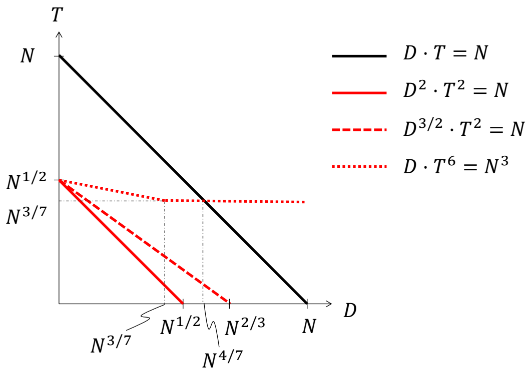

Fig. 3. Illustration of Tradeoff Curves (plotted in logarithmic scale)

3.3 Impact

The tradeoffs of the online-offline MitM attacks are compared in Table 1. The tradeoff curves are plotted in Fig. 3. As long as Q is an exponential size, the complexities of the quantum attacks are exponentially smaller than ones in the classical online-offline MitM. When Q is $O(\log N)$, the quantum attack improves T as long as $D \leq N^{4/7}$.

As we later discuss in Sect. 4, several existing schemes claim BBB security by setting the number of maximum queries to be less than $N^{1/2}$ to ensure the minimum number of computational cost is more than $N^{1/2}$ according to the classic tradeoff in Eq (1). Such security claims collapse against attackers with quantum computers even in Q1 model.

4 Applications of Online-Offline MitM Attacks

In this section, we discuss that the online-offline MitM attack can be applied to a lot of existing symmetric-key schemes. Section 4.1 focuses on the two schemes that claim BBB security by limiting the maximum number of queries per key. Section 4.2 shows a few more schemes where the quantum online-offline MitM attack can be directly applied.

4.1 Applications to Schemes with Beyond-Birthday-Bound Security

Chaskey. Chaskey [Mou15,MMH+14] is a light-weight MAC scheme. The construction follows CBC-MAC but the n-bit block cipher in CBC-MAC is replaced with Even-Mansour construction with a public n-bit permutation.

It uses an n-bit key K, and generates the second key K_1 by $K_1 \leftarrow 2 \cdot K$, where '$\cdot$' is a multiplication over a finite field. Suppose that the size of the input message M is a multiple of n. M is then divided into n-bit blocks such that $M_1 \| M_2 \| \cdots \| M_\ell \leftarrow M$. Let π be an n-bit public permutation. Then, a tag Z for M is computed as follows, which is illustrated in Fig. 4.

1. $\texttt{State} \leftarrow K$
2. $\texttt{State} \leftarrow \pi(\texttt{State} \oplus M_i)$ for $i = 1, 2, \cdots, \ell - 1$.
3. $\texttt{State} \leftarrow \pi(\texttt{State} \oplus M_\ell \oplus K_1)$
4. $Z \leftarrow \texttt{State} \oplus K_1$.

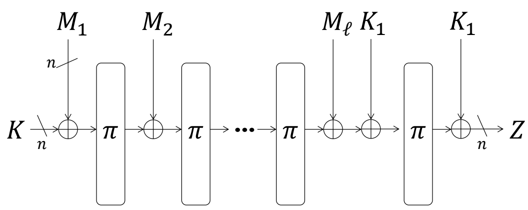

Fig. 4. Computation Structure of Chaskey

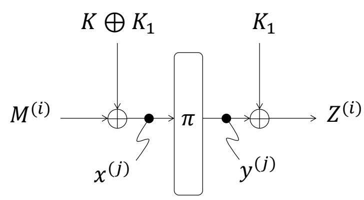

Fig. 5. Online-Offline MitM Attack against Chaskey

Security of Chaskey is the same level as the Even-Mansour construction. Indeed, when the input message length is 1-block, the construction becomes Even-Mansour construction with the first key $K \oplus K_1$ and the second key K_1. It is known that, even by the classical adversaries, Even-Mansour construction can be attacked with D queries and T offline computations satisfying $D \cdot T = 2^n$.

The size of the permutation π is 128 bits in Chaskey. Hence it can be attacked with $D = T = 2^{64}$ even by the classical adversaries, while 64-bit security is sometimes too small. To overcome this problem, the designers set the limitation that the number of MACs generated under a single key must be up to 2^{48}. Then, it offers 80-bit security against offline computations.

Attack Procedure. The online-offline MitM attack can be directly applied to Chaskey. The attack in [KM12] targets the two-key Even-Mansour construction, hence the attack uses two pairs of ciphertexts and takes the difference of them to eliminate the impact of the second key K_2. In our 1-block attack in Chaskey illustrated in Fig. 5, K_1 is linearly derived from K. Hence, we make a small optimization for Chaskey to improve the constant factor of 2.

We first revisit the attack in the classical model. The adversary chooses D distinct messages $M^{(i)}$ and obtains the corresponding tag $Z^{(i)}$ via encryption queries. In the offline phase, the adversary makes T guesses $x^{(j)}$ of the input value to π and calculates its output $y^{(j)}$ offline. Here, we have

$$M^{(i)} \oplus x^{(j)} \oplus y^{(j)} \oplus Z^{(i)} = K, \qquad K_1 = y^{(j)} \oplus Z^{(i)} = 2 \cdot K.$$

Hence, $2(M^{(i)} \oplus x^{(j)} \oplus y^{(j)} \oplus Z^{(i)}) = y^{(j)} \oplus Z^{(i)}$, which is converted to the match between two values computed online and offline;

$$2M^{(i)} \oplus 2Z^{(i)} \oplus Z^{(i)} = 2 \cdot x^{(j)} \oplus 2y^{(j)} \oplus y^{(j)}.$$

The match suggests the key K. Hence, with $DT = 2^n$, the key is recovered. In other words, we simply run Algorithm 1 by defining f and f_p as

$$f(m) : \{0,1\}^n \mapsto \{0,1\}^n \triangleq 2 \cdot m \oplus 2 \cdot \text{Chakey}(m) \oplus \text{Chakey}(m),$$
$$f_p(x) : \{0,1\}^n \mapsto \{0,1\}^n \triangleq 2 \cdot x \oplus 2 \cdot \pi(x) \oplus \pi(x).$$

As discussed in Sect 3.2, the complexity of the quantum algorithm depends on the assumptions of the quantum hardware architecture.

Case 1a (exponential qubits, free communication). The internal state (and then both keys) are recovered at the balanced point of the tradeoff curve, in which $D = T = Q = M = 2^{128/4} = 2^{32}$.

Case 1b (exponential qubits, realistic communication). The attack is performed at the balanced point; $D = T = Q = M = 2^{2 \cdot 128/7} \approx 2^{36.6}$.

Case 2 (non-exponential qubits). The balanced point $2^{3 \cdot 128/7} \approx 2^{54.9}$ cannot be reached due to the limitation of the number of queries. When $D = 2^{48}$, Q is $O(\log N) = 128 \cdot c$ for a small constant c and $M = D^{1/3} = 2^{16}$. The tradeoff curve becomes $2^{48} \cdot T^6 = 2^{3 \cdot 128}$, which leads to $T = 2^{56}$.

In any case, T is overwhelmingly smaller than 2^{80} of the classical attack.

Remarks on Chaskey-B. The original paper of Chaskey [MMH+14] proposes a block-cipher variant of Chaskey, called Chaskey-B. Roughly speaking, it replaces a public permutation π of Chaskey with block-cipher E_k, which makes the construction identical with a standard CBC-MAC.

As shown by Kaplan *et al.* [KLLN16a] and Liu and Liu [LL17b], (universal) forgery can be applied in Q2 model, while no method is known to break birthday bound in Q1 model. This indicates that Chaskey and Chaskey-B have very different security level against quantum adversaries in Q1 model.

Tweak-Dependent Rekeying (TDR). At FSE 2009, Minematsu proposed a block cipher mode-of-operation called *tweak-dependent rekeying (TDR)*, which constructs a TBC with BBB security [Min09]. Let E_K be a block cipher of which both the block size and key size are n bits. Let E_K^w be a construction in which the

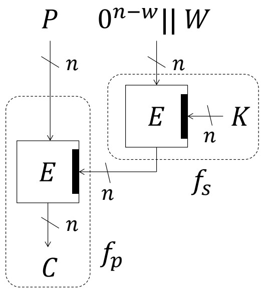

Fig. 6. Tweak Dependent Rekeying (TDR)

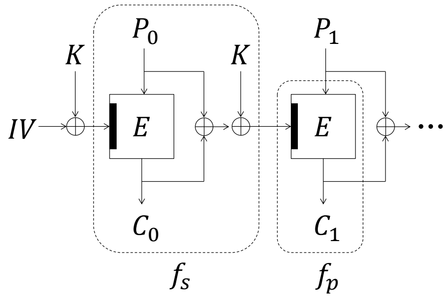

Fig. 7. McOE-X

first $n-w$ bits of the plaintext for E_K are fixed to 0, which reduces the plaintext space from n bits to w bits. TDR builds a tweakable block cipher (using w-bit tweak) with two E_K calls; $K' \leftarrow E^w_K(W)$ then $C \leftarrow E_{K'}(P)$. The construction is illustrated in Fig. 6.

Minematsu proved that TDR achieves the security curve $D \cdot T = 2^n$ against classical adversaries. This bound is tight. The online-offline MitM attack in Algorithm 1 can be applied by fixing P to an arbitrary chosen one, defining f as a oracle query to TDR and defining f_p as $E_{K'}$ with guessing K'. The attack reveals K'. Although K is not recovered, knowledge of K' allows the adversary to convert any P to C or C to P, thus confidentially is broken.

AES is considered as an underlying cipher, thus $n = 128$. When $w < n/2$, BBB security is proved against the offline computational cost. Minematsu recommended $w = n/3$ to ensure $2n/3$-bit security. For the AES instantiation, w is set to 42 bits, thus security for the offline computation is up to 86 bits.

Similarly to Chaskey, the quantum online-offline MitM can directly be applied with about 2^{32} and $2^{36.6}$ complexities for Case 1a and Case 1b, respectively. For Case 2, $D = 2^{42}$, $Q = 128 \cdot c$ qubits for a small constant c, $M = 2^{14}$ classical memory, and $T = 2^{57}$.

Comparison with other TBC constructions is of interest. On one hand, some TBC constructions such as LRW and XEX can be broken with $O(n)$ complexity in Q2 model [KLLN16a], while no attack is known in Q1 model (though we will propose another type of tradeoff for 2-key variants in Sect. 5). On the other hand TDR resists $O(n)$ attack in Q2 model, while security in Q1 model is worse than LRW and XEX. As shown in Fig. 1, those TBC constructions essentially belong to different classes. We again believe that such knowledge will help cryptographers to design new schemes with post-quantum security.

4.2 Application to Other Schemes

We show more applications that the quantum online-offline MitM attack in Q1 model can be applied while the attack with $O(n)$ complexity in Q2 model cannot be applied.

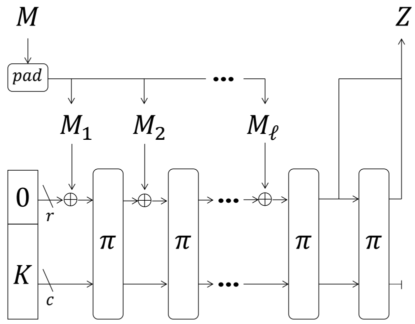

Fig. 8. Keyed Sponge

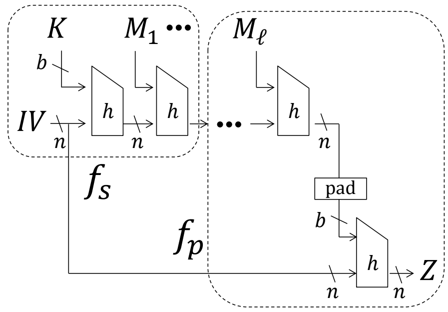

Fig. 9. H^2MAC

McOE-X. Fleischmann *et al.* proposed the McOE family of online authenticated encryption schemes [FFL12]. Their idea is to use a TBC to process each message block, where the tweak is an XOR of plaintext and ciphertext in the previous block. Let $E_{K,W}$ be a TBC under a key K and a tweak W. Then, the ciphertext C_i of the i-th message block P_i is computed by

$$W_i \leftarrow P_{i-1} \oplus C_{i-1}, \qquad\qquad C_i \leftarrow E_{K,W_i}(P_i).$$

Among several instances to compute $E_{K,W}$, McOE-X defines that $E_{K,W} = E_{K \oplus W}$. The construction is illustrated in Fig. 7.

Mendel *et al.* [MMRT12] showed that the key of McOE-X can be recovered with $D \cdot T = N$, by applying the meet-in-the-middle attack. According to the framework in Algorithm 1, we fix P_1 to arbitrary chosen one, define f as the query of $P_0 \| P_1$ and define f_p as the second block with guessing the key input.

By replacing the classical offline computation in Algorithm 1 with quantum one, the attack complexity is significantly improved as discussed in Sect 3.

Keyed Sponge. The sponge construction and its application to keyed usages were introduced by Bertoni *et al.* [BDPA08]. It is based on a permutation $\pi : \{0,1\}^b \mapsto \{0,1\}^b$ and has two parameters; rate r and c, where $r + c = b$. The keyed sponge construction takes as input a key $K \in \{0,1\}^k$ where $k < c$ and an arbitrary length message M to produce an n-bit tag Z. The b-bit state S is initialized to $0^{b-k} \| K$. The message M is separated into r-bit blocks as $M_1 \| M_2 \| \cdots \| M_\ell$ and is absorbed to the state block-by-block by $S \leftarrow \pi(S \oplus M_i \| 0^c)$ for $i = 1, 2, \cdots, \ell$. After all M_ℓ is absorbed, it starts to squeeze the output by r bits from each state. Let $trunc_r$ denote a truncation of r bits. When n is a multiple of r, Z is generated by $Z_i \leftarrow trunc_r(S), S \leftarrow \pi(S)$ for $i = 1, 2, 3, \cdots$, until the size of $Z = Z_1 \| Z_2 \| Z_3 \| \cdots$ reaches n bits. See Fig. 8 for the construction.

Liu and Liu [LL17a] found that the full-state keyed sponge ($c = 0$ during the absorption) can be attacked with $O(c)$ in Q2 model, as well as the Even-Mansour construction, by applying Simon's algorithm. In this paper, we analyze more popular case; quantum attacks in Q1 model on ordinary keyed sponge in Fig. 8. For example, KMAC standardized by NIST [NIS16] adopts the keyed sponge in a slightly different way from Fig. 8; first initializes the state to a constant and processes $K\|M$. This small difference does not impact to our attack.

With the classical environment, key recovery attack with a complexity $2^{c/2}$ is known that works as follows. Here, we assume that the tag size n is 1-block.

1. Iterate the following two steps D times.
   (a) Choose a random 1-block message M and query it to obtain Z_1.
   (b) Query a 2-block message $M' = M\|Z_1$ to obtain Z', and store it in L.
2. Make $2^c/D$ guesses of c-bit capacity and compute $S \leftarrow \pi(0^r\|c)$ offline. Check whether $trunc_r(S)$ matches one of the values in L.

Step 1b ensures that the rate of the state after Z_0 is observed is 0. Hence, L collects tag values for D randomly generated capacity values while the rate is 0. Step 2 takes a role of f_p in Algorithm 1. The match recovers the entire state value, thus key K can be recovered by backtracking the computation with π^{-1}.

As the procedure clearly suggests, this is an offline-online MitM and thus by replacing Step 2 with quantum algorithm, the keyed sponge construction can be attacked in Q1 model with complexity discussed in Sect 3.

$\mathbf{H^2}$-MAC. H^2-MAC, a variant of HMAC without second key, was proposed by Yasuda [Yas09] with birth-bound security proved. It takes a key K and a message $M = M_1\|M_2\|\ldots\|M_\ell$ as input and computes an n-bit MAC tag. Let $h : \{0,1\}^{b+n} \mapsto \{0,1\}^n$ be a compression function. Let also IV and H_i be an n-bit constant and n-bit variable, respectively. The scheme first computes $H_1 \leftarrow h(IV, K)$, then iteratively process message blocks by $H_{i+1} \leftarrow h(H_i, M_i)$ for $i = 1, 2, \cdots, \ell$. Finally, the tag Z is computed by $Z \leftarrow h(IV, \mathrm{pad}(H_{\ell+1}))$ with a proper padding scheme "pad." See Fig. 9 for its illustration.

The forgery attack in the classical setting was proposed by Liu *et al.* [LXS11] by online-offline MitM, which runs Algorithm 1 by defining f as the entire query and f_p as the offline computation from the second block with guessing H_2. As discussed in Sect 3, the quantum offline computation can be applied in Q1 model.

We stress that the same attack can be applied to other secret-prefix MACs [Tsu92], for example, LPMAC attacked by Sasaki [Sas12].

5 Attacks on the FX Construction in Q1 Model

This section gives a Q1-model attack on the FX construction by applying our strategy of general framework, inspired by the Q2-model attack by Leander and May [LM17]. The FX construction, proposed by Killian and Rogaway [KR96,KR01], is a block cipher adopting a similar structure as the Even-Mansour construction, where its public random permutation is replaced with a block cipher. Let E be an n-bit block cipher with m-bit key. Then the FX construction using E is an n-bit block cipher with $m+2n$-bit key, of which encryption of M is defined as

$$FX^E_{k_0,k_1,k_2}(M) = E_{k_0}(M \oplus k_1) \oplus k_2.$$

Since k_0 is secret, the quantum key recovery attack against the Even-Mansour construction in [KM12] can no longer be used.

Leander and May cleverly combined Grover's algorithm and Simon's algorithm to make a quantum key recovery attack on the FX construction [LM17]. Their attack requires Q2 model. In short, it runs Simon's algorithm in parallel to recover k_1 and runs Grover's algorithm to guess k_0, The time complexity is $\tilde{O}(2^{m/2})$ by using $O(m+n^2)$ qubits. Although the attack requires strong Q2 model, it costs exponential time owing to Grover's algorithm.

Here, we describe a *classical* key recovery attack against the FX construction with a cost of D queries and T computations satisfying $D \cdot T = 2^{m+n}$. Set $\alpha := \lceil \frac{m}{n} \rceil$. Let $H : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^{(\alpha+1)n}$ be a function defined by

$$H(k,x) := E_k(x) \oplus E_k(x \oplus 1) \| \cdots \| E_k(x) \oplus E_k(x \oplus (\alpha+1)).$$

1. Choose D distinct values of message $M^{(i)}$, query $M^{(i)}, M^{(i)} \oplus 1, \ldots, M^{(i)} \oplus (\alpha+1)$ to the encryption oracle, and obtain the corresponding ciphertexts $C_0^{(i)}, C_1^{(i)}, \ldots, C_{\alpha+1}^{(i)}$. Store $M^{(i)}$ in a table L along with $C_0^{(i)} \oplus C_1^{(i)} \| \cdots \| C_0^{(i)} \oplus C_{\alpha+1}^{(i)}$. (Note that $C_0^{(i)} \oplus C_1^{(i)} \| \cdots \| C_0^{(i)} \oplus C_{\alpha+1}^{(i)} = H(k_0, M^{(i)} \oplus k_1)$ holds.)
2. Make exhaustive 2^m guesses of k_0, denoted by k', T guesses of $M \oplus k_1$, and compute $H(k', M \oplus k_1)$. Check for a match of the value $H(k', M \oplus k_1) = C_0 \oplus C_1 \| \cdots \| C_0 \oplus C_{\alpha+1}$ with L.

The above attack succeeds with high probability, since H is an almost random function, and the following holds with high probability;

$$H(k,x) = H(k',y) \text{ if and only if } (k,x) = (k',y).$$

From a different point of view, the above attack procedure is essentially equal to running Algorithm 1 for $N = 2^{m+n}$ by defining f and f_p as

$$f(M) : \{0,1\}^n \mapsto \{0,1\}^n \triangleq H(k_0, M \oplus k_1),$$
$$f_p(k,x) : \{0,1\}^m \times \{0,1\}^n \mapsto \{0,1\}^n \triangleq H(k,x).$$

While the strategy of attacks in Sect. 4 is simply to find a collision of two functions f and f_p, here we additionally need to guess m-bit key k_0. Moreover, there is a limitation that $D \leq N/2^m$ since D cannot exceed 2^n.

Next, we convert the above classical attack to a quantum attack only with classical online queries. We again consider three cases. Due to the condition $D \leq N/2^m$, we set upper limit of m for each case.

Case 1a (exponential qubits, free-communication). Assume $m \leq 3n$. The attack is performed at the balanced point; $D = T = Q = M = 2^{\frac{(m+n)}{4}}$.

Case 1b (exponential qubits, realistic-communication). Assume $m \leq 5n/2$. The attack is performed at the balanced point; $D = T = Q = M = 2^{\frac{2(m+n)}{7}}$.

Case 2 (non-exponential qubits). Assume $m \leq 4n/3$. The attack is performed at the balanced point; $D = T = 2^{\frac{3(m+n)}{7}}$, using $O(n)$ qubits and $M = \tilde{O}(2^{\frac{m+n}{7}})$ classical memory.

Applications to Two-Key Variants of LRW, XEX and XE. The LRW construction [LRW11] is a TBC construction based on a block cipher proposed by Liskov *et al.* It replaces whitening keys k_1, k_2 of the FX construction with a single value $h(w)$, where w is a tweak and h is a secret function: $LRW^E_{k_0,w}(M) = E_{k_0}(M \oplus h(w)) \oplus h(w)$.

Kaplan *et al.* [KLLN16a] proposed polynomial-time attacks in Q2 model against the LRW, XEX and XE constructions, where XEX and XE are concrete instantiations of LRW.

Typically, h is dependent on the secret key k_0, though it may be of interest to consider a two-key variant of these constructions, i.e. h is independent from k_0. For the two-key variant, the structure becomes essentially the same as the FX construction, and thus we can apply the above attack in Q1 model to LRW, XEX, and XE, with the same complexities.

6 Concluding Remarks

We presented quantum attacks against symmetric-key schemes in Q1 model, which is more realistic than Q2 model but does not receive much attention before. We converted the classical online-offline MitM attacks into quantum ones in Q1 model. The complexity depends on the number of qubits available and communication models. We derived the new tradeoff in three models. Some existing schemes claim BBB security on T by limiting the maximum number of D by following the classical tradeoff $D \cdot T = N$. Our attack breaks such claims if adversary can access to quantum computers.

Efficiency of the quantum attacks depend on the construction of the schemes. Possible future directions are looking for more instances of $\mathtt{Class}^{\mathtt{Q1}}_{\mathtt{Exp}}$ and $\mathtt{Class}^{\mathtt{Q2}}_{\mathtt{Poly}}$, or searching for a class of schemes with different cryptanalysis approaches.

References

[BB17] Gustavo Banegas and Daniel J. Bernstein. Low-communication parallel quantum multi-target preimage search. Cryptology ePrint Archive, Report 2017/789, 2017. To appear at SAC2017.

[BBG+13] Robert Beals, Stephen Brierley, Oliver Gray, Aram W. Harrow, Samuel Kutin, Noah Linden, Dan Shepherd, and Mark Stather. Efficient distributed quantum computing. In *Proceedings of the Royal Society A*, volume 469, page 20120686. The Royal Society, 2013.

[BBHT98] Michel Boyer, Gilles Brassard, Peter Høyer, and Alain Tapp. Tight bounds on quantum searching. *Fortsch. Phys.*, 46(4-5):493–505, June 1998. https://arxiv.org/abs/quant-ph/9605034.

[BDPA08] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. On the indifferentiability of the sponge construction. In Nigel P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 181–197. Springer, 2008.

[Ber09] Daniel J. Bernstein. Cost analysis of hash collisions: will quantum computers make SHARCS obsolete? In *SHARCS 2009*, 2009.

[BHT97] Gilles Brassard, Peter Høyer, and Alain Tapp. Quantum algorithm for the collision problem. *CoRR*, quant-ph/9705002, 1997. Quantum Cryptanalysis of Hash and Claw-Free Functions. LATIN 1998: 163-169.

[Bon17] Xavier Bonnetain. Quantum key-recovery on full AEZ. Cryptology ePrint Archive, Report 2017/767, 2017. To appear at SAC 2017.

[CNPS17] André Chailloux, María Naya-Plasencia, and André Schrottenloher. An efficient quantum collision search algorithm and implications on symmetric cryptography. Cryptology ePrint Archive, Report 2017/847, 2017.

[FFL12] Ewan Fleischmann, Christian Forler, and Stefan Lucks. McOE: A family of almost foolproof on-line authenticated encryption schemes. In Anne Canteaut, editor, *FSE 2012*, volume 7549 of *LNCS*, pages 196–215. Springer, 2012. Cryptology ePrint Archive, Report 2011/644.

[GR04] Lov Grover and Terry Rudolph. How significant are the known collision and element distinctness quantum algorithms. *Quantum Info. Comput.*, 4(3):201–206, May 2004.

[Gro96] Lov. K Grover. A fast quantum mechanical algorithm for database search. In *STOC 1996*, pages 212–219, 1996. https://arxiv.org/abs/quant-ph/9605043.

[HA17] Akinori Hosoyamada and Kazumaro Aoki. On quantum related-key attacks on iterated Even-Mansour ciphers. In Satoshi Obana and Koji Chida, editors, *IWSEC 2017*, volume 10418 of *LNCS*, pages 3–18. Springer, 2017.

[Kap14] Marc Kaplan. Quantum attacks against iterated block ciphers. *arXiv preprint arXiv:1410.1434*, 2014.

[KLLN16a] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Breaking symmetric cryptosystems using quantum period finding. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part II*, volume 9815 of *LNCS*, pages 207–237. Springer, 2016.

[KLLN16b] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Quantum differential and linear cryptanalysis. *IACR Trans. Symmetric Cryptol.*, 2016(1):71–94, 2016.

[KM10] Hidenori Kuwakado and Masakatu Morii. Quantum distinguisher between the 3-round Feistel cipher and the random permutation. In *ISIT 2010*, pages 2682–2685. IEEE, 2010.

[KM12] Hidenori Kuwakado and Masakatu Morii. Security on the quantum-type Even-Mansour cipher. In *ISITA 2012*, pages 312–316. IEEE, 2012.

[KR96] Joe Kilian and Phillip Rogaway. How to protect DES against exhaustive key search. In Neal Koblitz, editor, *CRYPTO'96*, pages 252–267. Springer, 1996.

[KR01] Joe Kilian and Phillip Rogaway. How to protect DES against exhaustive key search (an analysis of DESX). *J. Cryptology*, 14:17–35, 2001.

[LL17a] Fanbao Liu and Fengmei Liu. Universal forgery and key recovery attacks: Application to FKS, FKD and Keyak. Cryptology ePrint Archive, Report 2017/691, 2017.

[LL17b] Fanbao Liu and Fengmei Liu. Universal forgery with birthday paradox: Application to blockcipher-based message authentication codes and authenticated encryptions. Cryptology ePrint Archive, Report 2017/653, 2017.

[LM17] Gregor Leander and Alexander May. Grover meets Simon - quantumly attacking the FX-construction. Cryptology ePrint Archive, Report 2017/427, 2017. To appear at Asiacrypt 2017.

[LRW11] Moses Liskov, Ronald L. Rivest, and David A. Wagner. Tweakable block ciphers. *J. Cryptology*, 24(3):588–613, 2011.

[LXS11] Fanbao Liu, Tao Xie, and Changxiang Shen. Breaking H^2-MAC using birthday paradox. Cryptology ePrint Archive, Report 2011/647, 2011.

[MBTM17] Kerry A. McKay, Larry Bassham, Meltem Snmez Turan, and Nicky Mouha. NISTIR 8114 Report on Lightweight Cryptography. Technical report, U.S. Department of Commerce, National Institute of Standards and Technology, 2017. https://doi.org/10.6028/NIST.IR.8114.

[Min09] Kazuhiko Minematsu. Beyond-birthday-bound security based on tweakable block cipher. In Orr Dunkelman, editor, *FSE 2009*, volume 5665 of *LNCS*, pages 308–326. Springer, 2009.

[MMH$^+$14] Nicky Mouha, Bart Mennink, Anthony Van Herrewege, Dai Watanabe, Bart Preneel, and Ingrid Verbauwhede. Chaskey: An efficient MAC algorithm for 32-bit microcontrollers. In Antoine Joux and Amr M. Youssef, editors, *SAC 2014*, volume 8781 of *LNCS*, pages 306–323. Springer, 2014.

[MMRT12] Florian Mendel, Bart Mennink, Vincent Rijmen, and Elmar Tischhauser. A simple key-recovery attack on McOE-X. In Josef Pieprzyk, Ahmad-Reza Sadeghi, and Mark Manulis, editors, *CANS 2012*, volume 7712 of *LNCS*, pages 23–31. Springer, 2012.

[Mou15] Nicky Mouha. Chaskey: a MAC algorithm for microcontrollers – status update and proposal of Chaskey-12 –. Cryptology ePrint Archive, Report 2015/1182, 2015.

[MS17] Bart Mennink and Alan Szepieniec. XOR of PRPs in a quantum world. In Tanja Lange and Tsuyoshi Takagi, editors, *PQCrypto 2017*, volume 10346 of *LNCS*, pages 367–383. Springer, 2017.

[NIS16] NIST. SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash. Technical report, U.S. Department of Commerce, National Institute of Standards and Technology, 2016. NIST Special Publication (SP) 800-185.

[Sas12] Yu Sasaki. Cryptanalyses on a merkle-damgård based MAC - almost universal forgery and distinguishing-h attacks. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 411–427. Springer, 2012.

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

[Tsu92] Gene Tsudik. Message authentication with one-way hash functions. In *ACM SIGCOMM Computer Communication Review*, volume 22(5), pages 29–38. ACM, 1992.

[VOW94] Paul C Van Oorschot and Michael J Wiener. Parallel collision search with application to hash functions and discrete logarithms. In *CCS'94*, pages 210–218. ACM, 1994.

[Yas09] Kan Yasuda. HMAC without the "second" key. In Pierangela Samarati, Moti Yung, Fabio Martinelli, and Claudio Agostino Ardagna, editors, *ISC 2009*, volume 5735 of *LNCS*, pages 443–458. Springer, 2009.