情報理論的に安全な Secret Handshake

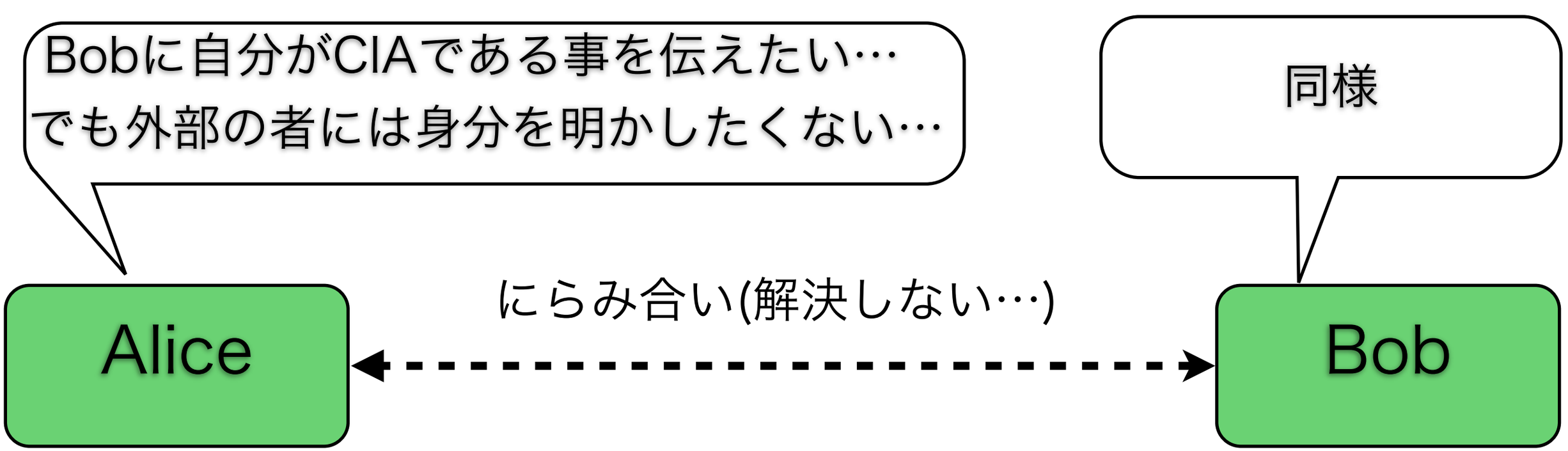
齋藤 匡恭 千葉大学大学院 理学研究科 基盤理学専攻
多田 充　千葉大学 統合情報センター

研究目的

- **Secret Handshakeについて**

- プライバシー保護を考慮された認証方式[D.Balfanzら, 2003]
- 互いが所属するグループが同じであれば認証
  そうでなければ互いのグループ情報が一切分からない

例：Alice, BobはCIAの職員



Secret Handshakeはこのような問題を解決できる

研究目的

- **Secret Handshakeについて**

- Secret Handshakeは２つのフェーズで構成される

鍵共有のために利用する暗号系として様々な方式が提案されている

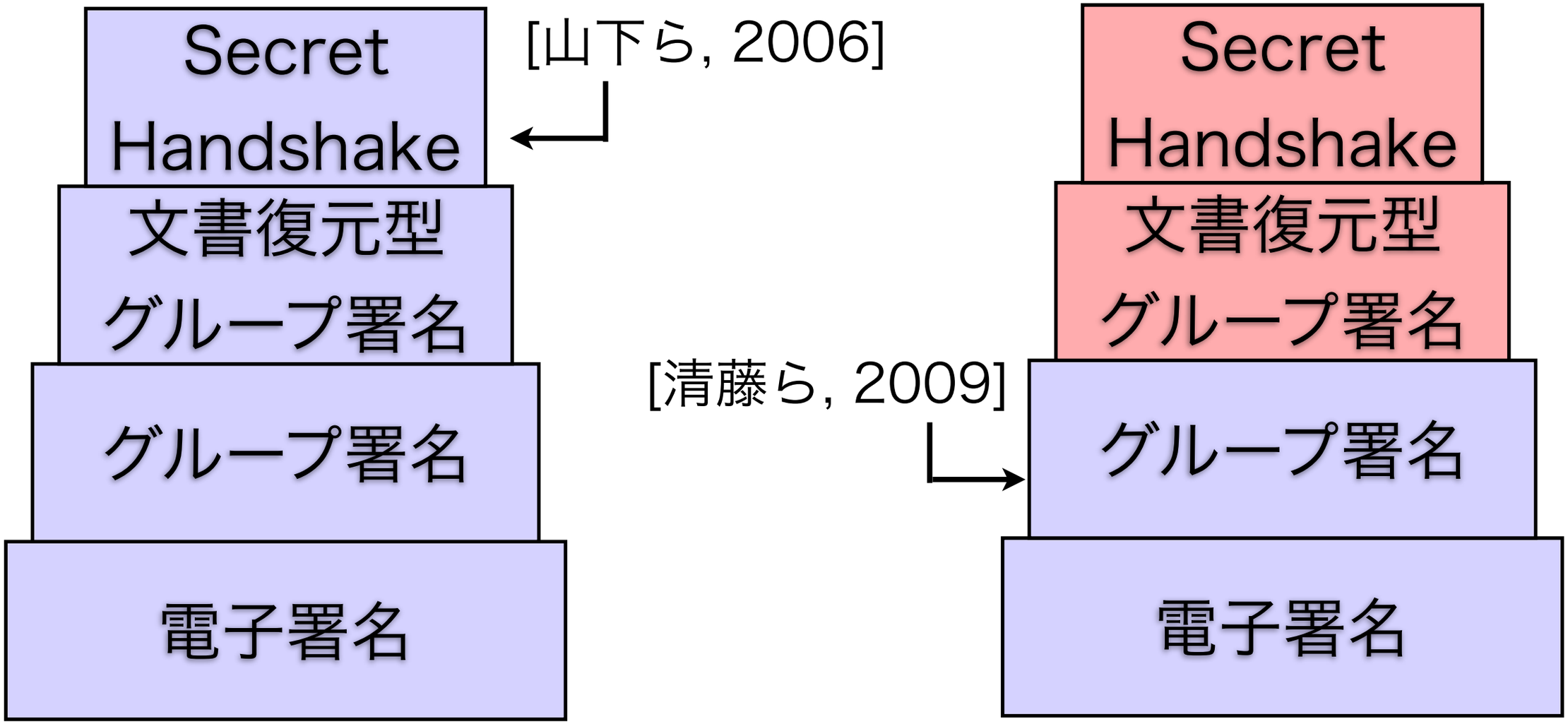
研究目的

- **代表的な既存研究と提案内容**

提案者	利用する暗号系	安全性
[D.Balfanzら, 2003]	ペアリング	計算量的
[Xuら, 2004]	RSA暗号	計算量的
[山下ら, 2006]	グループ署名	計算量的
提案方式	グループ署名	情報理論的

研究目的

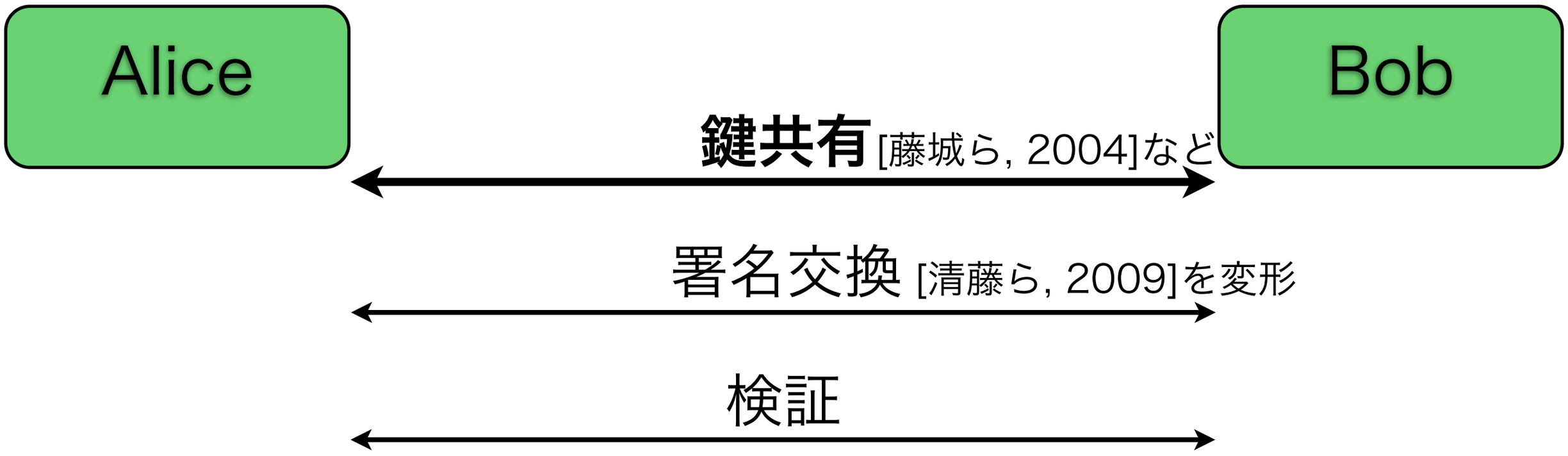
- **既存研究と提案内容**



研究目的

- **提案内容**

- 提案するSecret Handshakeの構成

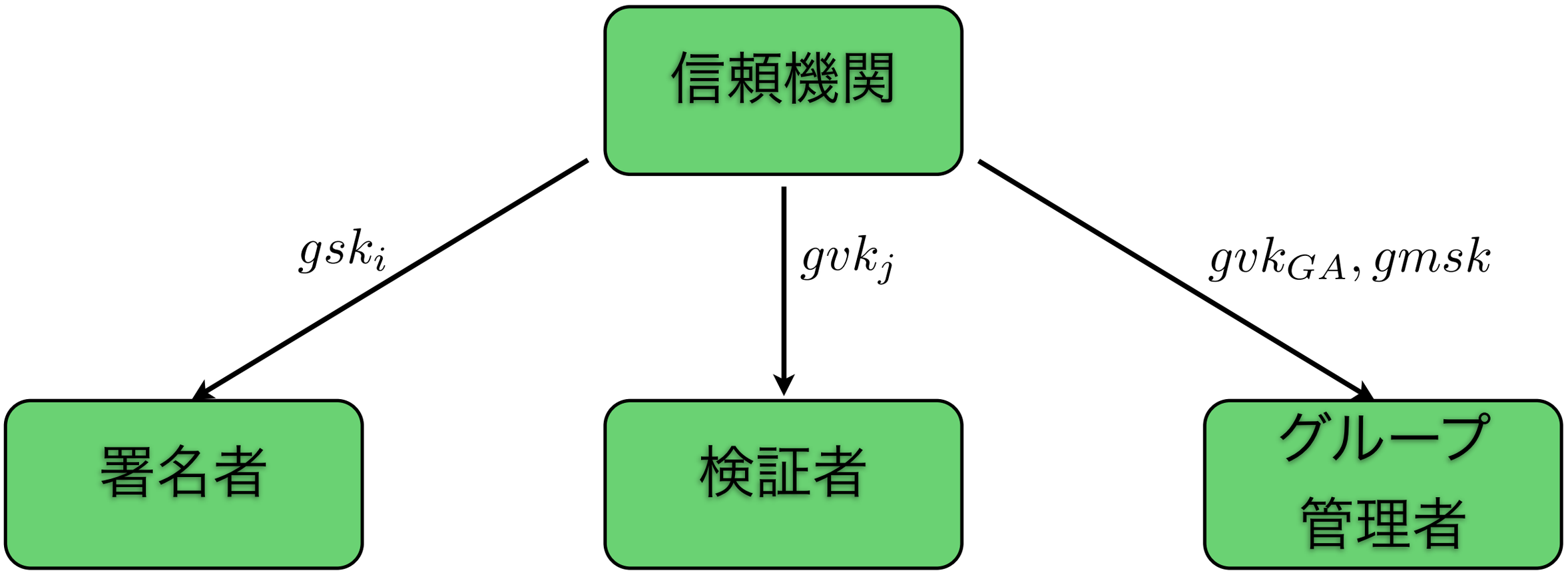


これだけでは安全性の性質は満たされなかった

そこで、署名交換の上に更に鍵共有を行うという流れにする

準備

- **情報理論的に安全なグループ署名(USGS) [清藤ら, 2009]**
  - グループ署名の性質を保持しつつ、安全性を情報理論的に保つ



これらは安全な通信路を用いて送られる

鍵生成 1/2 [清藤ら, 2009]

TA: $k$bitの素数のべき乗$q(\geq n_1(t_1+1))$を選び、有限体F_q, F_{q^2}を構成

$f(0,0)=0$となるような全単射の関数$f: F_q^2 \to F_q$ を構成

以下、署名者S_i のIDをS_iと書く これは各署名者ごとに異なる

多項式$F^{(d)}(Y) \in F_q, G_d(X, Y_1, \ldots, Y_{\omega+1}, Z) \in F_{q^2}$ $(0 \leq d \leq t_1)$ を以下のように構成

$$F^{(d)}(Y) = \sum_{j=0}^{n_1-1} a_j^{(d)} Y^j$$

$$G_d(X, Y_1, \ldots, Y_{\omega+1}, Z) = \sum_{i=0}^{n_1-1} \sum_{k=0}^{1} \delta_{i,0,k}^{(d)} X^i Z^k + \sum_{i=0}^{n_1-1} \sum_{j=1}^{\omega+1} \sum_{k=0}^{1} \delta_{i,j,k}^{(d)} X^i Y_j Z^k$$

$$a_j^{(d)} \overset{\$}{\in} F_q, \delta_{i,j,k}^{(d)} \overset{\$}{\in} F_{q^2}$$

鍵生成 2/2 [清藤ら, 2009]

$c_{i,d} = S_i + F^{(d)}(Y)|_{Y=\eta_{i,d}}, \mu_{i,d} = f(c_{i,d}, \eta_{i,d})$を計算($\eta_{i,d} \overset{\$}{\in} F_q \ (\eta_{i,d} \neq 0)$)

$v_j^{(d)} \overset{\$}{\in} F_q^{\omega+1}$ を選び、以下のように鍵を計算する

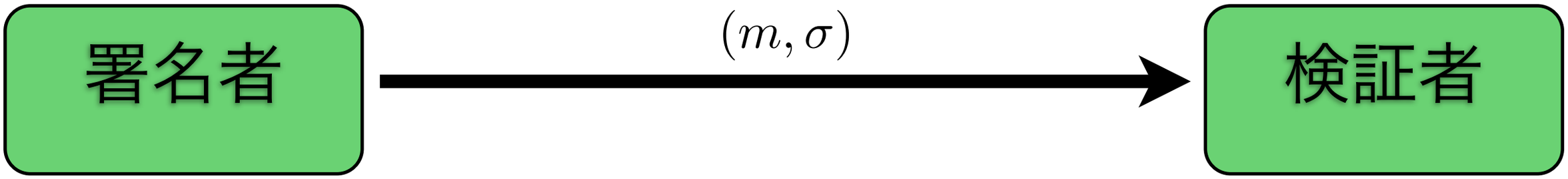
$$gsk_i^{(d)} = (c_{i,d}, \eta_{i,d}, G_d(\mu_{i,d}, Y_1, \ldots, Y_{\omega+1}, Z)) \ (0 \leq d \leq t_1)$$

$$gvk_j^{(d)} = (G_d(X, v_j^{(d)}, Z), v_j^{(d)})$$

$$gmsk^{(d)} = F^{(d)}(Y)$$

準備

- **情報理論的に安全なグループ署名(USGS) [清藤ら, 2009]**
  - グループ署名の性質を保持しつつ、安全性を情報理論的に保つ



$\mathrm{GSign}(gsk_i, m) \rightarrow \sigma$

$\alpha_d(Y_1, \ldots, Y_{\omega+1})$
$:= G_d(\mu_{i,d}, Y_1, \ldots, Y_{\omega+1}, Z)|_{Z=m}$
$(0 \leq d \leq t_1)$
$\sigma = (\alpha_d(Y_1, \ldots, Y_{\omega+1}), c_{i,d}, \mu_{i,d})$

$\mathrm{GVerify}(gvk_j, m, \sigma) \rightarrow \{\mathrm{accept}, \mathrm{reject}\}$

$\phi_1^{(d)} := \alpha_d(Y_1 \ldots, Y_{\omega+1})|_{Y_1 \ldots, Y_{\omega+1}=v_j}$
$\phi_2^{(d)} := G_d(X, v_j^{(d)}, Z)|_{X=f(c_{i,d},\eta_{i,d}),Z=m}$
$\phi_1^{(d)} \stackrel{?}{=} \phi_2^{(d)}$ i.e. $\dfrac{\phi_1^{(d)}}{\phi_2^{(d)}} \stackrel{?}{=} 1$

準備

- **情報理論的に安全なグループ署名(USGS) [清藤ら, 2009]**

  - USGSの安全性

USGSは以下の安全性を持つ

- **Unforgeability**
- **Anonymity**
- **Unlinkability**
- **Traceability**
- **Exculpability**
- **Undeniability**
- **Coalition Registance**
- **Framing**

今後構成する文書復元型グループ署名の安全性は
USGSの安全性に帰着される

準備

- **情報理論的に安全な**
  文書復元型グループ署名(USGS with MR)
  - 文書復元型グループ署名の性質を
    保持しつつ、安全性を情報理論的に保つ

署名者 → (r, σ) → 検証者

$\mathrm{MGSign}(gsk, r, m) \to \sigma$

$m_{i,0}, m_{i,1}, \ldots, m_{i,t_1-1} \overset{\$}{\in} F_{q^2},$

$m_{i,t_1} := m_{i,0} \oplus \cdots \oplus m_{i,t_1-1} \oplus m$

$\alpha_d(Y_1, \ldots, Y_{\omega+1})$

$:= m_{i,d} G_d(\mu_{i,d}, Y_1, \ldots, Y_{\omega+1}, Z)|_{Z=r}$

$(0 \le d \le t_1)$

$\sigma = (\alpha_d(Y_1, \ldots, Y_{\omega+1}), c_{i,d}, \mu_{i,d})_{0 \le d \le t_1}$

$\mathrm{MGVerify}(gvk, r, \sigma) \to m$

$\phi_1^{(d)} := \alpha_d(Y_1 \ldots, Y_{\omega+1})|_{Y_1 \ldots, Y_{\omega+1}=v_j}$

$\phi_2^{(d)} := G_d(X, v_j^{(d)}, Z)|_{X=f(c_{i,d},\eta_{i,d}), Z=r}$

$m'_{i,d} := \dfrac{\phi_1^{(d)}}{\phi_2^{(d)}}$

$m' := m'_{i,0} \oplus m'_{i,1} \oplus \cdots \oplus m'_{i,t_1}$

準備

- **情報理論的に安全な**
  文書復元型グループ署名(USGS with MR)
  - USGS with MRの安全性

- **Anonymity**：USGSの性質をそのまま保つ
- **Unlinkability**：USGSの性質をそのまま保つ
- **Traceability**：USGSの性質をそのまま保つ
- **Randomness**：攻撃者が、ランダムに選ばれた文書に対する署名成分とランダムな値を返す文書復元型グループ署名のシミュレータが出力した署名成分と識別することが難しい
- **Unforgeability**：USGSでは存在的偽造不可能であることを示したが、USGS with MRでは存在的偽造可能で、かつ一般的偽造不可能であることを示す必要がある[焦ら, 2007]

準備

- **情報理論的に安全な**
  文書復元型グループ署名(USGS with MR)
  - USGS with MRの安全性

証明

- **存在的偽造可能性**：攻撃者は USGS with MR における署名付き乱数 (r^*, σ^*) をランダムに生成するとする。検証者はこれを検証アルゴリズムを用いて検証すると、必ず文書の形のm^*を復元する。検証者はこれの正当性を検証する能力を持たない。これより、攻撃者は存在的偽造可能である。
- **一般的偽造不可能性**：以下の命題からの背理法で証明とする。

USGS with MRが一般的偽造可能ならばUSGSは存在的偽造可能である。

準備

- **情報理論的に安全な**
  文書復元型グループ署名(USGS with MR)
  - USGS with MRの安全性

証明

USGS with MRが一般的偽造可能なので、攻撃者の結託に含まれないS_iについて、検証アルゴリズムにおいてm_iを出力するような証明付き乱数(r, σ)が偽造可能となる。

今、この性質を利用して、USGSにおいてmを入力としてacceptされるような(m, σ)を偽造したい。mに対して、USGS with MRにおいて、署名者が選択する (r, m) を

$$(r, m) = \begin{cases} (m, 1)(\text{if } t_1 \text{ is odd}) \\ (m, 0)(\text{if } t_1 \text{ is even}) \end{cases}$$

として署名を偽造すると

準備

- **情報理論的に安全な**
  文書復元型グループ署名(USGS with MR)
  - USGS with MRの安全性

証明

得られる署名付き乱数は

$$(m, \sigma)\ (\sigma = (m_d G_d(\mu_{i,d}, Y_1, \ldots, Y_{\omega+1}, Z)|_{m_d=1, Z=m}, c_{i,d}, \eta_{i,d}))$$

となる。このσは、USGSにおいて、mを入力としたときにacceptされるものそのものとなっている。つまり、このσがそのまま求めたいσとして扱うと、偽造可能となる。

しかし、実際にはUSGSは存在的偽造不可能であるので、背理法により、USGS with MRは一般的偽造可能である。

研究目的

- **情報理論的に安全な**
  文書復元型グループ署名(USGS with MR)
  - USGS with MRの安全性

Alice

Bob

署名交換 [清藤ら, 2009]を変形

検証

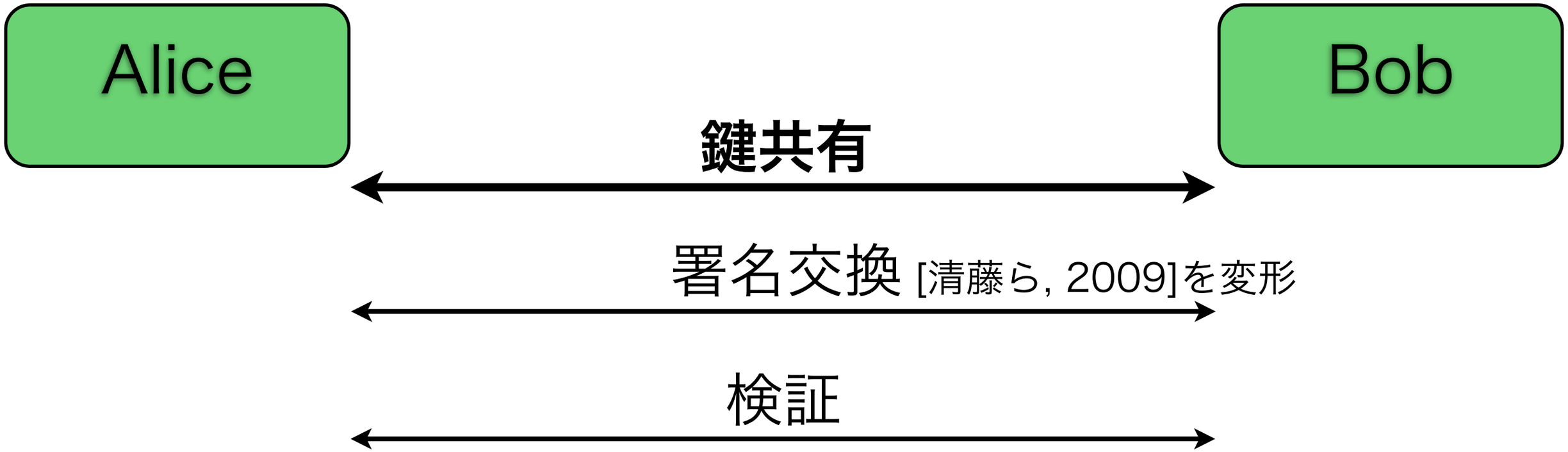
一般的偽造可能⇒グループ外の人間が署名偽造可能

存在的偽造不可能⇒署名からグループ内の人間かどうかが分かってしまう、つまりFairnessを満たさなくなる

しかし、このままでは、署名交換フェーズのやり取りを同グループ内のメンバーが見てしまうと互いの認証結果が分かってしまう

研究目的

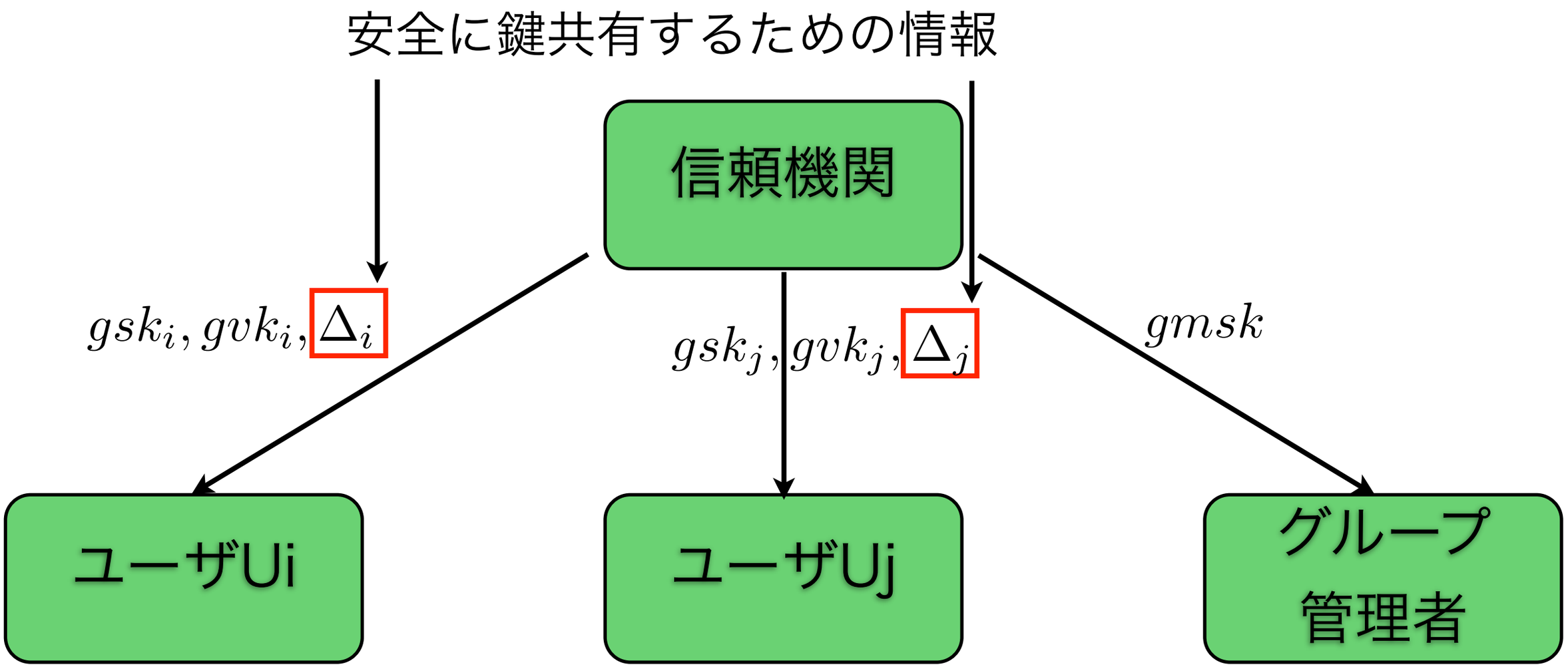
- **情報理論的に安全な**
  文書復元型グループ署名(USGS with MR)
  - USGS with MRの安全性



そこで、署名交換の前に鍵を共有させて検証フェーズに用いる事で、検証結果をグループ内の人間にも分からないようにする

Secret Handshake

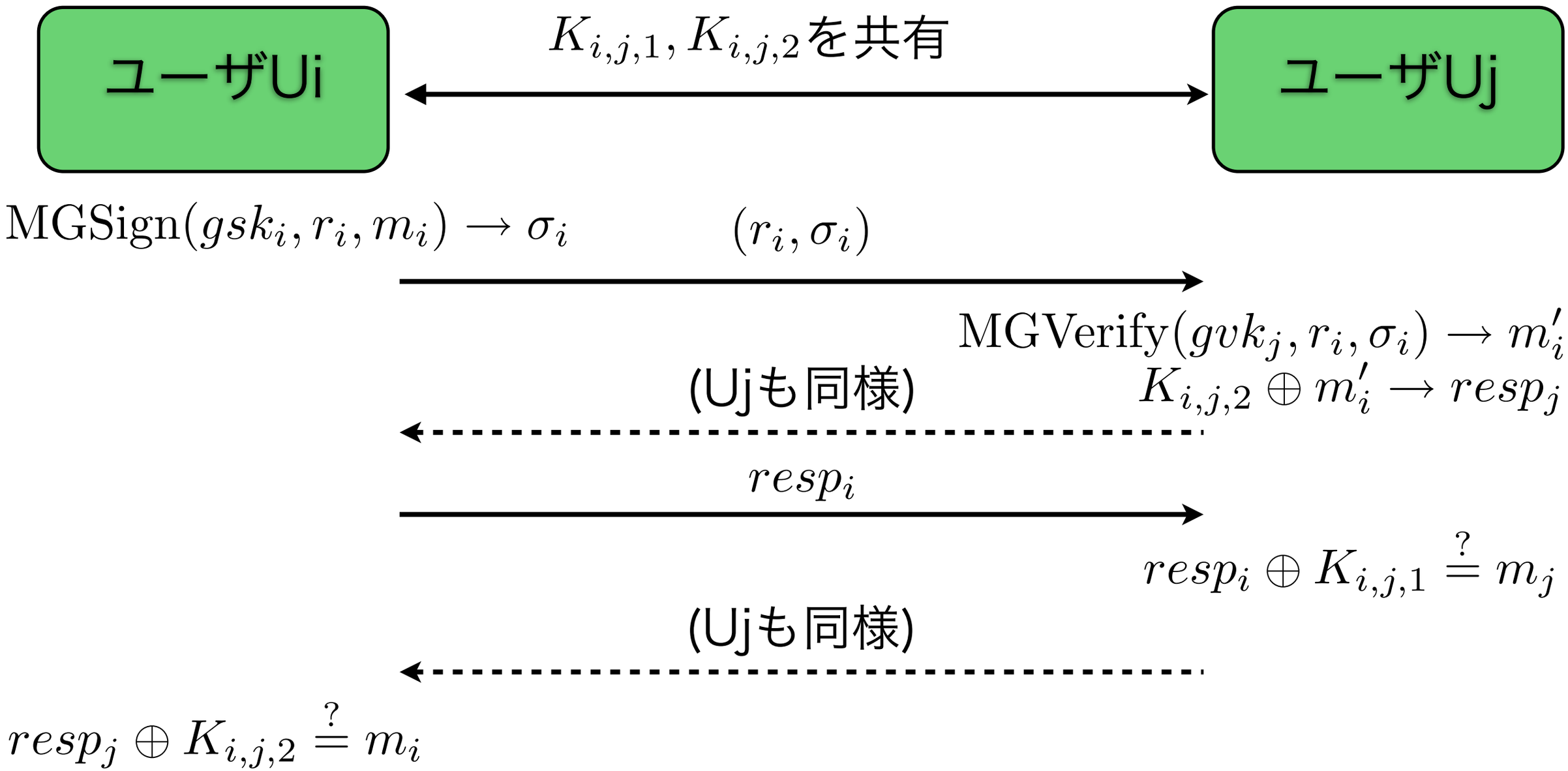
- **構成法**



これらは安全な通信路を用いて送られる

Secret Handshake

- **構成法**



Secret Handshake

- **安全性(必要なもの)**

- **Correctness(CO)**：同グループに所属する正規のユーザ同士で通信を行うと互いにacceptを出力
- **Impersonator Resistance(IR)**：グループGに所属していない攻撃者がGの正当なメンバーと通信した場合、acceptを返すことが難しい
- **Dececter Resistance(DR)**：攻撃者が正当なメンバーとランダムな系列を返すシミュレータとを区別する事が難しい
- **Indistinguishability to Eavesdroppers(IE)**：G内のメンバー同士の通信をG内の攻撃者が見ても、そのプロトコルが受理されたかどうかを区別する事が難しい

Secret Handshake

- **安全性(満たす事が望ましいもの)**

- **Unlinkability(Unlink)**：正当なメンバーが参加した2つの通信履歴に対して、たとえグループ外の攻撃者が通信に参加していたとしても、それらを関連付ける事が難しい
- **Traceability(TR)**：成功した通信履歴からグループ管理者は参加者を特定できる
- **Fairness(FN)**：たとえ片方が途中で通信を中断したり、事故により通信が途絶えたとしても、グループ情報を一方的に奪われない

提案方式ではTRを満たし、必要な安全性と,FNにおいて完全秘匿であり、Unlinkにおいては $\epsilon = \frac{2}{q}$ で準完全秘匿であることを示した。

Secret Handshake

- **安全性(満たす事が望ましいもの)**

- **完全秘匿**：攻撃者に情報が漏れる前と後の情報エントロピー、もしくは確率分布の差がない[Shannon, 1964]
- **準完全秘匿**： 攻撃者に情報が漏れる前と後の情報エントロピー、もしくは確率分布の差が小さい量 ϵ で抑えられる[四方ら, 2004]

まとめ

- 情報理論的に安全なSecret Handshakeの構成法の提案と安全性の検証

今後の課題

- Secret Handshakeに適した鍵共有法の検討