暗号安全性証明の
確率ホーア論理を用いた
形式的検証

東京大学大学院情報理工学系研究科
久保田 貴大

Outline

- 背景
- 確率ホーア論理 (検証の枠組み)
- 公開鍵暗号と安全性の定義 (検証の対象)
- 安全性証明の形式的検証
- 関連研究とまとめ

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きわめて煩雑で検証が難しい [Halevi 2006], [Shoup 2005],…
- 証明の形式的検証技術が提案されている
  - 仮定と推論をすべて明示し、証明の形式的・自動的なチェックを可能にしている
    - 確率ホーア論理 [Corin-Hartog 2002, 2006]
    - 確率プロセス計算 [Blanchet 2005]

      …

Outline

- 背景
- 確率ホーア論理 (検証の枠組み)
- 公開鍵暗号と安全性の定義 (検証の対象)
- 安全性証明の形式的検証
- 関連研究とまとめ

確率ホーア論理

- 確率的実行を含むプログラムの性質を表明する枠組み [Hartog2002, Corin-Hartog2005]
- ホーアトリプルによる表明
  - 「事前条件 p が成り立つとき, プログラム s を実行すると, 事後条件 q が成り立つ」ことを
    $\{p\}\ s\ \{q\}$ と表明
- 枠組みでは, ホーアトリプルを推論規則を用いて導いていく

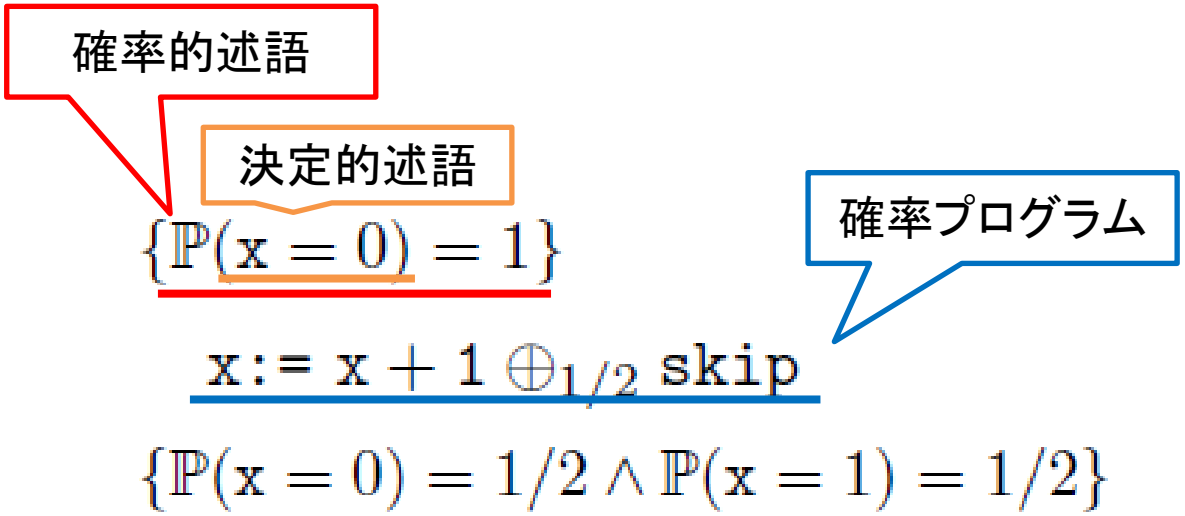
表明の例

$$\{\mathbb{P}(\mathtt{x} = 0) = 1\}$$

$$\mathtt{x := x + 1} \oplus_{1/2} \mathtt{skip}$$

$$\{\mathbb{P}(\mathtt{x} = 0) = 1/2 \wedge \mathbb{P}(\mathtt{x} = 1) = 1/2\}$$

表明の例


確率的述語
決定的述語
確率プログラム
$\{\mathbb{P}(\mathtt{x} = 0) = 1\}$
$\mathtt{x} := \mathtt{x} + 1 \oplus_{1/2} \mathtt{skip}$
$\{\mathbb{P}(\mathtt{x} = 0) = 1/2 \wedge \mathbb{P}(\mathtt{x} = 1) = 1/2\}$

確率プログラム

- 構文

$$
\begin{aligned}
s ::= \;& \texttt{skip} \mid \texttt{x} := e \mid (\texttt{x},...,\texttt{x}) := (e,...,e) \mid s \;;\; s \mid \textbf{if } c \textbf{ then } s \textbf{ else } s \textbf{ fi} \mid \\
& \textbf{repeat } n \textbf{ times } s \textbf{ end} \mid s \oplus_\rho s \mid \mathit{proc}(e,...,e;\texttt{x},...,\texttt{x}) \\
e ::= \;& n \mid \texttt{x} \mid e + e \mid e - e \mid e \cdot e \mid e \;\texttt{div}\; e \mid e \;\texttt{mod}\; e \mid f(e,...,e) \\
c ::= \;& \texttt{true} \mid \texttt{false} \mid \texttt{b} \mid e = e \mid e < e \mid ... \mid c \wedge c \mid c \vee c \mid \neg c \mid c \rightarrow c
\end{aligned}
$$

状態と確率状態

- プログラムの実行は、
  変数環境を更新する

(例) [x → 1, y →0] という環境は、
x := x + 1 というプログラムの実行によって、
[x → 2, y →0] に更新される

状態と確率状態

- 確率プログラムの実行は、
  変数環境の確率分布(確率状態とよぶ)
  を更新する

(例) $1 \cdot [x \to 1, y \to 0]$,

$$1/2 \cdot [x \to 1, y \to 0] + 1/2 \cdot [x \to 2, y \to 0]$$

状態と確率状態

- 確率プログラムの実行は、
  変数環境の確率分布(確率状態とよぶ)
  を更新する

(例) 確率分布 $1 \cdot [x \to 1, y \to 0]$ は、
$x := x + 1 \oplus_{1/2}$ skip という確率プログラムの
実行によって、
$1/2 \cdot [x \to 1, y \to 0] + 1/2 \cdot [x \to 2, y \to 0]$
に更新される

確率プログラム

- 確率プログラムは, 実行前の確率状態を受け取って実行後の確率状態を返す関数として解釈する
- 表示的意味論 $D : L \to (\Theta \to \Theta)$ の定義は

$$\mathcal{D}(\mathtt{skip})(\theta) = \theta$$

$$\mathcal{D}(\mathtt{x} := e)(\sum_i \rho_i \sigma_i) = \sum_i \rho_i \sigma_i[\mathtt{x} \mapsto \sigma_i(e)]$$

$$\mathcal{D}(s; s')(\theta) = \mathcal{D}(s')(\mathcal{D}(s)(\theta))$$

$$\mathcal{D}(\mathbf{if}\ c\ \mathbf{then}\ s\ \mathbf{else}\ s'\ \mathbf{fi})(\theta) = \mathcal{D}(s)(c?\theta) + \mathcal{D}(s')(\neg c?\theta)$$

$$\mathcal{D}(s \oplus_\rho s')(\theta) = \mathcal{D}(s)(\theta) \oplus_\rho \mathcal{D}(s')(\theta)$$

事前･事後条件の述語

- 構文

$$
\begin{aligned}
p ::= \ & \texttt{true} \mid \texttt{false} \mid e_r = e_r \mid e_r < e_r \mid \neg p \mid p \wedge p \mid p \vee p \mid p \rightarrow p \mid \rho \cdot p \mid \\
& p + p \mid p \oplus_\rho p \mid c?p \\
dp ::= \ & \texttt{true} \mid \texttt{false} \mid e = e \mid e < e \mid \neg dp \mid dp \wedge dp \mid dp \vee dp \mid dp \rightarrow dp \mid \\
e_r ::= \ & \rho \mid \mathtt{r} \mid \mathbb{P}(dp) \mid e_r + e_r \mid e_r - e_r \mid e_r * e_r \mid e_r / e_r \mid ...
\end{aligned}
$$

事前・事後条件の述語

- 変数環境 σ のもとで決定的述語 dp が成り立つことを $\sigma \models dp$ と書く
- 充足関係の定義は、

$$\sigma \models \text{true}$$

$$\sigma \not\models \text{false}$$

$$\sigma \models e \ \mathbf{rel}\ e' \quad \text{iff} \quad \sigma(e)\ \mathbf{rel}\ \sigma(e')$$

$$\sigma \models \neg dp \quad \text{iff}\ \sigma \not\models dp$$

$$\sigma \models dp \wedge dp' \quad \text{iff}\ \sigma \models dp \ \text{and}\ \sigma \models dp'$$

$$\sigma \models dp \vee dp' \quad \text{iff}\ \sigma \models dp \ \text{or}\ \ \sigma \models dp'$$

$$\sigma \models dp \rightarrow dp' \quad \text{iff}\ \sigma \models dp \ \text{implies}\ \ \sigma \models dp'$$

確率の解釈

- 確率状態 θ のもとで,
  決定的述語 *dp* が成り立つ確率 **P**(*dp*) の
  解釈は、$[\![\mathbb{P}(dp)]\!]_\theta := \sum_{\sigma \models dp} \theta(\sigma)$ となる。

事前・事後条件の述語

- 確率状態 θ のもとで確率述語 p が成り立つことを $\theta \models p$ と書く
- 充足関係の定義は、

$$\theta \models \rho \cdot p \qquad \text{iff } \exists \theta' : \theta = \rho \cdot \theta' \text{ and } \theta' \models p$$

$$\theta \models p + p' \qquad \text{iff } \exists \theta_1, \theta_2 : \theta = \theta_1 + \theta_2 \text{ and } \theta_1 \models p \text{ and } \theta_2 \models p'$$

$$\theta \models p \oplus_\rho p' \quad \text{iff } \exists \theta_1, \theta_2 : \theta = \theta_1 \oplus_\rho \theta_2 \text{ and } \theta_1 \models p \text{ and } \theta_2 \models p'$$

$$\theta \models c?p \qquad \text{iff } \exists \theta' : \theta = c?\theta' \text{ and } \theta' \models p$$

- 充足される例:

$$\frac{1}{2}[\mathrm{x} \to 0, \mathrm{y} \to 0] + \frac{1}{2}[\mathrm{x} \to 0, \mathrm{y} \to 1] \models \mathbb{P}(\mathrm{x} = \mathrm{y}) = \frac{1}{2}$$

ホーアトリプルの意味

- 表明 {*p*} *s* {*q*} の意味を

  任意の確率分布 θ に対して,
  $\theta \models p$ ならば $\mathcal{D}(s)(\theta) \models q$
  が成り立つ

  と定義する

推論規則

$$\{p\}\ \texttt{skip}\ \{p\} \quad \text{(Skip)} \qquad \{p[\mathtt{x}/e]\}\ \mathtt{x} := e\ \{p\} \quad \text{(Assign)}$$

$$\frac{\{p\}\ s\ \{p'\} \quad \{p'\}\ s'\ \{q'\}}{\{p\}\ s; s'\ \{q\}}\ \text{(Seq)} \qquad \frac{\{p\}\ s\ \{q\} \quad \{p\}\ s'\ \{q'\}}{\{p\}\ s \oplus_\rho s'\ \{q \oplus_\rho q'\}}\ \text{(Prob)}$$

$$\frac{\{p\}\ s\ \{q\} \quad \{p\}\ s\ \{q'\}}{\{p\}\ s\ \{q \wedge q'\}}\ \text{(And)} \qquad \frac{\{p\}\ s\ \{q\} \quad \{p'\}\ s\ \{q\}}{\{p \vee p'\}\ s\ \{q\}}\ \text{(Or)}$$

$$\frac{\{c?p\}\ s\ \{q\} \quad \{\neg c?p\}\ s'\ \{q'\}}{\{p\}\ \textbf{if}\ c\ \textbf{then}\ s\ \textbf{else}\ s'\ \textbf{fi}\ \{q + q'\}}\ \text{(If)}$$

$$\frac{\models p' \to p \quad \{p\}\ s\ \{q\} \quad \models q \to q'}{\{p'\}\ s\ \{q'\}}\ \text{(Cons)}$$

推論の例

$$\dfrac{\dfrac{\dfrac{}{\{\,[x+1=2]\,\}\ x := x+1\ \{\,[x=2]\,\}}(Assign)}{\{\,[x=1]\,\}\ x := x+1\ \{\,[x=2]\,\}}(Cons) \quad \dfrac{\dfrac{}{\{\,[x+2=3]\,\}\ x := x+2\ \{\,[x=3]\,\}}(Assign)}{\{\,[x=1]\,\}\ x := x+2\ \{\,[x=3]\,\}}(Cons)}{\{\,[x=1]\,\}\ (x := x+1) \oplus_{\frac{1}{2}} (x := x+2)\ \{\,[x=2] \oplus_{\frac{1}{2}} [x=3]\,\}}(Prob)$$

$$\dfrac{\{\,[x=1]\,\}\ (x := x+1) \oplus_{\frac{1}{2}} (x := x+2)\ \{\,[x=2] \oplus_{\frac{1}{2}} [x=3]\,\}}{\{\,[x=1]\,\}\ (x := x+1) \oplus_{\frac{1}{2}} (x := x+2)\ \{\,\mathbb{P}(x=2)=\tfrac{1}{2} \wedge \mathbb{P}(x=3)=\tfrac{1}{2}\,\}}(Cons)$$

[Corin-Hartog 2006]

暗号安全性証明の形式化のための準備 [Corin-Hartog2006]

- 一様性の述語

$$R_S(x) \;=\; \forall i : \mathbb{P}(\mathtt{x} = i) = 1/|S|$$

- 集合 $S = \{v_1, \ldots, v_n\}$ から一様にとる操作

$$\mathtt{x} := \mathtt{v_1} \oplus_{1/\mathtt{n}} \left(x := \mathtt{v_2} \oplus_{1/(\mathtt{n}-1)} \left(\cdots \oplus_{1/2} x := \mathtt{v_n} \right) \right)$$

すると

$$\{\, \mathbb{P}(\mathtt{true}) = 1 \,\}\; x \leftarrow S\; \{\, R_S(x) \,\}$$

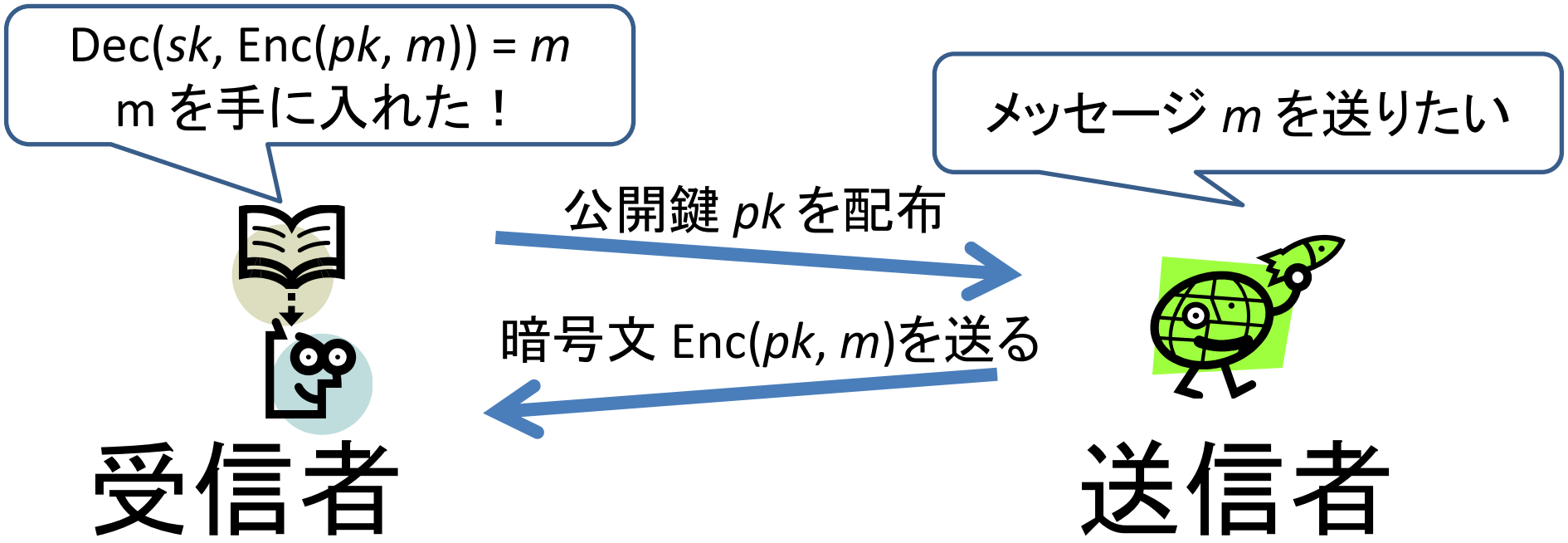
が成り立つ

Outline

- 背景
- 確率ホーア論理 (検証の枠組み)
- 公開鍵暗号と安全性の定義 (検証の対象)
- 安全性証明の形式的検証
- 関連研究とまとめ

公開鍵暗号

- 暗号化用の鍵を公開し (公開鍵 *pk*)
  復号用の鍵を秘密にする (秘密鍵 *sk*)



安全性の定義

- 「ゲーム」によって定義される
  - 「攻撃者がルールで許されているどのような攻撃をしても、暗号文から情報を得る、つまりゲームに勝つ確率が無視できるほど小さい」という定義
  - 強い安全性の定義とは

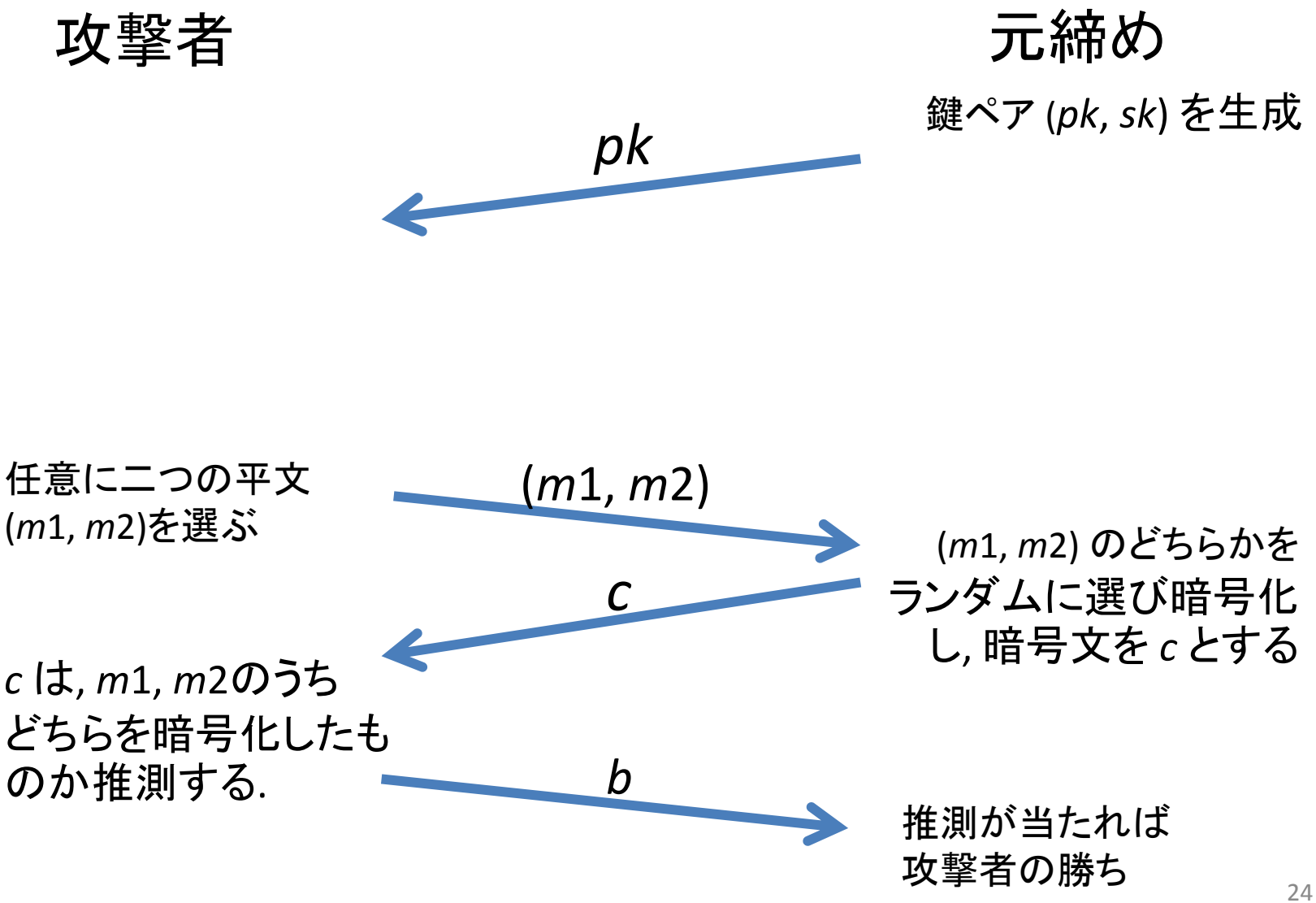
    ルールで許されている攻撃の範囲が広く

    CPA, CCA1, CCA2

    ゲームに勝つ条件が易しいような、定義である

    OW, IND, NM

IND-CPAゲーム


攻撃者
元締め
鍵ペア (pk, sk) を生成
pk
任意に二つの平文
(m1, m2)を選ぶ
(m1, m2)
(m1, m2) のどちらかを
ランダムに選び暗号化
し, 暗号文を c とする
c
c は, m1, m2のうち
どちらを暗号化したも
のか推測する.
b
推測が当たれば
攻撃者の勝ち

IND-CPAゲーム

攻撃者

元締め

鍵ペア (*pk*, *sk*) を生成

pk

対象の公開鍵暗号方式が IND-CPA安全
⇔任意の攻撃者が, その暗号方式に
対するIND-CPAゲームに勝つ
確率が1/2 からほとんどずれない

任意に
(*m*1, *m*

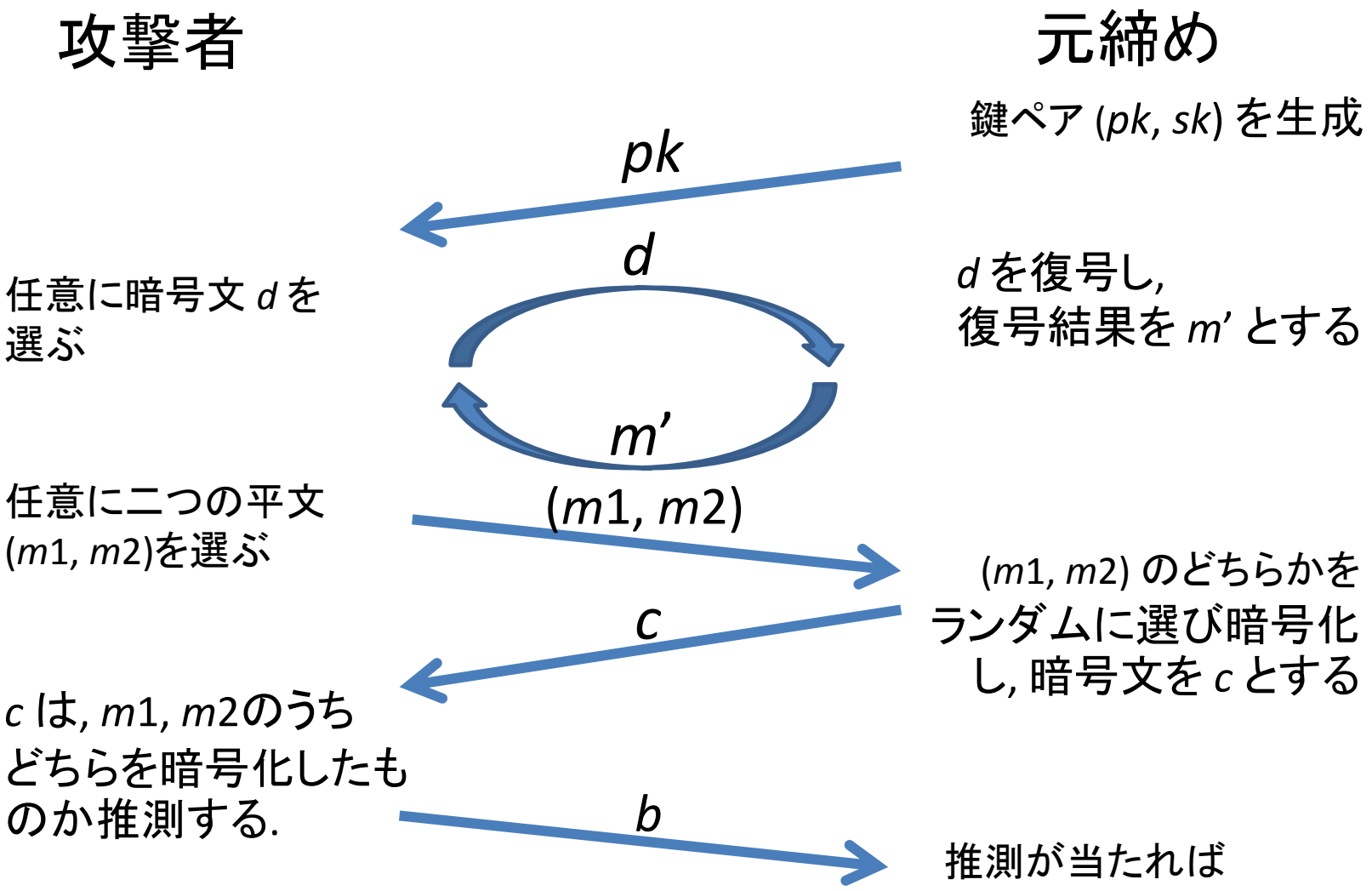
かを
号化
し, 暗号文を *c* とする

c は, *m*1, *m*2のうち
どちらを暗号化したも
のか推測する.

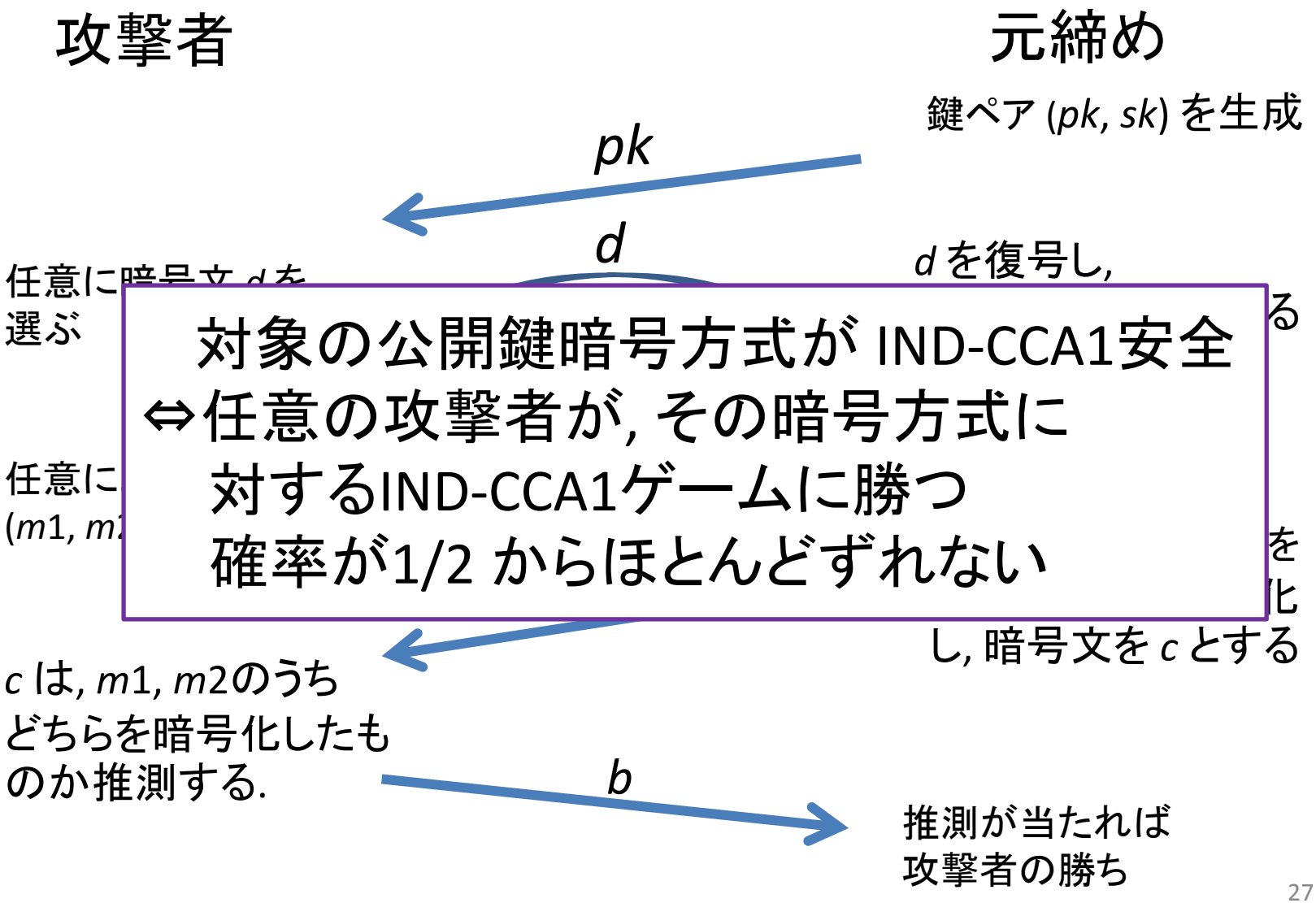
b

推測が当たれば
攻撃者の勝ち

IND-CCA1ゲーム


攻撃者
元締め
鍵ペア (pk, sk) を生成
pk
d
任意に暗号文 d を
選ぶ
d を復号し,
復号結果を m' とする
m'
任意に二つの平文
(m1, m2)を選ぶ
(m1, m2)
(m1, m2) のどちらかを
ランダムに選び暗号化
し, 暗号文を c とする
c
c は, m1, m2のうち
どちらを暗号化したも
のか推測する.
b
推測が当たれば
攻撃者の勝ち

IND-CCA1ゲーム


攻撃者
元締め
鍵ペア (pk, sk) を生成
pk
d
d を復号し,
任意に暗号文 d を
選ぶ
る
対象の公開鍵暗号方式が IND-CCA1安全
⇔任意の攻撃者が, その暗号方式に
対するIND-CCA1ゲームに勝つ
確率が1/2 からほとんどずれない
任意に
(m1, m
を
化
し, 暗号文を c とする
c は, m1, m2のうち
どちらを暗号化したも
のか推測する.
b
推測が当たれば
攻撃者の勝ち

計算論的安全性

- 攻撃者は、鍵の長さに対する確率的多項式時間に限定する
  - 指数時間を許すと、鍵を全部試せてしまう
- 公開鍵暗号の安全性は、確率的多項式時間攻撃者が、特定の計算問題を解くのが困難であることを仮定して証明される
  - 素因数分解問題, 離散対数問題, …

公開鍵暗号方式の例

- IND-CPA安全なもの
  - ElGamal 暗号方式, …
- IND-CCA1安全なもの
  - Naor-Yung 暗号方式, …
- IND-CCA2安全なもの
  - RSA-OAEP 暗号方式,
    Dolev-Dwork-Naor 暗号方式,
    Cremer-Shoup 暗号方式, …

安全性証明の形式的検証

- 確率ホーア論理による検証
  - 攻撃ゲームは確率プログラムとして形式化できる
  - 必要な仮定および安全性は
    ホーアトリプルの形で述べられる
    - 安全性の表明

      { P(true)=1 }
        /* 攻撃ゲーム */
      { “攻撃者が勝つ確率が無視できるほど小さい” }

Outline

- 背景
- 確率ホーア論理 (検証の枠組み)
- 公開鍵暗号と安全性の定義 (検証の対象)
- **安全性証明の形式的検証** [Corin-Hartog2006]
- 関連研究とまとめ

ElGamal暗号

- DDH問題の困難さに基づくIND-CPA安全な暗号
- DDH問題とは
  - 離散対数問題の一種で,
  - 素数位数の群 G の生成元 γ に対して,
    $(\gamma, \gamma^x, \gamma^y, X)$ が与えられたとき, Xが
    γ^{xy} か否かを判定する問題である
- DDH仮定
  - Gの位数が十分大きいとして,
    DDH問題を解くアルゴリズムが存在しないことを
    仮定し, その仮定のもとで安全性が証明される

ElGamal暗号方式

- 鍵生成アルゴリズム

KeyGen(η){

素数位数$q(\eta)$の群Gを選ぶ;

Gの生成元γを選ぶ;

$x \leftarrow \mathbf{Z}_q^*$;

sk := x; $pk := (q, G, \gamma, \gamma^x)$;

return (sk, pk);

}

ElGamal暗号方式

- 暗号化アルゴリズム

Enc(m, q, G, γ, γ^x){
    $y \leftarrow \mathbf{Z}_q^*$;
    c := ($m \cdot \gamma^{xy}$, γ^y);
    return c;
}

ElGamal暗号方式

- 復号アルゴリズム

Dec(x, $m \cdot \gamma^{xy}$, γ^{y}){
    m := $m \cdot \gamma^{xy} \cdot (\gamma^{xy})^{-1}$;
    return m;
}

ゲームと安全性の形式化

ElGamal 暗号に対するIND-CPA ゲームを表すプログラム

$$
\begin{aligned}
&S(\mathtt{v1},\mathtt{v2},\mathtt{v3},\mathtt{v4},\mathtt{v5};\mathtt{x1}) \equiv \\
&\quad \mathtt{m0} := A0(\mathtt{v1},\mathtt{v4});\mathtt{m1} := A1(\mathtt{v1},\mathtt{v4}); \\
&\quad \text{if } \mathtt{v5} = \mathtt{false} \text{ then } \mathtt{tmp} := \mathtt{v3}\cdot\mathtt{m0} \text{ else } \mathtt{tmp} := \mathtt{v3}\cdot\mathtt{m1} \text{ fi}; \\
&\quad \mathtt{b} := A2(\mathtt{v1},\mathtt{v2},\mathtt{tmp},\mathtt{v4}); \\
&\quad \text{if } \mathtt{v5} = \mathtt{b} \text{ then } \mathtt{x1} := true \text{ else } \mathtt{x1} := false \text{ fi};
\end{aligned}
$$

IND-CPA 安全性を表すホーアトリプル (導出したいもの)

$$
\{\mathbb{P}(\mathtt{true}) = 1\}
\quad \mathtt{x} \leftarrow Z_q^*;\ \mathtt{y} \leftarrow Z_q^*;\ \mathtt{r1} \leftarrow RND;\ \mathtt{b1} \leftarrow Bool;\ S(\gamma^{\mathtt{x}}, \gamma^{\mathtt{y}}, \gamma^{\mathtt{xy}}, \mathtt{r1}, \mathtt{b1}; \mathtt{out1})
$$

$$
\{|\mathbb{P}(\mathtt{out1}) - 1/2| \leq \varepsilon_{ddh}\}
$$

S の出力

無視できるほど小さい

DDH仮定の形式化

- 任意のサブプログラム D に対して，
  以下のホーアトリプルが正しいことを
  仮定する

$$\{\mathbb{P}(\mathtt{true}) = 1\}$$
$$\mathtt{x} \leftarrow Z_q^*;\ \mathtt{y} \leftarrow Z_q^*;\ \mathtt{r1} \leftarrow RND;\ \mathtt{b1} \leftarrow Bool;\ D(\gamma^{\mathtt{x}}, \gamma^{\mathtt{y}}, \gamma^{\mathtt{xy}}, \mathtt{r1}, \mathtt{b1}; \mathtt{out1});$$
$$\mathtt{z} \leftarrow Z_q^*;\ \mathtt{r2} \leftarrow RND;\ \mathtt{b2} \leftarrow Bool;\ D(\gamma^{\mathtt{x}}, \gamma^{\mathtt{y}}, \gamma^{\mathtt{z}}, \mathtt{r2}, \mathtt{b2}; \mathtt{out2})$$
$$\{|\mathbb{P}(\mathtt{out1}) - \mathbb{P}(\mathtt{out2})| \leq \varepsilon_{ddh}\}$$

形式検証の流れ

- まず、推論規則を駆使して、以下のホーアトリプルを導く

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

$$\mathtt{x} \leftarrow Z_q^*;\ \mathtt{y} \leftarrow Z_q^*;$$

$$\mathtt{z} \leftarrow Z_q^*;\ \mathtt{r2} \leftarrow RND;\ \mathtt{b2} \leftarrow Bool;\ S(\gamma^{\mathtt{x}}, \gamma^{\mathtt{y}}, \gamma^{\mathtt{z}}, \mathtt{r2}, \mathtt{b2}; \mathtt{out2})$$

$$\{\mathbb{P}(\mathtt{out2}) = 1/2\}$$

形式検証の流れ

- 他の部分と関係ないプログラムを追加しても、ホーアトリプルは正しい。

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

$$\mathtt{x} \leftarrow Z_q^*;\ \mathtt{y} \leftarrow Z_q^*;\ \boxed{\mathtt{r1} \leftarrow RND;\ \mathtt{b1} \leftarrow Bool;\ S(\gamma^{\mathtt{x}}, \gamma^{\mathtt{y}}, \gamma^{\mathtt{xy}}, \mathtt{r1}, \mathtt{b1}; \mathtt{out1});}$$

$$\mathtt{z} \leftarrow Z_q^*;\ \mathtt{r2} \leftarrow RND;\ \mathtt{b2} \leftarrow Bool;\ S(\gamma^{\mathtt{x}}, \gamma^{\mathtt{y}}, \gamma^{\mathtt{z}}, \mathtt{r2}, \mathtt{b2}; \mathtt{out2})$$

$$\{\mathbb{P}(\mathtt{out2}) = 1/2\}$$

形式検証の流れ

- ここで, S(…) を D(…)だと思えば,
  プログラムの部分はDDH問題に他ならない

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

$$\mathtt{x} \leftarrow Z_q^*;\ \mathtt{y} \leftarrow Z_q^*;\ \boxed{\mathtt{r1} \leftarrow RND;\ \mathtt{b1} \leftarrow Bool;\ S(\gamma^{\mathtt{x}}, \gamma^{\mathtt{y}}, \gamma^{\mathtt{xy}}, \mathtt{r1}, \mathtt{b1}; \mathtt{out1});}$$

$$\mathtt{z} \leftarrow Z_q^*;\ \mathtt{r2} \leftarrow RND;\ \mathtt{b2} \leftarrow Bool;\ S(\gamma^{\mathtt{x}}, \gamma^{\mathtt{y}}, \gamma^{\mathtt{z}}, \mathtt{r2}, \mathtt{b2}; \mathtt{out2})$$

$$\{\mathbb{P}(\mathtt{out2}) = 1/2\}$$

DDH仮定

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

$$\mathtt{x} \leftarrow Z_q^*;\ \mathtt{y} \leftarrow Z_q^*;\ \mathtt{r1} \leftarrow RND;\ \mathtt{b1} \leftarrow Bool;\ D(\gamma^{\mathtt{x}}, \gamma^{\mathtt{y}}, \gamma^{\mathtt{xy}}, \mathtt{r1}, \mathtt{b1}; \mathtt{out1});$$

$$\mathtt{z} \leftarrow Z_q^*;\ \mathtt{r2} \leftarrow RND;\ \mathtt{b2} \leftarrow Bool;\ D(\gamma^{\mathtt{x}}, \gamma^{\mathtt{y}}, \gamma^{\mathtt{z}}, \mathtt{r2}, \mathtt{b2}; \mathtt{out2})$$

$$\{|\mathbb{P}(\mathtt{out1}) - \mathbb{P}(\mathtt{out2})| \leq \varepsilon_{ddh}\}$$

形式検証の流れ

- DDH仮定の結論を追加

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

$$\mathtt{x} \leftarrow Z_q^*;\ \mathtt{y} \leftarrow Z_q^*; \quad \mathtt{r1} \leftarrow RND;\ \mathtt{b1} \leftarrow Bool;\ S(\gamma^{\mathtt{x}}, \gamma^{\mathtt{y}}, \gamma^{\mathtt{xy}}, \mathtt{r1}, \mathtt{b1}; \mathtt{out1});$$

$$\mathtt{z} \leftarrow Z_q^*;\ \mathtt{r2} \leftarrow RND;\ \mathtt{b2} \leftarrow Bool;\ S(\gamma^{\mathtt{x}}, \gamma^{\mathtt{y}}, \gamma^{\mathtt{z}}, \mathtt{r2}, \mathtt{b2}; \mathtt{out2})$$

$$\{\mathbb{P}(\mathtt{out2}) = 1/2 \wedge |\mathbb{P}(\mathtt{out1}) - \mathbb{P}(\mathtt{out2})| \leq \varepsilon_{ddh}\}$$

DDH仮定

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

$$\mathtt{x} \leftarrow Z_q^*;\ \mathtt{y} \leftarrow Z_q^*;\ \mathtt{r1} \leftarrow RND;\ \mathtt{b1} \leftarrow Bool;\ D(\gamma^{\mathtt{x}}, \gamma^{\mathtt{y}}, \gamma^{\mathtt{xy}}, \mathtt{r1}, \mathtt{b1}; \mathtt{out1});$$

$$\mathtt{z} \leftarrow Z_q^*;\ \mathtt{r2} \leftarrow RND;\ \mathtt{b2} \leftarrow Bool;\ D(\gamma^{\mathtt{x}}, \gamma^{\mathtt{y}}, \gamma^{\mathtt{z}}, \mathtt{r2}, \mathtt{b2}; \mathtt{out2})$$

$$\{|\mathbb{P}(\mathtt{out1}) - \mathbb{P}(\mathtt{out2})| \leq \varepsilon_{ddh}\}$$

形式検証の流れ

- 三角不等式を用いて 変数 out2 を削除

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

$$\mathtt{x} \leftarrow Z_q^*;\ \mathtt{y} \leftarrow Z_q^*; \quad \mathtt{r1} \leftarrow RND;\ \mathtt{b1} \leftarrow Bool;\ S(\gamma^{\mathtt{x}}, \gamma^{\mathtt{y}}, \gamma^{\mathtt{xy}}, \mathtt{r1}, \mathtt{b1}; \mathtt{out1});$$

$$\mathtt{z} \leftarrow Z_q^*;\ \mathtt{r2} \leftarrow RND;\ \mathtt{b2} \leftarrow Bool;\ S(\gamma^{\mathtt{x}}, \gamma^{\mathtt{y}}, \gamma^{\mathtt{z}}, \mathtt{r2}, \mathtt{b2}; \mathtt{out2})$$

$$\{|\mathbb{P}(\mathtt{out1}) - 1/2| \leq \varepsilon_{ddh}\}$$

形式検証の流れ

- 変数 out2 に関係ある部分はもう不要なので削除

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

$$\mathtt{x} \leftarrow Z_q^*;\ \mathtt{y} \leftarrow Z_q^*; \quad \mathtt{r1} \leftarrow RND;\ \mathtt{b1} \leftarrow Bool;\ S(\gamma^{\mathtt{x}}, \gamma^{\mathtt{y}}, \gamma^{\mathtt{xy}}, \mathtt{r1}, \mathtt{b1}; \mathtt{out1});$$

$$\{|\mathbb{P}(\mathtt{out1}) - 1/2| \leq \varepsilon_{ddh}\}$$

形式検証の流れ

- このホーアトリプルは、
  ElGamal 暗号のIND-CPA安全性を表明している

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

$$\mathtt{x} \leftarrow Z_q^*;\ \mathtt{y} \leftarrow Z_q^*; \quad \mathtt{r1} \leftarrow RND;\ \mathtt{b1} \leftarrow Bool;\ S(\gamma^{\mathtt{x}}, \gamma^{\mathtt{y}}, \gamma^{\mathtt{xy}}, \mathtt{r1}, \mathtt{b1}; \mathtt{out1});$$

$$\{|\mathbb{P}(\mathtt{out1}) - 1/2| \leq \varepsilon_{ddh}\}$$

(Q.E.D.)

関連研究

- Naor-Yung 暗号の検証 [久保田ら 2009]
  - IND-CCA1 というより強い安全性の証明に、確率ホーア論理を適用した

参考 : 自動検証に関する研究

- AVISPA http://www.avispa-project.org/
  - いくつかの暗号プロトコルに対する未知の攻撃を発見 [Armandoら 2005]
- CryptoVerif [Blanchet2005]
  - Kerberos認証プロトコル [Blanchetら. 2008]
  - FDH署名スキーム [Blanchet-Pointcheval 2006]
- EasyCrypt [Barthelら 2011]
  - Cramer-Shoup 暗号など

まとめ

- 暗号安全性証明は煩雑で検証が難しい
- 安全性証明の誤りを防ぐため、
  形式的検証技術が用いられている
- 確率ホーア論理を用いた、安全性証明の
  形式的検証の研究を紹介した