A Post-Quantum Oblivious PRF from Isogenies

Andrea Basso
University of Birmingham
United Kingdom
a.basso@cs.bham.ac.uk

ABSTRACT

At Asiacrypt 2020, Boneh et al. proposed a verifiable oblivious pseudorandom function based on isogenies. Basso et al. later demonstrated a subexponential attack on the pseudorandomness of the protocol.
In this work, we propose an efficient countermeasure against such an attack. We also propose several improvements that significantly reduce the computational and communication cost of the protocol. We introduce some countermeasures that make the protocol secure against the recent SIDH attacks. Putting everything together, we obtain the most efficient post-quantum OPRF protocol.

1 INTRODUCTION

An oblivious pseudorandom function (OPRF) is a protocol between a client and a server. The two parties obliviously evaluate a PRF on a client-controlled input with the server's secret key. After engaging in the protocol, the server does not learn anything about the client's input, whereas the client only learns the output of the PRF on its chosen input. If the OPRF is also *verifiable*, the client can verify that the server used a previously committed secret key.

Oblivious PRFs are a fundamental tool for developing privacy-preserving solutions, such as private-set intersection, password-protected secret sharing, privacy-preserving CAPTCHA systems, and password-authenticated key exchanges. There exist several efficient constructions of oblivious PRFs from classical assumptions. However, it appears that post-quantum OPRFs are much harder to obtain. One of the few constructions, and possibly the most efficient one, is due to Boneh et al. [BKW20]. The protocol is based on isogenies and the security of SIDH [JDF11] and related problems. This construction was later cryptanalyzed by Basso et al. [BKM+21], which demonstrated a subexponential attack against the pseudorandomness property. Moreover, Castryck and Decru [CD22] recently proposed a key-recovery attack on SIDH, which can easily be translated to an attack on the Boneh et al. construction.

Contributions. In this work, we propose the most efficient post-quantum OPRF construction, based on the previous work by Boneh et al. We first propose an efficient countermeasure that prevents the subexponential attack by Basso et al. (Sec.3.1). Then, we discuss several general improvements (Sec. 3.2) that reduce the communication cost and increase the performance of the protocol. Lastly, we address the recent attacks on SIDH, and we propose a countermeasure that guarantees the security of the protocol (Sec. 3.3). Putting everything together, we obtain a post-quantum OPRF protocol that overcomes existing attacks and achieves the highest efficiency among the post-quantum constructions reported in the literature.

2 THE BONEH ET AL. CONSTRUCTRION

In the Boneh et al. OPRF protocol, the client computes an isogeny ϕ_m, from the original curve E_0 to the curve E_m, based on the client's input message. Then, the client blinds its input by computing a second isogeny ϕ_r starting from E_m. Its target curve E_{mr}, together with some torsion point information, is sent to the server, which computes the isogeny ϕ_k. The server responds with the curve E_{mrk}, together with the images of torsion points on E_{mr}. Using these points, the client can invert the blinding isogeny to obtain the curve E_{mk}, which is the output of the OPRF[1]. Since the server does not reveal additional torsion information, the client cannot compute the curve E_k and evaluate the PRF independently.

The client also provides a zero-knowledge proof that the isogeny $\phi_r \circ \phi_m$ was computed honestly. In the verifiable version of the protocol, the server also commits to a secret key k, and it provides two zero-knowledge proofs that both the commitment and the isogeny ϕ_k are computed honestly, together with a third proof that the isogeny ϕ_k is parallel to the publicly-committed one.

3 A NEW OPRF PROTOCOL

3.1 Preventing the Basso et al. attack

The original protocol by Boneh et al. generates a basis P, Q for the torsion dedicated to the message space, i.e. $E_0[\ell^e]$ for some choice of ℓ and e such that $\ell^e \mid p+1$, and hashes a message m onto the message curve E_m by computing the isogeny ϕ_m given by

$$\phi_m : E_0 \to E_0/\langle P + [H(m)]Q \rangle =: E_m,$$

where $H(\cdot)$ maps the message m onto an element of $\mathbb{Z}_{\ell^e}$.

[1]This is a slight simplification. The output of the OPRF is computed as $F(k,x) = H(x, j(E_{mk}), \mathsf{pk})$, where H is a hash function and pk is the server's commitment to its key k. The value pk is only present in the verifiable version of the OPRF.

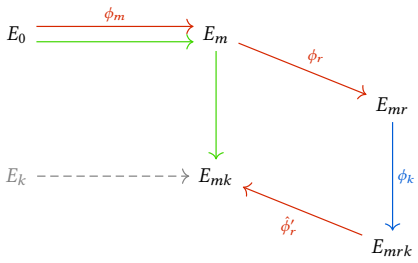

Figure 1: The Boneh et al. OPRF. Isogenies in red are computed by the client, while those in blue are computed by the server. The green isogenies represent the PRF evaluation. The curve E_k can be computed by an attacker, which allows them to evaluate the OPRF on any input via the dashed isogeny. Based on Fig. 1 of [BKM+21].

Basso et al. proposed a subexponential attack on the Boneh et al. construction where the attacker queries several PRF evaluations to compute the images of three linearly independent subgroups of $E_0[\ell^e]$ under the isogeny $\phi_{0k} : E_0 \mapsto E_k$. With this information, the attacker can map any point $M \in E_0[\ell^e]$ to E_k and compute the isogeny whose kernel is generated by the image of M, thus obtaining the corresponding curve E_{mk}. This allows an attacker to evaluate the OPRF on any input without further interacting with the server, which breaks the pseudorandomness of the protocol. The subexponential attack can be thwarted if a sufficiently long isogeny ϕ_m is chosen. The authors of [BKM+21] propose $\ell^e \approx 2^{\lambda^2}$, or $\ell^e \approx 2^{4224}$ if the number of queries can be restricted, but both options appear to be impractical. We propose an efficient countermeasure that prevents the existing attack with only a small computational overhead. Despite that, the improvements discussed in Sec. 3.2 compensate for this overhead.

In SIDH, the kernels of the isogenies are computed as a linear combination of torsion points because they need to be translated by a second isogeny. In the case of the OPRF protocol, the isogeny ϕ_m is never translated. Indeed, the images of the points generating $E_0[\ell^e]$ are never revealed. Instead, the client only needs to hash onto the curve E_m. This can be achieved by taking a sufficiently long random walk over the isogeny graph, as in the CGL hash function [CGL09] or its more efficient variant [DPB17]. We propose a similar approach as in [DPB17], using two isogenies. More formally, we map a message m to the curve E_m in the following way:

(1) Using a generic hash function $\bar{H}$, we map m to an element of $\mathbb{Z}_{\ell^e} \times \mathbb{Z}_{\ell^e}$, i.e. $(m_0, m_1) = \bar{H}(m)$.
(2) Given the starting curve E_0 and two points P_0, Q_0 spanning $E_0[\ell^e]$, we compute the isogeny

$$\phi_0 : E_0 \mapsto E_1 := E_0/\langle P_0 + [m_0]Q_0 \rangle.$$

(3) We determine a canonical basis P_1, Q_1 of $E_1[\ell^e]$ and compute the isogeny

$$\phi_1 : E_1 \mapsto E_m := E_1/\langle P_1 + [m_1]Q_1 \rangle,$$

where the target curve E_m of the isogeny ϕ_1 is the desired output.

With the proposed construction, an attacker may still compute the curve E_k and a torsion basis that allows them to evaluate the first isogeny ϕ_{0k} to obtain the curve E_{1k}. However, since the attacker does not know the isogeny between E_0 and E_k, they cannot map the canonical basis on E_1 to E_{1k}, and thus they cannot compute the remaining half of the isogeny. This situation is represented in Fig. 2. Note that the curve E_{1k} is message-dependent, and if we assume that the hash function $\bar{H}$ is collision-resistant in its first component, it is hard for an attacker to find two messages that have the same first curve E_1 and E_{1k}. Thus, the knowledge of E_{1k} does not help the attacker learn any information on the curve E_{mk} because the attacker cannot obtain the image of the canonical basis on E_1 on E_{1k} under the server's secret isogeny. This thus successfully prevents the subexponential attack.

Remark. *An attacker may find a basis of $E_0[\ell^{2e}]$, map it to E_k as in the existing attack, and use this knowledge to evaluate the longer isogeny from E_k to E_{mk}. However, the basis $E_0[\ell^{2e}]$ is defined over the extension field $\mathbb{F}_{p^{2\ell^e}}$. Given the size of $\ell^e \approx 2^{2\lambda}$, just representing a value in such an extension field, let alone doing any computation, would be exponential in the security parameter. It is thus important that the degree of ϕ_m is a prime power (as is in the original construction) and not a product of prime powers because otherwise an approach based on the Chinese Remainder Theorem might decrease the size of the extension field.*

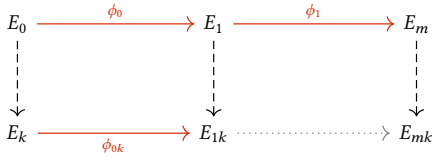

Figure 2: Summary of the proposed countermeasure (this does not depict the blinding/unblinding phase). Isogenies in red are known or can be computed by the attacker, isogenies in black are unknown to the attacker, and the dotted isogeny represents the missing isogeny that the attacker would like to recover.

3.2 Reducing the prime size

The original OPRF construction uses a prime p where $p - 1$ has 5 prime divisors, corresponding to the message space, the blinding space, the server's secret space, and one for

each of the two zero-knowledge proofs. This results in a prime of size $\log p \approx 12\lambda$, since all but one prime power are about $2^{5\lambda/2}$. In this section, we discuss several improvements that significantly reduce the prime size and lead to a more efficient protocol.

Firstly, the message isogeny does not need to commute or be translated by any other isogeny, as noted in Sec. 3.1. Instead, the message isogeny is computed only to obtain the curve E_m. This means that it does not need a dedicated message space. Instead, it can reuse the blinding space, i.e. the degrees of the message isogeny and the blinding isogeny can be both powers of the same prime. This reduces the size of the prime p from 12λ to 9.5λ. A similar argument applies to the $p-1$ factors dedicated to the zero-knowledge proofs. Thus, they do not need a dedicated $(p-1)$ factor, which further decreases the size of the prime p to 5λ.

Secondly, each prime power was originally chosen to be about $2^{5\lambda/2}$ due to an attack by Merz et al. [MMP20]. This, however, only applies to the message isogeny and does not need to be extended to the blinding or server's secret isogenies. Thus, both isogeny degrees can be decreased to $2^{2\lambda}$, reducing the size of the prime p to 4λ.

Lastly, it is possible to use even smaller primes since the memory requirements of the meet-in-the-middle attack are impractical for these sizes. Thus, for $\lambda = 128$ bits of security, one can use isogenies of degree $\approx 2^{216}$, as in SIDH.

3.3 Protecting against the SIDH attacks

The recent series of attacks on SIDH by Castryck and Decru [CD22], Maino and Martindale [MM22], and Robert [Rob22] also apply to the Boneh et al. construction and its improved variant presented here. All these attacks recover a secret isogeny if the image of a torsion subgroup under the secret isogeny is known.

Both the client and the server reveal torsion informations, and thus they both need to be protected against the SIDH attacks. We propose three different possible solutions. One can apply the countermeasures that are known to prevent such attacks on SIDH, such as those that relies on secret-degree isogenies [Mor22] or masked torsion points [Fou22]. These however require using a large prime, and their security needs to be further assessed. Another approach involves setting the isogeny degrees such that the SIDH attacks do not apply. The attack by Robert [Rob22] requires torsion information of degree N to recover an isogeny of degree N^2. In the OPRF setting, one can set the server's isogeny degree to be sufficiently larger than the blinding isogeny degree so that the server is protected. If the message isogeny is sufficiently long, the attacker can also not recover the message and blinding isogeny, which protects the client. Note, however, that this approach relies on the message space having sufficient entropy, and it does not protect the client's server if the possible message choices are limited. Alternatively, it may be possible to protect the server using generic MPC techniques to compute the functionality where one party inputs two torsion points P, Q and obtains no input, while the other inputs their secret x and obtains $P + [x]Q$. Further work is needed to estimate the requirements and the performance impact of this approach.

We also leave analyzing the zero-knowledge proofs needed for verifiability in light of the recent SIDH attack for future work.

4 CONCLUSION AND FUTURE WORK

We presented an an OPRF construction based on the one by Boneh et al. The countermeasures against the Basso et al. attack guarantees the security of the protocol without increasing the parameter size. Furthermore, we discussed countermeasures against the recent SIDH attacks, and presented several improvements that reduced the prime size.

The techniques presented in this work raise more research questions and further work is needed. Firstly, the security of the protocol needs to be thoroughly evaluated, especially in light of the recent Castryck-Decru attack [CD22]. While most of the security proofs can be inherited from the Boneh et al. construction, the proposed changes need to be taken into consideration.

Secondly, we have shown several improvements for the non-verifiable variant of the protocol. Next, we aim to take a closer look at the verifiability property and the zero-knowledge proofs used to achieve it. In particular, we believe it is possible to replace the isogeny proofs of knowledge with more efficient ones and to combine the three separate proofs (two proving knowledge of an isogeny and one proving parallelism of two isogenies) into a single non-interactive proof. The combined proof would have a significantly reduced cost. Moreover, the non-interactivity of the protocol would reduce the number of rounds from six, as in the original construction (the proof of parallel isogenies requires five rounds), to two, which is theoretically optimal.

Lastly, we would like to develop an optimized implementation of the protocol to obtain concrete performance results and demonstrate the practical applicability of the proposed OPRF.

REFERENCES

[BKM+21] Andrea Basso, Péter Kutas, Simon-Philipp Merz, Christophe Petit, and Antonio Sanso. Cryptanalysis of an oblivious PRF from supersingular isogenies. In Mehdi Tibouchi and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2021*, pages 160–184, Cham, 2021. Springer International Publishing.

[BKW20] Dan Boneh, Dmitry Kogan, and Katharine Woo. Oblivious Pseudorandom Functions from Isogenies. Technical Report 1532, 2020. http://eprint.iacr.org/2020/1532.

[CD22] Wouter Castryck and Thomas Decru. An efficient key recovery attack on SIDH (preliminary version). *Cryptology ePrint Archive*, 2022. https://eprint.iacr.org/2022/975.

[CGL09] Denis X Charles, Eyal Z Goren, and Kristin E. Lauter. Cryptographic hash functions from expander graphs. *Journal of Cryptology*, 22(1):93–113, 2009.

[DPB17] Javad Doliskani, Geovandro C. C. F. Pereira, and Paulo S. L. M. Barreto. Faster Cryptographic Hash Function From Supersingular Isogeny Graphs. *Selected areas in cryptography – SAC 2022*, 2017. https://eprint.iacr.org/2017/1202.

[Fou22] Tako Boris Fouotsa. SIDH with masked torsion point images. https://eprint.iacr.org/2022/1054, 2022.

[JDF11] David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In *International Workshop on Post-Quantum Cryptography*, pages 19–34. Springer, 2011.

[MM22] Luciano Maino and Chloe Martindale. An attack on SIDH with arbitrary starting curve. Cryptology ePrint Archive, Paper 2022/1026, 2022.

[MMP20] Simon-Philipp Merz, Romy Minko, and Christophe Petit. Another look at some isogeny hardness assumptions. In *Topics in Cryptology - CT-RSA 2020 - the Cryptographers' Track at the RSA Conference 2020, San Francisco, CA, USA, February 24-28, 2020, Proceedings*, pages 496–511, 2020.

[Mor22] Tomoki Moriya. Masked-degree SIDH. Cryptology ePrint Archive, Paper 2022/1019, 2022.

[Rob22] Damien Robert. Breaking SIDH in polynomial time. Cryptology ePrint Archive, Paper 2022/1038, 2022.