SCIENCE CHINA
Information Sciences

• Supplementary File •

Offline dedicated quantum attacks on block cipher constructions based on two parallel permutation-based pseudorandom functions

Xiao-Fan Zhen[1,2], Zhen-Qiang Li[2*], Jia-Cheng Fan[1], Su-Juan Qin[1] & Fei Gao[1,2*]

[1]*State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China*
[2]*State Key Laboratory of Cryptology, P. O. Box 5159, Beijing 100878, China*

Appendix A Dedicated attacks on PolyMAC and constructions based on TPP-PRFs

PolyMAC scheme [1] is a Double-block Hash-then-Sum construction based on polynomial evaluation, proposed in 2020. It uses two hashing keys $k_1, k_3 \in \{0,1\}^n$ and two encryption keys $k_2, k_4 \in \{0,1\}^m$. We consider the case with the two-block message. Throughout this section, $\odot$ denotes multiplication in $GF(2^n)$

$$\text{PolyMAC}(m_1, m_2) = E_{k_2}(k_1^2 \odot m_1 \oplus k_1 \odot m_2) \oplus E_{k_4}(k_3^2 \odot m_1 \oplus k_3 \odot m_2), \tag{A1}$$

where $M = m_1 \| m_2$, and $|m_1| = |m_2| = n$.

Based on PolyMAC, we construct the XOR-type function. Let β_0, β_1 be two fixed strings in $\{0,1\}^n$, $\beta_0 \neq \beta_1$, and $\alpha_i \in \{0,1\}^n$, we define the function as

$$\begin{aligned} f : \{0,1\}^n \times \{0,1\}^n &\to \{0,1\}^n \\ (\alpha_i, x) &\mapsto \text{PolyMAC}(\beta_0, x) \oplus \text{PolyMAC}\left(\beta_1, x \oplus \alpha_i\right). \end{aligned} \tag{A2}$$

Since the secret state α_i is XORed with x in the second term $\text{PolyMAC}(\beta_1, x \oplus \alpha_i)$ of Eq. (A2), and the function has the period $s = (k_1 \oplus k_3) \odot (\beta_0 \oplus \beta_1)$ when $\alpha_i = k_1 \odot (\beta_0 \oplus \beta_1)$ or $\alpha_i = k_3 \odot (\beta_0 \oplus \beta_1)$. Then, the XOR-type function given in Eq. (A2) satisfies the requirement of Shi *et al.*'s attack.

Now, we define a new function $F^{\mathcal{L}}$ using truncated input

$$\begin{aligned} F^{\mathcal{L}} : \{0,1\}^{n-t} \times \{0,1\}^{n-t} &\to \{0,1\}^m \\ (\alpha_i^l, x^l) &\mapsto \bigoplus_{u \in \mathcal{L}} f(\alpha_i^l \| 0^t, x^l \| 0^t \oplus u), \end{aligned} \tag{A3}$$

where $\mathcal{L} = \{u : u = 0^{n-t} \| *\}$, $\alpha_i = \alpha_i^l \| \alpha_i^r$, $x = x^l \| x^r$, $|\alpha_i^l| = |x^l| = n - t$, and $|\alpha_i^r| = |x^r| = t$. We deduce that the function $F^{\mathcal{L}}$ has a period $s^l = (k_1 \oplus k_3)^l \odot (\beta_0 \oplus \beta_1)^l$ when $\alpha_i^l = k_1^l \odot (\beta_0 \oplus \beta_1)^l$ or $k_3^l \odot (\beta_0 \oplus \beta_1)^l$. Applying Shi *et al.*'s attack [2] to PolyMAC, we can recover the high $(n-t)$-bit $k_1^l \odot (\beta_0 \oplus \beta_1)^l$ or $k_3^l \odot (\beta_0 \oplus \beta_1)^l$ with $O\big(2^{(n+t)/2} \cdot (n-t)\big)$ quantum queries to the PolyMAC oracle and $O(2^{(n-t)/2} \cdot n^3)$ time.

The remaining t bits can be recovered as follows. Taking $\alpha_i^l = k_1^l \odot (\beta_0 \oplus \beta_1)^l$ as an example, we define $f'(\alpha_i^r, x) = f\big(k_1^l \odot (\beta_0 \oplus \beta_1)^l \| \alpha_i^r, x\big)$. When $\alpha_i^r = k_1^r \odot (\beta_0 \oplus \beta_1)^r$, $f'(\alpha_i^r, x) = f'(\alpha_i^r, x \oplus s)$, which requires $O(2^{t/2})$ quantum queries.

A TPP-PRF [3] is defined by

$$g(x) = l_{33} P_1\big(l_{13}(x) \oplus l_{14}(k_1)\big) \oplus l_{34} P_2\big(l_{23}(x) \oplus l_{24}(k_2)\big) \oplus e(x) \oplus C, \tag{A4}$$

where $e(x) = l_{31} l_{11}(x) \oplus l_{32} l_{21}(x)$ and C is a key-dependent constant.

For this TPP-PRF, we construct the function

$$f(i, x) = g(x) \oplus e(x) \oplus l_{33} P_1\left(l_{13}(x)\right) \oplus l_{34} P_2\left(l_{23}(x \oplus i)\right), \tag{A5}$$

which satisfies $f(i,x) = f(i, x \oplus l_{13}^{-1} l_{14}(k_1))$ when $i = l_{23}^{-1} l_{24}(k_2)$ or $i = l_{23}^{-1} l_{24}(k_2) \oplus l_{13}^{-1} l_{14}(k_1)$. Therefore, constructions based on TPP-PRFs also admit such XOR-type functions and are therefore amenable to Shi *et al.*'s attack.

Applying the truncation techniques, we obtain

$$\begin{aligned} F^{\mathcal{L}} : \{0,1\}^{n-t} \times \{0,1\}^{n-t} &\to \{0,1\}^m \\ (\alpha_i^l, x^l) &\mapsto \bigoplus_{u \in \mathcal{L}} f(i^l \| 0^t, x^l \| 0^t \oplus u). \end{aligned} \tag{A6}$$

Then $F^{\mathcal{L}}(i^l, x^l)$ has an $(n-t)$-bit period $s^l = l_{13}^{-1} l_{14} k_1^l$ for $i^l = i_0^l$, where $i_0^l = l_{23}^{-1} l_{24} k_2^l$ or $i^l = l_{23}^{-1} l_{24} k_2^l \oplus l_{13}^{-1} l_{14} k_1^l$. Similarly, Shi *et al.*'s attack is applied to constructions based on TPP-PRFs to recover $l_{23}^{-1} l_{24} k_2^l$ with $O\big(2^{(n+t)/2} \cdot (n-t)\big)$ quantum queries and $O(2^{(n-t)/2} \cdot n^3)$ time. The remaining key bits can then be recovered by Grover-meets-Simon algorithm.

* Corresponding author (email: lizq@sklc.org, gaof@bupt.edu.cn)

Appendix B Construction of p-XOR-type functions from TPP-PRFs

Appendix B.1 General construction and proof of the period property

For the p-XOR-type function constructed by TPP-PRFs, the truncation in the Q2 model yields the same conditional periodic function as in Shi *et al.*'s attack, namely Eq. (A6). Then, we only need to define the corresponding function $F^{\mathcal{L}}$ in the Q1 model.

$$F^{\mathcal{L}}(i^l\|j^{l_2},x^{l_1}) = G_1^{\mathcal{L}}(x^{l_1}) \oplus P^{\mathcal{L}}(i^l\|j^{l_2},x^{l_1}), \tag{B1}$$

where $l_1 \in \{0,1\}^p$, $l_2 \in \{0,1\}^{n-t-p}$, $l = l_1\|l_2$. The function $G_1^{\mathcal{L}} : \{0,1\}^p \to \{0,1\}^n$ and the public function $P^{\mathcal{L}} : \{0,1\}^{2n-2t-p} \times \{0,1\}^p \to \{0,1\}^n$ are defined as

$$\begin{aligned} G_1^{\mathcal{L}}(x^{l_1}) &= \bigoplus_{u\in\mathcal{L}} g(x^{l_1}\|0^{n-t-p}\|0^t \oplus u) \oplus e(x^{l_1}\|0^{n-t-p}\|0^t \oplus u),\\ P^{\mathcal{L}}(i^l\|j^{l_2},x^{l_1}) &= \bigoplus_{u\in\mathcal{L}} l_{33}P_1\left(l_{13}(x^{l_1}\|j^{l_2})\|0^t \oplus u\right) \oplus l_{34}P_2\Big(l_{23}\big((x^{l_1}\|0^{n-t-p}) \oplus i^l\big)\|0^t \oplus u\Big). \end{aligned}$$

The function $F^{\mathcal{L}}$ given in Eq. (B1) has the period $s^{l_1} = l_{13}^{-1}l_{14}k_1^{l_1}$ when $i^l\|j^{l_2} = l_{23}^{-1}l_{24}k_2^l\|l_{13}^{-1}l_{14}k_1^{l_2}$ or $i^l\|j^{l_2} = l_{23}^{-1}l_{24}k_2^l \oplus (l_{13}^{-1}l_{14}k_1^{l_1}\|0^{n-t-p})\|l_{13}^{-1}l_{14}k_1^{l_2}$. Take $i^l\|j^{l_2} = l_{23}^{-1}l_{24}k_2^l\|l_{13}^{-1}l_{14}k_1^{l_2}$ as an example, we deduce that

$$\begin{aligned} &F^{\mathcal{L}}(l_{23}^{-1}l_{24}k_2^l\|l_{13}^{-1}l_{14}k_1^{l_2},x^{l_1})\\ =&\bigoplus_{u\in\mathcal{L}} l_{33}P_1\big((l_{13}x^{l_1} \oplus l_{14}k_1^{l_1})\|l_{14}k_1^{l_2}\|0^t \oplus u\big) \oplus l_{34}P_2\big((l_{23}x^{l_1} \oplus l_{24}k_2^{l_1})\|l_{24}k_2^{l_2}\|0^t \oplus u\big)\\ &\oplus l_{33}P_1\big(l_{13}(x^{l_1}\|l_{13}^{-1}l_{14}k_1^{l_2})\|0^t \oplus u\big) \oplus l_{34}P_2\big(l_{23}(x^{l_1}\|0^{n-t-p} \oplus l_{23}^{-1}l_{24}k_2^l)\|0^t \oplus u\big) \oplus C\\ =&\bigoplus_{u\in\mathcal{L}} l_{33}P_1(l_{13}x^{l_1}\|l_{14}k_1^{l_2}\|0^t \oplus u) \oplus l_{34}P_2\big((l_{23}x^{l_1} \oplus l_{23}l_{13}^{-1}l_{14}k_1^{l_1} \oplus l_{24}k_2^{l_1})\|l_{24}k_2^{l_2}\|0^t \oplus u\big)\\ &\oplus l_{33}P_1\Big(\big(l_{13}(x^{l_1} \oplus l_{13}^{-1}l_{14}k_1^{l_1})\|l_{13}^{-1}l_{14}k_1^{l_2}\big)\|0^t \oplus u\Big) \oplus l_{34}P_2\Big(\big(l_{23}(x^{l_1} \oplus l_{13}^{-1}l_{14}k_1^{l_1})\|0^{n-t-p} \oplus l_{23}^{-1}l_{24}k_2^l\big)\|0^t \oplus u\Big) \oplus C\\ =&F^{\mathcal{L}}(l_{23}^{-1}l_{24}k_2^l\|l_{13}^{-1}l_{14}k_1^{l_2},x^{l_1} \oplus l_{13}^{-1}l_{14}k_1^{l_1}). \end{aligned}$$

Appendix B.2 Instantiations of TPP-PRFs

The Xop construction [4] is defined by the bitwise XOR of the outputs from two distinct pseudorandom permutations (PRPs) applied to the same input x:

$$\mathrm{Xop}_{E_1,E_2}(x) = E_1(x) \oplus E_2(x),$$

where E_1 and E_2 represent the encryption algorithms of the respective PRPs.

Realizing the Xop construction with two Even-Mansour ciphers, $EM_1(x) = P_1(x\oplus k_1)\oplus k_2$ and $EM_2(x) = P_2(x\oplus k_3)\oplus k_4$, resulting in the XopEM function:

$$\mathsf{XopEM}(x) = P_1(x \oplus k_1) \oplus P_2(x \oplus k_3) \oplus k_2 \oplus k_4. \tag{B2}$$

We can obtain a p-XOR-type function as follows: $f(i,x) = P_1(x \oplus k_1) \oplus P_2(x \oplus k_3) \oplus P_1(x) \oplus P_2(x \oplus i)$, where $g_1(x) = \mathsf{XopEM}(x)$, and the public function is $p(i,x) = P_1(x) \oplus P_2(x \oplus i)$. This function has a period $s = k_1$ precisely when $i = k_3$ or $i = k_3 \oplus k_1$.

The function $F^{\mathcal{L}} : \{0,1\}^{n-t} \times \{0,1\}^{n-t-p} \times \{0,1\}^p \to \{0,1\}^n$ is defined as:

$$F^{\mathcal{L}}(i^l\|j^{l_2},x^{l_1}) = \bigoplus_{u\in\mathcal{L}} \mathsf{XopEM}(x^{l_1}\|0^{n-t-p}\|0^t \oplus u) \oplus P_1(x^{l_1}\|j^{l_2}\|0^t \oplus u) \oplus P_2\Big(\big((x^{l_1}\|0^{n-t-p}) \oplus i^l\big)\|0^t \oplus u\Big). \tag{B3}$$

It can be verified that $F^{\mathcal{L}}(i^l\|j^{l_2},x^{l_1}) = F^{\mathcal{L}}(i^l\|j^{l_2},x^{l_1} \oplus k_1^{l_1})$ when $i^l\|j^{l_2} = k_3^l\|k_1^{l_2}$ or $i^l\|j^{l_2} = k_3^l \oplus (k_1^{l_1}\|0^{n-t-p})\|k_1^{l_2}$.

SoEM22 [3]. The Sum of Even-Mansour (SoEM) construction employs two public permutations P_1, P_2, and two n-bit keys k_1, k_2. It is a specific instance of the XOR construction where $k_3 = k_2$ and $k_4 = k_1$, defined as:

$$\mathsf{SoEM22}(x) = P_1(x \oplus k_1) \oplus P_2(x \oplus k_2) \oplus k_1 \oplus k_2. \tag{B4}$$

We can construct a p-XOR-type function $f(i,x) = \mathsf{SoEM22}(x) \oplus P_1(x) \oplus P_2(x \oplus i)$, where $P_1(x) \oplus P_2(x \oplus i)$ is a public function. This function satisfies $f(i,x) = f(i,x \oplus k_1)$ when $i = k_2$ or $i = k_2 \oplus k_1$. Next, we construct the function $F^{\mathcal{L}}(i^l\|j^{l_2},x^{l_1})$ as:

$$F^{\mathcal{L}}(i^l\|j^{l_2},x^{l_1}) = \bigoplus_{u\in\mathcal{L}} \mathsf{SoEM22}(x^{l_1}\|0^{n-t-p}\|0^t \oplus u) \oplus P_1(x^{l_1}\|j^{l_2}\|0^t \oplus u) \oplus P_2\Big(\big((x^{l_1}\|0^{n-t-p}) \oplus i^l\big)\|0^t \oplus u\Big). \tag{B5}$$

The function $F^{\mathcal{L}}(i^l\|j^{l_2},x^{l_1})$ given in Eq. (B5) has a period $k_1^{l_1}$ when $i^l\|j^{l_2} = k_2^l\|k_1^{l_2}$ or $i^l\|j^{l_2} = k_2^l \oplus (k_1^{l_1}\|0^{n-t-p})\|k_1^{l_2}$.

If $P_1 = P$ and $P_2 = P^{-1}$, the above $\mathsf{SoEM22}$ construction corresponds to SUMPIP [5]. In the same way, a p-XOR-type function $f(i,x)$ and a hidden periodic function $F^{\mathcal{L}}$ can be constructed based on the truncation parameter.

DS-SoEM [6]. This construction is a domain-separated variant of the Xop construction that uses a d-bit domain-separation constant and is a sum of two Even-Mansour ciphers. For an input $x \in \{0,1\}^{n-d}$, it is defined as:

$$\mathsf{DS\text{-}SoEM}(x) = P\left((x \oplus \mathrm{msb}_{n-d}(k_1))\,\|0^d\right) \oplus P\left((x \oplus \mathrm{msb}_{n-d}(k_2))\,\|1^d\right) \oplus k_1 \oplus k_2, \tag{B6}$$

where 'msb_{n-d}' denotes truncation to the $n-d$ most significant bits.

We define a p-XOR-type function $f(i,x) = \mathsf{DS\text{-}SoEM}(x) \oplus P(x\|0^d) \oplus P\left((x\oplus i)\|1^d\right)$, where the public function is $P(x\|0^d) \oplus P\left((x\oplus i)\|1^d\right)$. This function satisfies $f(i,x) = f\left(i, x\oplus \mathrm{msb}_{n-d}(k_1)\right)$ when $i = \mathrm{msb}_{n-d}(k_2)$ or $i = \mathrm{msb}_{n-d}(k_2) \oplus \mathrm{msb}_{n-d}(k_1)$. The new function $F^{\mathcal{L}}$ is defined as:

$$F^{\mathcal{L}}(i^l\|j^{l_2}, x^{l_1}) = \bigoplus_{u\in\mathcal{L}} \mathsf{DS\text{-}SoEM}(x^{l_1}\|0^{n-t-p}\|0^t \oplus u) \oplus P\big((x^{l_1}\|j^{l_2}\|0^t\oplus u)\|0^d\big) \oplus P\Big(\big((x^{l_1}\|0^{n-t-p}\oplus i^l)\|0^t\oplus u\big)\|1^d\Big). \tag{B7}$$

This function has a p-bit period $[\mathrm{msb}_{n-d}(k_1)]^{l_1}$. It occurs when $i^l\|j^{l_2} = A$ or $i^l\|j^{l_2} = B$, where $A = [\mathrm{msb}_{n-d}(k_2)]^l\|[\mathrm{msb}_{n-d}(k_1)]^{l_2}$ and $B = [\mathrm{msb}_{n-d}(k_2)]^l \oplus \left([\mathrm{msb}_{n-d}(k_1)]^{l_1}\|0^{n-t-p}\right)\|[\mathrm{msb}_{n-d}(k_1)]^{l_2}$.

In summary, our analysis shows that several instances of TPP-PRF, including XopEM, SoEM22, SUMPIP, and DS-SoEM, can be used to construct p-XOR-type functions. Furthermore, by applying truncation techniques, we present their corresponding conditional periodic functions $F^{\mathcal{L}}$, as shown in Eqs. (B3), (B5), and (B7). These explicit forms of $F^{\mathcal{L}}$ will be used by the offline attack in Appendix C and by the applications to general TPP-PRF-based constructions in Appendix D.

Appendix C Algorithmic details of the offline dedicated quantum attack

Based on the above p-XOR-type functions constructed by TPP-PRFs, we propose an offline dedicated quantum attack on TPP-PRF-based constructions in the Q1 and Q2 models (see Algorithm C1).

Algorithm C1 Offline dedicated attack on block cipher constructions based on p-XOR-type function using truncated technique

Require: Prepared $\left|\psi_{G_1^{\mathcal{L}}}\right\rangle = \otimes^{c'}\left(\sum_{x^l\in\{0,1\}^{n-t}}|x^l\rangle|G_1^{\mathcal{L}}(x^l)\rangle\right)$,

Let $\mathcal{L} = \{u : u = 0^{n-t}||*\}$, $f(i,x)$ be a p-XOR-type function, and $f(i,\cdot)$ have a non-trivial period s when $i = i_0$.

Ensure: The high $(\kappa-t)$-bit of i_0 and $(n-t)$-bit of s, namely i_0^l and s^l, s.t., $F^{\mathcal{L}}(i^l,x^l) = F^{\mathcal{L}}(i^l, x^l\oplus s^l)$ when $i^l = i_0^l$.

1: Start $\left|\psi_{G_1^{\mathcal{L}}}\right\rangle|0^{\kappa-t}\rangle$.

2: Apply $I_{c'(n-t+m)} \otimes H^{\otimes\kappa-t}$ to obtain $|\Psi\rangle$:

$$|\Psi\rangle = |\psi_{G_1^{\mathcal{L}}}\rangle\left(\sum_{i^l\in\{0,1\}^{\kappa-t}}|i^l\rangle\right).$$

3: Repeat $\mathcal{O}(2^{(\kappa-t)/2})$ Grover iterations:

$$|i^l\rangle|b\rangle \overset{\text{test}}{\to} |v\rangle|b\oplus r\rangle.$$

Note that the test oracle is a unitary operator that takes $|\psi_{G_1^{\mathcal{L}}}\rangle|i^l\rangle$ as input, and tests whether $F^{\mathcal{L}}(i^l,\cdot)$ has a hidden period (see Algorithm C2 for details).

4: Measure the index i^l to obtain i_0^l.

Algorithm C2 The procedure checks whether a function $F^{\mathcal{L}}(i^l,x^l) = G_1^{\mathcal{L}}(x^l)\oplus P^{\mathcal{L}}(i^l,x^l)$ has a period, without making any new queries to g_1

1: Start $|\psi_{G_1^{\mathcal{L}}}\rangle|b\rangle$:

$$\left(\sum_{x_1^l,\cdots,x_{c'}^l\in\{0,1\}^{n-t}}|x_1^l\rangle\cdots|x_{c'}^l\rangle|G_1^{\mathcal{L}}(x_1^l)\rangle\cdots|G_1^{\mathcal{L}}(x_{c'}^l)\rangle\right)|b\rangle.$$

2: Apply c' $U_{P^{\mathcal{L}}}$ to obtain $|\psi_{F^{\mathcal{L}}}\rangle$:

$$|\psi_{F^{\mathcal{L}}}\rangle = \otimes^{c'}\left(\sum_{x^l\in\{0,1\}^{n-t}}|x^l\rangle|G_1^{\mathcal{L}}(x^l)\oplus P^{\mathcal{L}}(x^l)\rangle\right)|b\rangle = \otimes^{c'}\left(\sum_{x^l\in\{0,1\}^{n-t}}|x^l\rangle|F^{\mathcal{L}}(x^l)\rangle\right)|b\rangle.$$

3: Apply $(H^{\otimes(n-t)}\otimes I_m)^{\otimes c'}\otimes I_1$ to $|\psi_{F^{\mathcal{L}}}\rangle$, to get:

$$\left(\sum_{v_1,x_1^l\in\{0,1\}^{n-t}}(-1)^{v_1\cdot x_1^l}|v_1\rangle|F^{\mathcal{L}}(x_1^l)\rangle\right)\otimes\cdots\otimes\left(\sum_{v_{c'},x_{c'}^l\in\{0,1\}^{n-t}}(-1)^{v_{c'}\cdot x_{c'}^l}|v_{c'}\rangle|F^{\mathcal{L}}(x_{c'}^l)\rangle\right)|b\rangle.$$

4: Compute $d := \dim(\mathrm{Span}(v_1,\ldots,v_{c'}))$.

5: **if** $d = n-t$ **then**

6: set $r := 0$

7: **else**

8: set $r := 1$, and add r to b

9: **end if**

10: Uncompute steps 3-2 to obtain $|\psi_{G_1^{\mathcal{L}}}\rangle|b\oplus r\rangle$.

This algorithm is developed by integrating the offline Simon's algorithm with the dedicated quantum attack on block ciphers via the construction of p-XOR-type functions. Our algorithm is separated into two phases: the online phase prepares the superposition state $|\psi_{G_1^{\mathcal{L}}}\rangle$ via classical or quantum queries to the encryption oracle U_{g_1} (requiring $O(2^n)$ classical queries in the Q1 model by Algorithm C3, or $O(2^t\cdot(n-t))$ quantum queries in the Q2 model by Algorithm C4), and the offline phase performs the remaining quantum computations independently of the encryption oracle (using the test procedure in Algorithm C2 to check whether the function $F^{\mathcal{L}}$ has a hidden period without any new queries to the encryption oracle). This separation achieves a reduction in query complexity, as Grover iterations are executed offline after a limited number of online interactions.

We now explain the implementation of Algorithm C1. The goal is to recover the high $(\kappa-t)$ bits i_0^l such that $F^{\mathcal{L}}(i_0^l,\cdot)$ has a non-trivial period s^l. Starting with the superposition state $|\psi_{G_1^{\mathcal{L}}}\rangle = \otimes^{c'}\left(\sum_{x^l\in\{0,1\}^{n-t}}|x^l\rangle|G_1^{\mathcal{L}}(x^l)\rangle\right)$, the input is $|\psi_{G_1^{\mathcal{L}}}\rangle|0^{\kappa-t}\rangle$ of $(\kappa-t)+c'(n-t)+c'm$ qubits. The initial state $|\Psi\rangle$ required for the Grover iteration is obtained by several H transforms. The iterative

Algorithm C3 Prepare $|\psi_{G_1^{\mathcal{L}}}\rangle$ in the Q1 model

Require: Classical query to the encryption oracle g_1.
Ensure: $|\psi_{G_1^{\mathcal{L}}}\rangle = \otimes^{c'}\left(\sum_{x^l\in\{0,1\}^{n-t}}|x^l\rangle|G_1^{\mathcal{L}}(x^l)\rangle\right)$

1: Apply $(H^{\otimes(n-t)}\otimes I_m)^{\otimes c'}$ to obtain:

$$\sum_{x_1^l,\cdots,x_{c'}^l\in\{0,1\}^{n-t}}|x_1^l\rangle\cdots|x_{c'}^l\rangle|0^{c'm}\rangle.$$

2: For each $x^l\in\{0,1\}^{n-t}$, classical queries to g_1 to get $\bigoplus_{u\in\mathcal{L}}g_1(x^l||0^t\oplus u)$.

3: Apply unitary operation, which writes $\bigoplus_{u\in\mathcal{L}}g_1(x^l||0^t\oplus u)$ in the second register if the first contains the value x^l:

$$|\psi_{G_1^{\mathcal{L}}}\rangle = \otimes^{c'}\left(\sum_{x^l\in\{0,1\}^{n-t}}|x^l\rangle|\bigoplus_{u\in\mathcal{L}}g_1(x^l||0^t\oplus u)\rangle\right) = \otimes^{c'}\left(\sum_{x^l\in\{0,1\}^{n-t}}|x^l\rangle|G_1^{\mathcal{L}}(x^l)\rangle\right).$$

Algorithm C4 Prepare $|\psi_{G_1^{\mathcal{L}}}\rangle$ in the Q2 model

Require: quantum queries to the encryption oracle g_1.
Ensure: $|\psi_{G_1^{\mathcal{L}}}\rangle = \otimes^{c'}\left(\sum_{x^l\in\{0,1\}^{n-t}}|x^l\rangle|G_1^{\mathcal{L}}(x^l)\rangle\right)$

1: Apply $(H^{\otimes(n-t)}\otimes I_m)^{\otimes c'}$ to obtain:

$$\sum_{x_1^l,\cdots,x_{c'}^l\in\{0,1\}^{n-t}}|x_1^l\rangle\cdots|x_{c'}^l\rangle|0^{c'm}\rangle.$$

2: The XOR sum of 2^t distinct U_{g_1}, which can be implemented by using CNOTs, we can obtain $|\psi_{G_1^{\mathcal{L}}}\rangle$:

$$|\psi_{G_1^{\mathcal{L}}}\rangle = \otimes^{c'}\left(\sum_{x^l\in\{0,1\}^{n-t}}|x^l\rangle|G_1^{\mathcal{L}}(x^l)\rangle\right).$$

function $G = D_{|\Psi\rangle}O_{\text{test}}$ is run for $\mathcal{O}(2^{(\kappa-t)/2})$ iterations, where $D_{|\Psi\rangle} = (2|\Psi\rangle\langle\Psi| - I)$. The final step is measuring the index i^l to obtain i_0^l. The implementation of $U_{P^{\mathcal{L}}}$ and O_{test} in Algorithm C2 is similar to that in Ref. [2]. Specifically, $U_{P^{\mathcal{L}}}$ implements the function

$$P^{\mathcal{L}}(i^l, x^l) = \bigoplus_{u\in\mathcal{L}}p\big((x^l\oplus i^l)\|0^t\oplus u\big),$$

which is the XOR sum of 2^t public functions p and can be implemented in parallel without a sequential relationship.

Appendix D Offline dedicated attacks on constructions based on TPP-PRFs

Recall that the function $f(i,x)$ defined in Eq. (A5) is a p-XOR type function, with $g_1(x) = g(x)\oplus e(x)\oplus l_{33}P_1\big(l_{13}(x)\big)$, and the public function $p(i,x) = l_{34}P_2\big(l_{23}(x\oplus i)\big)$. Hence, our offline attack can be applied to constructions based on TPP-PRFs.

In the Q1 model, we construct a conditional periodic function $F^{\mathcal{L}}(i^l\|j^{l_2}, x^{l_1})$ given in Eq. (B1) by the truncation techniques, which has a p-bit period $s^{l_1} = l_{13}^{-1}l_{14}k_1^{l_1}$ when $i^l\|j^{l_2} = l_{23}^{-1}l_{24}k_2^l\|l_{13}^{-1}l_{14}k_1^{l_2}$ or $i^l\|j^{l_2} = l_{23}^{-1}l_{24}k_2^l\oplus(l_{13}^{-1}l_{14}k_1^{l_1}\|0^{n-t-p})\|l_{13}^{-1}l_{14}k_1^{l_2}$. The offline attack recovers either $l_{23}^{-1}l_{24}k_2^l\|l_{13}^{-1}l_{14}k_1^{l_2}$ or $i^l\|j^{l_2} = l_{23}^{-1}l_{24}k_2^l\oplus(l_{13}^{-1}l_{14}k_1^{l_1}\|0^{n-t-p})\|l_{13}^{-1}l_{14}k_1^{l_2}$, requiring $O(2^{p+t})$ classical queries to the encryption oracle and $O(2^{(2n-2t-p)/2}\cdot n^3)$ offline computation time, where $0\leqslant p\leqslant n-t$, $0<t\leqslant n/2$, $l_2\in\{0,1\}^{n-t-p}$ and $l\in\{0,1\}^{n-t}$. Let D be the number of classical queries and T be the time of offline computations. This attack achieves a tradeoff of $T^2D = 2^{2n-t}$, which is balanced at $T = D = \tilde{O}(2^{(2n-t)/3})$. The remaining keys can be recovered as follows. We can recover the period $s^{l_1} = l_{13}^{-1}l_{14}k_1^{l_1}$ by solving the equation system $s^{l_1}\cdot v_i^{l_1} = 0$, requiring $O(n^3)$ offline computation time. Subsequently, the remaining t bits can be recovered by applying the offline Simon's algorithm on $f'(i^r, x) = f(k_2^l\|i^r, x)$, which has the period $s = k_1$ when $i^r = k_2^r$.

In the Q2 model, the construction of $F^{\mathcal{L}}$ is the same as in Shi *et al.*'s attack; see Eq. (A6). Therefore, there is no need to further partition the $(n-t)$-bit subkey k_1^l into a p-bit part $k_1^{l_1}$ and an $(n-t-p)$-bit part $k_1^{l_2}$. The function $F^{\mathcal{L}}(i^l, x^l) = \bigoplus_{u\in\mathcal{L}}f(i^l\|0^t, x^l\|0^t\oplus u) = G_1^{\mathcal{L}}(x^l)\oplus P^{\mathcal{L}}(i^l, x^l)$ has an $(n-t)$-bit period $s^l = l_{13}^{-1}l_{14}k_1^l$ when $i^l = l_{23}^{-1}l_{24}k_2^l$ or $i^l = l_{23}^{-1}l_{24}k_2^l\oplus l_{13}^{-1}l_{14}k_1^l$. The state $|\psi_{G_1^{\mathcal{L}}}\rangle$ is first prepared by requiring $O\big(2^t\cdot(n-t)\big)$ quantum queries to the encryption oracle by Algorithm C4. According to Theorem 1, we successfully recover $l_{23}^{-1}l_{24}k_2^l$ or $l_{23}^{-1}l_{24}k_2^l\oplus l_{13}^{-1}l_{14}k_1^l$ with $O(2^{(n-t)/2}\cdot n^3)$ offline computation time by Algorithm C1. The remaining key bits can be recovered using the offline Simon techniques with negligible additional cost.

To further illustrate the offline dedicated attack on TPP-PRF-based constructions, we use SoEM22 as an example. Figure D1 compares Shi *et al.*'s dedicated attack with our offline dedicated attacks in the Q2 and Q1 models. In Shi *et al.*'s attack, each Grover iteration requires superposition queries to the SoEM22 oracle. In contrast, in our offline attacks, the oracle-dependent part is first extracted into the state $|\psi_{G_1^{\mathcal{L}}}\rangle$, and the Grover iterations involve only offline computation based on the public permutations.

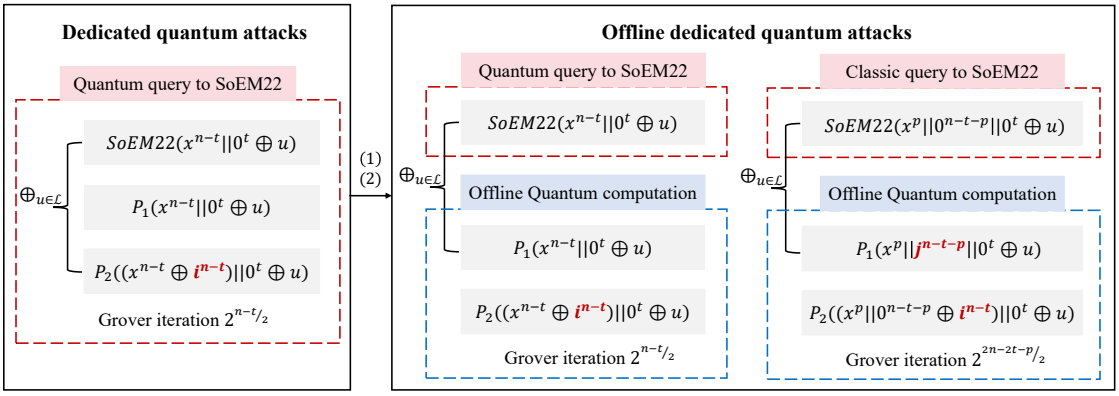
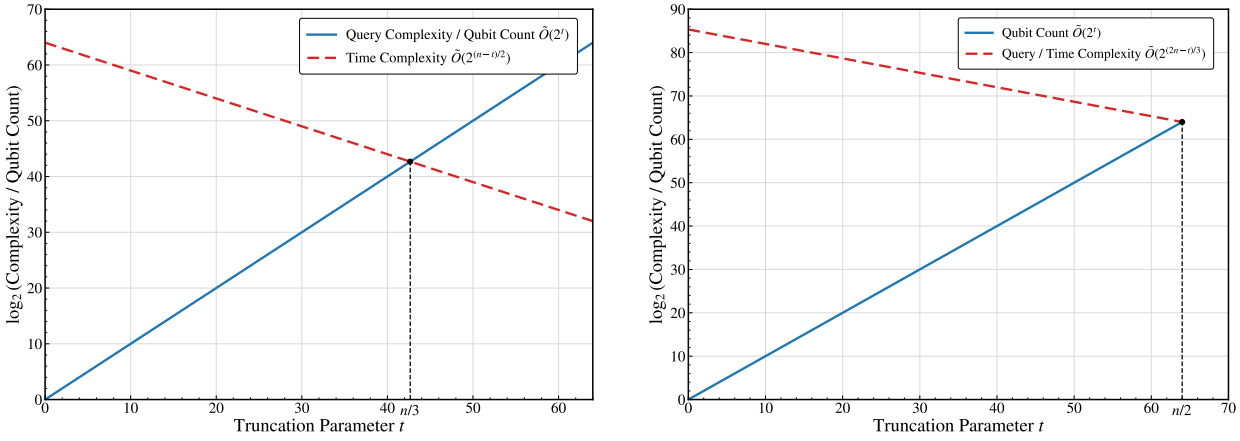


Figure D1 The overall framework of Shi *et al.*'s dedicated attacks [2] and our offline dedicated attack on SoEM22.

Our optimization relies on parallelization to construct $F^{\mathcal{L}}$, which increases the required qubits by a factor of 2^t compared with the offline Simon's algorithm. Figure D2 further shows the impact of the truncation parameter t on the complexities and qubit counts for our offline attack. In the Q2 model, our attack reduces the query complexity for the same time complexity and qubit count. In the Q1 model, it reduces both query and time complexities at the cost of additional qubits.



(a) In the Q2 model

(b) In the Q1 model

Figure D2 Impact of the truncation parameter t on the complexities and the number of qubits for our offline attack, assuming a fixed block size of $n = 128$. The left panel (a) illustrates the resource trade-offs in the Q2 model, while the right panel (b) shows the results in the Q1 model.

References

1 Kim S., Lee B., Lee J. Tight security bounds for double-block hash-then-sum MACs. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, 2020. 435–465
2 Shi T., Wu W., Hu B., et al. Dedicated quantum attacks on XOR-type function with applications to beyond-birthday-bound MACs. IEEE Trans. Inf. Forensics Secur., 2024, 19: 5971–5984
3 Chen Y. L., Lambooij E., Mennink B. How to build pseudorandom functions from public random permutations. In: Annual International Cryptology Conference, Santa Barbara, CA, USA, 2019. 266–293
4 Bellare M., Krovetz T., Rogaway P. Luby-Rackoff backwards: Increasing security by making block ciphers non-invertible. In: International Conference on the Theory and Applications of Cryptographic Techniques, Espoo, Finland, 1998. 266–280
5 Guo C., Shen Y., Wang L., et al. Beyond-birthday secure domain-preserving PRFs from a single permutation. Des. Codes Cryptogr., 2019, 87: 1297–1322
6 Bhattacharjee A., Dutta A., List E., et al. Cencpp*: beyond-birthday-secure encryption from public permutations. Des. Codes Cryptogr., 2022, 90: 1381–1425