基础协议

OT/OLE

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

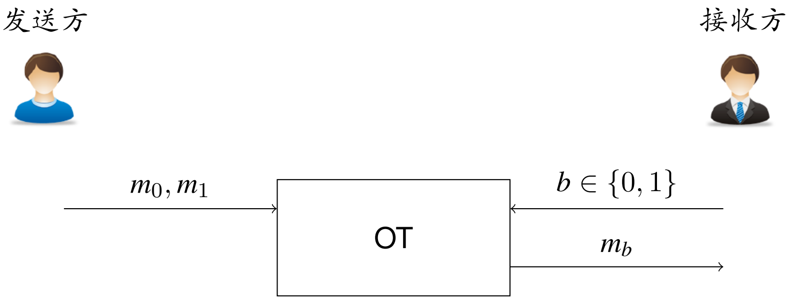
2023 年 1 月 13 日

OT/OLE 定义

不经意传输 (Oblivious Transfer, OT)[Rab05] 是一个重要的两方协议，在各种 MPC 协议中均有应用。不经意线性函数求值 (Oblivious Linear-function Evaluation,OLE) 作为 OT 在算数域上的推广，同样有着诸多应用：

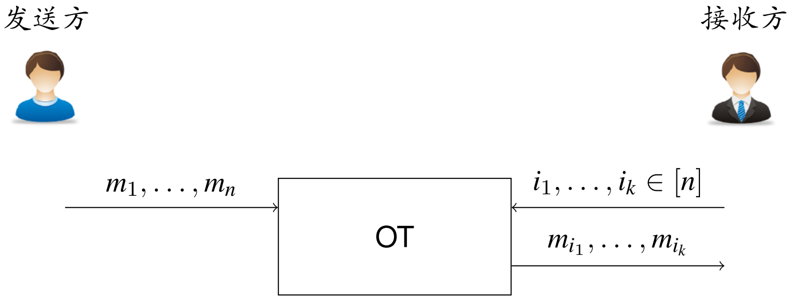
- Yao's GC
- GMW
- IT-MAC
- PSO
- ...

OT 定义

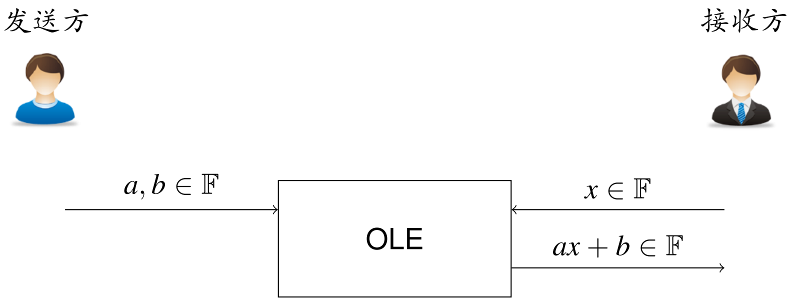


$$m_b = m_0 \oplus b(m_1 \oplus m_0)$$

OT 定义



OLE 定义



OT 构造

OT 可由诸多假设构造:

- DDH: [PVW08; MR19; MRR20; CSW20; MRR21]
- CDH: [NP01; CO15; Döt+20; MRR21]
- LWE: [PVW08; MR19; Bra+19; DD20; Qua20]
- LPN: [Döt+20]
- CSIDH: [LGSG21]

OT from DDH

$S(m_0, m_1)$ $R(b)$

$(\mathbb{G}, q, g) \leftarrow \mathcal{G}(1^\kappa), d \leftarrow \mathbb{G}$

$\xrightarrow{(\mathbb{G}, q, g, d)}$

$k \leftarrow \mathbb{Z}_q$

$h_b := g^k, h_{1-b} := d/g^k$

$\xleftarrow{h_0}$

$h_1 := d/h_0, r_0, r_1 \leftarrow \mathbb{Z}_q$

$c_0 := (g^{r_0}, h_0^{r_0} m_0), c_1 := (g^{r_1}, h_1^{r_1} m_1)$

$\xrightarrow{(c_0 = (c_0^1, c_0^2), c_1 = (c_1^1, c_1^2))}$

$m_b := c_b^2/(c_b^1)^k$

OT from Type-I PKE

$S(a, b)$ $\qquad\qquad$ $R(x)$

$$(pk_b, sk_b) \leftarrow \mathrm{KeyGen}(1^\kappa)$$
$$pk_{1-b} \leftarrow \mathrm{SamplePK}(1^\kappa)$$

$$\xleftarrow{\quad (pk_0, pk_1) \quad}$$

$$c_i := \mathrm{Enc}(pk_i, m_i), i \in \{0, 1\}$$

$$\xrightarrow{\quad (c_0, c_1) \quad}$$

$$m_b := \mathrm{Dec}(sk_b, c_b)$$

OT from Type-II PKE

$$S(m_0, m_1) \qquad\qquad R(b)$$

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

$$\xrightarrow{\quad pk \quad}$$

$$r \leftarrow \mathcal{M}$$

$$c_b := \mathrm{Enc}(pk, r), c_{1-b} \leftarrow \mathrm{SampleCt}(1^\kappa)$$

$$\xleftarrow{\quad (c_0, c_1) \quad}$$

$$r_i := \mathrm{Dec}(sk, c_i)$$

$$y_i := m_i \oplus r_i$$

$$\xrightarrow{\quad (y_0, y_1) \quad}$$

$$m_b := y_b \oplus r$$

OLE from AHE

$S(a, b)$ $R(x)$

$(pk, sk) \leftarrow \mathrm{KeyGen}(1^\kappa)$
$c := \mathrm{Enc}(pk, x)$

$$\xleftarrow{\quad pk, c \quad}$$

$\mathrm{Enc}(pk, y) := a\mathrm{Enc}(pk, x) + \mathrm{Enc}(pk, b)$

$$\xrightarrow{\quad \mathrm{Enc}(pk, y) \quad}$$

$y := \mathrm{Dec}(sk, \mathrm{Enc}(pk, y))$

OLE from OT

$S(a, b)$ $\qquad$ $R(x)$

$b := b_0 + \ldots, +b_{k-1}$ $\qquad$ $x := (x_0, \ldots, x_{k-1}) \in \{0,1\}^k$

$i \in [0, k-1]:$

$(b_i, 2^i a + b_i) \rightarrow$ OT $\leftarrow x_i$

OT $\rightarrow 2^i a x_i + b_i$

$y := \sum_{i \in [0,k-1]} 2^i a x_i + b_i$

几种 OT 变体

- 标准 OT：$\mathcal{F}_{OT}(\{m_{i,0},m_{i,1}\}_{i\in[n]},b\in\{0,1\}^n)\to(\perp,\{m_{i,b_i}\}_{i\in[n]})$
- 随机 OT：$\mathcal{F}_{ROT}(\perp,\perp)\to(\{m_{i,0},m_{i,1}\}_{i\in[n]},\{b_i,m_{i,b_i}\}_{i\in[n]})$
- 相关 OT：$\mathcal{F}_{COT}(\perp,\perp)\to((\{m_{i,0}\}_{i\in[n]},\Delta),\{b_i,m_{i,0}\oplus b_i\Delta\}_{i\in[n]})$

OT 预处理：COT$\Longrightarrow$ROT$\Longrightarrow$OT

OT 预处理

COT$\Longrightarrow$ROT: 令 $H:\{0,1\}^\kappa \to \{0,1\}^\kappa$ 是相关鲁棒哈希函数 (Correlated Robust Hash Function, CRHF).

S R

$\{m'_{i,0}\}_{i\in[n]}, \Delta$ COT $\{b_i, m'_{i,0} \oplus b_i\Delta\}$

$m_{i,0} := H(m'_{i,0}), m_{i,1} := H(m'_{i,0} \oplus \Delta)$ $m_{i,b_i} := H(m'_{i,0} \oplus b_i\Delta)$

相关鲁棒哈希函数

定义 (Correlated Robust Hash Function, CRHF)

令 $H:\{0,1\}^\kappa \to \{0,1\}^\kappa$ 是一个函数，令 $\mathcal{R}$ 是一个 $\{0,1\}^\kappa$ 上的分布，$R \in \{0,1\}^\kappa$，定义 $\mathcal{O}_R^{cr}(x) := H(x \oplus R)$。对一个区分器 D，定义：

$$\mathrm{Adv}_{H,\mathcal{R}}^{cr} := |Pr_{R\leftarrow\mathcal{R}}[D^{\mathcal{O}_R^{cr}(\cdot)} = 1] - Pr_{f\leftarrow F_k}[D^{f(\cdot)} = 1]|$$

称 H 是 (t,q,ρ,ϵ)-相关鲁棒哈希函数，如果对所有运行时间最多为 t，询问 $\mathcal{O}_R^{cr}(\cdot)$ 次数最多为 q 的 D，所有具有最小熵 ρ 的 $\mathcal{R}$，有 $\mathrm{Adv}_{H,\mathcal{R}}^{cr}(D) \le \epsilon$.

OT 预处理

ROT$\Longrightarrow$OT:

$S(\{m_{i,0}, m_{i,1}\}_{i\in[n]})$ $\qquad\qquad$ $R(b)$

$$\{m'_{i,0}, m'_{i,1}\}_{i\in[n]} \leftrightarrows \boxed{\text{ROT}} \leftrightarrows \{b'_i, m'_{i,b'_i}\}$$

$$\xleftarrow{c := b \oplus b'}$$

$$x_{i,0} := m'_{i,c_i} \oplus m_{i,0}$$
$$x_{i,1} := m'_{i,c_i\oplus 1} \oplus m_{i,1}$$

$$\xrightarrow{\{x_{i,0}, x_{i,1}\}_{i\in[n]}}$$

$$m_{i,b_i} := x_{i,b_i} \oplus m'_{i,b'_i}$$

1. OT/OLE 定义
2. OT/OLE 基本构造
3. OT 预处理
4. **OT 扩展**
   - IKNP 框架
   - PCG 框架
5. 参考文献

OT 扩展主要方法

由于使用公钥操作生成 OT 实例开销很大，Beaver[Bea96] 首先提出 OT 扩展 (OT extension, OTe) 的概念，OTe 是指用少量 OT 实例加上一些对称操作生成大量 OT 实例的方法。OTe 极大地缩减了生成 OT 所需的开销，使得很多 MPC 协议效率得到了提升。目前 OTe 的主要方法：

- Beaver 的 GC 方法 [Bea96].
  - 需要非黑盒求值 PRG 电路
  - 理论构造
- IKNP 框架 [Ish+03; Ash+13; Ash+15; KOS15; OOS17; Roy22].
  - 计算开销低
  - 每个 COT 实例通信 κ 比特
- Silent OT/PCG 框架 [Boy+19a; Boy+19b; Sch+19; Yan+20; Boy+20; Wen+21; CRR21; Guo+22]
  - 计算开销高.
  - 通信亚线性：生成 n 个 COT 实例只需 $O(\log n)$ 通信.

IKNP 框架

$S(\{m_{i,0}, m_{i,1}\}_{i\in[n]})$

$R(r \in \{0,1\}^n)$

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

$T \leftarrow \{0,1\}^{n\times\kappa}, T = [T_1|\ldots|T_\kappa]$

$i \in [\kappa]$:

$(T_i, T_i \oplus r)$

s_i

OT

$Q_i := T_i \oplus s_i r$

$Q := [Q_1|\ldots|Q_\kappa] = [q_1|\ldots|q_n]^T, q_j = t_j \oplus r_j s$

$y_{j,0} := m_{j,0} \oplus H(q_j)$

$y_{j,1} := m_{j,1} \oplus H(q_j \oplus s)$

$\{y_{j,0}, y_{j,1}\}_{j\in[n]}$

$m_{j,r_j} := y_{j,r_j} \oplus H(t_j)$

[Ash+13] 改进

$S(\{m_{i,0}, m_{i,1}\}_{i\in[n]})$

$R(r \in \{0,1\}^n)$

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

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

$i \in [\kappa]$:

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

$\xleftarrow{k_i^{s_i}}$

$$T_i := G(k_i^0), T := [T_1|\dots|T_\kappa] \in \{0,1\}^{n\times\kappa}$$

$$u_i := T_i \oplus G(k_i^1) \oplus r, i \in [\kappa]$$

$\xleftarrow{\{u_i\}_{i\in[\kappa]}}$

$$Q_i := (s_i \cdot u_i) \oplus G(k_i^{s_i}) = s_i r \oplus T_i, i \in [\kappa]$$

$$Q := [Q_1|\dots|Q_\kappa] = [q_1|\dots|q_n]^T$$

$\dots$

1. OT/OLE 定义
2. OT/OLE 基本构造
3. OT 预处理
4. OT 扩展
   - IKNP 框架
   - PCG 框架
5. 参考文献

PCG 框架

定义 ([Boy+19a], 相关生成器,Correlation Generator)

一个 PPT 算法 $\mathcal{C}$ 称为相关生成器，如果 $\mathcal{C}$ 输入安全参数 1^κ，输出一对 $\{0,1\}^n \times \{0,1\}^n$ 上的元素，其中 $n \in \mathrm{poly}(\kappa)$.

定义 (可逆采样相关生成器,Reverse-sampleable Correlation Generator)

令 $\mathcal{C}$ 是相关生成器，我们称 $\mathcal{C}$ 是可逆采样的，如果存在 PPT 算法 $\mathrm{RSample}$，对 $\sigma \in \{0,1\}$，有如下分布计算不可区分：

$$\{(R'_0, R'_1) | (R_0, R_1) \leftarrow \mathcal{C}(1^\kappa), R_\sigma := R'_\sigma, R'_{1-\sigma} := \mathrm{RSample}(\sigma, R_\sigma)\} \approx \{(R_0, R_1) | (R_0, R_1) \leftarrow \mathcal{C}(1^\kappa)\}$$

PCG 框架

伪随机相关生成器 (Pseudorandom Correlation Generator,PCG)[Boy+19a] 指的是两个算法 $(\mathrm{Gen}, \mathrm{Expand})$：

- $\mathrm{Gen}(1^\kappa)$：输入安全参数 1^κ，输出一对种子 (k_0, k_1).
- $\mathrm{Expand}(\sigma, k_\sigma)$：输入一个比特 $\sigma \in \{0,1\}$ 和一个种子 k_σ，输出比特串 $R_\sigma \in \{0,1\}^n$.

正确性. 如下分布计算不可区分：

$$\{(R_0, R_1) | (k_0, k_1) \leftarrow \mathrm{Gen}(1^\kappa), R_\sigma := \mathrm{Expand}(\sigma, k_\sigma), \sigma \in \{0,1\}\} \approx \{(R_0, R_1) | (R_0, R_1) \leftarrow \mathcal{C}(1^\kappa)\}$$

安全性. 对 $\sigma \in \{0,1\}$，如下分布计算不可区分：

$$\{(k_{1-\sigma}, R_\sigma) | (k_0, k_1) \leftarrow \mathrm{Gen}(1^\kappa), R_\sigma := \mathrm{Expand}(\sigma, k_\sigma)\} \approx \{(k_{1-\sigma}, R_\sigma) | (k_0, k_1) \leftarrow \mathrm{Gen}(1^\kappa), R_{1-\sigma} := \mathrm{Expand}(1-\sigma, k_{1-\sigma}), R_\sigma \leftarrow \mathrm{RSample}(1-\sigma, R_{1-\sigma})\}$$

PCG 框架 OTe

使用 PCG 框架生成 COT:

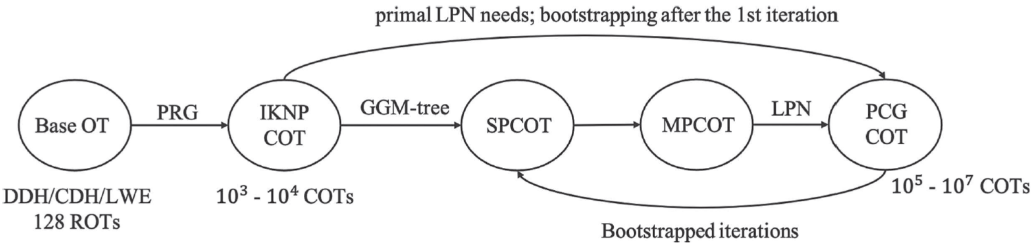
- $R_0 = (\{m_{i,0}\}_{i\in[n]}, \Delta), R_1 = (b, \{m_{i,0} \oplus b_i\Delta\}_{i\in[n]})$.
- 双方执行协议，该协议计算 Gen 算法，将 k_0 发给 P_0，将 k_1 发给 P_1.
- 双方根据协议的输出本地计算 $R_\sigma \leftarrow \mathrm{Expand}(\sigma, k_\sigma)$.

PCG 框架 OTe 路线

涉及到以下功能:

- COT: $\mathcal{F}_{COT}(\Delta \in \mathbb{F}_{2^\kappa}, \perp) \to (\vec{v} \in \mathbb{F}_{2^\kappa}^n, (\vec{u} \in \mathbb{F}_2^n, \vec{w} \in \mathbb{F}_{2^\kappa}^n)).\vec{w} = \vec{v} + \vec{u}\Delta$.
- 单点 COT(Single-Point COT, SPCOT): $\mathcal{F}_{SPCOT}(\Delta \in \mathbb{F}_{2^\kappa}, \alpha \in [n]) \to (\vec{v} \in \mathbb{F}_{2^\kappa}^n, (\vec{u} \in \mathbb{F}_2^n, \vec{w} \in \mathbb{F}_{2^\kappa}^n)), \vec{u} = \mathcal{I}(n, \alpha)$
- 多点 COT(Multi-Point COT, MPCOT): $\mathcal{F}_{MPCOT}(\Delta \in \mathbb{F}_{2^\kappa}, Q \subset [n]) \to (\vec{v} \in \mathbb{F}_{2^\kappa}^n, (\vec{u} \in \mathbb{F}_2^n, \vec{w} \in \mathbb{F}_{2^\kappa}^n)), \vec{u} = \mathcal{I}(n, Q), Q = \{\alpha_0, \ldots, \alpha_{t-1}\}$

PCG 框架 OTe 路线


primal LPN needs; bootstrapping after the 1st iteration
Base OT
PRG
IKNP COT
GGM-tree
SPCOT
MPCOT
LPN
PCG COT
DDH/CDH/LWE
128 ROTs
10^3 - 10^4 COTs
10^5 - 10^7 COTs
Bootstrapped iterations

SPCOT

$$G:\{0,1\}^{\kappa}\to\{0,1\}^{2\kappa}, h=\log n.$$

$S(\Delta)$ | $R(\alpha)$

$s_0^0 \leftarrow \{0,1\}^{\kappa}, (s_{2j}^i, s_{2j+1}^i) \leftarrow G(s_j^{i-1}), i\in[h], j\in[2^{i-1}]$

$K_0^i := \bigoplus_{j\in[2^{i-1}]} s_{2j}^i, K_1^i := \bigoplus_{j\in[2^{i-1}]} s_{2j+1}^i, i\in[h]$

$\vec{u} := \mathcal{I}(n,\alpha)$

$\alpha = (\alpha_1,\ldots,\alpha_h)\in\{0,1\}^h$

$i\in[h]:$

$(K_0^i, K_1^i) \rightarrow$ OT $\leftarrow \bar{\alpha}_i$

OT $\rightarrow K_{\bar{\alpha}_i}^i$

$\vec{v} := (s_0^h,\ldots,s_{n-1}^h)\in\mathbb{F}_{2^\kappa}^n$

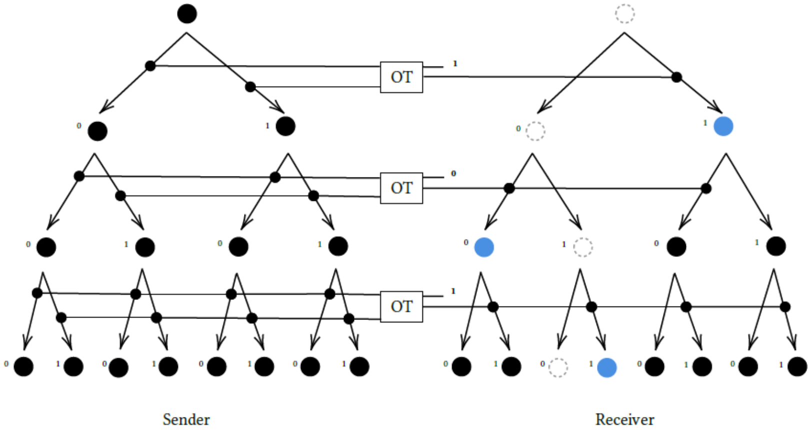
$c := \Delta + \sum_{i\in[n]} \vec{v}[i]$

计算 $\vec{w}[i], i\in[n]\setminus\{\alpha\}$

$\xrightarrow{c}$

$\vec{w}[\alpha] := c + \sum_{i\in[n]\setminus\{\alpha\}} \vec{w}[i]$

SPCOT



MPCOT-uniform noise

$S(\Delta)$

$\mathcal{B} \leftarrow \mathit{SimpleH}^m_{h_1,h_2,h_3}([n])$

$R(Q = \{\alpha_0, \ldots, \alpha_{t-1}\})$

$T \leftarrow \mathit{CuckooH}^m_{h_1,h_2,h_3}(Q), \mathcal{B} \leftarrow \mathit{SimpleH}^m_{h_1,h_2,h_3}([n])$

$\mathrm{pos}_j : \mathcal{B}_j \to [|\mathcal{B}_j|]$

$$p_j = \begin{cases} |\mathcal{B}_j| + 1 & T[j] = \perp; \\ \mathrm{pos}_j(T[j]) & \text{else} \end{cases}$$

$j \in [m]:$

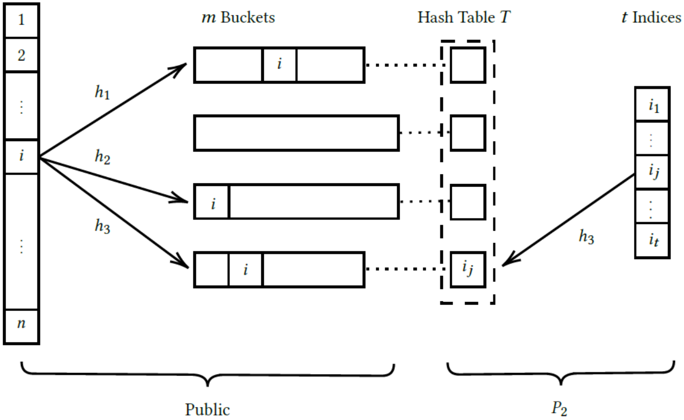
$x \in [n]:$

$\vec{v}[x] := \sum_{i\in[3]} \tilde{\vec{v}}_{h_i(x)}[\mathrm{pos}_{h_i(x)}(x)] \in \mathbb{F}_{2^\kappa}$

$x \in [n]:$

$\vec{w}[x] := \sum_{i\in[3]} \tilde{\vec{w}}_{h_i(x)}[\mathrm{pos}_{h_i(x)}(x)] \in \mathbb{F}_{2^\kappa}$

MPCOT- uniform noise



MPCOT-regular noise

假设 Q 的 t 个位置均匀分布在每个 n/t 长的块，即 $\alpha_i \in [in/t, (i+1)n/t]$.

$S(\Delta)$

$R(Q = \{\alpha_0, \ldots, \alpha_{t-1}\})$

$j \in [0, t-1]:$

Δ →

SPCOT

← α_j

← $\vec{v}_j \in \mathbb{F}_{2^\kappa}^{n/t}$

$\vec{w}_j \in \mathbb{F}_{2^\kappa}^{n/t}$ →

$\vec{v} := (\vec{v}_0, \ldots, \vec{v}_{t-1}) \in \mathbb{F}_{2^\kappa}^n$

$\vec{w} := (\vec{w}_0, \ldots, \vec{w}_{t-1}) \in \mathbb{F}_{2^\kappa}^n$

$\vec{u} := \mathcal{I}(n, Q) \in \mathbb{F}_2^n$

Learning Parity with Noise

定义 (Primal LPN)

令 $\mathcal{D}(\mathcal{R}) = \{\mathcal{D}_{k,n}\}$ 表示环 $\mathcal{R}$ 上的一族分布，使得对任意 $k, n \in \mathbb{N}$，$\mathrm{Im}(\mathcal{D}_{k,n}(\mathcal{R})) \subset \mathcal{R}^n$。令 C 是一个概率编码生成算法，使得 $C(k, n, \mathcal{R})$ 输出一个矩阵 $A \in \mathcal{R}^{k\times n}$。对于维度 $k = k(\kappa)$，采样数 $n = n(\kappa)$，环 $\mathcal{R} = \mathcal{R}(\kappa)$，$(\mathcal{D}, C, \mathcal{R})$-$LPN(k, n)$ 假设是说：

$$\{(A, b)|A \leftarrow C(k, n, \mathcal{R}), e \leftarrow \mathcal{D}_{k,n}(\mathcal{R}), u \leftarrow \mathcal{R}^k, b \leftarrow u{\cdot}A{+}e\} \approx \{(A, b)|A \leftarrow C(k, n, \mathcal{R}), b \leftarrow \mathcal{R}^n\}$$

定义 (Dual LPN/Regular Syndrome Decoding, RSD)

令 $\mathcal{D}(\mathcal{R})$ 和 C 和之前相同，$N, n \in \mathbb{N}, N > n$，定义 $C^\perp(N, n, \mathcal{R}) = \{H \in \mathcal{R}^{N\times n} : A \times H = 0, A \in C(N-n, N, \mathcal{R}), \mathrm{rank}(B) = n\}$。对 $n = n(\kappa), N = N(\kappa), \mathcal{R} = \mathcal{R}(\kappa)$，$(\mathcal{D}, C, \mathcal{R})$-dual-$LPN$ 假设是说：

$$\{(H, b)|H \leftarrow C^\perp(N, n, \mathcal{R}), e \leftarrow \mathcal{D}_{N-n,N}(\mathcal{R}), b \leftarrow e \cdot H\} \approx \{(H, b)|H \leftarrow C^\perp(N, n, \mathcal{R}), b \leftarrow \mathcal{R}^n\}$$

COT from Dual LPN

参数：$(\mathcal{HW}_t, C, \mathbb{F}_2)$-dual-$LPN$， $N = cn, c > 1(e.g.\ c = 2, 4), H \in \mathbb{F}_2^{N \times n}$.

$S(\Delta)$ $\qquad\qquad\qquad\qquad\qquad\qquad$ R

$\vec{e} \leftarrow \mathcal{HW}_t, \vec{e} = \mathcal{I}(N, Q)$

$$S \xrightarrow{\Delta} \boxed{\text{MPCOT}} \xleftarrow{Q} R$$

$$S \xleftarrow{\vec{s} \in \mathbb{F}_{2^\kappa}^N} \boxed{\text{MPCOT}} \xrightarrow{\vec{r} \in \mathbb{F}_{2^\kappa}^N} R$$

$\vec{v} := \vec{s} \cdot H \in \mathbb{F}_{2^\kappa}^n$

$\vec{u} := \vec{e} \cdot H \in \mathbb{F}_2^n$

$\vec{w} := \vec{r} \cdot H \in \mathbb{F}_{2^\kappa}^n$

COT from Primal LPN

参数：$(\mathcal{HW}_t, C, \mathbb{F}_2)$-*LPN*，$A \in \mathbb{F}_2^{k\times n}$.

$S(\Delta)$ R

$\vec{e} \leftarrow \mathcal{HW}_t, \vec{e} = \mathcal{I}(n, Q)$

Δ → **COT** ←

$\vec{b} \in \mathbb{F}_{2^\kappa}^k$ ← **COT** → $\vec{a} \in \mathbb{F}_2^k, \vec{c} \in \mathbb{F}_{2^\kappa}^k$

Δ → **MPCOT** ← Q

$\vec{s} \in \mathbb{F}_{2^\kappa}^n$ ← **MPCOT** → $\vec{r} \in \mathbb{F}_{2^\kappa}^n$

$\vec{v} := \vec{b} \cdot A + \vec{s} \in \mathbb{F}_{2^\kappa}^n$

$\vec{u} := \vec{a} \cdot A + \vec{e} \in \mathbb{F}_2^n$

$\vec{w} := \vec{c} \cdot A + \vec{r} \in \mathbb{F}_{2^\kappa}^n$

开销分析

一次 n 长 SPCOT：

- 需要 $\log n$ 次 COT.

一次 n 长 MPCOT:

- Uniform：需要 m 次 $|\mathcal{B}_j|+1$ 长 SPCOT，即 $m\log|\mathcal{B}_j|+1$ 次 COT。其中 $m\approx 1.5t, |\mathcal{B}_j|\approx 3n/m$，因此总共需要 $1.5t\log 2n/t$ 次 COT。
- Regular：需要 t 次 n/t 长 SPCOT，总共需要 $t\log n/t$ 次 COT。

一次 n 长 COT：

- Dual LPN：需要一次 N 长 MPCOT，其中 $N=cn, c>1$。即 $M=O(t\log n/t)$ 次 COT。
- Primal LPN：需要一次 n 长 MPCOT，一次 k 长 COT。即 $M=k+O(t\log n/t)$ 次 COT。

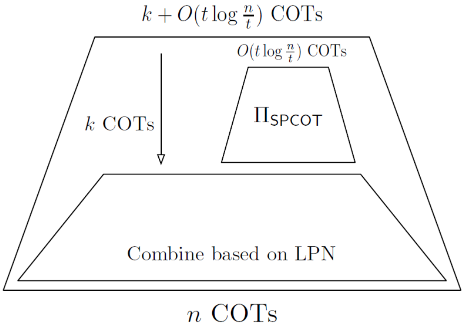
参数设置

由于需要的基础 COT 数量 M 也比较大，[Yan+20] 提出，可以先将 M 设置成第一阶段生成的 COT 数量（即 $n_0 = M$），以此确定一组更小的 LPN 参数 (t_0, k_0, n_0)，此时，为了生成 n_0 个 COT，需要 $M_0 = k_0 + \log n_0 / t_0$ 个基础 COT。再用 IKNP 框架生成这 M_0 个基础 COT。

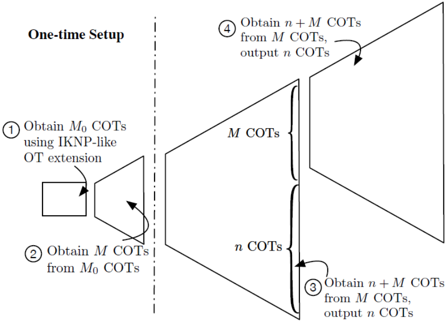
为了只做一次基础 COT，在第一次做 OT 扩展时，生成 $n + M$ 个 COT，保留 M 个留作下一次调用的基础 COT，剩下 n 个作为这一次的 COT 输出。

Protocol	One-time setup				Main iteration (output 10^7 COTs)			
	splen$_0$	k_0	n_0	t_0	splen	k	n	t
Ferret-Uni	2^{10}	37,248	616,092	1,254	2^{14}	588,160	10,616,092	1,324
Ferret-Reg	2^{9}	36,288	609,728	1,269	2^{13}	589,760	10,805,248	1,319

PCG 框架



(a) Structure of the COT amplifier.



(b) COT iterations with a one-time setup.

主要参考文献

1. [FY22] Dengguo Feng, and Kang Yang. "Concretely efficient secure multi-party computation protocols: survey and more." Security and Safety 1 (2022): 2021001.
2. [Ish+03] Yuval Ishai, Joe Kilian, Kobbi Nissim, Erez Petrank. Extending Oblivious Transfers Efficiently. CRYPTO 2003.
3. [Ash+13] Gilad Asharov, Yehuda Lindell, Thomas Schneider, Michael Zohner. More efficient oblivious transfer and extensions for faster secure computation. CCS 2013.
4. [Yan+20] Kang Yang, Chenkai Weng, Xiao Lan, Jiang Zhang, Xiao Wang. Ferret: Fast Extension for Correlated OT with Small Communication. CCS 2020.
5. [Sch+19] Phillipp Schoppmann, Adrià Gascón, Leonie Reichert, Mariana Raykova. Distributed Vector-OLE: Improved Constructions and Implementation. CCS 2019.

参考文献 I

[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 II

[Ash+15] Gilad Asharov et al. “More Efficient Oblivious Transfer Extensions with Security for Malicious Adversaries”. In: *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*. Ed. by Elisabeth Oswald and Marc Fischlin. Vol. 9056. Lecture Notes in Computer Science. Springer, 2015, pp. 673–701. DOI: 10.1007/978-3-662-46800-5_26. URL: https://doi.org/10.1007/978-3-662-46800-5_26.

参考文献 III

[Bea96] Donald Beaver. "Correlated Pseudorandomness and the Complexity of Private Computations". In: *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996*. Ed. by Gary L. Miller. ACM, 1996, pp. 479–488. DOI: 10.1145/237814.237996. URL: https://doi.org/10.1145/237814.237996.

[Boy+20] Elette Boyle et al. "Correlated Pseudorandom Functions from Variable-Density LPN". In: *61st IEEE Annual Symposium on Foundations of Computer Science, FOCS 2020, Durham, NC, USA, November 16-19, 2020*. Ed. by Sandy Irani. IEEE, 2020, pp. 1069–1080. DOI: 10.1109/FOCS46700.2020.00103. URL: https://doi.org/10.1109/FOCS46700.2020.00103.

参考文献 IV

[Boy+19a] Elette Boyle et al. "Efficient Pseudorandom Correlation Generators: Silent OT Extension and More". In: *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part III*. 2019, pp. 489–518. DOI: 10.1007/978-3-030-26954-8_16. URL: https://doi.org/10.1007/978-3-030-26954-8_16.

[Boy+19b] Elette Boyle et al. "Efficient Two-Round OT Extension and Silent Non-Interactive Secure Computation". In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS 2019, London, UK, November 11-15, 2019*. 2019, pp. 291–308. DOI: 10.1145/3319535.3354255. URL: https://doi.org/10.1145/3319535.3354255.

参考文献 V

[Bra+19] Pedro Branco et al. "A Framework for Universally Composable Oblivious Transfer from One-Round Key-Exchange". In: *Cryptography and Coding - 17th IMA International Conference, IMACC 2019, Oxford, UK, December 16-18, 2019, Proceedings*. Ed. by Martin Albrecht. Vol. 11929. Lecture Notes in Computer Science. Springer, 2019, pp. 78–101. DOI: 10.1007/978-3-030-35199-1_5. URL: https://doi.org/10.1007/978-3-030-35199-1_5.

参考文献 VI

[CSW20] Ran Canetti, Pratik Sarkar, and Xiao Wang. "Blazing Fast OT for Three-Round UC OT Extension". In: *Public-Key Cryptography - PKC 2020 - 23rd IACR International Conference on Practice and Theory of Public-Key Cryptography, Edinburgh, UK, May 4-7, 2020, Proceedings, Part II*. Ed. by Aggelos Kiayias et al. Vol. 12111. Lecture Notes in Computer Science. Springer, 2020, pp. 299–327. DOI: 10.1007/978-3-030-45388-6_11. URL: https://doi.org/10.1007/978-3-030-45388-6_11.

参考文献 VII

[CO15] Tung Chou and Claudio Orlandi. “The Simplest Protocol for Oblivious Transfer”. In: *Progress in Cryptology - LATINCRYPT 2015 - 4th International Conference on Cryptology and Information Security in Latin America, Guadalajara, Mexico, August 23-26, 2015, Proceedings*. Ed. by Kristin E. Lauter and Francisco Rodríguez-Henríquez. Vol. 9230. Lecture Notes in Computer Science. Springer, 2015, pp. 40–58. DOI: 10.1007/978-3-319-22174-8_3. URL: https://doi.org/10.1007/978-3-319-22174-8_3.

参考文献 VIII

[CRR21] Geoffroy Couteau, Peter Rindal, and Srinivasan Raghuraman. "Silver: Silent VOLE and Oblivious Transfer from Hardness of Decoding Structured LDPC Codes". In: *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part III*. Ed. by Tal Malkin and Chris Peikert. Vol. 12827. Lecture Notes in Computer Science. Springer, 2021, pp. 502–534. DOI: 10.1007/978-3-030-84252-9_17. URL: https://doi.org/10.1007/978-3-030-84252-9_17.

参考文献 IX

[DD20] Bernardo David and Rafael Dowsley. "Efficient Composable Oblivious Transfer from CDH in the Global Random Oracle Model". In: *Cryptology and Network Security - 19th International Conference, CANS 2020, Vienna, Austria, December 14-16, 2020, Proceedings*. Ed. by Stephan Krenn, Haya Shulman, and Serge Vaudenay. Vol. 12579. Lecture Notes in Computer Science. Springer, 2020, pp. 462–481. DOI: 10.1007/978-3-030-65411-5_23. URL: https://doi.org/10.1007/978-3-030-65411-5_23.

参考文献 X

[Döt+20] Nico Döttling et al. “Two-Round Oblivious Transfer from CDH or LPN”. 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*. Ed. by Anne Canteaut and Yuval Ishai. Vol. 12106. Lecture Notes in Computer Science. Springer, 2020, pp. 768–797. DOI: 10.1007/978-3-030-45724-2_26. URL: https://doi.org/10.1007/978-3-030-45724-2_26.

[FY22] Dengguo Feng and Kang Yang. “Concretely efficient secure multi-party computation protocols: survey and more”. In: *Security and Safety* 1 (2022), p. 2021001.

参考文献 XI

[Guo+22] Xiaojie Guo et al. “Half-Tree: Halving the Cost of Tree Expansion in COT and DPF”. In: *IACR Cryptol. ePrint Arch.* (2022), p. 1431. URL: https://eprint.iacr.org/2022/1431.

[Ish+03] Yuval Ishai et al. “Extending Oblivious Transfers Efficiently”. In: *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*. 2003, pp. 145–161. DOI: 10.1007/978-3-540-45146-4_9. URL: https://doi.org/10.1007/978-3-540-45146-4_9.

参考文献 XII

[KOS15] Marcel Keller, Emmanuela Orsini, and Peter Scholl. "Actively Secure OT Extension with Optimal Overhead". In: *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I*. Ed. by Rosario Gennaro and Matthew Robshaw. Vol. 9215. Lecture Notes in Computer Science. Springer, 2015, pp. 724–741. DOI: 10.1007/978-3-662-47989-6_35. URL: https://doi.org/10.1007/978-3-662-47989-6_35.

参考文献 XIII

[LGSG21] Yi-Fu Lai, Steven D. Galbraith, and Cyprien Delpech de Saint Guilhem. "Compact, Efficient and UC-Secure Isogeny-Based Oblivious Transfer". 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 I*. Ed. by Anne Canteaut and François-Xavier Standaert. Vol. 12696. Lecture Notes in Computer Science. Springer, 2021, pp. 213–241. DOI: 10.1007/978-3-030-77870-5_8. URL: https://doi.org/10.1007/978-3-030-77870-5_8.

参考文献 XIV

[MR19] Daniel Masny and Peter Rindal. “Endemic Oblivious Transfer”. 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. 309–326. DOI: 10.1145/3319535.3354210. URL: https://doi.org/10.1145/3319535.3354210.

参考文献 XV

[MRR21] Ian McQuoid, Mike Rosulek, and Lawrence Roy. “Batching Base Oblivious Transfers”. In: *Advances in Cryptology - ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6-10, 2021, Proceedings, Part III*. Ed. by Mehdi Tibouchi and Huaxiong Wang. Vol. 13092. Lecture Notes in Computer Science. Springer, 2021, pp. 281–310. DOI: 10.1007/978-3-030-92078-4_10. URL: https://doi.org/10.1007/978-3-030-92078-4_10.

参考文献 XVI

[MRR20] Ian McQuoid, Mike Rosulek, and Lawrence Roy. “Minimal Symmetric PAKE and 1-out-of-N OT from Programmable-Once Public Functions”. 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. 425–442. DOI: 10.1145/3372297.3417870. URL: https://doi.org/10.1145/3372297.3417870.

[NP01] Moni Naor and Benny Pinkas. “Efficient oblivious transfer protocols”. In: *Proceedings of the Twelfth Annual Symposium on Discrete Algorithms, January 7-9, 2001, Washington, DC, USA*. Ed. by S. Rao Kosaraju. ACM/SIAM, 2001, pp. 448–457. URL: http://dl.acm.org/citation.cfm?id=365411.365502.

参考文献 XVII

[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.

参考文献 XVIII

[PVW08] Chris Peikert, Vinod Vaikuntanathan, and Brent Waters. “A Framework for Efficient and Composable Oblivious Transfer”. In: *Advances in Cryptology - CRYPTO 2008, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings*. Ed. by David A. Wagner. Vol. 5157. Lecture Notes in Computer Science. Springer, 2008, pp. 554–571. DOI: 10.1007/978-3-540-85174-5_31. URL: https://doi.org/10.1007/978-3-540-85174-5_31.

参考文献 XIX

[Qua20] Willy Quach. "UC-Secure OT from LWE, Revisited". In: *Security and Cryptography for Networks - 12th International Conference, SCN 2020, Amalfi, Italy, September 14-16, 2020, Proceedings*. Ed. by Clemente Galdi and Vladimir Kolesnikov. Vol. 12238. Lecture Notes in Computer Science. Springer, 2020, pp. 192–211. DOI: 10.1007/978-3-030-57990-6_10. URL: https://doi.org/10.1007/978-3-030-57990-6_10.

[Rab05] Michael O. Rabin. *How To Exchange Secrets with Oblivious Transfer*. Cryptology ePrint Archive, Paper 2005/187. https://eprint.iacr.org/2005/187. 2005. URL: https://eprint.iacr.org/2005/187.

参考文献 XX

[Roy22] Lawrence Roy. “SoftSpokenOT: Quieter OT Extension from Small-Field Silent VOLE in the Minicrypt Model”. 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. 657–687. DOI: 10.1007/978-3-031-15802-5_23. URL: https://doi.org/10.1007/978-3-031-15802-5_23.

参考文献 XXI

[Sch+19] Phillipp Schoppmann et al. "Distributed Vector-OLE: Improved Constructions and Implementation". In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS 2019, London, UK, November 11-15, 2019*. 2019, pp. 1055–1072. DOI: 10.1145/3319535.3363228. URL: https://doi.org/10.1145/3319535.3363228.

[Wen+21] Chenkai Weng et al. "Wolverine: Fast, Scalable, and Communication-Efficient Zero-Knowledge Proofs for Boolean and Arithmetic Circuits". In: *42nd IEEE Symposium on Security and Privacy, SP 2021, San Francisco, CA, USA, 24-27 May 2021*. IEEE, 2021, pp. 1074–1091. DOI: 10.1109/SP40001.2021.00056. URL: https://doi.org/10.1109/SP40001.2021.00056.

参考文献 XXII

[Yan+20] Kang Yang et al. “Ferret: Fast Extension for Correlated OT with Small Communication”. In: *CCS ’20: 2020 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, USA, November 9-13, 2020*. 2020, pp. 1607–1626. DOI: 10.1145/3372297.3417276. URL: https://doi.org/10.1145/3372297.3417276.

Thanks!