Universal Forgery and Key Recovery Attacks: Application to FKS, FKD and Keyak

Fanbao Liu and Fengmei Liu

Science and Technology on Information Assurance Laboratory, Beijing, 10072, China
lfbjantie@163.com

Abstract. In this paper, we provide a security analysis of the Full-State Keyed Sponge (FKS), Full-State Keyed Duplex (FKD) and Keyak, one of the third-round CAESAR candidates, in the classic setting and the quantum model, respectively. In the classic setting, we present an universal forgery attack that can be implemented in $O(2^{c/2})$ queries, where c is the capacity.
In the quantum model, by utilizing the Simon's algorithm, we propose an efficient universal forgery attack to FKS, FKD and Keyak with complexity of $O(c)$. Moreover, we also propose an efficient key recovery attack that can be implemented in $O(c)$. Such attacks show that FKS, FKD and Keyak is completely broken in the quantum model.

Keywords: CAESAR, FKS, FKD, Keyak, Universal forgery, Key recovery, Quantum model.

1 Introduction

Authenticated encryption (AE) or authenticated encryption with associated data (AEAD) is a cryptographic primitive [ae]. AE's encryption scheme simultaneously provides confidentiality, integrity assurances on the processed messages, and its decryption is combined with data integrity verification.

CAESAR competition (Competition for Authenticated Encryption: Security, Applicability, and Robustness), announced in 2013, aims at fulfilling the needs of secure, efficient and robust authenticated encryption schemes. In total, 57 candidates were submitted to the competition. To process the associated data, a Message Authentication Code (MAC) [DK] must be employed in authenticated encryption. CAESAR candidates CLOC and SILC uses CBC-MAC [(re86,X9.86,I99] to authenticate the associated message [IMG$^+$]. The PMAC [BR02] type MACs are widely used in the CAESAR competition, such as OCB [KR11], AEZ [HKR15,HKR], COPA [ABL$^+$13], OTR [Min14], POET [AFF$^+$15,Nan14], OMD [CMN$^+$14], ELmD [DN], COLM [ABL$^+$], Deoxys [JNPS], and Minalpher [STA$^+$]. 10 of the 57 candidates are Sponge construction based, and there 4 candidates: Ascon [DEMS], Ketje [BDP$^+$d], Keyak [BDP$^+$e] and Norx [AJN], remain in the third round of CAESAR.

Post-quantum cryptography focuses on providing cryptographic primitives resisting quantum adversary, under the pressure of quantum computing maturation. In [KLLNP16], a general existential forgery attack to CBC-MAC variants,

PMAC variants MACs and authenticated encryptions with associated data was proposed, by utilizing the quantum period finding algorithm *Simon's* algorithm, the computational complexity is about $O(n)$ under the quantum computing setting which dramatically speeds up the classic setting of $O(2^{n/2})$ [PvO95]. Their attack really threats the security of such symmetric cryptosystems, such as authenticated encryption, however, we know that an existential forgery could not be easily used to launch meaningful message forgery, even universal forgery, since the message content can not be controlled by the attacker.

Based on the interesting property of that $a \oplus b = c \oplus d$ always implies $c \oplus b = a \oplus d$, where a, b, c, d are variables, for the $\oplus$ operation, Liu and Liu successfully transformed an existential forgery using birthday attack to an universal one by embedding the given messages in the 2-block colliding messages with the complexity unchanged, for the iterated blockcipher-based MACs and AEs [LLb]. For example, to forge the corresponding PMAC [MT06] tag τ for any given 2-block message $x||y$, the 2-block collision strategy is employed. The first block message is fixed with the given message x and the second message y_i is randomly chosen, in the first group G_1. And the second message is fixed with the given y and the first message x_j is randomly chosen, in the second group G_2. With complexity of $2^{n/2}$, there should exist a colliding pair $(x||y_i, x_j||y)$ satisfying $\tau_i = \text{PMAC}_K(x||y_i) = \tau_j = \text{PMAC}_K(x_j||y)$ for some i, j, by the generic birthday attack with two groups. Finally, it is true that $\text{PMAC}_K(x||y) = \text{PMAC}_K(x_j||y_i)$, which means that the very tag τ for the given 2-block message $x||y$ can be learned by querying $\text{PMAC}_K(x_j||y_i)$, and the universal forgery attack succeeds. However, this attack is not applicable with *Simon's* algorithm in the quantum model, since no period guarantee of messages is provided.

By exploiting the inner structure of the messages using the XOR operation, they also proposed another some generic universal forgery attacks, with complexity of $O(2^{n/2})$ in the classic setting. Fortunately, with fixed but unknown difference or period of the messages, such universal forgery attacks can be implemented with complexity about $O(n)$ by utilizing *Simon's* algorithm in the quantum model, which means that such schemes are completely broken in the quantum model [LLb].

Their attacks can be applied to CBC-MAC, XCBC [BR05], EMAC [PR00], TMAC [KI03], OMAC [IK03], CMAC [fBCMoO05], PC-MAC [MT06], MT-MAC [MT06], XOR-MAC [BRR95], PMAC, PMAC with parity [Yas12], LightMAC [LPTY16] and some of their variants. Moreover, such attacks are also applicable to the authenticated encryptions of the third round CAESAR candidates: CLOC, SILC, OCB, AEZ, OTR, COLM (including COPA and ELmD) and Deoxys [LLb].

However, whether such attacks can be applied to Sponge construction based MAC or AE is still an open problem, until this paper.

Since its introduction, the Sponge construction has been widely deployed, not only in hash function, like SHA-3 standard Keccak [BDP+i,BDP+c], but also MAC [BDP+f,BDP+g], AE [BDP+g,BDP+a] and et al. [BDP+h,Per].

However, the classic Sponge construction is a sequential application of a permutation p, and how to improve its efficiency is a challenging problem. To mostly improve the efficiency of classic Sponge construction based MAC and AE, the full-state keyed Sponge (FKS) and full-state keyed Duplex (FKD) with *full-state absorption*, the most efficient usage of the underlying permutation, was proposed [MRV15]. The full-state absorption differs from the classic construction in that it accepts input blocks as large as the width of the permutation (after padding) b-bit, instead of only the outer part r-bit. The generic security of the FKS and FKD is proved to be quite close to that of the classic keyed Sponge/Duplex construction [MRV15].

Keyak, a CAESAR candidate of the third round, is a direct application of the FKD construction. Keyak is proved to be secure in the classic setting [BDP$^+$e].

In [Unr], the post-quantum security of the Sponge construction was considered. The conclusion of that the Sponge construction is collapsing (and in consequence quantum collision-resistant), which means secure in the quantum model, under suitable assumption about the underlying block function was derived. In particular, if the block function is a random function or a (non-invertible) random permutation, the Sponge construction is collapsing.

We wonder if universal forgery attacks in [LLb] are applicable to FKS, FKD and eventually the CAESAR candidate Keyak, both in the classic setting and in the quantum model.

Our contributions: In the classic setting, we propose a kind of universal forgery attack, applicable to FKS, FKD and Keyak, that can be implemented in about $O(2^{c/2})$ queries, where c is the capacity. Our attacks show that *full-state absorption* eventually decrease the security of the classic Sponge and Duplex constructions in the classic setting.

In the quantum model, by utilizing the *Simon's* algorithm, we propose an efficient universal forgery attack to FKS, FKD and Keyak with complexity of $O(c)$. Moreover, we also propose an efficient key recovery attack that can be implemented in $O(c)$. Such attacks show that FKS, FKD and Keyak is completely broken in the quantum model.

However, we note that such attacks can not be applied to the classic Sponge and Duplex constructions, since a 2-block full collision is not directly available, which is crucial to such attacks.

Organization of the Paper. The rest of this paper is organized as follows. We introduce some preliminaries in section 2. In section 3, we present universal forgery attacks to FKS, FKD and Keyak, with complexity of about $O(2^{c/2})$, in the classic setting. We show how to employ universal forgery attack and key recovery attack in the quantum model with complexity of $O(c)$ in section 4. We summarize this paper in the last section.

2 Preliminaries

2.1 Full-State Keyed Sponge and Duplex Construction

The classic Sponge construction consists of a sequential application of a permutation p on a state of b-bit [BDP+j], which is consisted of an r-bit outer part and a c-bit inner part. In the absorption phase, message blocks of size r bits are absorbed and the state is transformed using p, while in the squeezing phase, digests are extracted from the outer part r bits at a time. The security of Sponge construction is proven to be $O(2^{c/2})$.

To mostly improve the efficiency of classic Sponge construction based message authentication code (MAC) and authenticated encryption (AE), the full-state keyed Sponge (FKS) and full-state keyed Duplex (FKD) with *full-state absorption*, the most efficient usage of the underlying permutation, is proposed [MRV15]. The full-state absorption differs from the classic construction in that it accepts input blocks as large as the width of the permutation (after padding) b-bit, instead of only the outer part r-bit. The generic security of the FKS and FKD is proved to be quite close to that of the classic keyed Sponge/Duplex construction [MRV15] of $O(2^{c/2})$.

Full-state Keyed Sponge (FKS) construction also uses a public permutation $p : \{0,1\}^b \rightarrow \{0,1\}^b$, and length parameters r, k, where $r \leq b$ and $k \leq (c = b-r)$. FKS takes a key $K \in \{0,1\}^k$, a message $M \in \{0,1\}^*$, and a natural number z, as input and outputs a string $Z \in \{0,1\}^z$:

$$\mathrm{FKS}^p(K, M, z) = FKS^p_K(M, z) = Z.$$

FKS computes on a state $s \in \{0,1\}^b$, initialized using a key K. The message M is first padded to be multiples of b bits, by using $\mathrm{pad}_b(M) = M||10^{b-1-|M| \bmod b}$, then $\mathrm{pad}_b(M)$ is further divided into b-bit blocks. These blocks are sequentially absorbed with the permutation. After that, the z-bit output is obtained through the squeezing phase. The process of FKS is shown in Fig. 1.

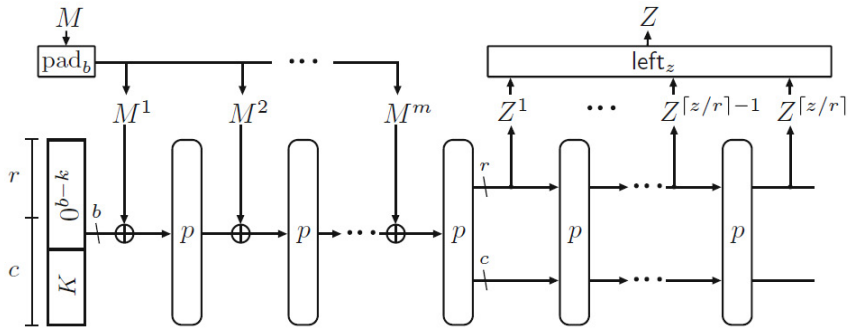

Fig. 1. The FKS construction [MRV15]

FKD is a generalization of the Duplex [BDP+b,BDP+a], and its parameters are similar to FKS. However, unlike FKS, FKD consists of two parts: initialization and duplexing. The initialization updates the state 0^b to be $0^{b-k}||K$ with a key K, but outputs nothing. The duplexing takes as input a message $M \in \{0,1\}^{<b}$ and $z \leq r$, and outputs a string $z \in \{0,1\}^z$. The process of FKD is shown in Fig. 2.

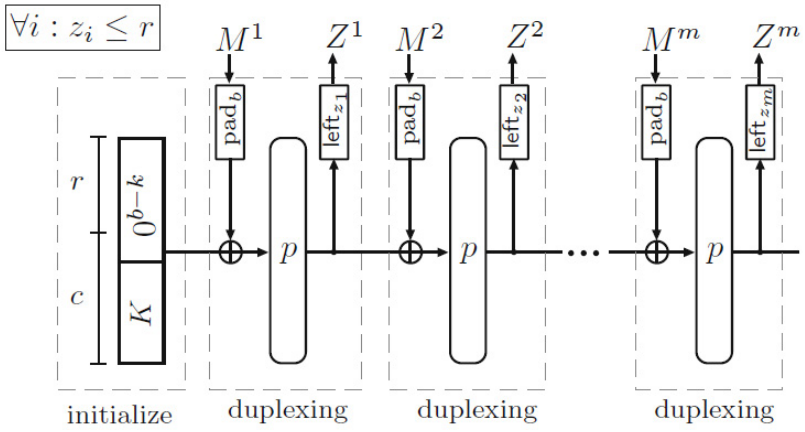

Fig. 2. The FKD construction [MRV15]

We point out that in the original FKS and FKD, the key length $k \leq c$, however, we assume the key is b-bit for simplicity in the following cryptanalysis.

2.2 CAESAR Candidate Keyak

Now, there are 15 candidates remain in the third round of CAESAR competition, Keyak is one of them. Keyak is a parameterized permutation-based authenticated encryption scheme with support for associated data and sessions. Keyak is based on the Motorist mode for authenticated encryption, and applies the FKD construction to improve the efficiency of message processing. The mode Motorist is Sponge-based and supports one or more Duplex instances operating in parallel. It makes duplexing calls with input containing key, nonce, plaintext and metadata bits and uses its output as tag or as key stream bits. The underlying permutation of Keyak is Keyak-p [BDP+e].

The FKD of Keyak calls a b-bit permutation p and operates on a b-bit state, initialized with the concatenation of a secret key K and a string δ_0 with $|K| + |\delta_0| = b$. After initialization, FKD supports duplexing calls, each one taking a b-bit input block δ_i and returning an r-bit output block Z_i [BDP+e].

The FKD applied in Keyak is shown in Fig. 3.

The claimed security strength of integrity for Keyak is $\min(c/2, |K|, |T|)$, it is also claimed that nonce violation (or reuse) and release of unverified decrypted

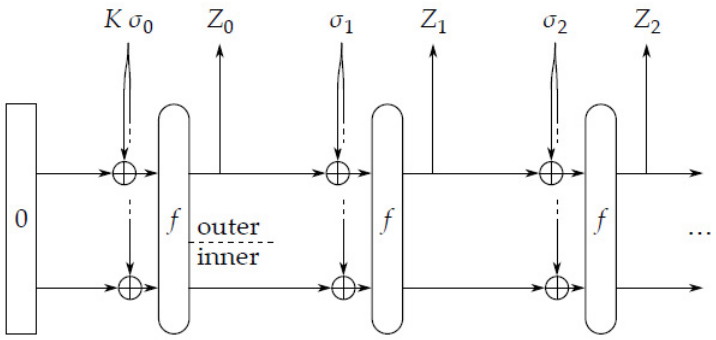

Fig. 3. The full-state keyed duplex construction applied in Keyak [BDP+e]

ciphertext have no consequences for integrity and do not put the key in danger for Keyak [BDP+e].

2.3 Collision Searching in the Quantum Model

***Simon's* Problem and Algorithm** *Simon's* problem says that: Given a boolean function $F : \{0,1\}^n \to \{0,1\}^n$ and the promise that there exists $s \in \{0,1\}^n$ such that for any $(x, y) \in \{0,1\}^n$, $[F(x) = F(y)] \Leftrightarrow [x \oplus y \in \{0^n, s\}]$, the goal is to find s [Sim97].

This problem can be solved by searching for collision in the classic setting, where the input messages have a fixed but unknown difference, with complexity about $O(2^{n/2})$. However, this problem can be solved by *Simon's* algorithm with quantum complexity of $O(n)$ in the quantum model, which dramatically speed up the process.

The original formulation of *Simon's* algorithm is for functions whose collisions happen only at some hidden period, which also means a fixed but unknown difference. In [KLLNP16], the authors extended it to functions that have more collisions, which immediately leads to a better analysis of previous applications of *Simon's* algorithm in the quantum model.

Application of *Simon's* algorithm, [KLLNP16]. The strategy is that: exhibit a new function F for the encryption oracle $E_K : \{0,1\}^n \to \{0,1\}^n$, that satisfies *Simon's* promise with two additional properties. First, The adversary can access the E_K in the quantum model, which means that he can query function F in superposition. Second, once the attacker get the information of s, it is sufficient to break the cryptographic scheme. In particular, the value s will usually be the difference in the internal state after processing a fixed pair of messages (α_0, α_1), i.e. $s = E_K(\alpha_0) \oplus E_K(\alpha_1)$. The input of F will be inserted into the state with the difference s so that $F(x) = F(x \oplus s)$ [LLb].

For simplicity, we keep in mind that if the colliding input messages have fixed but unknown difference s, the complexity to find such a difference is about $O(2^{n/2})$ in the classic setting, and about $O(n)$ in the quantum model, respec-

tively. If find such a difference is critical for the cryptographic scheme, then it immediately means broken in the quantum model.

3 Universal Forgery Attacks in the Classic Setting

3.1 Universal Forgery Attack to FKS in the Classic Setting

For a full colliding message pair (X, X') in FKS, we know that $\mathrm{FKS}_K(X) = \mathrm{FKS}_K(X')$, where the key K is embedded in the first state. We point out that $f_1(x) = p(K \oplus x)$ and $f_2(x) = x$ for the first two message blocks in FKS. If message length $l \geq 2$, we can fix the rest of messages as constant, for simplicity. In this attack, we need to first compute the difference of the second messages using the first fixed 1-block messages.

In the following, we show how to use a generic birthday attack with two groups to implement an universal forgery attack for any given message $x_1||x_2|| \cdots ||x_l$, where $l \geq 2$.

First, randomly generate $t = \lceil c/r \rceil$ b-bit messages named $\gamma_{3,4,\cdots,t+1}$, if $t > 1$.

Randomly generate $x_1' \neq x_1$. We also assume that x_1 and x_1' are already padded 1-block messages.

Query x_1 and x_1' to the oracle, respectively, get the value of $\mathrm{left}_r(Z(x_1))$ and $\mathrm{left}_r(Z(x_1'))$, from which the difference $\Delta_r = \mathrm{left}_r(Z(x_1)) \oplus \mathrm{left}_r(Z(x_1'))$ is computed.

Randomly generate $2^{c/2}$ 1-block messages x_2^i whose first r bits set to be Δ_r in group G_1, where $i \leq 2^{c/2}$, and query $x_1||x_2^i, \cdots, x_1||x_2^i||\gamma_{3,4,\cdots,t+1}$ to the oracle, there will be $t \times 2^{c/2}$ of corresponding results $\tau_i^t = \mathrm{FKS}_K(x_1||x_2^i||\gamma_{3,4,\cdots,t+1})$ returned in G_1, if $t > 1$.

Randomly generate $2^{c/2}$ message blocks x_2^j whose first r bits set to be 0^r in group G_2, where $j \leq 2^{c/2}$, and query $x_1'||x_2^j, \cdots, x_1||x_2^j||\gamma_{3,4,\cdots,t+1}$ to the oracle, there will be $t \times 2^{c/2}$ of corresponding results $\tau_j^t = \mathrm{FKS}_K(x_1'||x_2^j||\gamma_{3,4,\cdots,t+1})$ returned in G_2, if $t > 1$.

There should exist $\tau_i^t = \tau_j^t$ for some i, j with high probability, by the birthday paradox. So, we will get the key information that $p(K \oplus x_1) \oplus x_2^i = p(K \oplus x_1') \oplus x_2^j$, which means $\Delta = p(K \oplus x_1') \oplus p(K \oplus x_1) = x_2^j \oplus x_2^i$.

Query the message $x_1'||x_2 \oplus \Delta||x_3|| \cdots ||x_l$ to the oracle, a corresponding tag τ will be returned.

We note that the tag τ is also valid for the given message $x_1||x_2|| \cdots ||x_l$ with probability 1, which is never queried by the adversary to the oracle. The universal forgery attack succeeds with complexity of $O(2^{c/2})$.

3.2 Universal Forgery Attack to FKD and Keyak in the Classic Setting

In this attack, we first compute the difference of the second messages using the first fixed 1-block messages, as in FKS.

In the following, we show how to use a generic birthday attack with two groups to implement an universal forgery attack for any given message $x_1||x_2||\cdots||x_l$, where $l \geq 2$ and x_i are already padded messages. We recall that $f_1(x) = p(K \oplus x)$ and $f_2(x) = x$.

First, randomly generate $t = \lceil c/r \rceil$ b-bit messages named $\gamma_{3,4,\cdots,t+1}$, if $t > 1$.

Randomly generate $x_1' \neq x_1$.

Query x_1 and x_1' to the oracle, respectively, get the value of $\text{left}_r(Z(x_1))$ and $\text{left}_r(Z(x_1'))$, from which the difference $\Delta_r = \text{left}_r(Z(x_1)) \oplus \text{left}_r(Z(x_1'))$ is computed.

Randomly generate $2^{c/2}$ 1-block messages x_2^i whose first r bits set to be Δ_r in group G_1, where $i \leq 2^{c/2}$, and query $x_1||x_2^i||\gamma_{3,4,\cdots,t+1}$ to the oracle, there will be $2^{c/2}$ of corresponding results $\tau_i = \text{FKD}_K(x_1||x_2^i||\gamma_{3,4,\cdots,t+1})$ returned in G_1, if $t > 1$.

Randomly generate $2^{c/2}$ message blocks x_2^j whose first r bits set to be 0^r in group G_2, where $j \leq 2^{c/2}$, and query $x_1'||x_2^j||\gamma_{3,4,\cdots,t+1}$ to the oracle, there will be $2^{c/2}$ of corresponding results $\tau_j = \text{FKD}_K(x_1'||x_2^j||\gamma_{3,4,\cdots,t+1})$ returned in G_2, if $t > 1$.

There should exist $\tau_i = \tau_j$ for some i, j with high probability, by the birthday paradox. So, we will get the key information that $p(K \oplus x_1) \oplus x_2^i = p(K \oplus x_1') \oplus x_2^j$, which means $\Delta = p(K \oplus x_1') \oplus p(K \oplus x_1) = x_2^j \oplus x_2^i$.

Query the message $x_1'||x_2 \oplus \Delta||x_3||\cdots||x_l$ to the oracle, a corresponding tag τ will be returned.

We note that the result τ [1] is also valid for the given message $x_1||x_2||x_3||\cdots||x_l$ with probability 1, which is never queried by the adversary to the oracle FKD. The universal forgery attack succeeds with complexity of $O(2^{c/2})$.

Since Keyak is a direct application of FKD, this universal forgery attack is also applicable to Keyak in the classic setting.

4 Universal Forgery and Key Recovery Attacks in the Quantum Model

4.1 Universal Forgery Attack to FKS in the Quantum Model

We can build a powerful universal forgery attack on FKS with very low complexity using superposition queries in the quantum model. To forge the tag for the given message $M_1||M_2||\cdots||M_l$, we should first fix two message blocks α_0, α_1, with $\alpha_0 \neq \alpha_1$, more precisely, we fix $\alpha_0 = M_1$ and randomly generate α_1. Finally, we define the function F as follow.

$$F : \{0,1\} \times \{0,1\}^b \to \{0,1\}^b$$
$$d, x \longmapsto \text{FKS}(\alpha_d||x) = \text{left}_b(p^{\lceil b/z \rceil}(p(p(K \oplus \alpha_d) \oplus x) \oplus \mu))$$

[1] We should replace the first $z1$-bit output with the known value of $\text{left}_{z1}(p(K \oplus x_1))$, also known as Z^1 in the Fig. 2.

We note that in order to get b bits output, F must be iterated $\lceil b/z \rceil$ times by further appending the constant μ as input each time.

The function F can be computed with a single call to the FKS oracle, and F satisfies the promise of *Simon's* problem with $s = 1||p(K \oplus \alpha_0) \oplus p(K \oplus \alpha_1)$.

$$\begin{aligned} F(0,x) &= \mathrm{left}_b(p^{\lceil b/z \rceil}(p(p(K \oplus \alpha_1) \oplus x) \oplus \mu)), \\ F(1,x) &= \mathrm{left}_b(p^{\lceil b/z \rceil}(p(p(K \oplus \alpha_0) \oplus x) \oplus \mu)), \\ F(d,x) &= F(d \oplus 1, x \oplus p(K \oplus \alpha_0) \oplus p(K \oplus \alpha_1)) \end{aligned}$$

Therefore, we have:

$$\begin{aligned} F(d',x') = F(d,x) &\Leftrightarrow x \oplus p(K \oplus \alpha_d) = x' \oplus p(K \oplus \alpha_{d'}) \\ &\Leftrightarrow \begin{cases} x \oplus x' = 0 & \text{if } d' = d \\ x' \oplus x = p(K \oplus \alpha_0) \oplus p(K \oplus \alpha_1) & \text{if } d' \neq d \end{cases} \end{aligned}$$

Finally, we know that the application of *Simon's* algorithm will return the "difference" $p(K \oplus \alpha_0) \oplus p(K \oplus \alpha_1)$, which will leads to the following universal forgery easily:

1. Query the tag of $\alpha_1||M_2 \oplus p(K \oplus \alpha_0) \oplus p(K \oplus \alpha_1)|| \cdots ||M_l$;
2. The same tag is also valid for the given message $M_1||M_2|| \cdots ||M_l$.

Therefore, the FKS is broken by a quantum universal forgery attack with $O(b)$.

Moreover, the complexity can be optimized to $O(c)$, by utilizing the strategy of controlling the outer part r bits, as used in the attack of FKS in the classic setting. Once the outer part are fixed to be the same, the full collision is directly deduced by the inner collision of the inner part. Hence, the function F can be further defined in the following.

$$\begin{aligned} F : \{0,1\} \times \{0,1\}^c &\to \{0,1\}^c \\ d, x &\longmapsto \mathrm{FKS}(\alpha_d||x) = \mathrm{left}_c(p^{\lceil c/r \rceil}(p(p(K \oplus \alpha_d) \oplus x) \oplus \mu)) \end{aligned}$$

where the first r bits of x is fixed.

4.2 Key Recovery Attack to FKS in the Quantum Model

We can also build a powerful key recovery attack on FKS with very low complexity using superposition queries in the quantum model. To recover the secret key of the FKS used, we can simulate another FKS with the state initialized to 0^b, which means that such FKS is used as a pure hash function. Again, we should first fix two blocks α_0, α_1, with $\alpha_0 \neq \alpha_1$, however, we fix $\alpha_0 = 0^b$ and $\alpha_1 = K$. Here, we use the randomly generated message that $M_1' = M_1$. Finally, we define the function F as follow.

$$F : \{0,1\} \times \{0,1\}^b \to \{0,1\}^b$$
$$d, x \longmapsto \mathrm{FKS}(\alpha_d||x) = \mathrm{left}_b(p^{\lceil b/z \rceil}(p(p(M_1 \oplus \alpha_d) \oplus x) \oplus \mu))$$

The function F can be computed with a single call to the FKS oracle, and F satisfies the promise of *Simon's* problem with $s = 1||p(M_1 \oplus \alpha_0) \oplus p(M_1 \oplus \alpha_1)$.

$$\begin{aligned} F(0,x) &= \mathrm{left}_b(p^{\lceil b/z \rceil}(p(p(M_1 \oplus \alpha_1) \oplus x) \oplus \mu)), \\ F(1,x) &= \mathrm{left}_b(p^{\lceil b/z \rceil}(p(p(M_1 \oplus \alpha_0) \oplus x) \oplus \mu)), \\ F(d,x) &= F(d \oplus 1, x \oplus p(M_1 \oplus \alpha_0) \oplus p(M_1 \oplus \alpha_1)) \end{aligned}$$

Therefore, we have:

$$\begin{aligned} F(d',x') = F(d,x) &\Leftrightarrow x \oplus p(M_1 \oplus \alpha_d) = x' \oplus p(M_1 \oplus \alpha_{d'}) \\ &\Leftrightarrow \begin{cases} x \oplus x' = 0 & \text{if } d' = d \\ x' \oplus x = p(M_1 \oplus \alpha_0) \oplus p(M_1 \oplus \alpha_1) & \text{if } d' \neq d \end{cases} \end{aligned}$$

Finally, we know that the application of *Simon's* algorithm will return the "difference" $\Delta = p(M_1 \oplus \alpha_0) \oplus p(M_1 \oplus \alpha_1)$. Since we know the value of $\alpha_0 = 0^b$, which will leads to the following key recovery easily:

$$K = p^{-1}(\Delta \oplus p(M_1 \oplus \alpha_0)) \oplus M_1$$

Therefore, the FKS is broken by a quantum key recovery attack with complexity of $O(b)$.

Moreover, the complexity can be optimized to $O(c)$, by utilizing the strategy of controlling the outer part r bits to form inner collision. Hence, the function F can be further defined in the following.

$$F : \{0,1\} \times \{0,1\}^c \to \{0,1\}^c$$
$$d, x \longmapsto \mathrm{FKS}(\alpha_d||x) = \mathrm{left}_c(p^{\lceil c/r \rceil}(p(p(M_1 \oplus \alpha_d) \oplus x) \oplus \mu))$$

where the first r bits of x is fixed.

4.3 Universal Forgery Attack to FKD and Keyak in the Quantum Model

To forge the tag for the given message $M_1||M_2||\cdots||M_l$ in the quantum model. We fix $\alpha_0 = M_1$ and randomly generate α_1. Finally, we define the function F as follow.

$$F : \{0,1\} \times \{0,1\}^b \to \{0,1\}^b$$
$$d, x \longmapsto \mathrm{FKD}(\alpha_d||x) = \mathrm{left}_b(p^{\lceil b/r \rceil}(p(p(K \oplus \alpha_d) \oplus x) \oplus \mu))$$

where μ can be any non-zero constant, and $p^{\lceil b/r \rceil}$ means that the Duplex instantiation with input set to μ should be iterated $\lceil b/r \rceil$ times, to ensure the probability of the full collision to be 1.

The function F can be computed with a single call to the FKD oracle, and F satisfies the promise of *Simon's* problem with $s = 1||p(K \oplus \alpha_0) \oplus p(K \oplus \alpha_1)$.

As before, we know that the application of *Simon's* algorithm will return the "difference" $p(K \oplus \alpha_0) \oplus p(K \oplus \alpha_1)$, which will leads to the following universal forgery easily:

1. Query the tag of $\alpha_1||M_2 \oplus p(K \oplus \alpha_0) \oplus p(K \oplus \alpha_1)||\cdots||M_l$;
2. The same tags are also valid for the given message $M_1||M_2||\cdots||M_l$ [2].

Therefore, the FKD is broken by a quantum universal forgery attack with $O(b)$.

Moreover, the complexity can be optimized to $O(c)$, since in the Duplex instantiation the outer r bit is known to the adversary. Here, the values of the first r bits of used x can be fixed to any constant with the known difference of $\text{left}_{z_1} \oplus \text{left}_{z_1'}$ to make sure that the outer part after XORing are the same. Hence, the function can be further defined in the following.

$$F : \{0,1\} \times \{0,1\}^c \to \{0,1\}^c$$
$$d, x \longmapsto \text{FKD}(\alpha_d||x) = \text{left}_c(p^{\lceil c/r \rceil}(p(p(K \oplus \alpha_d) \oplus x) \oplus \mu))$$

where the first r bits of x is constant.

Since Keyak is a direct application of FKD, this universal forgery attack is also applicable to Keyak in the quantum model.

4.4 Key Recovery Attack to FKD and Keyak in the Quantum Model

To recover the secret key of the FKD used, we can simulate another FKD with the state initialized to 0^b, which means that such FKD is used as a pure hash function or pure public permutation. Again, we fix $\alpha_0 = 0^b$ and $\alpha_1 = K$. Here, we use the randomly generated message that $M_1' = M_1$. Finally, we define the function F as follow.

$$F : \{0,1\} \times \{0,1\}^b \to \{0,1\}^b$$
$$d, x \longmapsto \text{FKD}(\alpha_d||x) = \text{left}_b(p^{\lceil b/r \rceil}(p(p(M_1 \oplus \alpha_d) \oplus x) \oplus \mu))$$

where μ can be any non-zero constant, and $p^{\lceil b/r \rceil}$ means that the Duplex instantiation with input set to μ should be further iterated $t = \lceil b/r \rceil$ times, to ensure the probability of the full collision to be 1.

[2] Here, we point out that $\text{left}_{z1}(p(K \oplus \alpha_0))$ is already known, and from the left_{z2} to the last left_{zl} are the same.

The function F can be computed with a single call to the FKD oracle, and F satisfies the promise of *Simon's* problem with $s = 1||p(M_1 \oplus \alpha_0) \oplus p(M_1 \oplus \alpha_1)$.

As before, we know that the application of *Simon's* algorithm will return the "difference" $\Delta = p(M_1 \oplus \alpha_0) \oplus p(M_1 \oplus \alpha_1)$. Since we know the value of $\alpha_0 = 0^b$, which will leads to the following key recovery easily:

$$K = p^{-1}(\Delta \oplus p(M_1 \oplus \alpha_0)) \oplus M_1$$

Therefore, the FKD is broken by a quantum key recovery attack with complexity of $O(b)$.

Moreover, the attack complexity can be improved to be $O(c)$ after optimization like the universal forgery attack to FKD in the quantum model.

Since Keyak is a direct application of FKD, this key recovery attack is also applicable to Keyak in the quantum model.

5 Discussion and Conclusion

This paper discusses the security of FKS, FKD and Keyak in the classic setting and in the quantum model, respectively. Our attacks show that the application of "full-state absorption"eventually decrease the security of FKS and FKD constructions, both in the classic setting and in the quantum model, especially the latter one. How to improve the efficiency of Sponge and Duplex constructions is still an open problem.

However, our attacks are not applicable to the classic Sponge and Duplex constructions [LLa], since the core strategy of the attacks is a 2-block collision, which holds with probability 1 through the "full-state absorption", and the probability in classic Sponge and Duplex constructions is 2^{-c}, moreover, this kind of probability can not be further solved with *Simon's* algorithm.

We also note that the attack strategy using colliding pair $(x||y_i, x_j||y)$, where x, y are fixed, is not applicable to FKS, FKD, even for the classic Sponge and Duplex construction, with complexity of $O(2^{c/2})$. The outer parts will not be the same, since there are $2^{c/2}$ randomly generated x_j. However, such attack strategy can be directly applied with complexity of $O(2^{b/2})$.

Acknowledgments

This work was partially supported by Foundation of Science and Technology on Information Assurance Laboratory under Grant 6142112010202.

References

[ABL+] Elena Andreeva, Andrey Bogdanov, Atul Luykx, Bart Mennink, Elmar Tischhauser, and Kan Yasuda. Colm v1. caesar submission, september 2016.

[ABL+13] Elena Andreeva, Andrey Bogdanov, Atul Luykx, Bart Mennink, Elmar Tischhauser, and Kan Yasuda. *Parallelizable and Authenticated Online Ciphers*, pages 424–443. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[ae] Authenticated encryption. retrived april, 2017 https://en.wijipedia.org/wiki/authenticaed_encryption.

[AFF+15] Farzaneh Abed, Scott Fluhrer, Christian Forler, Eik List, Stefan Lucks, David McGrew, and Jakob Wenzel. *Pipelineable On-line Encryption*, pages 205–223. Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.

[AJN] Jean-Philippe Aumasson, Philipp Jovanovic, and Samuel Neves. Norx v3.0. caesar submission, september 2016.

[BDP+a] Guido Berton, Joan Daemen, Michael Peeters, Giles Van Assche, and Ronny Van Keer. Duplexing the sponge: single-pass authenticated encryption and other applications. in: Miri, a., vaudenay, s. (eds.) sac 2011. lncs, vol. 7118, pp. 320c337. springer, heidelberg (2012).

[BDP+b] Guido Berton, Joan Daemen, Michael Peeters, Giles Van Assche, and Ronny Van Keer. Duplexing the sponge: singlepass authenticated encryption and other applications. in: Iacr cryptology eprint archive 2011, vol. 499 (2011). http://eprint.iacr.org/2011/499.

[BDP+c] Guido Berton, Joan Daemen, Michael Peeters, Giles Van Assche, and Ronny Van Keer. Keccak specifications. in: Nist sha-3 submission (2008). http://keccak.noekeon.org/.

[BDP+d] Guido Berton, Joan Daemen, Michael Peeters, Giles Van Assche, and Ronny Van Keer. Ketje v2. caesar submission, september 2016.

[BDP+e] Guido Berton, Joan Daemen, Michael Peeters, Giles Van Assche, and Ronny Van Keer. Keyak v2. caesar submission, september 2016.

[BDP+f] Guido Berton, Joan Daemen, Michael Peeters, Giles Van Assche, and Ronny Van Keer. On the security of the keyed sponge construction. in: Symmetric key encryption workshop 2011 (2011).

[BDP+g] Guido Berton, Joan Daemen, Michael Peeters, Giles Van Assche, and Ronny Van Keer. Permutation-based encryption, authentication and authenticated encryption. in: Workshop records of diac 2012, pp. 159c170 (2012).

[BDP+h] Guido Berton, Joan Daemen, Michael Peeters, Giles Van Assche, and Ronny Van Keer. Sponge-based pseudorandom number generators. in: Mangard, s., standaert, f.-x. (eds.) ches 2010. lncs, vol. 6225, pp. 33c47. springer, heidelberg (2010).

[BDP+i] Guido Berton, Joan Daemen, Michael Peeters, Giles Van Assche, and Ronny Van Keer. Sponge functions. in: Ecrypt hash workshop (2007). http://csrc.nist.gov/groups/st/hash/documents/joandaemen.pdf.

[BDP+j] Guido Berton, Joan Daemen, Michael Peeters, Giles Van Assche, and Ronny Van Keer. Sponge functions. in: Ecrypt hash workshop (2007). http://csrc.nist.gov/groups/st/hash/documents/joandaemen.pdf.

[BR02] John Black and Phillip Rogaway. *A Block-Cipher Mode of Operation for Parallelizable Message Authentication*, pages 384–397. Springer Berlin Heidelberg, Berlin, Heidelberg, 2002.

[BR05] John Black and Phillip Rogaway. Cbc macs for arbitrary-length messages: The three-key constructions. *Journal of Cryptology*, 18(2):111–131, 2005.

[BRR95] Mihir Bellare, Guérin R., and Phillip Rogaway. *XOR MACs: new methods for message authentication using finite pseudorandom functions*, pages 15–28. Springer Berlin Heidelberg, Berlin, Heidelberg, 1995.

[CMN+14] Simon Cogliani, Diana-Ştefania MaimuŢ, David Naccache, Rodrigo Portella do Canto, Reza Reyhanitabar, Serge Vaudenay, and Damian Vizár. *OMD: A Compression Function Mode of Operation for Authenticated Encryption*, pages 112–128. Springer International Publishing, Cham, 2014.

[DEMS] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schlaer. Ascon v1.2. caesar submission, september 2016.

[DK] Hans Delfs and Helmut Knebl. *Introduction to Cryptography: Principles and Applications*.

[DN] Nilanjan Datta and Mridul Nandi. Elmd v2.0, submission to the caesar competition, august 2015.

[fBCMoO05] NIST. Recommendation for Block Cipher Modes of Operation. The cmac mode for authentication. *NIST Special Publication 800-38B*, 2005.

[HKR] Viet Tung Hoang, Ted Krovetz, and Phillip Rogaway. Aez v4.2: Authenticated encryption by enciphering. caesar submission, september 2016.

[HKR15] Viet Tung Hoang, Ted Krovetz, and Phillip Rogaway. *Robust Authenticated-Encryption AEZ and the Problem That It Solves*, pages 15–44. Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.

[IK03] Tetsu Iwata and Kaoru Kurosawa. *OMAC: One-Key CBC MAC*, pages 129–153. Springer Berlin Heidelberg, Berlin, Heidelberg, 2003.

[IMG+] Tetsu Iwata, Kazuhiko Minematsu, Jian Guo, Sumio Morioka, and Eita Kobayashi. Cloc and silc v3. caesar submission, september 2016.

[I99] Information technology Security techniques Message Authentication Codes (MACs) Part 1 ISO/IEC 9797C1. Mechanisms using a block cipher. *International Organization for Standardization, Genève, Switzerland*, 1999.

[JNPS] Jérémy Jean, Ivica Nikolić, Thomas Peyrin, and Yannick Seurin. Deoxys v1.41. caesar submission, september 2016.

[KI03] Kaoru Kurosawa and Tetsu Iwata. *TMAC: Two-Key CBC MAC*, pages 33–49. Springer Berlin Heidelberg, Berlin, Heidelberg, 2003.

[KLLNP16] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. *Breaking Symmetric Cryptosystems Using Quantum Period Finding*, pages 207–237. Springer Berlin Heidelberg, Berlin, Heidelberg, 2016.

[KR11] Ted Krovetz and Phillip Rogaway. *The Software Performance of Authenticated-Encryption Modes*, pages 306–327. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.

[LLa] Fanbao Liu and Fengmei Liu. Almost universal forgery: Application to ascon and more. *to appear*.

[LLb] Fanbao Liu and Fengmei Liu. Universal forgery with birthday paradox: Application to blockcipher-based message authentication codes and authenticated encryptions. *Cryptolgy ePrint Archive, Report 2017/653. 2017. http:/erpint.iacr.org*.

[LPTY16] Atul Luykx, Bart Preneel, Elmar Tischhauser, and Kan Yasuda. *A MAC Mode for Lightweight Block Ciphers*, pages 43–59. Springer Berlin Heidelberg, Berlin, Heidelberg, 2016.

[Min14] Kazuhiko Minematsu. *Parallelizable Rate-1 Authenticated Encryption from Pseudorandom Functions*, pages 275–292. Springer Berlin Heidelberg, Berlin, Heidelberg, 2014.

[MRV15] Bart Mennink, Reza Reyhanitabar, and Damian Vizár. *Security of Full-State Keyed Sponge and Duplex: Applications to Authenticated Encryption*, pages 465–490. Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.

[MT06] Kazuhiko Minematsu and Yukiyasu Tsunoo. Provably secure macs from differentially-uniform permutations and aes-based implementations. *FSE 2006. LNCS 4047*, pages 226–241, 2006.

[Nan14] Mridul Nandi. *Forging Attacks on Two Authenticated Encryption Schemes COBRA and POET*, pages 126–140. Springer Berlin Heidelberg, Berlin, Heidelberg, 2014.

[Per] R. Perlner. Extendable-output functions (xofs). in: Nist sha-3 2014 workshop (2014). http://csrc.nist.gov/groups/st/hash/sha-3/aug2014/documents/perlner_xofs.pdf.

[PR00] Erez Petrank and Charles Rackoff. Cbc mac for real-time data sources. *Journal of Cryptology*, 13(3):315–338, 2000.

[PvO95] Bart Preneel and Paul C. van Oorschot. *MDx-MAC and Building Fast MACs from Hash Functions*, pages 1–14. Springer Berlin Heidelberg, Berlin, Heidelberg, 1995.

[(re86] ANSI X9.9 (revised). Financial institution messages authentication (wholesale), american bankers association. 1986.

[Sim97] D.R. Simon. On the power of quantum computation. *SIAM J. Comput*, 26(5):1474–1483, 1997.

[STA+] Yu Sasaki, Yosuke Todo, Kazumaro Aoki, Yusuke Naito, Takeshi Sugawara, Yumiko Murakami, Mitsuru Matsui, and Shoichi Hirose. Minalpher v1.1. caesar submission, august 2015.

[Unr] Dominique Unruh. Collapsing sponges: Post-quantum security of the sponge construction. *Cryptolgy ePrint Archive, Report 2017/xxx. 2017. http:/erpint.iacr.org.*

[X9.86] ANSI X9.19. Financial institution retail messages authentication, american bankers association. 1986.

[Yas12] Kan Yasuda. *PMAC with Parity: Minimizing the Query-Length Influence*, pages 203–214. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.