Breaking Tweakable Enciphering Schemes using Simon's Algorithm

Sebati Ghosh and Palash Sarkar
Indian Statistical Institute
203, B.T.Road, Kolkata, India - 700108.
{sebati_r,palash}@isical.ac.in

June 14, 2019

Abstract

The threat of the possible advent of quantum computers has motivated the cryptographic community to search for quantum safe solutions. There have been some works in past few years showing the vulnerability of symmetric key crypto-systems in the quantum setting. Among these the works by Kuwakado et al. and Kaplan et al. use the quantum period finding procedure called Simon's algorithm to attack several symmetric crypto-systems.

In this work, we use Simon's algorithm to break six tweakable enciphering schemes (TESs) in the quantum setting. These are CMC, EME, XCB, TET, AEZ and FAST. All of them have usual proofs of security in the classical sense. A version of EME and a version of XCB are IEEE standardised TESs.

Keywords: TES, Simon's algorithm, Quantum period finding algorithm.

1 Introduction

Tweakable Enciphering scheme (TES) is an important notion in cryptography. It is mainly known for its use in disk encryption algorithms. But, the full functionality of a TES is broader than disk encryption. The notion of a TES was first formalised by Halevi and Rogaway [3]. This security of a TES is in the sense of being indistinguishable from an ideal tweakble SPRP. There are several proposals of TESs in the literature of classical cryptography.

In the classical setting the adversary is given only classical access to the corresponding oracles, i.e. all the oracle queries and other computations are classical. But in the quantum setting we consider adversaries with quantum access to the oracles and quantum computation power. Quantum oracle access means querying an oracle in quantum superposition of different states. In this setting, Simon's algorithm [1] can be used to find the period of the function, implemented by the oracle.

As can be seen in this work, some important TESs, which are provably secure in the classical setting, are broken in the quantum setting. Surprisingly enough these TESs contain a lot of structures within them which make them vulnerable to Simon's algorithm.

Our Contributions

In this work we have considered six important TESs, viz. CMC, EME (EME2), XCB, TET, AEZ and FAST in the post-quantum setting. All of these schemes are provably secure in the classical setting. EME2 and a version of XCB are IEEE standards as TES. Here we have considered these

standardised versions also. CMC is the first proposed TES. AEZ is a recent proposal, which has received a fair amount of attention as part of the CAESAR competition.

For each of the six TESs we have been able to define a Simon's function, i.e. a function having a non-zero period, exploiting the underlying structure of the TES. Given a superposition access to the TES, it is possible to built a circuit implementing Simon's function providing superposition access. This is discussed in more detail in [2]. This non-zero period can be retrieved with high probability by using Simon's algorithm. On the other hand, Simon's algorithm applied to the same function built from an ideal tweakable SPRP is very unlikely to output a non-zero value. Thus, with high probability each of these TESs can be distinguished from an ideal tweakable SPRP, proving their vulnerability in the quantum setting. This is the main finding of the present work.

For each of the schemes, along with defining the Simon's function, a detailed calculation has been provided to show that the claimed quantity is indeed the period of the function. In some of the cases, along with the distinguisher, some crucial information about the scheme, eg. the hash key or some encryption key, is also revealed by the attack.

2 Quantum Attacks on TESs

2.1 Application to the CMC construction

In 2003, Halevi and Rogaway formalised [3] the notion of a tweakable enciphering scheme. This paper also described a TES called CMC which is based on the CBC mode of operation. As a result it is sequential in nature.

In the following, we define a Simon function from CMC and give a quantum period finding attack on this function, which gives a distinguisher of CMC from an ideal tweakable SPRP. Our attack considers messages with three blocks. Let the message be $x_1||x_2||x_3$. We refer the reader to Figure 1 of [3] for the encryption algorithm. We use T' in place of $\mathbb{T}$ used in this original description. All other notation are unchanged.

Fix arbitrary $K, \tilde{K} \in \mathcal{K}$; $T, m, \alpha_0, \alpha_1 \in \{0,1\}^n$, such that $\alpha_0 \neq \alpha_1$; let b denote a bit and we define the following function:

$$\begin{aligned} f : \{0,1\} \times \{0,1\}^n &\rightarrow \{0,1\}^n \\ (b, x) &\overset{f}{\mapsto} c_1, \text{ where } c_1||c_2||c_3 \longleftarrow \mathsf{CMC}[E]^T_{K,\tilde{K}}(m||\alpha_b||x). \end{aligned}$$

In the following discussion, we observe, $f(b,x) = f(b',x') \Leftrightarrow x \oplus x' = E_K(E_K(m \oplus T') \oplus \alpha_b) \oplus E_K(E_K(m \oplus T') \oplus \alpha_{b'})$.

For the input $m||\alpha_0||x$, we have,

$$\begin{aligned} PPP_1 &= E_K(m \oplus T'); \\ PPP_2 &= E_K(\alpha_0 \oplus E_K(m \oplus T')); \\ PPP_3 &= E_K(x \oplus E_K(\alpha_0 \oplus E_K(m \oplus T'))); \\ M &= 2(PPP_1 \oplus PPP_3); \\ CCC_1 &= PPP_3 \oplus M; \\ C_1 &= E_K(CCC_1) \oplus T'; \end{aligned} \tag{1}$$

For the input $m||\alpha_1||x \oplus s$, where $s = E_K(E_K(m \oplus T') \oplus \alpha_0) \oplus E_K(E_K(m \oplus T') \oplus \alpha_1)$ we have,

$$\begin{aligned}
PPP_1 &= E_K(m \oplus T'); \\
PPP_2 &= E_K(\alpha_1 \oplus E_K(m \oplus T')); \\
PPP_3 &= E_K(x \oplus s \oplus E_K(\alpha_1 \oplus E_K(m \oplus T'))); \\
&= E_K(x \oplus E_K(E_K(m \oplus T') \oplus \alpha_0) \oplus E_K(E_K(m \oplus T') \oplus \alpha_1) \oplus E_K(\alpha_1 \oplus E_K(m \oplus T'))) \\
&= E_K(x \oplus E_K(E_K(m \oplus T') \oplus \alpha_0); \\
M &= 2(PPP_1 \oplus PPP_3); \\
CCC_1 &= PPP_3 \oplus M; \\
C_1 &= E_K(CCC_1) \oplus T';
\end{aligned} \tag{2}$$

For the above inputs PPP_1s and PPP_3s are same, implying C_1s are same. It establishes that $1||E_K(E_K(m \oplus T') \oplus \alpha_0) \oplus E_K(E_K(m \oplus T') \oplus \alpha_1)$ is a period for the function f. Given a superposition access to an oracle for CMC, a circuit implementing f can be built and by using Simon's algorithm, with high probability we get this non-zero period for this function. But in case of an ideal tweakable SPRP construction with high probability Simon's algorithm outputs zero. This gives a distinguisher rendering CMC a quantum insecure TES.

2.2 Application to the EME construction

EME [4] is a well known TES construction proposed by Halevi and Rogaway. It is a parallelisable mode of operation of a block cipher. EME was extended to handle arbitrary length messages by Halevi [5] and the resulting scheme was called EME*. EME* has been standardised as a TES by IEEE [8] in the name EME2.

Our attack considers messages with three blocks. For this message length the constructions EME and EME2 are identical, with only the minor replacement of the tweak by a function of the tweak in the latter. Hence, we will describe the attack in the context of EME only.

Let the message be $x_1||x_2||x_3$. We refer the reader to Figure 1 of [4] for the encryption algorithm.

Fix arbitrary $K \in \mathcal{K}$; $T, m \in \{0,1\}^n$ and we define the following function:

$$\begin{aligned}
f : \{0,1\}^n &\rightarrow \{0,1\}^n \\
x &\overset{f}{\mapsto} c_1, \text{ where } c_1||c_2||c_3 \longleftarrow \mathsf{EME}[E]_K^T(m||x||x).
\end{aligned}$$

This function satisfies $f(x) = f(x \oplus s)$, with $s = 6L$. Consider the two inputs $m||x||x$ and $m||x \oplus 6L||x \oplus 6L$ for any $x \in \{0,1\}^n$.
For the input $m||x||x$, we have,

$$\begin{aligned}
MP &= E_K(m \oplus L) \oplus E_K(x \oplus 2L) \oplus E_K(x \oplus 4L) \oplus T; \\
MC &= E_K(MP); \\
M &= MP \oplus MC; \\
SC &= E_K(x \oplus 2L) \oplus 2M \oplus E_K(x \oplus 4L) \oplus 4M; \\
C_1 &= E_K(MC \oplus SC \oplus T) \oplus L; \\
C_2 &= E_K(E_K(x \oplus 2L) \oplus 2M) \oplus 2L; \\
C_3 &= E_K(E_K(x \oplus 4L) \oplus 4M) \oplus 4L;
\end{aligned} \tag{3}$$

For the input $m||x \oplus 6L||x \oplus 6L$, we have,

$$\begin{aligned} MP &= E_K(m \oplus L) \oplus E_K(x \oplus 2L) \oplus E_K(x \oplus 4L) \oplus T; \\ MC &= E_K(MP); \\ M &= MP \oplus MC; \\ SC &= E_K(x \oplus 2L) \oplus 2M \oplus E_K(x \oplus 4L) \oplus 4M; \\ C_1 &= E_K(MC \oplus SC \oplus T) \oplus L; \\ C_2 &= E_K(E_K(x \oplus 4L) \oplus 2M) \oplus 2L; \\ C_3 &= E_K(E_K(x \oplus 2L) \oplus 4M) \oplus 4L; \end{aligned} \tag{4}$$

From above we see that for both the inputs, MP, MC, M and SC are equal and hence C_1s are equal. Given a superposition access to an oracle for EME, a circuit implementing f can be built. By using Simon's algorithm, with high probability we get this non-zero period $6L$ for this function when the underlying construction is EME, whereas in case of an ideal tweakable SPRP construction this is not the case. This gives a distinguisher rendering EME quantum insecure.

2.3 Application to the XCB construction

Construction of a TES using a counter based mode of operation of a block cipher and a Horner type hash function was first proposed by McGrew and Fluhrer [6]. This scheme was called XCB. A later variant [7] of this scheme was proposed to improve efficiency and reduce key size. This version was later standardised as a TES by IEEE [8].

In the following we describe the quantum attack on the standardised version [7] in full detail. There are some differences between this attack and the attack on the previous version [6]. We mention the attack on this previous version briefly.

Both the attacks considers messages with three blocks. Let the message be $x_1||x_2||x_3$. We refer the reader to Algorithm 1 of [7] for the encryption algorithm.

Fix arbitrary $K \in \{0,1\}^k$; $m, \alpha_0, \alpha_1 \in \{0,1\}^n$, such that $\alpha_0 \neq \alpha_1$; let the associated data $Z = \varepsilon$, i.e. an empty string; let b denote a bit. For the standardised version [7], we define the following Simon's function.

$$\begin{aligned} f : \{0,1\} \times \{0,1\}^n &\rightarrow \{0,1\}^n \\ (b, x) &\overset{f}{\mapsto} c_3, \text{ where } c_1||c_2||c_3 \longleftarrow \mathsf{XCB}_K(\varepsilon, \alpha_b||x||m). \end{aligned}$$

In the following discussion we observe, $f(b,x) = f(b',x') \Leftrightarrow x \oplus x' = \alpha_b H \oplus \alpha_{b'} H$.

For the input $\alpha_0||x||m$,

$$\begin{aligned} A &= m; \\ B &= \alpha_0||x; \\ C &= \mathbf{e}(K_e, m); \\ D &= \mathbf{e}(K_e, m) \oplus \alpha_0 H^3 \oplus xH^2 \oplus \gamma H, \text{ where } \gamma = [128]_{64}||[384]_{64}; \\ E &= \alpha_0 \oplus \mathbf{e}(K_c, D)||x \oplus \mathbf{e}(K_c, \mathsf{incr}(D)); \\ F &= \mathbf{e}(K_e, m) \oplus \alpha_0 H^3 \oplus xH^2 \oplus \gamma H \oplus \alpha_0 H^4 \oplus \mathbf{e}(K_c, D)H^4 \oplus xH^3 \oplus \mathbf{e}(K_c, \mathsf{incr}(D))H^3 \oplus \gamma' H^2 \oplus \gamma'' H; \\ &\qquad \text{where } \gamma' = [128]_{64}||[256]_{64}, \gamma'' = [128]_{64}||[384]_{64}; \\ G &= \mathbf{d}(K_d, F); \end{aligned}$$

For the input $\alpha_1||x \oplus \alpha_0 H \oplus \alpha_1 H||m$,

$$
\begin{aligned}
A &= m;\\
B &= \alpha_1||x \oplus \alpha_0 H \oplus \alpha_1 H;\\
C &= \mathbf{e}(K_e, m);\\
D &= \mathbf{e}(K_e, m) \oplus \alpha_0 H^3 \oplus x H^2 \oplus \gamma H, \text{ where } \gamma = [128]_{64}||[384]_{64};\\
E &= \alpha_1 \oplus \mathbf{e}(K_c, D)||x \oplus \alpha_0 H \oplus \alpha_1 H \oplus \mathbf{e}(K_c, \mathsf{incr}(D));\\
F &= \mathbf{e}(K_e, m) \oplus \alpha_0 H^3 \oplus x H^2 \oplus \gamma H \oplus \alpha_0 H^4 \oplus \mathbf{e}(K_c, D) H^4 \oplus x H^3 \oplus \mathbf{e}(K_c, \mathsf{incr}(D)) H^3 \oplus \gamma' H^2 \oplus \gamma'' H;\\
&\qquad \text{where } \gamma' = [128]_{64}||[256]_{64}, \gamma'' = [128]_{64}||[384]_{64};\\
G &= \mathbf{d}(K_d, F);
\end{aligned}
$$

For the above inputs Gs, i.e. the third blocks of the outputs are same, establishing that $1||\alpha_0 H \oplus \alpha_1 H$ is a period of f. Given a superposition access to an oracle for XCB, a circuit implementing f can be built and by using Simon's algorithm, with high probability we get this non-zero period for this function. But in case of an ideal tweakable SPRP construction with high probability Simon's algorithm outputs zero. This gives a distinguisher rendering XCB a quantum insecure TES. Note that, the output of Simon's algorithm also reveals H for XCB.

Now we come to the previous version [6] of XCB. For this version, the Simon's function is the following.

$$
\begin{aligned}
f : \{0,1\} \times \{0,1\}^n &\rightarrow \{0,1\}^n\\
(b, x) &\xmapsto{f} c_2 \oplus \alpha_b, \text{ where } c_1||c_2||c_3 \longleftarrow \mathsf{XCB}_K(\varepsilon, m||\alpha_b||x).
\end{aligned}
$$

With a similar calculation like above, we observe that, $f(b, x) = f(b', x') \Leftrightarrow x \oplus x' = \alpha_b K_1 \oplus \alpha_{b'} K_1$, i.e. $1||\alpha_0 K_1 \oplus \alpha_1 K_1$ is a period of f. Here Simon's algorithm reveals K_1, along with giving a distinguisher of this version of XCB from an ideal tweakable SPRP.

2.4 Application to the TET construction

Halevi, in the year 2007, proposed a TES, called TET [9], based on electronic codebook mode (ECB).

In the following, we define a Simon's function from TET and give a quantum period finding attack on this function, which gives a distinguisher of TET from an ideal tweakable SPRP. This attack also considers messages with three blocks. Let the message be $x_1||x_2||x_3$. We refer the reader to Figure 2 of [9] for the encryption algorithm.

Fix arbitrary $K_1||K_2$ from the key-space and arbitrary T from the tweak-space of the algorithm.

We define the following function.

$$
\begin{aligned}
f : \{0,1\}^n \times \{0,1\}^n &\rightarrow \{0,1\}^n\\
(x, x') &\xmapsto{f} c_1 \oplus c_3, \text{ where } c_1||c_2||c_3 \longleftarrow \mathsf{TET}_{K_1,K_2}(T, x||x'||x).
\end{aligned}
$$

In the following discussion, we observe, $f(x||x'||x) = f(x \oplus \alpha^2\beta \oplus \beta||x' \oplus \frac{(\alpha^2\beta \oplus \beta)(\tau \oplus \tau^3)}{\tau^2}||x \oplus \alpha^2\beta \oplus \beta)$.

For the input $x||x'||x$, we have,

$$\begin{aligned}
SP &= (x\tau^3 \oplus x'\tau^2 \oplus x\tau)/\sigma;\\
PPP_1 &= x \oplus SP \oplus \beta;\\
PPP_2 &= x' \oplus SP \oplus \alpha\beta;\\
PPP_3 &= x \oplus SP \oplus \alpha^2\beta;\\
CC_1 &= E_{K_2}(x \oplus SP \oplus \beta) \oplus \beta;\\
CC_2 &= E_{K_2}(x' \oplus SP \oplus \alpha\beta) \oplus \alpha\beta;\\
CC_3 &= E_{K_2}(x \oplus SP \oplus \alpha^2\beta) \oplus \alpha^2\beta;\\
C_1 \oplus C_3 &= E_{K_2}(x \oplus SP \oplus \beta) \oplus \beta \oplus E_{K_2}(x \oplus SP \oplus \alpha^2\beta) \oplus \alpha^2\beta;
\end{aligned}$$

For the input $x \oplus \alpha^2\beta \oplus \beta||x' \oplus \frac{(\alpha^2\beta\oplus\beta)(\tau\oplus\tau^3)}{\tau^2}||x \oplus \alpha^2\beta \oplus \beta$, we have,

$$\begin{aligned}
SP &= (x\tau^3 \oplus x'\tau^2 \oplus x\tau)/\sigma;\\
PPP_1 &= x \oplus \alpha^2\beta \oplus \beta \oplus SP \oplus \beta = x \oplus \alpha^2\beta \oplus SP;\\
PPP_2 &= x' \oplus \frac{(\alpha^2\beta \oplus \beta)(\tau \oplus \tau^3)}{\tau^2} \oplus SP \oplus \alpha\beta;\\
PPP_3 &= x \oplus \alpha^2\beta \oplus \beta \oplus SP \oplus \alpha^2\beta = x \oplus \beta \oplus SP;\\
CC_1 &= E_{K_2}(x \oplus \alpha^2\beta \oplus SP) \oplus \beta;\\
CC_2 &= E_{K_2}(x' \oplus \frac{(\alpha^2\beta \oplus \beta)(\tau \oplus \tau^3)}{\tau^2} \oplus SP \oplus \alpha\beta) \oplus \alpha\beta;\\
CC_3 &= E_{K_2}(x \oplus \beta \oplus SP) \oplus \alpha^2\beta;\\
C_1 \oplus C_3 &= E_{K_2}(x \oplus \alpha^2\beta \oplus SP) \oplus \beta \oplus E_{K_2}(x \oplus \beta \oplus SP) \oplus \alpha^2\beta;
\end{aligned}$$

The above equations establishes that $\alpha^2\beta \oplus \beta||\frac{(\alpha^2\beta\oplus\beta)(\tau\oplus\tau^3)}{\tau^2}||\alpha^2\beta \oplus \beta$ is a period for the function f. Given a superposition access to an oracle for TET, a circuit implementing f can be built, for which Simon's algorithm outputs this non-zero period with high probability. Moreover, from this period we get a degree 3 single variate equation in the hash key τ, from which the correct τ can be determined. On the other hand, for an ideal tweakable SPRP construction with high probability Simon's algorithm outputs zero. This gives a distinguisher rendering TET a quantum insecure TES. The possibility of finding out τ is also a major weakness of TET in this context.

2.5 Application to the AEZ construction

AEZ [10], proposed recently by Hoang et al., is a single key TESs using only the encryption function of the block cipher. It is parallelisable.

AEZ is an AEAD, which has an underlined TES. The nonce and the associated data of the AEAD is converted to a tweak of the TES. As in this work, we are considering only TESs, we will take the TES portion of AEZ as an independent scheme with a tweak input by the user. As a result, we need not deal with the issue regarding repetition of nonce mentioned in the paper by Kaplan [2] et al.

There are different versions of AEZ [10] built from different variants of AES. We will consider the version where the proper AES algorithm is used. Messages of lengths at least 2n bits are handled differently from messages of lengths less than 2n bits. Our attack uses messages of lengths $2n$ bits. Hence, the portion relevant to our attack is the one which can handle messages of lengths

at least 2n bits. The corresponding algorithm is called Encipher-AEZ-core, described in Figure 5 of [10].

Fix distinct T_0 and T_1 from the tweak-space of the algorithm Encipher-AEZ-core and an arbitrary K from the key-space; let b denote a bit. We define the following Simon's function.

$$\begin{aligned} f : \{0,1\} \times \{0,1\}^n &\rightarrow \{0,1\}^n \\ (b, M_x) &\overset{f}{\mapsto} C_y, \text{ where } C_x||C_y \longleftarrow \text{ Encipher-AEZ-core}(K, T_b, M_x||0^{128}). \end{aligned}$$

Let $\Delta_0 =$ AEZ-hash(K, T_0) and $\Delta_1 =$ AEZ-hash(K, T_1), where AEZ-hash is described in Figure 6 of [10]. In the following discussion, we observe, $f(b, M_x) = f(b', M'_x) \Leftrightarrow M_x \oplus M'_x = \Delta_b \oplus \Delta_{b'}$.

For the input $(K, T_0, M_x||0^{128})$, we have,

$$\begin{aligned} S_x &= M_x \oplus \Delta_0 \oplus E_K^{0,1}(0^{128}); \\ S_y &= E_K^{-1,1}(S_x); \\ C_y &= M_x \oplus \Delta_0 \oplus E_K^{0,1}(0^{128}) \oplus E_K^{-1,2}(E_K^{-1,1}(S_x)); \end{aligned}$$

For the input $(K, T_1, M_x \oplus \Delta_0 \oplus \Delta_1||0^{128})$, we have,

$$\begin{aligned} S_x &= M_x \oplus \Delta_0 \oplus \Delta_1 \oplus \Delta_1 \oplus E_K^{0,1}(0^{128}) = M_x \oplus \Delta_0 \oplus E_K^{0,1}(0^{128}); \\ S_y &= E_K^{-1,1}(S_x); \\ C_y &= M_x \oplus \Delta_0 \oplus E_K^{0,1}(0^{128}) \oplus E_K^{-1,2}(E_K^{-1,1}(S_x)); \end{aligned}$$

The above discussion proves that there is a non-zero period, viz. $1||\Delta_0 \oplus \Delta_1$, of f built from AEZ, which can be retrieved by Simon's algorithm with high probability. This gives a distinguisher of AEZ from an ideal tweakable SPRP.

2.6 Application to the FAST construction

FAST [11] is a new family of tweakable enciphering schemes, proposed by Chakraborty et al. It is built using a fixed input length pseudo-random function and an appropriate hash function. FAST uses a single-block key, is parallelisable and can be instantiated using only the encryption function of a block cipher.

From a top level view, FAST consists of three distinct layers - hash-encrypt-hash. The hashing layers are based on two universal hash function calls and a two-round Feistel based on a PRF F_K, which constitute the encryption of the first two blocks of the plaintext. The remaining plaintext is encrypted in CTR mode based on F_K with an offset, derived from the input and output of the Feistel layer. We refer the reader to Table 2 of [11] for detailed encryption algorithm of FAST.

Our attack considers plaintext consisting of four blocks. Let it be $p_1||p_2||p_3||p_4$.

Fix arbitrary $K \in \mathcal{K}$, $T \in \mathcal{T}$, $\alpha_0, \alpha_1, p_3 \in \{0,1\}^n$, such that $\alpha_0 \oplus \alpha_1 = 0^{126}11$; let b denote a bit. Now, we define the following Simon's function.

$$\begin{aligned} f : \{0,1\} \times \{0,1\}^n &\rightarrow \{0,1\}^n \\ (b, x) &\overset{f}{\mapsto} c_3 \oplus c_4, \text{ where } c_1||c_2||c_3||c_4 \longleftarrow \mathsf{FAST.Encrypt}_K(T, \alpha_b||x||p_3||p_3). \end{aligned}$$

In the following discussion, we observe, $f(b, x) = f(b', x') \Leftrightarrow x \oplus x' = \alpha_b\tau \oplus \alpha_{b'}\tau$.

For the input $(T, \alpha_0||x||p_3||p_3)$,

$$\begin{aligned}
A_1 &= \alpha_0 \oplus h_\tau(T, p_3||p_3);\\
F_1 &= x \oplus \tau(\alpha_0 \oplus h_\tau(T, p_3||p_3));\\
F_2 &= \alpha_0 \oplus h_\tau(T, p_3||p_3) \oplus F_K(F_1);\\
Z &= F_1 \oplus \alpha_0 \oplus h_\tau(T, p_3||p_3) \oplus F_K(F_1);\\
c_3 &= p_3 \oplus F_K(F_1 \oplus \alpha_0 \oplus h_\tau(T, p_3||p_3) \oplus F_K(F_1) \oplus \mathsf{bin}_n(1));\\
c_4 &= p_3 \oplus F_K(F_1 \oplus \alpha_0 \oplus h_\tau(T, p_3||p_3) \oplus F_K(F_1) \oplus \mathsf{bin}_n(2));\\
c_3 \oplus c_4 &= F_K(F_1 \oplus \alpha_0 \oplus h_\tau(T, p_3||p_3) \oplus F_K(F_1) \oplus \mathsf{bin}_n(1)) \oplus F_K(F_1 \oplus \alpha_0 \oplus h_\tau(T, p_3||p_3) \oplus F_K(F_1) \oplus \mathsf{bin}_n(2));
\end{aligned}$$

For the input $(T, \alpha_1||x \oplus \alpha_0\tau \oplus \alpha_1\tau||p_3||p_3)$,

$$\begin{aligned}
A_1 &= \alpha_1 \oplus h_\tau(T, p_3||p_3);\\
F_1 &= x \oplus \alpha_0\tau \oplus \alpha_1\tau \oplus \tau(\alpha_1 \oplus h_\tau(T, p_3||p_3)) = x \oplus \alpha_0\tau \oplus \tau h_\tau(T, p_3||p_3);\\
F_2 &= \alpha_1 \oplus h_\tau(T, p_3||p_3) \oplus F_K(F_1);\\
Z &= F_1 \oplus \alpha_1 \oplus h_\tau(T, p_3||p_3) \oplus F_K(F_1);\\
c_3 &= p_3 \oplus F_K(F_1 \oplus \alpha_1 \oplus h_\tau(T, p_3||p_3) \oplus F_K(F_1) \oplus \mathsf{bin}_n(1));\\
c_4 &= p_3 \oplus F_K(F_1 \oplus \alpha_1 \oplus h_\tau(T, p_3||p_3) \oplus F_K(F_1) \oplus \mathsf{bin}_n(2));\\
c_3 \oplus c_4 &= F_K(F_1 \oplus \alpha_1 \oplus h_\tau(T, p_3||p_3) \oplus F_K(F_1) \oplus \mathsf{bin}_n(1)) \oplus F_K(F_1 \oplus \alpha_1 \oplus h_\tau(T, p_3||p_3) \oplus F_K(F_1) \oplus \mathsf{bin}_n(2));\\
&= F_K(F_1 \oplus \alpha_0 \oplus \mathsf{bin}_n(3) \oplus h_\tau(T, p_3||p_3) \oplus F_K(F_1) \oplus \mathsf{bin}_n(1)) \oplus F_K(F_1 \oplus \alpha_0 \oplus \mathsf{bin}_n(3) \oplus h_\tau(T, p_3||p_3)\\
&\qquad \oplus F_K(F_1) \oplus \mathsf{bin}_n(2)), \text{ as } \alpha_0 \oplus \alpha_1 = \mathsf{bin}_n(3);\\
&= F_K(F_1 \oplus \alpha_0 \oplus h_\tau(T, p_3||p_3) \oplus F_K(F_1) \oplus \mathsf{bin}_n(2)) \oplus F_K(F_1 \oplus \alpha_0 \oplus h_\tau(T, p_3||p_3) \oplus F_K(F_1) \oplus \mathsf{bin}_n(1));
\end{aligned}$$

The above discussion establishes that $1||\alpha_0\tau \oplus \alpha_1\tau$ is a period for the function f, built from FAST. Simon's algorithm, applied on it, outputs this non-zero period with high probability. Moreover, from this period the hash key τ can be determined. On the other hand, for an ideal tweakable SPRP construction with high probability Simon's algorithm outputs zero. This gives a distinguisher rendering FAST a quantum insecure TES. Retrieving the hash key also breaks the security of the system.

3 Conclusion

This work shows that many of the well known and significant TESs that are secure in the classical world are broken in the quantum world. This leaves us with the question: can any simple modification of any of these schemes make it quantum secure, or, do we need to start the search from the scratch? To the best of our knowledge, yet we do not have any quantum secure TES.

References

[1] Daniel R. Simon. On the Power of Quantum Computation. Volume 26(5) of *SIAM journal on computing*, pages 14741483, 1997.

[2] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier and María Naya-Plasencia. Breaking Symmetric Cryptosystems Using Quantum Period Finding. In Matthew Robshaw and Jonathan

Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*, volume 9815 of *Lecture Notes in Computer Science*, pages 207–237. Springer, 2016.

[3] Shai Halevi and Phillip Rogaway. A tweakable enciphering mode. In Dan Boneh, editor, *CRYPTO*, volume 2729 of *Lecture Notes in Computer Science*, pages 482–499. Springer, 2003.

[4] Shai Halevi and Phillip Rogaway. A parallelizable enciphering mode. In Tatsuaki Okamoto, editor, CT-RSA, volume 2964 of Lecture Notes in Computer Science, pages 292304. Springer, 2004.

[5] Shai Halevi. EME* : Extending EME to handle arbitrary-length messages with associated data. In Anne Canteaut and Kapalee Viswanathan, editors, INDOCRYPT, volume 3348 of Lecture Notes in Computer Science, pages 315327. Springer, 2004.

[6] David A. McGrew and Scott R. Fluhrer. The extended codebook (XCB) mode of operation. Cryptology ePrint Archive, Report 2004/278, 2004. `http://eprint.iacr.org/`.

[7] David A. McGrew and Scott R. Fluhrer. The security of the extended codebook (xcb) mode of operation. In Carlisle M. Adams, Ali Miri, and Michael J. Wiener, editors, *Selected Areas in Cryptography*, volume 4876 of *Lecture Notes in Computer Science*, pages 311–327. Springer, 2007.

[8] IEEE Std 1619.2-2010: IEEE standard for wide-block encryption for shared storage media. http://standards.ieee.org/findstds/standard/1619.2-2010.html, March 2011.

[9] Shai Halevi. Invertible universal hashing and the TET encryption mode. In Alfred Menezes, editor, *CRYPTO*, volume 4622 of *Lecture Notes in Computer Science*, pages 412–429. Springer, 2007.

[10] Viet Tung Hoang, Ted Krovetz, and Phillip Rogaway. Robust authenticated-encryption AEZ and the problem that it solves. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*, volume 9056 of *Lecture Notes in Computer Science*, pages 15–44. Springer, 2015.

[11] Debrup Chakraborty, Sebati Ghosh, Cuauhtemoc Mancillas-López and Palash Sarkar. FAST: Disk Encryption and Beyond. IACR Cryptology ePrint Archive, Report 2017/849, 2017. `http://eprint.iacr.org/2017/849`.