Verifiable Oblivious PRFs

Armando Faz Hernandez
Research Engineer
ask-research@cloudflare.com

MPTS 2023:
NIST Workshop on Multi-party Threshold Schemes
September 28th, 2023

CLOUDFLARE

Agenda

- ❏ What is an OPRF?
- ❏ Construction
- ❏ Additional Properties
- ❏ Threshold Version
- ❏ Remarks

CLOUDFLARE

Oblivious Pseudorandom Function (PRF)

Two-party protocol between a Server holding a key **k** and a Client holding input **x** to compute a PRF.

$$y = PRF_k(x)$$

When protocol ends:

- Client learns the output **y** of the PRF, and
- **Obliviousness**
  - Client learns nothing about the Server's key.
  - Server learns nothing about the input nor the output.

CLOUDFLARE

Oblivious PRF – Applications

- Private Set Intersection
- Searchable Encryption
- Password-authentication Protocols
  - OPAQUE (uses OPRF as a subroutine)

    draft-irtf-cfrg-opaque
- Authorization Protocols
  - Privacy Pass (uses VOPRF as a subroutine)

    draft-ietf-privacypass-protocol

CLOUDFLARE

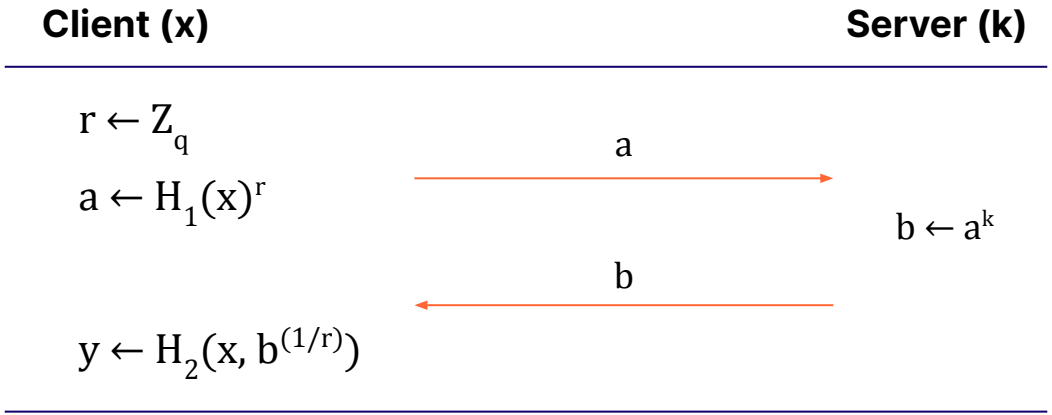
2HashDH – Construction

Jarecki, Kiayias, Krawczyk (2014)

G, an elliptic curve group of order q.

$H_1 : \{0,1\}^* \rightarrow G$ (hash to curve function)

$H_2 : \{0,1\}^* \rightarrow \{0,1\}^n$ (hash function)



https://doi.org/10.1007/978-3-662-45608-8_13

CLOUDFLARE

Additional Properties

- **Verifiability**
  - Ensure the server used a committed key.
- Partial-Obliviousness
  - Additional public input.
- Updatability
  - Mechanisms to rotate the key.
- Threshold Scheme
  - Key distributed to several parties.

CLOUDFLARE

2HashDH-NIZK – Verifiable OPRF

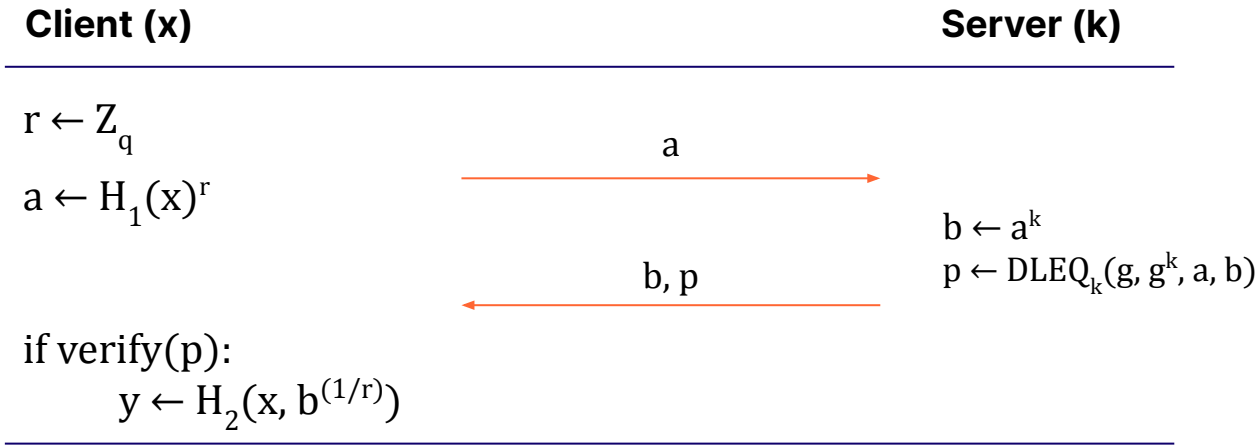
Jarecki, Kiayias, Krawczyk (2014)

G, an elliptic curve group of order q.

$H_1 : \{0,1\}^* \rightarrow G$ (hash to curve function)

$H_2 : \{0,1\}^* \rightarrow \{0,1\}^n$ (hash function)

DLEQ zk-proof



https://doi.org/10.1007/978-3-662-45608-8_13

CLOUDFLARE

Additional Properties

- Verifiability
  - Ensure the server used a committed key.
- **Partial-Obliviousness**
  - Additional public input.
- Updatability
  - Mechanisms to rotate the key.
- Threshold Scheme
  - Key distributed to several parties.

CLOUDFLARE

3HashSDHI – Partial Oblivious PRF

Tyagi, et al. (2022)

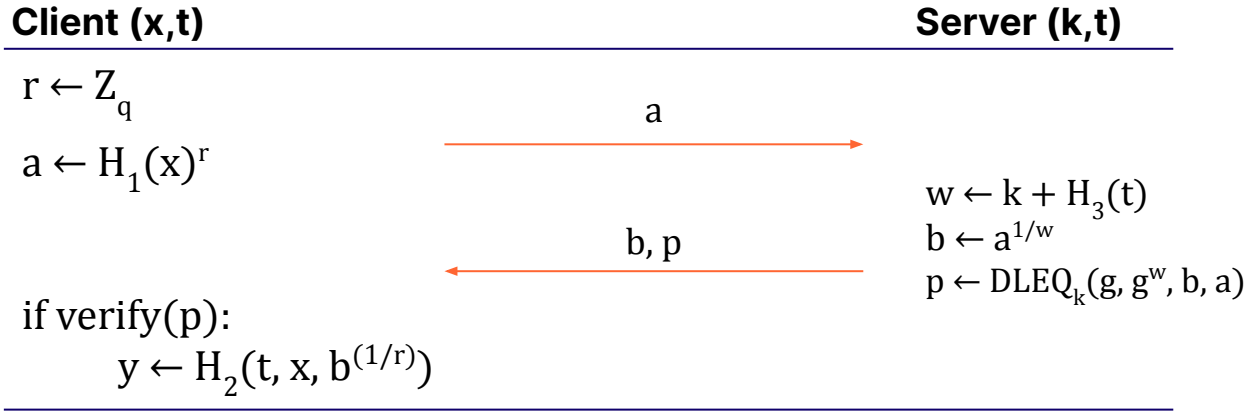
G, an elliptic curve group of order q.

$H_1 : \{0,1\}^* \rightarrow G$ (hash to curve function)

$H_2 : \{0,1\}^* \rightarrow \{0,1\}^n$ (hash function)

$H_3 : \{0,1\}^* \rightarrow \{0,1\}^{2n}$ (hash function)

DLEQ zk-proof



https://doi.org/10.1007/978-3-031-07085-3_23

CLOUDFLARE

Additional Properties

- Verifiability
  - Ensure the server used a committed key.
- Partial-Obliviousness
  - Additional public input.
- **Updatability**
  - Mechanisms to rotate the key.
  - See: https://ia.cr/2019/1275
- Threshold Scheme
  - Key distributed to several parties.

CLOUDFLARE

Additional Properties

- Verifiability
  - Ensure the server used a committed key.
- Partial-Obliviousness
  - Additional public input.
- Updatability
  - Mechanisms to rotate the key.
- **Threshold Scheme**
  - Key distributed to several parties.

CLOUDFLARE

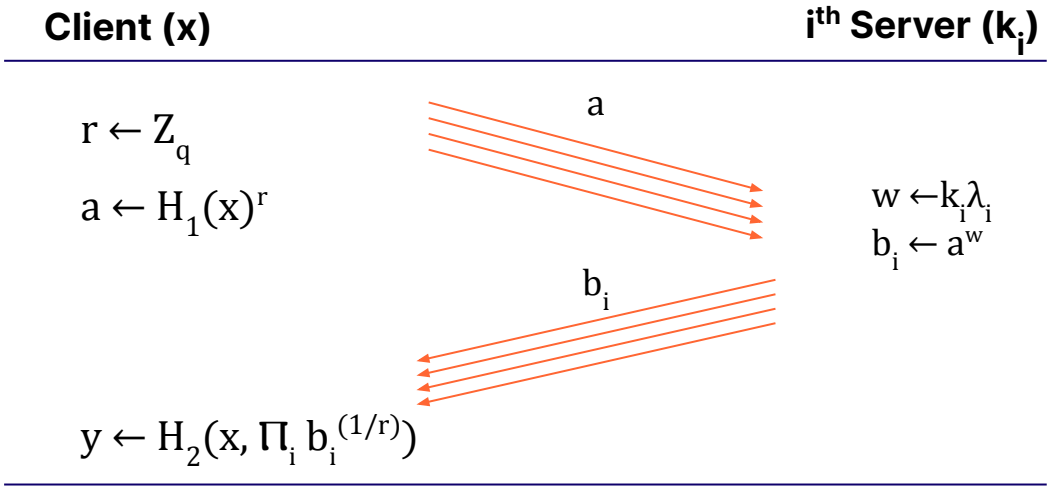
Threshold OPRF

Jarecki, Krawczyk, Resch (2018)

G, an elliptic curve group of order q.

$H_1 : \{0,1\}^* \rightarrow G$ (hash to curve function)

$H_2 : \{0,1\}^* \rightarrow \{0,1\}^n$ (hash function)



https://doi.org/10.1007/978-3-662-45608-8_13

CLOUDFLARE

Specification of OPRFs

Work in progress at CFRG/IETF.

Document:

draft-irtf-cfrg-voprf

Describes:

OPRF, VOPRF, POPRF

Ciphersuites:

P-384 & P-521 & Decaf448

Implementations:

C, Go, rust, Typescript, SageMath

https://datatracker.ietf.org/doc/draft-irtf-cfrg-voprf/

CLOUDFLARE

Points to Consider

Goal: Raise interest in the research, application, as well as in the standardization of OPRFs.

Specification for Threshold OPRFs.

Alternatives and other constructions.

Use cases and applications.

Threshold OPRF as a gadget for other protocols:

- t-PAKE.
- t-Authorization Tokens.

Thanks!

Cloudflare Research

ask-research@cloudflare.com

https://research.cloudflare.com