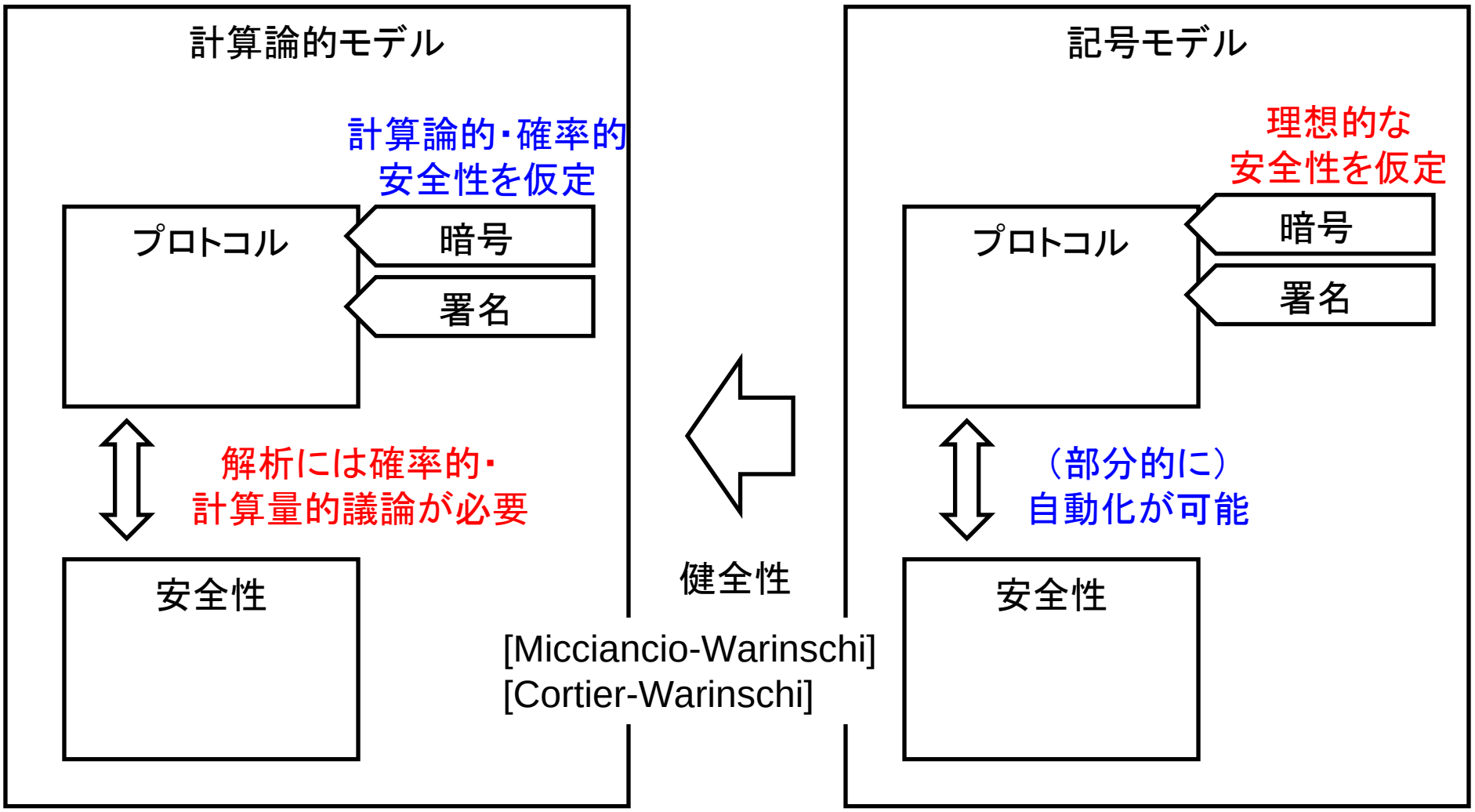
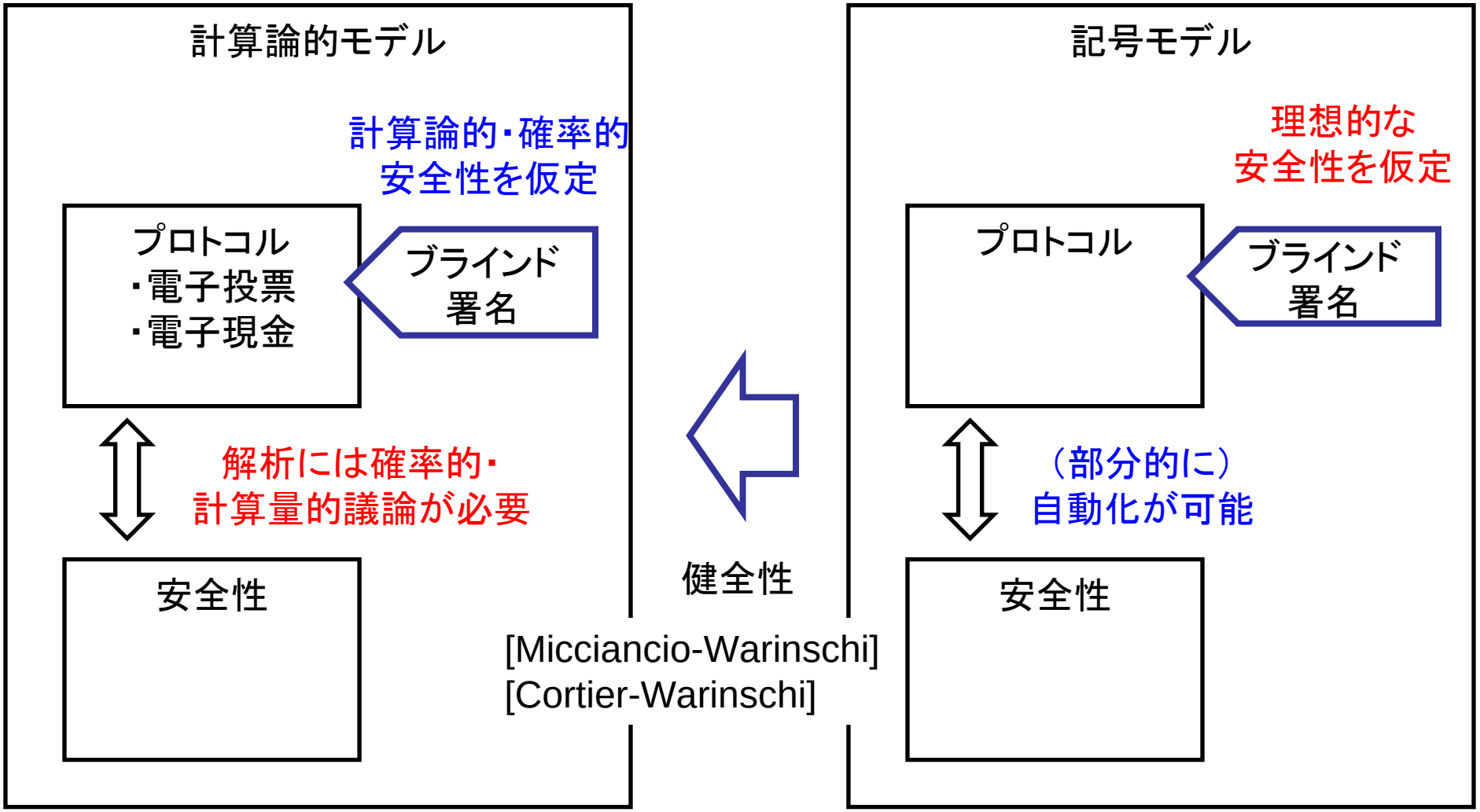
ブラインド署名の計算論的に健全な形式化

櫻田英樹[1], 萩谷昌己[1,2]
NTTコミュニケーション科学基礎研究所
東京大学大学院情報理工学系研究科

背景

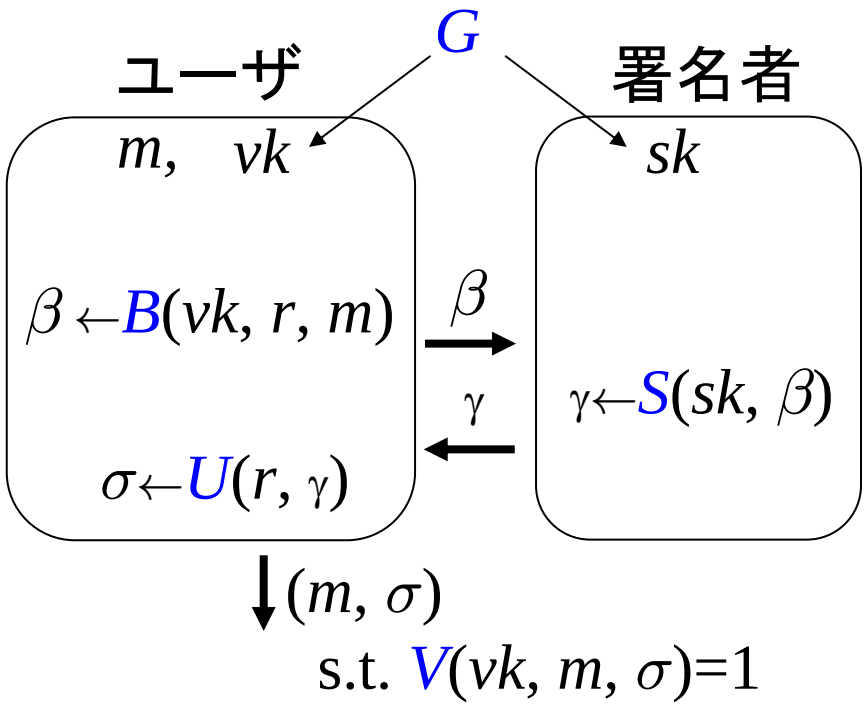

計算論的モデル
計算論的・確率的
安全性を仮定
プロトコル
暗号
署名
解析には確率的・
計算量的議論が必要
安全性
健全性
[Micciancio-Warinschi]
[Cortier-Warinschi]
記号モデル
理想的な
安全性を仮定
プロトコル
暗号
署名
（部分的に）
自動化が可能
安全性

本研究の目的


計算論的モデル
計算論的・確率的
安全性を仮定
プロトコル
・電子投票
・電子現金
ブラインド
署名
解析には確率的・
計算量的議論が必要
安全性
記号モデル
理想的な
安全性を仮定
プロトコル
ブラインド
署名
（部分的に）
自動化が可能
安全性
健全性
[Micciancio-Warinschi]
[Cortier-Warinschi]

ブラインド署名

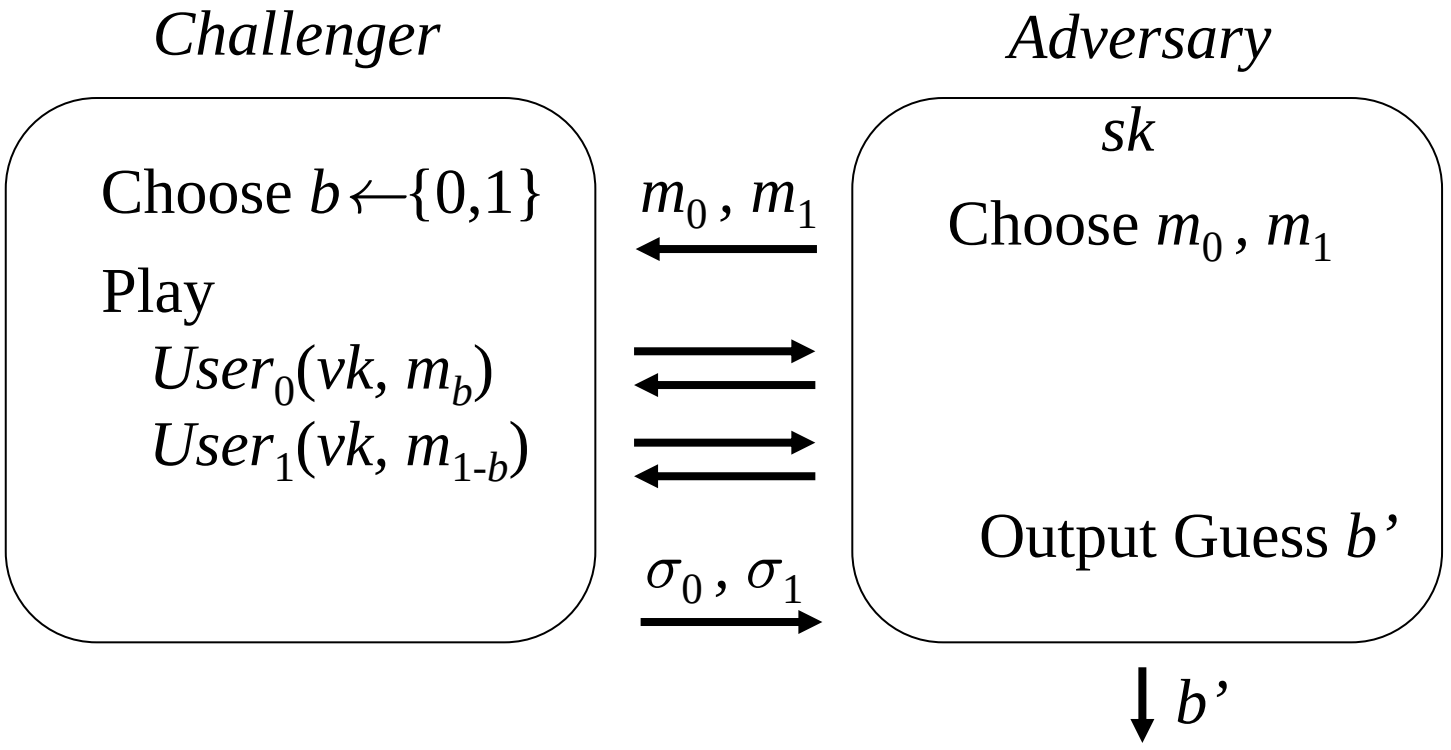
- 電子署名の一種
  - ユーザはメッセージmを明かさずに署名 σを得られる
  - 例えば、電子投票[FOO]では、投票内容を明かさずに投票への署名を得る



- 安全性：ブラインド性・偽造不能性

ブラインド性

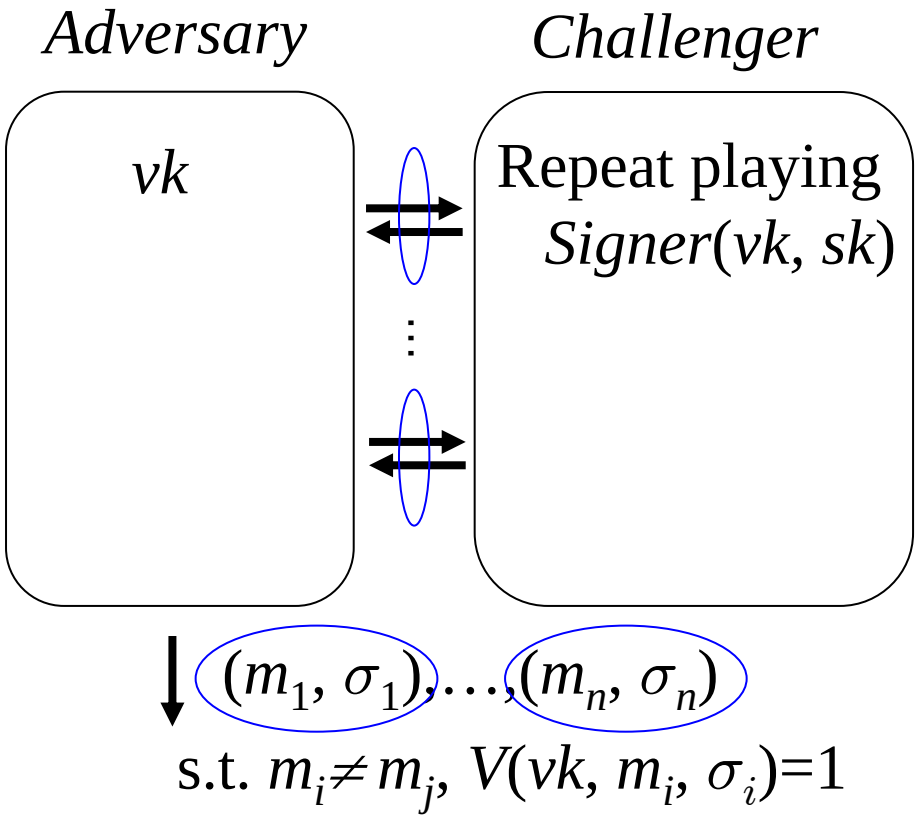
- （署名鍵を持つ）攻撃者はユーザのメッセージについて知ることができない



偽造不能性

- 攻撃者(ユーザ)が得られる署名の数
  ≤ 挑戦者(署名者)が署名した数

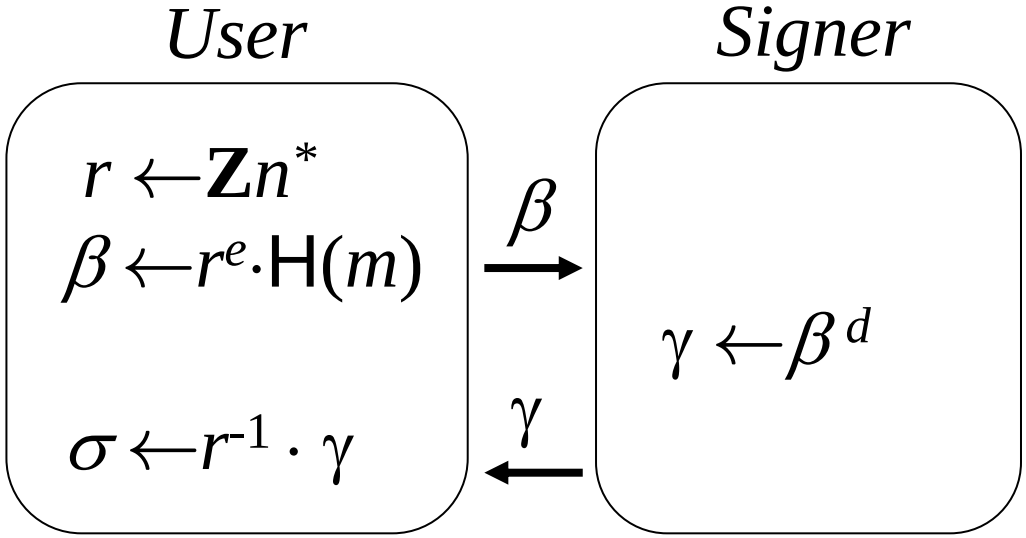
- 攻撃者がプロトコルに従わない“変な”メッセージを送って署名を得る可能性がある



“変な” リクエスト（FDH-RSA）

- ユーザ（攻撃者）は
  - βの代わりに$\beta' = \beta^{1/2}$を送り
  - 応答γ'からもとの$\gamma = \gamma'^2$を構成

$$(e, d, n) \leftarrow G$$
$$\text{s.t. } x^{ed} = x \pmod{n}$$



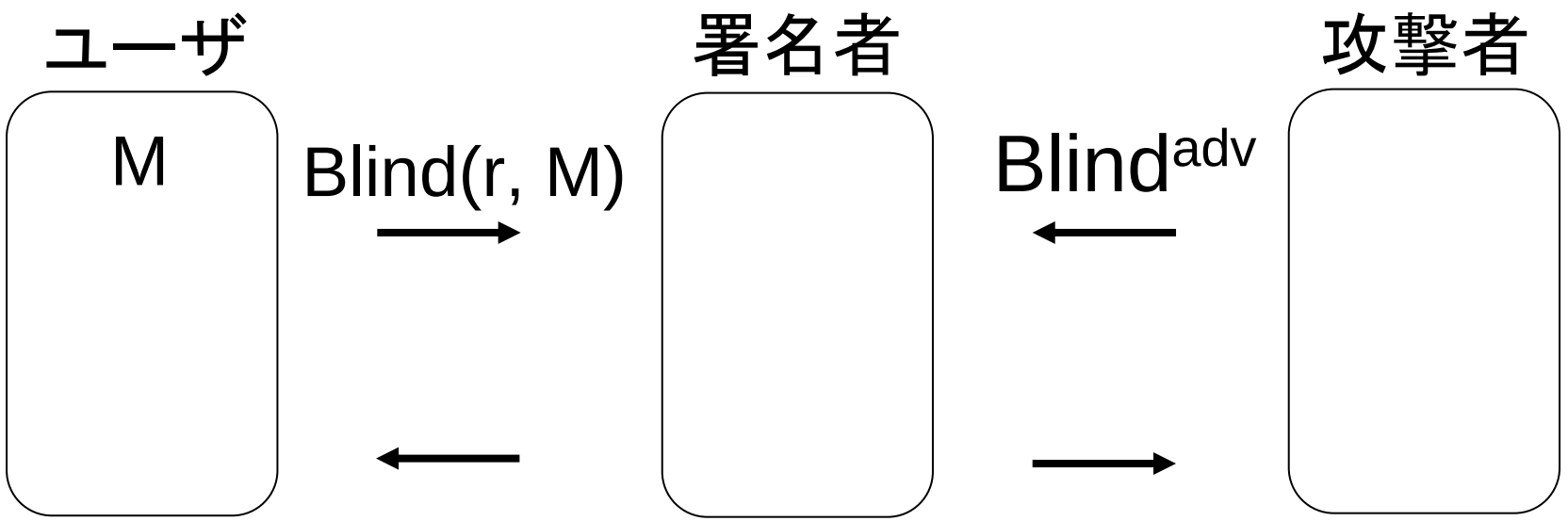
- 記号モデルでは
  このような実行も考慮が必要

(m, σ)

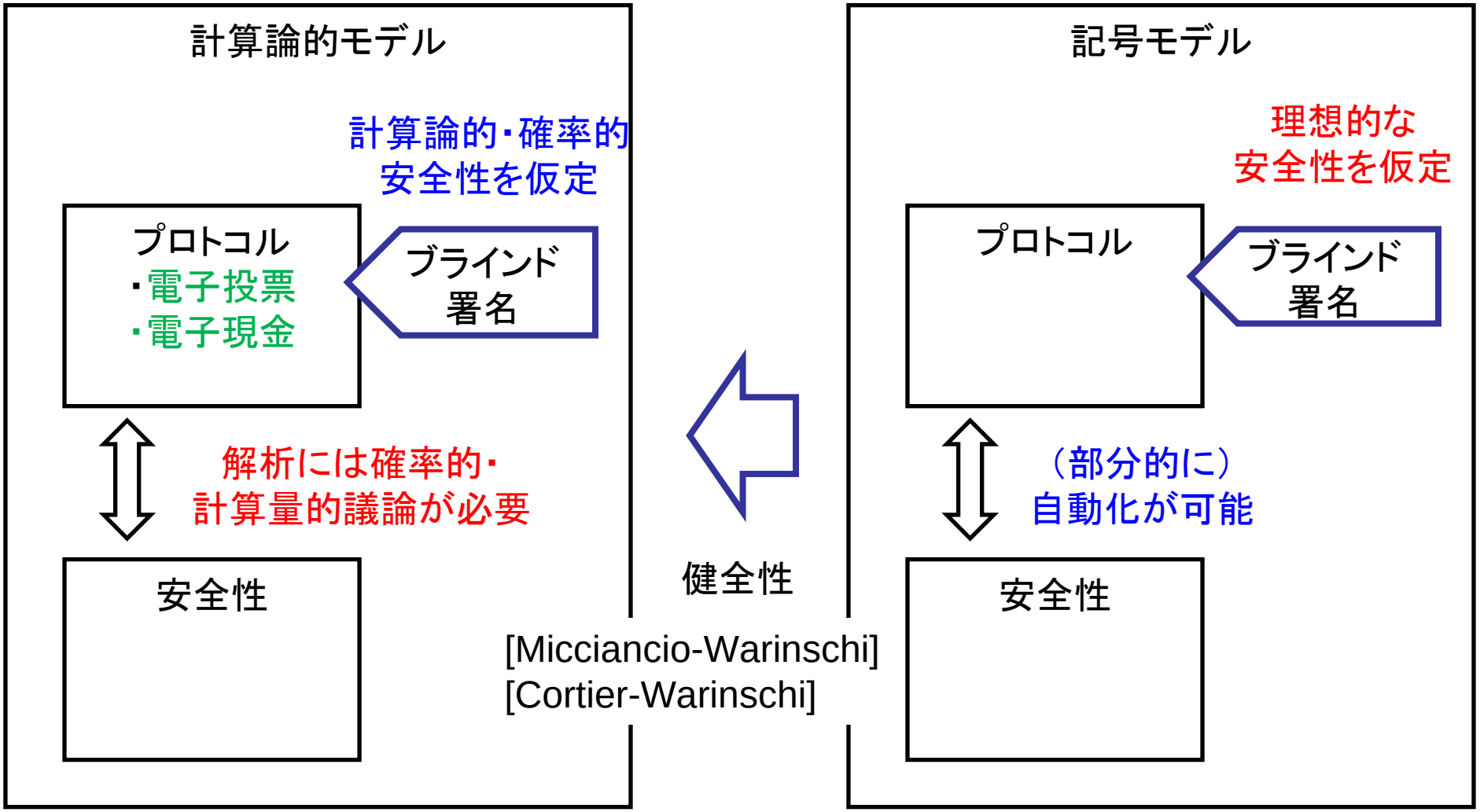
$$\sigma = r^{-1} \cdot r^{ed} \cdot \mathrm{H}(m)^d = \mathrm{H}(m)^d$$

アプローチ

- 正しいリクエストも、“変な”リクエストも、署名を得ることができるようなリクエストは同じ記号 Blind^{adv}で表す



本研究の目的(再掲)


計算論的モデル
計算論的・確率的
安全性を仮定
プロトコル
・電子投票
・電子現金
ブラインド
署名
解析には確率的・
計算量的議論が必要
安全性
健全性
[Micciancio-Warinschi]
[Cortier-Warinschi]
記号モデル
理想的な
安全性を仮定
プロトコル
ブラインド
署名
(部分的に)
自動化が可能
安全性

プロトコル言語

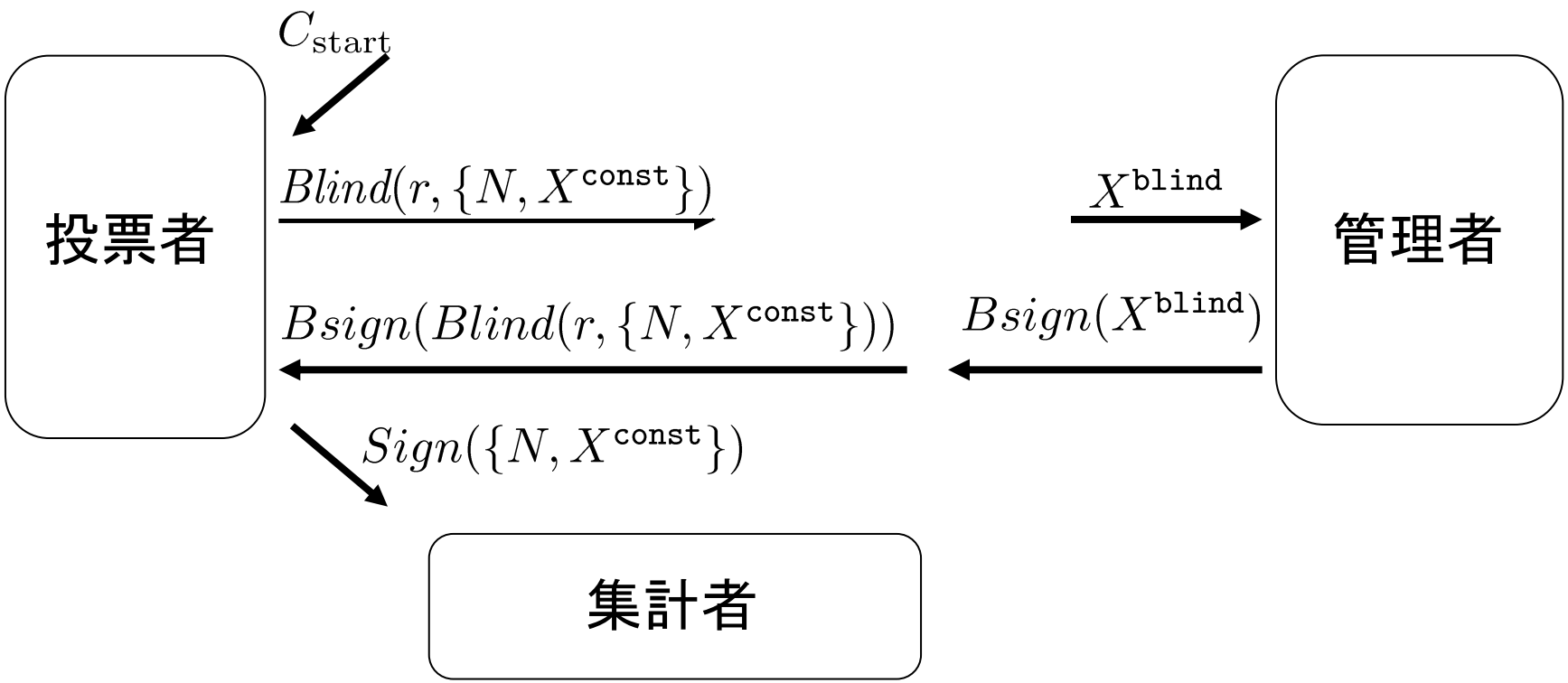
- メッセージ

$$M ::= C \mid N \mid X^{\tau} \mid Blind(r, M) \mid Bsign(M) \mid Sign(M)$$
$$\tau ::= \texttt{const} \mid \texttt{nonce} \mid \texttt{blind}$$

- 各参加者の動作は（受信するメッセージ，送信するメッセージ）の列 $((M^r_1, M^s_1) \ldots ((M^r_n, M^s_n))$ で記述する

例：簡単な投票プロトコル

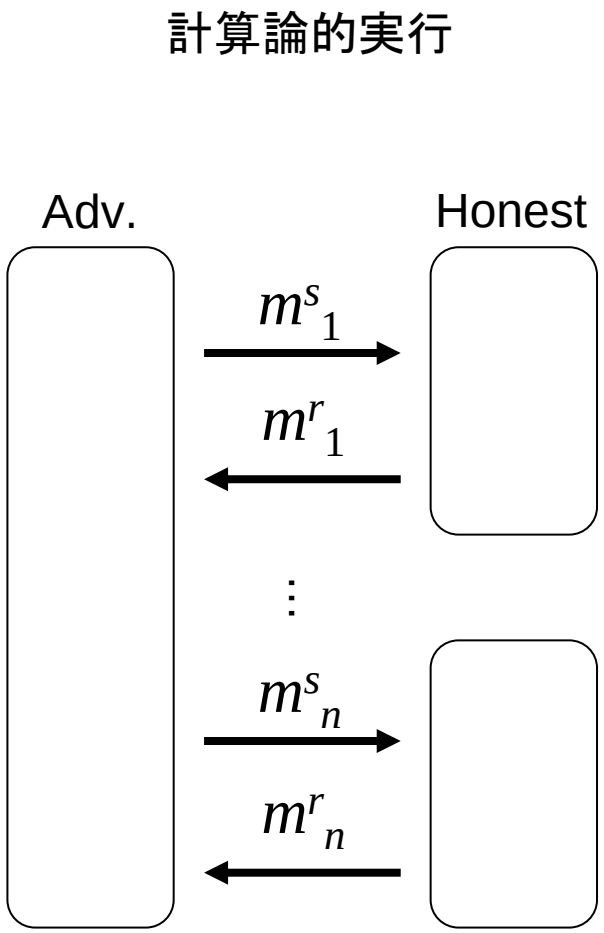
$$\rho_{\mathrm{voter}}(X^{\mathtt{const}}) = (C_{\mathrm{start}}, Blind(r, \{N, X^{\mathtt{const}}\}))$$
$$(Bsign(Blind(r, \{N, X^{\mathtt{const}}\})), Sign(\{N, X^{\mathtt{const}}\}))$$
$$\rho_{\mathrm{admin}} = (X^{\mathtt{blind}}, Bsign(X^{\mathtt{blind}}))$$



計算論的モデル

- 攻撃者・参加者は*PPTM*
- メッセージはビット列
- 参加者は
  - プロトコルに従い送受信
  - 特に、Bsign(Blind(r, M'))を受信する際は受け取ったメッセージmに対し次の計算を行い確認

$$V(sk, U(t(r), m), [\![M']\!]_{\eta}^{t}) = 1$$

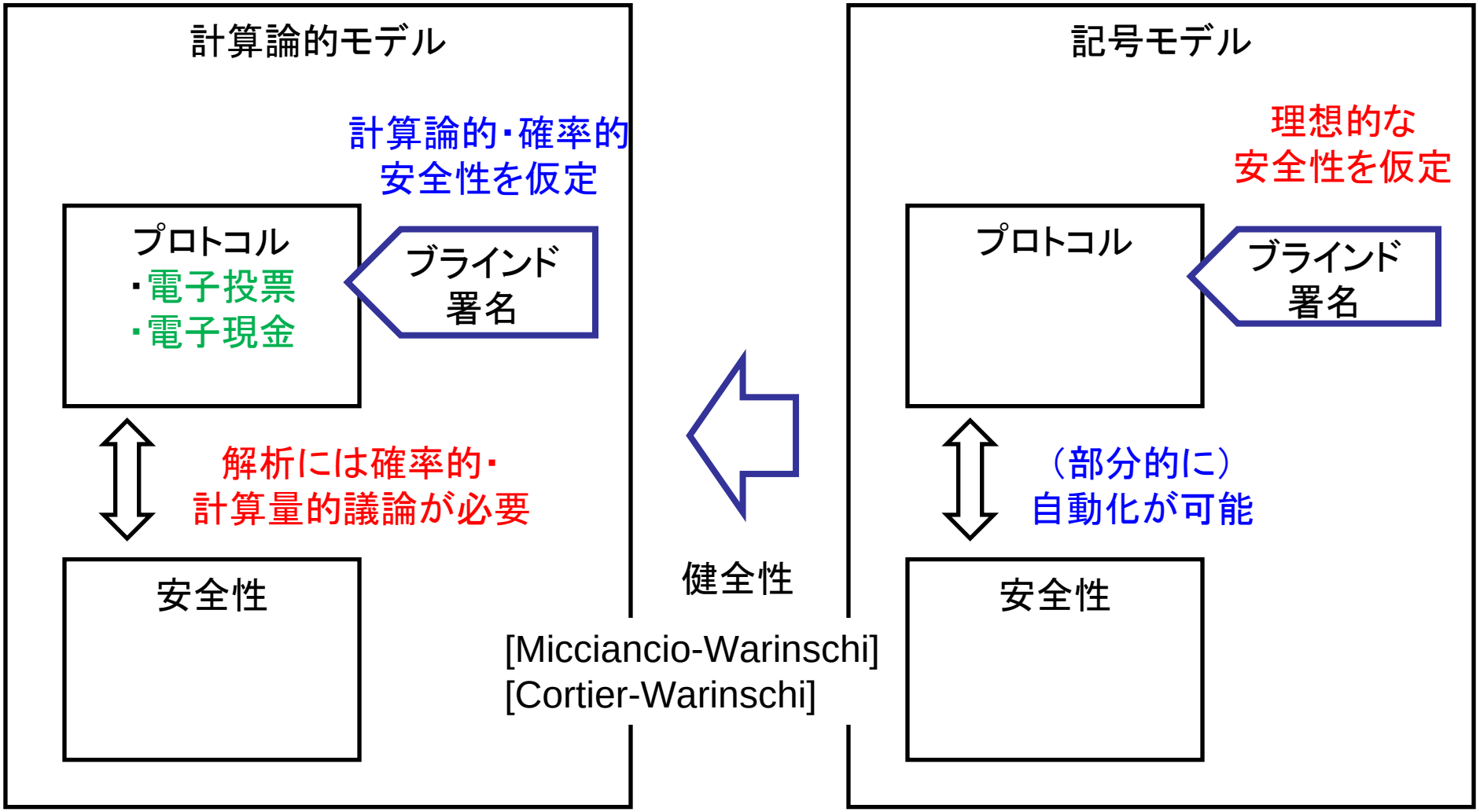


計算論的モデルのメッセージ

- ビット列に符号化される

$$
\begin{aligned}
[\![C]\!]^t_\eta &= \langle \mathtt{const}, t(C) \rangle \\
[\![N]\!]^t_\eta &= \langle \mathtt{nonce}, t(N) \rangle \\
[\![\{M_0, M_1\}]\!]^t_\eta &= \langle \mathtt{pair}, [\![M_0]\!]^t_\eta, [\![M_1]\!]^t_\eta \rangle \\
[\![Blind(r, M)]\!]^t_\eta &= \langle \mathtt{blind}, B(t(r), [\![M]\!]^t_\eta) \rangle \\
[\![Bsign(M)]\!]^t_\eta &= \langle \mathtt{bsign}, S(t(M)) \rangle \\
[\![Sign(M)]\!]^t_\eta &= \langle \mathtt{sign}, U(t(r), t(Bsign(Blind(r, M)))) \rangle
\end{aligned}
$$

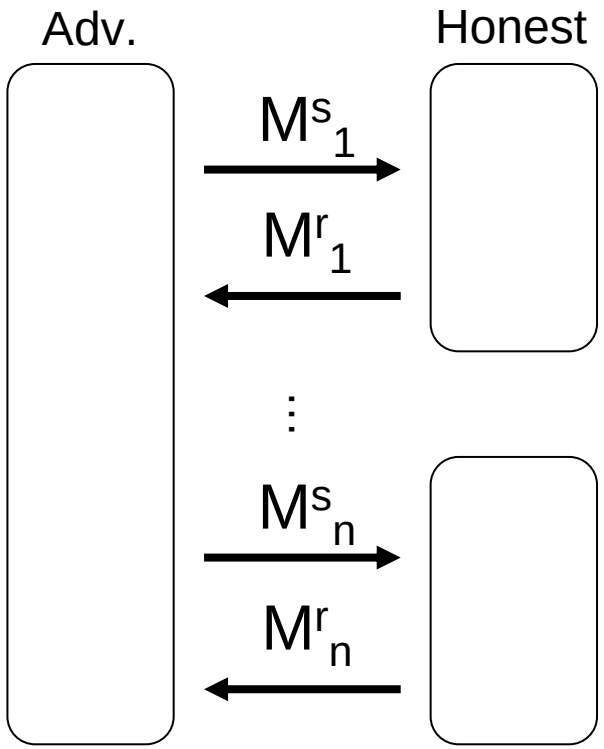
本研究の目的(再掲)


計算論的モデル
計算論的・確率的
安全性を仮定
プロトコル
・電子投票
・電子現金
ブラインド
署名
解析には確率的・
計算量的議論が必要
安全性
健全性
[Micciancio-Warinschi]
[Cortier-Warinschi]
記号モデル
理想的な
安全性を仮定
プロトコル
ブラインド
署名
(部分的に)
自動化が可能
安全性

記号モデル

- メッセージ(記号列)

$$M ::= C \mid N \mid \{M, M\}$$
$$\mid \mathrm{Blind}(r, M) \mid \mathrm{Bsign}(M) \mid \mathrm{Sign}(M)$$
$$\mid N^{adv} \mid \mathrm{Blind}^{adv} \mid \mathrm{Sign}^{adv}(M)$$



- 簡単のため署名鍵は1つと仮定
- 記号的実行は次を満たす
  1. 攻撃者が送信するメッセージM^s_iは
     以前に受信したメッセージから
     *構成できる*ものに限る
  2. 攻撃者がアンブラインドして得られる署名
     $\mathrm{Sign}^{adv}(\_)$ の数
     $\leq$ 参加者が$\mathrm{Bsign}(\mathrm{Blind}^{adv})$ を作る回数

記号モデルで構成できるメッセージ

- 攻撃者によって M がΓから構成できる
  ⇔ $\Gamma \vdash$ M が次のルールで導出できる

$$\Gamma \vdash C \qquad \Gamma \vdash N^{adv} \qquad \Gamma \vdash Blind^{adv} \qquad \frac{\Gamma \vdash Bsign(Blind^{adv}) \quad \Gamma \vdash M}{\Gamma \vdash Sign^{adv}(M)}$$

$$\frac{M \in \Gamma}{\Gamma \vdash M} \qquad \frac{\Gamma \vdash M_0 \quad \Gamma \vdash M_1}{\Gamma \vdash \{M_0, M_1\}} \qquad \frac{\Gamma \vdash \{M_0, M_1\}}{\Gamma \vdash M_i} \qquad \frac{\Gamma \vdash Sign(M)}{\Gamma \vdash M}$$

- Blind(M) からは新しいメッセージを導出できない
  （ブラインド性に対応）

マッピング補題と健全性

- マッピング補題：計算論的モデルにおける実行は、記号モデルにおける実行に対応させることができる（計算論的モデルでの攻撃は記号モデルでも考慮）

$$\Pr[tr_c \leftarrow Run_c(\Pi) \mid f(tr_c) \in Run_s(\Pi)] < \text{negligible}$$

- 健全性：記号モデルで安全⇒計算論的モデルでも安全

マッピング補題

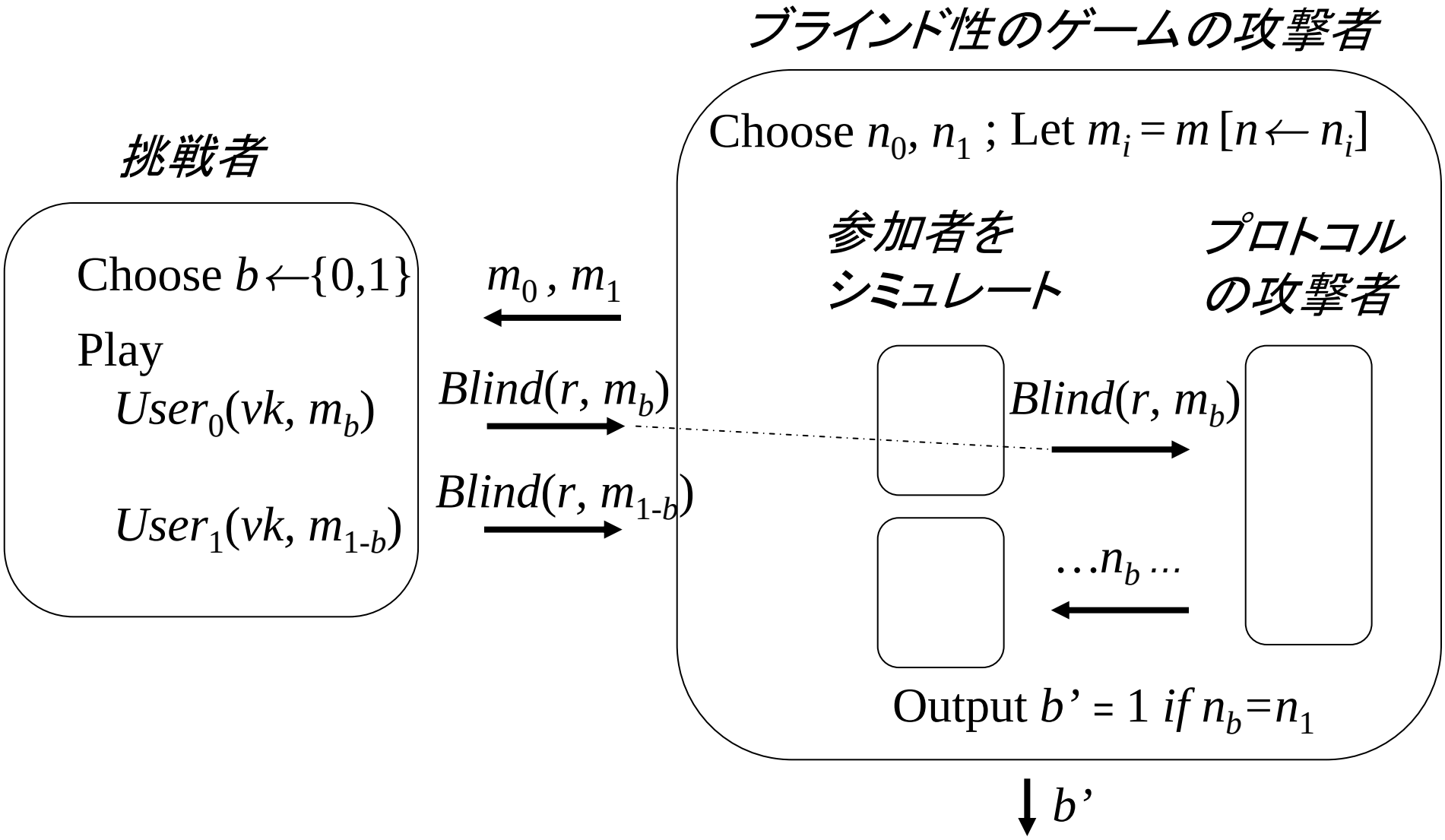
証明の手順

1. 計算論的実行 tr_c を記号的メッセージ列 tr_s に対応させ、
2. それが計算論的実行の条件を満たすことを示す
   A) 攻撃が送信するメッセージは導出可能
   B) 攻撃者が構成する署名 $Sign^{adv}(\_)$ の数
      $\leq$ 参加者が $Bsign(Blind^{adv})$ を作る回数

計算論的実行から記号的実行へ

- <const, c> $\mapsto$ C
- <nonce, n> $\mapsto$ N, if generated by honest party
  $\mapsto$ N^{adv}, otherwise
- <blind, m> $\mapsto$ Blind(r, M), if generated by honest party
  $\mapsto$ $Blind^{adv}$, otherwise
- <bsign, m> $\mapsto$ Bsign(M')
  where m' $\mapsto$M' and Bsign(sk, m')=m
- <sign, m> $\mapsto$ Sign(M'), if unblinded by honest party
  $\mapsto$ $Sign^{adv}$ (M') otherwise
  where m' $\mapsto$M' and V(vk, m, m')=1

A) ブラインド性に帰着


ブラインド性のゲームの攻撃者
挑戦者
Choose n_0, n_1 ; Let $m_i = m\,[n \leftarrow n_i]$
参加者を
シミュレート
プロトコル
の攻撃者
Choose $b \leftarrow \{0,1\}$
Play
$User_0(vk, m_b)$
$User_1(vk, m_{1-b})$
m_0 , m_1
$Blind(r, m_b)$
$Blind(r, m_{1-b})$
$Blind(r, m_b)$
…n_b …
Output $b' = 1$ *if* $n_b = n_1$
b'

B) 偽造不能性からAの場合に帰着

- 次の例では、偽造不能性より $M_1' = M_1$ or M_2
- M_1についてブラインド性が保たれないことになる

受信したBsign		*構成したSign*
$Bsign(Blind(M_0))$		$Sign(M_0)$
$Bsign(Blind(M_1))$		$Sign^{adv}(M_1')$
$Bsign(Blind^{adv})$	<	$Sign^{adv}(M_2)$

まとめ

- ブラインド署名を用いるようなプロトコルを扱うための記号的モデルを構成
- 記号的モデルの計算論的モデルに対する健全性を示した