CPA安全な暗号とゼロ知識証明から構成される CCA1安全な暗号の 確率的ホーア論理を用いた形式的検証

久保田貴大
東京大学理学部情報科学科

川本裕輔　萩谷昌己
東京大学情報理工学系研究科
コンピュータ科学専攻

背景

- 暗号方式には計算量理論に基づく安全性証明が必要
- 暗号方式の安全性証明は一般に極めて煩雑で、人手による非形式的な証明は間違いやすい
  - 暗黙の仮定を使ってしまうことがよくある
  - 自動的なチェックが不可能
- 形式的手法(数理的技法)においては、仮定を全て明示し、自動的なチェックを目指す

研究の目的

- 暗号方式の複雑な安全性証明に対する形式的手法の有効性を明らかにする
  - ElGamal暗号方式のIND-CPA安全性証明は、確率的ホーア論理で形式化されている [Corin-Hartog2006]
  - より複雑な安全性証明に対する有効性を明らかにしたい
    - 復号オラクルを含むIND-CCA1安全性証明は、IND-CPA安全性証明よりも複雑な議論になる

研究の概要

- 確率的ホーア論理[Corin-Hartog2006]を用いて、Naor-Yungの構成法による暗号方式のIND-CCA1安全性証明を形式化した
- そのために、確率的ホーア論理に改良を加えた

目次

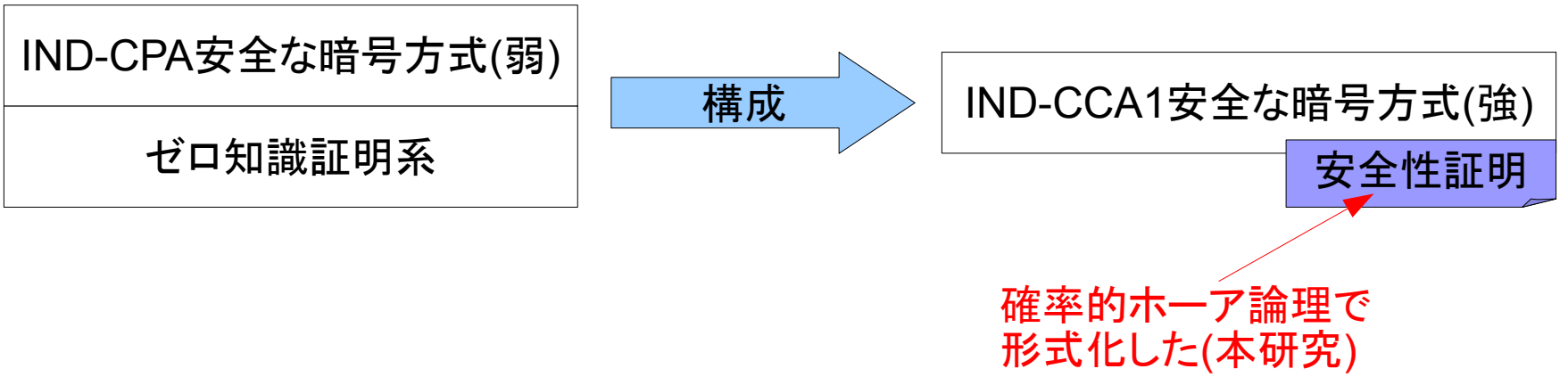
- 本研究における検証対象
  - Naor-Yungの暗号構成法
- 形式化の枠組み
  - 確率的ホーア論理
- 我々の貢献
- 結論
- 関連研究
- 今後の課題

目次

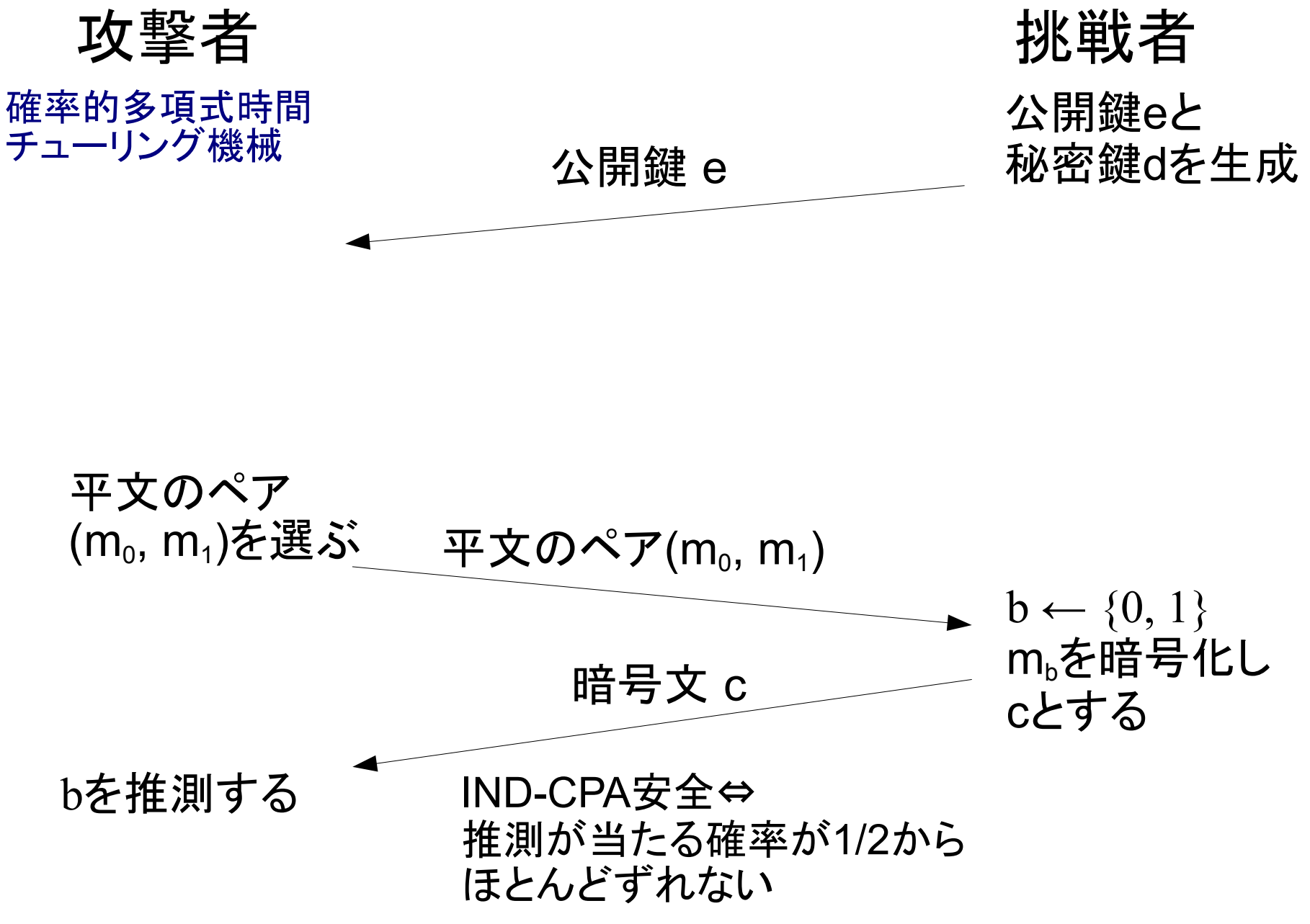
- 本研究における検証対象
  - Naor-Yungの暗号構成法
- 形式化の枠組み
  - 確率的ホーア論理
- 我々の貢献
- 結論
- 関連研究
- 今後の課題

本研究における検証対象

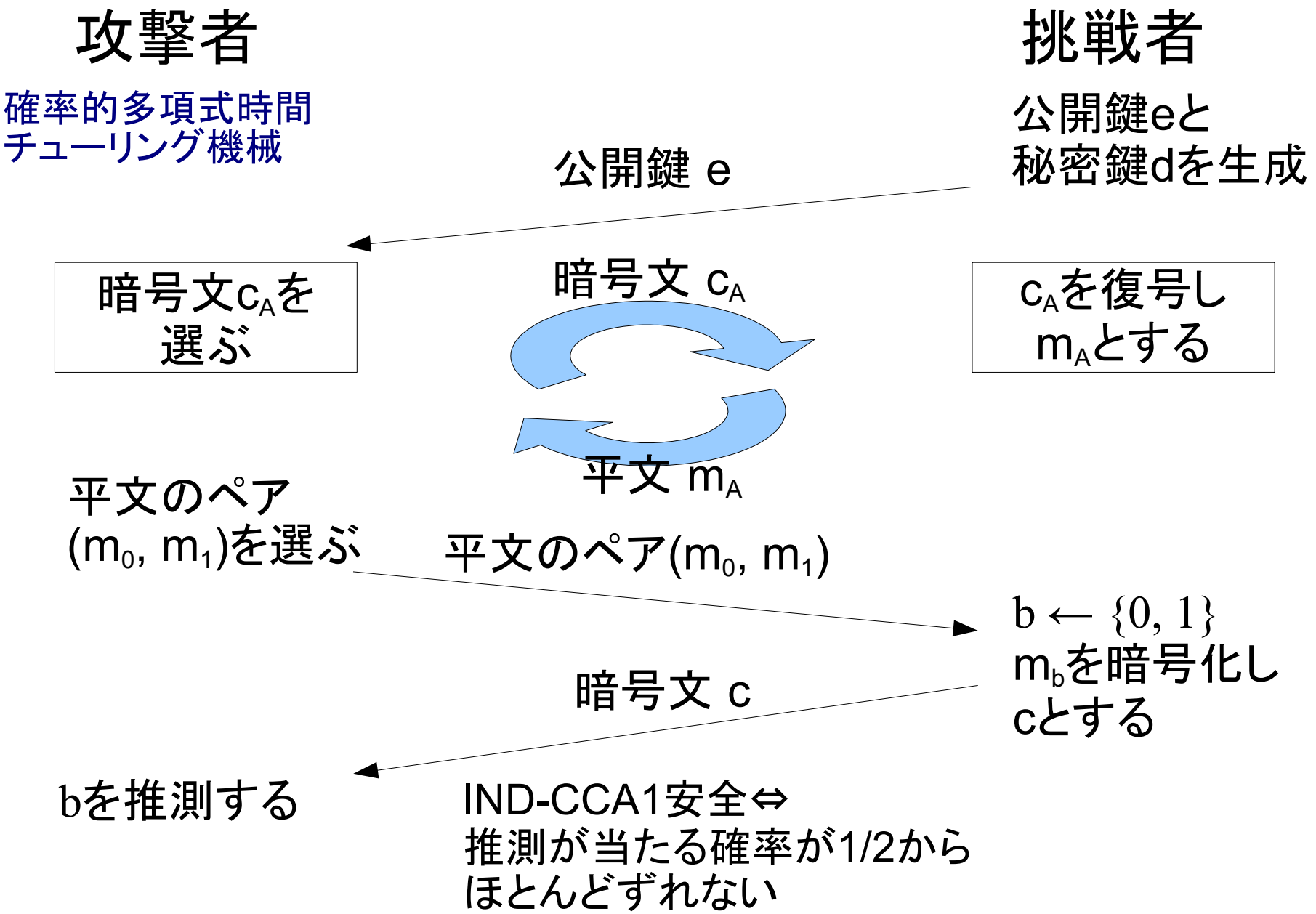
- Naor-Yungの暗号構成法[Naor-Yung1990]
  - IND-CPA安全な暗号方式と、
    適応的非対話ゼロ知識証明系を使って
    IND-CCA1安全な暗号方式を構成する
- この構成法に対する安全性証明が形式化の対象



IND-CPAゲーム


攻撃者
確率的多項式時間
チューリング機械
挑戦者
公開鍵eと
秘密鍵dを生成
公開鍵 e
平文のペア
(m0, m1)を選ぶ
平文のペア(m0, m1)
b ← {0, 1}
mbを暗号化し
cとする
暗号文 c
bを推測する
IND-CPA安全⇔
推測が当たる確率が1/2から
ほとんどずれない

IND-CCA1ゲーム


攻撃者
確率的多項式時間
チューリング機械
挑戦者
公開鍵eと
秘密鍵dを生成
公開鍵 e
暗号文cAを
選ぶ
暗号文 cA
cAを復号し
mAとする
平文 mA
平文のペア
(m0, m1)を選ぶ
平文のペア(m0, m1)
b ← {0, 1}
mbを暗号化し
cとする
暗号文 c
bを推測する
IND-CCA1安全⇔
推測が当たる確率が1/2から
ほとんどずれない

本研究における検証対象

[仮定]
(攻撃者の勝率)≒1/2
であるとする

IND-CPA

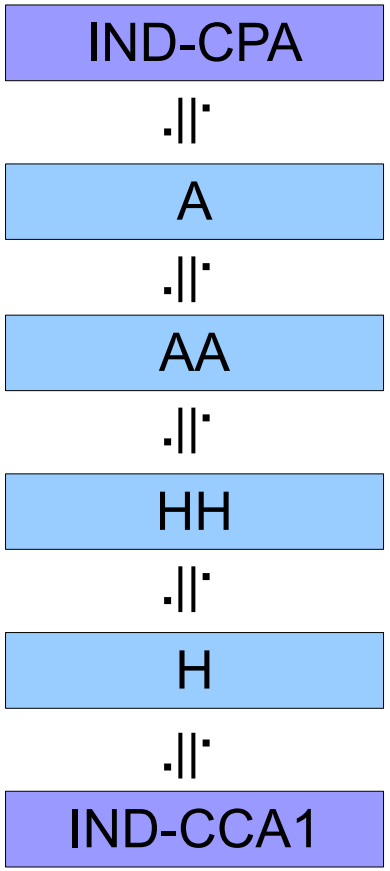
- 形式化すべき安全性証明は、
  ハイブリッド論法によってなされている
  [Naor-Yung1990]

IND-CCA1

[目標]
(攻撃者の勝率)≒1/2
を示す

本研究における検証対象

[仮定]
(攻撃者の勝率)≒1/2
であるとする



[目標]
(攻撃者の勝率)≒1/2
を示す

- 形式化すべき安全性証明は、
  ハイブリッド論法によってなされている
  [Naor-Yung1990]
  - 「安全性を証明したいゲーム」を
    「攻撃者の勝率が評価しやすいゲーム」に
    変換していく方法である

Naor-Yungの暗号構成法

- IND-CPA安全暗号方式(G, E, D)
- 適応的非対話ゼロ知識証明系(P, V)
  - 完全性
  - ゼロ知識性
  - Weak-simulation soundness

適応的非対話ゼロ知識証明系 (P, V)

- NP言語 L に付随する関係 L_R のもとで定義される

  $x \in L$ iff $\exists w.\ (x, w) \in L_R$

- ビット列 r は、common reference string
- P は証明者の確率的多項式時間アルゴリズム
  - $(x, w) \in L_R$ と r を受け取り、証明 π を返す
- V は検証者の多項式時間アルゴリズム
  - x, r, π を受け取り、検証結果 b を返す

適応的非対話ゼロ知識証明系 (P, V)

- 完全性
- ゼロ知識性
- weak-simulation soundness

$(\Xi(r), W(r)) \in L_R$ を満たす任意の
(多項式サイズの回路により実現可能な)関数Ξ, Wに関して

$r \leftarrow \{0, 1\}^*$
$\pi \leftarrow P(\Xi(r), W(r), r)$
$b := V(\Xi(r), r, \pi)$
$\Pr(b = 0) < \varepsilon_{ZKC}$

証明者Pによる証明は
検証者Vによってほぼ確実に受理される

適応的非対話ゼロ知識証明系 (P, V)

- 完全性
- ゼロ知識性
- weak-simulation soundness

シミュレータの組(S_1, S_2)が存在して、
$(\Xi(r), W(r)) \in L_R$ を満たす任意の関数Ξ, Wと
任意の確率的多項式時間アルゴリズムDに対して、
$r \leftarrow \{0, 1\}^*$
$s \leftarrow RND$
$(r_{sim}, s) \leftarrow S_1(1^n, s)$
$\pi \leftarrow P(\Xi(r), r, W(r))$
$\pi' \leftarrow S_2(\Xi(r_{sim}), s)$
$b \leftarrow D(\Xi(r), \pi, r)$
$b' \leftarrow D(\Xi(r_{sim}), \pi', r_{sim})$
$| Pr(b = 1) - Pr(b' = 1) | < \varepsilon_{AZK}$

$W(r)$に関する知識がほぼ無い

適応的非対話ゼロ知識証明系 (P, V)

- 完全性
- ゼロ知識性
- weak-simulation soundness

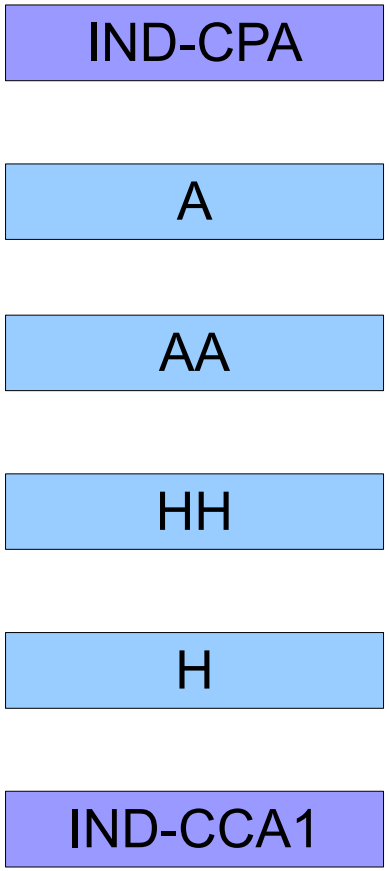
任意の関数Ξ, Πと、
ゼロ知識性を満たすシミュレータS_1に対して、

$s \leftarrow RND$
$(r_{sim}, s) \leftarrow S_1(1^n, s)$
$b := V(\Xi(r_{sim}), r_{sim}, \Pi(r_{sim}))$
$\Pr(\Xi(r_{sim}) \notin L \wedge b = 1) < \varepsilon_{WSS}$

誤った入力が受理されることは
ほぼ無い

Naor-Yungの暗号構成法

[仮定]
(攻撃者の勝率)≒1/2
であるとする

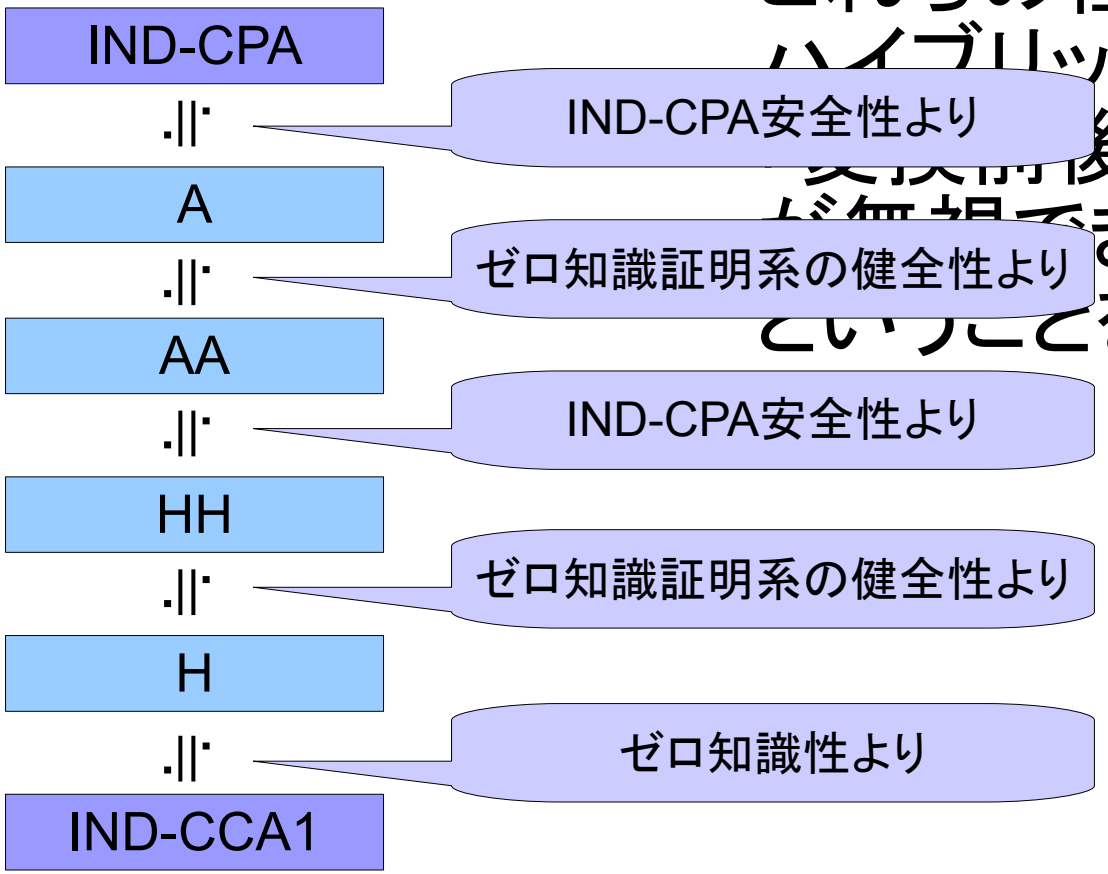


[目標]
(攻撃者の勝率)≒1/2
を示す

- これらの性質は、
  ハイブリッド論法において、
  「変換前後のゲームの違い
  が無視できるほど小さい」
  ということを示すのに利用される

Naor-Yungの暗号構成法

[仮定]
(攻撃者の勝率)≒1/2
であるとする



[目標]
(攻撃者の勝率)≒1/2
を示す

- これらの性質は、
  ハイブリッド論法において、
  変換前後のゲームの違い
  が無視できるほど小さい」
  ということを示すのに利用される

Naor-Yungの暗号構成法

- 構成される暗号方式 (G', E', D')
  - 鍵生成アルゴリズム G'

$G'(1^n)$ {
  $(e_1, d_1) \leftarrow G(1^n)$
  $(e_2, d_2) \leftarrow G(1^n)$
  $r \leftarrow \{0, 1\}^*$
  return $((e_1, e_2, r), (d_1, d_2))$
}

秘密鍵

公開鍵

Naor-Yungの暗号構成法

- 構成される暗号方式 (G', E', D')
  - 暗号化アルゴリズム E'

$E'((e_1, e_2, r), x)$ {
  $s_1 \leftarrow RND$
  $s_2 \leftarrow RND$
  $y_1 := E(e_1, x, s_1)$
  $y_2 := E(e_2, x, s_2)$
  $\pi \leftarrow P((e_1, e_2, y_1, y_2), r, (x, s_1, s_2))$
  return (y_1, y_2, π)
}

$((e_1, e_2, y_1, y_2), (x, s_1, s_2)) \in L_R$

Naor-Yungの暗号構成法

- 構成される暗号方式 (G', E', D')
  - 復号アルゴリズム D'

$D'((d_1, d_2), (e_1, e_2, r), (y_1, y_2, \pi))$ {
  if $V((e_1, e_2, y_1, y_2), r, \pi) = 1$
    then x := $D(d_1, y_1)$
      return x
    else return “error”
}

目次

- 本研究における検証対象
  - Naor-Yungの暗号構成法
- 形式化の枠組み
  - 確率的ホーア論理
- 我々の貢献
- 結論
- 関連研究
- 今後の課題

形式化の枠組み

- (G', E', D') に対する安全性証明全体を記述できるような枠組みを選ぶ
  - 攻撃ゲームの議論では、確率の記述が必要
  - 逐次実行のプログラムが書ければ十分

形式化の枠組み

- 確率的ホーア論理[Corin-Hartog2006]
  - 確率的な実行を含む逐次的なプログラムの性質を、記述する形式体系
  - ホーアの三つ組
    {P}　　事前条件Pが成り立つとき
    　S　　プログラムSを実行すると
    {Q}　　事後条件Qが成り立つ

確率的ホーア論理

- 確率の記述
  - 確率的実行文　$S_1 \oplus_\rho S_2$
    確率ρでS_1を実行して、確率1-ρでS_2を実行する

    $\{\mathbb{P}(x=1)=1\}$
    $\quad x:=0 \oplus_{1/2}$ skip
    $\{\mathbb{P}(x=1)=1/2\}$

確率的ホーア論理

- 乱択　$x \leftarrow S$
  - 集合Sから、ランダムに値を選択して変数xに代入
- unspecified function
  - 任意の攻撃者を表現
- 直交性
  - ゲームの書き換えの正当化
- 確率変数のランダム性(一様性)と独立性

確率的ホーア論理

- 確率 $\mathbb{P}(dp)$
  - 述語 *dp* を満たす確率
  - $\mathbb{P}(\mathrm{true})=1$ は、「ここ以前のプログラムは必ず停止する」という意味
    - オリジナルの文法には無限ループになりうるwhile文がある
    - たとえば $\mathbb{P}(\mathrm{true})=2/3$ は、無限ループの確率が 1/3

確率的ホーア論理

- 攻撃ゲームおよびゼロ知識証明系(*P*, *V*)の性質を記述することができる
- (*G*, *E*, *D*)の IND-CPA安全性

$$\{\mathbb{P}(\mathtt{true}) = 1\}$$

$$\mathtt{r_G} \leftarrow RND;\ \sigma_\mathtt{A} \leftarrow RND;\ \mathtt{j} \leftarrow BOOL;$$

乱択

$$(\mathtt{e}, \mathtt{d}) := G(1^n, \mathtt{r_G});$$

Unspecified function

$$(\mathtt{x_0}, \mathtt{x_1}, \sigma_\mathtt{A}) := A1(\mathtt{e}, \sigma_\mathtt{A});$$

Unspecified function

$$\mathtt{r_E} \leftarrow RND;$$

乱択

$$\mathtt{if\ j\ then\ y} := E(\mathtt{x_1}, \mathtt{r_E})$$

$$\mathtt{else\ \ y} := E(\mathtt{x_0}, \mathtt{r_E})\ \ \mathtt{fi};$$

$$\mathtt{out_A} := A2(\mathtt{e}, \mathtt{y}, \sigma_\mathtt{A});$$

$$\{|\ \mathbb{P}(\mathtt{out_A} = \mathtt{j}) - 1/2\ | < \epsilon_{cpa}(n)\}$$

確率的ホーア論理

- (*P*, *V*)の完全性

$$\{\mathbb{P}(\mathrm{true}) = 1\}$$

$$\mathbf{r} \leftarrow REF;\ \mathbf{r_P} \leftarrow RND;$$

$$\mathbf{x} := \Xi(\mathbf{r});\ \mathbf{w} := W(\mathbf{r});$$

$$\pi := P(\mathbf{x}, \mathbf{w}, \mathbf{ref}, \mathbf{r_P})$$

$$\mathbf{b} := V(\mathbf{x}, \mathbf{r}, \pi);$$

$$\{\mathbb{P}(\mathbf{b} = 0) < \epsilon_{zkc}(n)\}$$

形式化

r ← {0, 1}*
π ← *P*(Ξ(r), *W*(r), r)
b := *V*(Ξ(r), r, π)
Pr(b = 0) < ε_{ZKC}

確率的ホーア論理

- (*P*, *V*)の完全性

$$\{\mathbb{P}(\mathrm{true}) = 1\}$$

$$\mathtt{r} \leftarrow REF;\ \mathtt{r_P} \leftarrow RND;$$ 乱択

$$\mathtt{x} := \Xi(\mathtt{r});\ \mathtt{w} := W(\mathtt{r});$$ Unspecified function

$$\pi := P(\mathtt{x}, \mathtt{w}, \mathtt{ref}, \mathtt{r_P})$$ Unspecified function

$$\mathtt{b} := V(\mathtt{x}, \mathtt{r}, \pi);$$ Unspecified function

$$\{\mathbb{P}(\mathtt{b} = 0) < \epsilon_{zkc}(n)\}$$

確率的ホーア論理

- (*P*, *V*)のweak-simulation soundness

$$\{\mathbb{P}(\mathtt{true}) = 1\}$$

$$\mathtt{r_{S1}} \leftarrow RND;$$

$$(\mathtt{rsim}, \mathtt{s}) := S1(1^n, \mathtt{r_{S1}});$$

$$\mathtt{x} := \Xi(\mathtt{rsim});\ \pi := \Pi(\mathtt{rsim});$$

$$\{\mathbb{P}(V(\mathtt{x}, \mathtt{rsim}, \pi) = 1 \wedge \mathtt{x} \notin L) < \epsilon_{wss}(n)\}$$

形式化

s ← *RND*
(r_{sim}, s) ← $S_1(1^n, s)$
b := $V(\Xi(r_{sim}), r_{sim}, \Pi(r_{sim}))$
$Pr(\Xi(r_{sim}) \in L \wedge b = 1) < \varepsilon_{WSS}$

確率的ホーア論理

- (*P*, *V*)のゼロ知識性

$$\{\mathbb{P}(\mathrm{true}) = 1\}$$

$$\mathtt{ref} \leftarrow REF;\ \mathtt{r_{S1}} \leftarrow RND;\ \mathtt{r_P} \leftarrow RND;$$

$$(\mathtt{rsim}, \mathtt{s}) := S1(1^n, \mathtt{r_{S1}});$$

$$\mathtt{x} := \Xi(\mathtt{ref});\ \mathtt{x_{sim}} := \Xi(\mathtt{rsim});$$

$$\mathtt{w} := W(\mathtt{ref});\ \pi := P(\mathtt{x}, \mathtt{w}, \mathtt{ref}, \mathtt{r_P})$$

$$\pi_{\mathtt{sim}} := S2(\mathtt{x_{sim}}, \mathtt{s});$$

$$\mathtt{r1} \leftarrow RND;\ \mathtt{r2} \leftarrow RND;$$

$$\mathtt{out1} := D(\mathtt{ref}, \mathtt{x}, \pi, \mathtt{r1});$$

$$\mathtt{out2} := D(\mathtt{rsim}, \mathtt{x_{sim}}, \pi_{\mathtt{sim}}, \mathtt{r2});$$

$$\{|\mathbb{P}(\mathtt{out1}) - \mathbb{P}(\mathtt{out2})| < \epsilon_{azk}(n)\}$$

形式化

r ← {0, 1}*
s ← *RND*
(r_{sim}, s) ← $S_1(1^n, s)$
π ← *P*(Ξ(r), r, *W*(r))
π' ← $S_2(\Xi(r_{sim}), s)$
b ← *D*(Ξ(r), π, r)
b' ← *D*(Ξ(r_{sim}), π', r_{sim})
| Pr(b = 1) – Pr(b' = 1) | < ε_{AZK}

目次

- 本研究における検証対象
  - Naor-Yungの暗号構成法
- 形式化の枠組み
  - 確率的ホーア論理
- 我々の貢献
- 結論
- 関連研究
- 今後の課題

我々の貢献(1)

- Naor-Yungの証明を形式化するために、既存の確率的ホーア論理に改良を加えた
  - 復号オラクルのループを形式化しやすいrepeat文を導入した
    - オリジナルの文法におけるwhile文は停止性が自明でないため、形式化を困難にする
    - repeat文は有限回のループであり、攻撃ゲームの形式化には十分である
      - なぜならば、攻撃者のオラクルアクセスはセキュリティパラメタの多項式の回数に制限されているからである

我々の貢献(1)

- repeat文の導入
  - プログラムの記述は十分可能

$\mathtt{r_{G1}} \leftarrow RND;\ \mathtt{r_G} \leftarrow RND;\ \mathtt{ref} \leftarrow REF;$

$\mathtt{j} \leftarrow BOOL;$

$G'(1^n,\ \mathtt{r_{G1}},\ \mathtt{r_G};\ \mathtt{e}_1,\ \mathtt{d}_1,\ \mathtt{e},\ \mathtt{d},\ \mathtt{ref});$

$\sigma \leftarrow RND;$

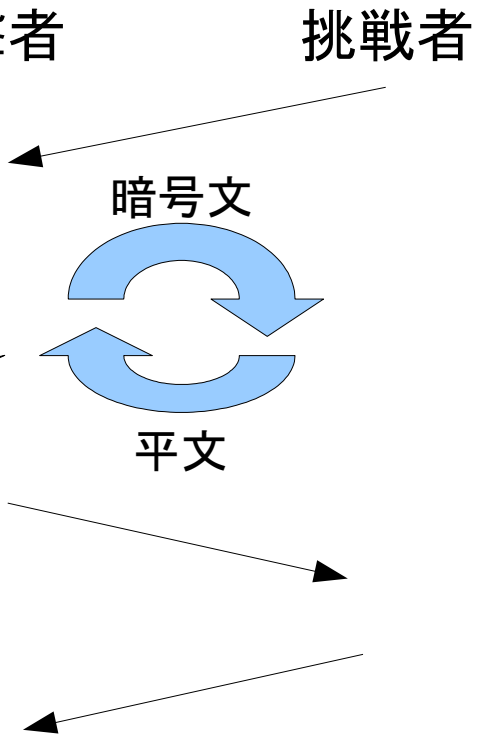
repeat $p(n)$ times

$A1(\mathtt{e}_1,\ \mathtt{e},\ \mathtt{ref},\ \sigma\ ;\ \mathtt{q}_1,\ \mathtt{q}_2,\ \mathtt{q}_3);$

$D'(\mathtt{e}_1,\ \mathtt{e},\ \mathtt{q}_1,\ \mathtt{q}_2,\ \mathtt{ref},\ \mathtt{q}_3,\ \mathtt{d}_1,\ \mathtt{d}_2\ ;\ \mathtt{m});$

$A2(\mathtt{e}_1,\ \mathtt{e},\ \mathtt{ref},\ \mathtt{m},\ \sigma\ ;\ \sigma)$

end;



我々の貢献(1)

- repeat文の導入

$\mathtt{r_{G1}} \leftarrow RND;\ \mathtt{r_G} \leftarrow RND;\ \mathtt{ref} \leftarrow REF;$

$\mathtt{j} \leftarrow BOOL;$

$G'(1^n,\ \mathtt{r_{G1}},\ \mathtt{r_G};\ \mathtt{e_1},\ \mathtt{d_1},\ \mathtt{e},\ \mathtt{d},\ \mathtt{ref});$

$\sigma \leftarrow RND;$

repeat $p(n)$ **times**

$A1(\mathtt{e_1},\ \mathtt{e},\ \mathtt{ref},\ \sigma\ ;\ \mathtt{q_1},\ \mathtt{q_2},\ \mathtt{q_3});$

$D'(\mathtt{e_1},\ \mathtt{e},\ \mathtt{q_1},\ \mathtt{q_2},\ \mathtt{ref},\ \mathtt{q_3},\ \mathtt{d_1},\ \mathtt{d_2}\ ;\ \mathtt{m});$

$A2(\mathtt{e_1},\ \mathtt{e},\ \mathtt{ref},\ \mathtt{m},\ \sigma\ ;\ \sigma)$

end;

- 推論規則の追加

$$\frac{\{q(k)\}\ s\ \{q(k+1)\}}{\{q(0)\}\ \textbf{repeat}\ n\ \textbf{times}\ s\ \textbf{end}\ \{q(n)\}}$$

我々の貢献(2)

- ゼロ知識証明系の性質の形式化
  - 健全性を定義どおりに表現しても、
    安全性証明全体の形式化の議論に適用できなかった

ゼロ知識証明系の健全性

$$\{\mathbb{P}(\mathtt{true}) = 1\}$$

$$\mathtt{r}_{S1} \leftarrow RND;$$

$$(\mathtt{rsim}, \mathtt{s}) := S1(1^n, \mathtt{r}_{S1});$$

$$\mathtt{x} := \Xi(\mathtt{rsim});\ \pi := \Pi(\mathtt{rsim});$$

$$\{\mathbb{P}(V(\mathtt{x}, \mathtt{rsim}, \pi) = 1 \wedge \mathtt{x} \notin L) < \epsilon_{wss}(n)\}$$

我々の貢献(2)

- ゼロ知識証明系の性質の形式化
  - 健全性を定義どおりに表現しても、
    安全性証明全体の形式化の議論に適用できなかった

ゼロ知識証明系の健全性

$$\{\mathbb{P}(\mathtt{true}) = 1\}$$

$$\mathtt{r}_{S1} \leftarrow RND;$$

$$(\mathtt{rsim}, \mathtt{s}) := S1(1^n, \mathtt{r}_{S1});$$

$$\mathtt{x} := \Xi(\mathtt{rsim});\ \pi := \Pi(\mathtt{rsim});$$

$$\{\mathbb{P}(V(\mathtt{x}, \mathtt{rsim}, \pi) = 1 \wedge \mathtt{x} \notin L) < \epsilon_{wss}(n)\}$$

x のインスタンスは (e_1, e_2, y_1, y_2)
π のインスタンスは P((e_1, e_2, y_1, y_2), rsim, (x, s_1, s_2))
x, π ともに rsim のみの関数ではなく、
鍵生成、暗号化の乱数にも依存する

我々の貢献(2)

- ゼロ知識証明系の性質の形式化
  - そこで、[Corin-Hartog2006]の手法を応用して、
    全体の形式化に適用できるホーアの三つ組を導いた

ゼロ知識証明系の健全性から導かれる、有用な形式化

$$\{\mathbb{P}(\mathtt{true}) = 1 \wedge R_{RND^3}(\mathtt{r_{S1}}, \mathtt{r_G}, \mathtt{r_{G1}}) \wedge (\mathtt{rsim}, \mathtt{s}) = S1(1^n, \mathtt{r_{S1}})$$

$$\wedge (\mathtt{e}, \mathtt{d}) = G(1^n, \mathtt{r_G}) \wedge (\mathtt{e_1}, \mathtt{d_1}) = G(1^n, \mathtt{r_{G1}}) \wedge I(\mathtt{r_{S1}}, \sigma_\mathtt{A})\}$$

$$A'(\mathtt{rsim}, \mathtt{e_1}, \mathtt{e}, \sigma_\mathtt{A}; \mathtt{q_1}, \mathtt{q_2}, \mathtt{q_3});$$

$$\{\mathbb{P}(V(\mathtt{e_1}, \mathtt{e}, \mathtt{q_1}, \mathtt{q_2}, \mathtt{rsim}, \mathtt{q_3}) = 1 \wedge D(\mathtt{d_1}, \mathtt{q_1}) \neq D(\mathtt{d}, \mathtt{q_2})) < \epsilon_{wss}(n)\}$$

我々の貢献(2)

- ゼロ知識証明系の性質の形式化
  - まず、Ξ(rsim), Π(rsim) のインスタンスを以下のようにとることができる
    - *A'* は決定的手続きで、関数と等価。k は *RND* の任意の元

$$\{\mathbb{P}(\mathtt{true}) = 1\}$$

$$\mathtt{r_{S1}} \leftarrow RND;$$

$$(\mathtt{rsim}, \mathtt{s}) := S1(1^n, \mathtt{r_{S1}});$$

$$\mathtt{x} := \Xi(\mathtt{rsim});\ \pi := \Pi(\mathtt{rsim});$$

$$\{\mathbb{P}(V(\mathtt{x}, \mathtt{rsim}, \pi) = 1 \wedge \mathtt{x} \notin L) < \epsilon_{wss}(n)\}$$

$$\{\mathbb{P}(\mathtt{true}) = 1\}$$

$$\mathtt{r_{S1}} \leftarrow RND;$$

$$(\mathtt{rsim}, \mathtt{s}) := S1(1^n, \mathtt{r_{S1}});$$

$$\mathtt{r_G} := k;$$

$$(\mathtt{e}, \mathtt{d}) := G(1^n, \mathtt{r_G});$$

$$A'(\mathtt{rsim}, \mathtt{e}; \mathtt{x}, \pi);$$

返り値

$$\{\mathbb{P}(V(\mathtt{x}, \mathtt{rsim}, \pi) = 1 \wedge \mathtt{x} \notin \mathtt{L}) < \epsilon_{wss}(n)\}$$

我々の貢献(2)

- ゼロ知識証明系の性質の形式化
  - この三つ組を仮定すると、

$$\{\mathbb{P}(\mathtt{true}) = 1\}$$

$$\mathtt{r}_{\mathtt{S1}} \leftarrow RND;$$

$$(\mathtt{rsim}, \mathtt{s}) := S1(1^n, \mathtt{r}_{\mathtt{S1}});$$

$$\boxed{\mathtt{r}_{\mathtt{G}} := k;}$$

$$\boxed{(\mathtt{e}, \mathtt{d}) := G(1^n, \mathtt{r}_{\mathtt{G}});}$$

$$\boxed{A'(\mathtt{rsim}, \mathtt{e}; \mathtt{x}, \pi);}$$

返り値

$$\{\mathbb{P}(V(\mathtt{x}, \mathtt{rsim}, \pi) = 1 \wedge \mathtt{x} \notin \mathtt{L}) < \epsilon_{wss}(n)\}$$

我々の貢献(2)

- ゼロ知識証明系の性質の形式化
  - この三つ組を仮定すると、
    推論規則を使って、乱択の場合の正しさを導ける

$$\{\mathbb{P}(\mathtt{true}) = 1\}$$

$$\mathtt{r}_{S1} \leftarrow RND;$$

$$(\mathtt{rsim}, \mathtt{s}) := S1(1^n, \mathtt{r}_{S1});$$

$$\boxed{\mathtt{r}_G \leftarrow RND;}$$

$$(\mathtt{e}, \mathtt{d}) := G(1^n, \mathtt{r}_G);$$

$$A'(\mathtt{rsim}, \mathtt{e};\ \mathtt{x}, \pi);$$

$$\{\mathbb{P}(V(\mathtt{x}, \mathtt{rsim}, \pi) = 1 \wedge \mathtt{x} \notin \mathrm{L}) < \epsilon_{wss}(n)\}$$

$$\{\mathbb{P}(\mathtt{true}) = 1\}$$

$$\mathtt{r}_{S1} \leftarrow RND;$$

$$(\mathtt{rsim}, \mathtt{s}) := S1(1^n, \mathtt{r}_{S1});$$

$$\boxed{\mathtt{r}_G := k;}$$

$$\boxed{(\mathtt{e}, \mathtt{d}) := G(1^n, \mathtt{r}_G);}$$

$$\boxed{A'(\mathtt{rsim}, \mathtt{e}; \mathtt{x}, \pi);}$$

返り値

$$\{\mathbb{P}(V(\mathtt{x}, \mathtt{rsim}, \pi) = 1 \wedge \mathtt{x} \notin \mathrm{L}) < \epsilon_{wss}(n)\}$$

我々の貢献(2)

- ゼロ知識証明系の性質の形式化
  - 同じように、乱数を増やしていくことができる

$$\{\mathbb{P}(\mathtt{true}) = 1\}$$

$$\mathtt{r}_{S1} \leftarrow RND;$$

$$(\mathtt{rsim}, \mathtt{s}) := S1(1^n, \mathtt{r}_{S1});$$

$$\mathtt{r}_G \leftarrow RND;\ \mathtt{r}_{G1} \leftarrow RND;$$

鍵生成の乱数を組み込めた

$$(\mathtt{e}, \mathtt{d}) := G(1^n, \mathtt{r}_G); (\mathtt{e}_1, \mathtt{d}_1) := G(1^n, \mathtt{r}_{G1});$$

$$A''(\mathtt{rsim}, \mathtt{e}_1, \mathtt{e}; \mathtt{q}_1, \mathtt{q}_2, \mathtt{q}_3);$$

x∉Lのインスタンス

$$\{\mathbb{P}(V(\mathtt{e}_1, \mathtt{e}, \mathtt{q}_1, \mathtt{q}_2, \mathtt{rsim}, \mathtt{q}_3) = 1 \wedge D(\mathtt{d}_1, \mathtt{q}_1) \neq D(\mathtt{d}, \mathtt{q}_2)) < \epsilon_{wss}(n)\}$$

我々の貢献(2)

- ゼロ知識証明系の性質の形式化
  - さらに、意味論的な考察からシミュレータS_1の乱数r_{S1}と独立な確率変数σ_Aを、手続きA'の引数としても正しいことがわかる
    - 新たな推論規則として定式化可能

$$\{\mathbb{P}(\mathtt{true}) = 1 \wedge R_{RND^3}(\mathtt{r_{S1}}, \mathtt{r_G}, \mathtt{r_{G1}}) \wedge (\mathtt{rsim}, \mathtt{s}) = S1(1^n, \mathtt{r_{S1}})$$

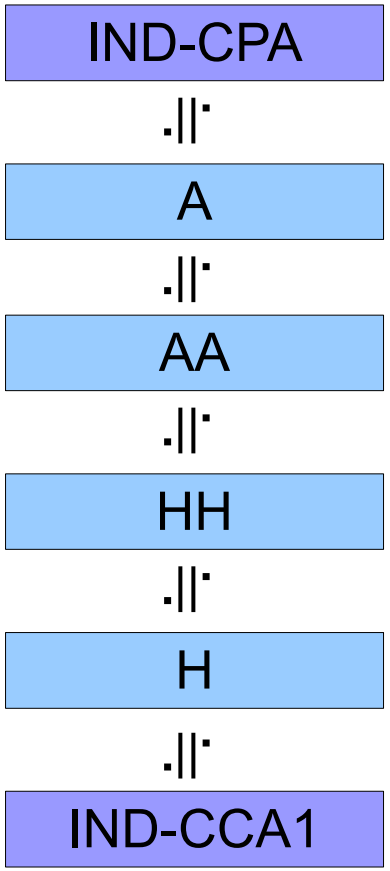
$$\wedge (\mathtt{e}, \mathtt{d}) = G(1^n, \mathtt{r_G}) \wedge (\mathtt{e_1}, \mathtt{d_1}) = G(1^n, \mathtt{r_{G1}}) \wedge \boxed{I(\mathtt{r_{S1}}, \sigma_\mathtt{A})}\}$$

$$A'(\mathtt{rsim}, \mathtt{e_1}, \mathtt{e}, \boxed{\sigma_\mathtt{A}}; \mathtt{q_1}, \mathtt{q_2}, \mathtt{q_3});$$

$$\{\mathbb{P}(V(\mathtt{e_1}, \mathtt{e}, \mathtt{q_1}, \mathtt{q_2}, \mathtt{rsim}, \mathtt{q_3}) = 1 \wedge D(\mathtt{d_1}, \mathtt{q_1}) \neq D(\mathtt{d}, \mathtt{q_2})) < \epsilon_{wss}(n)\}$$

我々の貢献(3)

[仮定]
(攻撃者の勝率)≒1/2
であるとする

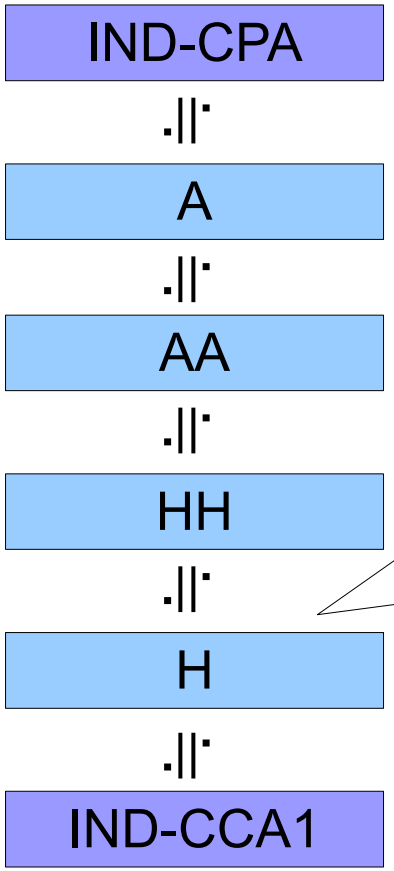


[目標]
(攻撃者の勝率)≒1/2
を示す

- Naor-Yungの安全性証明全体の形式化
  - [Naor-Yung1990]における
    ハイブリッド論法の議論を、
    確率的ホーア論理の枠組み
    で記述できた

我々の貢献(3)

[仮定]
(攻撃者の勝率)≒1/2
であるとする



[目標]
(攻撃者の勝率)≒1/2
を示す

- Naor-Yungの安全性証明全体の形式化(一例)

貢献(2)の結果から、ゲームHとゲームHHの差に関するホーアの三つ組が導かれる

$$\{\mathbb{P}(\mathtt{true}) = 1\}$$

$$\mathtt{r_{G1}} \leftarrow RND;\ \mathtt{r_G} \leftarrow RND;\ \mathtt{ref} \leftarrow REF;$$

$$\mathtt{j} \leftarrow BOOL;$$

$$\ldots$$

$$A4(\mathtt{e_1}, \mathtt{e}, \mathtt{rsim}, \mathtt{y_{1H}}, \mathtt{y_{2H}}, \pi_{\mathtt{H}}, \sigma_{\mathtt{H}};\ \mathtt{out_H});$$

$$A4(\mathtt{e_1}, \mathtt{e}, \mathtt{rsim}, \mathtt{y_{1H}}, \mathtt{y_{2H}}, \pi_{\mathtt{HH}}, \sigma_{\mathtt{HH}};\ \mathtt{out_{HH}});$$

$$\{|\mathbb{P}(\mathtt{out_H} = \mathtt{j}) - \mathbb{P}(\mathtt{out_{HH}} = \mathtt{j})| < p(n) * \epsilon_{wss}(n)\}$$

我々の貢献(3)

- repeat文と、形式的に表現したゼロ知識証明系の性質を用いて、安全性証明全体を形式化した

$$\{\boxed{\mathbb{P}(\mathtt{true}) < \epsilon_{wss}(n)} \ \wedge \ R_{RND^3}(\mathtt{r_{S1}}, \mathtt{r_G}, \mathtt{r_{G1}}) \ \wedge \ (\mathtt{rsim},\ \mathtt{s}) = S1(1^n,\ \mathtt{r_{S1}})$$
$$\wedge\ (\mathtt{e},\ \mathtt{d}) = G(1^n,\ \mathtt{r_G}) \ \wedge\ (\mathtt{e_1},\ \mathtt{d_1}) = G(1^n,\ \mathtt{r_{G1}}) \ \wedge\ I(\mathtt{r_{S1}},\ \sigma_{\mathtt{H}})$$
$$\wedge\ \neg\mathtt{FAIL} \rightarrow (\sigma_{\mathtt{H}} = \sigma_{\mathtt{HH}} \ \wedge ...) \ \wedge\ \mathbb{P}(\mathtt{FAIL}) < k * \epsilon_{wss}(n)\}$$
$$\mathtt{FAIL} := \mathtt{true};$$
$$\{\boxed{\mathbb{P}(\mathtt{FAIL}) < \epsilon_{wss}(n)} \ \wedge \ R_{RND^3}(\mathtt{r_{S1}}, \mathtt{r_G}, \mathtt{r_{G1}}) \ \wedge \ (\mathtt{rsim},\ \mathtt{s}) = S1(1^n,\ \mathtt{r_{S1}})$$
$$\wedge\ (\mathtt{e},\ \mathtt{d}) = G(1^n,\ \mathtt{r_G}) \ \wedge\ (\mathtt{e_1},\ \mathtt{d_1}) = G(1^n,\ \mathtt{r_{G1}}) \ \wedge\ I(\mathtt{r_{S1}},\ \sigma_{\mathtt{H}})$$
$$\wedge\ \neg\mathtt{FAIL} \rightarrow (\sigma_{\mathtt{H}} = \sigma_{\mathtt{HH}} \ \wedge ...) \ \wedge\ \boxed{\mathbb{P}(\mathtt{FAIL}) < k * \epsilon_{wss}(n)}\}$$
$$\Longrightarrow \{\boxed{\mathbb{P}(\mathtt{FAIL}) < \epsilon_{wss}(n)} \ \wedge \ R_{RND^3}(\mathtt{r_{S1}}, \mathtt{r_G}, \mathtt{r_{G1}}) \ \wedge \ (\mathtt{rsim},\ \mathtt{s}) = S1(1^n,\ \mathtt{r_{S1}})$$
$$\wedge\ (\mathtt{e},\ \mathtt{d}) = G(1^n,\ \mathtt{r_G}) \ \wedge\ (\mathtt{e_1},\ \mathtt{d_1}) = G(1^n,\ \mathtt{r_{G1}}) \ \wedge\ I(\mathtt{r_{S1}},\ \sigma_{\mathtt{H}})$$
$$\wedge\ \neg\mathtt{FAIL} \rightarrow (\sigma_{\mathtt{H}} = \sigma_{\mathtt{HH}} \ \wedge ...)\} \quad \equiv p2$$

我々の貢献(3)

- repeat文と、形式的に表現したゼロ知識証明系の性質を用いて、安全性証明全体を形式化した

$$\{\boxed{\mathbb{P}(\mathtt{true}) < \epsilon_{wss}(n)} \ \wedge \ R_{RND^3}(\mathtt{r_{S1}}, \mathtt{r_G}, \mathtt{r_{G1}}) \ \wedge \ (\mathtt{rsim},\ \mathtt{s}) = S1(1^n,\ \mathtt{r_{S1}})$$

$$\wedge\ (\mathtt{e},\ \mathtt{d}) = G(1^n,\ \mathtt{r_G}) \ \wedge\ (\mathtt{e_1},\ \mathtt{d_1}) = G(1^n,\ \mathtt{r_{G1}}) \ \wedge\ I(\mathtt{r_{S1}},\ \sigma_{\mathtt{H}})$$

$$\wedge\ \neg\mathtt{FAIL} \rightarrow (\sigma_{\mathtt{H}} = \sigma_{\mathtt{HH}} \ \wedge ...) \ \wedge\ \mathbb{P}(\mathtt{FAIL}) < k * \epsilon_{wss}(n)\}$$

$\mathtt{FAIL} := \mathtt{true};$ 代入の公理

$$\{\boxed{\mathbb{P}(\mathtt{FAIL}) < \epsilon_{wss}(n)} \ \wedge \ R_{RND^3}(\mathtt{r_{S1}}, \mathtt{r_G}, \mathtt{r_{G1}}) \ \wedge \ (\mathtt{rsim},\ \mathtt{s}) = S1(1^n,\ \mathtt{r_{S1}})$$

$$\wedge\ (\mathtt{e},\ \mathtt{d}) = G(1^n,\ \mathtt{r_G}) \ \wedge\ (\mathtt{e_1},\ \mathtt{d_1}) = G(1^n,\ \mathtt{r_{G1}}) \ \wedge\ I(\mathtt{r_{S1}},\ \sigma_{\mathtt{H}})$$

弱い条件を消去

$$\wedge\ \neg\mathtt{F} \ldots \wedge \boxed{\mathbb{P}(\mathtt{FAIL}) < k * \epsilon_{wss}(n)}\}$$

$$\Longrightarrow \{\boxed{\mathbb{P}(\mathtt{FAIL}) < \epsilon_{wss}(n)} \ \wedge \ R_{RND^3}(\mathtt{r_{S1}}, \mathtt{r_G}, \mathtt{r_{G1}}) \ \wedge \ (\mathtt{rsim},\ \mathtt{s}) = S1(1^n,\ \mathtt{r_{S1}})$$

$$\wedge\ (\mathtt{e},\ \mathtt{d}) = G(1^n,\ \mathtt{r_G}) \ \wedge\ (\mathtt{e_1},\ \mathtt{d_1}) = G(1^n,\ \mathtt{r_{G1}}) \ \wedge\ I(\mathtt{r_{S1}},\ \sigma_{\mathtt{H}})$$

$$\wedge\ \neg\mathtt{FAIL} \rightarrow (\sigma_{\mathtt{H}} = \sigma_{\mathtt{HH}} \ \wedge ...)\} \quad \equiv p2$$

我々の貢献(3)

[仮定]
(攻撃者の勝率)≒1/2
であるとする

IND-CPA

.||.

A

.||.

AA

.||.

HH

.||.

H

.||.

IND-CCA1

[目標]
(攻撃者の勝率)≒1/2
を示す

- ゲームの橋渡しは

$$\{\mathbb{P}(\mathtt{true}) = 1\}$$

$$\mathtt{r_{G1}} \leftarrow RND;\ \mathtt{r_G} \leftarrow RND;\ \mathtt{ref} \leftarrow REF;$$

$$\ldots$$

$$A4(\mathtt{e_1}, \mathtt{e}, \mathtt{ref}, \mathtt{y_1}, \mathtt{y_2}, \pi, \sigma;\ \mathtt{out});$$

$$A4(\mathtt{e_1}, \mathtt{e}, \mathtt{rsim}, \mathtt{y_{1H}}, \mathtt{y_{2H}}, \pi_{\mathtt{H}}, \sigma_{\mathtt{H}};\ \mathtt{out_H});$$

$$A4(\mathtt{e_1}, \mathtt{e}, \mathtt{rsim}, \mathtt{y_{1HH}}, \mathtt{y_{2HH}}, \pi_{\mathtt{HH}}, \sigma_{\mathtt{HH}};\ \mathtt{out_{HH}});$$

$$\{|\mathbb{P}(\mathtt{out_H} = \mathtt{j}) - \mathbb{P}(\mathtt{out_{HH}} = \mathtt{j})| < p(n) * \epsilon_{wss}(n)$$

$$\wedge\ |\mathbb{P}(\mathtt{out} = \mathtt{j}) - \mathbb{P}(\mathtt{out_H} = \mathtt{j})| < \epsilon_{azk}(n)\}$$

我々の貢献(3)

[仮定]
(攻撃者の勝率)≒1/2
であるとする

IND-CPA

.||.

A

.||.

AA

.||.

HH

.||.

H

.||.

IND-CCA1

[目標]
(攻撃者の勝率)≒1/2
を示す

- ゲームの橋渡しは

$$\{\mathbb{P}(\mathtt{true}) = 1\}$$

$$\mathtt{r_{G1}} \leftarrow RND;\ \mathtt{r_G} \leftarrow RND;\ \mathtt{ref} \leftarrow REF;$$

$$\ldots$$

$$A4(\mathtt{e_1}, \mathtt{e}, \mathtt{ref}, \mathtt{y_1}, \mathtt{y_2}, \pi, \sigma;\ \mathtt{out});$$

$$A4(\mathtt{e_1}, \mathtt{e}, \mathtt{rsim}, \mathtt{y_{1H}}, \mathtt{y_{2H}}, \pi_{\mathtt{H}}, \sigma_{\mathtt{H}};\ \mathtt{out_H});$$

$$A4(\mathtt{e_1}, \mathtt{e}, \mathtt{rsim}, \mathtt{y_{1HH}}, \mathtt{y_{2HH}}\ \pi_{\mathtt{HH}}, \sigma_{\mathtt{HH}};\ \mathtt{out_{HH}});$$

$$\{|\mathbb{P}(\mathtt{out} = \mathtt{j}) - \mathbb{P}(\mathtt{out_{HH}} = \mathtt{j})| < p(n) * \epsilon_{wss}(n) + \epsilon_{azk}(n)\}$$

三角不等式を適用

我々の貢献(3)

[仮定]
(攻撃者の勝率)≒1/2
であるとする

IND-CPA

.||.

A

.||.

AA

.||.

HH

.||.

H

.||.

IND-CCA1

[目標]
(攻撃者の勝率)≒1/2
を示す

- ゲームの橋渡しは

$$\{\mathbb{P}(\mathtt{true}) = 1\}$$

$$\mathtt{r_{G1}} \leftarrow RND;\ \mathtt{r_G} \leftarrow RND;\ \mathtt{ref} \leftarrow REF;$$

$$\ldots$$

$$A4(\mathtt{e_1}, \mathtt{e}, \mathtt{ref}, \mathtt{y_1}\ , \mathtt{y_2}, \pi, \sigma;\ \mathtt{out});$$

$$A4(\mathtt{e_1}, \mathtt{e}, \mathtt{rsim}, \mathtt{y_{1H}}\ , \mathtt{y_{2H}}, \pi_{\mathtt{H}}, \sigma_{\mathtt{H}};\ \mathtt{out_H});$$

$$A4(\mathtt{e_1}, \mathtt{e}, \mathtt{rsim}\ \mathtt{y_{1HH}}, \mathtt{y_{2HH}}\ \pi_{\mathtt{HH}}, \sigma_{\mathtt{HH}};\ \mathtt{out_{HH}});$$

$$\{|\mathbb{P}(\mathtt{out} = \mathtt{j}) - \mathbb{P}(\mathtt{out_{HH}} = \mathtt{j})| < p(n) * \epsilon_{wss}(n) + \epsilon_{azk}(n)\}$$

我々の貢献(3)

[仮定]
(攻撃者の勝率)≒1/2
であるとする

IND-CPA

.||.

A

.||.

AA

.||.

HH

.||.

H

.||.

IND-CCA1

[目標]
(攻撃者の勝率)≒1/2
を示す

- ゲームの橋渡しは

$$\{\mathbb{P}(\mathtt{true}) = 1\}$$

$$\mathtt{r_{G1}} \leftarrow RND;\ \mathtt{r_G} \leftarrow RND;\ \mathtt{ref} \leftarrow REF;$$

$$\ldots$$

$$A4(\mathtt{e_1}, \mathtt{e}, \mathtt{ref}, \mathtt{y_1}\ , \mathtt{y_2}, \pi, \sigma;\ \mathtt{out});$$

直交性を適用

$$A4(\mathtt{e_1}, \mathtt{e}, \mathtt{rsim}\, \mathtt{y_{1HH}}, \mathtt{y_{2HH}}\ \pi_{\mathtt{HH}}, \sigma_{\mathtt{HH}};\ \mathtt{out_{HH}});$$

$$\{|\mathbb{P}(\mathtt{out} = \mathtt{j}) - \mathbb{P}(\mathtt{out_{HH}} = \mathtt{j})| < p(n) * \epsilon_{wss}(n) + \epsilon_{azk}(n)\}$$

目次

- 本研究における検証対象
  - Naor-Yungの暗号構成法
- 形式化の枠組み
  - 確率的ホーア論理
- 我々の貢献
- 結論
- 関連研究
- 今後の課題

結論

- 攻撃ゲームを定義に忠実に形式化できるように
  確率的ホーア論理を改良した
- ゼロ知識証明系の性質を
  ホーアの三つ組として形式化した
- Naor-Yungの構成法による暗号方式が
  IND-CCA1安全性を満たすという証明を、
  確率的ホーア論理で形式化した

目次

- 本研究における検証対象
  - Naor-Yungの暗号構成法
- 形式化の枠組み
  - 確率的ホーア論理
- 我々の貢献
- 結論
- 関連研究
- 今後の課題

関連研究

- Cryptoverif
  - ゲーム列による安全性検証を自動で行うプログラム
  - FDH署名の安全性検証の自動化[Blanchet-Pointcheval2006]
- Certicrypt
  - 定理証明系Coqを用いる検査器
- M. Backes, M. Berg and D. Unruh (2008)
  “A Formal Language for Cryptographic Pseudocode”
  - 定理証明系 Isabelle/HOLを用いる検査器
  - オラクルを表現する文法をもつ

関連研究

- D. Nowak (2007)
  “A framework for game-based security proofs”
  - ML風の関数型言語を定義してゲームを表現し、Coqによって自動検証する
  - ElGamal暗号のIND-CPA安全性証明に適用

目次

- 本研究における検証対象
  - Naor-Yungの暗号構成法
- 形式化の枠組み
  - 確率的ホーア論理
- 我々の貢献
- 結論
- 関連研究
- 今後の課題

今後の課題

- 我々の枠組みを、より複雑な安全性証明に適用する
  - (例)IND-CCA2安全性証明への適用
- さまざまな暗号方式の安全性を扱うために、有用な公理と推論規則を検討する
- 我々の枠組みを定理証明系に実装し、安全性証明の自動化を実現する

ご静聴ありがとうございました