A Note on Isogeny Group Action-Based Pseudorandom Functions

Yi-Fu Lai

Ruhr-Universität Bochum

Yi-Fu.Lai@rub.de

December 18, 2024

Abstract

In PKC'24, de Saint Guilhem and Pedersen give a pseudorandom function basing on a relaxed group action assumption in the semi-honest setting. Basing on the assumption, they build an oblivious pseudorandom function (OPRF). Later, a recent paper by Levin and Pedersen uses the same function to build a verifiable random function (VRF), using the same assumption.

We give a structural attack on this problem by reducing it to a few group action inverse problems (GAIP/DLog) over small subgroups. This reduction allows us to apply a CRT-based attack to recover the secret key, ultimately lowering the problem's effective security strength to under 70 classical bits when using CSIDH-512. Hence the strength of their pseudorandom functions is bounded above by the GAIP over the largest prime order subgroup. Clearly, Kuperberg's subexponential attack can be used to further reduce its quantum security.

1 Introduction

In [DP24], de Saint Guilhem and Pedersen introduce a pseudorandom function (PRF) basing on a relaxed group action assumption, which they then use to construct an oblivious pseudorandom function

Later, Levin and Pedersen [LP24] recently extended their work to address the limitations of feasible yet slow verifiable random functions (VRFs) in the group action literature [Lai24], resulting in a few new VRF constructions.

2 Preliminary

Notations. Let $\mathbb{Z}_N$ denote the quotient $\mathbb{Z}/N\mathbb{Z}$.

Definition 2.1 (Group Action Inverse Problem (GAIP)). *Let $\Pi = (\mathcal{X}, G, \star)$ be a group action tuple where G acts on the set $\mathcal{X}$ by the action $\star$. Given $(E, E') \in \mathcal{X}^2$ where $E' = s \star E$ and $s \xleftarrow{\$} G$, the* group action inverse problem *over Π is to find $[s'] \in G$ such that $s' \star E_0 = E'$.*

CSIDH Group Action. Let $(E_0, \mathcal{X}, \mathbb{Z}_N, \star)$ denote a group action, where G acts on $\mathcal{X}$ by a computationally feasible action $\star$ and the group order N is known. Write $N = p_1 \times \cdots \times p_n \approx 2^{256}$ where $p_1, \cdots, p_n$ are distinct odd primes and in an increasing order. Concretely, in CSIDH-512 we have

$$N = 3 \times 37 \times 1407181 \times 51593604295295867744293584889 \\ \times 315994145046819958530082787455878322049 09,$$

where log_2 value of each prime is approximately $2, 6, 21, 96, 134$.

3 The Group-Action Differential Attack

Formally, [DP24, LP24] base their constructions on the following problem for their pseudorandom functions.

Problem 1. Let $f(x)$ be a secret polynomial chosen over $\mathbb{Z}_N$. The adversary $\mathcal{A}$ is given access to an oracle, which on input $m \in \mathbb{N}$ and coprime with N outputs $[f(m)] \star E_0$. We say $\mathcal{A}$ breaks the problem if $\mathcal{A}$ outputs a pair $(m', [f(m')] \star E0)$ where m' has not been queried before.

To be more specific, the OPRF of [DP24] in the *semi-honest* setting takes any input over $\mathbb{Z}_N^\times$ while in the malicious setting, the input space is taken to be over a prime-order subgroup, where our reduction is NOT applicable.

In the abovementioned works, the secret polynomial $f(x)$ is chosen to of degree between 1 to 3. Inspired by the cryptoanalysis in the work [KLLQ23], we show how to reduce the problem to a group action inverse problem over a smaller group. The key observation is that for any polynomial $f(x) \in R[x]$ over a ring R, we always have $X - Y | f(X) - f(Y)$.

Case $\deg(f) = 1$**.** Let $f(x) = ax + b$ be the secret polynomial. The adversary's reduction proceeds as follows.

1. Take $m_1 = 1, m_2 = 1 + p_n, m_3 = 1 + p_{n-1} \in \mathbb{N}$ as input for the oracle and obtain $E_1 = [f(m_1)] \star E_0$, $E_2 = [f(m_2)] \star E_0$ and $E_3 = [f(m_3)] \star E_0$.
2. Solve for the group action inverse problems between E_1, E_2 and between E_1, E_3 over the group $p_n \cdot \mathbb{Z}_N$ and $p_{n-1} \cdot \mathbb{Z}_N$ respectively. We obtain $a \pmod{N/p_n}$ and $a \pmod{N/p_{n-1}}$.
3. By using CRT, we can recover $a \pmod{N}$.
4. Since a has been recover, the adversary is able to evaluate $f(k) \star E_0$ for any $k \in \mathbb{N}$ by itself.

Remark 3.1. We can take $m_3 = p_1 \times \cdots \times p_{n-1} + 1$. This makes the costs of 2 group action inverse problems approximately the same.

Case $\deg(f) = 3$**.** Let $f(x) = ax^3 + bx^2 + cx + d$ be the secret polynomial. Write $N = p_1 \times \cdots \times p_n$ where $p_1, \cdots, p_n$ are distinct odd primes and in an increasing order. The attacks proceeds as follows.

1. Take $m_1 = 1, m_{2,i} = 1 + h_{2,i} \cdot p_n, m_{3,i} = 1 + h_{3,i} \cdot p_{n-1} \in \mathbb{N}$ as input for the oracle and obtain $E_1 = [f(m_1)] \star E_0 \cdots, E_{3,i} = [f(m_{3,i})] \star E_0$ for $i \in [3]$ where elements in $\{h_{2,i}\}$ are distinct and so are those in $\{h_{3,i}\}$.
2. Solve for the group action inverse problems between the pairs $\{(E_1, E_{2,i})\}_{i\in[3]}$ and $\{(E_1, E_{3,i})\}_{i\in[3]}$ over the group $p_n \cdot \mathbb{Z}_N$ and $p_{n-1} \cdot \mathbb{Z}_N$ respectively. Then, by using 3 linear equations and solving for 3 variables, we obtain $a, b, c \pmod{N/p_n}$ and $a, b, c \pmod{N/p_{n-1}}$.
3. By using CRT, we can recover $a, b, c \pmod{N}$.

4 Conclusion

We reduce Problem 1 to a group action inverse problem where the group size is the largest prime order subgroup of G. In their setting, the size is of 134-bits. Hence, the classical security level of the semi-honest OPRF in [DP24] and the VRF in [LP24] are less than 70 bits. The subexponential-time quantum algorithm [Kup05] will take less than that. We remark that the attack does not affect the proof systems developed in [DP24] and the other VRF construction in [LP24].

Acknowledgements

We thank Pedersen for confirming the validity. Yi-Fu Lai is supported by the European Union (ERC AdG REWORC - 101054911).

References

[DP24] Cyprien Delpech de Saint Guilhem and Robi Pedersen. New proof systems and an OPRF from CSIDH. In Qiang Tang and Vanessa Teague, editors, *PKC 2024, Part II*, volume 14603 of *LNCS*, pages 217–251. Springer, Cham, April 2024.

[KLLQ23] Shuichi Katsumata, Yi-Fu Lai, Jason T. LeGrow, and Ling Qin. CSI-Otter: Isogeny-based (partially) blind signatures from the class group action with a twist. In Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Part III*, volume 14083 of *LNCS*, pages 729–761. Springer, Cham, August 2023.

[Kup05] Greg Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *SIAM Journal on Computing*, 35(1):170–188, 2005.

[Lai24] Yi-Fu Lai. Capybara and tsubaki: Verifiable random functions from group actions and isogenies. *IACR Communications in Cryptology*, 1(3), 2024.

[LP24] Shai Levin and Robi Pedersen. Faster proofs and VRFs from isogenies. Cryptology ePrint Archive, Paper 2024/1626, 2024.