

Oblivious Pseudorandom Functions in a Post-Quantum World

Lena Heimberger

Paris Crypto Days, 16th of January 2026

heimberger.xyz/oprfs.html

Oblivious Pseudorandom Functions

- simple(r) primitive from asymmetric cryptography
- gives rise to a number of cool constructions
- cheap! ...pre-quantum

Pseudorandom Function

A pseudorandom function (PRF) [GGM84, GGM86] is a deterministic and polynomial time function $F: \mathcal{K} \times \mathcal{X} \rightarrow \mathcal{Y}$ such that there is no probabilistic polynomial-time algorithm to distinguish any output y from a randomly chosen element from \mathcal{Y} .

Definitions

Client



input $x \in \mathcal{X}$,
gets y

compute

$$y := F_k(x)$$

Server



key $k \in \mathcal{K}$

Oblivious Pseudorandom Function

An oblivious pseudorandom function (OPRF) [FIPR05] is a protocol between two parties. One party holds the secret key k and the other holds their secret input x . The OPRF privately realizes the joint computation outputting $F_k(x)$ for a PRF F to the party holding x , and nothing to the party holding k .

Partial Obliviousness In a POPRF, the client submits a tag t in addition to the input x and gets the evaluation $y := F_k(t, x)$. t contains additional information, e.g. a validity period.

Threshold Get a valid evaluation from a t -out-of- n servers.

Verifiability The client can ensure that a pre-committed server key k was used to compute $y = F_k(x)$.

VOPRF+POPRF=VPOPRF

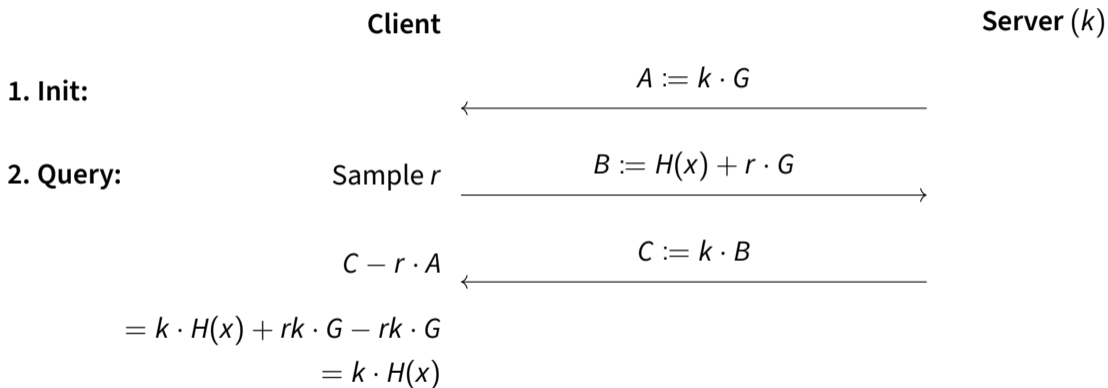
Public Verifiability means we built a blind signature.

Classical OPRFs

- 1 The client hashes the input to the group, samples an invertible blinding element, and blinds the hashed element that is then sent to the server.
- 2 The server then faithfully evaluates the element with the key and returns the result.
- 3 The client unblinds the server result and has a PRF evaluation without having to reveal the input.

Question: what could go wrong at each step?

Pre-quantum Blind-evaluate-unblind: 2HashDH



How would an ideal OPRF look like?

Security. ideally malicious security, i.e. a malicious adversary cannot learn anything they shouldn't (doesn't imply detection). Semi-honest adversaries follow the protocol but only follow passively.

Round-Optimality. A **round** is a period where all parties can exchange messages simultaneously.

Round-optimality for non-interactive protocol (e.g. NIZK): single round

interactive protocol: two rounds

Communication size. Elliptic curve OPRFs: 766 bits of communication.

Computational complexity. Maybe better than classical: e.g. Kyber768 takes between a third to half of the computational time of ECDH Curve 25519.

- Preprocessing.** Repeated computations? Shift data-independent communication and computation to a preprocessing phase. Fully online protocols: online variant or perform the precomputation on the fly.
- Trusted Setup.** In addition to preprocessing, some OPRFs rely on a trusted setup. But: trust is a hard problem in itself, and sometimes a trusted setup just isn't available (e.g. for CSIDH).

OPAQUE and Private Set Intersection

OPAQUE

Client (pwd)

Server (k)

1. Registration: $k' = F_k(pwd)$

OPRF



Sample (pk, sk)

$pk, ct = Enc_{k'}(sk)$



Store (pk, ct)

2. Login:

ct



$k' = F_k(pwd)$

OPRF



$sk = Dec_{k'}(ct)$

AKE using sk



Question: Which properties are important?

- doesn't reveal output
- server still passively observes the success or failure of an authentication attempt
- OPRF must be secure against a malicious server
- Verifiability?

Private Set Intersection (PSI)

OPRFs are useful for **unbalanced** sets, where one party, typically the server in client-server protocols, has a significantly larger set than the other party.

Client (x_1, \dots, x_m)

Server $(y_1, \dots, y_n), k$

$\{F_k(x_i)\}_{i \in [m]}$

OPRF



$\{z_j = F_k(y_j)\}_{j \in [n]}$



$F_k(x_i) = z_j$. Otherwise $F_k(y_j)$ is pseudorandom.

Question: Which properties are important?

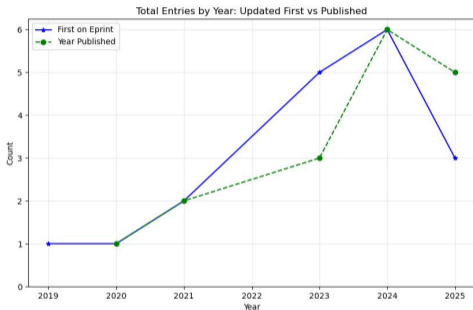
- per-client keys may cause segmentation
- semi-honest server may be realistic:
 - regulatory and reputational incentives [KRS⁺19]
 - inherent trust
government agencies identifying duplicate entries
 - anywhere where PSI is applied to limit the risk of data breaches

And more [CHL22]

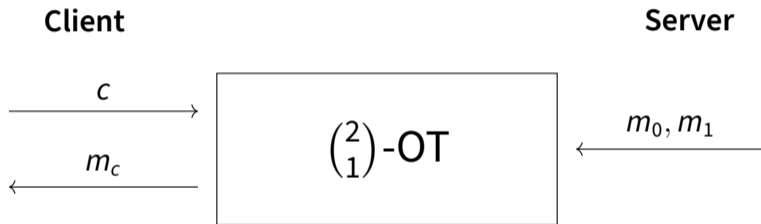
- oblivious keyword search
- password-protected secret sharing
- private information retrieval
- cloud key management
- de-duplication systems
- secure pattern matching
- untraceable contact tracing
- ...

Post-Quantum OPRFs today

- Currently ≈ 18 papers proposing OPRFs
- rely heavily on methods from MPC and zero-knowledge
- Plan:
 - 1 scheme
 - 2 trivial OPRF
 - 3 specialized constructions
 - 4 performance comparison
- repeat four times
- probably biased

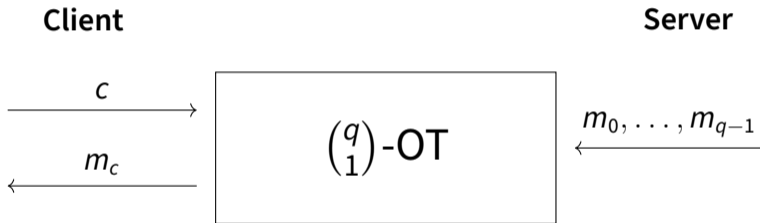


A little help from MPC friends

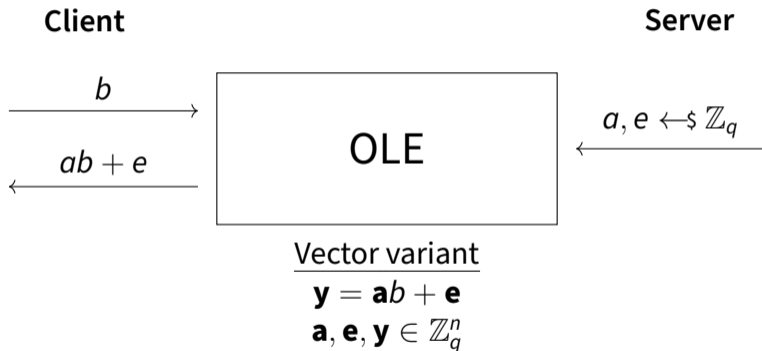


Extend with symmetric operations!

A little help from MPC friends (cont.)



A little help from MPC friends (cont.)



- Garble cipher circuit, evaluate with PQ-OT
- \approx 7MB communication
- what is missing?
 - malicious security
 - verifiability
 - efficient PQ-OT
 - use MPC-friendly ciphers instead of AES
- good baseline!

Lattice OPRFs

2HashDH, but make it Lattices [ADDS21]

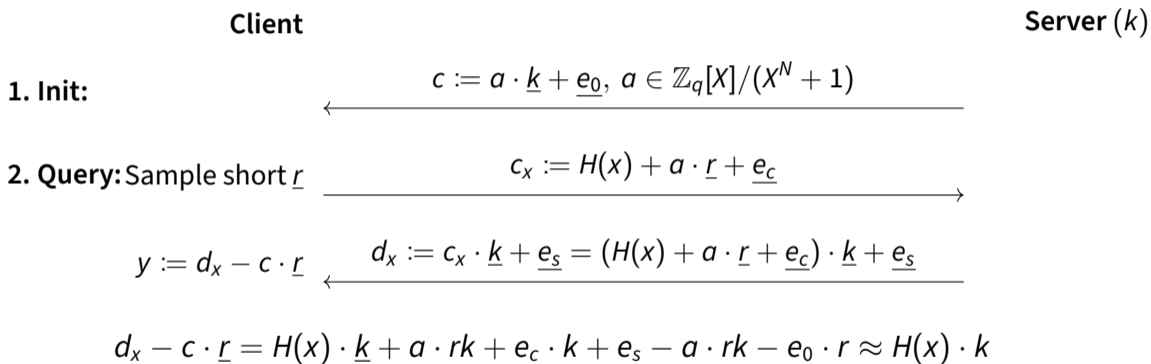


Figure: Generic construction for 2HashDH OPRF from LWE [ADDS21]. Underlined variables are short.

How could a malicious client attack when we forego ZK?

- Is it safe to output $c_x \mathbf{k} + \underline{\mathbf{e}}$ for arbitrary c_x ? no, trapdoors!
- Noise Leakage: the client learns $\mathbf{e}_c \mathbf{k} + \mathbf{e}_s - \mathbf{e}_0 \mathbf{r}$ where they choose \mathbf{e}_0 and \mathbf{r} before rounding.
- trivial attack:
 - Write $\mathbf{a} := (\mathbf{e}, -\mathbf{r})$ and $s := (\mathbf{k}, \mathbf{e}_0)$
 - Rewrite $\mathbf{e}_c \mathbf{k} + \mathbf{e}_0 - \mathbf{e}_s \mathbf{r}$ as $\mathbf{a} \mathbf{s} + \mathbf{e}_1$
 - This is essentially an instance of LWE without modular reduction! [BDE⁺18] which is easy.¹

¹This is a bit of a simplification because \mathbf{e}_1 is sampled fresh in each invocation so the attack does not apply directly.

The OPRF requires the client to prove in zero-knowledge that the initial message $\mathbf{c}_x := H(x) + \mathbf{a}\mathbf{r} + \mathbf{e}_c$ is well-formed.

More concretely, the client has to prove that:

- 1 they know an $\mathbf{x} \in \{0, 1\}^\kappa$
- 2 $\mathbf{r} \in R$ is a small element with $\ll \mathbf{r} \ll_\infty \leq \sigma\sqrt{n}$
- 3 $\mathbf{e}_c \in R^{1 \times \ell}$ where $\ll \mathbf{e}_c \ll_\infty \leq \sigma\sqrt{n}$

Question Which proof is most expensive? The first one. This is the main bottleneck in lattice protocols.

- 1 correctness requirements on the ring modulus
 - semihonest: 256-bit modulus and a ring dimension of 2^{14} , which sums to about 2MB of communication (over 0.5 MB per ring element).
 - malicious secure correctness: 2048 bit modulus

2 Statistical Noise Drowning

- **Question** What is the size of the error terms $\mathbf{e}_c, \mathbf{e}_s$?
- have to be small in relation to q :

$$q \overset{\text{correctness of } \approx}{\gg} \mathbf{e}_s \overset{\text{hide } \mathbf{k}}{\gg} \mathbf{e}_c \cdot \mathbf{k}$$

- avoid 1D-SIS assumption by adding output of random oracle to client input
- remove superpolynomial dependency on the norm of additive terms using Rényi Noise Drownings
- Impact on game-based proof: search instead of a distinguishing game
- bound on number of queries
- a few other tricks: Labrador for proofs.
- [ADDS21] \approx 128 GB per evaluation using [YAZ⁺19]
- [AG24]: \approx 538 kB per evaluation using [BS23]

- Computational Assumption $\ll \mathbf{e}' \ll \geq \text{poly}(\lambda)\sqrt{Q} \ll \mathbf{ek} - \mathbf{e}''\mathbf{r} \ll$ [ESTX24]
- new assumption iMLWE-RU-R+MLWE+MSIS
 - 222 kB [AG24] to 159 kB online
 - 316 kB [AG24] to 20 kB preprocessing

- binary LWR: $\lfloor H(x)^T \cdot k \rfloor_p, H : \{0, 1\}^* \mapsto \mathbb{Z}_q^n, k \in \{0, 1\}^n$
- 12 kB, round-optimal, semi-honest
- same problem with proving the hash, new assumption

Naor-Reingold Constructions

Naor-Reingold PRF [NR04]

- The Naor-Reingold PRF [NR04] that generically builds a PRF from an Abelian group action $*$.
- To compute the PRF over m input bits, we sample $m + 1$ group elements $[g_0, g_1, \dots, g_m]$.
- Start with group action with g_0
- For every following group element, the group action is performed when the i^{th} bit of the input is set.

Example (Naor-Reingold with seven input bits)

For example, for 0110111 we would compute the group action

$$g_0 * g_2 * g_3 * g_5 * g_6 * g_7.$$

PRF from rounded Subset-Product over Rings

- 2014: SPRING [BBL⁺15], an LWR-style PRF with small modulus
- focus in SPRING-BCH: $q = 257$, rounding bias reduction using extended BCH code [128, 64, 22]
- Oblivious evaluation: 304 bytes/ 11 μ s client, 22 kB/227 μ s server

$$\mathcal{F}_{\mathbf{K}}(c_1, \mathcal{F}_{\mathbf{K}}(c_2, \dots, \mathcal{F}_{\mathbf{K}}(c_m, \epsilon_1, \epsilon_2, \dots, \epsilon_m)))$$

lattice-ish OPRF overview

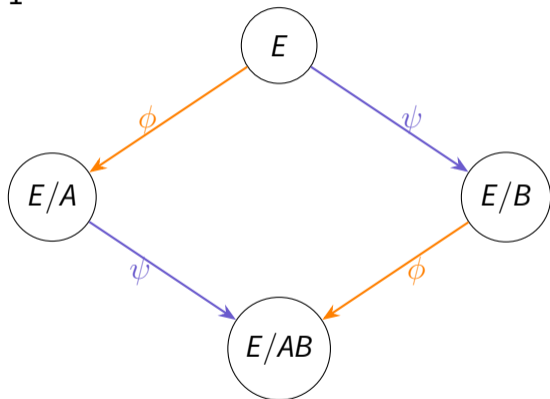
Construction	rounds	malicious secure	comms	preprocessing
[ADDS21]	2	✗	2MB	/
[ADDS21]	2	✓	128 kB	/
[AG24]	2	✓	222 kB	316 kB (2^6 queries)
[ESTX24]	2	✓	159 kB	20 kB
[DDT25]	2	✗	12 kB	1.5 MB (amortizable)
[HKL ⁺ 25]	6	✗	23 kB	793 kB (amortizable)

Isogenies

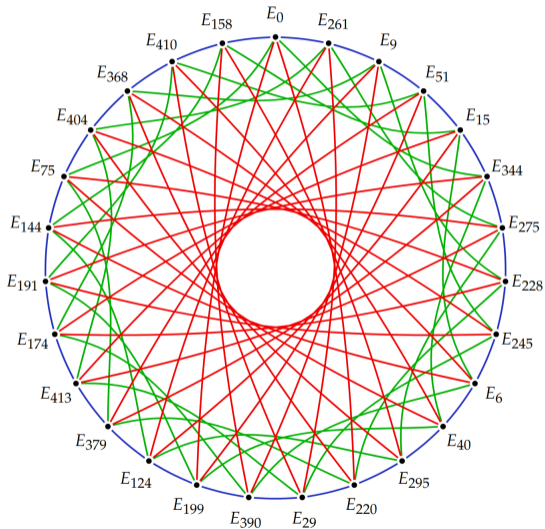
2HashDH from SIDH [Bas24]

- repairs 2HashDH construction [BKW20] from SIDH isogenies
- No MPC!
- malicious security
- round-optimal
- 8.7 MB comms

1-







- random walk on commutative graph
- node: curve with Montgomery coefficient
- private key describes number of steps and orientation



Naor-Reingold OPRF from CSIDH

- blind key and reduce via relational lattice [HHM⁺24, DP24]
- CSIDH OT needs trusted setup
→ doesn't exist for CSIDH
- Explicit consecutive evaluation: OPUS [HHM⁺24], no trusted setup, no class group structure

protocol	rounds	comm. cost	isog. comp.	model (C-S)
NR-OT	2	$2\sigma \cdot \gamma + 2\gamma^2 + \sigma$	$5\gamma + 2$	
NR-OT	4	$5\sigma \cdot \gamma + 5\gamma^2 + \sigma$	$11\gamma + 2$	
OPUS	$2\gamma + 2$	$3\sigma \cdot \gamma + 2\sigma$	$3\gamma + 3$	
[DP24]	2	$(\lambda + 5)\gamma + 2\lambda$	$4\lambda + 2$	

γ input bits, ρ CSIDH modulus

Legendre OPRFs

Definition (Legendre Symbol)

An integer a is a quadratic residue mod p if the equation $x^2 \equiv a \pmod{p}$ is solvable and $\gcd(a, p) = 1$. The Legendre symbol for some integer a and an odd prime p is

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p \\ -1 & \text{if } a \text{ is a quadratic non-residue mod } p \\ 0 & \text{if } a \equiv 0 \pmod{p} \end{cases}$$

Definition (Legendre PRF [Dam90])

$$F_k(x) := (k + x)^{\frac{p-1}{2}}$$

$x = -k$: $F_k(x) = 0$, distinguisher in OPRF setting

Definition (Sequential Legendre PRF)

$$\{a\}_K := \left(\frac{K}{p}\right), \left(\frac{K+1}{p}\right), \dots, \left(\frac{K+a-1}{p}\right)$$

A straightforward Legendre OPRF [SHB23]

- oblivious evaluation using a trusted third party for
 - Beaver triples to multiply additively shared values
 - perfect square s^2 for shared Legendre symbol computation
- \approx 13kB online, expensive preprocessing

- replicated secret sharing for fast online multiplications (semihonest variant)
- avoids zero-knowledge proofs, but requires checks in precomputation
- doubly replicated secret sharing for malicious security: not round-optimal
- concrete performance depends on number of corrupted servers

Frame, then build: 2HashDH UC Framework [BDFH25]

- sequential Legendre PRF well-proven in UC
- general idea: use perfect square a^2 to mask $K + h + l'_i$ since $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$
 - server samples random vector \mathbf{a} and defines

$$\mathbf{u} = \{(K + l'_i)a_i^2\}_{i \in [\ell_{eval}]} \text{ and } \mathbf{v} = \{a_i^2\}_{i \in [\ell_{eval}]}$$

- VOLE computes

$$\mathbf{o} := \mathbf{u} + h * \mathbf{v} = \{(K + h + l'_i)a_i^2\}_{i \in [\ell_{eval}]}$$

- user receives $o_i = (K + h + l'_i)a_i^2$ and can compute

$$\left(\frac{o_i}{p}\right) = \left(\frac{(K + h + l'_i)a_i^2}{p}\right) = \left(\frac{K + h + l'_i}{p}\right)$$

- Power Residue PRF: Generalization of Legendre PRF $(k + x)^g \pmod p$, $p = 2^\lambda \cdot g + 1 \in \mathbb{P}$ to get $\approx \mathcal{O}(\lambda)$ output instead of a single bit.
- for PQ security, p needs to be > 384 bits
- VOLE correlations to compute PRF obliviously
- three variants:
 - 2PC-Gold (reverse DLOG): $(k + x)^g$, k, x are private
 - O-Gold: more 2HashDH-style $H_2(x, \text{Gold}_k(H_1(x)))$
performance similar to 2PC-Gold
 - UC gold: UC provable, removes edge case of $x = -k$
- three rounds of communication

Legendre OPRF overview

Construction	rounds	malicious secure	comms	preprocessing
[KCM25]	2	✗	144 kB	432 kB
[BDFH25]	9	✓	356 kB	392 kB
[YBH ⁺ 25]	3	✓	970 kB (1.9 kB)	-

Alternating Moduli constructions

Alternating Moduli PRF

- linear functions over different moduli (2 and 3)
- $\mathbf{B} \in \mathbb{Z}_3^{t \times m}$ is public, $\mathbf{K} \in \mathbb{Z}_2^{m \times n}$ is secret, $\mathbf{x} \in \mathbb{Z}_2^n$ is the input, $\mathbf{y} \in \mathbb{Z}_3^n$ is the output
- Core idea: use linear maps as high degree functions (i.e. map over \mathbb{Z}_2 is a high degree function over \mathbb{Z}_3 and vice versa)
 - 1 compute non-compressive (secret) linear map $\mathbf{w} = \mathbf{K} \times \mathbf{x}$
 - 2 reinterpreted over \mathbb{Z}_3
 - 3 compute compressive public linear map over \mathbb{Z}_3 by computing $\mathbf{B} \times \mathbf{w} = \mathbf{y}$
- weak PRF: only uniformly random inputs are allowed

- new alternating-moduli PRFs, friendly for OT correlations
- semi-honest, round-optimal construction
limited usage recommended ($\approx 2^{40}$ evaluations)
- (V)OLE for oblivious evaluation
- preprocessing for conversion between rings mod 2 to mod 3
- subset-sum symmetric hardness
- performs better in preprocessing/communication/computation because of efficient modulus conversion gates instead of generic OT

- use torus FHE for malicious security
wPRF is MPC and FHE friendly!
- no preprocessing
- not verifiable [CJ25]

- point-wise alternating moduli PRFs
- small signatures, 3/4 constructions broken [SW25]
- reverse many-to-one construction:
setup + \approx 130 bytes comms

alternating moduli OPRF overview

Construction	rounds	malicious secure	comms	preprocessing
[DGH ⁺ 21]	2	✗	80 bytes	200 bytes
[ADDG24]	2	✓	160 kB	2.5 MB
[APRR24]	2	✗	≈ 130 bytes	5 bytes(amort.)

- OPRFs vs. blind signatures?
- Find better algebra?
- design oblivious-evaluation friendly PRFs
- better MPC techniques + MPC-friendly symmetric primitives (e.g. random OT from lattices)
- lift semi-honest constructions to malicious constructions
- We still don't have a great, general-purpose construction! But we have good amortizable PRFs.

Acknowledgements

This presentation was prepared using funds from the Digital Europe Program under grant agreement number 101091642 (QCI-CAT).

- [ADDG24] Martin R. Albrecht, Alex Davidson, Amit Deo, and Daniel Gardham. **Crypto dark matter on the torus - oblivious PRFs from shallow PRFs and TFHE.**
In Marc Joye and Gregor Leander, editors, EUROCRYPT 2024, Part VI, volume 14656 of LNCS, pages 447–476. Springer, Cham, May 2024.
- [ADDS21] Martin R. Albrecht, Alex Davidson, Amit Deo, and Nigel P. Smart. **Round-optimal verifiable oblivious pseudorandom functions from ideal lattices.**
In Juan Garay, editor, PKC 2021, Part II, volume 12711 of LNCS, pages 261–289. Springer, Cham, May 2021.

- [AG24] Martin R. Albrecht and Kamil Doruk Gür.
Verifiable oblivious pseudorandom functions from lattices: Practical-ish and thresholdisable.
In Kai-Min Chung and Yu Sasaki, editors, ASIACRYPT 2024, Part IV, volume 15487 of LNCS, pages 205–237. Springer, Singapore, December 2024.
- [APRR24] Navid Alamati, Guru-Vamsi Policharla, Srinivasan Raghuraman, and Peter Rindal.
Improved alternating-moduli PRFs and post-quantum signatures.
In Leonid Reyzin and Douglas Stebila, editors, CRYPTO 2024, Part VIII, volume 14927 of LNCS, pages 274–308. Springer, Cham, August 2024.

- [Bas24] Andrea Basso.
A post-quantum round-optimal oblivious PRF from isogenies.
In Claude Carlet, Kalikinkar Mandal, and Vincent Rijmen, editors, SAC 2023, volume 14201 of LNCS, pages 147–168. Springer, Cham, August 2024.
- [BBL⁺15] Abhishek Banerjee, Hai Brenner, Gaëtan Leurent, Chris Peikert, and Alon Rosen.
SPRING: Fast pseudorandom functions from rounded ring products.
In Carlos Cid and Christian Rechberger, editors, FSE 2014, volume 8540 of LNCS, pages 38–57. Springer, Berlin, Heidelberg, March 2015.

- [BDE⁺18] Jonathan Bootle, Claire Delaplace, Thomas Espitau, Pierre-Alain Fouque, and Mehdi Tibouchi.
LWE without modular reduction and improved side-channel attacks against BLISS.
In Thomas Peyrin and Steven Galbraith, editors, ASIACRYPT 2018, Part I, volume 11272 of LNCS, pages 494–524. Springer, Cham, December 2018.
- [BDFH25] Ward Beullens, Lucas Dodgson, Sebastian H. Faller, and Julia Hesse.
The 2Hash OPRF framework and efficient post-quantum instantiations.
In Serge Fehr and Pierre-Alain Fouque, editors, EUROCRYPT 2025, Part VIII, volume 15608 of LNCS, pages 332–362. Springer, Cham, May 2025.

- [BKW20] Dan Boneh, Dmitry Kogan, and Katharine Woo.
Oblivious pseudorandom functions from isogenies.
In Shiho Moriai and Huaxiong Wang, editors, ASIACRYPT 2020, Part II, volume 12492 of LNCS, pages 520–550. Springer, Cham, December 2020.
- [BS23] Ward Beullens and Gregor Seiler.
LaBRADOR: Compact proofs for R1CS from module-SIS.
In Helena Handschuh and Anna Lysyanskaya, editors, CRYPTO 2023, Part V, volume 14085 of LNCS, pages 518–548. Springer, Cham, August 2023.

- [CHL22] Sílvia Casacuberta, Julia Hesse, and Anja Lehmann.
SoK: Oblivious pseudorandom functions.
In 2022 IEEE European Symposium on Security and Privacy, pages 625–646. IEEE Computer Society Press, June 2022.
- [CJ25] Jung Hee Cheon and Daehyun Jang.
Cryptanalysis on lightweight verifiable homomorphic encryption.
In International Conference on the Theory and Application of Cryptology and Information Security, pages 366–397. Springer, 2025.
- [Dam90] Ivan Damgård.
On the randomness of Legendre and Jacobi sequences.
In Shafi Goldwasser, editor, CRYPTO'88, volume 403 of LNCS, pages 163–172. Springer, New York, August 1990.

- [DDT25] Alex Davidson, Amit Deo, and Louis Tremblay Thibault.
Pool: A practical OT-based OPRF from learning with rounding.
In Chun-Ying Huang, Jyh-Cheng Chen, Shih-Pyng Shieh, David Lie, and Véronique Cortier, editors, ACM CCS 2025, pages 1038–1052. ACM Press, October 2025.
- [DGH⁺21] Itai Dinur, Steven Goldfeder, Tzipora Halevi, Yuval Ishai, Mahimna Kelkar, Vivek Sharma, and Greg Zaverucha.
MPC-friendly symmetric cryptography from alternating moduli: Candidates, protocols, and applications.
In Tal Malkin and Chris Peikert, editors, CRYPTO 2021, Part IV, volume 12828 of LNCS, pages 517–547, Virtual Event, August 2021. Springer, Cham.

References VIII

- [DP24] Cyprien Delpéch 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.
- [ESTX24] Muhammed F. Esgin, Ron Steinfeld, Erkan Tairi, and Jie Xu.
LeOPaRd: Towards practical post-quantum oblivious PRFs via interactive lattice problems.
Cryptology ePrint Archive, Report 2024/1615, 2024.
- [FIPR05] Michael J. Freedman, Yuval Ishai, Benny Pinkas, and Omer Reingold.
Keyword search and oblivious pseudorandom functions.
In Joe Kilian, editor, TCC 2005, volume 3378 of LNCS, pages 303–324. Springer, Berlin, Heidelberg, February 2005.

[FOO23] Sebastian H. Faller, Astrid Ottenhues, and Johannes Ottenhues.
Composable oblivious pseudo-random functions via garbled circuits.

In Abdelrahman Aly and Mehdi Tibouchi, editors, LATINCRYPT 2023, volume 14168 of LNCS, pages 249–270. Springer, Cham, October 2023.

[GGM84] Oded Goldreich, Shafi Goldwasser, and Silvio Micali.
On the cryptographic applications of random functions.

In G. R. Blakley and David Chaum, editors, CRYPTO'84, volume 196 of LNCS, pages 276–288. Springer, Berlin, Heidelberg, August 1984.

[GGM86] Oded Goldreich, Shafi Goldwasser, and Silvio Micali.
How to construct random functions.

Journal of the ACM, 33(4):792–807, October 1986.

- [HMM⁺24] Lena Heimberger, Tobias Hennerbichler, Fredrik Meisingseth, Sebastian Ramacher, and Christian Rechberger.
OPRFs from isogenies: Designs and analysis.
In Jianying Zhou, Tony Q. S. Quek, Debin Gao, and Alvaro A. Cárdenas, editors, ASIACCS 24. ACM Press, July 2024.
- [HKL⁺25] Lena Heimberger, Daniel Kales, Riccardo Lolato, Omid Mir, Sebastian Ramacher, and Christian Rechberger.
Leap: A fast, lattice-based OPRF with application to private set intersection.
In Serge Fehr and Pierre-Alain Fouque, editors, EUROCRYPT 2025, Part VII, volume 15607 of LNCS, pages 254–283. Springer, Cham, May 2025.

References XI

- [KCM25] Novak Kaludjerović, Nan Cheng, and Aikaterini Mitrokotsa.
A post-quantum distributed oprf from the legendre prf.
In European Symposium on Research in Computer Security, pages 205–225. Springer, 2025.
- [KRS⁺19] Daniel Kales, Christian Rechberger, Thomas Schneider, Matthias Senker, and Christian Weinert.
Mobile private contact discovery at scale.
In Nadia Heninger and Patrick Traynor, editors, USENIX Security 2019, pages 1447–1464. USENIX Association, August 2019.
- [NR04] Moni Naor and Omer Reingold.
Number-theoretic constructions of efficient pseudo-random functions.
Journal of the ACM, 51(2):231–262, March 2004.

- [SHB23] István András Seres, Máté Horváth, and Péter Burcs.
The legendre pseudorandom function as a multivariate quadratic cryptosystem: security and applications.
In AAECC. Springer, 01 2023.
- [SW25] Antoine Sidem and Qingju Wang.
General key recovery attack on pointwise-keyed functions: Application to alternating moduli weak prfs.
In International Conference on the Theory and Application of Cryptology and Information Security, pages 131–154. Springer, 2025.

- [YAZ⁺19] Rupeng Yang, Man Ho Au, Zhenfei Zhang, Qiuliang Xu, Zuoxia Yu, and William Whyte.
Efficient lattice-based zero-knowledge arguments with standard soundness: Construction and applications.
In Alexandra Boldyreva and Daniele Micciancio, editors, CRYPTO 2019, Part I, volume 11692 of LNCS, pages 147–175. Springer, Cham, August 2019.
- [YBH⁺25] Yibin Yang, Fabrice Benhamouda, Shai Halevi, Hugo Krawczyk, and Tal Rabin.
Gold OPRF: Post-quantum oblivious power-residue PRF.
In Marina Blanton, William Enck, and Cristina Nita-Rotaru, editors, 2025 IEEE Symposium on Security and Privacy, pages 259–278. IEEE Computer Society Press, May 2025.

Approach	Pros	Cons	Practical Viability
Generic Composition	Flexible construction, strong security	Large signatures (112 kB), slow (660 ms)	Low: Performance is not great
Hash-and-sign	Potentially tiny signatures, lots of optimization potential	Current implementation large and slow	Low: Performance is not great
Hash-and-sign with aborts	Full AC system, good balance in communication	Slow runtimes (1s)	Medium: promising but performance would need to improve
VOLEitH	Excellent potential performance (<50ms, 7.5 kB)	not a full AC system, not peer-reviewed	Medium: promising research direction, no full solution available so far

Figure: Blind signatures in the context of anonymous credentials <https://blog.cloudflare.com/pq-anonymous-credentials/>