SCIENCE CHINA
Information Sciences

• LETTER •

August 2026, Vol. 69, Iss. 8, 180507:1–180507:2
https://doi.org/10.1007/s11432-026-5030-8

Special Topic: Quantum Information

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*

Received 7 January 2026/Revised 6 May 2026/Accepted 1 July 2026/Published online 16 July 2026

Citation Zhen X-F, Li Z-Q, Fan J-C, et al. Offline dedicated quantum attacks on block cipher constructions based on two parallel permutation-based pseudorandom functions. Sci China Inf Sci, 2026, 69(8): 180507, https://doi.org/10.1007/s11432-026-5030-8

Quantum computing poses unprecedented threats to cryptographic security. Simon's algorithm [1] and Grover-meets-Simon algorithm [2] have become important tools in the quantum cryptanalysis of symmetric cryptography. The resulting attacks generally rely on superposition queries to the encryption oracle (i.e., the Q2 model), which limits their practical relevance. To remove this limitation, Bonnetain et al. [3] introduced the offline Simon's algorithm, which decouples the queries to the encryption oracle from the Grover iterations, allowing the attack to be performed using either superposition queries or classical queries (i.e., the Q1 model). Recently, Shi et al. [4] proposed a dedicated quantum attack on XOR-type functions in the Q2 model, applied it to several BBB MACs, and showed that it simultaneously reduces the circuit depth, width, and gate count compared with the parallel Grover-meets-Simon algorithm. However, two questions remain open: whether their attack applies to other cryptographic constructions, and whether it can be performed in the offline setting (particularly using only classical queries to the encryption oracle).

To address these two questions, we make the following contributions.

(1) We identify new cryptographic structures amenable to Shi et al.'s attack, namely PolyMAC and block cipher constructions based on two parallel permutation-based pseudorandom functions (TPP-PRFs), including XopEM, SoEM22, SUMPIP, and DS-SoEM, thereby answering Shi et al.'s open question [4].

(2) We construct decoupled XOR-type functions and propose an offline quantum attack on constructions based on TPP-PRFs, which breaks the obstacle that Shi et al.'s attack relies on superposition queries. Compared to previous results, our attack reduces the query complexity from $O(2^{(n+t)/2}\cdot(n-t))$ to $O(2^t\cdot(n-t))$ in the Q2 model, where t is a truncation parameter satisfying $0<t<n$ and n is the input length. Further, we reduce both the time complexity and classical query complexity from $\tilde{O}(2^{2n/3})$ to $\tilde{O}(2^{(2n-t)/3})$ in the Q1 model for $0<t\leqslant n/2$ (for example, see SoEM22 in Table 1).

New instances amenable to Shi et al.'s attack. Shi et al. [4] proposed a dedicated quantum attack on XOR-type functions of the form $f(i,x)=g_1(x)\oplus g_2(x\oplus\alpha_i)$, where $f(i,\cdot)$ is periodic for the correct value of i. We show that PolyMAC is vulnerable to this attack by constructing the XOR-type function

$$f(i,x)=\mathrm{PolyMAC}(\beta_0,x)\oplus\mathrm{PolyMAC}\left(\beta_1,x\oplus\alpha_i\right), \tag{1}$$

where $\beta_0,\beta_1\in\{0,1\}^n$ are fixed strings. The function f has a 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 $k_3\odot(\beta_0\oplus\beta_1)$. This identifies PolyMAC as a new application of Shi et al.'s attack.

Moreover, constructions based on TPP-PRFs also admit such XOR-type functions and are therefore amenable to this attack. A brief description of the attack is given in Appendix A.

Obstacle to offline conversion and a way around it. For the above attack on PolyMAC, the calculation of both $g_1(x)=\mathrm{PolyMAC}(\beta_0,x)$ and $g_2(x\oplus\alpha_i)=\mathrm{PolyMAC}(\beta_1,x\oplus\alpha_i)$ require quantum access to PolyMAC. Thus, for XOR-type functions in which both components depend on the encryption oracle, including the PolyMAC instance above and those derived from BBB MACs [4], each Grover iteration of Shi et al.'s attack still requires quantum access to the encryption oracle.

This suggests looking for XOR-type functions whose queries to the encryption oracle can be decoupled from the Grover iterations. We next consider functions of the form

$$f(i,x)=g_1(x)\oplus p(x\oplus\alpha_i), \tag{2}$$

where p is a public function that can be computed offline and only g_1 requires access to the encryption oracle. We call this form a decoupled XOR-type function, or simply a p-XOR-type function. To simplify the presentation throughout the remainder of this work, we assume $\alpha_i=i$, so that $f(i,x)=g_1(x)\oplus p(x\oplus i)$.

Construction of p-XOR-type functions from TPP-PRFs. We show that TPP-PRFs can be used to construct p-XOR-type functions. A TPP-PRFs takes an n-bit input x and two parallel permutations P_1 and P_2, and is defined by $g(x)=l_{33}P_1\big(l_{13}(x)\oplus l_{14}(k_1)\big)\oplus l_{34}P_2\big(l_{23}(x)\oplus l_{24}(k_2)\big)\oplus e(x)\oplus C$, where $e(x)=l_{31}l_{11}(x)\oplus l_{32}l_{21}(x)$ and C is a key-dependent constant.

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

Table 1 Previous and new quantum attacks on SoEM22. #Query: queries to SoEM22. #Time: offline computation time. $0 < t < n$ in the Q2 model, and $0 < t \leqslant n/2$ in the Q1 model. The best results are in bold.

Algorithm	Model	Iteration	#Query	#Time	Qubit	Refs.
Grover-meets-Simon	Q2	$2^{n/2}$	$O(2^{n/2} \cdot n)$	$O(2^{n/2} \cdot n^3)$	$O(n^2)$	[2]
Dedicated attack	Q2	$2^{(n-t)/2}$	$O\big(2^{(n+t)/2} \cdot (n-t)\big)$	$O(2^{(n-t)/2} \cdot n^3)$	$\tilde{O}(2^t)$	[4], Ours
Offline dedicated attack	Q2	$2^{(n-t)/2}$	$\boldsymbol{O\big(2^t \cdot (n-t)\big)}$	$O(2^{(n-t)/2} \cdot n^3)$	$\tilde{O}(2^t)$	Ours
Offline Simon	Q1	$2^{2n/3}$	$O(2^{2n/3})$	$O(2^{2n/3} \cdot n^3)$	$O(n^2)$	[3, 5]
Offline dedicated attack	Q1	$2^{(2n-t)/3}$	$\boldsymbol{O(2^{(2n-t)/3})}$	$\boldsymbol{O(2^{(2n-t)/3} \cdot n^3)}$	$\tilde{O}(2^t)$	Ours

Based on this TPP-PRF, we construct the function

$$f(i,x) = g(x) \oplus e(x) \oplus l_{33}P_1\left(l_{13}(x)\right) \oplus l_{34}P_2\left(l_{23}(x \oplus i)\right), \quad (3)$$

which means $g_1(x) = g(x) \oplus e(x) \oplus l_{33}P_1(l_{13}(x))$ and $p(x \oplus i) = l_{34}P_2(l_{23}(x \oplus i))$. The function $f(i,x)$ 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 $i = l_{23}^{-1}l_{24}(k_2) \oplus l_{13}^{-1}l_{14}(k_1)$. Since i is XORed with x in the public function P_2, f is a p-XOR-type function.

To derive the form needed for the offline attack, we further apply Shi et al.'s truncation technique to (3) and obtain

$$F^{\mathcal{L}}(i^l, x^l) = \bigoplus_{u \in \mathcal{L}} f(i^l \| 0^t, x^l \| 0^t \oplus u) = G_1^{\mathcal{L}}(x^l) \oplus P^{\mathcal{L}}(i^l, x^l), \quad (4)$$

where $G_1^{\mathcal{L}}(x^l) = \bigoplus_{u \in \mathcal{L}} g_1(x^l \| 0^t \oplus u)$ and $P^{\mathcal{L}}(i^l, x^l) = \bigoplus_{u \in \mathcal{L}} p\big((x^l \oplus i^l) \| 0^t \oplus u\big)$. 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 $i^l = l_{23}^{-1}l_{24}k_2^l \oplus l_{13}^{-1}l_{14}k_1^l$.

Several block cipher constructions, including XopEM, SoEM22, SUMPIP, and DS-SoEM, are instantiations of TPP-PRFs. Thus, the above analysis yields the corresponding p-XOR-type functions and truncated conditional periodic functions for these constructions. The details are given in Appendix B.

Offline dedicated quantum attack on block ciphers based on TPP-PRFs. Based on (3) and (4), we adapt the offline Simon framework to Shi et al.'s attack to propose offline dedicated quantum attacks on TPP-PRF-based constructions in the Q1 and Q2 models. The key observation is that the decoupled property of p-XOR-type functions allows the superposition state $|\psi_{G_1^{\mathcal{L}}}\rangle = \bigotimes^{c'}\left(\sum_{x^l \in \{0,1\}^{n-t}} |x^l\rangle |G_1^{\mathcal{L}}(x^l)\rangle\right)$ to be prepared first, and the remaining computations become independent of the encryption oracle. Accordingly, our attack has two phases.

(1) Online phase: prepare the state $|\psi_{G_1^{\mathcal{L}}}\rangle$ requiring $O(2^n)$ classical queries in the Q1 model or $O\big(2^t \cdot (n-t)\big)$ quantum queries in the Q2 model.

(2) Offline phase: starting from the prepared state $|\psi_{G_1^{\mathcal{L}}}\rangle$, the test procedure is applied to $F^{\mathcal{L}}(i^l, x^l)$ to check whether it has a hidden period. After the test, the state $|\psi_{G_1^{\mathcal{L}}}\rangle$ is restored and can be reused in subsequent iterations.

The complete descriptions of two phases in the Q1 and Q2 models are provided in Appendix C. The complexity of the offline dedicated attack is summarized in Theorem 1.

Theorem 1. Let $f : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^m$ be a decoupled XOR-type function. There exists an offline dedicated quantum attack on block cipher constructions based on TPP-PRFs, which recovers $i_0^l \in \{0,1\}^{\kappa-t}$ with $O(2^{(\kappa-t)/2} \cdot n^3)$ time and $\tilde{O}(2^t)$ qubits, requiring $O(2^n)$ classical queries to the encryption oracle in the Q1 model, or $O(2^t \cdot (n-t))$ quantum queries in the Q2 model, where $0 < t < n$, $c' = n + \kappa - 2t + \tau + 1$.

Taking SoEM22 as an example, we construct the p-XOR-type function $f(i,x) = \mathsf{SoEM22}(x) \oplus P_1(x) \oplus P_2(x \oplus i)$, which satisfies $f(i,x) = f(i, x \oplus k_1)$ when $i = k_2$ or $i = k_2 \oplus k_1$.

In the Q2 model, we obtain $F^{\mathcal{L}}(i^l, x^l) = \bigoplus_{u \in \mathcal{L}} \mathsf{SoEM22}(x^l \| 0^t \oplus u) \oplus P_1(x^l \| 0^t \oplus u) \oplus P_2\left((x^l \oplus i^l) \| 0^t \oplus u\right)$, which has an $(n-t)$-bit period k_1^l when $i^l = k_2^l$ or $i^l = k_2^l \oplus k_1^l$. According to Theorem 1, we recover either k_2^l or $k_2^l \oplus k_1^l$ with $O\big(2^t \cdot (n-t)\big)$ quantum queries to the SoEM22 oracle and $O(2^{(n-t)/2} \cdot n^3)$ offline computation time.

In the Q1 model, we construct the function $F^{\mathcal{L}}(i^l \| j^{l_2}, x^{l_1}) = \bigoplus_{u \in \mathcal{L}} \mathsf{SoEM22}(x^{l_1} \| 0^{n-t-p} \| 0^t \oplus u) \oplus P_1(x^{l_1} \| j^{l_2} \| 0^t \oplus u) \oplus P_2\Big(\big((x^{l_1} \| 0^{n-t-p}) \oplus i^l\big) \| 0^t \oplus u\Big)$, which has a p-bit period $k_1^{l_1}$ when $i^l \| j^{l_2} = k_2^l \| k_1^{l_2}$ or $i^l \| j^{l_2} = k_2^l \oplus (k_1^{l_1} \| 0^{n-t-p}) \| k_1^{l_2}$. We can recover one of $k_2^l \| k_1^{l_2}$ and $k_2^l \oplus (k_1^{l_1} \| 0^{n-t-p}) \| k_1^{l_2}$ by applying Theorem 1, requiring $O(2^{p+t})$ classical queries to the SoEM22 oracle and $O(2^{(2n-2t-p)/2} \cdot n^3)$ offline computation time. Let D be the number of classical queries and T be the offline computation time. This attack achieves a tradeoff of $T^2D = 2^{2n-t}$, which is balanced at $T = D = \tilde{O}(2^{(2n-t)/3})$ for $0 < t \leqslant n/2$. The remaining key bits can be recovered using the offline Simon's algorithm with negligible additional cost.

A comparison with previous attacks on SoEM22 is given in Table 1. The offline dedicated attacks on general TPP-PRFs are presented in Appendix D.

Conclusion. In this work, we identified PolyMAC and block cipher constructions based on TPP-PRFs as new instances vulnerable to dedicated quantum attacks. By defining a decoupled XOR-type function, we further proposed offline dedicated quantum attacks on constructions based on TPP-PRFs, with lower query complexity than previous attacks in both the Q1 and Q2 models. Our results provide new insights into the quantum security of block ciphers based on pseudorandom functions and motivate further investigation into more generic and effective offline dedicated quantum attacks applicable to other cryptographic structures.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. U25B2014, 62372048, 62272056, 62371069).

Supporting information Appendixes A–D. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Simon D. R. On the power of quantum computation. In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, 1994. 116–123
2 Leander G, May A. Grover meets Simon-quantumly attacking the FX-construction. In: Proceedings of International Conference on the Theory and Application of Cryptology and Information Security, Hong Kong, 2017. 161–178
3 Bonnetain X, Hosoyamada A, Naya-Plasencia M, et al. Quantum attacks without superposition queries: the offline Simon's algorithm. In: Proceedings of International Conference on the Theory and Application of Cryptology and Information Security, Kobe, 2019. 552–583
4 Shi T, Wu W, Hu B, et al. Dedicated quantum attacks on XOR-type function with applications to beyond-birthday- bound MACs. IEEE Trans Inform Forensic Secur, 2024, 19: 5971–5984
5 Sun H W, Gao F, Xu R X, et al. Quantum key-recovery attacks on permutation-based pseudorandom functions. IEEE Internet Things J, 2025, 12: 35692–35704