特殊 MPC 协议构造

隐私集合操作 (Private Set Operations) 协议

张聪
zhangcong@iie.ac.cn

中国科学院信息工程研究所国家重点实验室

2023 年 5 月 27 日

1. 介绍
2. 隐私集合求交：PSI
3. 隐私集合求并：PSU
4. 参考文献

1 介绍

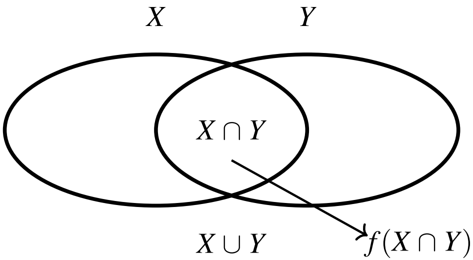
2 隐私集合求交：PSI

3 隐私集合求并：PSU

4 参考文献

PSO 介绍

隐私集合操作 (Private Set Operation, PSO) 协议是一类特殊的 MPC 协议。在 PSO 协议中，协议参与方的输入是一个集合，各方想要计算这个集合的函数，例如，交集、并集，交集大小，交集的秘密分享等。



PSO 介绍

最早关于 PSO 的研究集中于隐私集合求交 (Private Set Intersection, PSI)，目前 PSI 也是研究成果最多，效率最高，最具实用价值的一类 PSO 协议。近年来也有越来越多的其他 PSO 协议被提了出来，例如隐私集合求并 (Private Set Union,PSU)，隐私交集求势 (Private Set Intersection Cardinality, PSI-CA/PSI-card)，隐私交集的势与和 (PSI-card-sum)，电路隐私集合交集 (Circuit-PSI) 等。相比 PSI，这些相关的协议效率依然很低，有待进一步提升。

PSO 介绍

PSI 的相关工作：

- 两方半诚实：[Mea86; HFH99; FNP04; CT10; ACT11; CT12; DCW13; PSZ14; Pin+15; Kol+16; PSZ18; FNO19; Pin+19b; CM20; RS21; Gar+21a; RT21; RR22; Cho+22; KBM23; BC23]
- 两方恶意：[FNP04; HL08; JL09; JL10; HN10; CKT10; Dac+09; Fre+16; RR17a; RR17b; OOS17; Pin+20; RS21; RT21; RR22; Cho+22; GHL22; BC23]
- 多方半诚实：[FNP04; KS05; HV17; Kol+17; IOP18; Cha+21; Bay+22]
- 多方恶意：[KS05; HV17; GN19; AMZ21; Zha+19; Ben+22; NTY21; GHL22; Qiu+22]
- 非平衡场景：[Pin+15; CLR17; Che+18; Con+21; Kis+17; Kal+19; RA18; Li+19] [Dit+22]
- 第三方辅助计算：[Ker12; Kam+14; ATD16; Aba+19; LRG19; Aba+22]

PSO 介绍

Circuit-PSI 相关工作：

- 两方半诚实：[HEK12; Pin+15; CO18; Pin+18; Pin+19a; Gar+21b; RS21; CGS22; HMS22]
- 多方半诚实：[Cha+21]

PSU 相关工作：

- 两方半诚实：[BS05; Fri07; BA12; DC17; Kol+19; Gar+21b; Jia+22a; Jia+22b; Zha+23; Gor+22; Tu+22; Che+22b]
- 两方恶意：[HN10; Gor+22]
- 多方半诚实：[KS05; Fri07; Hon+11; SCK12; BA12]
- 多方恶意：[Fri07; Hon+11; SCK12; BA12]

PSO 介绍

PSI-card 相关工作：

- 两方半诚实：[HFH99; AES03; FNP04; CZ09; CGT12; Ege+15; DPT20; Gar+21b; Che+22b]
- 多方半诚实：[KS05; VC05; Nar+09; Cha+21; TYG22; Che+22a]
- 多方恶意：[KS05]

PSI-card-sum 相关工作：

- 两方半诚实：[Ion+17; Ion+20; Gar+21b; Che+22b]
- 两方恶意：[Mia+20]
- 多方半诚实：[Che+22a]

PSO 介绍

其他 PSI 相关工作：

- 标签 PSI(Labeled PSI)：[CGN98; FNP04; Fre+05; Che+18; Con+21]
- 门限 PSI(Threshold PSI)：[HOS17; ZC18; GS19; Bad+21; BDP21]
- 可更新 PSI(Updatable PSI)：[BMX22]
- 简洁 PSI(Laconic PSI)：[Ala+21; Ara+22]
- 输出交集中的一项：[BXR22]
- 模糊 PSI(Fuzzy PSI)：[FNP04; CFR21; GRS22; GRS23]
- 输入是秘密分享：[MRR20]
- Private Over-Threshold Set-Union/Quorum PSI：[KS05; Cha+21]

1 介绍

2 隐私集合求交：PSI
- 基于公钥
- 基于多项式
- 基于 GBF
- 基于 OPRF
- 基于电路

3 隐私集合求并：PSU

4 参考文献

Private Set Intersection

发送方

接收方

发送方集合 $\longrightarrow$

$Y = \{b, c, e, f, h\}$

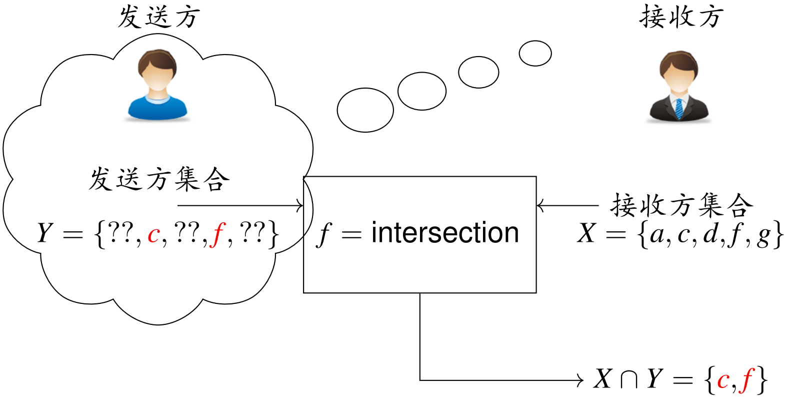
$f =$ intersection

$\longleftarrow$ 接收方集合

$X = \{a, c, d, f, g\}$

$X \cap Y = \{c, f\}$

Private Set Intersection



Naive Hash

最简单的一个想法是，设 H 是一个密码学 hash 函数，两方进行如下协议：

$S(X = \{x_1, \ldots, x_n\})$ $\qquad$ $R(Y = \{y_1, \ldots, y_n\})$

计算 $H(x_i), i \in [n]$

$$\xrightarrow{\Omega := \{H(x_i)\}_{i\in[n]}}$$

$$X \cap Y := \{y | H(y) \in \Omega, y \in Y\}$$

Naive Hash

最简单的一个想法是，设 H 是一个密码学 hash 函数，两方进行如下协议：

$S(X = \{x_1, \ldots, x_n\})$ $\qquad\qquad$ $R(Y = \{y_1, \ldots, y_n\})$

计算 $H(x_i), i \in [n]$

$$\xrightarrow{\Omega := \{H(x_i)\}_{i\in[n]}}$$

$$X \cap Y := \{y | H(y) \in \Omega, y \in Y\}$$

不安全：R 可以进行字典攻击，即，计算 $H(u), \forall u \in U$.

PSI 思路

目前 PSI 主要构造思路有以下几种：

1. 基于公钥：[Mea86; HFH99; CT10; ACT11; CT12]
2. 基于多项式：[FNP04; KS05; HN10; Dac+09; Fre+16; HV17; GN19; GHL22; Cho+22]
3. 基于 GBF：[DCW13; PSZ14; RR17a; IOP18; Bay+22; Zha+19; Ben+22]
4. 基于 OPRF：[HL08; PSZ14; Pin+15; Kol+16; RR17b; OOS17; PSZ18; FNO19; Pin+19b; Pin+20; CM20; RS21; Gar+21a; RT21; RR22; KBM23; BC23]
5. 基于电路：[HEK12; Pin+15; CO18; Pin+18; Pin+19a; Gar+21b; RS21; CGS22; HMS22]

1 介绍

2 隐私集合求交：PSI

- 基于公钥
- 基于多项式
- 基于 GBF
- 基于 OPRF
- 基于电路

3 隐私集合求并：PSU

4 参考文献

基于 DDH 的构造 [Mea86; HFH99](DH-PSI)

最早的 PSI 协议就是基于公钥的 DH 密钥交换协议，其特点是构造简单，通信低，缺点是计算开销大。

$$S(X = \{x_1, \ldots, x_n\}) \qquad\qquad R(Y = \{y_1, \ldots, y_n\})$$

$$a \leftarrow \mathbb{Z}_q, A := \{H(x_i)^a\}_{i \in [n]}$$

$$\xrightarrow{\quad A \quad}$$

$$b \leftarrow \mathbb{Z}_q, B := \{H(y_i)^b\}_{i \in [n]}$$

$$\xleftarrow{\quad B \quad}$$

$$C := \{B_i^a\}_{i \in [n]}$$

$$\xrightarrow{\quad C \quad}$$

输出 $X \cap Y := \{y_i \in Y | C_i \in A^b\}$

基于 RSA 盲签名的构造 [CT10]

参数：RSA 模数 N，hash 函数 H

$S(X = \{x_1, \dots, x_n\})$ | $R(Y = \{y_1, \dots, y_n\})$

$(e, d) \leftarrow \mathrm{KeyGen}(1^\kappa), A := \{H(x_i^d)\}_{i\in[n]}$

$r_i \leftarrow \mathbb{Z}_N^*, i \in [n]$

$\xrightarrow{A, e}$

$B := \{y_i r_i^e\}_{i\in[n]}$

$\xleftarrow{B}$

$C := \{B_i^d\}_{i\in[n]}$

$\xrightarrow{C}$

输出 $X \cap Y := \{y_i \in Y | H(C_i r_i^{-1}) \in A\}$

基于 RSA 盲签名的构造 [CT10]

参数：RSA 模数 N，hash 函数 H

$$
\begin{array}{lcr}
S(X = \{x_1, \ldots, x_n\}) & & R(Y = \{y_1, \ldots, y_n\}) \\
(e, d) \leftarrow \mathrm{KeyGen}(1^\kappa), A := BF(\{x_i^d\}_{i\in[n]}) & & r_i \leftarrow \mathbb{Z}_N^*, i \in [n] \\
& \xrightarrow{\quad A, e \quad} & \\
& & B := \{y_i r_i^e\}_{i\in[n]} \\
& \xleftarrow{\quad B \quad} & \\
C := \{B_i^d\}_{i\in[n]} & & \\
& \xrightarrow{\quad C \quad} & \\
& & \text{输出 } X \cap Y := \{y_i \in Y | C_i r_i^{-1} \in A\}
\end{array}
$$

1 介绍

2 隐私集合求交：PSI
- 基于公钥
- 基于多项式
- 基于 GBF
- 基于 OPRF
- 基于电路

3 隐私集合求并：PSU

4 参考文献

基于多项式的 PSI

[FNP04] 最早提出了 PSI 的概念，第一个提出使用多项式表示集合，思想是令集合元素为多项式的根，即集合 $X = \{x_1, \ldots, x_n\}$ 的多项式表示为 $f(x) := \Pi_{i\in[n]}(x - x_i) = x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_0$，然后根据要求的集合对多项式进行运算。例如，对两个集合 X, Y，设其多项式表示为 f, g，则 $X \cap Y$ 的多项式表示为 $f + g$，$X \cup Y$ 的多项式表示为 fg。使用多项式表示的好处是标准模型，可以方便地扩展到多方情况 [KS05; HV17; GN19]，且天然地支持多重集合 (multiset)[KS05]，缺点是效率较低，且容易出现安全问题 [AMZ21]。

[GS19] 第一次使用 $f(x) = x^{x_1} + \cdots + x^{x_n}$ 表示集合 $X = \{x, \ldots, x_n\}$，用于构造门限 PSI。

基于多项式的 PSI[FNP04]

$S(X)$ $\qquad\qquad$ $R(Y)$

$$(pk, sk) \leftarrow \mathrm{KeyGen}(1^\kappa)$$

$$P(y) := \Pi_{i\in[n]}(y - y_i) = \sum_{i\in[0,n]} \alpha_i y^i$$

$$pk, \{\mathrm{Enc}_{pk}(\alpha_i)\}_{i\in[0,n]}$$

$$\longleftarrow$$

$$\mathrm{Enc}_{pk}(P(x_i)) := \sum_{j\in[0,n]} x_i^j \mathrm{Enc}_{pk}(\alpha_j), i \in [n]$$

$$r_i \leftarrow \mathbb{F}, \mathrm{Enc}_{pk}(r_i P(x_i) + x_i) := r_i \mathrm{Enc}_{pk}(P(x_i)) + x_i$$

$$\{c_i := \mathrm{Enc}_{pk}(r_i P(x_i) + x_i)\}_{i\in[n]}$$

$$\longrightarrow$$

$$X \cap Y := \{\mathrm{Dec}_{sk}(c_i) | \mathrm{Dec}_{sk}(c_i) \in Y\}$$

基于多项式的 PSI[FNP04]

$S(X)$ $\qquad\qquad$ $R(Y)$

$$(pk, sk) \leftarrow \mathrm{KeyGen}(1^\kappa)$$

$$P(y) := \Pi_{i\in[n]}(y - y_i) = \sum_{i\in[0,n]} \alpha_i y^i$$

$$\xleftarrow{pk, \{\mathrm{Enc}_{pk}(\alpha_i)\}_{i\in[0,n]}}$$

$$\mathrm{Enc}_{pk}(P(x_i)) := \sum_{j\in[0,n]} x_i^j \mathrm{Enc}_{pk}(\alpha_j), i \in [n]$$

$$r_i \leftarrow \mathbb{F}, \mathrm{Enc}_{pk}(r_i P(x_i) + x_i||p_{x_i}) := r_i \mathrm{Enc}_{pk}(P(x_i)) + x_i||p_{x_i}$$

$$\xrightarrow{\{c_i := \mathrm{Enc}_{pk}(r_i P(x_i) + x_i||p_{x_i})\}_{i\in[n]}}$$

$$X \cap Y := \{\mathrm{Dec}_{sk}(c_i) | \mathrm{Dec}_{sk}(c_i) \in Y\}$$

基于多项式的 PSI[KS05]

$$S(X, pk, sk_1) \qquad\qquad R(Y, pk, sk_2)$$

$$P_1(x) := \Pi_{i\in[n]}(x - x_i) \qquad\qquad P_2(y) := \Pi_{i\in[n]}(y - y_i)$$

$$\xrightarrow{\mathrm{Enc}_{pk}(P_1)}$$

$$\xleftarrow{\mathrm{Enc}_{pk}(P_2)}$$

$$r_1^1, r_1^2 \leftarrow \mathbb{F} \qquad\qquad r_2^1, r_2^2 \leftarrow \mathbb{F}$$

$$\mathrm{Enc}_{pk}(\phi_1 := r_1^1 P_1 + r_1^2 P_2) \qquad\qquad \mathrm{Enc}_{pk}(\phi_2 := r_2^1 P_1 + r_2^2 P_2)$$

$$\xrightarrow{\mathrm{Enc}_{pk}(\phi_1)}$$

$$\xleftarrow{\mathrm{Enc}_{pk}(\phi_1 + \phi_2)}$$

$$(\mathrm{Enc}_{pk}(\phi_1 + \phi_2), sk_1) \longrightarrow \boxed{\text{门限解密}} \longleftarrow (\mathrm{Enc}_{pk}(\phi_1 + \phi_2), sk_2)$$

$$\phi = \phi_1 + \phi_2 \longleftarrow \boxed{\text{门限解密}} \longrightarrow \phi = \phi_1 + \phi_2$$

$$X \cap Y := \{x \in X | \phi(x) = 0\} \qquad\qquad X \cap Y := \{y \in Y | \phi(y) = 0\}$$

1 介绍

2 隐私集合求交：PSI
- 基于公钥
- 基于多项式
- 基于 GBF
- 基于 OPRF
- 基于电路

3 隐私集合求并：PSU

4 参考文献

基于 GBF 的 PSI 协议

[DCW13] 提出了 Garbled Bloom Filter(GBF) 的概念，并用 GBF 和 OT 给出了第一个只基于 OT 和对称运算构造的 PSI 协议，使得 PSI 协议的效率有了极大的提升。目前基于 GBF 的协议已经可以扩展到多方 [IOP18] 和恶意 [RR17a; Zha+19; Ben+22] 情况，但由于后面计算和通信都更高效的 OPRF-based 的协议的提出，我个人认为 GBF-based 的 PSI 协议已经不再是 PSI 研究的主流，但 GBF 作为一个密码学组件还是值得了解的，它也是后面提出的 Oblivious Key-Value Store (OKVS) 的一个特例。

基于 GBF 的 PSI 协议

Bloom Filter (BF) [Blo70] 是一种用于集合成员测试的数据结构。表示 n 个元素的 BF 是由一个 m 长的比特串 F 和 k 个 hash 函数 $h_1, \ldots, h_k : \{0,1\}^* \to [m]$ 组成。F 初始化为全 0 字符串，当插入一个元素 x 时，令 $F[h_i(x)] := 1, i \in [k]$。要检查一个元素是否在 F 中，只需检查是否对所有的 $i \in [k], F[h_i(x)] = 1$。

BF 可以保证插入过的元素一定能检查出来，但是没有插入过的元素有可能检查出来，设这种失败的情况称为 false positive。[DCW13] 给出的参数选择为：设 false positive 概率是 ϵ，选取 $k = \log 1/\epsilon, m \approx 1.44kn$。在实际应用中，一般需要 $\epsilon = 2^{-\lambda}, k = \lambda, m = 1.44\lambda n$.

基于 GBF 的 PSI 协议

Garbled Bloom Filter (GBF) [DCW13] 和 BF 类似，也是使用 k 个 hash 函数 $h_1, \ldots, h_k : \{0,1\}^* \to [m]$ 做映射，但和 BF 的区别是，GBF 的每个位置不再是一个比特，而是一个 l 长字符串，表示集合元素的输入分享。一个 GBF $G \in \{0,1\}^{ml}$ 初始化为空字符串，当插入一个元素 x 时，对每个位置 $h_i(x)$，令其位置的 GBF 为 x 的一个加法分享，即令 $\bigoplus_{i\in[k]} G[h_i(x)] := x$。当插入完 n 个元素后，如果还有位置为空，则赋一个随机值。要检查一个元素是否在 G 中，只需检查是否有 $\bigoplus_{i\in[k]} G[h_i(x)] = x$。

GBF 的参数选择和 BF 相同，即 $\epsilon = 2^{-\lambda}, k = \lambda, m = 1.44\lambda n$.

注：GBF 可进一步扩展为插入 key-value 对 [PSZ14; Gar+21a]，即插入 (x, y) 时，令 $\bigoplus_{i\in[k]} G[h_i(x)] := y$ 即可。

基于 GBF 的 PSI 协议 [DCW13]

$H := \{h_1, \ldots, h_k\}$ 是 BF/GBF 方案用到的 hash 函数集合。

$S(X)$

$G_X := \mathrm{GBF}_H(X)$

$r_i \leftarrow \{0,1\}^l, i \in [m]$

$R(Y)$

$F_Y := \mathrm{BF}_H(Y)$

$i \in [m]$:

$(r_i, G_X[i]) \longrightarrow$ $\boxed{\text{OT}}$ $\longleftarrow F_Y[i]$

$\boxed{\text{OT}} \longrightarrow G_{X\cap Y}[i]$

输出 $X \cap Y := \{y \in Y | y \in G_{X\cap Y}\}$

基于 GBF 的 PSI 协议 [PSZ14]

$S(X)$ $\qquad\qquad$ $R(Y)$

$$F_Y := BF_H(Y)$$

$$i \in [m]:$$

$$\xleftarrow{(m_{i,0}, m_{i,1})} \boxed{\text{ROT}} \xleftarrow{F_Y[i]}$$

$$\boxed{\text{ROT}} \xrightarrow{m_{i,F_Y[i]}}$$

$$G_1[i] := m_{i,1}, i \in [m] \qquad\qquad G_2[i] := m_{i,F_Y[i]}, i \in [m]$$

$$\xrightarrow{\Omega := \{\bigoplus_{i\in[k]}(G_1[h_i(x)])\}_{x\in X}}$$

$$X \cap Y := \{y \in Y | \bigoplus_{i\in[k]}(G_2[h_i(y)]) \in \Omega\}$$

1 介绍

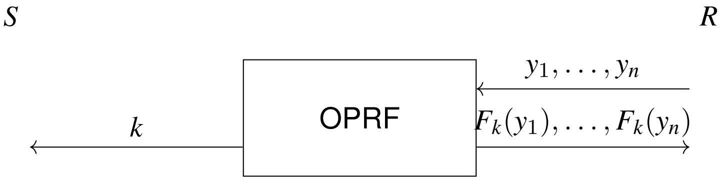
2 隐私集合求交：PSI
- 基于公钥
- 基于多项式
- 基于 GBF
- 基于 OPRF
  - 单点 OPRF
  - 多点 OPRF
- 基于电路

3 隐私集合求并：PSU

4 参考文献

ORPF 定义

Oblivious Pseudo-Random Function (OPRF) [Fre+05] 是一个特殊的两方协议，它允许发送方选择/得到一个 PRF 密钥 k，接收方输入一个集合 $Y = \{y_1, \ldots, y_n\}$，得到对应的 PRF 值 $\{F_k(y_1), \ldots, F_k(y_n)\}$。早期的 OPRF 构造主要是基于公钥的 PRF，例如 Naor-Reingold PRF [NR04; Fre+05; HL08; JL09]，因此效率很低。[PSZ14; Kol+16] 则给出了基于 OT 的 OPRF 构造，使得 OPRF 效率极大提升，但是只能计算单点 PRF 值，[Pin+19b; CM20; RS21] 进一步基于 OT/VOLE 给出了多点 OPRF 的构造。关于 OPRF 的一个综述可参考 [CHL22]。



基于 OPRF 的 PSI 协议框架

回忆 naive hash 方案：

$S(X = \{x_1, \ldots, x_n\})$ $\qquad\qquad$ $R(Y = \{y_1, \ldots, y_n\})$

计算 $H(x_i), i \in [n]$

$$\xrightarrow{\Omega := \{H(x_i)\}_{i \in [n]}}$$

$$X \cap Y := \{y | H(y) \in \Omega, y \in Y\}$$

不安全原因：R 可以任意测试 S 的元素。

基于 OPRF 的 PSI 协议框架

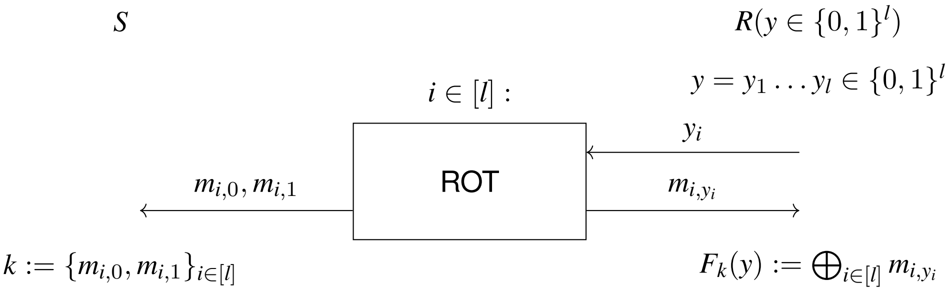
$S(X = \{x_1, \ldots, x_n\})$ $\qquad$ $R(Y = \{y_1, \ldots, y_n\})$

$\Omega := \{F_k(x)\}_{x \in X}$

$$\xrightarrow{\quad\Omega\quad}$$

$X \cap Y := \{y \in Y | F_k(y) \in \Omega\}$

单点 OPRF [PSZ14]



单点 OPRF [PSZ14]

参数：$\log N = \eta, t = l/\eta$

S

$R(y \in [0, \eta - 1]^t)$

$y = y_1 \dots y_t \in [0, \eta - 1]^t$

$i \in [t]:$

$$m_{i,0}, \dots, m_{i,N-1} \longleftarrow \boxed{\binom{N}{1}\text{-ROT}} \xleftarrow{\; y_i \;} \quad \boxed{\binom{N}{1}\text{-ROT}} \xrightarrow{\; m_{i,y_i} \;}$$

$k := \{m_{i,0}, \dots, m_{i,N-1}\}_{i \in [t]}$

$F_k(y) := \bigoplus_{i \in [t]} m_{i,y_i}$

单点 OPRF [Kol+16]

S $\qquad\qquad$ $R(y \in \{0,1\}^l)$

$y \in \{0,1\}^l$

$$m_0, \ldots, m_{2^l-1} \longleftarrow \boxed{\binom{2^l}{1}\text{-ROT}} \xleftarrow{y}$$

$$\boxed{\binom{2^l}{1}\text{-ROT}} \xrightarrow{m_y}$$

$k := \{m_0, \ldots, m_{2^l-1}\}$ $\qquad\qquad$ $F_k(y) := m_y$

单点 OPRF [Kol+16]

S $\qquad\qquad$ $R(y \in \{0,1\}^l)$

$y \in \{0,1\}^l$

$$m_0, \ldots, m_{2^l-1} \longleftarrow \boxed{\binom{2^l}{1}\text{-ROT}} \xleftarrow{\;y\;} \qquad \boxed{\binom{2^l}{1}\text{-ROT}} \xrightarrow{\;m_y\;}$$

$k := \{m_0, \ldots, m_{2^l-1}\}$ $\qquad\qquad$ $F_k(y) := m_y$

注：实际上 $k := (q, s), m_x = F_k(x) = H(q \oplus (C(x) \cdot s))$，$C$ 是伪随机编码 (PRC).

单点 OPRF→ 单点 PSI

$S(X = \{x_1, \ldots, x_n\})$ $R(y)$

y

OPRF

k $F_k(y)$

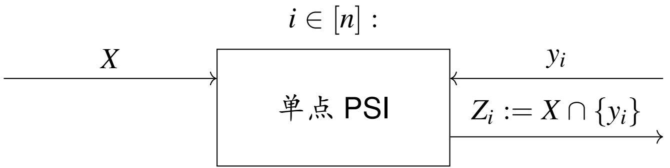
$\Omega := \{F_k(x)\}_{x \in X}$

$\xrightarrow{\Omega}$

$X \cap \{y\} := \{y | F_k(y) \in \Omega\}$

单点 PSI $\rightarrow$ PSI

$S(X)$ $R(Y = \{y_1, \ldots, y_n\})$



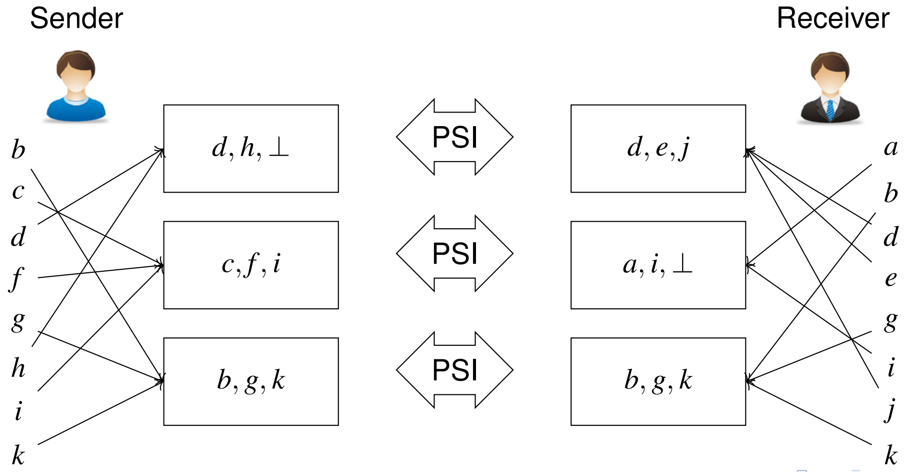
$X \cap Y := \cup_{i \in [n]} Z_i$

问题：对每个 y 都要重新执行一次 n 长的单点 OPRF，效率太低。

Hash to bin 技术

由于平凡地执行 n 次单点 PSI 开销太大，一般考虑使用 hash to bin 技术进行优化。hash to bin 技术的思想是双方使用相同的 hash 函数将各自的元素映射到很多 bin 中，即将 n 个元素 $e_1,\ldots,e_n$ 用 hash 函数映射到 m 个 bin 中，记为 $B_1,\ldots,B_m$，之后在每个 bin 中求 PSI。这样就将两个大集合元素的 PSI 问题转化到了求很多小集合元素的 PSI 问题，设 $X=\cup_{i\in[m]}X_i, Y=\cup_{i\in[m]}Y_i, X\cap Y=\cup_{i\in[m]}X_i\cap Y_i$，能够节省开销。

Hash to bin 技术



Hash to bin 技术

simple hash

设 $h:\{0,1\}^\sigma \to [m]$ 是随机 hash 函数。对每个输入项 e，映射到 $B_{h(e)}$ 中。

参数分析：

考虑将 n 个球放入 m 个 bin 的游戏，则：

$Pr[\exists$ 某个 bin 中球的个数 $\geq max_m]$

$\leq \sum_{i=1}^{m} Pr[$ 第 i 个 bin 中球的个数 $\geq max_m]$

$= m \cdot Pr[$ 第 i 个 bin 中球的个数 $\geq max_m]$

$= m \cdot (\sum_{i=max_m}^{n} \binom{n}{i} \cdot (\frac{1}{m})^i \cdot (1-\frac{1}{m})^{n-i}) \leq 2^{-\lambda}$

当固定 n 和 m 时，可求得 max_m 的大小。

[Gon81] 分析表明，当 $m=n$ 时，$max_m = \frac{lnn}{lnlnn}(1+o(1))$。

当 $m = O(n/\log n)$ 时，$max_m = O(\log n)$。

Hash to bin 技术

balanced hash

设 $h_1, h_2 : \{0,1\}^\sigma \to [m]$ 是 2 个随机 hash 函数。对每个输入项 e，映射到 $B_{h_1(e)}$ 与 $B_{h_2(e)}$ 中较少的 bin 中。

[Aza+94] 表明，$m = n$ 时，$max_m = \frac{lnlnn}{ln2}(1 + o(1))$

Hash to bin 技术

cuckoo hash [PR04]

设 $h_1,\ldots,h_k:\{0,1\}^\sigma\rightarrow[m]$ 是 k 个随机 hash 函数。对每个输入项 e:
首先将其放入 $B_{h_1(e)}$ 中，如果 $B_{h_1(e)}$ 已有元素 o，则把 o 放到新的 $B_{h_i(o)}$ 中，
$i\in[k],h_i(o)\neq h_1(e)$。重复此过程，直到没有元素被重放，或重放次数达到门限值。
如果达到门限值，则将最后一个元素放入 stash 中。stash 大小记为 s。
注：cuckoo hash 每个 bin 中至多有一个元素。
参数分析 [Pin+18]:
cuckoo hash 有 3 个参数需要分析：stash 大小 s，hash 函数数量 k，bin 的个数 m。
一般取 $m=O(n)$(具体来说 $k=3,m=1.2n,k=2,m=2.4n$)。
s: 当 $m=O(n)$ 时，失败概率为 $O(n^{-s})$。要使 $n^{-s}<2^{-\lambda}$，取 $s=O(\lambda/\log n)$
k: 一般 k 取 2，但是此时 bin 的数量大概为 $2n$，即利用率为 50%。若 $s=0$，$\lambda=40$，实验表明，当 $k=3$ 时，bin 的数量大概为 $1.27n$，当 $k=4$ 时，bin 的数量大概为 $1.09n$，当 $k=5$ 时，bin 的数量大概为 $1.05n$。

Hash to bin 技术

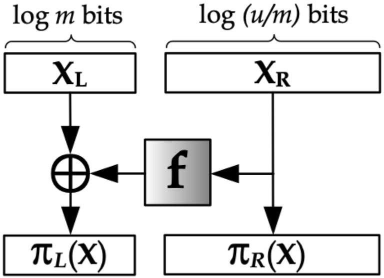
基于置换的 hash [ANS10]

为了降低每个 bin 中元素的存储长度，可以考虑使用基于置换的 hash。
设每个元素 $x \in \{0,1\}^l$，bin 的数量是 m。考虑利用 bin 位置的信息降低存储 x 需要的空间，设 π 是 $\{0,1\}^l$ 上的随机置换，令 $\pi(x) = \pi_L(x)||\pi_R(x) \in \{0,1\}^{\log m + (l - \log m)}$。
要存储 x，只需将 $\pi_R(x)$ 存储在第 $\pi_L(x)$ 个 bin 中。此时每个元素的存储空间由 l 降低到 $l - \log m$，当 l 和 $\log m$ 接近时 (e.g. $l = 32, m = 2^{20}$)，开销会有很大提升。
使用这种方法，如果两个元素 x, x' 都存储在同一个 bin 中，且存储值相同，则一定有 $x = x'$。即 $\pi_L(x) = \pi_L(x'), \pi_R(x) = \pi_R(x') \Longrightarrow \pi^{-1}(\pi(x)) = \pi^{-1}(\pi(x')), x = x'$.

Hash to bin 技术

基于置换的 hash [ANS10]

构造置换 π：由于直接构造 $\{0,1\}^l$ 上的置换比较困难，考虑使用 Feistel 结构，设 $f:\{0,1\}^{l-\log m} \to \{0,1\}^{\log m}$ 是一个 k-wise independent 函数 ($k = poly \log n$)，令 $\pi(x) := (x_L \oplus f(x_R), x_R)$.



单点 PSI+Hash→ PSI

$S(X=\{x_1,\ldots,x_n\})$

$R(Y=\{y_1,\ldots,y_n\})$

$\mathcal{X} \leftarrow SimpleH^m_{h_1,h_2,h_3}(X)$

$(\mathcal{Y},\mathcal{S}) \leftarrow CuckooH^m_{h_1,h_2,h_3}(Y)$

$i \in [m]$:

$\mathcal{X}[i] \rightarrow$ 单点 PSI $\leftarrow \mathcal{Y}[i]$

$\rightarrow Z_i := \mathcal{X}[i] \cap \{\mathcal{Y}[i]\}$

$j \in [s]$:

$X \rightarrow$ 单点 PSI $\leftarrow \mathcal{S}[j]$

$\rightarrow Z_{m+j} := X \cap \{\mathcal{S}[j]\}$

$X \cap Y := \cup_{i\in[m+s]} Z_i$

多点 OPRF [Pin+19a]

回忆 OTe 协议 [Ash+13]:

S $\qquad\qquad\qquad\qquad$ $R(r \in \{0,1\}^N)$

$s \leftarrow \{0,1\}^\kappa$ $\qquad$ $k_i^0, k_i^1 \leftarrow \{0,1\}^\kappa, i \in [\kappa]$

$i \in [\kappa]$:

$$\xrightarrow{s_i} \boxed{\text{OT}} \xleftarrow{(k_i^0, k_i^1)}$$

$$\xleftarrow{q_i = k_i^{s_i}}$$

$$T := [G(k_1^0)| \dots |G(k_\kappa^0)]_{N\times\kappa}$$

$$U := [G(k_1^1)| \dots |G(k_\kappa^1)]_{N\times\kappa}$$

$$C := [r| \dots |r]_{N\times\kappa}$$

$$\xleftarrow{P := T \oplus U \oplus C}$$

$$Q := [G(q_1)| \dots |G(q_\kappa)]_{N\times\kappa}$$

$$Q(j) = T(j) \oplus s(P(j) \oplus r_j \cdot 1^\kappa)$$

$$m_{j,0} := H(Q(j) \oplus s \cdot P(j)), j \in [N]$$

$$m_{j,1} := H(Q(j) \oplus s \cdot P(j) \oplus s), j \in [N]$$

$$m_{j,r_j} := H(T(j)), j \in [N]$$

多点 OPRF [Pin+19a]

核心观察：OTe 的每一行表示一个 OT 实例，如果把 OTe 的行数 i 看做 PRF 输入，考虑 $F : [N] \to \{0,1\}^\kappa$，令 $F_k(i) := m_{i,0}$，这里 $k = (s, Q)$。此时，发送方可以对任意 $i \in [N]$ 计算 $F_k(i)$，而接收方只能得到对应 $r_i = 0$ 那些行的 $F_k(i)$。

多点 OPRF [Pin+19a]

核心观察：OTe 的每一行表示一个 OT 实例，如果把 OTe 的行数 i 看做 PRF 输入，考虑 $F : [N] \to \{0,1\}^\kappa$，令 $F_k(i) := m_{i,0}$，这里 $k = (s, Q)$。此时，发送方可以对任意 $i \in [N]$ 计算 $F_k(i)$，而接收方只能得到对应 $r_i = 0$ 那些行的 $F_k(i)$。

问题 1：这里 N 表示矩阵的行数，只能是多项式长度，即 $N = poly(\kappa)$，当双方元素很长时，例如 $l = 128$，需要取 $N = 2^{128}$，由于要发送的矩阵 P 是 $N \times \kappa$，通信太大无法实现。

多点 OPRF [Pin+19a]

核心观察：OTe 的每一行表示一个 OT 实例，如果把 OTe 的行数 i 看做 PRF 输入，考虑 $F : [N] \to \{0,1\}^\kappa$，令 $F_k(i) := m_{i,0}$，这里 $k = (s, Q)$。此时，发送方可以对任意 $i \in [N]$ 计算 $F_k(i)$，而接收方只能得到对应 $r_i = 0$ 那些行的 $F_k(i)$。

问题 1：这里 N 表示矩阵的行数，只能是多项式长度，即 $N = poly(\kappa)$，当双方元素很长时，例如 $l = 128$，需要取 $N = 2^{128}$，由于要发送的矩阵 P 是 $N \times \kappa$，通信太大无法实现。

解决思路：只需要让接受者发送 $y \in Y$ 对应的 n 行即可。

多点 OPRF [Pin+19a]

核心观察：OTe 的每一行表示一个 OT 实例，如果把 OTe 的行数 i 看做 PRF 输入，考虑 $F:[N]\to\{0,1\}^\kappa$，令 $F_k(i):=m_{i,0}$，这里 $k=(s,Q)$。此时，发送方可以对任意 $i\in[N]$ 计算 $F_k(i)$，而接收方只能得到对应 $r_i=0$ 那些行的 $F_k(i)$。

问题 1：这里 N 表示矩阵的行数，只能是多项式长度，即 $N=poly(\kappa)$，当双方元素很长时，例如 $l=128$，需要取 $N=2^{128}$，由于要发送的矩阵 P 是 $N\times\kappa$，通信太大无法实现。

解决思路：只需要让接受者发送 $y\in Y$ 对应的 n 行即可。

问题 2：这样会暴露所有 y 的信息。

多点 OPRF [Pin+19a]

核心观察：OTe 的每一行表示一个 OT 实例，如果把 OTe 的行数 i 看做 PRF 输入，考虑 $F:[N]\rightarrow\{0,1\}^{\kappa}$，令 $F_k(i):=m_{i,0}$，这里 $k=(s,Q)$。此时，发送方可以对任意 $i\in[N]$ 计算 $F_k(i)$，而接收方只能得到对应 $r_i=0$ 那些行的 $F_k(i)$。

问题 1：这里 N 表示矩阵的行数，只能是多项式长度，即 $N=poly(\kappa)$，当双方元素很长时，例如 $l=128$，需要取 $N=2^{128}$，由于要发送的矩阵 P 是 $N\times\kappa$，通信太大无法实现。

解决思路：只需要让接受者发送 $y\in Y$ 对应的 n 行即可。

问题 2：这样会暴露所有 y 的信息。

解决思路：利用多项式插值 P 隐藏 y 的信息。即，令 $P(y)$ 是需要发送的目标行，发送方只能求 $P(x)$ 那些行

多点 OPRF [Pin+19a]

参数:$l = \log|\mathbb{F}|$, PRF $F : \{0,1\}^\kappa \times \{0,1\}^l \to \{0,1\}$,CRHF$H : \{0,1\}^l \to \{0,1\}^{\lambda+2\log n}$

S $R(Y = \{y_1, \ldots, y_n\})$

$s \leftarrow \{0,1\}^\kappa$ $k_i^0, k_i^1 \leftarrow \{0,1\}^\kappa, i \in [\kappa]$

$i \in [l]$:

$s_i \rightarrow$ OT $\leftarrow (k_i^0, k_i^1)$

$q_i = k_i^{s_i} \leftarrow$ OT

对 $y \in Y$:

$T(y) := F(k_1^0, y)|| \ldots ||F(k_l^0, y)$

$U(y) := F(k_1^1, y)|| \ldots ||F(k_l^1, y)$

$R(y) := T(y) \oplus U(y)$

计算 $P := \mathrm{Interp}_{\mathbb{F}}(\{(y, R(y))\}_{y \in Y})$

$\xleftarrow{\quad P \quad}$

定义 $Q(x) := F(q_1, x)|| \ldots ||F(q_l, x)$，令 $k := (s, Q, P)$ 输出 $\{\bar{F}_k(y) := H(T(y))\}_{y \in Y}$

$\bar{F}_k(x) := H(Q(x) \oplus s \cdot P(x))$

多点 OPRF [CM20]

回忆 OTe 协议 [KK13; Kol+16]:

S

$s \leftarrow \{0,1\}^\kappa$

$R(r \in [0, 2^l - 1]^N)$

$k_i^0, k_i^1 \leftarrow \{0,1\}^\kappa, i \in [\kappa]$

$i \in [\rho]$:

$$s_i \longrightarrow \boxed{\text{OT}} \longleftarrow (k_i^0, k_i^1)$$

$$q_i = k_i^{s_i} \longleftarrow \boxed{\text{OT}}$$

$T := [G(k_1^0)| \dots |G(k_\rho^0)]_{N\times\rho}$

$U := [G(k_1^1)| \dots |G(k_\rho^1)]_{N\times\rho}$

$C := [\mathcal{C}(r_1)| \dots |\mathcal{C}(r_N)]^T_{N\times\rho}$

$$\xleftarrow{P := T \oplus U \oplus C}$$

$Q := [G(q_1)| \dots |G(q_\rho)]_{N\times\rho}$

$Q(j) = T(j) \oplus s(P(j) \oplus \mathcal{C}(r_j))$

$m_{j,t} := H(Q(j) \oplus s \cdot P(j) \oplus s \cdot \mathcal{C}(t)), j \in [N], t \in [0, 2^l - 1]$

$m_{j,r_j} := H(T(j)), j \in [N]$

多点 OPRF [CM20]

回忆 OTe 协议 [KK13; Kol+16]：

S

$s \leftarrow \{0,1\}^\kappa$

$R(r \in [0, 2^l - 1]^N)$

$k_i^0, k_i^1 \leftarrow \{0,1\}^\kappa, i \in [\kappa]$

$i \in [\rho]$:

s_i → OT ← (k_i^0, k_i^1)

$q_i = k_i^{s_i}$ ←

$T := [G(k_1^0)| \ldots |G(k_\rho^0)]_{N \times \rho}$

$U := [G(k_1^1)| \ldots |G(k_\rho^1)]_{N \times \rho}$

$C := [\mathcal{C}(r_1)| \ldots |\mathcal{C}(r_N)]^T_{N \times \rho}$

← $P := T \oplus U \oplus C$

$Q := [G(q_1)| \ldots |G(q_\rho)]_{N \times \rho}$

$Q(j) = T(j) \oplus s(P(j) \oplus \mathcal{C}(r_j))$

$m_{j,t} := H(Q(j) \oplus s \cdot P(j) \oplus s \cdot \mathcal{C}(t)), j \in [N], t \in [0, 2^l - 1]$

$m_{j,r_j} := H(T(j)), j \in [N]$

每一行是一个输入为 $\{0,1\}^l$ 的单点 OPRF 实例，$k_j = (s, \mathcal{C}, Q(j))$

多点 OPRF [CM20]

主要观察：把每一行 $C(r_j)$ 的每个比特均匀随机放在不同的行中，密钥 $k = (s, Q)$
设 PRF $F : \{0,1\}^\kappa \times \{0,1\}^l \to [N]^\rho$ 是将每个元素映射到所有 ρ 列对应位置的函数。
考虑这样的构造：

$\mathrm{MatGen}(\{r_j \in \{0,1\}^l\}_{j\in[N]})$:

1. 初始化 $C = [C_1|\ldots|C_\rho] := [1]_{N\times\rho}$
2. $k \leftarrow \{0,1\}^\kappa$
3. 对 $j \in [N]$:
    1. 计算 $v_j := F_k(r_j)$
    2. 令 $C_i[v_j[i]] := 0, i \in [\rho]$
4. 输出 C

此算法相当于把每个 r_j 的编码随机映射到了矩阵的不同行，而不再只是第 j 行

多点 OPRF [CM20]

参数：PRF $F:\{0,1\}^\kappa \times \{0,1\}^l \to [n]^\rho$,CRHF $H:\{0,1\}^\rho \to \{0,1\}^{\lambda+2\log n}$

S | $R(Y=\{y_1,\ldots,y_n\})$

$s \leftarrow \{0,1\}^\kappa$

$k_i^0, k_i^1 \leftarrow \{0,1\}^\kappa, i\in[\kappa]$

$i \in [\rho]:$

$\xrightarrow{s_i}$ OT $\xleftarrow{(k_i^0, k_i^1)}$

$\xleftarrow{q_i = k_i^{s_i}}$

$T := [G(k_1^0)|\ldots|G(k_\rho^0)]_{n\times\rho}$

$U := [G(k_1^1)|\ldots|G(k_\rho^1)]_{n\times\rho}$

$C := \mathrm{MatGen}(Y)$

$\xleftarrow{P := T \oplus U \oplus C, k}$

$Q := [G(q_1)\oplus s_1P_1|\ldots|G(q_\rho)\oplus s_\rho P_\rho]_{n\times\rho}$

输出 $\bar{k} := (s, Q)$

$F_{\bar{k}}(x) := H(Q_1[v_x[1]]||\ldots||Q_\rho[v_x[\rho]])$

输出 $\{F_{\bar{k}}(y) := H(T_1[v_y[1]]||\ldots||T_\rho[v_y[\rho]])\}_{y\in Y}$

其中 $v_y = F_k(y)$

OKVS

定义 (Key-Value Store [Pin+20; Gar+21a])

一个键值存储 (Key-Value Store) 包括以键集合 $\mathcal{K}$，值集合 $\mathcal{V}$，和函数集合 H 为参数的两个算法:

- $\mathrm{Encode}_H(\{(x_1, y_1), \ldots, (x_n, y_n)\})$: 输入键值对 $\{(x_i, y_i)\}_{i\in[n]} \subseteq \mathcal{K} \times \mathcal{V}$, 输出数据结构 D (或以可忽略概率输出错误符号 $\perp$).
- $\mathrm{Decode}_H(D, x)$: 输入数据结构 D 和一个键 x，输出一个值 $y \in \mathcal{V}$.

正确性. 对所有具有不同键的 $A \subseteq \mathcal{K} \times \mathcal{V}$:

$$(x, y) \in A \text{ 且 } \perp \neq D \leftarrow \mathrm{Encode}_H(A) \implies \mathrm{Decode}_H(D, x) = y$$

OKVS

不经意性. 对所有不同的 $\{x_1^0, \ldots, x_n^0\}$ 和 $\{x_1^1, \ldots, x_n^1\}$，如果 Encode_H 对输入 $\{x_1^0, \ldots, x_n^0\}$ 或 $\{x_1^1, \ldots, x_n^1\}$ 不输出 $\perp$，则

$$\{D | y_i \leftarrow \mathcal{V}, i \in [n], \mathrm{Encode}_H((x_1^0, y_1), \ldots, (x_n^0, y_n))\} \approx \{D | y_i \leftarrow \mathcal{V}, i \in [n], \mathrm{Encode}_H((x_1^1, y_1), \ldots, (x_n^1, y_n))\}$$

随机性. 对任意 $A = \{(x_1, y_1), \ldots, (x_n, y_n)\}$ 且 $x^* \notin \{x_1, \ldots, x_n\}$，$\mathrm{Decode}_H(D, x^*)$ 的输出和 $\mathcal{V}$ 上的均匀分布统计不可区分，其中 $D \leftarrow \mathrm{Encode}_H(A)$.

一个键值存储如果满足不经意性，则称为不经意键值存储 (Oblivious Key-Value Store, OKVS).

OKVS

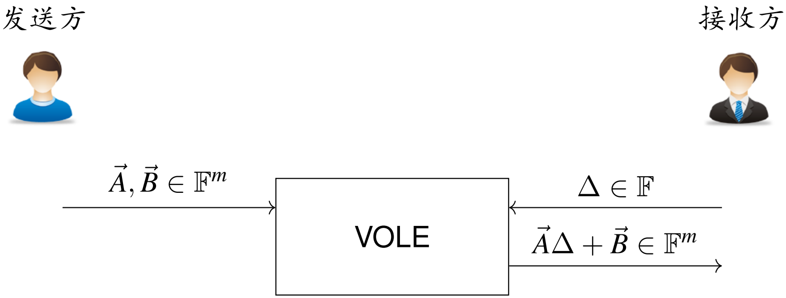
OKVS 的效率可以用以下三个参数衡量：

- 比率 **(Rate):** 令 n/m 作为 OKVS 的比率，其中 m 是 D 的大小。最优比率为 1。
- 编码复杂度 **(Encoding complexity):** Encode_H 算法的计算复杂度，是键值对数量 n 的函数
- 解码复杂度 **(Decoding complexity):** Decode_H 算法的计算复杂度。

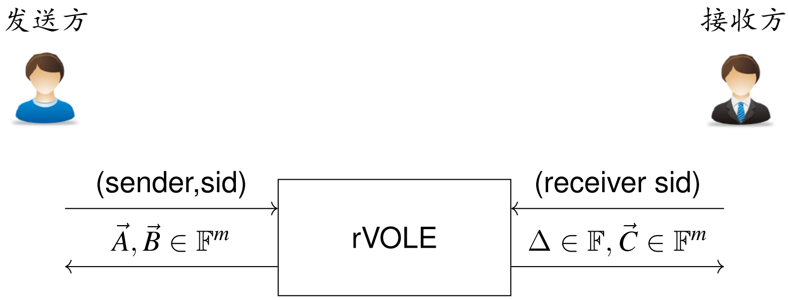
方案	比率	编码	解码	不经意性	随机性
多项式	1	$O(n\log^2 n)$	$O(\log n)$	$\surd$	$\times$
GBF [DCW13]	$O(1/\lambda)$	$O(\lambda n)$	$O(\lambda)$	$\surd$	$\surd$
2H-GCT [Pin+20]	$0.42-o(1)$	$O(\lambda n)$	$O(\lambda)$	$\times$	$\times$
XoPaXoS [RS21]	$0.42-o(1)$	$O(\lambda n)$	$O(\lambda)$	$\surd$	$\surd$
3H-GCT [Gar+21a]	$0.81-o(1)$	$O(\lambda n)$	$O(\lambda)$	$\times$	$\times$
3H-GCT++ [Zha+23]	$0.81-o(1)$	$O(\lambda n)$	$O(\lambda)$	$\surd$	$\surd$

表 1: 不同 OKVS 方案比较

VOLE


发送方
接收方
$\vec{A}, \vec{B} \in \mathbb{F}^m$
$\Delta \in \mathbb{F}$
VOLE
$\vec{A}\Delta + \vec{B} \in \mathbb{F}^m$

VOLE



$$\vec{C} = \vec{A}\Delta + \vec{B}$$

多点 OPRF [RS21]

参数:$l = \log|\mathbb{F}|$, RO $H : \{0,1\}^l \to \{0,1\}^{\lambda+2\log n}$

S $\qquad$ $R(Y = \{y_1, \dots, y_n\})$

$$\xrightarrow{\text{(receiver sid)}} \boxed{\text{rVOLE}} \xleftarrow{\text{(sender sid)}}$$

$$\xleftarrow{\Delta \in \mathbb{F}, \vec{C} \in \mathbb{F}^m} \qquad \xrightarrow{\vec{A}, \vec{B} \in \mathbb{F}^m}$$

$\vec{P} \leftarrow \mathrm{Encode}(\{(y_i, 0)\}_{i\in[n]})$

$$\xleftarrow{\vec{A} + \vec{P}}$$

输出 $\vec{K} := \vec{C} - \Delta(\vec{A} + \vec{P})$

$F_{\vec{K}}(x) := H(\mathrm{Decode}(\vec{K}, x))$

输出 $\{F_{\vec{K}}(y) := H(\mathrm{Decode}(\vec{B}, y))\}_{y\in Y}$

1. 介绍
2. 隐私集合求交：PSI
   - 基于公钥
   - 基于多项式
   - 基于 GBF
   - 基于 OPRF
   - 基于电路
3. 隐私集合求并：PSU
4. 参考文献

电路 PSI

电路 PSI (Circuit-PSI) 概念的内涵是有演变的，早期的电路 PSI 论文 [HEK12; Pin+15; Pin+18] 指的是构造 PSI 电路，使用一般的 MPC 协议 (如 GC，GMW) 计算集合交集的协议，重点在于优化电路，降低比较次数，协议的输出就是交集；后面的电路 PSI 协议 [CO18; Pin+19a; Gar+21b; RS21; CGS22; HMS22] 则主要指协议输出是交集的秘密分享，以便用通用协议对交集进行后续计算 (即 $f(X \cap Y)$)，其构造思路不局限于只使用电路，也会使用其他的组件，如 OT，OKVS，OPPRF，HE 等。前者的电路体现在计算交集用电路，后者的电路体现在执行后续计算用电路。
注：两种概念也不是互斥的，使用电路计算交集的协议自然可以轻松地改造成计算任意交集函数的协议，后者相当于使用更灵活的思路得到交集的秘密分享。
个人分析概念变化的原因：早期的电路 PSI[HEK12; Pin+15] 和基于公钥的 PSI 协议效率还是可以扳一扳手腕的，因此指的就是用电路计算 PSI，随着基于 OT 的 PSI 的提出，基于电路的 PSI 效率就完全跟不上了，因此后续的研究会强调电路 PSI 的优势是可以计算交集的函数。

电路 PSI

[HEK12] 首先构造了 SCS(sort-compare-shuffle) 电路，然后用 Garbled circuit 的方法构造了 PSI 协议。这里 SCS 电路的设计思路是，首先对两方集合的所有元素同时进行排序，然后比较两两相邻的元素，如果相等则在交集中，最后为了隐藏顺序可能会泄露的集合信息，把集合重新打乱。[HEK12] 设计协议的通信复杂度为 $O(ln\log n)$，这里 n 是集合元素个数，l 是集合元素的长度。
随后 Pinkas 等人 [Pin+15] 利用 Circuit-Phasing 技术，即将元素用 hash 函数映射到不同的 bin 中，并将 bin 的位置信息作为额外的元素信息，可以降低每个元素的存储空间，然后使用 pairwise-comparison (PWC) 电路对每个 bin 中的元素进行比较，构造的协议通信复杂度为 $O(ln\log n/\log\log n)$。
[Pin+18] 提出了新的哈希表构造方法，2D 哈希，通信复杂度为 $\omega(ln)$，可以任意接近线性复杂度。[Pin+19a] 则构造了第一个线性通信复杂度 $O(ln)$ 的电路 PSI 协议。后续的工作均基于 PSTY 框架，改进了协议提高效率 [Gar+21b; Cha+21; RS21; HMS22]。

PPRF

可编程 PRF(Programmable PRF,PPRF) [Kol+17] 指的是一类特殊的 PRF，它可以将“编程”的输入映射到“编程”的输出。一个 PPRF 由下述算法组成：

- $\mathrm{KeyGen}(1^\kappa, \mathcal{P}) \to (k, \mathrm{hint})$: 输入安全参数和一个有不同 x_i 构成的点集 $\mathcal{P} = \{(x_1, y_1), \ldots, (x_n, y_n)\}$，生成一个 PRF 密钥 k 和一个公开的辅助信息 hint。
- $F(k, \mathrm{hint}, x) \to y$: 输入 x，输出 y.

正确性. 一个 PPRF 满足正确性如果 $(x, y) \in \mathcal{P}$ 且 $(k, \mathrm{hint}) \leftarrow \mathrm{KeyGen}(1^\kappa, \mathcal{P})$，则 $F(k, \mathrm{hint}, x) = y$.

PPRF

安全性. 对于安全性，考虑下述实验：

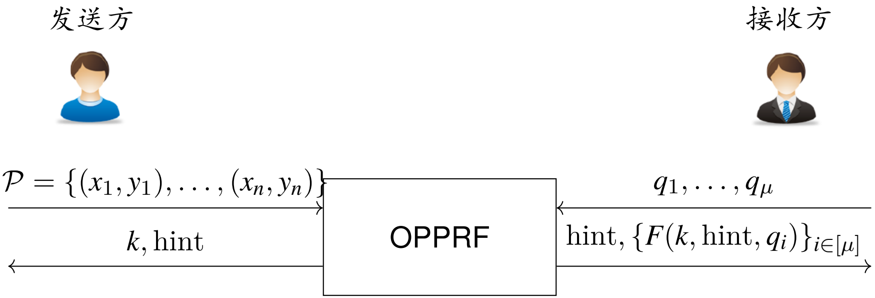
$$\begin{array}{l}\mathrm{Exp}^{\mathcal{A}}(X,Q,\kappa): \\ \text{对每个 } x_i \in X\text{，选随机的 } y_i \leftarrow \mathcal{V} \\ (k,\mathrm{hint}) \leftarrow \mathrm{KeyGen}(1^\kappa, \{(x_i,y_i) | x_i \in X\}) \\ \text{返回 } \mathcal{A}(\mathrm{hint}, \{F(k,\mathrm{hint},q) | q \in Q\})\end{array}$$

我们称一个 PPRF 是 (n,μ)-安全，如果对所有 $|X_0| = |X_1| = n$，所有 $|Q| = \mu$，和所有 PPT 的 $\mathcal{A}$:

$$|Pr[\mathrm{Exp}^{\mathcal{A}}(X_0,Q,\kappa) = 1] - Pr[\mathrm{Exp}^{\mathcal{A}}(X_1,Q,\kappa) = 1]| \le negl(\kappa)$$

OPPRF

Oblivious PPRF (OPPRF) [Kol+17] 定义如下：



OPPRF

$S(\mathcal{P} = \{(x_1, y_1), \ldots, (x_n, y_n)\})$ $R(Q = \{q_1, \ldots, q_\mu\})$

$P \leftarrow \mathrm{Encode}(\{(x_i, \bar{F}_k(x_i) \oplus y_i)\}_{i \in [n]})$

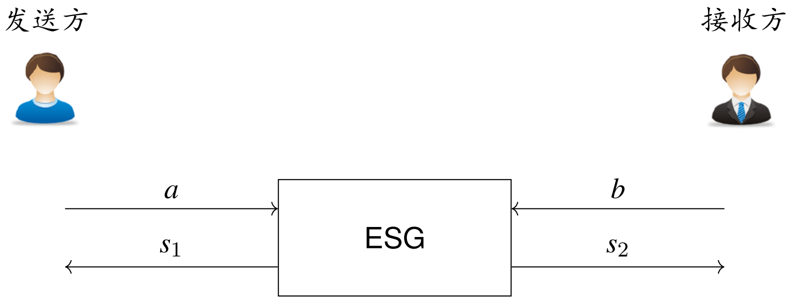
$\xrightarrow{P}$

$\mathrm{hint} := P$ $\mathrm{hint} := P$

输出 (k, hint) 输出 $\{F(k, \mathrm{hint}, q) := \mathrm{Decode}(P, q) \oplus \bar{F}_k(q)\}_{y \in Y}$

ESG

相等分享生成 (Equality Share Generation) 功能定义如下：



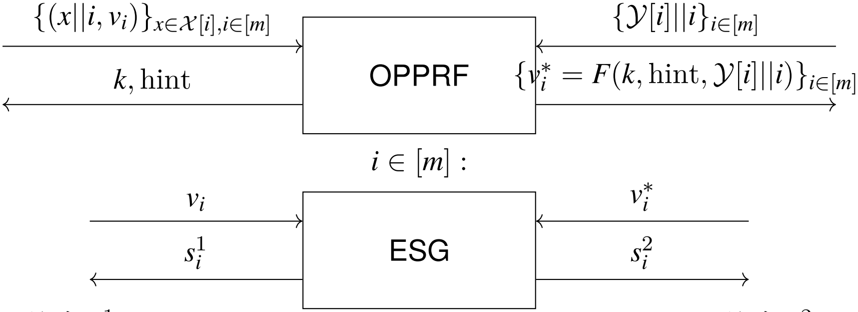
$$s_1 \oplus s_2 = \begin{cases} 1 & a = b; \\ 0 & a \neq b \end{cases}$$

PSTY 框架 [Pin+19a]

$S(X = \{x_1, \ldots, x_n\})$ $\quad$ $R(Y = \{y_1, \ldots, y_n\})$

$\mathcal{X} \leftarrow SimpleH^m_{h_1,h_2,h_3}(X)$ $\quad$ $\mathcal{Y} \leftarrow CuckooH^m_{h_1,h_2,h_3}(Y)$

$v_i \leftarrow \{0,1\}^l, i \in [m]$



输出 s^1 $\quad$ 输出 s^2

1. 介绍
2. 隐私集合求交：PSI
3. 隐私集合求并：PSU
   - 基于 AHE
   - 基于 (mq-)RPMT+OT
4. 参考文献

Private Set Union

Sender

Receiver

Sender's set $\longrightarrow$ $f =$ union $\longleftarrow$ Receiver's set

$Y = \{b, c, e, f, h\}$

$X = \{a, c, d, f, g\}$

Private Set Union

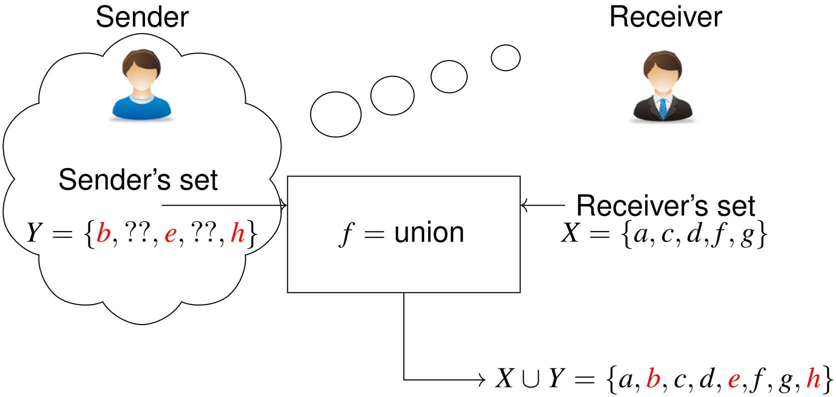
Sender

Receiver

Sender's set $Y = \{b, c, e, f, h\}$ → $f =$ union ← Receiver's set $X = \{a, c, d, f, g\}$

$$X \cup Y = \{a, b, c, d, e, f, g, h\}$$

Private Set Union



1. 介绍
2. 隐私集合求交：PSI
3. 隐私集合求并：PSU
   - 基于 AHE
   - 基于 (mq-)RPMT+OT
4. 参考文献

基于 AHE 的 PSU [Fri07]

$S(X)$ $R(Y)$

$(pk, sk) \leftarrow \mathrm{KeyGen}(1^\kappa)$

$P(y) := \Pi_{i\in[n]}(y - y_i) = \sum_{i\in[0,n]} \alpha_i y^i$

$$\xleftarrow{pk, \{\mathrm{Enc}_{pk}(\alpha_i)\}_{i\in[0,n]}}$$

$c_i^1 = \mathrm{Enc}_{pk}(P(x_i)) := \sum_{j\in[0,n]} x_i^j \mathrm{Enc}_{pk}(\alpha_j), i \in [n]$

$c_i^2 = \mathrm{Enc}_{pk}(x_i \cdot P(x_i)) := x_i \cdot \mathrm{Enc}_{pk}(P(x_i)), i \in [n]$

$$\xrightarrow{\{(c_i^1, c_i^2)\}_{i\in[n]}}$$

$X \cup Y := \{\mathrm{Dec}_{sk}(c_i^1)^{-1} \cdot \mathrm{Dec}_{sk}(c_i^2) | \mathrm{Dec}_{sk}(c_i^1) \neq 0, i \in [n]\}$

基于 AHE 的 PSU [DC17]

$S(X)$ $\qquad\qquad$ $R(Y)$

$$(pk, sk) \leftarrow \text{KeyGen}(1^\kappa)$$

$$F := \text{IBF}(Y) = f_1 f_2 \ldots f_m \in \{0,1\}^m$$

$$\xleftarrow{\quad pk, \{\text{Enc}_{pk}(f_i)\}_{i\in[m]} \quad}$$

$$c_i^1 = \textstyle\sum_{j\in[\lambda]} \text{Enc}_{pk}(f_{h_j(x_i)}), i \in [n]$$

$$c_i^2 := x_i \cdot c_i^1, i \in [n]$$

$$\xrightarrow{\quad \{(c_i^1, c_i^2)\}_{i\in[n]} \quad}$$

$$X \cup Y := \{\text{Dec}_{sk}(c_i^1)^{-1} \cdot \text{Dec}_{sk}(c_i^2) | \text{Dec}_{sk}(c_i^1) \neq 0, i \in [n]\}$$

1 介绍

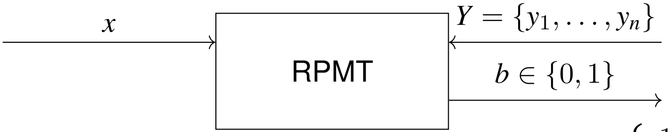
2 隐私集合求交：PSI

3 隐私集合求并：PSU
- 基于 AHE
- 基于 (mq-)RPMT+OT

4 参考文献

Reverse Private Membership Test (RPMT) [Kol+19]

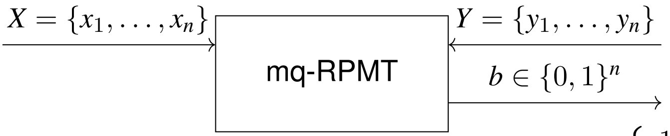
$S(x)$ $\qquad\qquad$ $R(Y = \{y_1, \dots, y_n\})$



$$b = \begin{cases} 1 & x \in Y; \\ 0 & x \notin Y \end{cases}$$

Multi-Query Reverse Private Membership Test (mq-RPMT) [Zha+23]

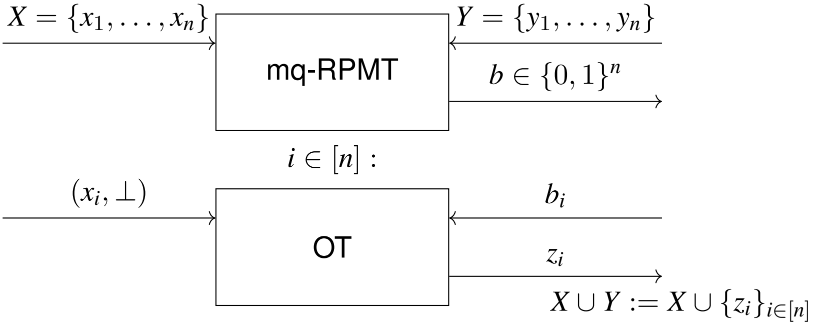
$S(X = \{x_1, \ldots, x_n\})$ $R(Y = \{y_1, \ldots, y_n\})$



$$b_i = \begin{cases} 1 & x_i \in Y; \\ 0 & x_i \notin Y \end{cases}$$

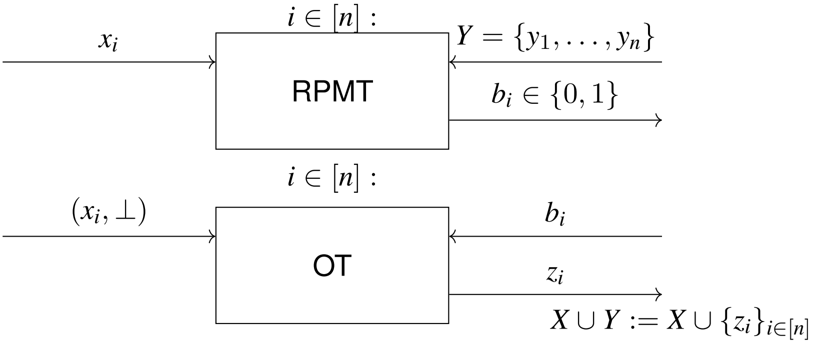
mq-RPMT+OT$\Longrightarrow$ PSU

$S(X = \{x_1, \ldots, x_n\})$ $\qquad$ $R(Y = \{y_1, \ldots, y_n\})$

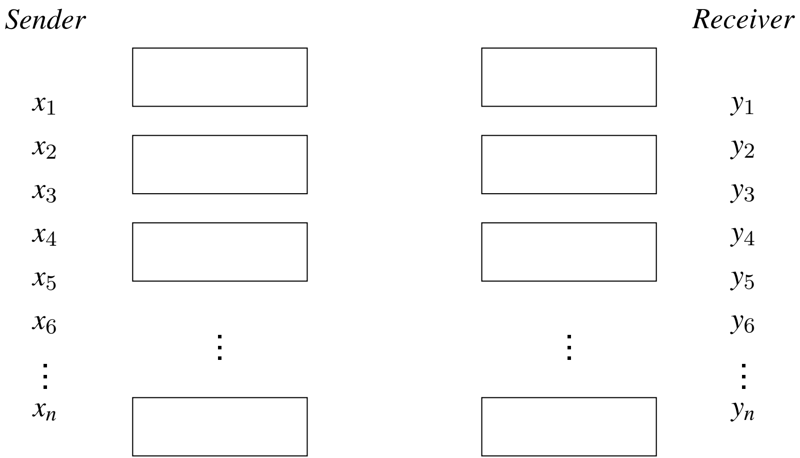


RPMT+OT$\Longrightarrow$ PSU

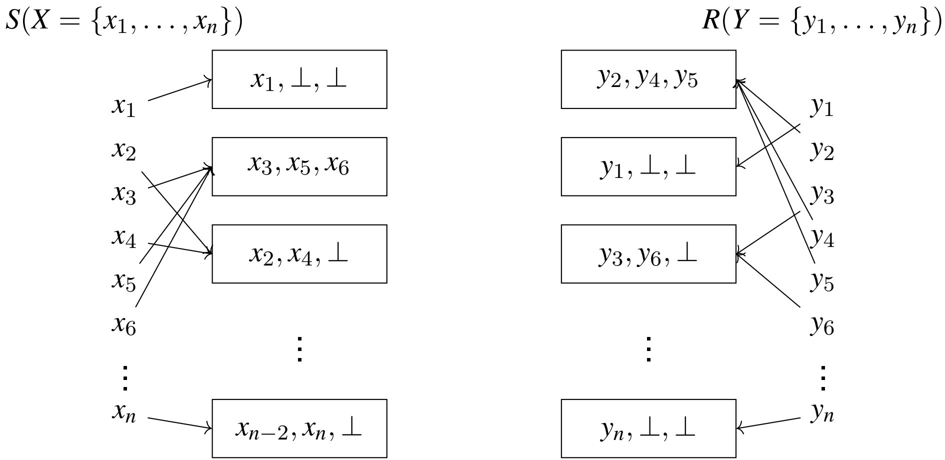
$S(X = \{x_1, \ldots, x_n\})$ $R(Y = \{y_1, \ldots, y_n\})$



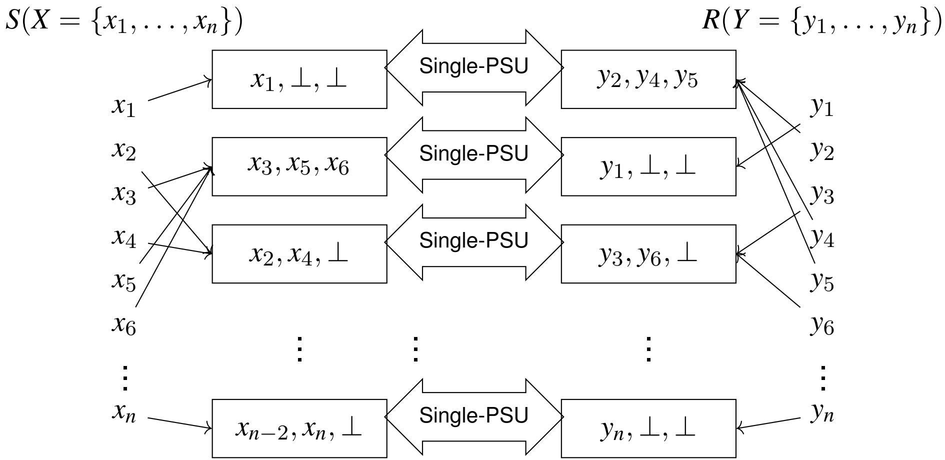
Single PSU +Simple Hash $\Longrightarrow$ PSU [Kol+19]



Single PSU +Simple Hash $\Longrightarrow$ PSU [Kol+19]



Single PSU +Simple Hash $\Longrightarrow$ PSU [Kol+19]



Hash to Bin 的问题

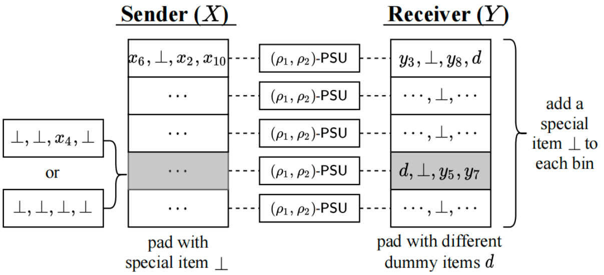
[Kol+19] 指出需要注意的地方：

- 每个 bin 需要填充 $\perp$ 至最大值：防止 receiver 缩小交集范围
- 只能使用 simple hash：如果 sender 使用 cuckoo hash，每个元素的位置和整个集合相关，当这个元素被 receiver 得到后会泄露整个集合的信息，无法模拟

即使如此，[Jia+22a] 指出上述协议依然是不安全的：

- 当 receiver 在某个 bin 发现得到的 b_i 全为 0 时，sender 在这个 bin 里全是 $\perp$ 和至少有一个真实元素的概率是不同的，而且这个概率相差很大，因此 receiver 有很大概率会得到部分交集信息

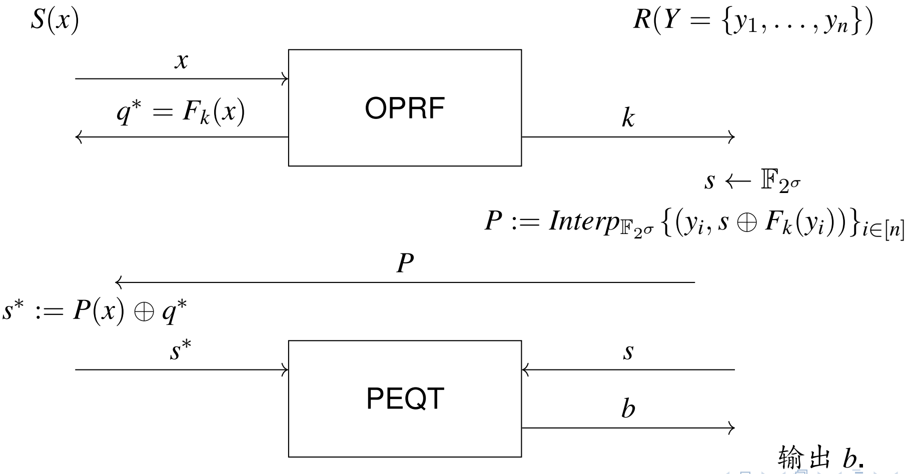
Hash to Bin 的问题



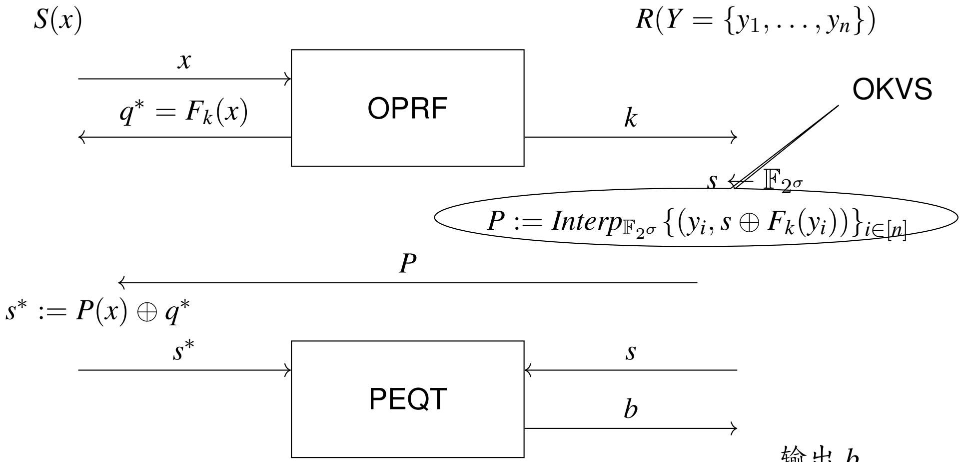
设集合大小为 n，bin 数量为 αn，则 $Pr[case_2] = (1 - 1/\alpha n)^n \approx e^{-1/\alpha}$

parameters	set size n							
	2^8	2^{10}	2^{12}	2^{14}	2^{16}	2^{18}	2^{20}	2^{22}
α	0.043	0.055	0.05	0.053	0.058	0.052	0.06	0.051
$\Pr(\times 10^{-11})$	7.946	1270	206.1	639.4	3252	444.8	5778	305.1

RPMT [Kol+19]


$S(x)$
$R(Y = \{y_1, \ldots, y_n\})$
x
OPRF
$q^* = F_k(x)$
k
$s \leftarrow \mathbb{F}_{2^\sigma}$
$P := Interp_{\mathbb{F}_{2^\sigma}}\{(y_i, s \oplus F_k(y_i))\}_{i \in [n]}$
P
$s^* := P(x) \oplus q^*$
s^*
PEQT
s
b
输出 b.

RPMT $\longrightarrow$ mq-RPMT [Zha+23]



输出 b.

RPMT $\longrightarrow$ mq-RPMT [Zha+23]

$S(x)$ $\qquad\qquad$ $R(Y = \{y_1, \ldots, y_n\})$

$x \longrightarrow$ **OPRF**

$q^* = F_k(x) \longleftarrow$ **OPRF** $\longrightarrow k$

$s \leftarrow \mathbb{F}_{2^\sigma}$

$D := \text{Encode}\{(y_i, s \oplus F_k(y_i))\}_{i \in [n]}$

$\xleftarrow{\quad D \quad}$

$s^* := \text{Decode}(D, x) \oplus q^*$

$s^* \longrightarrow$ **PEQT** $\longleftarrow s$

PEQT $\longrightarrow b$

输出 b.

RPMT $\longrightarrow$ mq-RPMT [Zha+23]

$S(X = \{x_1, \ldots, x_n\})$ $\qquad\qquad$ $R(Y = \{y_1, \ldots, y_n\})$

$\{x_i\}_{i \in [n]}$ → OPRF

OPRF → $\{q_i^* = F_k(x_i)\}_{i \in [n]}$ (to S)

OPRF → k (to R)

$s \leftarrow \mathbb{F}_{2^\sigma}$

$D := \text{Encode}\{(y_i, s \oplus F_k(y_i))\}_{i \in [n]}$

$R \xrightarrow{D} S$

$i \in [n]:$

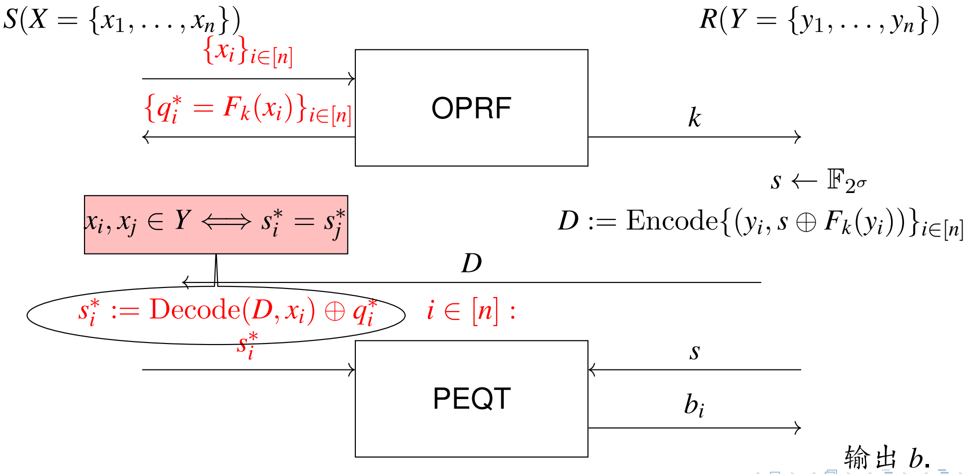
$s_i^* := \text{Decode}(D, x_i) \oplus q_i^*$

s_i^* → PEQT ← s

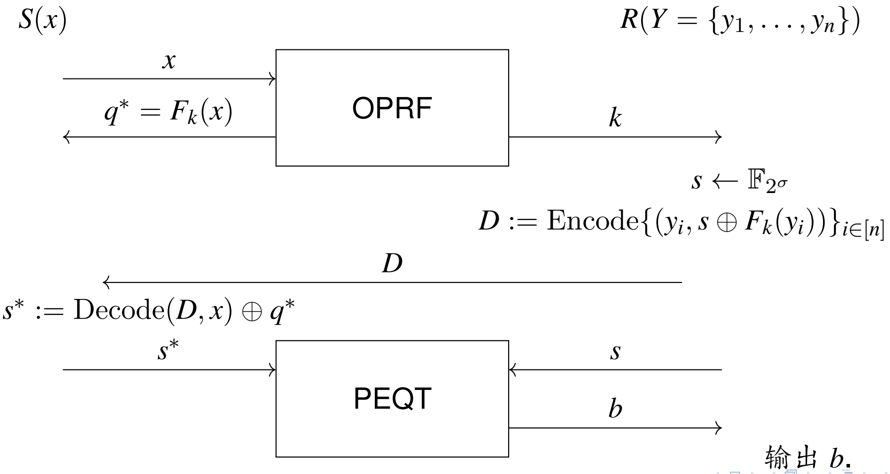
PEQT → b_i (to R)

输出 b.

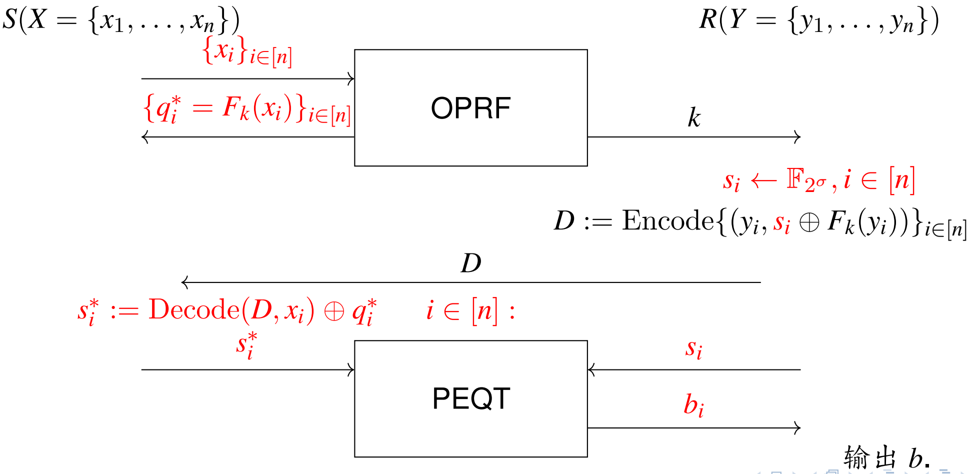
RPMT $\longrightarrow$ mq-RPMT [Zha+23]



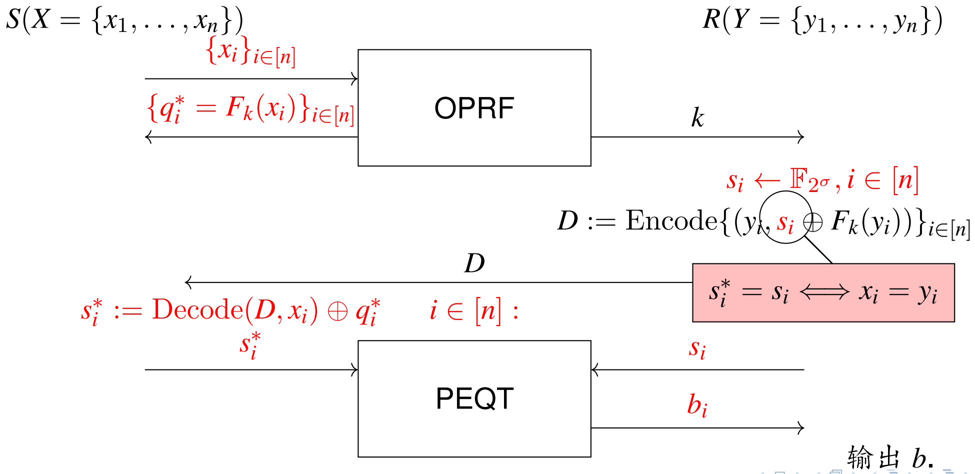
RPMT $\longrightarrow$ mq-RPMT [Zha+23]



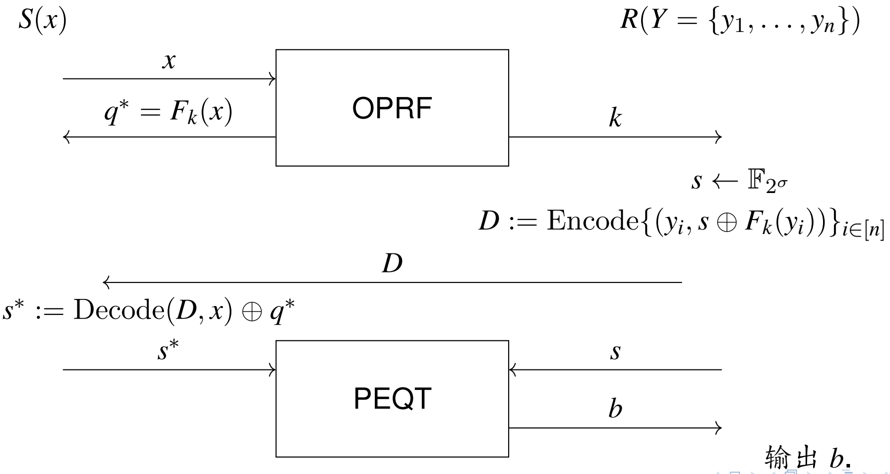
RPMT $\longrightarrow$ mq-RPMT [Zha+23]



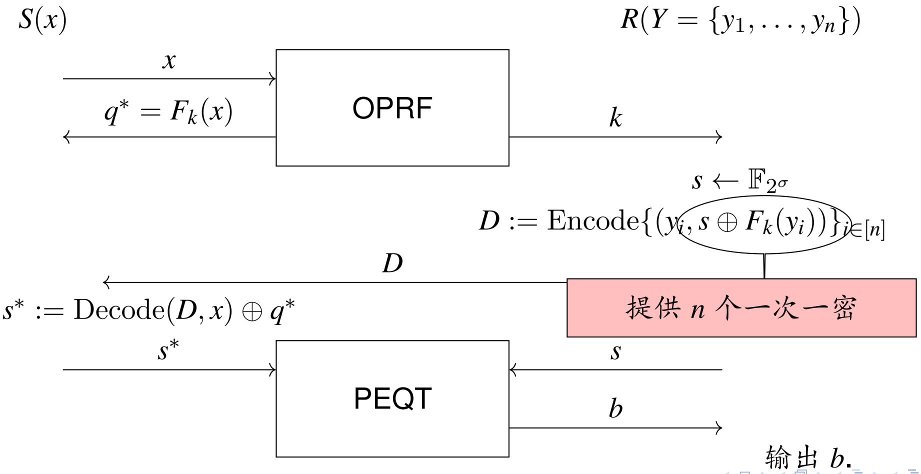
RPMT $\longrightarrow$ mq-RPMT [Zha+23]



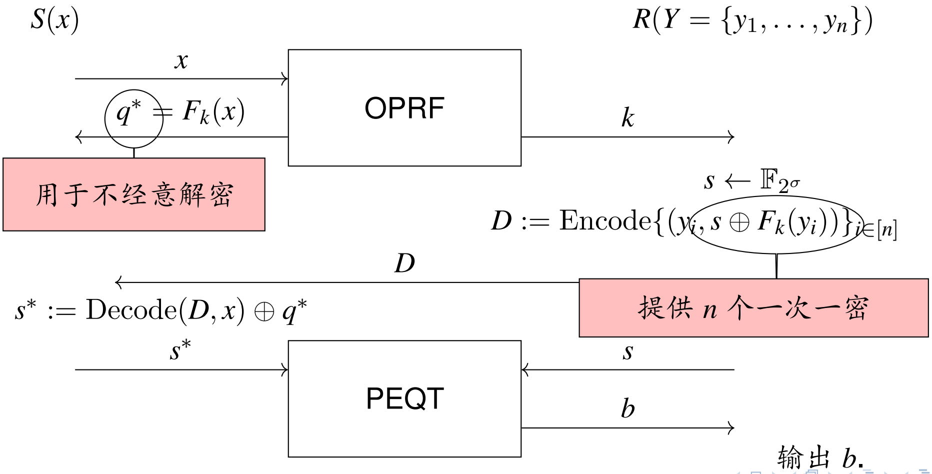
RPMT $\longrightarrow$ mq-RPMT [Zha+23]



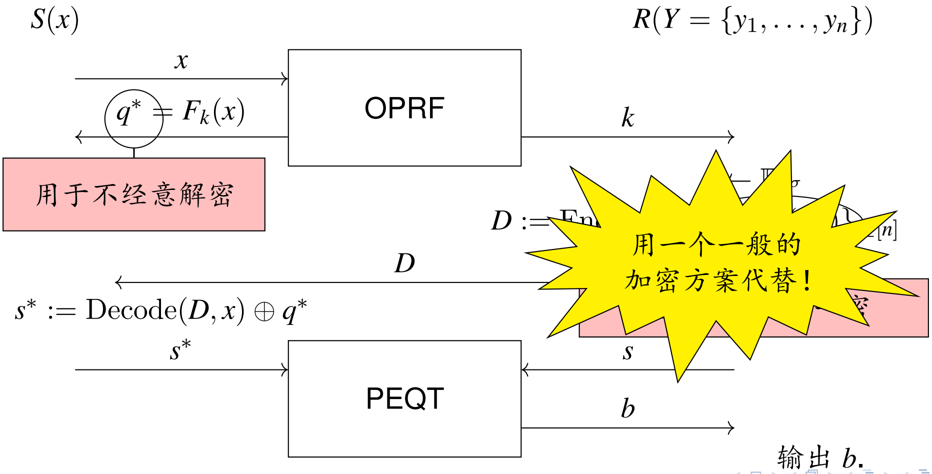
RPMT $\longrightarrow$ mq-RPMT [Zha+23]



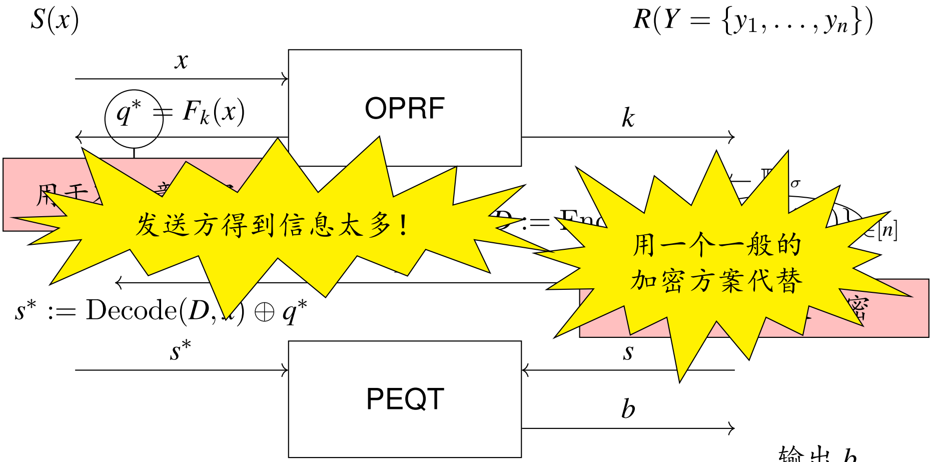
RPMT $\longrightarrow$ mq-RPMT [Zha+23]



RPMT $\longrightarrow$ mq-RPMT [Zha+23]

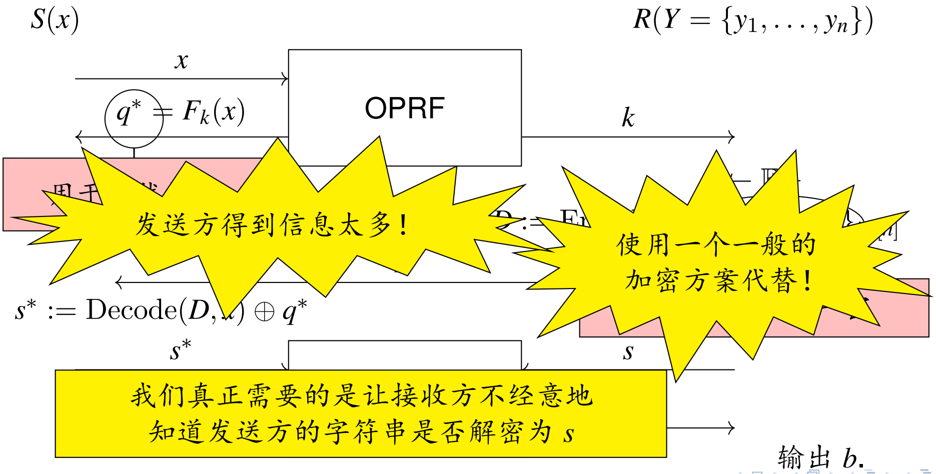


RPMT $\longrightarrow$ mq-RPMT [Zha+23]



输出 b.

RPMT $\longrightarrow$ mq-RPMT [Zha+23]



RPMT $\longrightarrow$ mq-RPMT [Zha+23]

$S(x)$ $\qquad\qquad$ $R(Y = \{y_1, \dots, y_n\})$

$x \longrightarrow$ OPRF

$q^* = F_k(x) \longleftarrow$ OPRF

$k \leftarrow \mathrm{KeyGen}(1^\kappa)$

$s \leftarrow \mathbb{F}_{2^\sigma}$

$D := \mathrm{Encode}\{(y_i, \mathrm{Enc}(k, s))\}_{i \in [n]}$

$\xleftarrow{\quad D \quad}$

$s^* := \mathrm{Decode}(D, x) \oplus q^*$

$s^* \longrightarrow$ PEQT $\longleftarrow s$

PEQT $\xrightarrow{\ b\ }$

输出 b.

RPMT $\longrightarrow$ mq-RPMT [Zha+23]

$S(x)$ $\qquad$ $R(Y = \{y_1, \ldots, y_n\})$

$$k \leftarrow \mathrm{KeyGen}(1^\kappa)$$

$$s \leftarrow \mathbb{F}_{2^\sigma}$$

$$D := \mathrm{Encode}\{(y_i, \mathrm{Enc}(k, s))\}_{i \in [n]}$$

$$\xleftarrow{\quad D \quad}$$

$$s_i^* := \mathrm{Decode}(D, x_i), i \in [n]$$

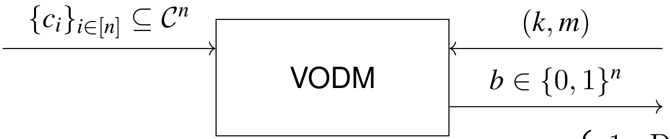
将不经意解密和 PEQT 功能合并

输出 b.

Vector Oblivious Decryption-then-Matching (VODM)

令 (Setup, KeyGen, Enc, Dec) 是一个加密方案：

$S(C = \{c_1, \ldots, c_n\})$ $R(k, m)$



$$b_i = \begin{cases} 1 & \mathrm{Dec}(k, c_i) = m; \\ 0 & \mathrm{Dec}(k, c_i) \neq m \end{cases}$$

mq-RPMT [Zha+23]

$S(X = \{x_1, \ldots, x_n\})$

$R(Y = \{y_1, \ldots, y_n\})$

$k \leftarrow \mathrm{KeyGen}(1^\kappa)$

$s \leftarrow \mathbb{F}_{2^\sigma}$

$D := \mathrm{Encode}\{(x_i, \mathrm{Enc}(k, s))\}_{i \in [n]}$

$\xleftarrow{\quad D \quad}$

$s_i^* := \mathrm{Decode}(D, y_i), i \in [n]$

$\{s_i^*\}_{i\in[n]} \rightarrow$ VODM $\leftarrow (k, s)$

VODM $\xrightarrow{\quad b \quad}$

输出 b.

mq-RPMT from ReRand PKE [Zha+23]

$S(X=\{x_1,\ldots,x_n\})$

$R(Y=\{y_1,\ldots,y_n\})$

$k \leftarrow \mathrm{KeyGen}(1^\kappa)$

$s \leftarrow \mathbb{F}_{2^\sigma}$

$D := \mathrm{Encode}\{(y_i, \mathrm{Enc}(k,s))\}_{i\in[n]}$

$$\xleftarrow{\quad D \quad}$$

$s_i^* := \mathrm{Decode}(D, x_i), i \in [n]$

$\overline{s_i^*} := \mathrm{ReRand}(s_i^*; r_i), i \in [n]$

$$\xrightarrow{\quad \{\overline{s_i^*}\}_{i\in[n]} \quad}$$

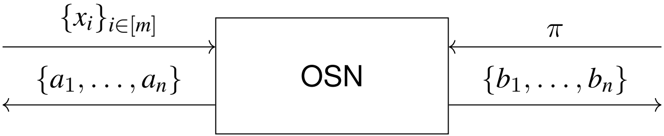
$$b_i = \begin{cases} 1 & \mathrm{Dec}(sk, \overline{s_i^*}) = s; \\ 0 & \mathrm{Dec}(sk, \overline{s_i^*}) \neq s \end{cases}$$

输出 b.

Oblivious Switching Network (OSN)

设 $\pi : [n] \to [m]$ 是单射，Oblivious Switching Network (OSN) [MS13] /Permute+Share [CGP20] 功能定义如下：

$S(X = \{x_1, \ldots, x_m\})$ $R(\pi)$



$$a_i \oplus b_i = x_{\pi(i)}, i \in [n]$$

(permuted) mq-RPMT [Gar+21b]

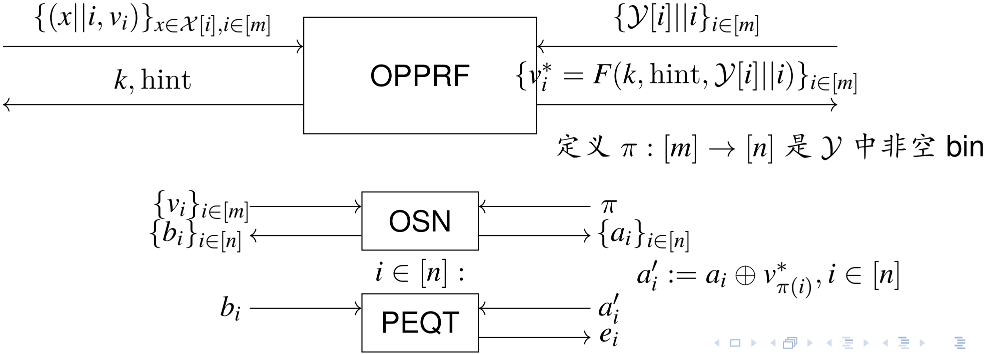
$S(X = \{x_1, \ldots, x_n\})$

$\mathcal{X} \leftarrow SimpleH^m_{h_1,h_2,h_3}(X)$

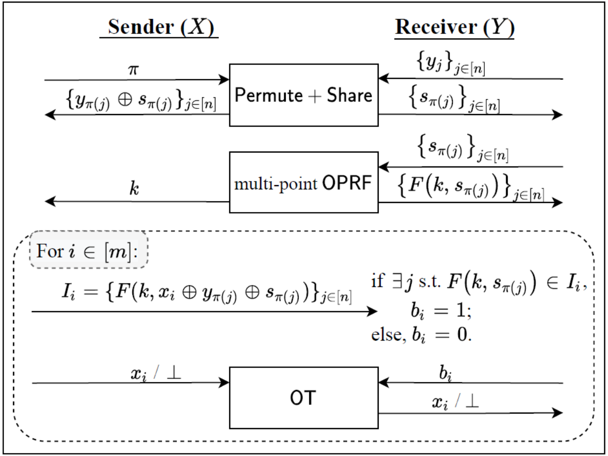
$v_i \leftarrow \{0,1\}^l, i \in [m]$

$R(Y = \{y_1, \ldots, y_n\})$

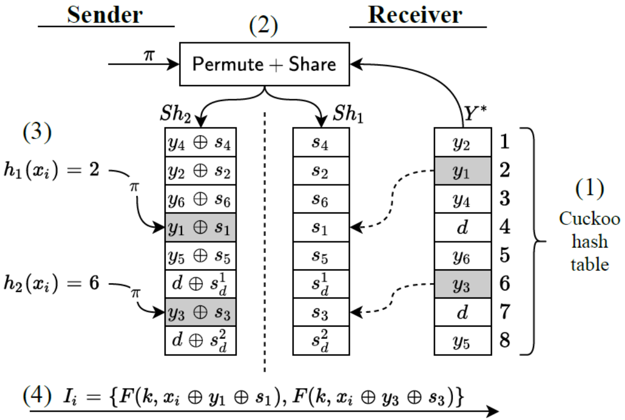
$\mathcal{Y} \leftarrow CuckooH^m_{h_1,h_2,h_3}(Y)$



mq-RPMT [Jia+22a]



mq-RPMT [Jia+22a]



mq-RPMT [Che+22b]

回忆 DH-PSI：

$$S(X = \{x_1, \ldots, x_n\}) \qquad\qquad R(Y = \{y_1, \ldots, y_n\})$$

$$a \leftarrow \mathbb{Z}_q, A := \{H(x_i)^a\}_{i\in[n]}$$

$$\xrightarrow{\quad A \quad}$$

$$b \leftarrow \mathbb{Z}_q, B := \{H(y_i)^b\}_{i\in[n]}$$

$$\xleftarrow{\quad B \quad}$$

$$C := \{B_i^a\}_{i\in[n]}$$

$$\xrightarrow{\quad C \quad}$$

输出 $X \cap Y := \{y_i \in Y | C_i \in A^b\}$

mq-RPMT [Che+22b]

$S(X = \{x_1, \ldots, x_n\})$ $\qquad\qquad$ $R(Y = \{y_1, \ldots, y_n\})$

$a \leftarrow \mathbb{Z}_q, A := \{H(x_i)^a\}_{i \in [n]}$

$$\xrightarrow{\qquad\qquad A \qquad\qquad}$$

$b \leftarrow \mathbb{Z}_q, B := \{H(y_i)^b\}_{i \in [n]}$

$$\xleftarrow{\qquad\qquad B \qquad\qquad}$$

$C := \{\pi(B_i^a)\}_{i \in [n]}$

$$\xrightarrow{\qquad\qquad C \qquad\qquad}$$

$$e_i = \begin{cases} 1 & A_i^b \in C; \\ 0 & A_i^b \notin C \end{cases}$$

mq-RPMT [Che+22b]

$S(X = \{x_1, \ldots, x_n\})$ $\qquad$ $R(Y = \{y_1, \ldots, y_n\})$

$a \leftarrow \mathbb{Z}_q, A := \{H(x_i)^a\}_{i \in [n]}$

$$\xrightarrow{\quad A \quad}$$

$b \leftarrow \mathbb{Z}_q, B := \{H(y_i)^b\}_{i \in [n]}$

$$\xleftarrow{\quad B \quad}$$

$C := BF(\{B_i^a\}_{i \in [n]})$

$$\xrightarrow{\quad C \quad}$$

$$e_i = \begin{cases} 1 & A_i^b \in C; \\ 0 & A_i^b \notin C \end{cases}$$

1. 介绍
2. 隐私集合求交：PSI
3. 隐私集合求并：PSU
4. 参考文献

参考文献 I

[AMZ21] Aydin Abadi, Steven J. Murdoch, and Thomas Zacharias. “Polynomial Representation Is Tricky: Maliciously Secure Private Set Intersection Revisited”. In: *Computer Security - ESORICS 2021 - 26th European Symposium on Research in Computer Security, Darmstadt, Germany, October 4-8, 2021, Proceedings, Part II*. Ed. by Elisa Bertino, Haya Shulman, and Michael Waidner. Vol. 12973. Lecture Notes in Computer Science. Springer, 2021, pp. 721–742. DOI: 10.1007/978-3-030-88428-4_35. URL: https://doi.org/10.1007/978-3-030-88428-4_35.

参考文献 II

[ATD16] Aydin Abadi, Sotirios Terzis, and Changyu Dong. “VD-PSI: Verifiable Delegated Private Set Intersection on Outsourced Private Datasets”. In: *Financial Cryptography and Data Security - 20th International Conference, FC 2016, Christ Church, Barbados, February 22-26, 2016, Revised Selected Papers*. Ed. by Jens Grossklags and Bart Preneel. Vol. 9603. Lecture Notes in Computer Science. Springer, 2016, pp. 149–168. DOI: 10.1007/978-3-662-54970-4_9. URL: https://doi.org/10.1007/978-3-662-54970-4_9.

参考文献 III

[Aba+19] Aydin Abadi et al. "Efficient Delegated Private Set Intersection on Outsourced Private Datasets". In: *IEEE Trans. Dependable Secur. Comput.* 16.4 (2019), pp. 608–624. DOI: 10.1109/TDSC.2017.2708710. URL: https://doi.org/10.1109/TDSC.2017.2708710.

[Aba+22] Aydin Abadi et al. "Multi-party Updatable Delegated Private Set Intersection". In: *Financial Cryptography and Data Security - 26th International Conference, FC 2022, Grenada, May 2-6, 2022, Revised Selected Papers*. Ed. by Ittay Eyal and Juan A. Garay. Vol. 13411. Lecture Notes in Computer Science. Springer, 2022, pp. 100–119. DOI: 10.1007/978-3-031-18283-9_6. URL: https://doi.org/10.1007/978-3-031-18283-9_6.

参考文献 IV

[AES03] Rakesh Agrawal, Alexandre V. Evfimievski, and Ramakrishnan Srikant. “Information Sharing Across Private Databases”. In: *Proceedings of the 2003 ACM SIGMOD International Conference on Management of Data, San Diego, California, USA, June 9-12, 2003*. Ed. by Alon Y. Halevy, Zachary G. Ives, and AnHai Doan. ACM, 2003, pp. 86–97. DOI: 10.1145/872757.872771. URL: https://doi.org/10.1145/872757.872771.

参考文献 V

[Ala+21] Navid Alamati et al. "Laconic Private Set Intersection and Applications". In: *Theory of Cryptography - 19th International Conference, TCC 2021, Raleigh, NC, USA, November 8-11, 2021, Proceedings, Part III*. Ed. by Kobbi Nissim and Brent Waters. Vol. 13044. Lecture Notes in Computer Science. Springer, 2021, pp. 94–125. DOI: 10.1007/978-3-030-90456-2_4. URL: https://doi.org/10.1007/978-3-030-90456-2_4.

参考文献 VI

[Ara+22] Diego F. Aranha et al. “Laconic Private Set-Intersection From Pairings”. In: *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, CCS 2022, Los Angeles, CA, USA, November 7-11, 2022*. Ed. by Heng Yin et al. ACM, 2022, pp. 111–124. DOI: 10.1145/3548606.3560642. URL: https://doi.org/10.1145/3548606.3560642.

参考文献 VII

[ANS10] Yuriy Arbitman, Moni Naor, and Gil Segev. "Backyard Cuckoo Hashing: Constant Worst-Case Operations with a Succinct Representation". In: *51th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2010, October 23-26, 2010, Las Vegas, Nevada, USA*. IEEE Computer Society, 2010, pp. 787–796. DOI: 10.1109/FOCS.2010.80. URL: https://doi.org/10.1109/FOCS.2010.80.

参考文献 VIII

[Ash+13] Gilad Asharov et al. “More efficient oblivious transfer and extensions for faster secure computation”. In: *2013 ACM SIGSAC Conference on Computer and Communications Security, CCS'13, Berlin, Germany, November 4-8, 2013*. Ed. by Ahmad-Reza Sadeghi, Virgil D. Gligor, and Moti Yung. ACM, 2013, pp. 535–548. DOI: 10.1145/2508859.2516738. URL: https://doi.org/10.1145/2508859.2516738.

参考文献 IX

[ACT11] Giuseppe Ateniese, Emiliano De Cristofaro, and Gene Tsudik. "(If) Size Matters: Size-Hiding Private Set Intersection". In: *Public Key Cryptography - PKC 2011 - 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, March 6-9, 2011. Proceedings*. Ed. by Dario Catalano et al. Vol. 6571. Lecture Notes in Computer Science. Springer, 2011, pp. 156–173. DOI: 10.1007/978-3-642-19379-8_10. URL: https://doi.org/10.1007/978-3-642-19379-8_10.

参考文献 X

[Aza+94] Yossi Azar et al. “Balanced allocations (extended abstract)”. In: *Proceedings of the Twenty-Sixth Annual ACM Symposium on Theory of Computing, 23-25 May 1994, Montréal, Québec, Canada*. Ed. by Frank Thomson Leighton and Michael T. Goodrich. ACM, 1994, pp. 593–602. DOI: 10.1145/195058.195412. URL: https://doi.org/10.1145/195058.195412.

[BMX22] Saikrishna Badrinarayanan, Peihan Miao, and Tiancheng Xie. “Updatable Private Set Intersection”. In: *Proc. Priv. Enhancing Technol.* 2022.2 (2022), pp. 378–406. DOI: 10.2478/popets-2022-0051. URL: https://doi.org/10.2478/popets-2022-0051.

参考文献 XI

[Bad+21] Saikrishna Badrinarayanan et al. "Multi-party Threshold Private Set Intersection with Sublinear Communication". In: *Public-Key Cryptography - PKC 2021 - 24th IACR International Conference on Practice and Theory of Public Key Cryptography, Virtual Event, May 10-13, 2021, Proceedings, Part II*. Ed. by Juan A. Garay. Vol. 12711. Lecture Notes in Computer Science. Springer, 2021, pp. 349–379. DOI: 10.1007/978-3-030-75248-4_13. URL: https://doi.org/10.1007/978-3-030-75248-4_13.

[Bay+22] Aslí Bay et al. "Practical Multi-Party Private Set Intersection Protocols". In: *IEEE Trans. Inf. Forensics Secur.* 17 (2022), pp. 1–15. DOI: 10.1109/TIFS.2021.3118879. URL: https://doi.org/10.1109/TIFS.2021.3118879.

参考文献 XII

[BXR22] Tyler Beauregard, Janabel Xia, and Mike Rosulek. “Finding One Common Item, Privately”. In: *Security and Cryptography for Networks - 13th International Conference, SCN 2022, Amalfi, Italy, September 12-14, 2022, Proceedings*. Ed. by Clemente Galdi and Stanislaw Jarecki. Vol. 13409. Lecture Notes in Computer Science. Springer, 2022, pp. 462–480. DOI: 10.1007/978-3-031-14791-3_20. URL: https://doi.org/10.1007/978-3-031-14791-3_20.

参考文献 XIII

[Ben+22] Aner Ben-Efraim et al. “PSImple: Practical Multiparty Maliciously-Secure Private Set Intersection”. In: *ASIA CCS ’22: ACM Asia Conference on Computer and Communications Security, Nagasaki, Japan, 30 May 2022 - 3 June 2022*. Ed. by Yuji Suga et al. ACM, 2022, pp. 1098–1112. DOI: 10.1145/3488932.3523254. URL: https://doi.org/10.1145/3488932.3523254.

[BA12] Marina Blanton and Everaldo Aguiar. “Private and oblivious set and multiset operations”. In: *7th ACM Symposium on Information, Compuer and Communications Security, ASIACCS ’12, Seoul, Korea, May 2-4, 2012*. 2012, pp. 40–41. DOI: 10.1145/2414456.2414479. URL: https://doi.org/10.1145/2414456.2414479.

参考文献 XIV

[Blo70] Burton H. Bloom. "Space/Time Trade-offs in Hash Coding with Allowable Errors". In: *Commun. ACM* 13.7 (1970), pp. 422–426. DOI: 10.1145/362686.362692. URL: https://doi.org/10.1145/362686.362692.

[BDP21] Pedro Branco, Nico Döttling, and Sihang Pu. "Multiparty Cardinality Testing for Threshold Private Intersection". In: *Public-Key Cryptography - PKC 2021 - 24th IACR International Conference on Practice and Theory of Public Key Cryptography, Virtual Event, May 10-13, 2021, Proceedings, Part II*. Ed. by Juan A. Garay. Vol. 12711. Lecture Notes in Computer Science. Springer, 2021, pp. 32–60. DOI: 10.1007/978-3-030-75248-4_2. URL: https://doi.org/10.1007/978-3-030-75248-4_2.

参考文献 XV

[BS05] Justin Brickell and Vitaly Shmatikov. "Privacy-Preserving Graph Algorithms in the Semi-honest Model". In: *Advances in Cryptology - ASIACRYPT 2005, 11th International Conference on the Theory and Application of Cryptology and Information Security, Chennai, India, December 4-8, 2005, Proceedings*. Ed. by Bimal K. Roy. Vol. 3788. Lecture Notes in Computer Science. Springer, 2005, pp. 236–252. DOI: 10.1007/11593447_13. URL: https://doi.org/10.1007/11593447_13.

[BC23] Dung Bui and Geoffroy Couteau. "Improved Private Set Intersection for Sets with Small Entries". In: *Public-Key Cryptography - PKC 2023*. 2023.

参考文献 XVI

[CZ09] Jan Camenisch and Gregory M. Zaverucha. "Private Intersection of Certified Sets". In: *Financial Cryptography and Data Security, 13th International Conference, FC 2009, Accra Beach, Barbados, February 23-26, 2009. Revised Selected Papers*. Ed. by Roger Dingledine and Philippe Golle. Vol. 5628. Lecture Notes in Computer Science. Springer, 2009, pp. 108–127. DOI: 10.1007/978-3-642-03549-4_7. URL: https://doi.org/10.1007/978-3-642-03549-4_7.

参考文献 XVII

[CHL22] Sílvia Casacuberta, Julia Hesse, and Anja Lehmann. “SoK: Oblivious Pseudorandom Functions”. In: *7th IEEE European Symposium on Security and Privacy, EuroS&P 2022, Genoa, Italy, June 6-10, 2022*. IEEE, 2022, pp. 625–646. DOI: 10.1109/EuroSP53844.2022.00045. URL: https://doi.org/10.1109/EuroSP53844.2022.00045.

[CFR21] Anrin Chakraborti, Giulia Fanti, and Michael K. Reiter. “Distance-Aware Private Set Intersection”. In: *CoRR* abs/2112.14737 (2021). arXiv: 2112.14737. URL: https://arxiv.org/abs/2112.14737.

参考文献 XVIII

[CGS22] Nishanth Chandran, Divya Gupta, and Akash Shah. “Circuit-PSI With Linear Complexity via Relaxed Batch OPPRF”. In: *Proc. Priv. Enhancing Technol.* 2022.1 (2022), pp. 353–372. DOI: 10.2478/popets-2022-0018. URL: https://doi.org/10.2478/popets-2022-0018.

[Cha+21] Nishanth Chandran et al. “Efficient Linear Multiparty PSI and Extensions to Circuit/Quorum PSI”. In: *CCS ’21: 2021 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, Republic of Korea, November 15 - 19, 2021*. Ed. by Yongdae Kim et al. ACM, 2021, pp. 1182–1204. DOI: 10.1145/3460120.3484591. URL: https://doi.org/10.1145/3460120.3484591.

参考文献 XIX

[CGP20] Melissa Chase, Esha Ghosh, and Oxana Poburinnaya. "Secret-Shared Shuffle". In: *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part III*. Ed. by Shiho Moriai and Huaxiong Wang. Vol. 12493. Lecture Notes in Computer Science. Springer, 2020, pp. 342–372. DOI: 10.1007/978-3-030-64840-4_12. URL: https://doi.org/10.1007/978-3-030-64840-4_12.

参考文献 XX

[CM20] Melissa Chase and Peihan Miao. “Private Set Intersection in the Internet Setting from Lightweight Oblivious PRF”. In: *Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part III*. 2020, pp. 34–63. DOI: 10.1007/978-3-030-56877-1_2. URL: https://doi.org/10.1007/978-3-030-56877-1_2.

参考文献 XXI

[CLR17] Hao Chen, Kim Laine, and Peter Rindal. “Fast Private Set Intersection from Homomorphic Encryption”. In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017*. Ed. by Bhavani M. Thuraisingham et al. ACM, 2017, pp. 1243–1255. DOI: 10.1145/3133956.3134061. URL: https://doi.org/10.1145/3133956.3134061.

参考文献 XXII

[Che+18] Hao Chen et al. “Labeled PSI from Fully Homomorphic Encryption with Malicious Security”. In: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018*. Ed. by David Lie et al. ACM, 2018, pp. 1223–1237. DOI: 10.1145/3243734.3243836. URL: https://doi.org/10.1145/3243734.3243836.

[Che+22a] You Chen et al. “Practical Multi-party Private Set Intersection Cardinality and Intersection-Sum Under Arbitrary Collusion”. In: *Inscrypt 2022*. Ed. by Wenhao Wang and Moti Yung. Springer, 2022.

参考文献 XXIII

[Che+22b] Yu Chen et al. *Private Set Operations from Multi-Query Reverse Private Membership Test*. Cryptology ePrint Archive, Paper 2022/652. https://eprint.iacr.org/2022/652. 2022. URL: https://eprint.iacr.org/2022/652.

[Cho+22] Wutichai Chongchitmate et al. "PSI from Ring-OLE". In: *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, CCS 2022, Los Angeles, CA, USA, November 7-11, 2022*. Ed. by Heng Yin et al. ACM, 2022, pp. 531–545. DOI: 10.1145/3548606.3559378. URL: https://doi.org/10.1145/3548606.3559378.

参考文献 XXIV

[CGN98] Benny Chor, Niv Gilboa, and Moni Naor. *Private Information Retrieval by Keywords*. Cryptology ePrint Archive, Paper 1998/003. https://eprint.iacr.org/1998/003. 1998. URL: https://eprint.iacr.org/1998/003.

[CO18] Michele Ciampi and Claudio Orlandi. "Combining Private Set-Intersection with Secure Two-Party Computation". In: *Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings*. Ed. by Dario Catalano and Roberto De Prisco. Vol. 11035. Lecture Notes in Computer Science. Springer, 2018, pp. 464–482. DOI: 10.1007/978-3-319-98113-0_25. URL: https://doi.org/10.1007/978-3-319-98113-0_25.

参考文献 XXV

[Con+21] Kelong Cong et al. “Labeled PSI from Homomorphic Encryption with Reduced Computation and Communication”. In: *CCS ’21: 2021 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, Republic of Korea, November 15 - 19, 2021*. Ed. by Yongdae Kim et al. ACM, 2021, pp. 1135–1150. DOI: 10.1145/3460120.3484760. URL: https://doi.org/10.1145/3460120.3484760.

参考文献 XXVI

[CGT12] Emiliano De Cristofaro, Paolo Gasti, and Gene Tsudik. “Fast and Private Computation of Cardinality of Set Intersection and Union”. In: *Cryptology and Network Security, 11th International Conference, CANS 2012, Darmstadt, Germany, December 12-14, 2012. Proceedings*. Ed. by Josef Pieprzyk, Ahmad-Reza Sadeghi, and Mark Manulis. Vol. 7712. Springer, 2012, pp. 218–231. DOI: 10.1007/978-3-642-35404-5_17. URL: https://doi.org/10.1007/978-3-642-35404-5_17.

参考文献 XXVII

[CKT10] Emiliano De Cristofaro, Jihye Kim, and Gene Tsudik. "Linear-Complexity Private Set Intersection Protocols Secure in Malicious Model". In: *Advances in Cryptology - ASIACRYPT 2010 - 16th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 5-9, 2010. Proceedings*. Ed. by Masayuki Abe. Vol. 6477. Lecture Notes in Computer Science. Springer, 2010, pp. 213–231. DOI: 10.1007/978-3-642-17373-8_13. URL: https://doi.org/10.1007/978-3-642-17373-8_13.

参考文献 XXVIII

[CT12] Emiliano De Cristofaro and Gene Tsudik. “Experimenting with Fast Private Set Intersection”. In: *Trust and Trustworthy Computing - 5th International Conference, TRUST 2012, Vienna, Austria, June 13-15, 2012. Proceedings*. Ed. by Stefan Katzenbeisser et al. Vol. 7344. Lecture Notes in Computer Science. Springer, 2012, pp. 55–73. DOI: 10.1007/978-3-642-30921-2_4. URL: https://doi.org/10.1007/978-3-642-30921-2_4.

参考文献 XXIX

[CT10] Emiliano De Cristofaro and Gene Tsudik. “Practical Private Set Intersection Protocols with Linear Complexity”. In: *Financial Cryptography and Data Security, 14th International Conference, FC 2010, Tenerife, Canary Islands, Spain, January 25-28, 2010, Revised Selected Papers*. Ed. by Radu Sion. Vol. 6052. Lecture Notes in Computer Science. Springer, 2010, pp. 143–159. DOI: 10.1007/978-3-642-14577-3_13. URL: https://doi.org/10.1007/978-3-642-14577-3_13.

参考文献 XXX

[Dac+09] Dana Dachman-Soled et al. “Efficient Robust Private Set Intersection”. In: *Applied Cryptography and Network Security, 7th International Conference, ACNS 2009, Paris-Rocquencourt, France, June 2-5, 2009. Proceedings*. Ed. by Michel Abdalla et al. Vol. 5536. Lecture Notes in Computer Science. 2009, pp. 125–142. DOI: 10.1007/978-3-642-01957-9_8. URL: https://doi.org/10.1007/978-3-642-01957-9_8.

参考文献 XXXI

[DC17] Alex Davidson and Carlos Cid. "An Efficient Toolkit for Computing Private Set Operations". In: *Information Security and Privacy - 22nd Australasian Conference, ACISP 2017, Auckland, New Zealand, July 3-5, 2017, Proceedings, Part II*. 2017, pp. 261–278. DOI: 10.1007/978-3-319-59870-3_15. URL: https://doi.org/10.1007/978-3-319-59870-3_15.

[Dit+22] Samuel Dittmer et al. "Streaming and Unbalanced PSI from Function Secret Sharing". In: *Security and Cryptography for Networks - 13th International Conference, SCN 2022, Amalfi, Italy, September 12-14, 2022, Proceedings*. 2022.

参考文献 XXXII

[DCW13] Changyu Dong, Liqun Chen, and Zikai Wen. “When private set intersection meets big data: an efficient and scalable protocol”. In: *2013 ACM SIGSAC Conference on Computer and Communications Security, CCS'13, Berlin, Germany, November 4-8, 2013*. Ed. by Ahmad-Reza Sadeghi, Virgil D. Gligor, and Moti Yung. ACM, 2013, pp. 789–800. DOI: 10.1145/2508859.2516701. URL: https://doi.org/10.1145/2508859.2516701.

参考文献 XXXIII

[DPT20] Thai Duong, Duong Hieu Phan, and Ni Trieu. “Catalic: Delegated PSI Cardinality with Applications to Contact Tracing”. In: *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part III*. Ed. by Shiho Moriai and Huaxiong Wang. Vol. 12493. Lecture Notes in Computer Science. Springer, 2020, pp. 870–899. DOI: 10.1007/978-3-030-64840-4_29. URL: https://doi.org/10.1007/978-3-030-64840-4_29.

参考文献 XXXIV

[Ege+15] Rolf Egert et al. "Privately Computing Set-Union and Set-Intersection Cardinality via Bloom Filters". In: *Information Security and Privacy - 20th Australasian Conference, ACISP 2015, Brisbane, QLD, Australia, June 29 - July 1, 2015, Proceedings*. Ed. by Ernest Foo and Douglas Stebila. Vol. 9144. Lecture Notes in Computer Science. Springer, 2015, pp. 413–430. DOI: 10.1007/978-3-319-19962-7_24. URL: https://doi.org/10.1007/978-3-319-19962-7_24.

参考文献 XXXV

[FNO19] Brett Hemenway Falk, Daniel Noble, and Rafail Ostrovsky. "Private Set Intersection with Linear Communication from General Assumptions". In: *Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society, WPES@CCS 2019, London, UK, November 11, 2019*. Ed. by Lorenzo Cavallaro, Johannes Kinder, and Josep Domingo-Ferrer. ACM, 2019, pp. 14–25. DOI: 10.1145/3338498.3358645. URL: https://doi.org/10.1145/3338498.3358645.

参考文献 XXXVI

[FNP04] Michael J. Freedman, Kobbi Nissim, and Benny Pinkas. “Efficient Private Matching and Set Intersection”. In: *Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings*. Ed. by Christian Cachin and Jan Camenisch. Vol. 3027. Lecture Notes in Computer Science. Springer, 2004, pp. 1–19. DOI: 10.1007/978-3-540-24676-3_1. URL: https://doi.org/10.1007/978-3-540-24676-3_1.

参考文献 XXXVII

[Fre+16] Michael J. Freedman et al. “Efficient Set Intersection with Simulation-Based Security”. In: *J. Cryptology* 29.1 (2016), pp. 115–155. DOI: 10.1007/s00145-014-9190-0. URL: https://doi.org/10.1007/s00145-014-9190-0.

[Fre+05] Michael J. Freedman et al. “Keyword Search and Oblivious Pseudorandom Functions”. In: *Theory of Cryptography, Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12, 2005, Proceedings*. Ed. by Joe Kilian. Vol. 3378. Lecture Notes in Computer Science. Springer, 2005, pp. 303–324. DOI: 10.1007/978-3-540-30576-7_17. URL: https://doi.org/10.1007/978-3-540-30576-7_17.

参考文献 XXXVIII

[Fri07] Keith B. Frikken. “Privacy-Preserving Set Union”. In: *Applied Cryptography and Network Security, 5th International Conference, ACNS 2007, Zhuhai, China, June 5-8, 2007, Proceedings*. 2007, pp. 237–252. DOI: 10.1007/978-3-540-72738-5_16. URL: https://doi.org/10.1007/978-3-540-72738-5_16.

[GRS23] Gayathri Garimella, Mike Rosulek, and Jaspal Singh. “Malicious Secure, Structure-Aware Private Set Intersection”. In: *Advances in Cryptology - CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023*. 2023.

参考文献 XXXIX

[GRS22] Gayathri Garimella, Mike Rosulek, and Jaspal Singh. "Structure-Aware Private Set Intersection, with Applications to Fuzzy Matching". In: *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part I*. Ed. by Yevgeniy Dodis and Thomas Shrimpton. Vol. 13507. Lecture Notes in Computer Science. Springer, 2022, pp. 323–352. DOI: 10.1007/978-3-031-15802-5_12. URL: https://doi.org/10.1007/978-3-031-15802-5_12.

参考文献 XL

[Gar+21a] Gayathri Garimella et al. “Oblivious Key-Value Stores and Amplification for Private Set Intersection”. In: *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part II*. Ed. by Tal Malkin and Chris Peikert. Vol. 12826. Lecture Notes in Computer Science. Springer, 2021, pp. 395–425. DOI: 10.1007/978-3-030-84245-1_14. URL: https://doi.org/10.1007/978-3-030-84245-1_14.

参考文献 XLI

[Gar+21b] Gayathri Garimella et al. “Private Set Operations from Oblivious Switching”. In: *Public-Key Cryptography - PKC 2021 - 24th IACR International Conference on Practice and Theory of Public Key Cryptography, Virtual Event, May 10-13, 2021, Proceedings, Part II*. Ed. by Juan A. Garay. Vol. 12711. Lecture Notes in Computer Science. Springer, 2021, pp. 591–617. DOI: 10.1007/978-3-030-75248-4_21. URL: https://doi.org/10.1007/978-3-030-75248-4_21.

参考文献 XLII

[GN19] Satrajit Ghosh and Tobias Nilges. “An Algebraic Approach to Maliciously Secure Private Set Intersection”. In: *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part III*. Ed. by Yuval Ishai and Vincent Rijmen. Vol. 11478. Lecture Notes in Computer Science. Springer, 2019, pp. 154–185. DOI: 10.1007/978-3-030-17659-4_6. URL: https://doi.org/10.1007/978-3-030-17659-4_6.

参考文献 XLIII

[GS19] Satrajit Ghosh and Mark Simkin. “The Communication Complexity of Threshold Private Set Intersection”. In: *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II*. Ed. by Alexandra Boldyreva and Daniele Micciancio. Vol. 11693. Lecture Notes in Computer Science. Springer, 2019, pp. 3–29. DOI: 10.1007/978-3-030-26951-7_1. URL: https://doi.org/10.1007/978-3-030-26951-7_1.

[Gon81] Gaston H. Gonnet. “Expected Length of the Longest Probe Sequence in Hash Code Searching”. In: *J. ACM* 28.2 (1981), pp. 289–304. DOI: 10.1145/322248.322254. URL: https://doi.org/10.1145/322248.322254.

参考文献 XLIV

[Gor+22] Dov Gordon et al. *More Efficient (Reusable) Private Set Union*. Cryptology ePrint Archive, Paper 2022/713. https://eprint.iacr.org/2022/713. 2022. URL: https://eprint.iacr.org/2022/713.

[GHL22] S. Dov Gordon, Carmit Hazay, and Phi Hung Le. "Fully Secure PSI via MPC-in-the-Head". In: *Proc. Priv. Enhancing Technol.* 2022.3 (2022), pp. 291–313. DOI: 10.56553/popets-2022-0073. URL: https://doi.org/10.56553/popets-2022-0073.

参考文献 XLV

[HOS17] Per A. Hallgren, Claudio Orlandi, and Andrei Sabelfeld. “PrivatePool: Privacy-Preserving Ridesharing”. In: *30th IEEE Computer Security Foundations Symposium, CSF 2017, Santa Barbara, CA, USA, August 21-25, 2017*. IEEE Computer Society, 2017, pp. 276–291. DOI: 10.1109/CSF.2017.24. URL: https://doi.org/10.1109/CSF.2017.24.

[HMS22] Kyoohyung Han, Dukjae Moon, and Yongha Son. “Improved Circuit-based PSI via Equality Preserving Compression”. In: *SAC 2022*. Lecture Notes in Computer Science. 2022.

参考文献 XLVI

[HL08] Carmit Hazay and Yehuda Lindell. “Efficient Protocols for Set Intersection and Pattern Matching with Security Against Malicious and Covert Adversaries”. In: *Theory of Cryptography, Fifth Theory of Cryptography Conference, TCC 2008, New York, USA, March 19-21, 2008*. Ed. by Ran Canetti. Vol. 4948. Lecture Notes in Computer Science. Springer, 2008, pp. 155–175. DOI: 10.1007/978-3-540-78524-8_10. URL: https://doi.org/10.1007/978-3-540-78524-8_10.

参考文献 XLVII

[HN10] Carmit Hazay and Kobbi Nissim. “Efficient Set Operations in the Presence of Malicious Adversaries”. In: *Public Key Cryptography - PKC 2010, 13th International Conference on Practice and Theory in Public Key Cryptography, Paris, France, May 26-28, 2010. Proceedings*. Ed. by Phong Q. Nguyen and David Pointcheval. Vol. 6056. Lecture Notes in Computer Science. Springer, 2010, pp. 312–331. DOI: 10.1007/978-3-642-13013-7_19. URL: https://doi.org/10.1007/978-3-642-13013-7_19.

参考文献 XLVIII

[HV17] Carmit Hazay and Muthuramakrishnan Venkitasubramaniam. "Scalable Multi-party Private Set-Intersection". In: *Public-Key Cryptography - PKC 2017 - 20th IACR International Conference on Practice and Theory in Public-Key Cryptography, Amsterdam, The Netherlands, March 28-31, 2017, Proceedings, Part I*. Ed. by Serge Fehr. Vol. 10174. Lecture Notes in Computer Science. Springer, 2017, pp. 175–203. DOI: 10.1007/978-3-662-54365-8_8. URL: https://doi.org/10.1007/978-3-662-54365-8_8.

参考文献 XLIX

[Hon+11] Jeongdae Hong et al. *Constant-Round Privacy Preserving Multiset Union*. Cryptology ePrint Archive, Paper 2011/138. https://eprint.iacr.org/2011/138. 2011. URL: https://eprint.iacr.org/2011/138.

[HEK12] Yan Huang, David Evans, and Jonathan Katz. "Private Set Intersection: Are Garbled Circuits Better than Custom Protocols?" In: *19th Annual Network and Distributed System Security Symposium, NDSS 2012, San Diego, California, USA, February 5-8, 2012*. The Internet Society, 2012. URL: https://www.ndss-symposium.org/ndss2012/private-set-intersection-are-garbled-circuits-better-custom-protocols.

参考文献 L

[HFH99] Bernardo A. Huberman, Matthew K. Franklin, and Tad Hogg. "Enhancing privacy and trust in electronic communities". In: *Proceedings of the First ACM Conference on Electronic Commerce (EC-99), Denver, CO, USA, November 3-5, 1999*. Ed. by Stuart I. Feldman and Michael P. Wellman. ACM, 1999, pp. 78–86. DOI: 10.1145/336992.337012. URL: https://doi.org/10.1145/336992.337012.

参考文献 LI

[IOP18] Roi Inbar, Eran Omri, and Benny Pinkas. “Efficient Scalable Multiparty Private Set-Intersection via Garbled Bloom Filters”. In: *Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings*. Ed. by Dario Catalano and Roberto De Prisco. Vol. 11035. Lecture Notes in Computer Science. Springer, 2018, pp. 235–252. DOI: 10.1007/978-3-319-98113-0_13. URL: https://doi.org/10.1007/978-3-319-98113-0_13.

参考文献 LII

[Ion+20] Mihaela Ion et al. “On Deploying Secure Computing: Private Intersection-Sum-with-Cardinality”. In: *IEEE European Symposium on Security and Privacy, EuroS&P 2020, Genoa, Italy, September 7-11, 2020*. IEEE, 2020, pp. 370–389. DOI: 10.1109/EuroSP48549.2020.00031. URL: https://doi.org/10.1109/EuroSP48549.2020.00031.

[Ion+17] Mihaela Ion et al. *Private Intersection-Sum Protocol with Applications to Attributing Aggregate Ad Conversions*. Cryptology ePrint Archive, Paper 2017/738. https://eprint.iacr.org/2017/738. 2017. URL: https://eprint.iacr.org/2017/738.

参考文献 LIII

[JL09] Stanislaw Jarecki and Xiaomin Liu. “Efficient Oblivious Pseudorandom Function with Applications to Adaptive OT and Secure Computation of Set Intersection”. In: *Theory of Cryptography, 6th Theory of Cryptography Conference, TCC 2009, San Francisco, CA, USA, March 15-17, 2009. Proceedings*. Ed. by Omer Reingold. Vol. 5444. Lecture Notes in Computer Science. Springer, 2009, pp. 577–594. DOI: 10.1007/978-3-642-00457-5_34. URL: https://doi.org/10.1007/978-3-642-00457-5_34.

参考文献 LIV

[JL10] Stanislaw Jarecki and Xiaomin Liu. “Fast Secure Computation of Set Intersection”. In: *Security and Cryptography for Networks, 7th International Conference, SCN 2010, Amalfi, Italy, September 13-15, 2010. Proceedings*. Ed. by Juan A. Garay and Roberto De Prisco. Vol. 6280. Lecture Notes in Computer Science. Springer, 2010, pp. 418–435. DOI: 10.1007/978-3-642-15317-4_26. URL: https://doi.org/10.1007/978-3-642-15317-4_26.

参考文献 LV

[Jia+22a] Yanxue Jia et al. “Shuffle-based Private Set Union: Faster and More Secure”. In: *31st USENIX Security Symposium, USENIX Security 2022, Boston, MA, USA, August 10-12, 2022*. Ed. by Kevin R. B. Butler and Kurt Thomas. USENIX Association, 2022, pp. 2947–2964. URL: https://www.usenix.org/conference/usenixsecurity22/presentation/jia.

[Jia+22b] Yanxue Jia et al. “The Ideal Functionalities for Private Set Union, Revisited”. In: *IACR Cryptol. ePrint Arch.* (2022), p. 750. URL: https://eprint.iacr.org/2022/750.

参考文献 LVI

[Kal+19] Daniel Kales et al. "Mobile Private Contact Discovery at Scale". In: *28th USENIX Security Symposium, USENIX Security 2019, Santa Clara, CA, USA, August 14-16, 2019*. Ed. by Nadia Heninger and Patrick Traynor. USENIX Association, 2019, pp. 1447–1464. URL: https://www.usenix.org/conference/usenixsecurity19/presentation/kales.

参考文献 LVII

[Kam+14] Seny Kamara et al. “Scaling Private Set Intersection to Billion-Element Sets”. In: *Financial Cryptography and Data Security - 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers*. Ed. by Nicolas Christin and Reihaneh Safavi-Naini. Vol. 8437. Lecture Notes in Computer Science. Springer, 2014, pp. 195–215. DOI: 10.1007/978-3-662-45472-5_13. URL: https://doi.org/10.1007/978-3-662-45472-5_13.

参考文献 LVIII

[Ker12] Florian Kerschbaum. "Outsourced private set intersection using homomorphic encryption". In: *7th ACM Symposium on Information, Compuer and Communications Security, ASIACCS '12, Seoul, Korea, May 2-4, 2012*. Ed. by Heung Youl Youm and Yoojae Won. ACM, 2012, pp. 85–86. DOI: 10.1145/2414456.2414506. URL: https://doi.org/10.1145/2414456.2414506.

参考文献 LIX

[KBM23] Florian Kerschbaum, Erik-Oliver Blass, and Rasoul Akhavan Mahdavi. “Faster Secure Comparisons with Offline Phase for Efficient Private Set Intersection”. In: *30th Annual Network and Distributed System Security Symposium, NDSS 2023, San Diego, California, USA, February 27 - March 3, 2023*. The Internet Society, 2023. URL: https://www.ndss-symposium.org/ndss-paper/faster-secure-comparisons-with-offline-phase-for-efficient-private-set-intersection/.

[Kis+17] Ágnes Kiss et al. “Private Set Intersection for Unequal Set Sizes with Mobile Applications”. In: *Proc. Priv. Enhancing Technol.* 2017.4 (2017), pp. 177–197. DOI: 10.1515/popets-2017-0044. URL: https://doi.org/10.1515/popets-2017-0044.

参考文献 LX

[KS05] Lea Kissner and Dawn Xiaodong Song. "Privacy-Preserving Set Operations". In: *Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings*. 2005, pp. 241–257. DOI: 10.1007/11535218_15. URL: https://doi.org/10.1007/11535218_15.

参考文献 LXI

[KK13] Vladimir Kolesnikov and Ranjit Kumaresan. “Improved OT Extension for Transferring Short Secrets”. In: *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part II*. Ed. by Ran Canetti and Juan A. Garay. Vol. 8043. Lecture Notes in Computer Science. Springer, 2013, pp. 54–70. DOI: 10.1007/978-3-642-40084-1_4. URL: https://doi.org/10.1007/978-3-642-40084-1_4.

参考文献 LXII

[Kol+16] Vladimir Kolesnikov et al. “Efficient Batched Oblivious PRF with Applications to Private Set Intersection”. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*. Ed. by Edgar R. Weippl et al. ACM, 2016, pp. 818–829. DOI: 10.1145/2976749.2978381. URL: https://doi.org/10.1145/2976749.2978381.

参考文献 LXIII

[Kol+17] Vladimir Kolesnikov et al. "Practical Multi-party Private Set Intersection from Symmetric-Key Techniques". In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017*. Ed. by Bhavani M. Thuraisingham et al. ACM, 2017, pp. 1257–1272. DOI: 10.1145/3133956.3134065. URL: https://doi.org/10.1145/3133956.3134065.

参考文献 LXIV

[Kol+19] Vladimir Kolesnikov et al. “Scalable Private Set Union from Symmetric-Key Techniques”. In: *Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8-12, 2019, Proceedings, Part II*. 2019, pp. 636–666. DOI: 10.1007/978-3-030-34621-8_23. URL: https://doi.org/10.1007/978-3-030-34621-8_23.

参考文献 LXV

[LRG19] Phi Hung Le, Samuel Ranellucci, and S. Dov Gordon. “Two-party Private Set Intersection with an Untrusted Third Party”. In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS 2019, London, UK, November 11-15, 2019*. Ed. by Lorenzo Cavallaro et al. ACM, 2019, pp. 2403–2420. DOI: 10.1145/3319535.3345661. URL: https://doi.org/10.1145/3319535.3345661.

参考文献 LXVI

[Li+19] Lucy Li et al. “Protocols for Checking Compromised Credentials”. In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS 2019, London, UK, November 11-15, 2019*. Ed. by Lorenzo Cavallaro et al. ACM, 2019, pp. 1387–1403. DOI: 10.1145/3319535.3354229. URL: https://doi.org/10.1145/3319535.3354229.

[Mea86] Catherine A. Meadows. “A More Efficient Cryptographic Matchmaking Protocol for Use in the Absence of a Continuously Available Third Party”. In: *Proceedings of the 1986 IEEE Symposium on Security and Privacy, Oakland, California, USA, April 7-9, 1986*. IEEE Computer Society, 1986, pp. 134–137. DOI: 10.1109/SP.1986.10022. URL: https://doi.org/10.1109/SP.1986.10022.

参考文献 LXVII

[Mia+20] Peihan Miao et al. “Two-Sided Malicious Security for Private Intersection-Sum with Cardinality”. In: *Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part III*. Ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12172. Lecture Notes in Computer Science. Springer, 2020, pp. 3–33. DOI: 10.1007/978-3-030-56877-1_1. URL: https://doi.org/10.1007/978-3-030-56877-1_1.

参考文献 LXVIII

[MRR20] Payman Mohassel, Peter Rindal, and Mike Rosulek. “Fast Database Joins and PSI for Secret Shared Data”. In: *CCS ’20: 2020 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, USA, November 9-13, 2020*. Ed. by Jay Ligatti et al. ACM, 2020, pp. 1271–1287. DOI: 10.1145/3372297.3423358. URL: https://doi.org/10.1145/3372297.3423358.

参考文献 LXIX

[MS13] Payman Mohassel and Seyed Saeed Sadeghian. “How to Hide Circuits in MPC an Efficient Framework for Private Function Evaluation”. In: *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*. Ed. by Thomas Johansson and Phong Q. Nguyen. Vol. 7881. Lecture Notes in Computer Science. Springer, 2013, pp. 557–574. DOI: 10.1007/978-3-642-38348-9_33. URL: https://doi.org/10.1007/978-3-642-38348-9_33.

参考文献 LXX

[NR04] Moni Naor and Omer Reingold. “Number-theoretic constructions of efficient pseudo-random functions”. In: *J. ACM* 51.2 (2004), pp. 231–262. DOI: 10.1145/972639.972643. URL: https://doi.org/10.1145/972639.972643.

参考文献 LXXI

[Nar+09] G. Sathya Narayanan et al. “Multi Party Distributed Private Matching, Set Disjointness and Cardinality of Set Intersection with Information Theoretic Security”. In: *Cryptology and Network Security, 8th International Conference, CANS 2009, Kanazawa, Japan, December 12-14, 2009. Proceedings*. Ed. by Juan A. Garay, Atsuko Miyaji, and Akira Otsuka. Vol. 5888. Lecture Notes in Computer Science. Springer, 2009, pp. 21–40. DOI: 10.1007/978-3-642-10433-6_2. URL: https://doi.org/10.1007/978-3-642-10433-6_2.

参考文献 LXXII

[NTY21] Ofri Nevo, Ni Trieu, and Avishay Yanai. “Simple, Fast Malicious Multiparty Private Set Intersection”. In: *CCS ’21: 2021 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, Republic of Korea, November 15 - 19, 2021*. Ed. by Yongdae Kim et al. ACM, 2021, pp. 1151–1165. DOI: 10.1145/3460120.3484772. URL: https://doi.org/10.1145/3460120.3484772.

参考文献 LXXIII

[OOS17] Michele Orrù, Emmanuela Orsini, and Peter Scholl. "Actively Secure 1-out-of-N OT Extension with Application to Private Set Intersection". In: *Topics in Cryptology - CT-RSA 2017 - The Cryptographers' Track at the RSA Conference 2017, San Francisco, CA, USA, February 14-17, 2017, Proceedings*. Ed. by Helena Handschuh. Vol. 10159. Lecture Notes in Computer Science. Springer, 2017, pp. 381–396. DOI: 10.1007/978-3-319-52153-4_22. URL: https://doi.org/10.1007/978-3-319-52153-4_22.

[PR04] Rasmus Pagh and Flemming Friche Rodler. "Cuckoo hashing". In: *J. Algorithms* 51.2 (2004), pp. 122–144. DOI: 10.1016/j.jalgor.2003.12.002. URL: https://doi.org/10.1016/j.jalgor.2003.12.002.

参考文献 LXXIV

[PSZ14] Benny Pinkas, Thomas Schneider, and Michael Zohner. "Faster Private Set Intersection Based on OT Extension". In: *Proceedings of the 23rd USENIX Security Symposium, San Diego, CA, USA, August 20-22, 2014*. Ed. by Kevin Fu and Jaeyeon Jung. USENIX Association, 2014, pp. 797–812. URL: https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/pinkas.

[PSZ18] Benny Pinkas, Thomas Schneider, and Michael Zohner. "Scalable Private Set Intersection Based on OT Extension". In: *ACM Trans. Priv. Secur.* 21.2 (2018), 7:1–7:35. DOI: 10.1145/3154794. URL: https://doi.org/10.1145/3154794.

参考文献 LXXV

[Pin+18] Benny Pinkas et al. “Efficient Circuit-Based PSI via Cuckoo Hashing”. In: *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part III*. Ed. by Jesper Buus Nielsen and Vincent Rijmen. Vol. 10822. Lecture Notes in Computer Science. Springer, 2018, pp. 125–157. DOI: 10.1007/978-3-319-78372-7_5. URL: https://doi.org/10.1007/978-3-319-78372-7_5.

参考文献 LXXVI

[Pin+19a] Benny Pinkas et al. “Efficient Circuit-Based PSI with Linear Communication”. In: *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part III*. Ed. by Yuval Ishai and Vincent Rijmen. Vol. 11478. Lecture Notes in Computer Science. Springer, 2019, pp. 122–153. DOI: 10.1007/978-3-030-17659-4_5. URL: https://doi.org/10.1007/978-3-030-17659-4_5.

参考文献 LXXVII

[Pin+15] Benny Pinkas et al. “Phasing: Private Set Intersection Using Permutation-based Hashing”. In: *24th USENIX Security Symposium, USENIX Security 15, Washington, D.C., USA, August 12-14, 2015*. Ed. by Jaeyeon Jung and Thorsten Holz. USENIX Association, 2015, pp. 515–530. URL: https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/pinkas.

参考文献 LXXVIII

[Pin+20] Benny Pinkas et al. “PSI from PaXoS: Fast, Malicious Private Set Intersection”. In: *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part II*. 2020, pp. 739–767. DOI: 10.1007/978-3-030-45724-2_25. URL: https://doi.org/10.1007/978-3-030-45724-2_25.

参考文献 LXXIX

[Pin+19b] Benny Pinkas et al. “SpOT-Light: Lightweight Private Set Intersection from Sparse OT Extension”. In: *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part III*. Ed. by Alexandra Boldyreva and Daniele Micciancio. Vol. 11694. Lecture Notes in Computer Science. Springer, 2019, pp. 401–431. DOI: `10.1007/978-3-030-26954-8\_13`. URL: `https://doi.org/10.1007/978-3-030-26954-8\_13`.

参考文献 LXXX

[Qiu+22] Zhi Qiu et al. “Maliciously Secure Multi-party PSI with Lower Bandwidth and Faster Computation”. In: *Information and Communications Security - 24th International Conference, ICICS 2022, Canterbury, UK, September 5-8, 2022, Proceedings*. Ed. by Cristina Alcaraz et al. Vol. 13407. Lecture Notes in Computer Science. Springer, 2022, pp. 69–88. DOI: 10.1007/978-3-031-15777-6_5. URL: https://doi.org/10.1007/978-3-031-15777-6_5.

参考文献 LXXXI

[RR22] Srinivasan Raghuraman and Peter Rindal. “Blazing Fast PSI from Improved OKVS and Subfield VOLE”. In: *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, CCS 2022, Los Angeles, CA, USA, November 7-11, 2022*. Ed. by Heng Yin et al. ACM, 2022, pp. 2505–2517. DOI: 10.1145/3548606.3560658. URL: https://doi.org/10.1145/3548606.3560658.

参考文献 LXXXII

[RA18] Amanda Cristina Davi Resende and Diego F. Aranha. “Faster Unbalanced Private Set Intersection”. In: *Financial Cryptography and Data Security - 22nd International Conference, FC 2018, Nieuwpoort, Curaçao, February 26 - March 2, 2018, Revised Selected Papers*. Ed. by Sarah Meiklejohn and Kazue Sako. Vol. 10957. Lecture Notes in Computer Science. Springer, 2018, pp. 203–221. DOI: 10.1007/978-3-662-58387-6_11. URL: https://doi.org/10.1007/978-3-662-58387-6_11.

参考文献 LXXXIII

[RR17a] Peter Rindal and Mike Rosulek. “Improved Private Set Intersection Against Malicious Adversaries”. In: *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part I*. Ed. by Jean-Sébastien Coron and Jesper Buus Nielsen. Vol. 10210. Lecture Notes in Computer Science. 2017, pp. 235–259. DOI: 10.1007/978-3-319-56620-7_9. URL: https://doi.org/10.1007/978-3-319-56620-7_9.

参考文献 LXXXIV

[RR17b] Peter Rindal and Mike Rosulek. “Malicious-Secure Private Set Intersection via Dual Execution”. In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017*. Ed. by Bhavani M. Thuraisingham et al. ACM, 2017, pp. 1229–1242. DOI: 10.1145/3133956.3134044. URL: https://doi.org/10.1145/3133956.3134044.

参考文献 LXXXV

[RS21] Peter Rindal and Phillipp Schoppmann. “VOLE-PSI: Fast OPRF and Circuit-PSI from Vector-OLE”. In: *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part II*. Ed. by Anne Canteaut and François-Xavier Standaert. Vol. 12697. Lecture Notes in Computer Science. Springer, 2021, pp. 901–930. DOI: 10.1007/978-3-030-77886-6_31. URL: https://doi.org/10.1007/978-3-030-77886-6_31.

参考文献 LXXXVI

[RT21] Mike Rosulek and Ni Trieu. “Compact and Malicious Private Set Intersection for Small Sets”. In: *CCS ’21: 2021 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, Republic of Korea, November 15 - 19, 2021*. Ed. by Yongdae Kim et al. ACM, 2021, pp. 1166–1181. DOI: 10.1145/3460120.3484778. URL: https://doi.org/10.1145/3460120.3484778.

参考文献 LXXXVII

[SCK12] Jae Hong Seo, Jung Hee Cheon, and Jonathan Katz. “Constant-Round Multi-party Private Set Union Using Reversed Laurent Series”. In: *Public Key Cryptography - PKC 2012 - 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, May 21-23, 2012. Proceedings*. Ed. by Marc Fischlin, Johannes Buchmann, and Mark Manulis. Vol. 7293. Lecture Notes in Computer Science. Springer, 2012, pp. 398–412. DOI: 10.1007/978-3-642-30057-8_24. URL: https://doi.org/10.1007/978-3-642-30057-8_24.

参考文献 LXXXVIII

[TYG22] Ni Trieu, Avishay Yanai, and Jiahui Gao. *Multiparty Private Set Intersection Cardinality and Its Applications*. Cryptology ePrint Archive, Paper 2022/735. `https://eprint.iacr.org/2022/735`. 2022. URL: `https://eprint.iacr.org/2022/735`.

[Tu+22] Binbin Tu et al. *Fast Unbalanced Private Set Union from Fully Homomorphic Encryption*. Cryptology ePrint Archive, Paper 2022/653. `https://eprint.iacr.org/2022/653`. 2022. URL: `https://eprint.iacr.org/2022/653`.

参考文献 LXXXIX

[VC05] Jaideep Vaidya and Chris Clifton. "Secure set intersection cardinality with application to association rule mining". In: *J. Comput. Secur.* 13.4 (2005), pp. 593–622. DOI: 10.3233/jcs-2005-13401. URL: https://doi.org/10.3233/jcs-2005-13401.

[Zha+23] Cong Zhang et al. "Linear Private Set Union from Multi-Query Reverse Private Membership Test". In: *32st USENIX Security Symposium, USENIX Security 2023, Boston, MA, USA, August 10-12, 2023*. USENIX Association, 2023.

参考文献 XC

[Zha+19] En Zhang et al. “Efficient Multi-Party Private Set Intersection Against Malicious Adversaries”. In: *Proceedings of the 2019 ACM SIGSAC Conference on Cloud Computing Security Workshop, CCSW@CCS 2019, London, UK, November 11, 2019*. Ed. by Radu Sion and Charalampos Papamanthou. ACM, 2019, pp. 93–104. DOI: 10.1145/3338466.3358927. URL: https://doi.org/10.1145/3338466.3358927.

参考文献 XCI

[ZC18] Yongjun Zhao and Sherman S. M. Chow. “Can You Find The One for Me?” In: *Proceedings of the 2018 Workshop on Privacy in the Electronic Society, WPES@CCS 2018, Toronto, ON, Canada, October 15-19, 2018*. Ed. by David Lie, Mohammad Mannan, and Aaron Johnson. ACM, 2018, pp. 54–65. DOI: 10.1145/3267323.3268965. URL: https://doi.org/10.1145/3267323.3268965.

Thanks!