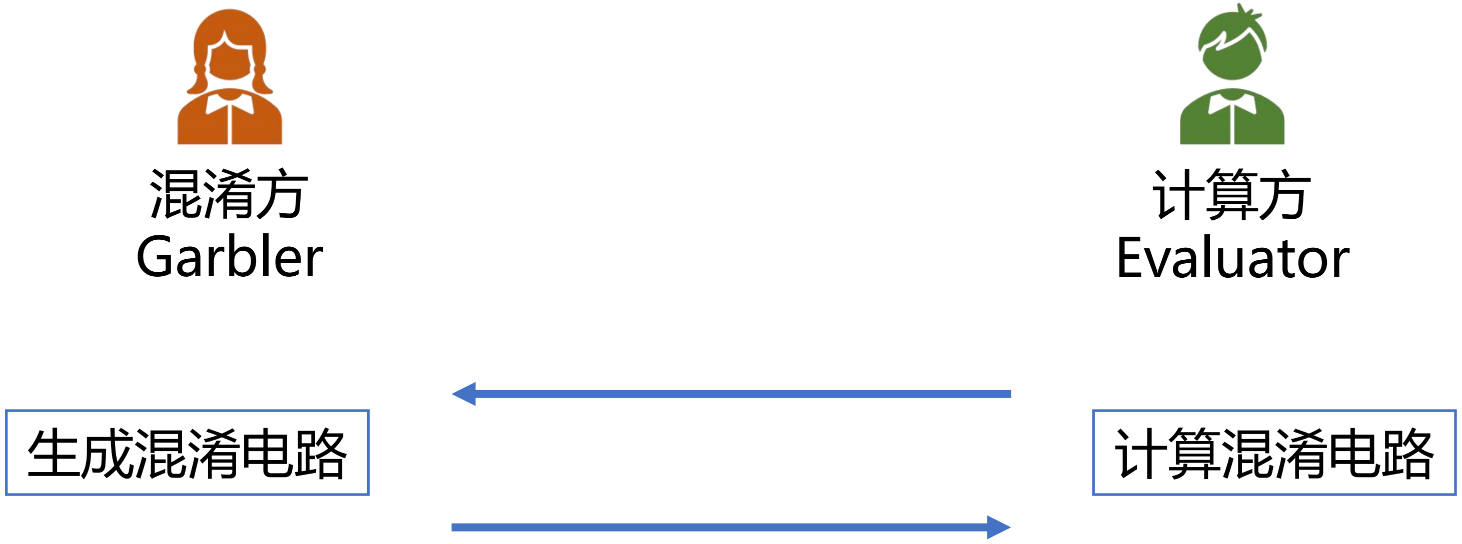
基于混淆电路方法的安全多方计算协议

冯登国

内容概要

本讲主要介绍安全两方计算（2PC）协议的设计方法，重点涉及混淆电路的构造方法



- 本讲介绍的MPC协议具有 $O(1)$ 轮数复杂度，与电路深度 d 无关
- 第二讲介绍的 MPC 协议要求 $O(d)$ 轮数复杂度

常数轮的 MPC 协议

常数轮安全多方计算（n >2）

- 不同于两方情况，在多方情况下，存在**多个参与方合谋**
- 不能让任何一方计算整个混淆电路，需要**所有参与方共同分布式计算混淆电路**

BMR类分布式混淆电路

- **对称性**：所有参与方都能计算混淆电路
- 混淆电路大小：共发送 $4n^2|C|\kappa$ 比特
- 在线轮数：2 轮

$|C|$ 表示 AND 门数量，n 表示参与方数量

WRK类分布式混淆电路

- **非对称性**：只有一方能计算混淆电路
- 混淆电路大小：共发送 $4n(n-1)|C|\kappa$ 比特
- 在线轮数：2-4 轮

[YWZ20]：$(4n-6)(n-1)|C|\kappa$ 比特

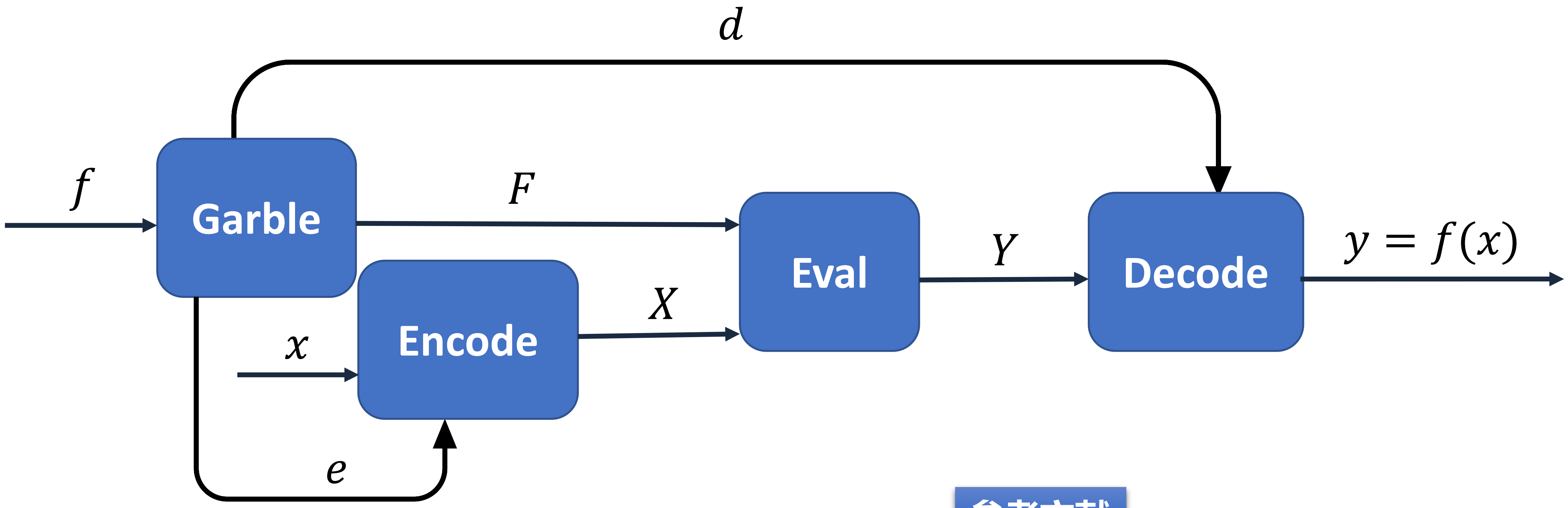
[YWZ20] Kang Yang, Xiao Wang, and Jiang Zhang. More efficient MPC from improved triple generation and authenticated garbling. In *ACM CCS 2020*

报告提纲

一、Yao 半诚实安全两方计算协议

二、混淆电路构造与效率比较

混淆电路基本定义回顾



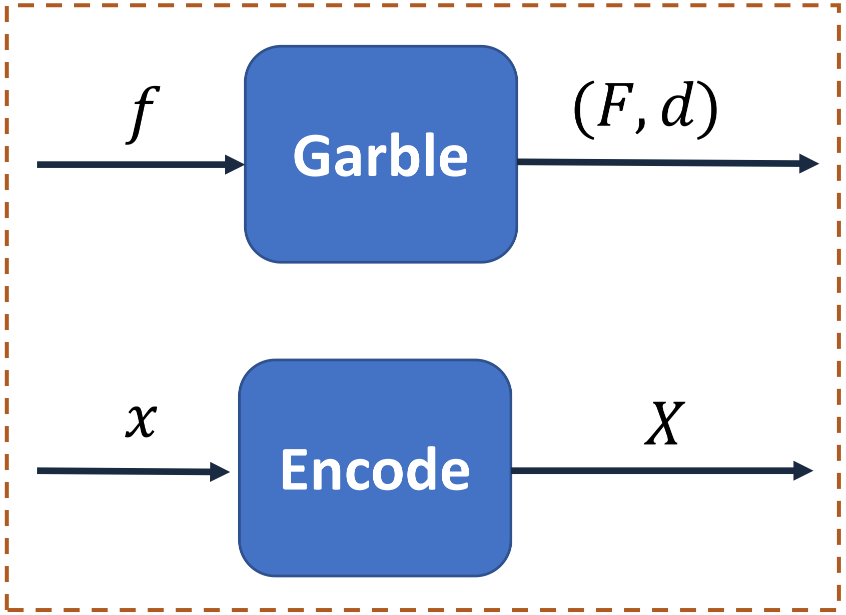
- f 为电路，F 为混淆电路
- e 编码信息，d 解码信息
- x 电路输入，y 电路输出
- X 输入编码，Y 输出编码

- Garble 混淆算法
- Encode 编码算法
- Eval 计算算法
- Decode 解码算法

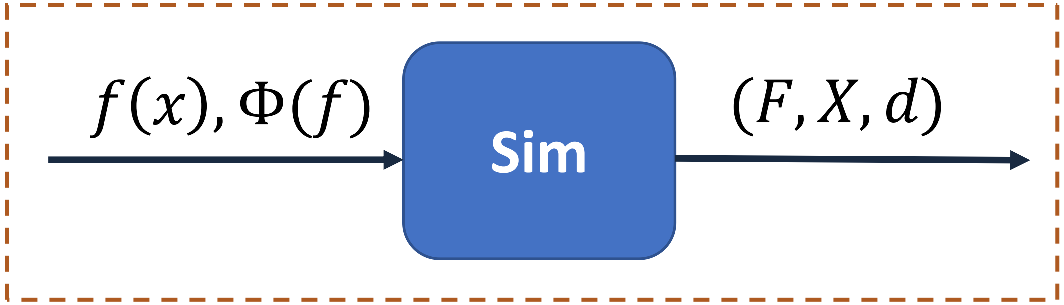
参考文献

- [Yao86] Andrew Chi-Chih Yao. How to generate and exchange secrets. In *FOCS 1986*
- [BHR12] Mihir Bellare, Viet Tung Hoang and Phillip Rogaway. Foundations of Garbled Circuits. In *ACM CCS 2012*

混淆电路的模拟安全定义



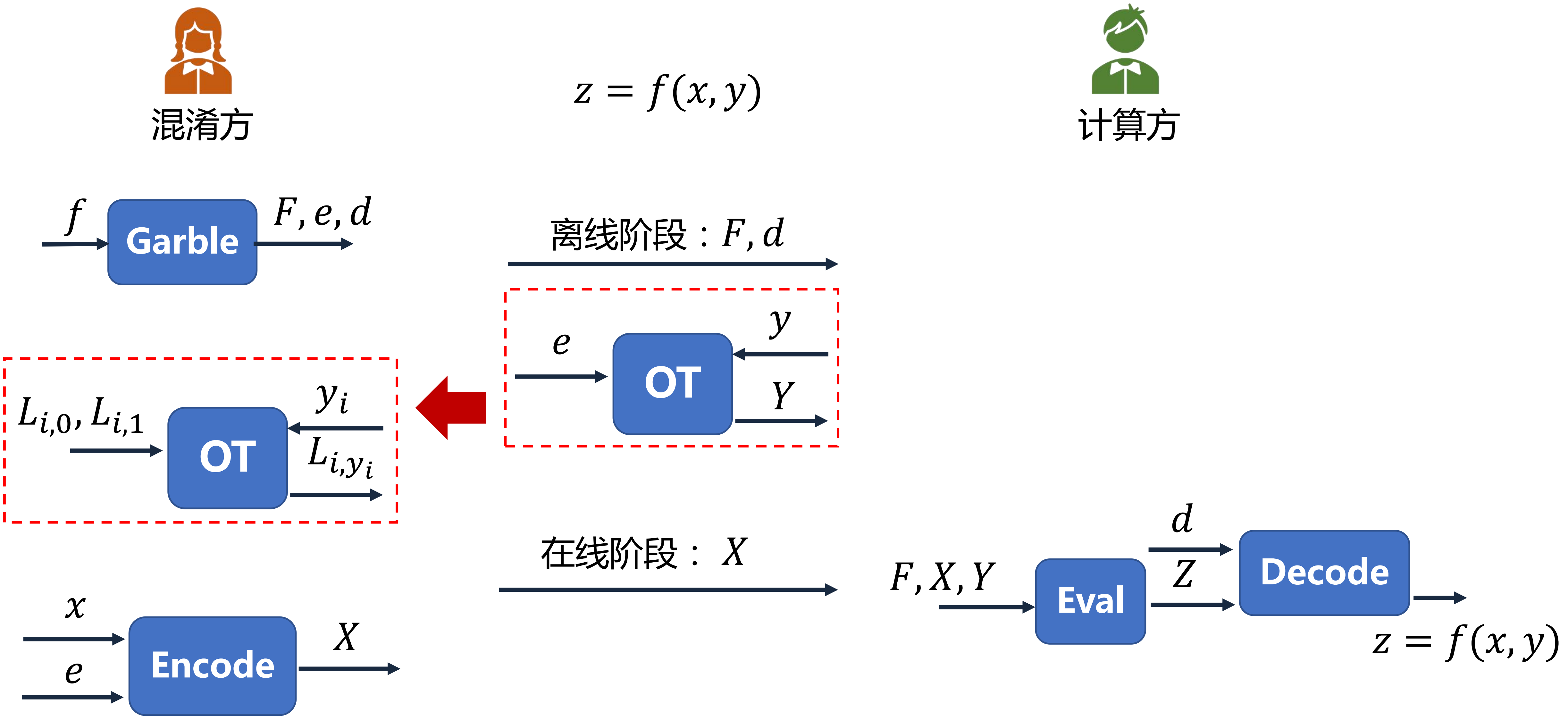
$\approx$



$\Phi(f) = f$ 或 $\Phi(f) = |f|$

[BHR12] Mihir Bellare, Viet Tung Hoang and Phillip Rogaway. Foundations of Garbled Circuits. In *ACM CCS 2012*

Yao 半诚实安全两方计算协议

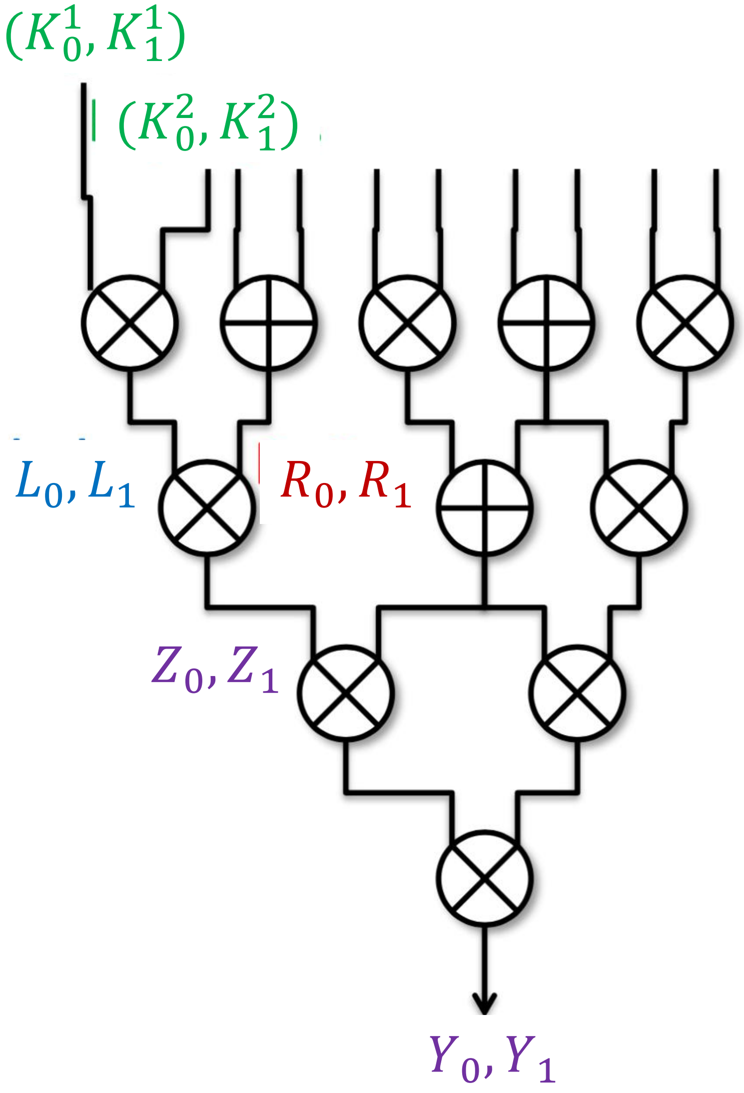


报告提纲

一、Yao 半诚实安全两方计算协议

二、混淆电路构造与效率比较

混淆电路基础框架（1）



Garble

- 每条电路线：选取密钥 (K_0^i, K_1^i)
- 每个电路门：
  - 左输入线密钥 (L_0, L_1)
  - 右输入线密钥 (R_0, R_1)
  - 输出线密钥 (Z_0, Z_1)
  - 计算混淆门 $gg \leftarrow Gb(g, L_0, L_1, R_0, R_1, Z_0, Z_1)$
- 电路输入线的密钥构成编码信息 $e = \{(K_0^i, K_1^i)\}$
- 电路输出线的密钥构成解码信息 $d = (Y_0, Y_1)$
- 所有混淆门构成混淆电路 $F = \{gg^i\}$

图来自 Claudio Orlandi 的 CIS 2018 学术报告（修改）

混淆电路基础框架（2）

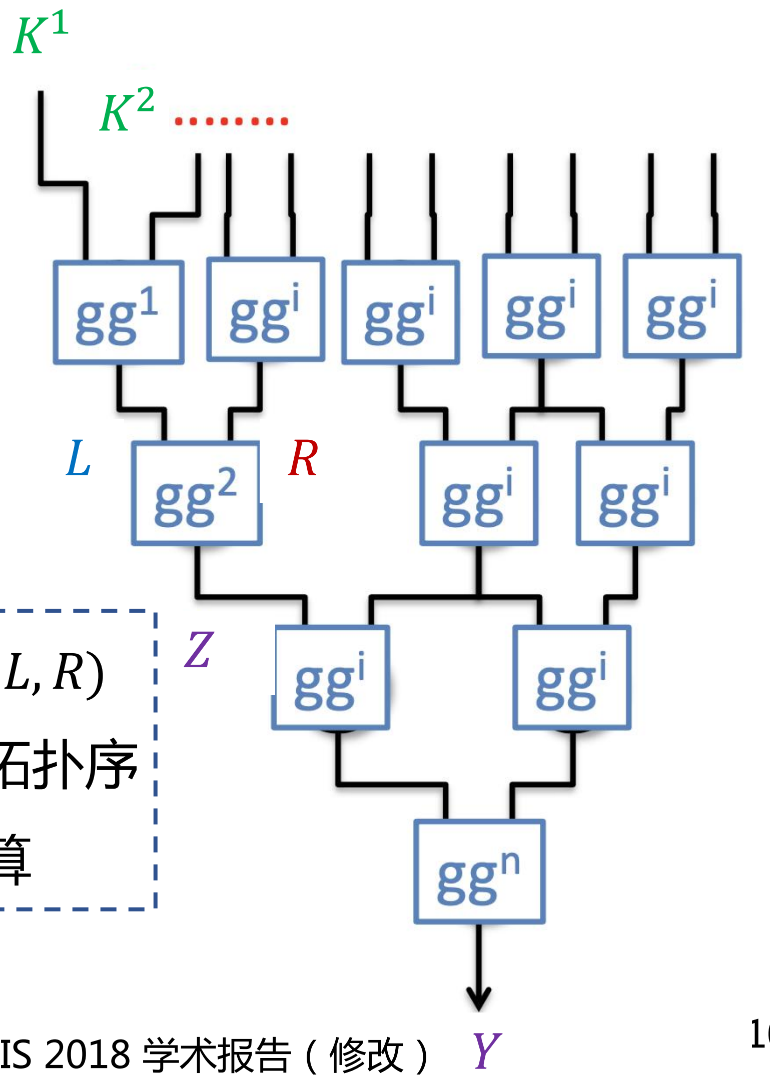
$X \leftarrow Encode(e, x)$

- 输入： $e = \{(K_0^i, K_1^i)\}$ 和 $x = (x_1, \cdots, x_m)$
- 输出： $X = (K_{x_1}^1, \cdots, K_{x_m}^m)$

$y \leftarrow Decode(d, Y)$

- 输入： $d = \{Y_0, Y_1\}$ 和 Y
- 输出： 若 $Y = Y_0$，则输出 $y = 0$；若 $Y = Y_1$，则输出 $y = 1$；否则，输出中止符 $\perp$

$Y \leftarrow Eval(F, X)$

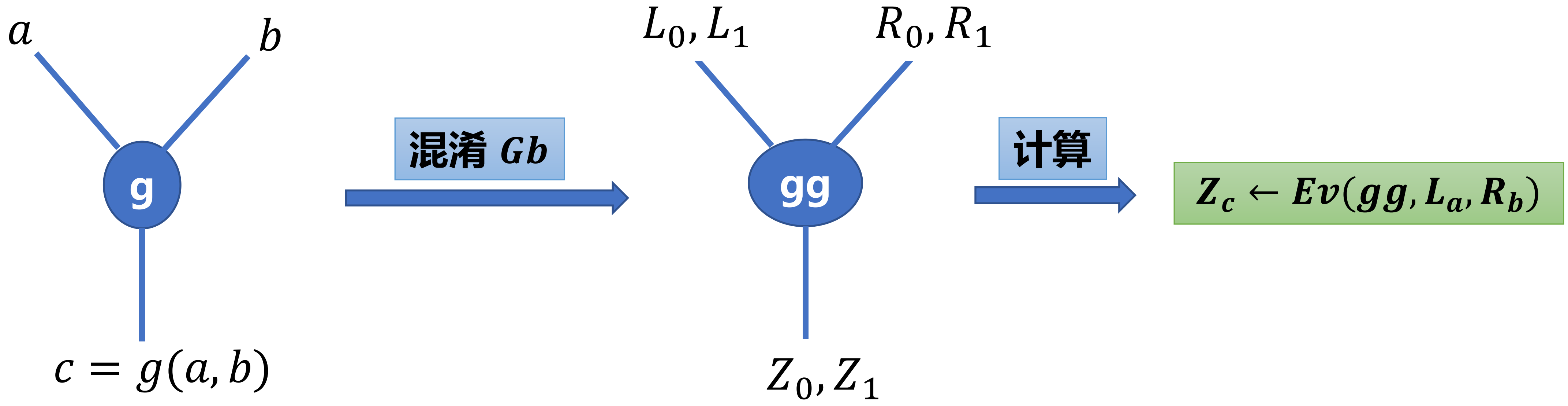


$Z \leftarrow Ev(gg^2, L, R)$

- 按照电路拓扑序
- 逐个门计算

图来自 Claudio Orlandi 的 CIS 2018 学术报告（修改）

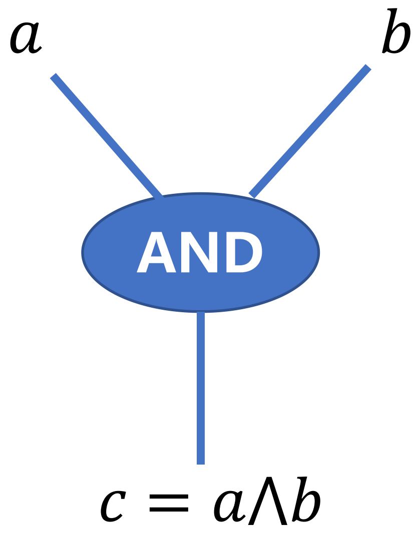
混淆单个电路门



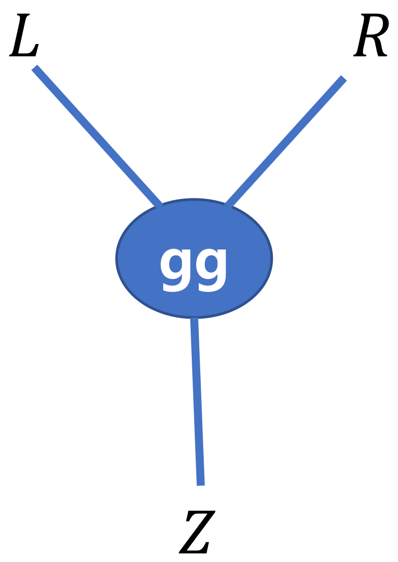
$g \in \{\text{AND, XOR}\}$

$gg \Rightarrow$ 混淆门

Textbook Yao 混淆电路（1）



a	b	c
0	0	0
0	1	0
1	0	0
1	1	1



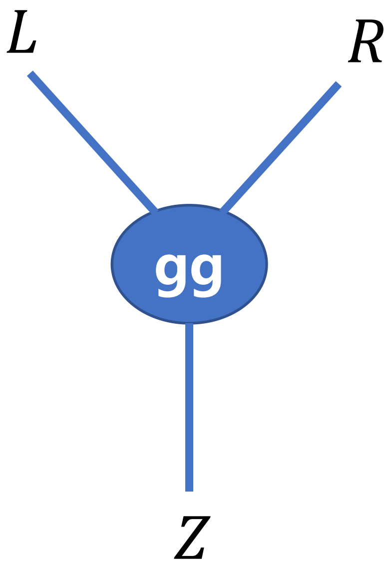
L	R	Z
L_0	R_0	Z_0
L_0	R_1	Z_0
L_1	R_0	Z_0
L_1	R_1	Z_1

以 AND 门为例，XOR 门完全类似

$Enc_{L,R}(Z)$

- [Yao86] Andrew Chi-Chih Yao. How to generate and exchange secrets. In *FOCS 1986*
- [LP09] A Proof of Security of Yao’s Protocol for Two-Party Computation. In *JoC 2009* (原稿发表于 ASIACRYPT 2004)

Textbook Yao 混淆电路（2）



$Enc_{L,R}(Z)$
$C_{00} = H(L_0, R_0) \oplus Z_0$
$C_{01} = H(L_0, R_1) \oplus Z_0$
$C_{10} = H(L_1, R_0) \oplus Z_0$
$C_{11} = H(L_1, R_1) \oplus Z_1$

$Enc_{L,R}(Z)$ 置换
$C_{00} = H(L_0, R_0) \oplus Z_0$
$C_{01} = H(L_0, R_1) \oplus Z_0$
$C_{10} = H(L_1, R_0) \oplus Z_0$
$C_{11} = H(L_1, R_1) \oplus Z_1$

无法判断哪个密文被正确解密

- $H \Rightarrow$ “密钥导出函数”，保证加密安全性
- 原理：输入线密钥 加密 输出线密钥
- $Ev(gg, L_a, R_b) \Rightarrow Z_c = C_{ab} \oplus H(L_a,\ R_b)$
- 泄漏输入 (a, b) 和输出 $c = a \wedge b$ 的信息

Textbook Yao 混淆电路（3）

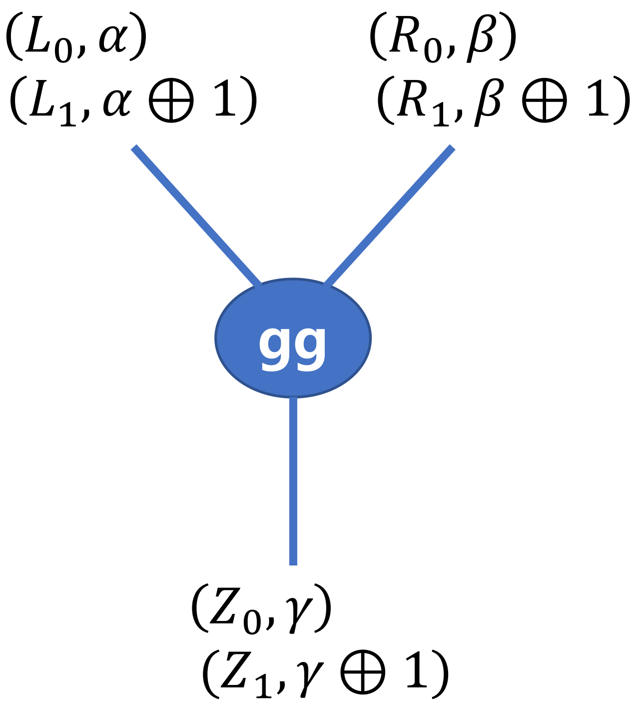
$Enc_{L,R}(Z)$
$C_0 = H(L_0, R_0) \oplus (Z_0, 0^\kappa)$
$C_1 = H(L_0, R_1) \oplus (Z_0, 0^\kappa)$
$C_2 = H(L_1, R_0) \oplus (Z_0, 0^\kappa)$
$C_3 = H(L_1, R_1) \oplus (Z_1, 0^\kappa)$

- 逐一解密每个密文
- 解密结果包含 0^κ 的密文为正确解密
- $(Z, T) = C \oplus H(L_a,\ R_b)$：若 $T = 0^\kappa$，则密文解密正确，Z 为输出线密钥

混淆电路方案	通信开销 (单位：κ 比特/门)		计算开销 (H数量/门)				假设
			Garbler		Evaluator		
	AND	XOR	AND	XOR	AND	XOR	
Textbook Yao [Yao86]	8	8	4	4	2.5	2.5	PRF

点置换优化（Point-and-Permute）（1）

- ➢ Textbook Yao 混淆电路每个电路门需要 $\mathbf{8\kappa}$ 比特通信，并要求计算方（Evaluator）每个电路门平均解密 **2.5** 次（从第一个密文开始逐一尝试解密，直至解密成功）
- ➢ 点置换优化降低通信开销至每个电路门 $\mathbf{4\kappa}$ 比特，同时降低平均解密次数为 **1** 次



- 添加随机置换比特 $\alpha,\ \beta, \gamma \in \{0,1\}$
- 可用密钥 $L_0, R_0,\ Z_0$ 的最低比特作为置换比特
- $gg \leftarrow Gb(g, L_0, L_1, \alpha, R_0, R_1, \beta, Z_0, Z_1, \gamma)$
- $(Z_c, c\oplus\gamma) \leftarrow Ev(gg, L_a, a\oplus\alpha, R_b, b\oplus\beta)$

[BMR90] Donald Beaver, Silvio Micali, and Phillip Rogaway. The round complexity of secure protocols. In *STOC 1990*

点置换优化（Point-and-Permute）（2）

① 移除冗余

$Enc_{L,R}(Z)$
$C_{00} = H(L_0, R_0) \oplus (Z_0, \gamma)$
$C_{01} = H(L_0, R_1) \oplus (Z_0, \gamma)$
$C_{10} = H(L_1, R_0) \oplus (Z_0, \gamma)$
$C_{11} = H(L_1, R_1) \oplus (Z_1, \gamma\oplus 1)$

采用比特 α, β 实现密文置换

② 添加置换

$Enc_{L,R}(Z)$
$C'_{00} = H(L_\alpha, R_\beta) \oplus (Z_{\alpha\beta}, \gamma \oplus \alpha\beta)$
$C'_{01} = H(L_\alpha, R_{\beta\oplus 1}) \oplus (Z_{\alpha(\beta\oplus 1)}, \gamma \oplus \alpha(\beta\oplus 1))$
$C'_{10} = H(L_{\alpha\oplus 1}, R_\beta) \oplus (Z_{(\alpha\oplus 1)\beta}, \gamma \oplus (\alpha\oplus 1)\beta)$
$C'_{11} = H(L_{\alpha\oplus 1}, R_{\beta\oplus 1}) \oplus (Z_{(\alpha\oplus 1)(\beta\oplus 1)}, \gamma \oplus (\alpha\oplus 1)(\beta\oplus 1))$

$a\oplus\alpha$	$b\oplus\beta$	a	b	c
0	0	α	β	$\alpha\beta$
0	1	α	$\beta\oplus 1$	$\alpha(\beta\oplus 1)$
1	0	$\alpha\oplus 1$	β	$(\alpha\oplus 1)\beta$
1	1	$\alpha\oplus 1$	$\beta\oplus 1$	$(\alpha\oplus 1)(\beta\oplus 1)$

点置换优化（Point-and-Permute）（3）

$Enc_{L,R}(Z)$
$C'_{00} = H(L_\alpha, R_\beta) \oplus (Z_{\alpha\beta}, \gamma \oplus \alpha\beta)$
$C'_{01} = H(L_\alpha, R_{\beta\oplus 1}) \oplus (Z_{\alpha(\beta\oplus 1)}, \gamma \oplus \alpha(\beta\oplus 1))$
$C'_{10} = H(L_{\alpha\oplus 1}, R_\beta) \oplus (Z_{(\alpha\oplus 1)\beta}, \gamma \oplus (\alpha\oplus 1)\beta)$
$C'_{11} = H(L_{\alpha\oplus 1}, R_{\beta\oplus 1}) \oplus (Z_{(\alpha\oplus 1)(\beta\oplus 1)}, \gamma \oplus (\alpha\oplus 1)(\beta\oplus 1))$

$$Ev(gg, L_a, a\oplus\alpha, R_b, b\oplus\beta) \Rightarrow (Z_{ab}, ab \oplus \gamma) = C'_{a\oplus\alpha, b\oplus\beta} \oplus H(L_a, R_b)$$

- α, β, γ 是输入/输出比特 $a, b, c = ab$ 的“一次一密本”
- $a\oplus\alpha, b\oplus\beta, c\oplus\gamma$ 未泄漏门输入/输出比特的任何信息

点置换优化（Point-and-Permute）（4）

混淆电路方案	通信开销 (单位：κ 比特/门)		计算开销 (H数量/门)				假设
			Garbler		Evaluator		
	AND	XOR	AND	XOR	AND	XOR	
Textbook Yao [Yao86]	8	8	4	4	2.5	2.5	PRF
点置换优化 [BMR90]	4	4	4	4	1	1	PRF

混淆电路计算效率的改进（1）

$2\ Hash > 1\ Hash > 1\ block\ cipher > 1\ block\ cipher\ without\ key\ schedule$

$Enc_{L,R}(Z) = H(L,R) \oplus Z$	生成 AES 的混淆电路计算时间
$PRF(L, \text{gateID}) \oplus PRF(R, \text{gateID}) \oplus Z$ [NPS99]	约 6 秒 [MNPS04], $PRF = SHA256$
$H(L \parallel R \parallel \text{gateID}) \oplus Z$ [LPS08]	约 0.15 秒 [sS12], $H = SHA256$
$PRF(L \parallel R, \text{gateID}) \oplus Z$ [KsS12]	约 0.12 秒 [KsS12], $PRF = AES256$
$\pi(K) \oplus K \oplus Z$, 其中 π 为随机置换和$K = 2L \oplus 4R \oplus \text{gateID}$ [BHKR13]	约 0.0003 秒 [BHKR13], $\pi = AES128\ w/o\ key\ schedule$

表格参考 Mike Rosulek 的学术报告“Practical Garbled Circuit Optimizations”的PPT

- [NPS99] Moni Naor, Benny Pinkas, and Reuban Sumner. Privacy preserving auctions and mechanism design. In *Proceedings of the 1st ACM Conference on Electronic Commerce, 1999*
- [MNPS04] Dahlia Malkhi, Noam Nisan, Benny Pinkas, and Yaron Sella. Fairplay — A Secure Two-Party Computation System. In *USENIX Security 2004*
- [LPS08] Yehuda Lindell, Benny Pinkas, and Nigel P. Smart. Implementing Two-Party Computation Efficiently with Security Against Malicious Adversaries. In *SCN 2008*
- [KsS12] Benjamin Kreuter, abhi shelat and Chih-hao Shen. Billion-Gate Secure Computation with Malicious Adversaries. In *USENIX Security 2012*
- [BHKR13] Mihir Bellare, Viet Tung Hoang, Sriram Keelveedhi, and Phillip Rogaway. Efficient Garbling from a Fixed-Key Blockcipher. In *IEEE S&P 2013*

混淆电路计算效率的改进（2）

- 随机置换（如：固定密钥 AES）可实现混淆电路构造中特殊 Hash 函数 [BHKR13]
- 基于硬件指令（AES-NI）加速，**混淆电路的效率瓶颈是通信开销**

拓展研读：后续混淆电路方案的计算效率优化方法

- [ZRE15] Samee Zahur, Mike Rosulek, and David Evans. Two Halves Make a Whole：Reducing Data Transfer in Garbled Circuits using Half Gates. In *EUROCRYPT 2015*
- [GKWY20] Chun Guo, Jonathan Katz, Xiao Wang and Yu Yu. Efficient and Secure Multiparty Computation from Fixed-Key Block Ciphers. In *IEEE S&P 2020*
- [RR21] Mike Rosulek and Lawrence Roy. Three Halves Make a Whole? Beating the Half-Gates Lower Bound for Garbled Circuits. In *CRYPTO 2021*

混淆行约化技术（Garbled Row Redution）（1）

基本思想

$Enc_{L,R}(Z)$
$C_{00} = H(L_0, R_0) \oplus Z_0 = \mathbf{0}^\kappa$ $Z_0 = H(L_0, R_0)$
$C_{01} = H(L_0, R_1) \oplus Z_0$
$C_{10} = H(L_1, R_0) \oplus Z_0$
$C_{11} = H(L_1, R_1) \oplus Z_1$

- 与点置换优化兼容
- **与 Free XOR 技术（即将介绍）兼容**
- 降低通信开销 κ比特/门

[NPS99] Moni Naor, Benny Pinkas, and Reuban Sumner. Privacy preserving auctions and mechanism design. In *Proceedings of the 1st ACM Conference on Electronic Commerce, 1999*

拓展研读

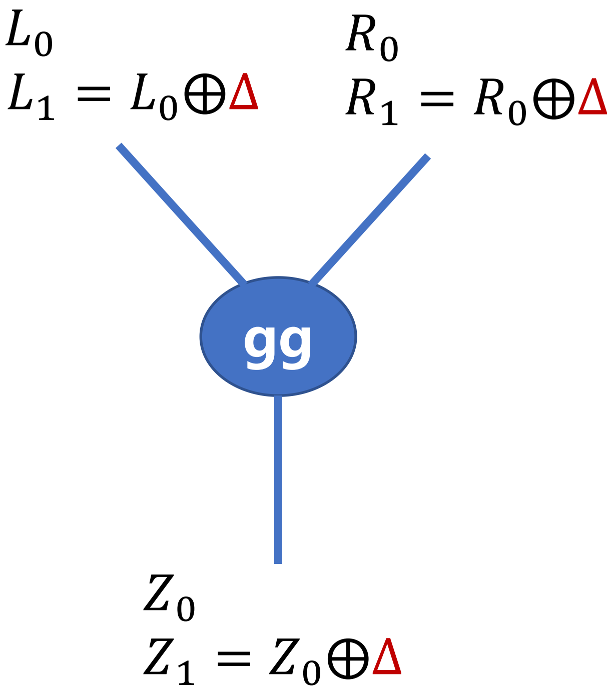
- 采用多项式插值技术实现混淆行约化，降低通信开销 2κ比特/门
- 与点置换优化兼容，**但与 Free XOR 技术不兼容，XOR 门仍然需要通信开销**

[PSSW09] Benny Pinkas, Thomas Schneider, Nigel P. Smart, and Stephen C. Williams. Secure two-party computation is practical. In *ASIACRYPT 2009*

混淆行约化技术（Garbled Row Redution）（2）

混淆电路方案	通信开销 (单位：κ 比特/门)		计算开销 (H数量/门)				假设
			Garbler		Evaluator		
	AND	XOR	AND	XOR	AND	XOR	
Textbook Yao [Yao86]	8	8	4	4	2.5	2.5	PRF
点置换优化 Yao [BMR90]	4	4	4	4	1	1	PRF
4-to-3 GRR [NPS99]	3	3	4	4	1	1	PRF
4-to-2 GRR [PSSW09]	2	2	4	4	1	1	PRF

Free XOR 技术（1）

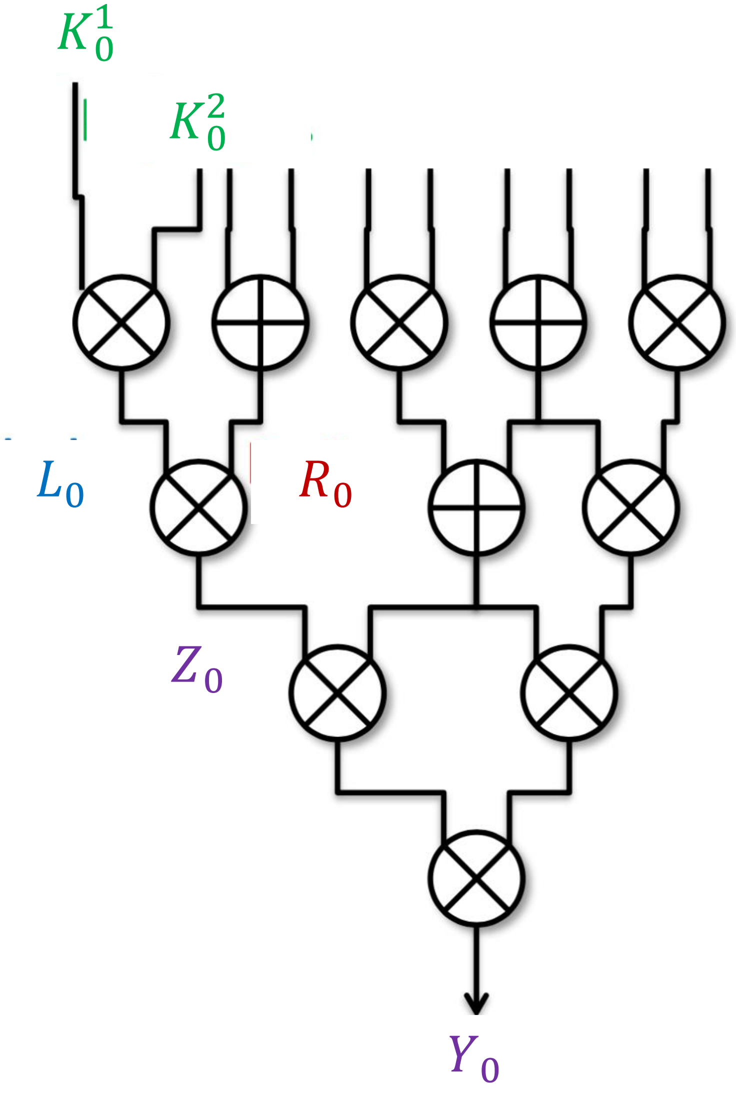


- ➢ 第二讲介绍的基于线性秘密分享的 MPC 协议均对于加法等线性门满足“free”特性
- ➢ 混淆电路是否可行？
- ➢ 引入全局密钥 Δ，使得密钥 L_0, L_1 满足固定相关性 $L_0 \oplus L_1 = \Delta$

- $(gg, Z_0) \leftarrow Gb(g, L_0,\ R_0, \Delta)$
- $Z_{g(a,b)} \leftarrow Ev(gg, L_a, R_b)$

[KS08] Vladimir Kolesnikov and Thomas Schneider. Improved garbled circuit: Free XOR gates and applications. In *ICALP 2008*

Free XOR 技术（2）



图来自 Claudio Orlandi 的 CIS 2018 学术报告（修改）

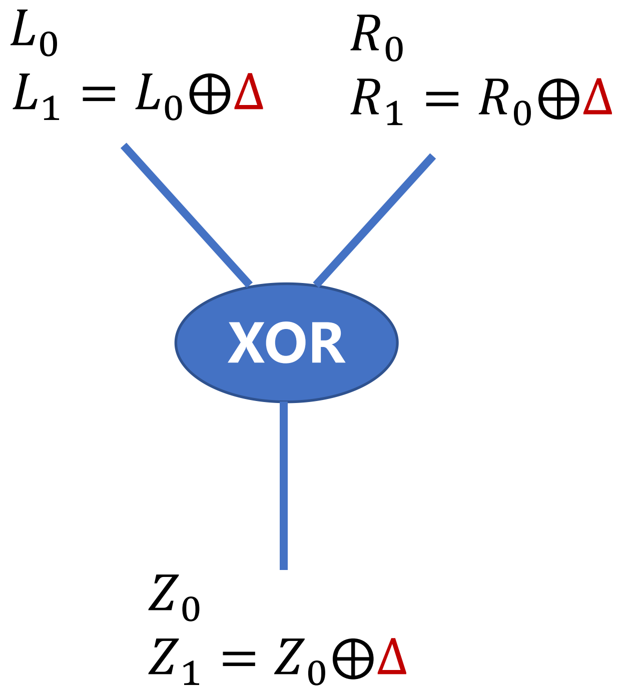
- 每条电路输入线随机选取密钥 K_0^i
- 随机选取全局密钥 Δ
- $L_0 \oplus L_1 = \Delta$
- 混淆 **AND** 门方法与之前相同，但需要“循环安全假设”
- 例如：$C_{00} = H(L_0 \oplus \Delta, R_0 \oplus \Delta) \oplus (Z_0 \oplus \Delta)$

- H 需满足循环相关强健性的定义
- Circular Correlation Robustness (CCR)

拓展研读

[CKKZ12] Seung Geol Choi, Jonathan Katz, Ranjit Kumaresan, and Hong-Sheng Zhou. On the security of the “free-XOR” technique. In *TCC 2012*

Free XOR 技术（3）



- $Z_0 \leftarrow Gb(\mathrm{XOR}, L_0, R_0, \Delta)$：$Z_0 = L_0 \oplus R_0$
  - **XOR 门无需通信，密钥 XOR 即可**
- $Z_{a\oplus b} \leftarrow Ev(\mathrm{XOR}, L_a, R_b)$：$Z_{a\oplus b} = L_a \oplus R_b$

$$= L_a \oplus R_b$$
$$= (L_0 \oplus a\Delta) \oplus (R_0 \oplus b\Delta)$$
$$= (L_0 \oplus R_0) \oplus \big((a \oplus b)\Delta\big)$$
$$= Z_0 \oplus \big((a \oplus b)\Delta\big)$$
$$= Z_{a\oplus b}$$

Free XOR 技术（4）

混淆电路方案	通信开销 (单位：κ 比特/门)		计算开销 (H数量/门)				假设
			Garbler		Evaluator		
	AND	XOR	AND	XOR	AND	XOR	
Textbook Yao [Yao86]	8	8	4	4	2.5	2.5	PRF
点置换优化 Yao [BMR90]	4	4	4	4	1	1	PRF
4-to-3 GRR [NPS99]	3	3	4	4	1	1	PRF
4-to-2 GRR [PSSW09]	2	2	4	4	1	1	PRF
Free XOR [KS08]	3	**0**	4	**0**	1	**0**	CCR
Flexible XOR [KMR14]	2	{0,1,2}	4	{0,2,4}	1	{0,1,2}	CCR

[KMR14] Vladimir Kolesnikov, Payman Mohassel, and Mike Rosulek. FleXOR: Flexible garbling for XOR gates that beats free-XOR. In *CRYPTO 2014*

混淆电路构造——进一步改进优化

混淆电路方案	通信开销 (单位：κ 比特/门)		计算开销 (H数量/门) Garbler		计算开销 (H数量/门) Evaluator		假设
	AND	XOR	AND	XOR	AND	XOR	
Half-gates [ZRE15]	2	0	4	0	2	0	CCR
快速 4-to-2 GRR [GLNP15]	2	1	4	3	2	1.5	PRF
Three halves [RR21]	1.5	0	≤ 6	0	≤ 3	0	CCR

当前通信效率最优构造

拓展研读

- [ZRE15] Samee Zahur, Mike Rosulek, and David Evans. Two halves make a whole - reducing data transfer in garbled circuits using half gates. In *EUROCRYPT 2015*
- [GLNP15] Shay Gueron, Yehuda Lindell, Ariel Nof, and Benny Pinkas. Fast garbling of circuits under standard assumptions. In *ACM CCS 2015*
- [RR21] Mike Rosulek and Lawrence Roy. Three Halves Make a Whole? Beating the Half-Gates Lower Bound for Garbled Circuits. In *CRYPTO 2021*

谢谢！不妥之处，敬请指正！

- 安全多方计算基础讲义（1）—— 安全多方计算基本定义及基础组件
- 安全多方计算基础讲义（2）—— 基于秘密分享方法的安全多方计算协议
- 安全多方计算基础讲义（3）—— 基于混淆电路方法的安全多方计算协议

MPC综述论文

- [Lin20] Yehuda Lindell. Secure multiparty computation. In *Communications of the ACM 2020*
- [Ors20] Emmanuela Orsini. Efficient, actively secure MPC with a dishonest majority: A survey. In *WAIFI 2020*
- [FY21] Dengguo Feng and Kang Yang. Concretely Efficient Secure Multi-Party Computation Protocols: Survey and More. In *Security and Safety 2021*