Leap

A Fast, Lattice-based OPRF with Application to Private Set Intersection

Lena Heimberger[†] Daniel Kales[♣] Riccardo Lolato[*] Omid Mir[◊]
Sebastian Ramacher[◊] Christian Rechberger[†,♣]

[†] Graz University of Technology [♣] Taceo [*] University of Trento (Work done @AIT)
[◊] Austrian Institute of Technology

Eurocrypt 2025

Main Results

- blazingly fast OPRF (online computation)

Main Results

- blazingly fast OPRF (online computation)
- unbalanced set intersection between 16 million and 32 thousand items in under a minute online, two minutes overall

Main Results

- blazingly fast OPRF (online computation)
- unbalanced set intersection between 16 million and 32 thousand items in under a minute online, two minutes overall
- simple arithmetic operations

Main Results

- blazingly fast OPRF (online computation)
- unbalanced set intersection between 16 million and 32 thousand items in under a minute online, two minutes overall
- simple arithmetic operations
- 1^{st} modification of 2HashDH UC proof for Naor-Reingold OPRF

Leap is an Oblivious Pseudorandom Function (OPRF)

Client

input $c \in \mathcal{C}$

gets y

compute

$$y := F_k(c)$$

Server

key $k \in \mathcal{K}$

Spring [Ban+15] is a lattice-based PRF

- 2014: heuristic LWR PRF with small modulus

Spring [Ban+15] is a lattice-based PRF

- 2014: heuristic LWR PRF with small modulus
- two modes:

Spring [Ban+15] is a lattice-based PRF

- 2014: heuristic LWR PRF with small modulus
- two modes:
  - Spring-BCH with $q = 257$

Spring [Ban+15] is a lattice-based PRF

- 2014: heuristic LWR PRF with small modulus
- two modes:
    - Spring-BCH with $q = 257$
    - Spring-CRT with $q = 514$

Spring [Ban+15] is a lattice-based PRF

- 2014: heuristic LWR PRF with small modulus
- two modes:
  - SPRING-BCH with $q = 257$
  - SPRING-CRT with $q = 514$
- focus in SPRING-BCH: rounding bias reduction using extended BCH code $[128, 64, 22]$

Spring [Ban+15] is a lattice-based PRF

- 2014: heuristic LWR PRF with small modulus
- two modes:
  - SPRING-BCH with $q = 257$
  - SPRING-CRT with $q = 514$
- focus in SPRING-BCH: rounding bias reduction using extended BCH code $[128, 64, 22]$

$$\mathcal{F}_{\mathbf{K}}(c_1, \cdots, c_m) = S\left(\mathbf{k}_0 \prod_{i=1}^{m} \mathbf{k}_i^{c_i}\right)$$

Spring [Ban+15] is a lattice-based PRF

- 2014: heuristic LWR PRF with small modulus
- two modes:
  - Spring-BCH with $q = 257$
  - Spring-CRT with $q = 514$
- focus in Spring-BCH: rounding bias reduction using extended BCH code $[128, 64, 22]$

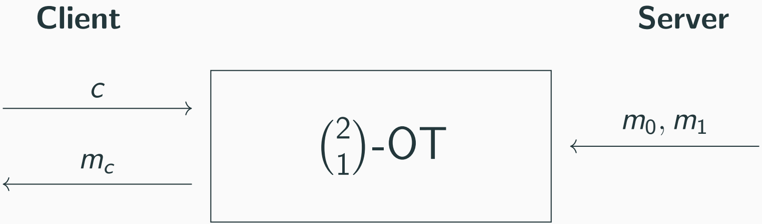
$$\mathcal{F}_{\mathbf{K}}(c_1, \cdots, c_m) = S\left(\mathrm{iNTT}\left(\mathbf{k}_0 \cdot \prod_{i=1}^{m} \mathbf{k}_i^{c_i}\right)\right)$$

Spring [Ban+15] is a lattice-based PRF

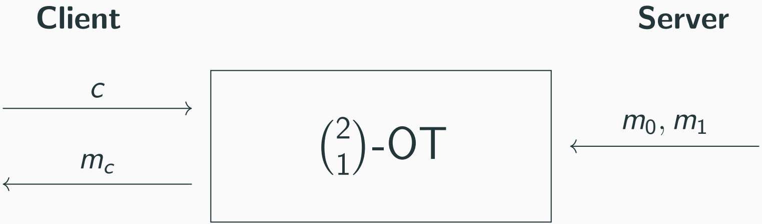
- 2014: heuristic LWR PRF with small modulus
- two modes:
  - Spring-BCH with $q = 257$
  - Spring-CRT with $q = 514$
- focus in Spring-BCH: rounding bias reduction using extended BCH code $[128, 64, 22]$

$$\mathcal{F}_{\mathbf{K}}(c_1, \cdots, c_m) = S\left(\mathrm{iNTT}\left(\mathrm{lookup}\left(\mathbf{k}_0 + \sum_{i=1}^{m} c_i \mathbf{k}_i\right)\right)\right)$$

A little help from MPC friends: Oblivious Transfer

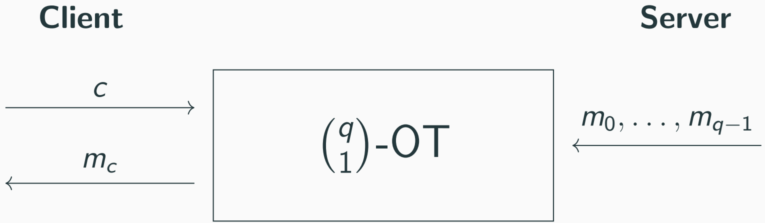


A little help from MPC friends: Oblivious Transfer

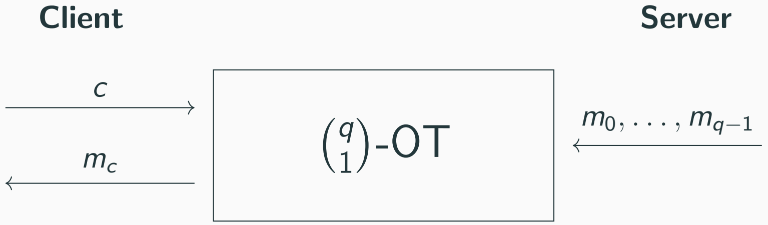


Extend with symmetric operations!

A little help from MPC friends: Oblivious Transfer (cont.)

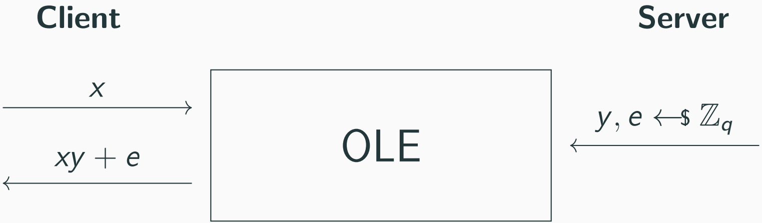


A little help from MPC friends: Oblivious Transfer (cont.)

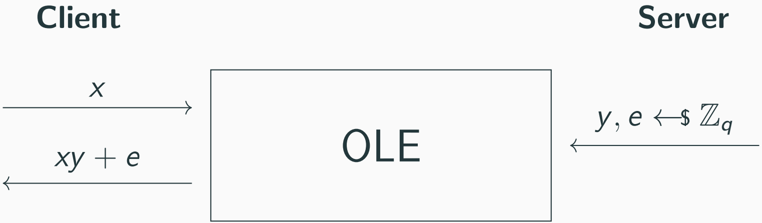


Generic construction from $\lceil \log q \rceil$ $\binom{2}{1}$-OTs !

A little help from MPC friends: Oblivious Linear Evaluation



A little help from MPC friends: Oblivious Linear Evaluation



Generic construction from $\lceil \log q \rceil$ $\binom{2}{1}$-OTs !

An OPRF from Spring

Client

$\mathbf{c} = [c_1, \ldots, c_m] \in \{0,1\}^m$

Server

$\mathbf{K} = [k_0, k_1, \ldots, k_m] \in \mathbb{Z}_{q-1}^{n \times (m+1)}$

$$\xrightarrow{c_i} \quad \boxed{\binom{2}{1}\text{-OT}} \quad \xleftarrow{\mathbf{r}_i,\, \mathbf{r}_i + \mathbf{k}_i}$$

$$\xleftarrow{\mathbf{r}_i + \mathbf{k}_i c_i}$$

$$S\left(\mathrm{iNTT}\left(\mathrm{lookup}\left(\mathbf{k}_0 + \sum_{i=1}^{m} c_i \mathbf{k}_i\right)\right)\right)$$

An OPRF from Spring

Client		**Server**
$\mathbf{c} = [c_1, \ldots, c_m] \in \{0,1\}^m$		$\mathbf{K} = [k_0, k_1, \ldots, k_m] \in \mathbb{Z}_{q-1}^{n \times (m+1)}$
$\xrightarrow{c_i}$	$\binom{2}{1}$-OT	$\xleftarrow{\mathbf{r}_i, \mathbf{r}_i + \mathbf{k}_i}$
$\xleftarrow{\mathbf{r}_i + \mathbf{k}_i c_i}$		
$\sum_{i=1}^{\kappa} \mathbf{r_i} + c_i \mathbf{k_i}$		$\mathbf{k}_0 - (\sum_{i=1}^{\kappa} \mathbf{r}_i)$

$$S\left(\mathrm{iNTT}\left(\mathrm{lookup}\left(\mathbf{k}_0 + \sum_{i=1}^{m} c_i \mathbf{k}_i\right)\right)\right)$$

An OPRF from Spring

Client		**Server**
$\mathbf{c} = [c_1, \ldots, c_m] \in \{0,1\}^m$		$\mathbf{K} = [k_0, k_1, \ldots, k_m] \in \mathbb{Z}_{q-1}^{n\times(m+1)}$
$\xrightarrow{c_i}$	$\binom{2}{1}$-OT	$\xleftarrow{\mathbf{r}_i, \mathbf{r}_i + \mathbf{k}_i}$
$\xleftarrow{\mathbf{r}_i + \mathbf{k}_i c_i}$		
$\sum_{i=1}^{\kappa} \mathbf{r_i} + c_i \mathbf{k_i}$	♻	$\mathbf{k}_0 - (\sum_{i=1}^{\kappa} \mathbf{r}_i)$
$\mathbf{b} \leftarrow \prod_{i=1}^{\kappa} \mathbf{r_i} \mathbf{k_i}^{c_i}$		$\mathbf{a} \leftarrow \mathbf{k}_0 (\prod_{i=1}^{\kappa} \mathbf{r}_i)^{-1}$

$$S\left(\mathrm{iNTT}\left(\mathrm{lookup}\left(\mathbf{k}_0 + \sum_{i=1}^{m} c_i \mathbf{k}_i\right)\right)\right)$$

An OPRF from Spring

$$S\left(\mathrm{iNTT}\left(\mathrm{lookup}\left(\mathbf{k}_0 + \sum_{i=1}^{m} c_i \mathbf{k}_i\right)\right)\right)$$

Client		**Server**
$\mathbf{c} = [c_1, \ldots, c_m] \in \{0,1\}^m$		$\mathbf{K} = [k_0, k_1, \ldots, k_m] \in \mathbb{Z}_{q-1}^{n\times(m+1)}$
$\xrightarrow{c_i}$	$\binom{2}{1}$-OT	$\xleftarrow{\mathbf{r}_i, \mathbf{r}_i + \mathbf{k}_i}$
$\xleftarrow{\mathbf{r}_i + \mathbf{k}_i c_i}$		
$\sum_{i=1}^{\kappa} \mathbf{r_i} + c_i \mathbf{k_i}$		$\mathbf{k}_0 - (\sum_{i=1}^{\kappa} \mathbf{r}_i)$
$\mathbf{b} \leftarrow \prod_{i=1}^{\kappa} \mathbf{r_i} \mathbf{k_i}^{c_i}$		$\mathbf{a} \leftarrow \mathbf{k}_0 (\prod_{i=1}^{\kappa} \mathbf{r}_i)^{-1}$
$\xrightarrow{b_i}$	OLE	$\xleftarrow{a_i, e_i \leftarrow\$\, \mathbb{Z}_q}$
$\xleftarrow{y_i = a_i b_i + e_i}$		

An OPRF from Spring

$$S\left(\mathrm{iNTT}\left(\mathrm{lookup}\left(\mathbf{k}_0 + \sum_{i=1}^{m} c_i \mathbf{k}_i\right)\right)\right)$$

Client		**Server**
$\mathbf{c} = [c_1, \ldots, c_m] \in \{0,1\}^m$		$\mathbf{K} = [k_0, k_1, \ldots, k_m] \in \mathbb{Z}_{q-1}^{n\times(m+1)}$
$\xrightarrow{c_i}$	$\binom{2}{1}$-OT	$\xleftarrow{\mathbf{r}_i, \mathbf{r}_i + \mathbf{k}_i}$
$\xleftarrow{\mathbf{r}_i + \mathbf{k}_i c_i}$		
$\sum_{i=1}^{\kappa} \mathbf{r_i} + c_i \mathbf{k_i}$	♻	$\mathbf{k}_0 - (\sum_{i=1}^{\kappa} \mathbf{r}_i)$
$\mathbf{b} \leftarrow \prod_{i=1}^{\kappa} \mathbf{r_i}\mathbf{k_i}^{c_i}$		$\mathbf{a} \leftarrow \mathbf{k}_0(\prod_{i=1}^{\kappa} \mathbf{r}_i)^{-1}$
$\xrightarrow{b_i}$	OLE	$\xleftarrow{a_i, e_i \leftarrow\$ \mathbb{Z}_q}$
$\xleftarrow{y_i = a_i b_i + e_i}$		
$\mathbf{y} \leftarrow \sum_{i=0}^{n-1}(a_i \cdot b_i + e_i)X^i$		$\mathbf{e} \leftarrow \sum_{i=0}^{n-1} e_i X^i$

An OPRF from Spring

$$S\left(\mathrm{iNTT}\left(\mathrm{lookup}\left(\mathbf{k}_0 + \sum_{i=1}^{m} c_i \mathbf{k}_i\right)\right)\right)$$

Client		**Server**
$\mathbf{c} = [c_1, \ldots, c_m] \in \{0,1\}^m$		$\mathbf{K} = [k_0, k_1, \ldots, k_m] \in \mathbb{Z}_{q-1}^{n\times(m+1)}$
$\xrightarrow{c_i}$	$\binom{2}{1}$-OT	$\xleftarrow{\mathbf{r}_i, \mathbf{r}_i + \mathbf{k}_i}$
$\xleftarrow{\mathbf{r}_i + \mathbf{k}_i c_i}$		
$\sum_{i=1}^{\kappa} \mathbf{r_i} + c_i \mathbf{k_i}$	♻	$\mathbf{k}_0 - (\sum_{i=1}^{\kappa} \mathbf{r}_i)$
$\mathbf{b} \leftarrow \prod_{i=1}^{\kappa} \mathbf{r_i} \mathbf{k_i}^{c_i}$		$\mathbf{a} \leftarrow \mathbf{k}_0 (\prod_{i=1}^{\kappa} \mathbf{r}_i)^{-1}$
$\xrightarrow{b_i}$	OLE	$\xleftarrow{a_i, e_i \leftarrow\$ \mathbb{Z}_q}$
$\xleftarrow{y_i = a_i b_i + e_i}$		
$\mathbf{y} \leftarrow \sum_{i=0}^{n-1} (a_i \cdot b_i + e_i) X^i$	iNTT	$\mathbf{e} \leftarrow \sum_{i=0}^{n-1} e_i X^i$

An OPRF from Spring

$$S\left(\mathrm{iNTT}\left(\mathrm{lookup}\left(\mathbf{k}_0 + \sum_{i=1}^{m} c_i \mathbf{k}_i\right)\right)\right)$$

Client | **Server**

$\mathbf{c} = [c_1, \ldots, c_m] \in \{0,1\}^m$ | $\mathbf{K} = [k_0, k_1, \ldots, k_m] \in \mathbb{Z}_{q-1}^{n\times(m+1)}$

$\xrightarrow{c_i}$ $\binom{2}{1}$-OT $\xleftarrow{\mathbf{r}_i, \mathbf{r}_i + \mathbf{k}_i}$

$\xleftarrow{\mathbf{r}_i + \mathbf{k}_i c_i}$

$\sum_{i=1}^{\kappa} \mathbf{r_i} + c_i \mathbf{k_i}$ | $\mathbf{k}_0 - (\sum_{i=1}^{\kappa} \mathbf{r}_i)$

$\mathbf{b} \leftarrow \prod_{i=1}^{\kappa} \mathbf{r_i}\mathbf{k_i}^{c_i}$ | $\mathbf{a} \leftarrow \mathbf{k}_0 (\prod_{i=1}^{\kappa} \mathbf{r}_i)^{-1}$

$\xrightarrow{b_i}$ OLE $\xleftarrow{a_i, e_i \leftarrow\$ \mathbb{Z}_q}$

$\xleftarrow{y_i = a_i b_i + e_i}$

$\mathbf{y} \leftarrow \sum_{i=0}^{n-1} (a_i \cdot b_i + e_i) X^i$ | $\mathbf{e} \leftarrow \sum_{i=0}^{n-1} e_i X^i$

iNTT

An OPRF from Spring

$$S\left(\mathrm{iNTT}\left(\mathrm{lookup}\left(\mathbf{k}_0 + \sum_{i=1}^{m} c_i \mathbf{k}_i\right)\right)\right)$$

Client | **Server**

$\mathbf{c} = [c_1, \ldots, c_m] \in \{0,1\}^m$ | $\mathbf{K} = [k_0, k_1, \ldots, k_m] \in \mathbb{Z}_{q-1}^{n\times(m+1)}$

$\xrightarrow{c_i}$ $\binom{2}{1}$-OT $\xleftarrow{\mathbf{r}_i, \mathbf{r}_i + \mathbf{k}_i}$

$\xleftarrow{\mathbf{r}_i + \mathbf{k}_i c_i}$

$\sum_{i=1}^{\kappa} \mathbf{r_i} + c_i \mathbf{k_i}$ ♻ $\mathbf{k}_0 - (\sum_{i=1}^{\kappa} \mathbf{r}_i)$

$\mathbf{b} \leftarrow \prod_{i=1}^{\kappa} \mathbf{r_i}\mathbf{k_i}^{c_i}$ | $\mathbf{a} \leftarrow \mathbf{k}_0(\prod_{i=1}^{\kappa} \mathbf{r}_i)^{-1}$

$\xrightarrow{b_i}$ OLE $\xleftarrow{a_i, e_i \leftarrow\$ \mathbb{Z}_q}$

$\xleftarrow{y_i = a_i b_i + e_i}$

$\mathbf{y} \leftarrow \sum_{i=0}^{n-1}(a_i \cdot b_i + e_i)X^i$ | $\mathbf{e} \leftarrow \sum_{i=0}^{n-1} e_i X^i$

iNTT

$\xrightarrow{y_i}$ $\binom{q}{1}$-OT $\xleftarrow{\lfloor(q_i - e_i)\rceil_p}$ $\forall q_i \in \mathbb{Z}_q$

$\xleftarrow{\lfloor y_i - e_i \rceil_p}$

An OPRF from Spring

$$S\left(\mathrm{iNTT}\left(\mathrm{lookup}\left(\mathbf{k}_0+\sum_{i=1}^{m} c_i\mathbf{k}_i\right)\right)\right)$$

Client		**Server**
$\mathbf{c}=[c_1,\ldots,c_m]\in\{0,1\}^m$		$\mathbf{K}=[k_0,k_1,\ldots,k_m]\in\mathbb{Z}_{q-1}^{n\times(m+1)}$
$\xrightarrow{c_i}$	$\binom{2}{1}$-OT	$\xleftarrow{\mathbf{r}_i,\mathbf{r}_i+\mathbf{k}_i}$
$\xleftarrow{\mathbf{r}_i+\mathbf{k}_i c_i}$		
$\sum_{i=1}^{\kappa}\mathbf{r_i}+c_i\mathbf{k_i}$	♻	$\mathbf{k}_0-(\sum_{i=1}^{\kappa}\mathbf{r}_i)$
$\mathbf{b}\leftarrow\prod_{i=1}^{\kappa}\mathbf{r_i}\mathbf{k_i}^{c_i}$		$\mathbf{a}\leftarrow\mathbf{k}_0(\prod_{i=1}^{\kappa}\mathbf{r}_i)^{-1}$
$\xrightarrow{b_i}$	OLE	$\xleftarrow{a_i,\,e_i\,\leftarrow\$\,\mathbb{Z}_q}$
$\xleftarrow{y_i=a_ib_i+e_i}$		
$\mathbf{y}\leftarrow\sum_{i=0}^{n-1}(a_i\cdot b_i+e_i)X^i$	iNTT	$\mathbf{e}\leftarrow\sum_{i=0}^{n-1}e_iX^i$
		$\mathbf{d}\leftarrow\$\,\{0,1\}^n$
$\xrightarrow{y_i}$	$\binom{q}{1}$-OT	$\xleftarrow{\lfloor(q_i-e_i)\rceil_p\oplus d_i}$
$\xleftarrow{\lfloor y_i-e_i\rceil_p\oplus d_i}$		$\forall q_i\in\mathbb{Z}_q$
$\xleftarrow{\mathrm{BCH}(\mathbf{d})}$		

Precomputation

Client

$\mathbf{c} = [c_1, \ldots, c_m] \in \{0,1\}^m$

Server

$\mathbf{K} = [k_0, k_1, \ldots, k_m] \in \mathbb{Z}_{q-1}^{n\times(m+1)}$

- input length $m = 128$

Precomputation

Client $\mathbf{c} = [c_1, \ldots, c_m] \in \{0,1\}^m$

Server $\mathbf{K} = [k_0, k_1, \ldots, k_m] \in \mathbb{Z}_{q-1}^{n\times(m+1)}$

$$\text{Client} \xrightarrow{c_i} \boxed{\tbinom{2}{1}\text{-OT}} \xleftarrow{\mathbf{r}_i,\, \mathbf{r}_i + \mathbf{k}_i} \text{Server}$$

$$\text{Client} \xleftarrow{\mathbf{r}_i + \mathbf{k}_i c_i} \boxed{\tbinom{2}{1}\text{-OT}}$$

- input length $m = 128$
- m $\binom{2}{1}$-OTs

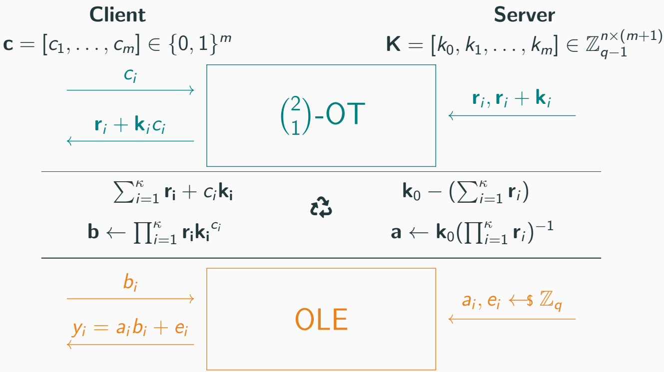
Precomputation

- input length $m = 128$
- m $\binom{2}{1}$-OTs
- polynomial degree $n = 128$, modulus $q = 257$, $\lceil \log q \rceil = 9$

Client		Server
$\mathbf{c} = [c_1, \ldots, c_m] \in \{0,1\}^m$		$\mathbf{K} = [k_0, k_1, \ldots, k_m] \in \mathbb{Z}_{q-1}^{n \times (m+1)}$
$\xrightarrow{c_i}$	$\binom{2}{1}$-OT	$\xleftarrow{\mathbf{r}_i,\, \mathbf{r}_i + \mathbf{k}_i}$
$\xleftarrow{\mathbf{r}_i + \mathbf{k}_i c_i}$		
$\sum_{i=1}^{\kappa} \mathbf{r_i} + c_i \mathbf{k_i}$		$\mathbf{k}_0 - (\sum_{i=1}^{\kappa} \mathbf{r}_i)$
$\mathbf{b} \leftarrow \prod_{i=1}^{\kappa} \mathbf{r_i} \mathbf{k_i}^{c_i}$		$\mathbf{a} \leftarrow \mathbf{k}_0 (\prod_{i=1}^{\kappa} \mathbf{r}_i)^{-1}$

Precomputation

- input length $m = 128$
- m $\binom{2}{1}$-OTs
- polynomial degree $n = 128$, modulus $q = 257$, $\lceil \log q \rceil = 9$
- $N \log q$ $\binom{2}{1}$-OTs $= 1152$



Precomputation

- input length $m = 128$
- m $\binom{2}{1}$-OTs
- polynomial degree $n = 128$, modulus $q = 257$, $\lceil \log q \rceil = 9$
- $N \log q$ $\binom{2}{1}$-OTs $= 1152$

Client | **Server**

$\mathbf{c} = [c_1, \ldots, c_m] \in \{0,1\}^m$ | $\mathbf{K} = [k_0, k_1, \ldots, k_m] \in \mathbb{Z}_{q-1}^{n\times(m+1)}$

$\xrightarrow{c_i}$ $\boxed{\binom{2}{1}\text{-OT}}$ $\xleftarrow{\mathbf{r}_i,\, \mathbf{r}_i + \mathbf{k}_i}$

$\xleftarrow{\mathbf{r}_i + \mathbf{k}_i c_i}$

$\sum_{i=1}^{\kappa} \mathbf{r_i} + c_i \mathbf{k_i}$ | $\mathbf{k}_0 - (\sum_{i=1}^{\kappa} \mathbf{r}_i)$

$\mathbf{b} \leftarrow \prod_{i=1}^{\kappa} \mathbf{r_i} \mathbf{k_i}^{c_i}$ | $\mathbf{a} \leftarrow \mathbf{k}_0 (\prod_{i=1}^{\kappa} \mathbf{r}_i)^{-1}$

$\xrightarrow{b_i}$ $\boxed{\text{OLE}}$ $\xleftarrow{a_i,\, e_i \leftarrow_{\$} \mathbb{Z}_q}$

$\xleftarrow{y_i = a_i b_i + e_i}$

$\mathbf{y} \leftarrow \sum_{i=0}^{n-1} (a_i \cdot b_i + e_i) X^i$ | $\mathbf{e} \leftarrow \sum_{i=0}^{n-1} e_i X^i$

iNTT

Precomputation

- input length $m = 128$
- m $\binom{2}{1}$-OTs
- polynomial degree $n = 128$, modulus $q = 257$, $\lceil \log q \rceil = 9$
- $N \log q$ $\binom{2}{1}$-OTs $= 1152$
- $N \log q$ $\binom{2}{1}$-OTs $= 1152$

Client

$\mathbf{c} = [c_1, \ldots, c_m] \in \{0,1\}^m$

Server

$\mathbf{K} = [k_0, k_1, \ldots, k_m] \in \mathbb{Z}_{q-1}^{n \times (m+1)}$

$\xrightarrow{c_i}$ $\binom{2}{1}$-OT $\xleftarrow{\mathbf{r}_i, \mathbf{r}_i + \mathbf{k}_i}$

$\xleftarrow{\mathbf{r}_i + \mathbf{k}_i c_i}$

$\sum_{i=1}^{\kappa} \mathbf{r_i} + c_i \mathbf{k_i}$ ♻ $\mathbf{k}_0 - (\sum_{i=1}^{\kappa} \mathbf{r}_i)$

$\mathbf{b} \leftarrow \prod_{i=1}^{\kappa} \mathbf{r_i} \mathbf{k_i}^{c_i}$ $\mathbf{a} \leftarrow \mathbf{k}_0 (\prod_{i=1}^{\kappa} \mathbf{r}_i)^{-1}$

$\xrightarrow{b_i}$ OLE $\xleftarrow{a_i, e_i \leftarrow_{\$} \mathbb{Z}_q}$

$\xleftarrow{y_i = a_i b_i + e_i}$

$\mathbf{y} \leftarrow \sum_{i=0}^{n-1} (a_i \cdot b_i + e_i) X^i$ $\mathbf{e} \leftarrow \sum_{i=0}^{n-1} e_i X^i$

iNTT

$\xrightarrow{y_i}$ $\binom{q}{1}$-OT $\xleftarrow{\lfloor (q_i - e_i) \rceil_p}$ $\forall q_i \in \mathbb{Z}_q$

$\xleftarrow{\lfloor y_i - e_i \rceil_p}$

Precomputation

- input length $m = 128$
- m $\binom{2}{1}$-OTs
- polynomial degree $n = 128$, modulus $q = 257$, $\lceil \log q \rceil = 9$
- $N \log q$ $\binom{2}{1}$-OTs $= 1152$
- $N \log q$ $\binom{2}{1}$-OTs $= 1152$
- 2432 OTs

Client

$\mathbf{c} = [c_1, \ldots, c_m] \in \{0,1\}^m$

Server

$\mathbf{K} = [k_0, k_1, \ldots, k_m] \in \mathbb{Z}_{q-1}^{n\times(m+1)}$

$\xrightarrow{c_i}$ $\binom{2}{1}$-OT $\xleftarrow{\mathbf{r}_i, \mathbf{r}_i + \mathbf{k}_i}$

$\xleftarrow{\mathbf{r}_i + \mathbf{k}_i c_i}$

$\sum_{i=1}^{\kappa} \mathbf{r_i} + c_i \mathbf{k_i}$ ♻ $\mathbf{k}_0 - (\sum_{i=1}^{\kappa} \mathbf{r}_i)$

$\mathbf{b} \leftarrow \prod_{i=1}^{\kappa} \mathbf{r_i} \mathbf{k_i}^{c_i}$ $\mathbf{a} \leftarrow \mathbf{k}_0 (\prod_{i=1}^{\kappa} \mathbf{r}_i)^{-1}$

$\xrightarrow{b_i}$ OLE $\xleftarrow{a_i, e_i \leftarrow_\$ \mathbb{Z}_q}$

$\xleftarrow{y_i = a_i b_i + e_i}$

$\mathbf{y} \leftarrow \sum_{i=0}^{n-1} (a_i \cdot b_i + e_i) X^i$ $\mathbf{e} \leftarrow \sum_{i=0}^{n-1} e_i X^i$

iNTT

$\xrightarrow{y_i}$ $\binom{q}{1}$-OT $\xleftarrow[\forall q_i \in \mathbb{Z}_q]{\lfloor (q_i - e_i) \rceil_p}$

$\xleftarrow{\lfloor y_i - e_i \rceil_p}$

Precomputation

- input length $m = 128$
- m $\binom{2}{1}$-OTs
- polynomial degree $n = 128$, modulus $q = 257$, $\lceil \log q \rceil = 9$
- $N \log q$ $\binom{2}{1}$-OTs $= 1152$
- $N \log q$ $\binom{2}{1}$-OTs $= 1152$
- ~~2432~~ 128 base OTs + OT extension

Client | **Server**

$\mathbf{c} = [c_1, \ldots, c_m] \in \{0,1\}^m$ | $\mathbf{K} = [k_0, k_1, \ldots, k_m] \in \mathbb{Z}_{q-1}^{n \times (m+1)}$

$\binom{2}{1}$-OT: Client sends c_i, receives $\mathbf{r}_i + \mathbf{k}_i c_i$; Server inputs $\mathbf{r}_i, \mathbf{r}_i + \mathbf{k}_i$

$\sum_{i=1}^{\kappa} \mathbf{r_i} + c_i \mathbf{k_i}$ | $\mathbf{k}_0 - (\sum_{i=1}^{\kappa} \mathbf{r}_i)$

$\mathbf{b} \leftarrow \prod_{i=1}^{\kappa} \mathbf{r_i} \mathbf{k_i}^{c_i}$ | $\mathbf{a} \leftarrow \mathbf{k}_0 (\prod_{i=1}^{\kappa} \mathbf{r}_i)^{-1}$

OLE: Client sends b_i, receives $y_i = a_i b_i + e_i$; Server inputs $a_i, e_i \leftarrow\$ \mathbb{Z}_q$

$\mathbf{y} \leftarrow \sum_{i=0}^{n-1} (a_i \cdot b_i + e_i) X^i$ | $\mathbf{e} \leftarrow \sum_{i=0}^{n-1} e_i X^i$

iNTT

$\binom{q}{1}$-OT: Client sends y_i, receives $\lfloor y_i - e_i \rceil_p$; Server inputs $\lfloor (q_i - e_i) \rceil_p$ $\forall q_i \in \mathbb{Z}_q$

Online Communication

Client

$\mathbf{c} = [c_1, \ldots, c_m] \in \{0, 1\}^m$

Server

$\mathbf{K} = [k_0, k_1, \ldots, k_m] \in \mathbb{Z}_{q-1}^{n \times (m+1)}$

Online Communication

Client

$\mathbf{c} = [c_1, \ldots, c_m] \in \{0,1\}^m$

Server

$\mathbf{K} = [k_0, k_1, \ldots, k_m] \in \mathbb{Z}_{q-1}^{n\times(m+1)}$

$$\xrightarrow{\binom{2}{1}\text{-OT correction bits}}$$

$$\xleftarrow{\text{correction polynomials}}$$

Online Communication

Client		**Server**
$\mathbf{c} = [c_1, \ldots, c_m] \in \{0,1\}^m$		$\mathbf{K} = [k_0, k_1, \ldots, k_m] \in \mathbb{Z}_{q-1}^{n\times(m+1)}$
m bits	$\xrightarrow{\binom{2}{1}\text{-OT correction bits}}$	$mN(q-1)$ bits
	$\xleftarrow{\text{correction polynomials}}$	

Online Communication

Client		**Server**
$\mathbf{c} = [c_1, \ldots, c_m] \in \{0,1\}^m$		$\mathbf{K} = [k_0, k_1, \ldots, k_m] \in \mathbb{Z}_{q-1}^{n\times(m+1)}$
m bits	$\xrightarrow{\binom{2}{1}\text{-OT correction bits}}$	$mN(q-1)$ bits
16 bytes	$\xleftarrow{\text{correction polynomials}}$	16 384 bytes

Online Communication

Client		Server
$\mathbf{c} = [c_1, \ldots, c_m] \in \{0,1\}^m$		$\mathbf{K} = [k_0, k_1, \ldots, k_m] \in \mathbb{Z}_{q-1}^{n\times(m+1)}$
m bits	$\xrightarrow{\binom{2}{1}\text{-OT correction bits}}$	$mN(q-1)$ bits
16 bytes	$\xleftarrow{\text{correction polynomials}}$ ♻	16 384 bytes

Online Communication

Client		**Server**
$\mathbf{c} = [c_1, \ldots, c_m] \in \{0,1\}^m$		$\mathbf{K} = [k_0, k_1, \ldots, k_m] \in \mathbb{Z}_{q-1}^{n\times(m+1)}$
m bits	$\binom{2}{1}$-OT correction bits $\longrightarrow$	$mN(q-1)$ bits
16 bytes	$\longleftarrow$ correction polynomials	16 384 bytes
	♻	
	OLE correction bits $\longrightarrow$	
	$\longleftarrow$ packed OLE corrections	

Online Communication

Client		**Server**
$\mathbf{c} = [c_1, \ldots, c_m] \in \{0,1\}^m$		$\mathbf{K} = [k_0, k_1, \ldots, k_m] \in \mathbb{Z}_{q-1}^{n \times (m+1)}$
m bits	$\xrightarrow{\binom{2}{1}\text{-OT correction bits}}$	$mN(q-1)$ bits
16 bytes	$\xleftarrow{\text{correction polynomials}}$	16 384 bytes
$N \log q$ bits	$\xrightarrow{\text{OLE correction bits}}$	$N \log q \log q$ bits
	$\xleftarrow{\text{packed OLE corrections}}$	

Online Communication

Client		Server
$\mathbf{c} = [c_1, \ldots, c_m] \in \{0,1\}^m$		$\mathbf{K} = [k_0, k_1, \ldots, k_m] \in \mathbb{Z}_{q-1}^{n\times(m+1)}$
m bits	$\binom{2}{1}$-OT correction bits $\longrightarrow$	$mN(q-1)$ bits
16 bytes	$\longleftarrow$ correction polynomials	16 384 bytes
$N \log q$ bits	OLE correction bits $\longrightarrow$	$N \log q \log q$ bits
144 bytes	$\longleftarrow$ packed OLE corrections	1 296 bytes

Online Communication

Client		**Server**
$\mathbf{c} = [c_1, \ldots, c_m] \in \{0,1\}^m$		$\mathbf{K} = [k_0, k_1, \ldots, k_m] \in \mathbb{Z}_{q-1}^{n \times (m+1)}$
m bits	$\binom{2}{1}$-OT correction bits $\longrightarrow$	$mN(q-1)$ bits
16 bytes	$\longleftarrow$ correction polynomials	16 384 bytes
$N \log q$ bits	OLE correction bits $\longrightarrow$	$N \log q \log q$ bits
144 bytes	$\longleftarrow$ packed OLE corrections	1 296 bytes
	iNTT	

Online Communication

Client		**Server**
$\mathbf{c} = [c_1, \ldots, c_m] \in \{0,1\}^m$		$\mathbf{K} = [k_0, k_1, \ldots, k_m] \in \mathbb{Z}_{q-1}^{n\times(m+1)}$
m bits	$\binom{2}{1}$-OT correction bits $\longrightarrow$	$mN(q-1)$ bits
16 bytes	$\longleftarrow$ correction polynomials	16 384 bytes
	♻	
$N \log q$ bits	OLE correction bits $\longrightarrow$	$N \log q \log q$ bits
144 bytes	$\longleftarrow$ packed OLE corrections	1 296 bytes
	iNTT	
	rounding corrections $\longrightarrow$	
	$\longleftarrow$ packed rounding results	

Online Communication

Client		Server
$\mathbf{c} = [c_1, \ldots, c_m] \in \{0,1\}^m$		$\mathbf{K} = [k_0, k_1, \ldots, k_m] \in \mathbb{Z}_{q-1}^{n\times(m+1)}$
m bits	$\binom{2}{1}$-OT correction bits $\longrightarrow$	$mN(q-1)$ bits
16 bytes	$\longleftarrow$ correction polynomials	16 384 bytes
	♻	
$N \log q$ bits	OLE correction bits $\longrightarrow$	$N \log q \log q$ bits
144 bytes	$\longleftarrow$ packed OLE corrections	1 296 bytes
	iNTT	
$N \log q$ bits	rounding corrections $\longrightarrow$	Nq bits
	$\longleftarrow$ packed rounding results	

Online Communication

Client		Server
$\mathbf{c} = [c_1, \ldots, c_m] \in \{0,1\}^m$		$\mathbf{K} = [k_0, k_1, \ldots, k_m] \in \mathbb{Z}_{q-1}^{n\times(m+1)}$
m bits	$\binom{2}{1}$-OT correction bits $\longrightarrow$	$mN(q-1)$ bits
16 bytes	$\longleftarrow$ correction polynomials	16 384 bytes
$N \log q$ bits	OLE correction bits $\longrightarrow$	$N \log q \log q$ bits
144 bytes	$\longleftarrow$ packed OLE corrections	1 296 bytes
	iNTT	
$N \log q$ bits	rounding corrections $\longrightarrow$	Nq bits
144 bytes	$\longleftarrow$ packed rounding results	4 112 bytes

Online Communication

Client		Server
$\mathbf{c} = [c_1, \ldots, c_m] \in \{0,1\}^m$		$\mathbf{K} = [k_0, k_1, \ldots, k_m] \in \mathbb{Z}_{q-1}^{n\times(m+1)}$
m bits	$\binom{2}{1}$-OT correction bits $\longrightarrow$	$mN(q-1)$ bits
16 bytes	$\longleftarrow$ correction polynomials	16 384 bytes
	♻	
$N \log q$ bits	OLE correction bits $\longrightarrow$	$N \log q \log q$ bits
144 bytes	$\longleftarrow$ packed OLE corrections	1 296 bytes
	iNTT	
$N \log q$ bits	rounding corrections $\longrightarrow$	$Nq + \lvert\mathrm{BCH}\rvert$ bits
144 bytes	$\longleftarrow$ packed rounding results + BCH code	4 120 bytes

Online Communication

Client		Server
$\mathbf{c} = [c_1, \ldots, c_m] \in \{0,1\}^m$		$\mathbf{K} = [k_0, k_1, \ldots, k_m] \in \mathbb{Z}_{q-1}^{n\times(m+1)}$
m bits	$\binom{2}{1}$-OT correction bits $\longrightarrow$	$mN(q-1)$ bits
16 bytes	$\longleftarrow$ correction polynomials	16 384 bytes
	♻	
$N \log q$ bits	OLE correction bits $\longrightarrow$	$N \log q \log q$ bits
144 bytes	$\longleftarrow$ packed OLE corrections	1 296 bytes
	iNTT	
$N \log q$ bits	rounding corrections $\longrightarrow$	$Nq + \lvert\mathrm{BCH}\rvert$ bits
144 bytes	$\longleftarrow$ packed rounding results + BCH code	4 120 bytes
304 bytes		**22 kB**

Online Communication

Client		Server
$\mathbf{c} = [c_1, \ldots, c_m] \in \{0,1\}^m$		$\mathbf{K} = [k_0, k_1, \ldots, k_m] \in \mathbb{Z}_{q-1}^{n\times(m+1)}$
m bits	$\binom{2}{1}$-OT correction bits $\longrightarrow$	$mN(q-1)$ bits
16 bytes	$\longleftarrow$ correction polynomials	16 384 bytes
$N \log q$ bits	OLE correction bits $\longrightarrow$	$N \log q \log q$ bits
144 bytes	$\longleftarrow$ packed OLE corrections	1 296 bytes
	iNTT	
$N \log q$ bits	rounding corrections $\longrightarrow$	$Nq + \lvert\mathrm{BCH}\rvert$ bits
144 bytes	$\longleftarrow$ packed rounding results + BCH code	4 120 bytes
304 bytes		**22 kB**
11 μs		**227 μs**

Online Communication

Client		Server
$\mathbf{c} = [c_1, \ldots, c_m] \in \{0,1\}^m$		$\mathbf{K} = [k_0, k_1, \ldots, k_m] \in \mathbb{Z}_{q-1}^{n\times(m+1)}$
m bits	$\binom{2}{1}$-OT correction bits $\longrightarrow$	$mN(q-1)$ bits
16 bytes	$\longleftarrow$ correction polynomials	16 384 bytes
$N \log q$ bits	OLE correction bits $\longrightarrow$	$N \log q \log q$ bits
144 bytes	$\longleftarrow$ packed OLE corrections	1 296 bytes
	iNTT	
$N \log q$ bits	rounding corrections $\longrightarrow$	$Nq + \lvert\mathrm{BCH}\rvert$ bits
144 bytes	$\longleftarrow$ packed rounding results + BCH code	4 120 bytes
304 bytes **11 μs**	**+ network overhead**	**22 kB** **227 μs**

Interchangable Building Blocks: Precomputation Numbers

#	Protocol	Communication		Computation	
		Client	Server	Client	Server
2^0	Simplest OT+IKNP	39 kB	**4 kB**	63 ms	63 ms
	Kyber OT+IKNP	465 kB	328 kB	**10 ms**	**10 ms**
	Simplest OT+Silent	**22 kB**	22 kB	68 ms	68 ms
	Kyber OT+Silent	448 kB	392 kB	**10 ms**	10 ms
2^{13}	Simplest OT+IKNP	319 MB	**4.26 kB**	420 ms	463 ms
	Kyber OT+IKNP	319 MB	328 kB	**311 ms**	**423 ms**
	Simplest OT+Silent	**46 kB**	155 kB	2065 ms	3371 ms
	Kyber OT+Silent	487 kB	559 kB	2130 ms	3496 ms

Application: Private Set Intersection (PSI)

- unlikely to replace 2HashDH

Application: Private Set Intersection (PSI)

- unlikely to replace 2HashDH
  - not verifiable (and unlikely to be)

Application: Private Set Intersection (PSI)

- unlikely to replace 2HashDH
  - not verifiable (and unlikely to be)
  - great for applications that need many OPRF calls, like PSI

Application: Private Set Intersection (PSI)

- unlikely to replace 2HashDH
  - not verifiable (and unlikely to be)
  - great for applications that need many OPRF calls, like PSI

Client $(x_1, \ldots, x_m)$ **Server** $(y_1, \ldots, y_n), k$

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

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

Application: Private Set Intersection (PSI)

- unlikely to replace 2HashDH
  - not verifiable (and unlikely to be)
  - great for applications that need many OPRF calls, like PSI

Client $(x_1, \ldots, x_m)$ **Server** $(y_1, \ldots, y_n), k$

$\{F_k(x_i)\}_{i \in [m]}$ $\xleftrightarrow{\hspace{4em} OPRF \hspace{4em}}$

$\xleftarrow{\hspace{2em} \{z_j = F_k(y_i)\}_{j \in [n]} \hspace{2em}}$

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

	Parameters		Setup		Online	
	$\|S\|$	$\|C\|$	$\|S\|$	$\|C\|$	$\|S\|$	$\|C\|$
Leap (IKNP+Kyber)	2^0	2^0	1 ms 117 bytes	1 ms 0 bytes	0.2s 73.4 kiB	6 ms 20 KiB
	2^5	2^5	1 ms 246 bytes	1 ms 0 bytes	0.08 s 802 kiB	0.07 s 47.5 kiB
	2^{10}	2^{10}	4 ms 4.30 kiB	5 ms 0 bytes	2.4 s 22.39 MiB	2.46 s 646.5 kiB
NR-OT (FHE OT) [Hei+24]	2^0	2^0	0.26 s 134 bytes	0.51 s 1 byte	0.06 s 128 kiB	0.10 s 0.75MiB
	2^5	2^5	1.63 s 263 bytes	1.88 s 1 byte	3.11 s 4MiB	3.15 s 8.5 MiB
	2^{10}	2^{10}	45.04 s 4.31 MiB	45.28 s 1 byte	99.66 s 128 MiB	99.71 s 256.6 MiB
OPUS [Hei+24]	2^0	2^0	0.26 s 133 bytes	0.26 s 0 bytes	15.47 s 17.07 kiB	15.91 s 9.04 kiB
	2^5	2^5	8.71 s 262 bytes	8.71 s 0 bytes	328.46 s 546.25 kiB	329.14 s 290.26 kiB
	2^{10}	2^{10}	303.38 s 4.31 kiB	303.38 s 0 bytes	16367.12 s 34.14 MiB	16367.60 s 18.08 MiB
ECNR (Simplest OT + IKNP) [Kal+19]	2^0	2^0	10 ms 133 bytes	0 s 0 bytes	0.23 s 12.04 kiB	0.05 s 16 bytes
	2^5	2^5	0.02 s 262 bytes	0 s 0 bytes	0.21 s 137.05 kiB	0.06 s 512 bytes
	2^{10}	2^{10}	0.3 s 4.36 kiB	0 s 0 bytes	0.64 s 4.04 MiB	0.57 s 16 kiB

work	assumption	rounds	comm. cost	security(C-S)	preprocessing	no trusted setup	verifiable	available
ADDS21	(R)LWE+SIS	2	2 MB	semihonest-semihonest	-	YES	NO	YES
ADDS21	(R)LWE+SIS	2	128 GB	malicious-malicious	-	YES	YES	NO
AG24	(R)LWE+SIS	2	316 kB	malicious-malicious	221.5 kB	YES	YES	NO
ADDG23	mod(2,3)+lattices	2	10 KB	malicious-semihonest	2.5 MB	YES	NO	NO
ADDG23	mod(2,3)+lattices	2	160 KB	malicious-semihonest	2.5 MB	YES	YES	NO
HKL+25	heuristic LWR	6	23 KB	semihonest-semihonest	793 KB	YES	NO	YES
ESTX24	iMLWER-RU+MLE+SIS	2	126 KB*	malicious-malicious	10 KB	YES	YES	NO
APRR24	mod(2,3)	2	916 bits	malicious-semihonest	38 bits	YES	YES	NO
DGH+21	mod(2,3)	2	641 bits	semihonest-semihonest	1836 bits	NO	NO	NO
SHB23	Legendre PRF	3	13 kB	semihonest-semihonest	?	YES	YES	NO
KCM24	Legendre PRF	2	?	semihonest-semihonest	?	YES	YES	YES
BDFH24	Legendre PRF as 2HashDH	9	356 KB	malicious-malicious	392 kB	YES	YES	YES
YBHKR24	generalized power residue (Legendre) PRF	3	774 kB	malicious-semihonest	-	YES	YES	NO
YBHKR24	generalized power residue (Legendre) PRF	3	970 kB	malicious-malicious	-	YES	YES	NO
FOO23	AES+Garbled Circuits	2	6.79MB	semihonest-semihonest	-	YES	NO	YES
HKLS24	Minicrypt	?	22 bytesÂ¶	malicious-malicious	-	YES	NO	NO
Basso23	Isogenies F_p^2	2	3.0 MB	malicious-malicious	-	NO	NO	NO
Basso23	Isogenies F_p^2	2	8.7 MB	malicious-malicious	-	NO	YES	NO
Basso24	Higher-Dimensional isogenies	2	28.9 kB	malicious-malicious	-	YES	YES	YES
BKW20	Isogenies F_p + lattices	2	20.54 kB	semihonest-semihonest	-	NO	NO	NO
BKW20	Isogenies F_p + lattices	4	34.88 kB	malicious-semihonest	-	NO	NO	NO
HHM+23	Isogenies F_p + lattices + HE OT	2	640 kB	semihonest-semihonest	-	YES	NO	YES
HHM+23	Isogenies F_p	258	24.7 kB	semihonest-semihonest	-	YES	NO	YES
dSP23	Isogenies F_p	2	384 bytes	malicious-semihonest	68.4 kB	YES	YES	NO
dSP23	Isogenies F_p	2	16.38 kB	malicious-semihonest	-	YES	YES	NO

work	assumption	rounds	comm. cost	security(C-S)	preprocessing	no trusted setup	verifiable	available
ADDS21	(R)LWE+SIS					YES	NO	YES
ADDS21	(R)LWE+SIS					YES	YES	NO
AG24	(R)LWE+SIS				kB	YES	YES	NO
ADDG23	mod(2,3)+lattices				MB	YES	NO	NO
ADDG23	mod(2,3)+lattices				MB	YES	YES	NO
HKL+25	heuristic LWR				KB	YES	NO	YES
ESTX24	iMLWER-RU+MLE+SIS				B	YES	YES	NO
APRR24	mod(2,3)				ts	YES	YES	NO
DGH+21	mod(2,3)				its	NO	NO	NO
SHB23	Legendre PRF					YES	YES	NO
KCM24	Legendre PRF					YES	YES	YES
BDFH24	Legendre PRF as 2HashDH				kB	YES	YES	YES
YBHKR24	generalized power residue (Legendre					YES	YES	NO
YBHKR24	generalized power residue (Legendre					YES	YES	NO
FOO23	AES+Garbled Circuits					YES	NO	YES
HKLS24	Minicrypt					YES	NO	NO
Basso23	Isogenies F_p^2					NO	NO	NO
Basso23	Isogenies F_p^2					NO	YES	NO
Basso24								YES
BKW20								NO
BKW20								NO
HHM+23								YES
HHM+23								YES
dSP23	Isogenies F_p	2	384 bytes	malicious-semihonest	68.4 kB	YES	YES	NO
dSP23	Isogenies F_p	2	16.38 kB	malicious-semihonest	-	YES	YES	NO

heimberger.xyz/oprfs.html

Leap

A Fast, Lattice-based OPRF with Application to Private Set Intersection

Lena Heimberger[†] Daniel Kales[♣] Riccardo Lolato[*] Omid Mir[◊]
Sebastian Ramacher[◊] Christian Rechberger[†,♣]

[†] Graz University of Technology [♣] Taceo [*] University of Trento (Work done @AIT)
[◊] Austrian Institute of Technology

Eurocrypt 2025

Performance

Phase	Client			Server		
	Comm.	Comp.	Idle	Comm.	Comp.	Idle
Subset-Sum	16 bytes	5 μs	21 μs	16 384 bytes	863 μs	46 μs
OLE	144 bytes	4 μs	3 μs	1 296 bytes	72 μs	88 μs
Rounding	144 bytes	2 μs	726 μs	4 118 bytes	814 μs	67 μs
BCH	0 bytes	1 μs	0 μs	8 bytes	/	26 μs
Overall (Network)	304 bytes (328 bytes)	11 μs	750 μs	21 806 bytes (22 840 bytes)	1.7 ms	227 μs

References

[Ban+15] Abhishek Banerjee et al. "SPRING: Fast Pseudorandom Functions from Rounded Ring Products". In: *FSE 2014*. Ed. by Carlos Cid and Christian Rechberger. Vol. 8540. LNCS. Springer, Berlin, Heidelberg, Mar. 2015, pp. 38–57. DOI: 10.1007/978-3-662-46706-0_3.

[Hei+24] Lena Heimberger et al. "OPRFs from Isogenies: Designs and Analysis". In: *ASIACCS 24*. Ed. by Jianying Zhou et al. ACM Press, July 2024. DOI: 10.1145/3634737.3645010.

[Kal+19] Daniel Kales et al. "Mobile Private Contact Discovery at Scale". In: *USENIX Security 2019*. Ed. by Nadia Heninger and Patrick Traynor. USENIX Association, Aug. 2019, pp. 1447–1464.