最適な通信量の2者間秘密計算における乱数長について

2024/3/7

樋渡 啓太郎 (東京大学)

目次

- 秘密計算について
- 研究紹介

(前半) 秘密計算について

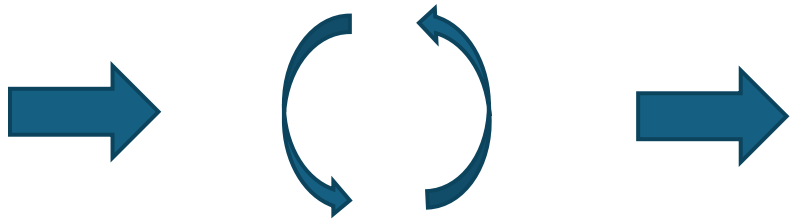
秘密計算

入力を隠したまま計算を行える暗号技術

e.g.,

Alice (貯金:a円)

Bob (貯金:b円)



Alice (私の方が多い！)

相手の貯金額はわからない！

Bob （僕の方が少ない…)

秘密計算

“プライバシー保護 × データの活用”の両立

⇒ 様々な応用先：

〇ゲノム解析

　　ゲノム情報は隠したいけど，解析はしてほしい．

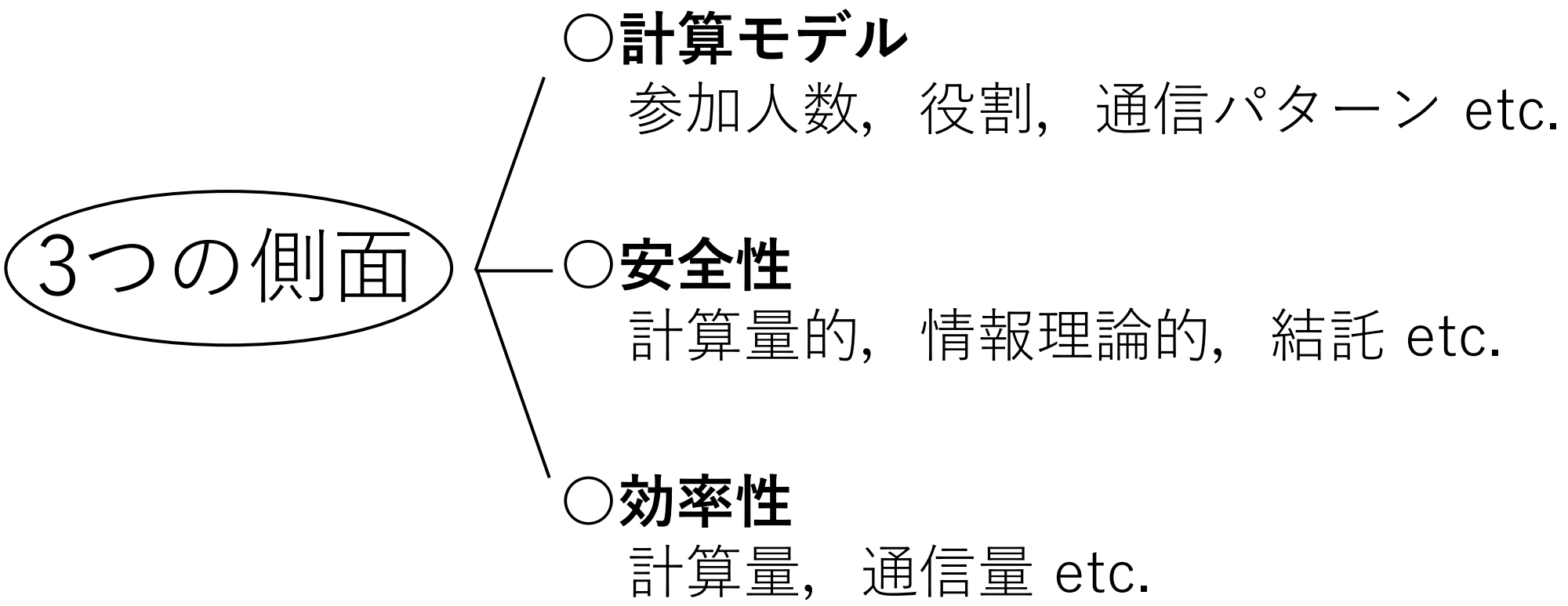
〇秘匿検索

　　(クエリ側)検索したいけど，何を検索したかは隠したい．

　　(サーバ側)クエリされたもの以外の情報は開示したくない．

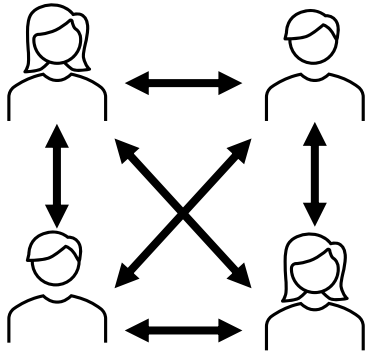
etc.

秘密計算

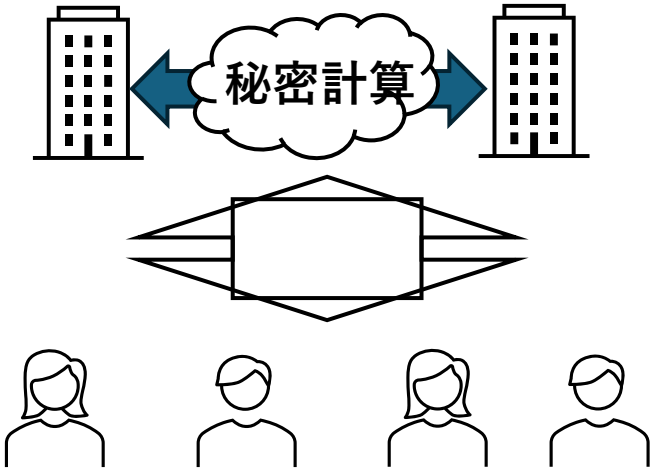

3つの側面
○計算モデル
参加人数，役割，通信パターン etc.
○安全性
計算量的，情報理論的，結託 etc.
○効率性
計算量，通信量 etc.

計算モデル

一般的な設定：
　入力を持つN人で計算をする.



サーバ補助型：
　計算サーバが秘密計算処理を行い，ユーザは入出力のみに関わる.



安全性

- 安全性の根拠
  - 計算量的安全性　：何らかの困難性の仮定に依存
  - 情報理論的安全性：困難性の仮定が不要
- 攻撃者のふるまい
  - semi-honest：プロトコルには従う
  - malicious　：プロトコルに従わないことがある
- 結託
  - 参加者のうちの何人かが協力して情報を得ようとする

効率性

- 通信コスト：もっとも重要な指標
  - 通信回数：何回の通信が必要か
  - 通信量　：何ビットの通信が必要か

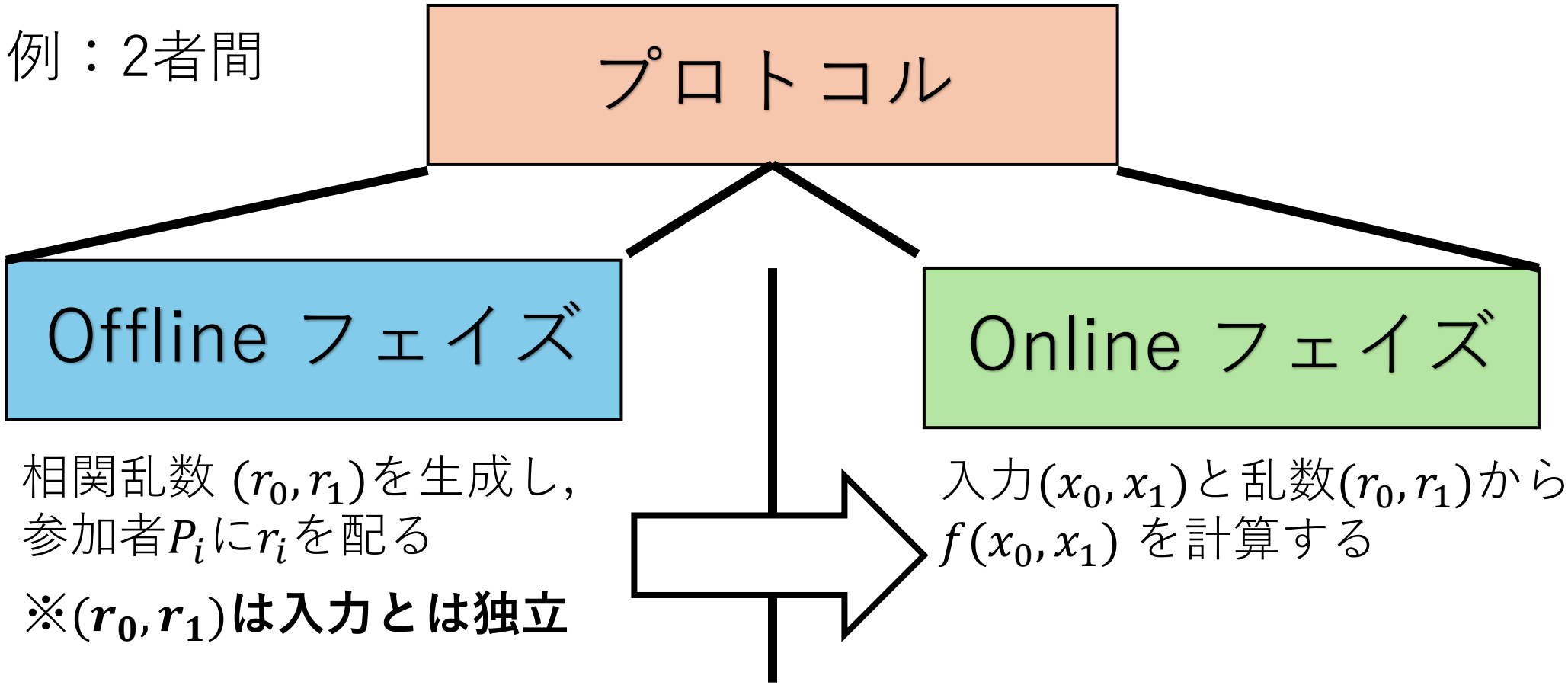
- 計算量

- 乱数長　⇦ CRモデル(事前計算モデル)では重要な指標

CRモデル(事前計算モデル)

入力に依らない相関乱数(Correlated Randomness, CR)を事前計算するモデル

例：2者間



CRモデル(事前計算モデル)

- メリット：
  - (第三者が事前計算をする設定で)任意の関数が**“安全に”**計算可能
    - 情報理論的安全性 + semi-honest安全
  - 通信コスト（通信回数，通信量）を削減可能

- デメリット：
  - 事前計算のコストが生じる
    - 例：莫大なサイズのCRが必要

例：秘密分散を用いた2者間秘密計算

値は$\{0,1\}$の元とする.

秘密分散：情報を複数に“分割”して隠す暗号技術

分散の仕方

$$x \to [x] = ([x]_0, [x]_1) \quad \text{s.t.} \quad x = [x]_0 \oplus [x]_1$$

xのシェアと呼ばれる.

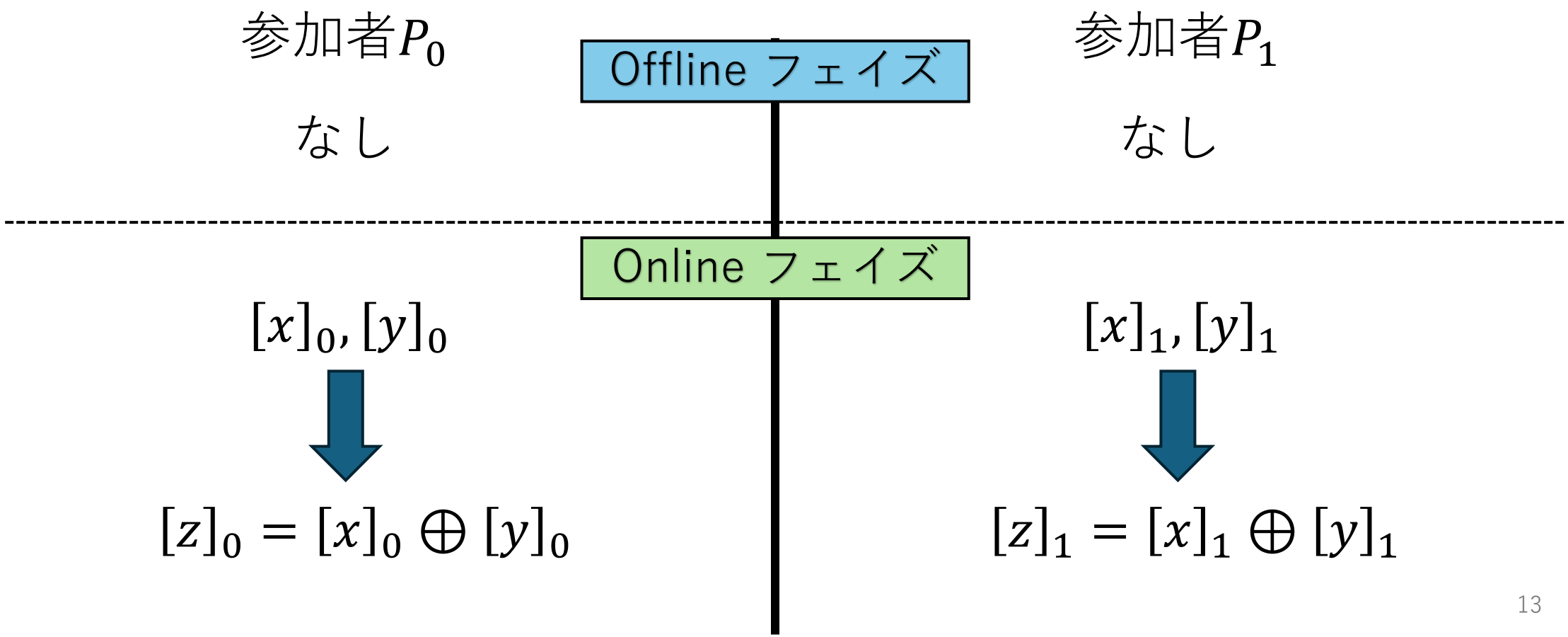
足すと復元できる.

以降，入出力がシェア形式のXOR, AND演算を構成していく.

⇒ これらの組み合わせで，任意の論理回路が計算できる

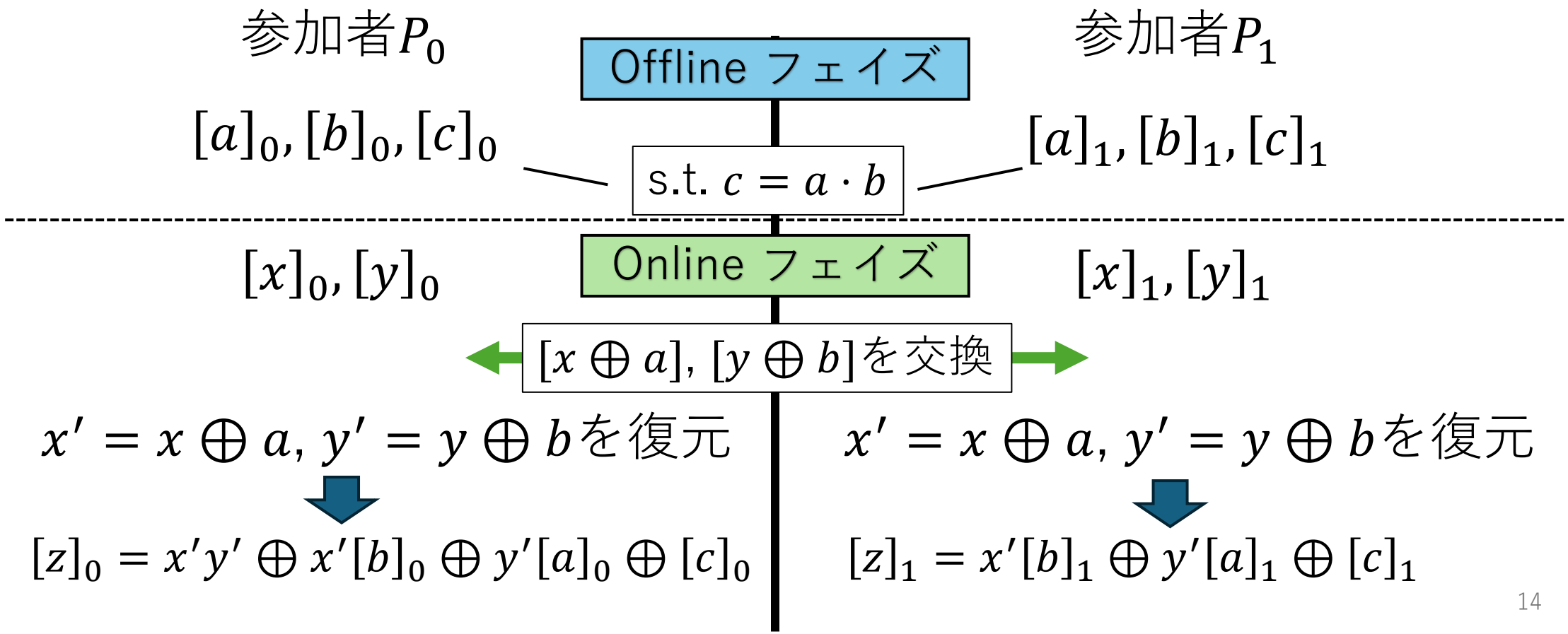
例：秘密分散を用いた2者間秘密計算

XOR演算：$[x], [y] \mapsto [z], z = x \oplus y$



例：秘密分散を用いた2者間秘密計算

AND演算：$[x], [y] \mapsto [z], z = x \cdot y$



例：秘密分散を用いた2者間秘密計算

安全性：

途中で得られる情報は$x \oplus a, y \oplus b$

➡ a, bが一様ランダムなので，これらも一様ランダム

正当性：

$$[z]_0 = x'y' \oplus x'[b]_0 \oplus y'[a]_0 \oplus [c]_0$$
$$[z]_1 = \quad x'[b]_1 \oplus y'[a]_1 \oplus [c]_1$$

➡
$$z = x'y' \oplus x'b \oplus y'a \oplus c$$
$$= (x' \oplus a)(y' \oplus b)$$
$$= xy$$

$\because c = a \cdot b$

(後半) 研究紹介

最適な通信量の2者間秘密計算における乱数長について

CRモデル(再掲)

- メリット：
  - (第三者が事前計算をする設定で)任意の関数が**“安全に”**計算可能
    - 情報理論的安全性 + semi-honest安全
  - 通信コスト（通信回数，通信量）を削減可能

- デメリット：
  - 事前計算のコストが生じる
    - 例：莫大なサイズのCRが必要

トレードオフ

トレードオフの例

回路Cやドメインが$[N] \times [N]$の関数をシェア出力の形式で計算

	通信回数	通信量	乱数長
[Beaver91]	$O(\mathrm{depth}(C))$	$O(\mathrm{size}(C))$	$O(\mathrm{size}(C))$
[IKM+13]	1	$\log N$	$O(N^2)$
[BIKK14]	2	$O(\sqrt{N})$	$O(\sqrt{N})$

赤字：最適な値

上記は具体的な構成(上界)によるもの.

下界が気になる.

e.g., 通信コストを変えずに，乱数長を$o(N^2)$にはできない?

示したこと

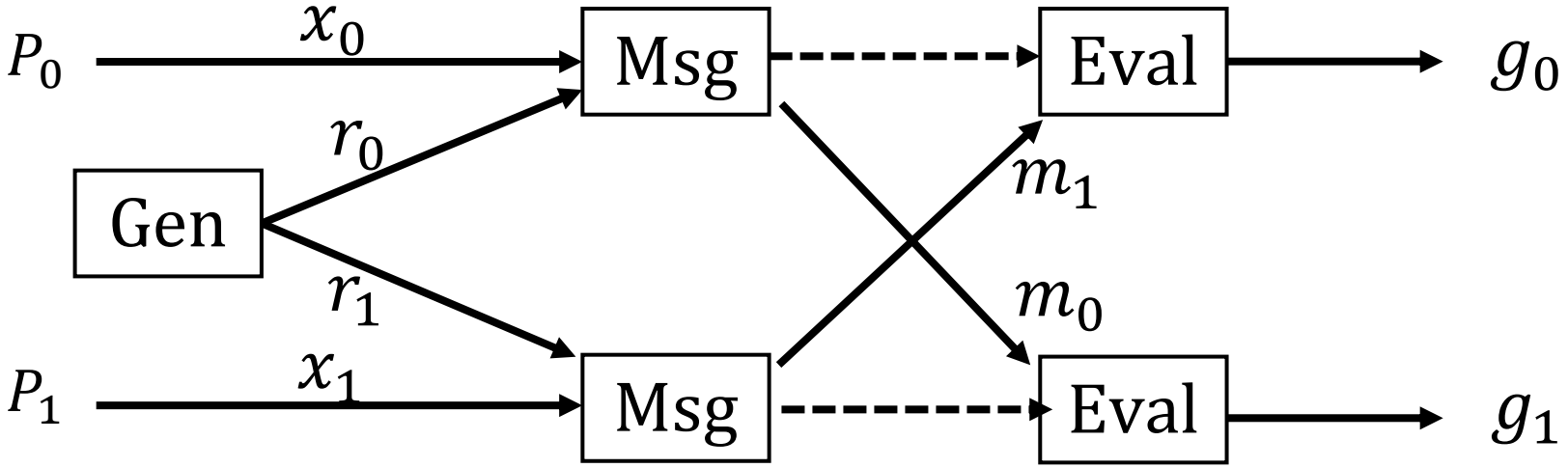
- 通信回数：1回, 通信量：$\log N \Rightarrow$乱数長：$\Omega(N^2)$
  となる関数が存在
  - 通信コストが最適という条件の下での，[IKM+13]の最適性

- 通信量：$\log N \Rightarrow$乱数長：$\Omega(N)$
  となる関数が存在.
  - 通信量が最適という条件でも，指数サイズの乱数長が必要

準備

シンタックス

- $f: X \times X \to G$, G：可換群
- fに対するオンライン最適な2者間秘密計算:
  - Gen : $\emptyset \to CR \subseteq R \times R$, R：乱数空間
  - Msg : $X \times R \to M$, M：メッセージ空間
  - Eval : $X \times M \times R \to G$



満たすべき性質

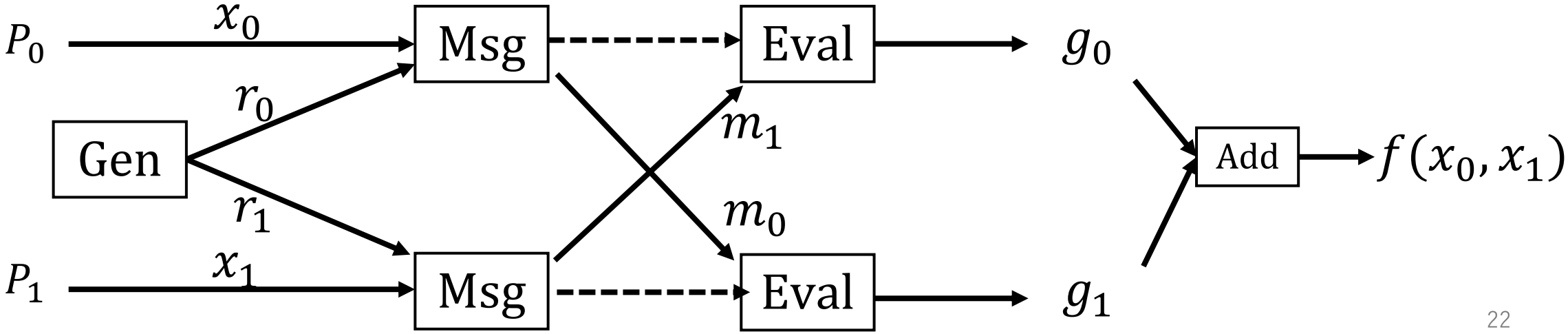
- 最適性：$\#M = \#X$
- 正当性：

$$\mathrm{Eval}(x_0, m_1, r_0) + \mathrm{Eval}(x_1, m_0, r_1) = f(x_0, x_1)$$

ただし$m_b = \mathrm{Msg}(x_b, r_b)$

- 安全性：

$(m_b, r_{\bar{b}})$ の分布がx_bに依存しない.



使用する補題

Lemma 1

任意の $r \in R$に対して, $\mathrm{Msg}(\cdot, r): X \to M$ は全単射.

Lemma 2

任意の $r_b \in R, (x, m) \in X \times M$に対して,
$(r_0, r_1) \in CR, \mathrm{Msg}(x, r_{\bar{b}}) = m$ を満たす$r_{\bar{b}} \in R$が存在する.

行列表現 (1/2)

$P_r, E_r : X \times M$ 行列

$$P_r[x, m] = \begin{cases} 1 & (\mathrm{Msg}(x, r) = m) \\ 0 & (\text{otherwise}) \end{cases}$$

$$E_r[x, m] = \mathrm{Eval}(x, m, r)$$

$$\Rightarrow E_{r_0} P_{r_1}^{\mathrm{T}}[x_0, x_1] = \mathrm{Eval}(x_0, m_1, r_0),\ m_1 = \mathrm{Msg}(x_1, r_1)$$

正当性の要件 $\Leftrightarrow \forall (r_0, r_1) \in CR\ , E_{r_0} P_{r_1}^{\mathrm{T}} + P_{r_0} E_{r_1}^{\mathrm{T}} = \underline{F}$

$[x_0, x_1]$成分が$f(x_0, x_1)$である行列

行列表現 (2/2)

P_rは置換行列（∵ Lemma 1より$\mathrm{Msg}(\cdot, r)$は全単射）

正当性の要件$\Leftrightarrow \forall (r_0, r_1) \in CR\ , E_{r_0} P_{r_1}^{\mathrm{T}} + P_{r_0} E_{r_1}^{\mathrm{T}} = F$

$\Leftrightarrow \forall (r_0, r_1) \in CR\ \ A_{r_0} + A_{r_1}^{\mathrm{T}} = P_{r_0}^{\mathrm{T}} F P_{r_1}$

乱数長の下界

主定理

$F = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & & \vdots \\ \vdots & & \ddots & \vdots \\ 0 & & \cdots & 0 \end{pmatrix}$ となるFを考える

Theorem

Let $r \in R$ satisfy $\mathrm{Msg}(0, r) = 0$.
$\Rightarrow \forall i, j \in \{1, \ldots, N-1\}, \exists r' \in R$ s.t. $\mathrm{Msg}(0, r') = 0$ and

$$A_r + A_{r'} = \left(\begin{array}{c|ccc} * & & * & \\ \hline & 0 & \cdots & 0 \\ * & \vdots & & 1 \\ & 0 & \cdots & 0 \end{array}\right)$$

j-th

i-th

証明 (1/4)

Observation:

$$A_{r_0} + A_{r_1}^{\mathrm{T}} = P_{r_0}^{T} F P_{r_1} = \begin{pmatrix} 0 & \vdots & 0 \\ & 1 & \cdots \\ 0 & & 0 \end{pmatrix}$$

$\mathrm{Msg}(0, r_1)$-th

$\mathrm{Msg}(0, r_0)$-th

証明 (2/4)

Lemma 2より

- $\exists r_1$ s.t. $(r, r_1) \in CR$ and $\mathrm{Msg}(0, r_1) = j$
- $\exists r''$ s.t. $(r'', r_1) \in CR$ and $\mathrm{Msg}(0, r'') = i$

$$A_r + A_{r''} = (A_r + A_{r_1}^{\mathrm{T}}) + (A_{r''} + A_{r_1}^{\mathrm{T}}) =$$

$$\begin{pmatrix} & \mathrm{Msg}(0,r_1) = j\text{-th} & \\ 0 & 1 \cdots 0 & \cdots \mathrm{Msg}(0, r) = 0\text{-th} \\ & \vdots & \\ & 1 & \cdots \mathrm{Msg}(0, r'') = i\text{-th} \\ 0 & & 0 \end{pmatrix}$$

Goal : Find r' s.t.

$$\mathrm{Msg}(0, r') = 0 \text{ and } A_r + A_{r'} =$$

$$\left(\begin{array}{c|ccc} * & & j\text{-th} & \\ & * & & \\ \hline * & 0 & \cdots & 0 \\ \vdots & \vdots & & \\ * & 0 & 1 & \cdots i\text{-th} \\ & 0 & \cdots & 0 \end{array}\right)$$

証明 (3/4)

Lemma 2より

- $\exists r_1'$ s.t. $(r'', r_1') \in CR$ and $\mathrm{Msg}(0, r_1') = 0$
- $\exists r'$ s.t. $(r', r_1') \in CR$ and $\mathrm{Msg}(0, r') = 0$

$$A_{r'} + A_{r''} = (A_{r'} + A_{r_1'}^{\mathrm{T}}) + (A_{r''} + A_{r_1'}^{\mathrm{T}}) = \begin{pmatrix} & \mathrm{Msg}(0, r_1') = 0\text{-th} & \\ \vdots & & \\ 1 & \cdots\cdots & 0 \cdots \mathrm{Msg}(0, r') = 0\text{-th} \\ \vdots & & \\ 1 & \cdots\cdots & \mathrm{Msg}(0, r'') = i\text{-th} \\ 0 & & 0 \end{pmatrix}$$

Goal : Find r' s.t.

$$\mathrm{Msg}(0, r') = 0 \text{ and } A_r + A_{r'} = \begin{pmatrix} & & j\text{-th} & \\ * & * & & \\ \hline & 0 \cdots & 0 & \\ * & \vdots & 1 & \cdots\cdots i\text{-th} \\ & 0 \cdots & 0 & \end{pmatrix}$$

証明 (4/4)

これより,

$$A_r + A_{r'} = \begin{pmatrix} & 0\text{-th} & j\text{-th} & \\ & \vdots & \vdots & \\ & 1 & 1 & 0 \quad 0\text{-th} \\ & \vdots & \vdots & \\ & 1 & 1 & i\text{-th} \\ & & & \\ & 0 & & 0 \end{pmatrix}$$

and $\mathrm{Msg}(0, r') = 0$

Goal : Find r' s.t.

$$\mathrm{Msg}(0, r') = 0 \text{ and } A_r + A_{r'} = \begin{pmatrix} & & j\text{-th} & \\ * & * & \vdots & \\ & 0 & 0 & \\ * & \vdots & 1 & i\text{-th} \\ & 0 & 0 & \end{pmatrix}$$

■

乱数長の下界

Let $r \in R$ satisfy $\mathrm{Msg}(0, r) = 0$.
Then, $\forall M \in \{0,1\}^{(N-1)\times(N-1)}$, $\exists r' \in R$ s.t. $\mathrm{Msg}(0, r') = 0$ and

$$A_r + A_{r'} = \left(\begin{array}{c|c} * & * \\ \hline * & M \end{array}\right)$$

$$\#\{A_r + A_{r'} \mid r' \in R\} \geq \#\{0,1\}^{(N-1)\times(N-1)}$$

$$\therefore \text{CR size} \geq (N-1)^2 \text{ bits}$$

オンライン最適 ⟷ 通信量最適

$P_0 \to P_1$のメッセージ

(x_0, r_0)のみに依存	(x_0, r_0) と $(\boldsymbol{x_1}, \boldsymbol{r_1})$に依存

下界

$\forall M, \exists r' \in R$ s.t. $A_r + A_{r'} =$ $\begin{pmatrix} * & * \\ * & M \end{pmatrix}$	$\forall M, \exists r' \in R$ s.t. $A_r + A_{r'} =$ $\begin{pmatrix} * & * \\ M & * \end{pmatrix}$
$\therefore$ CR size $\geq (N-1)^2$ bits	$\therefore$ CR size $\geq \boldsymbol{N-1}$ bits

今後の課題

- “通信量最適”の制約はかなり大きい
  - 例えば，入力長に線形サイズ，制限を緩めるとどうなるか？
- 通信回数↔通信量↔乱数長の定量的なトレードオフ関係
- 参加者の数が増えた場合でも似たような議論ができるか