Errata for Proceedings of Central European Conference on Cryptology CECC '22

Karol Nemoga Roderik Ploszek Pavol Zajac

July 5, 2022

Contents

Introduction

This document contains errata for the Proceedings of Central European Conference on Cryptology CECC '22. Corrected submissions are presented in full form. The list of corrections follows.

1. **Recent Advances in Fully Homomorphic Encryption** by *Kamil Kluczniak* — last paragraph of the original submission was removed.
2. **Superposition Attacks on Pseudorandom Schemes based on Two or Less Permutations** by *Shaoxuan Zhang*, *Chun Guo* and *Qingju Wang* — corrected author affiliations.

Recent Advances in Fully Homomorphic Encryption

Kamil Kluczniak
CISPA Helmholtz Center for Information Security
kamil.kluczniak@cispa.de

Fully homomorphic encryption (FHE) is an encryption scheme that allows performing arbitrary computation on encrypted data. In particular, a client encrypts a message m and sends the ciphertext to a server which, given a function F, returns another ciphertext that decrypts to $F(m)$. The concept of fully homomorphic encryption was first introduced by Rivest, and Dertouzos [16]. The first theoretical realization of that concept is due to Gentry [10].

Circuit Private Fully Homomorphic Encryption. A critical property for fully homomorphic encryption is circuit privacy. Roughly speaking, the ciphertext that is the product of the server computing a function F on encrypted data should not reveal any information on the function F except that the ciphertext decrypts to $F(m)$. In more technical terms, to prove circuit privacy, we need to show a simulator that, on input $F(m)$, outputs a fresh encryption of $F(m)$, which is indistinguishable from the servers' computed ciphertext. In particular, the distribution of an evaluated ciphertext should be close or the same as the distribution of a fresh encryption.

We can easily see that circuit private fully-homomorphic encryption gives us semi-honest two-party computation with optimal communication. Namely, we only need one round of communication. The first message can be reused, and the communication complexity is independent of the size of the computation. Furthermore, for so-called multi-hop fully homomorphic encryption schemes, which is the focus of this paper, we can reuse the ciphertexts output from the evaluation process and keep computing on them.

Surprisingly, despite over a decade of advances in constructing scalable fully homomorphic encryption schemes [11, 4, 3, 12, 1, 13, 5, 2, 14, 8, 7, 6, 15], and numerous implementations there is very little constructions and nearly no implementation that we are aware of that natively provides circuit privacy. We believe that the current state of practical circuit private FHE can be attributed to the shortcomings in currently available methods to achieve circuit private FHE.

Applications. Since circuit private FHE gives us two-party computation, all applications for two-party computation protocols apply here as well. Among other these are private set intersection, neural network inference or analysis on genomic data.

We note that circuit privacy is not always needed. Without circuit privacy FHE reduces to secure delegation. For example, in (single-server) private information retrieval protocol (PIR) we are only interested in protecting the user's query, but not in the confidentiality of a potentially large database of the server. Since we don't protect the database, a trivial solution is to publish the database. In PIR protocols, the goal, however, is to reduce communication complexity while protecting the users' queries.

On the other hand, we believe that for neural network inference, the confidentiality of the model is essential. In contrast to PIR, it is difficult to make an argument for compressing the communication costs, as current FHE schemes require sending public keys that are much larger than the size of the models that these FHE schemes are practically able to evaluate. While there is a multitude of proposals to use FHE for neural network inference, to the best of our knowledge, there is no proposal that provably guarantees the secrecy of the model.

A Trivial Attack. We note that the evaluation process in most FHE implementations is deterministic. Thus the most trivial attack is to guess the circuit, perform the evaluation and check whether the servers output ciphertext matches the locally computed ciphertext. This

attack can be run even without knowledge of the secret key. We stress, however, that even when the evaluation process is randomized, the question of whether it is circuit private or not is not immediately clear for many encryption schemes because the distribution of the ciphertext may hugely differ from the distribution of a freshly chosen ciphertext and may still leak non-trivial information on the computation. For example, all currently known FHE schemes have noisy ciphertexts. This noise hidden from the server may depend on the evaluated circuit, thus leaking information to the client.

The Talk. In this talk we will discuss our recent research on circuit private fully homomorphic encryption schemes. In particular, we design randomized bootstrapping algorithms that can sanitize a given ciphertext. We refer to our suit of bootstrapping algorithms as Simul-E. Consequently, we obtain circuit privacy by running our bootstrapping before returning a ciphertext to the client. To evaluate a circuit, we can use any other FHE scheme that has ciphertexts represented as learning with errors samples, given that the scheme computes correctly with high probability. Additionally, our bootstrapping can be programmed, and aside from re-encrypting a ciphertext, it can compute a function on the underlying ciphertext along the way. In contrast to the washing machine method, [9] that requires to run bootstrapping multiple times, we only need to apply Simul-E once. We give a tight error analysis, propose parameters and provide several optimizations. Finally, we implement our schemes in C++ and give performance tests. To the best of our knowledge, this is the first realization of a FHE scheme that is designed, instantiated and implemented to support circuit privacy, and which does not use noise flooding.

References

[1] Jacob Alperin-Sheriff and Chris Peikert. Practical bootstrapping in quasilinear time. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part I*, volume 8042 of *LNCS*, pages 1–20. Springer, Heidelberg, August 2013.

[2] Jacob Alperin-Sheriff and Chris Peikert. Faster bootstrapping with polynomial error. In Juan A. Garay and Rosario Gennaro, editors, *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 297–314. Springer, Heidelberg, August 2014.

[3] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (Leveled) fully homomorphic encryption without bootstrapping. In Shafi Goldwasser, editor, *ITCS 2012*, pages 309–325. ACM, January 2012.

[4] Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. In Rafail Ostrovsky, editor, *52nd FOCS*, pages 97–106. IEEE Computer Society Press, October 2011.

[5] Zvika Brakerski and Vinod Vaikuntanathan. Lattice-based FHE as secure as PKE. In Moni Naor, editor, *ITCS 2014*, pages 1–12. ACM, January 2014.

[6] Hao Chen and Kyoohyung Han. Homomorphic lower digits removal and improved FHE bootstrapping. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part I*, volume 10820 of *LNCS*, pages 315–337. Springer, Heidelberg, April / May 2018.

[7] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *ASIACRYPT 2016, Part I*, volume 10031 of *LNCS*, pages 3–33. Springer, Heidelberg, December 2016.

[8] Léo Ducas and Daniele Micciancio. FHEW: Bootstrapping homomorphic encryption in less than a second. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part I*, volume 9056 of *LNCS*, pages 617–640. Springer, Heidelberg, April 2015.

[9] Léo Ducas and Damien Stehlé. Sanitization of FHE ciphertexts. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part I*, volume 9665 of *LNCS*, pages 294–310. Springer, Heidelberg, May 2016.

[10] Craig Gentry. Fully homomorphic encryption using ideal lattices. In Michael Mitzenmacher, editor, *41st ACM STOC*, pages 169–178. ACM Press, May / June 2009.

[11] Craig Gentry and Shai Halevi. Fully homomorphic encryption without squashing using depth-3 arithmetic circuits. In Rafail Ostrovsky, editor, *52nd FOCS*, pages 107–109. IEEE Computer Society Press, October 2011.

[12] Craig Gentry, Shai Halevi, and Nigel P. Smart. Better bootstrapping in fully homomorphic encryption. In Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors, *PKC 2012*, volume 7293 of *LNCS*, pages 1–16. Springer, Heidelberg, May 2012.

[13] Craig Gentry, Amit Sahai, and Brent Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part I*, volume 8042 of *LNCS*, pages 75–92. Springer, Heidelberg, August 2013.

[14] Shai Halevi and Victor Shoup. Bootstrapping for HElib. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part I*, volume 9056 of *LNCS*, pages 641–670. Springer, Heidelberg, April 2015.

[15] Shai Halevi and Victor Shoup. Bootstrapping for HElib. *Journal of Cryptology*, 34(1):7, January 2021.

[16] RL Rivest, L Adleman, and ML Dertouzos. On data banks and privacy homomorphisms. foundations of secure computation (1978), 169–180. *Search in*, 1978.

Superposition Attacks on Pseudorandom Schemes based on Two or Less Permutations

Shaoxuan Zhang[1,2] Chun Guo[1,2,3](✉) and Qingju Wang[4](✉)

[1] School of Cyber Science and Technology, Shandong University
[2] Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University
[3] State Key Laboratory of Information Security (Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093)
[4] SnT, University of Luxembourg
shaoxuanzhang@mail.sdu.edu.cn,chun.guo@sdu.edu.cn,qjuwang@gmail.com

1 Introduction

A remarkable trend in cryptography is the development of constructions built upon *(public) keyless cryptographic permutations*. The approach of using two permutations has appeared as the best trade-off between efficiency and security.

We study quantum superposition attacks against permutation-based pseudorandom cryptographic schemes. In particular, we propose key recovery attacks against two Permutation-based PseudoRandom cryptographic schemes using the improved Grover-meet-Simon method of Bonnetain et al., with $O(n)$ superposition queries and $O(n2^{n/2})$ quantum steps. Our attacks are applicable to 2-round (tweakable) Even-Mansour ciphers and recently proposed permutation-based PRFs PEDM and SoKAC1. From a constructive perspective, our results establish new quantum Q2 security upper bounds for two permutation-based pseudorandom schemes as well as sound design choices.

2 Notation

We introduce some of the notation we will use through the rest of the paper: For two bit strings X, Y (of any length), we denote by $X||Y$ their concatenation. $\oplus$ denote bitwise XOR.

3 Main Results

We first formally define our model for two-permutation-based pseudorandom (TPPR) schemes. Formally, let P_1, P_2 be two n-bit permutations. For a 3×3 matrix A of the form

$$\mathsf{A} = \begin{pmatrix} a_{00} & a_{01} & 0 \\ a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \end{pmatrix}, \tag{1}$$

with $a_{ij} \in \mathbb{F}_2^n$. The keyed function $\mathsf{F2P}_{\mathsf{A},\mathbf{k}}^{P_1,P_2} : \{0,1\}^{3n} \times \{0,1\}^n \to \{0,1\}^n$ is defined as

$$\begin{aligned} \mathsf{F2P}_{\mathsf{A},\mathbf{k}}^{P_1,P_2}(x) = z, \text{ where } & y_1 \leftarrow P_1(a_{00}k_1 \oplus a_{01}x), \\ & y_2 \leftarrow P_2(a_{10}k_2 \oplus a_{11}x \oplus a_{12}y_1), \\ & z \leftarrow a_{20}k_3 \oplus a_{21}x \oplus a_{22}y_1 \oplus y_2. \end{aligned} \tag{2}$$

where multiplications are on the finite field $\mathbb{F}_2^n$. The function $\mathsf{F2P}_{\mathsf{A},\mathbf{k}}^{P_1,P_2}$ is depicted in Fig. 1. This in particular includes the 2-round Even-Mansour, the SoEM PRF, the SoKAC1 PRF, and the PEDM PRF.

An initial observation is that the final operation of XORing $a_{21}x$ has no influence on key recovery security since x is public, and we can always define $\mathsf{F2P}_{\mathsf{A},\mathbf{k}}^{P_1,P_2\prime}(x) := \mathsf{F2P}_{\mathsf{A},\mathbf{k}}^{P_1,P_2}(x) \oplus a_{21}x$ as the target of the attack. For the remaining parameters, our conclusion in short is that *to have "non-trivial" quantum Q2 security, it is necessary to have* $Bo(a_{10})Bo(a_{12}) + Bo(a_{10})Bo(a_{22})Bo(a_{11}) = 1$, *where the indicator function* $Bo(a_{ij}) = 0$ *if* $a_{ij} = 0$ *and* $Bo(a_{ij}) = 1$ *otherwise*. Our concrete discussions are as follows.

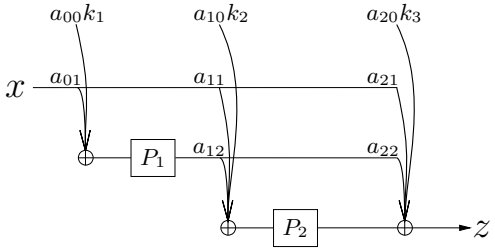

Fig. 1: The two permutation-based keyed function $\mathsf{F}_{\mathbf{A},\mathbf{k}}$ of Eq. (2).

3.1 Fully Degenerated Cases and Attacks using Simon's Algorithm

We first identify "fully degenerated" TPPR schemes, i.e., those provide no Q2 security at all due to Simon's algorithm. For simplicity, we write $a_{ij}^{-1} = 0$ when $a_{ij} = 0$.

Case 1: $Bo(a_{01}) = 0$ Then the P_1 invocation does not depend on x at all, and the construction becomes

$$\mathsf{F2P}^{P_1,P_2}_{\mathbf{A},\mathbf{k}}(x) = P_2(a_{12}P_1(a_{00}k_1) \oplus a_{11}x \oplus a_{10}k_2) \oplus a_{22}P_1(a_{00}k_1) \oplus a_{20}k_3.$$

Let $k_2' = a_{12}P_1(a_{00}k_1) \oplus a_{10}k_2$, $k_3' = a_{22}P_1(a_{00}k_1) \oplus a_{20}k_3$. Then the scheme becomes $\mathsf{F2P}^{P_1,P_2}_{\mathbf{A},\mathbf{k}}(x) = P_2(k_2' \oplus a_{11}x) \oplus k_3'$, and it again collapses to the EM construction.

Case 2: Other Degenerated Cases

1. when $(\overline{Bo(a_{10})}+\overline{Bo(a_{11})})\overline{Bo(a_{12})}\ \overline{Bo(a_{22})} = 1$, the construction provides no security even in the classical setting. In detail, when $\overline{Bo(a_{12})} = \overline{Bo(a_{22})} = 1$, the scheme becomes $\mathsf{F2P}^{P_1,P_2}_{\mathbf{A},\mathbf{k}}(x) = P_2(a_{11}x \oplus a_{10}k_2) \oplus a_{20}k_3$.
   - when $\overline{Bo(a_{10})} = 1$, the scheme becomes $\mathsf{F2P}^{P_1,P_2}_{\mathbf{A},\mathbf{k}}(x) = P_2(a_{11}x) \oplus a_{20}k_3$, we can recover k_3 by $a_{20}^{-1}(\mathsf{F2P}^{P_1,P_2}_{\mathbf{A},\mathbf{k}}(x) \oplus P_2(a_{11}x)) = k_3$;
   - when $\overline{Bo(a_{11})} = 1$, the scheme $\mathsf{F2P}^{P_1,P_2}_{\mathbf{A},\mathbf{k}}(x) = P_2(a_{10}k_2) \oplus a_{20}k_3$ is a constant, which is also trivially insecure.
2. when $\overline{Bo(a_{10})}(\overline{Bo(a_{12})}Bo(a_{22})+\overline{Bo(a_{11})}Bo(a_{12}))+Bo(a_{10})\overline{Bo(a_{12})}(Bo(a_{11})\oplus Bo(a_{22})) = 1$, the scheme again collapses to the EM construction.
3. when $\overline{Bo(a_{00})}(\overline{Bo(a_{12})} \oplus \overline{Bo(a_{11})}) = 1$, the scheme again collapses to the EM construction.

The remaining cases appear resisting Simon's algorithm and will be addressed in the subsequent sections.

3.2 Cascaded Constructions with unkeyed Davies-Meyer

In this section, we identify the "partially degenerated" cascaded constructions with unkeyed Davies-Meyer (CUDM). Such constructions could be viewed as cascading a single permutation-based keyed "round function" and a variant of the (keyless) Davies-Meyer construction. The permutation invocation in the Davies-Meyer is somewhat "wasted" due to the non-secrecy. Though, no periodicity can be exhibited.

Subcase 1: Keyed round comes first. By "keyed round comes first", it means the function is defined as

$$\mathsf{CUDM1}^{P_1,P_2}_{k_1}(x) := P_2(a_{12}P_1(a_{01}x \oplus a_{00}k_1) \oplus a_{11}x) \oplus a_{22}P_1(a_{01}x \oplus a_{00}k_1),$$

where $Bo(a_{00}), Bo(a_{01}), Bo(a_{11}), Bo(a_{12}), Bo(a_{22}) \neq 0$. The simplest variant has all the constants equal 1, and is depicted in Fig. 2.

For simplicity, define $\mathrm{DMx}^{P_2}(u) := P_2(a_{12}u) \oplus a_{22}u$. Then we have $\mathsf{CUDM1}^{P_1,P_2}_{k_1}(x) \oplus a_{22}a_{12}^{-1}a_{11}x = \mathrm{DMx}^{P_2}\big(P_1(a_{01}x \oplus a_{00}k_1) \oplus a_{12}^{-1}a_{11}x\big)$. For our attack, we seek for $x, u \in \{0,1\}^n$ such that $\mathsf{CUDM1}^{P_1,P_2}_{k_1}(x) \oplus$

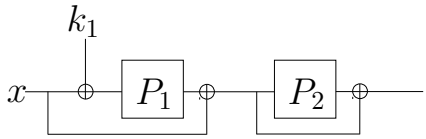

Fig. 2: Simplest variant of the function $\mathsf{CUDM1}_{k_1}^{P_1,P_2}$.

$a_{22}a_{12}^{-1}a_{11}x = \mathrm{DMx}^{P_2}(u)$. Once such a pair is found, it might indicate $P_1(a_{01}x \oplus a_{00}k_1) \oplus a_{12}^{-1}a_{11}x = u$, and k_1 is recovered by $k_1 = a_{00}^{-1}\big(P_1^{-1}(a_{12}^{-1}a_{11}x \oplus u) \oplus a_{01}x\big)$. Define $h : \{0,1\} \times \{0,1\}^n \to \{0,1\}^n$ such that $h(0\|x) := \mathsf{CUDM1}_{k_1}^{P_1,P_2}(x) \oplus a_{22}a_{12}^{-1}a_{11}x$ and $h(1\|x) := \mathrm{DMx}^{P_2}(x)$. Then, we can apply [2, Algorithm 4] to find a collision $h(b\|x) = h(b'\|u)$. As long as the pair $\big((b\|x),(b'\|u)\big)$ returned by [2, Algorithm 4] has $b \neq b'$, we obtain the desired collision $\mathsf{CUDM1}_{k_1}^{P_1,P_2}(x) \oplus a_{22}a_{12}^{-1}a_{11}x = \mathrm{DMx}^{P_2}(u)$. The attacker then outputs $k_1 = a_{00}^{-1}\big(P_1^{-1}(a_{12}^{-1}a_{11}x \oplus u) \oplus a_{01}x\big)$ as the key. The complexities are the same as Chailloux et al., i.e., $O(n)$ qubits, $O(2^{2n/5})$ quantum steps, and $O(2^{n/5})$ classical memory. This remains faster than the naïve Grover key search (which needs $O(2^{n/2})$ quantum steps).

Subcase 2: Davies-Meyer comes first. When $Bo(a_{00}) = 0$ and further $Bo(a_{12})Bo(a_{11}) \neq 0$, let $k_2' = a_{10}k_2$, $k_3' = a_{20}k_3$. Then the input to P_1 is not secret, and the scheme becomes CUDM with "Davies-Meyer coming first". In detail, the function is defined as

$$\mathsf{CUDM2}_{k_2,k_3}^{P_1,P_2}(x) := P_2\big(a_{12}P_1(a_{01}x) \oplus a_{11}x \oplus k_2'\big) \oplus k_3'.$$

Let $u = P_1(a_{01}x) \oplus a_{12}^{-1}a_{11}x$, then we have $\mathsf{CUDM2}_{k_2,k_3}^{P_1,P_2}(x) = \mathsf{EMx}_{k_2',k_3'}^{P_2}(u) := P_2(a_{12}u \oplus k_2') \oplus k_3'$. While $\mathsf{EMx}_{k_2',k_3'}^{P_2}$ is a variant of the Even-Mansour cipher with known periodic properties for Simon's algorithm, the interesting observation is that the keyless "first round" function $x \mapsto P_1(a_{01}x) \oplus a_{12}^{-1}a_{11}x$ is unlikely injective, and this effectively destroys the periodic properties for applying Simon's algorithm.

On the other hand, the idea of Kuwakado and Morii's attack [6] remains exploitable. Concretely, note that the periodic property of the "second round"

$$u = u' \oplus a_{12}^{-1}k_2 \Leftrightarrow P_2(a_{12}u \oplus k_2') \oplus k_3' \oplus P_2(u) = P_2(a_{12}u' \oplus k_2') \oplus k_3' \oplus P_2(u')$$

can be naturally extended to

$$\begin{aligned} &a_{12}P_1(a_{01}x) \oplus a_{11}x = a_{12}P_1(a_{01}x') \oplus a_{11}x' \oplus k_2' \\ \Rightarrow\ &\mathsf{CUDM2}_{k_2,k_3}^{P_1,P_2}(x) \oplus P_2(a_{12}P_1(a_{01}x) \oplus a_{11}x) = \mathsf{CUDM2}_{k_2,k_3}^{P_1,P_2}(x') \oplus P_2(a_{12}P_1(a_{01}x') \oplus a_{11}x'). \end{aligned} \tag{3}$$

With this in mind, define $h(x) := \mathsf{CUDM2}_{k_2,k_3}^{P_1,P_2}(x) \oplus P_2(a_{12}P_1(a_{01}x) \oplus a_{11}x)$. Then, once we observe $h(x) = h(x')$, it might hold $a_{12}P_1(a_{01}x) \oplus a_{11}x = a_{12}P_1(a_{01}x') \oplus a_{11}x' \oplus k_2'$, in which case k_2' could be recovered by $k_2' = a_{12}P_1(a_{01}x) \oplus a_{11}x \oplus a_{12}P_1(a_{01}x') \oplus a_{11}x'$. Using a quantum collision searching algorithm [2, Algorithm 4], this can be achieved within $O(2^{2n/5})$ quantum queries and $O(2^{2n/5})$ quantum steps.

3.3 The Non-degenerated Case and Its Grover-meet-Simon Attack

When (and only when) $Bo(a_{10})Bo(a_{12}) + Bo(a_{10})Bo(a_{22})Bo(a_{11}) = 1$, the best key recovery attack we found is based on the Grover-meet-Simon algorithm. We call such cases non-degenerated.

In detail, we define $g(k,u) = P_2(a_{12}P_1(a_{01}u) \oplus a_{11}u \oplus k) \oplus a_{22}P_1(a_{01}u)$, $\mathsf{F2P}_{\mathsf{A},\mathbf{k}}^{P_1,P_2} = P_2(a_{12}P_1(a_{01}x \oplus a_{00}k_1) \oplus a_{11}x \oplus a_{10}k_2) \oplus a_{22}P_1(a_{01}x \oplus a_{00}k_1) \oplus a_{20}k_3$, and further

$$f'(x) = \mathsf{F2P}_{\mathsf{A},\mathbf{k}}^{P_1,P_2}(x) \oplus \mathsf{F2P}_{\mathsf{A},\mathbf{k}}^{P_1,P_2}(x \oplus 1), \qquad g'(k,x) = g(k,x) \oplus g(k,x \oplus 1)$$

Then,

$$f'(x) \oplus g'(k',x) = f'(x \oplus a_{01}^{-1}a_{00}k_1) \oplus g'(k', x \oplus a_{01}^{-1}a_{00}k_1)$$

holds with $k' = a_{10}k_2 \oplus a_{11}a_{01}^{-1}a_{00}k_1$, i.e., $f'(x) \oplus g'(k',x)$ has a period $a_{01}^{-1}a_{00}k_1$. Thus we can recovering $\mathbf{k}$ using Bonnetain et al.'s algorithm Alg-PolyQ2 [1], the attack proceeds as follows.

1. Run Algorithm Alg-PolyQ2 in [1] for the above f' and g' to recover k'.
2. Apply Simon's algorithm to $f'(x) \oplus g'(k', x)$ to recover k_1.
3. Compute the two involved secret keys $a_{10}k_2 = k' \oplus a_{11}a_{01}^{-1}a_{00}k_1$ and $a_{20}k_3 = \mathsf{F2P}^{P_1,P_2}_{\mathsf{A},\mathbf{k}}(0^n) \oplus P_2(a_{12}P_1(a_{00}k_1) \oplus a_{10}k_2) \oplus a_{22}P_1(a_{00}k_1)$.

Our results are summarized in Table 1.

Table 1. Summary of our results. $\mathsf{SoEM}^{P_1,P_2}_{\nu_1,\nu_2}$ [4], $\mathsf{SoKAC1}^{P}_{\nu_1,\nu_2}$ [4,3] and $\mathsf{PEDM}^{P}_{\nu_1,\nu_2}$ [5] are recently proposed PRFs built upon two public permutation invocations.

Condition	Quantum queries	Quantum steps	Classical steps	Examples
$Bo(a_{01}) = 0$	$O(n)$	$O(n)$	$O(n^3)$	Even-Mansour
$(\overline{Bo(a_{10})} + \overline{Bo(a_{11})})\overline{Bo(a_{12})}\ \overline{Bo(a_{22})} = 1$	no security	no security	no security	
$\overline{Bo(a_{10})}(\overline{Bo(a_{12})}Bo(a_{22}) + \overline{Bo(a_{11})}Bo(a_{12})) +$ $Bo(a_{10})\overline{Bo(a_{12})}(Bo(a_{11}) \oplus Bo(a_{22})) = 1$	$O(n)$	$O(n)$	$O(n^3)$	Even-Mansour
$\overline{Bo(a_{00})}(\overline{Bo(a_{12})} \oplus \overline{Bo(a_{11})}) = 1$	$O(n)$	$O(n)$	$O(n^3)$	Even-Mansour
$\mathsf{CUDM1}^{P_1,P_2}_{k_1}$ (x)	$O(2^{2n/5})$	$O(2^{2n/5})$	$O(2^{2n/5})$	
$\mathsf{CUDM2}^{P_1,P_2}_{k_2,k_3}$ (x)	$O(2^{2n/5})$	$O(2^{2n/5})$	$O(2^{2n/5})$	
$Bo(a_{10})Bo(a_{12}) + Bo(a_{10})Bo(a_{22})Bo(a_{11}) = 1$	$O(n2^{n/2})$	$O(n2^{n/2})$	$O(n^3 2^{n/2})$	$\mathsf{SoEM}^{P_1,P_2}_{\nu_1,\nu_2}$ $\mathsf{SoKAC1}^{P}_{\nu_1,\nu_2}$ $\mathsf{PEDM}^{P}_{\nu_1,\nu_2}$ 2-round (tweakable) Even-Mansour

4 Conclusions

We study superposition attacks against pseudorandom schemes built upon n-bit keyless permutations. Using the recently proposed improved Grover-meet-Simon algorithm, we exhibit key recovery attacks against all "full-domain" pseudorandom schemes built upon two permutations, with $O(n^2)$ quantum data and $O(n^3 2^{n/2})$ quantum computations. We also identify certain weak designs and exhibit faster attacks using either Simon's algorithm or quantum collision searching. Our attacks are applicable to a number of popular permutation-based schemes. On the other hand, our results also clarify necessary conditions for "non-trivial" quantum Q2 security within two permutations.

References

1. Bonnetain, X., Hosoyamada, A., Naya-Plasencia, M., Sasaki, Y., Schrottenloher, A.: Quantum attacks without superposition queries: The offline Simon's algorithm. In: Galbraith, S.D., Moriai, S. (eds.) ASIACRYPT 2019, Part I. LNCS, vol. 11921, pp. 552–583. Springer, Heidelberg (Dec 2019)
2. Chailloux, A., Naya-Plasencia, M., Schrottenloher, A.: An efficient quantum collision search algorithm and implications on symmetric cryptography. In: Takagi, T., Peyrin, T. (eds.) ASIACRYPT 2017, Part II. LNCS, vol. 10625, pp. 211–240. Springer, Heidelberg (Dec 2017)
3. Chakraborti, A., Nandi, M., Talnikar, S., Yasuda, K.: On the composition of single-keyed tweakable Even-Mansour for achieving BBB security. IACR Trans. Symm. Cryptol. 2020(2), 1–39 (2020)
4. Chen, Y.L., Lambooij, E., Mennink, B.: How to build pseudorandom functions from public random permutations. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019, Part I. LNCS, vol. 11692, pp. 266–293. Springer, Heidelberg (Aug 2019)
5. Dutta, A., Nandi, M., Talnikar, S.: Permutation based edm: An inverse free bbb secure prf. IACR Transactions on Symmetric Cryptology 2021(2), 31–70 (Jun 2021), https://tosc.iacr.org/index.php/ToSC/article/view/8905
6. Kuwakado, H., Morii, M.: Security on the quantum-type even-mansour cipher. In: Proceedings of the International Symposium on Information Theory and its Applications, ISITA 2012, Honolulu, HI, USA, October 28-31, 2012. pp. 312–316 (2012), https://ieeexplore.ieee.org/document/6400943/