リング署名の計算論的に健全な形式化

川本 裕輔 † 櫻田 英樹 ‡ 萩谷 昌己 †

† 東京大学大学院情報理工学系研究科

‡NTT コミュニケーション科学基礎研究所

目次

- 記号的手法と計算論的手法
- リング署名
- 実行モデル
- マッピング健全性
- 識別不能性の健全性
- 結論

プロトコルの解析手法

記号的手法 vs 計算論的手法 (形式的手法)

- Dolev-Yao 項
- 代数的操作

- ビット列
- 確率的多項式時間 (PPT) アルゴリズム

プロトコルの解析手法

記号的手法 vs 計算論的手法 (形式的手法)

- Dolev-Yao 項
- 代数的操作
- 理想的な安全性
- 単純で (半) 自動化

- ビット列
- 確率的多項式時間 (PPT) アルゴリズム
- 計算量理論に基づく
- 難しく間違いやすい

プロトコルの解析手法

記号的手法 vs 計算論的手法 (形式的手法)

- 記号トレース
  (記号的状態遷移列)
- 状態遷移: 項のやり取り

- 計算論的トレース
  (計算論的状態遷移列)
- 状態遷移: ビット列のやり取り

計算論的健全性

記号的手法 $\Longrightarrow$ 計算論的手法

計算論的健全性

計算論的健全性

記号的手法 $\Longrightarrow$ 計算論的手法

計算論的健全性

1. マッピング健全性 [Micciancio-Warinschi'04]

各計算論的トレースに対して，圧倒的な確率で，
対応する記号トレースが存在する.

対応とは...

- 状態遷移の種類が同じ.
- 計算論的トレースに現れるビット列に対して，項を返す写像が存在.

計算論的健全性

記号的手法 $\Longrightarrow$ 計算論的手法

計算論的健全性

1. マッピング健全性 [Micciancio-Warinschi'04]

各計算論的トレースに対して，圧倒的な確率で，
対応する記号トレースが存在する.

$\Downarrow$ 対偶

項 m が任意の記号トレースで導出できないならば，

ビット列 $[\![m]\!]$ が計算論的トレースに現れる確率が無視できる.

計算論的健全性

記号的手法 $\Longrightarrow$ 計算論的手法

計算論的健全性

1. マッピング健全性 [Micciancio-Warinschi'04]

各計算論的トレースに対して，圧倒的な確率で，
対応する記号トレースが存在する.

- 「トレースの集合」で表される安全性 (例: 偽造不能性) には有用.
- 「トレースの確率分布の間の識別不能性」で表される安全性
  (例: 匿名性) には直接役立たない.

計算論的健全性

記号的手法 $\Longrightarrow$ 計算論的手法

計算論的健全性

1. マッピング健全性 [Micciancio-Warinschi'04]

各計算論的トレースに対して，圧倒的な確率で，
対応する記号トレースが存在する．

2. 記号的識別不能性の健全性 [Abadi-Rogaway'00]

$$\mathbf{Exec}^{s,\leq h}(\Pi_0) \cong \mathbf{Exec}^{s,\leq h}(\Pi_1) \Longrightarrow \mathbf{Exec}^{c,h}_{\Pi_0(\cdot),\mathcal{A}(\cdot)}(\eta) \approx \mathbf{Exec}^{c,h}_{\Pi_1(\cdot),\mathcal{A}(\cdot)}(\eta)$$

記号的識別不能性　　計算論的識別不能性

研究の概要

リング署名に対する２種類の計算論的健全性

1. マッピング健全性 [Micciancio-Warinschi'04]

各計算論的トレースに対して，圧倒的な確率で，
対応する記号トレースが存在する．

2. 記号的識別不能性の健全性 [Abadi-Rogaway'00]

$$\mathbf{Exec}^{s,\leq h}(\Pi_0) \cong \mathbf{Exec}^{s,\leq h}(\Pi_1) \implies \mathbf{Exec}^{c,h}_{\Pi_0(\cdot),\mathcal{A}(\cdot)}(\eta) \approx \mathbf{Exec}^{c,h}_{\Pi_1(\cdot),\mathcal{A}(\cdot)}(\eta)$$

記号的識別不能性　　計算論的識別不能性

目次

- 記号的手法と計算論的手法
- リング署名
- 実行モデル
- マッピング健全性
- 記号的識別不能性の健全性
- 結論

リング署名

検証鍵 (公開鍵): $\mathcal{L} = \{ vk_1, \cdots, vk_6 \}$
署名鍵 (秘密鍵): $sk_1, \cdots, sk_6$

(1 人以上の) 署名者のグループ

署名者 2 $sk_2 vk_2$　　署名者 3 $sk_3 vk_3$

署名者 1 $sk_1 vk_1$　　署名者 4 $sk_4 vk_4$

署名者 6 $sk_6 vk_6$　　署名者 5 $sk_5 vk_5$

リング署名

検証鍵 (公開鍵): $\mathcal{L} = \{ vk_1, \cdots, vk_6 \}$

署名鍵 (秘密鍵): $sk_1, \cdots, sk_6$

(1 人以上の) 署名者のグループ

署名者 2 $sk_2 vk_2$　　署名者 3 $sk_3 vk_3$

署名者 1 $sk_1 vk_1$　　署名者 4 $sk_4 vk_4$

署名者 6 $sk_6 vk_6$　　署名者 5 $sk_5 vk_5$

署名生成

$\sigma := \mathcal{S}(sk_i, \mathcal{L}, m, r)$

検証者

署名検証

$1/0 \leftarrow \mathcal{V}(\mathcal{L}, m, \sigma)$

リング署名

検証鍵 (公開鍵): $\mathcal{L} = \{vk_1, \cdots, vk_6\}$
署名鍵 (秘密鍵): $sk_1, \cdots, sk_6$

(1 人以上の) 署名者のグループ

署名者 2 $sk_2 vk_2$　　署名者 3 $sk_3 vk_3$

署名者 1 $sk_1 vk_1$　　署名者 4 $sk_4 vk_4$

署名者 6 $sk_6 vk_6$　　署名者 5 $sk_5 vk_5$

署名生成

$\sigma := \mathcal{S}(sk_i, \mathcal{L}, m, r)$

検証者

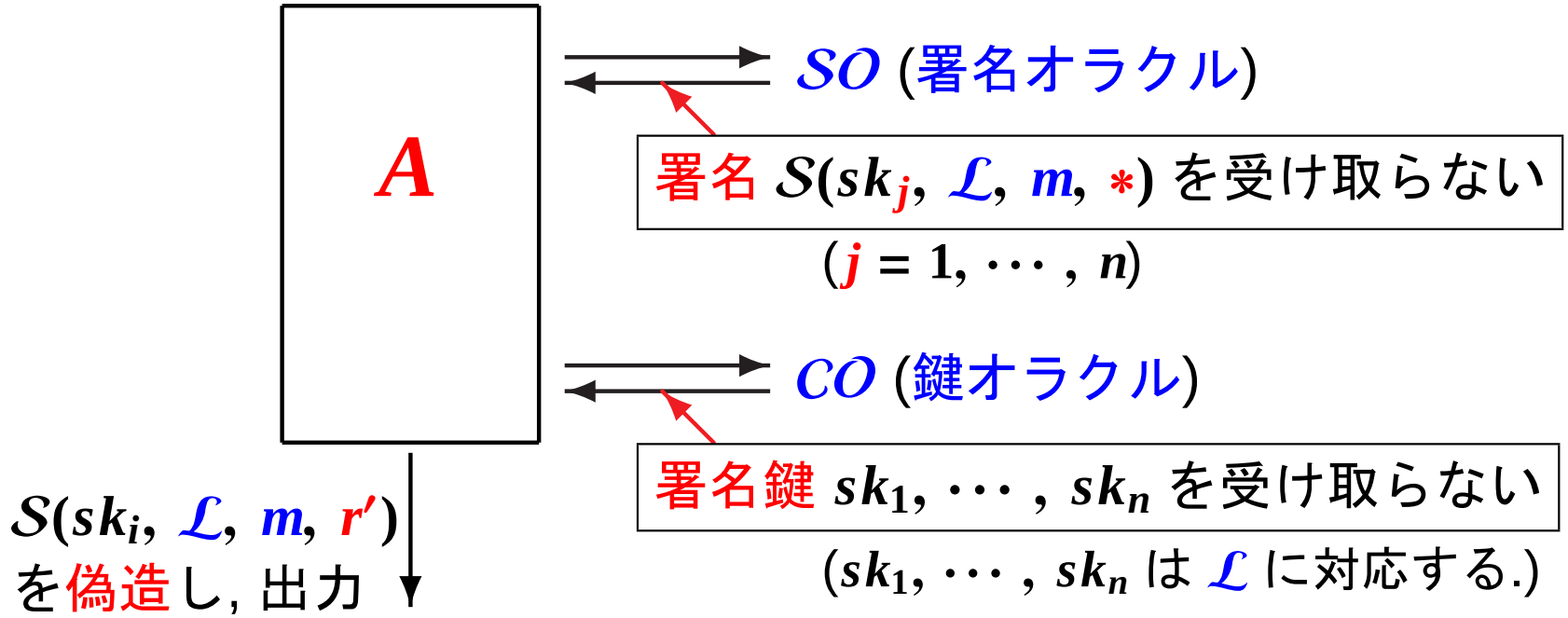
署名検証

$1/0 \leftarrow \mathcal{V}(\mathcal{L}, m, \sigma)$

- $\mathcal{V}(\mathcal{L}, m, \mathcal{S}(sk_i, \mathcal{L}, m, r)) = 1$
- 偽造不能性: 署名鍵がなければ，署名を偽造できない.
- 匿名性: 署名から実際の署名者が分からない.

存在的偽造不能性 [Bender-Katz-Morselli'06]

任意の計算論的攻撃者 A に対して,
次を満たす確率が無視できる.

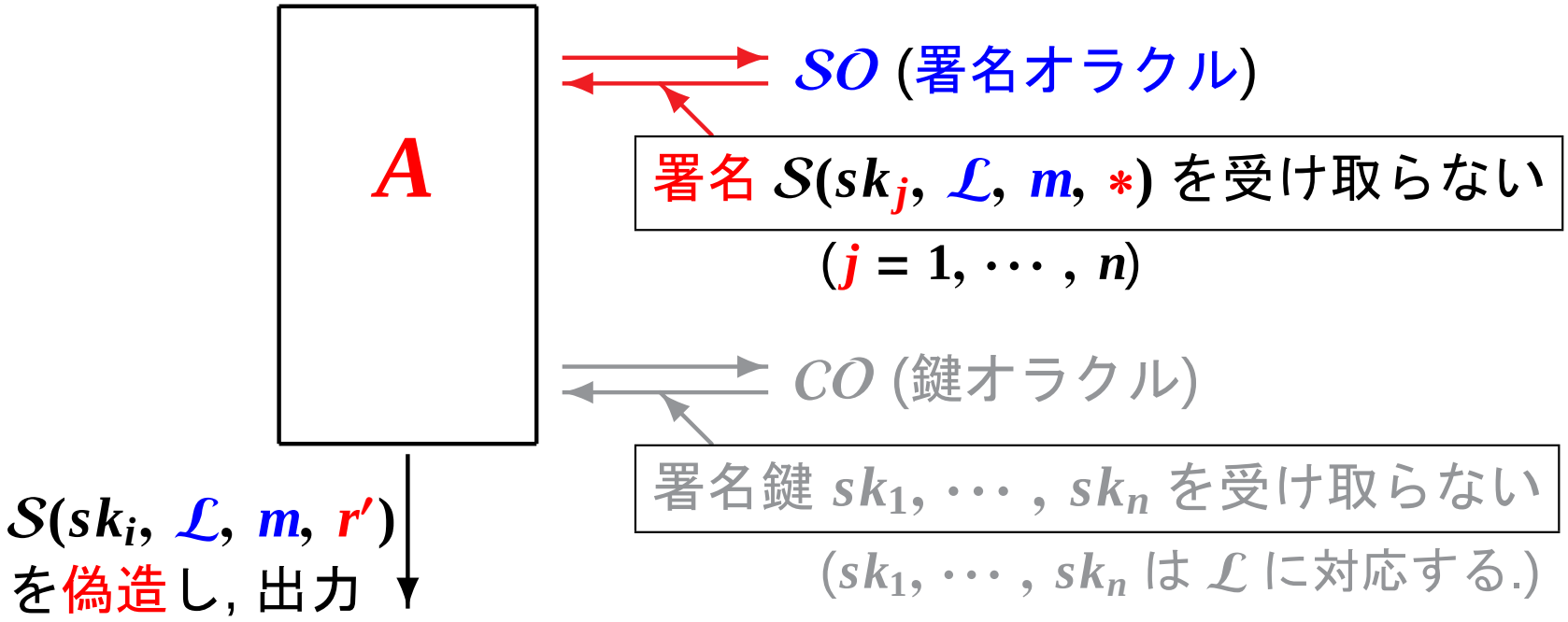


存在的偽造不能性 [Bender-Katz-Morselli'06]

攻撃者 A が,

- 署名 $S(sk_j, \mathcal{L}, m, r)$ から
- 署名 $S(sk_i, \mathcal{L}, m, r')$ を　　$(vk_i \in \mathcal{L})$

生成できたとしても，偽造不能性の定義に矛盾しない.



目次

- 記号的手法と計算論的手法
- リング署名
- 実行モデル
- マッピング健全性
- 記号的識別不能性の健全性
- 結論

実行モデル

[Cortier-Warinschi'05] と同様の記号実行モデル, 計算論的実行モデルを用いる.

- エージェント と適応的能動的攻撃者 がいる.
- 各エージェントは必ずプロトコルに従う.
- 攻撃者は通信路としてモデル化されている.

記号実行モデル

項の定義

Term ∋ $m ::= a \mid g \mid n \mid \mathsf{sk}(a) \mid \mathsf{vk}(a) \mid \mathsf{vk}(g) \mid \langle m, m \rangle \mid [\, m \,]^{R}_{\mathsf{sk}(a),\, \mathsf{VK}(G)}$

a: エージェント ID 記号, g: ゴミメッセージ記号, n: ノンス記号

$\mathsf{sk}(a)$: エージェント a の署名鍵, $\mathsf{vk}(a)$: エージェント a の検証鍵

$\mathsf{vk}(g)$: 偽検証鍵,

$\langle m_1, m_2 \rangle$: m_1 と m_2 のペア

$[\, m \,]^{R}_{\mathsf{sk}(a),\, \mathsf{VK}(G)}$: 署名鍵 $\mathsf{sk}(a)$ と 検証鍵集合 $\mathsf{VK}(G)$ と 乱数 R による, 文書 m の署名.

記号実行モデル

推論規則の定義

$$\frac{}{\varphi \vdash m}\ m \in \varphi \qquad \frac{}{\varphi \vdash a,\ \mathsf{vk}(a)}\ a \in \mathsf{AG} \qquad \frac{}{\varphi \vdash g,\ \mathsf{vk}(g)}\ g \in \mathsf{Garbage}$$

$$\frac{\varphi \vdash \mathsf{vk}(x_1),\ \cdots,\ \varphi \vdash \mathsf{vk}(x_n)}{\varphi \vdash \mathsf{VK}(G)}\ G = \{\, x_1,\ \cdots,\ x_n \,\} \subseteq \mathsf{AG} \cup \mathsf{Garbage}$$

$$\frac{\varphi \vdash m_0 \quad \varphi \vdash m_1}{\varphi \vdash \langle m_0,\ m_1 \rangle} \qquad \frac{\varphi \vdash \langle m_0,\ m_1 \rangle}{\varphi \vdash m_i}\ i = 0,\ 1 \qquad \frac{\varphi \vdash [\, m \,]^{R}_{\mathsf{sk}(a),\,\mathsf{VK}(G)}}{\varphi \vdash [\, m \,]^{R'}_{\mathsf{sk}(b),\,\mathsf{VK}(G)}}\ b \in G,\ R' \in \mathsf{Rand}_{adv}$$

$$\frac{\varphi \vdash \mathsf{sk}(a) \quad \varphi \vdash \mathsf{VK}(G) \quad \varphi \vdash m}{\varphi \vdash [\, m \,]^{R}_{\mathsf{sk}(a),\,\mathsf{VK}(G)}}\ R \in \mathsf{Rand}_{adv},\ a \in G \qquad \frac{\varphi \vdash [\, m \,]^{R}_{\mathsf{sk}(a),\,\mathsf{VK}(G)}}{\varphi \vdash m}$$

記号実行モデルをマッピング健全にするために

計算論的攻撃者 A が,

- 署名 $S(sk_j, \mathcal{L}, m, r)$ から
- 署名 $S(sk_i, \mathcal{L}, m, r')$ を　　$(vk_i \in \mathcal{L})$

生成できたとしても，偽造不能性の定義に矛盾しない.

$$\frac{\varphi \vdash [\, m \,]^{R}_{\mathsf{sk}(a),\mathsf{VK}(G)}}{\varphi \vdash [\, m \,]^{R'}_{\mathsf{sk}(b),\mathsf{VK}(G)}} \quad b \in G,\ R' \in \mathsf{Rand}_{adv}$$

「ある署名から別の署名を生成する操作」は, 計算論的には
具体的に与えられていないが, 禁止されていない.

記号実行モデルをマッピング健全にするために

計算論的攻撃者 A が,

- 署名 $S(sk_j, \mathcal{L}, m, r)$ から
- 署名 $S(sk_i, \mathcal{L}, m, r')$ を　　$(vk_i \in \mathcal{L})$

生成できたとしても，偽造不能性の定義に矛盾しない.

$$\frac{\varphi \vdash [\, m \,]^{R}_{\mathsf{sk}(a),\mathsf{VK}(G)}}{\varphi \vdash [\, m \,]^{R'}_{\mathsf{sk}(b),\mathsf{VK}(G)}} \quad b \in G,\ R' \in \mathsf{Rand}_{adv}$$

もし，この推論規則を入れなければ,
「計算論的攻撃者がある署名から別の署名を作る計算論的トレース」
に対応する記号トレースが存在しないことになる.

目次

- 記号的手法と計算論的手法
- リング署名
- 実行モデル
- マッピング健全性
- 記号的識別不能性の健全性
- 結論

マッピング健全性

各計算論的トレースに対して，圧倒的な確率で，
対応する記号トレースが存在する.

(証明の概要)

- 証明方法は, 先行研究 [Cortier-Warinschi'05] と同様.
- 計算論的トレースに記号トレースが対応しないと仮定して，「署名の偽造不能性を破る計算論的攻撃者」を構成できてしまうことを導く.

目次

- 記号的手法と計算論的手法
- 署名プリミティブ
- 実行モデル
- マッピング健全性
- 記号的識別不能性の健全性
- 結論

記号的識別不能性の健全性

Π_0, Π_1: 存在的偽造不能性 と基本的匿名性 (basic anonymity)
を満たすリング署名を用いたプロトコル

$$\mathbf{Exec}^{s,\leq h}(\Pi_0) \cong \mathbf{Exec}^{s,\leq h}(\Pi_1) \implies \mathbf{Exec}^{c,h}_{\Pi_0(\cdot),\mathcal{A}(\cdot)}(\eta) \approx \mathbf{Exec}^{c,h}_{\Pi_1(\cdot),\mathcal{A}(\cdot)}(\eta)$$

実行トレースの長さ h は, セキュリティパラメータ η と独立な定数.

(h が η に依存する場合は, [Comon-Cortier'08] の枠組みで現在検討中.)

記号的識別不能性の健全性

Π_0, Π_1: 存在的偽造不能性 と基本的匿名性 (basic anonymity)
を満たすリング署名を用いたプロトコル

記号的識別不能性

$$\mathbf{Exec}^{s,\leq h}(\Pi_0) \cong \mathbf{Exec}^{s,\leq h}(\Pi_1) \implies \mathbf{Exec}^{c,h}_{\Pi_0(\cdot),\mathcal{A}(\cdot)}(\eta) \approx \mathbf{Exec}^{c,h}_{\Pi_1(\cdot),\mathcal{A}(\cdot)}(\eta)$$

$$\Updownarrow \textbf{def}$$

1. $\forall\, t_0^s \in \mathbf{Exec}^{s,\leq h}(\Pi_0) \quad \exists\, t_1^s \in \mathbf{Exec}^{s,\leq h}(\Pi_1) \quad t_0^s \cong t_1^s$, and
2. $\forall\, t_1^s \in \mathbf{Exec}^{s,\leq h}(\Pi_1) \quad \exists\, t_0^s \in \mathbf{Exec}^{s,\leq h}(\Pi_0) \quad t_0^s \cong t_1^s$.

$t_0^s \cong t_1^s$: 記号トレース t_0^s と t_1^s の Abadi-Rogaway パターンが
記号的に 識別不能である.

記号的識別不能性の健全性

Π_0, Π_1: 存在的偽造不能性 と基本的匿名性 (basic anonymity)
を満たすリング署名を用いたプロトコル

計算論的識別不能性

$$\mathrm{Exec}^{s,\leq h}(\Pi_0) \cong \mathrm{Exec}^{s,\leq h}(\Pi_1) \implies \mathrm{Exec}^{c,h}_{\Pi_0(\cdot),\mathcal{A}(\cdot)}(\eta) \approx \mathrm{Exec}^{c,h}_{\Pi_1(\cdot),\mathcal{A}(\cdot)}(\eta)$$

$$\Updownarrow \text{def}$$

次が η に関して無視できる.

$$\Pr[t_0^c \leftarrow \mathrm{Exec}^{c,k}_{\Pi_0(\cdot),\mathcal{A}(\cdot)}(\eta) : A(t_0^c, \eta) = 1] - \Pr[t_1^c \leftarrow \mathrm{Exec}^{c,k}_{\Pi_1(\cdot),\mathcal{A}(\cdot)}(\eta) : A(t_1^c, \eta) = 1]$$

目次

- 記号的手法と計算論的手法
- 署名プリミティブ
- 実行モデル
- マッピング健全性
- 記号的識別不能性の健全性
- **結論**

結論

能動的攻撃者の下でリング署名を扱える
記号モデルを提案し，計算論的健全性を示した．

1. マッピング健全性

> 各計算論的トレースに対して，圧倒的な確率で，
> 対応する記号トレースが存在する．

2. 記号的識別不能性の健全性

$$\mathbf{Exec}^{s,\leq h}(\Pi_0) \cong \mathbf{Exec}^{s,\leq h}(\Pi_1) \implies \mathbf{Exec}^{c,h}_{\Pi_0(\cdot),\mathcal{A}(\cdot)}(\eta) \approx \mathbf{Exec}^{c,h}_{\Pi_1(\cdot),\mathcal{A}(\cdot)}(\eta)$$

今後の課題

より多くの暗号プリミティブに対して,

計算論的に健全な記号モデルを与える

ための一般的な方法を得ることを目指す.

ご清聴ありがとうございました.