サイドチャネル攻撃に対する安全性の確率的ホーア論理を用いた形式的検証

久保田貴大　萩谷昌己
東京大学大学院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
- 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
  - 直接的方法の一つとして確率的ホーア論理がある
    - ElGamal暗号のIND-CPA安全性[Corin-Hartog2006]
    - Naor-Yung暗号のIND-CCA安全性[久保田et al.2009]
- 別の種類の安全性証明に対する有効性を明らかにしたい
  - たとえばサイドチャネル攻撃を考慮した安全性は従来のものよりも複雑になるであろう

研究の概要

- 確率的ホーア論理[Corin-Hartog2006]を用いて、二種類の安全性証明を検証した
  - Micali-Reyzinのモデル[Micali-Reyzin2005]に基づいたビットコミットメントプロトコルの秘匿性証明
  - サイドチャネル攻撃に耐性を持つストリーム暗号の安全性証明の補題[Dziembowski-Pietrzak2008]
- 検証を見通し良くするため、有用な推論規則を導入した

目次

- 確率的ホーア論理
- 検証(1)　ビットコミットメント
- 検証(2)　ストリーム暗号
- 我々の貢献
- 結論
- 今後の課題

目次

- 確率的ホーア論理
  - ホーアトリプルの意味
  - 有用な推論規則
- 検証(1)　ビットコミットメント
- 検証(2)　ストリーム暗号
- 我々の貢献
- 結論
- 今後の課題

確率的ホーア論理

- 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

$$s ::= \mathtt{skip} \mid \mathtt{x} := e \mid (\mathtt{x},...,\mathtt{x}) := (e,...,e) \mid s\ ;\ s \mid \mathbf{if}\ c\ \mathbf{then}\ s\ \mathbf{else}\ s\ \mathbf{fi} \mid$$
$$\mathbf{repeat}\ n\ \mathbf{times}\ s\ \mathbf{end} \mid s \oplus_\rho s \mid proc(e,...,e;\mathtt{x},...,\mathtt{x})$$

$$p ::= \mathtt{true} \mid \mathtt{false} \mid e_r = e_r \mid e_r < e_r \mid \neg p \mid p \wedge p \mid p \vee p \mid p \to p \mid \rho \cdot p \mid$$
$$p + p \mid p \oplus_\rho p \mid c?p$$

- ホーアトリプル　$\{p\}\ s\ \{q\}$
  - 事前条件pが成り立つときにプログラムsを実行すると事後条件qが成り立つ

ホーアトリプルの意味

- 確率状態θのもとで、述語を解釈する

$$\theta = \sum_i \rho_i \sigma_i$$

  - (例) $1/2[\mathrm{x} \to 1] + 1/2[\mathrm{x} \to 2] \models \mathrm{P}(\mathrm{x} = 1) = 1/2$
- プログラムは、確率状態を操作する関数に解釈される.
  D: プログラム→(確率状態→確率状態)
  (例) $D(\mathrm{y} := 0)(1/2[\mathrm{x} \to 1] + 1/2[\mathrm{x} \to 2])$

$$= 1/2[\mathrm{x} \to 1, \mathrm{y} \to 0] + 1/2[\mathrm{x} \to 2, \mathrm{y} \to 0]$$

- $\{p\}\ s\ \{q\}$ が正しいとは
  - 任意の確率状態θに対して、$\theta \models p$ ならば $D(s)(\theta) \models q$

基本的な推論規則[Corin-Hartog2006]

$$\{p\}\ \mathtt{skip}\ \{p\} \quad \text{(Skip)}$$

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

$$\frac{\{p\}\ s\ \{p'\} \quad \{p'\}\ s'\ \{q'\}}{\{p\}\ s; s'\ \{q\}} \quad \text{(Seq)}$$

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

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

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

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

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

証明に有用な推論規則(貢献1)

(乱択)

$$\frac{\{p\}\ \mathtt{r} := 0; s\ \{q\}, ..., \{p\}\ \mathtt{r} := n; s\ \{q\}}{\{p\}\ \mathtt{r} \leftarrow RND; s\ \{q\}}$$

(独立な式の追加)

$$\frac{For\ all\ procedure\ A.\quad \{p\}\ A(e_1, ..., e_n; \mathtt{x})\ \{q\}}{For\ all\ procedure\ A'.\quad \{p \wedge I(e_1, e) \wedge ... \wedge I(e_n, e)\} A'(e_1, ..., e_n, e; \mathtt{x}) \{q\}}$$

例

- f(x)が一方向性関数であることの形式化は、

$\{R(x) \wedge y = f(x)\}$　　$D(y ; x')$　　$\{P(x=x') < \varepsilon\}$

例

- xと独立な変数zを、攻撃者が受け取っても、逆関数を計算するアドバンテージにならない

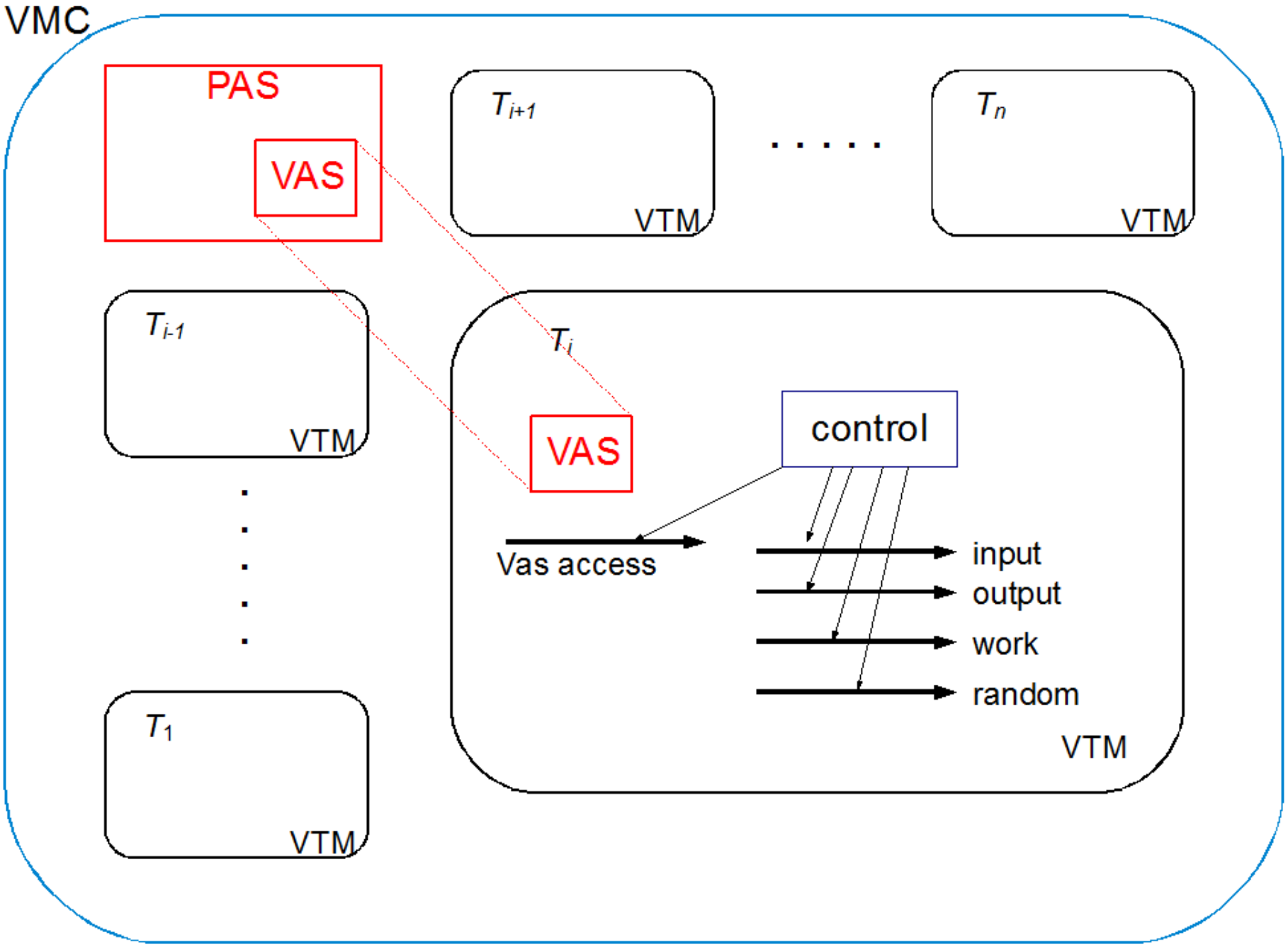
$$\frac{\{R(x) \wedge y = f(x)\} \qquad D(y\,;\,x') \quad \{P(x=x') < \varepsilon\}}{\{R(x) \wedge y = f(x) \wedge I(x, z)\} \quad D'(y, z\,;\,x') \; \{P(x=x') < \varepsilon\}}$$

目次

- 確率的ホーア論理
- 検証(1)　ビットコミットメント
  - サイドチャネル攻撃を受けるハードウェアのモデルについて
  - 検証対象のビットコミットメントプロトコルについて
  - 主定理について
- 検証(2)　ストリーム暗号
- 我々の貢献
- 結論
- 今後の課題

Micali-ReyzinのComputational Model

- Abstract Virtual-Memory Computers (VMC)
  - Virtual memory Turing machine (VTM) の列
    $T = (T_1, \ldots, T_n)$
  - T1 だけが、外部に対する入出力と
    サブルーチンコール($T_2, \ldots, T_n$の呼出し)が可能
  - 各VTMは、入力、出力、作業、乱数のテープを
    持ち、T_1はそれらに加えてサブルーチンコール用の
    テープをもつ
  - 各VTMは仮想アドレス空間とそのアクセス用テープ
    をもつ

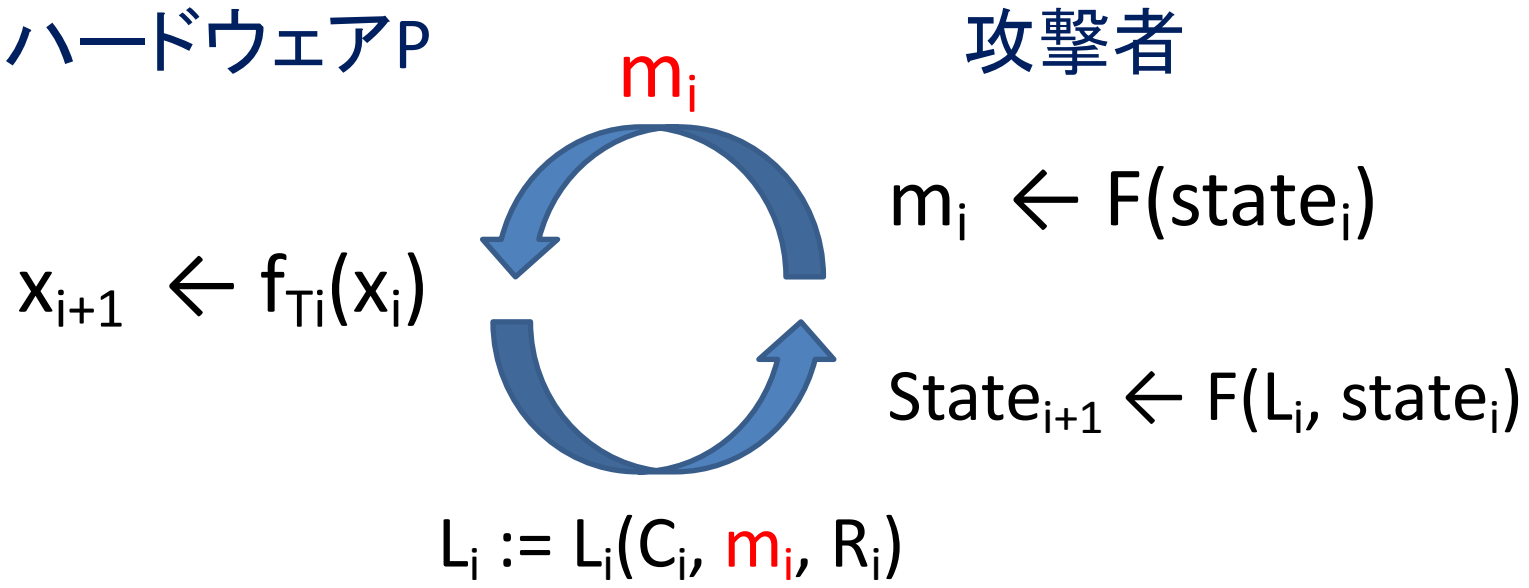

VMC
PAS
VAS
T_{i+1}
VTM
T_n
VTM
T_{i-1}
VTM
T_i
VAS
control
Vas access
input
output
work
random
VTM
T_1
VTM

Computational Model

- Physical virtual memory Turing machine の列 $P = (P_1, \ldots, P_n)$
- $P_i = (L_i, T_i)$
  - T_i は VTM
  - $L_i(\cdot, \cdot, \cdot)$ は T_iのコンフィグ、攻撃者の観測装置の情報、乱数を受け取って、漏れる情報を返す
    - 漏洩関数と呼ばれる

サイドチャネル攻撃のモデル

- ハードウェアP が、関数$f_P(x) = f_{Tn}(f_{Tn-1}(\ldots f_{T2}(x)\ldots)$ を計算するとき、攻撃者は各VTMに対して、適応的に攻撃をする



サイドチャネル攻撃のステートメント

- 入力x_Pを受け取って出力y_Pを計算するハードウェアPにサイドチャネル攻撃をする攻撃者が、入力x_Fを受け取りy_Fを出力することを

$$y_P \leftarrow P(x_P) \Rightarrow F(x_F) \rightarrow y_F$$

と書くことにする

サイドチャネル攻撃の形式化

$$y_P \leftarrow P(x_P) \Rightarrow F(x_F) \rightarrow y_F$$

$\equiv$

$i := 2;\ x_2^P := x_P;\ x_2^F := x_F;$

repeat $n-1$ **times**

$(x_{i+1}^P, C_i) := f_{A_i}(x_i^P, R_i^P)$

$M_i := F(x_i^F)$

$L_i := L_i(C_i, M_i, R_i)$

$x_{i+1}^F := F(x_i^F, L_i)$

$i := i+1$

end

$y_P := x_{n+1}^P;\ y_F := x_{n+1}^F$

安全性の定義

- Durable function
  ハードウェアPがdurable functionであるとは、

$$p_k^P = \Pr[x \xleftarrow{R} \{0,1\}^k;\ y \leftarrow P(x) \Rightarrow F(1^k) \rightarrow state :\ F(state, y)=1]$$

$$p_k^R = \Pr[x \xleftarrow{R} \{0,1\}^k;\ y \leftarrow P(x) \Rightarrow F(1^k) \rightarrow state;\ z \xleftarrow{R} \{0,1\}^k:\ F(state, z)=1]$$

  としたとき、
  $|p_k^P - p_k^R|$ がセキュリティパラメタ k
  に対して無視できる関数になることである

ビットコミットメント

- Sender S と Receiver R の二者間プロトコル
  - 1. Sは、ビットbを任意に選び、
    bがわからないようにしてRに送る
  - 2. Sは、好きな時間にRにbを開示する。

1.で送ってしまったビットbを誰も改ざんできないこと(拘束性)と、2.で開示するまでS以外にビットbが知られないこと(秘匿性)が、要求される性質である。

一方向性関数→ビットコミットメント

- ハードコア述語hを持つような、
  全単射の一方向性関数fがあれば、
  ビットコミットメントを作れる
  1. ビットbを選んで、
     $s \leftarrow \{0, 1\}^k$
     $y \leftarrow f(s)$
     $v \leftarrow h(s)$ xor b を計算して、(y, v)をコミット
  2. s, bを開示

サイドチャネルを考えると

- 1. ビットbを選んで、
  $s \leftarrow \{0, 1\}^k$
  $y \leftarrow P(s)$ ⇒ F(state) → state
  $v \leftarrow h(s)$ xor b ⇒ F(state) → state
  を計算して、(y, v)をコミット
- 2. s, bを開示

Pやxorに関する適当な仮定から、
秘匿性を示したい

検証のターゲット

{P(true) = 1}

σ0 ← RND;

s0 ← RND;

y0 := P(s0) ⇒ F(σ0) → σ0;

b0 := b(s0);

c0 := 0 xor b0 ⇒ F(σ0) → σ0;

v0 := F(y0, c0, σ0)

σ1 ← RND;

s1 ← RND;

y1 := P(s1) ⇒ F(σ1) → σ1;

b1 := b(s1);

c1 := 1 xor b1 ⇒ F(σ1) → σ1;

v1 := F(y1, c1, σ1)

{ | P(v0 = 0) - P(v1 = 0) | < ε}

検証1の結果

- 「PがDurable permutationで、
  f_Pがnatural hardcore bitをもち、
  サイドチャネル攻撃に対して安全なxor演算
  があれば、このビットコミットメントは
  秘匿性をもつ」
- この証明は、すべて形式化できた

目次

- 確率的ホーア論理
- 検証(1)　ビットコミットメント
- 検証(2)　ストリーム暗号
  - 安全性の定義について
  - 検証対象について
- 我々の貢献
- 結論
- 今後の課題

Dziembowski-Pietrzak暗号

- サイドチャネル攻撃に耐性をもつ
  ストリーム暗号
- 安全な乱数抽出器と乱数生成器の存在を
  仮定する

安全性の定義

- 鍵を生成する計算によって情報が漏れる
  - 漏洩関数は返り値が有限ビットであるような任意の関数とする
- 安全性は、
「i番目までの鍵と、それまでにサイドチャネルから得た情報をもってしても、i+1番目の鍵と乱数列が区別できない」
ことであると定義する

検証対象

- 乱数生成器の性質に関する補題

仮定
ある集合*S*の
任意の元 *a* に対して、
ある攻撃者*D*が存在して、

$$\{\epsilon_{prg} < \frac{\epsilon^2}{2^\lambda} - 2^{-\Delta}\}$$
$$\mathbf{seed} \leftarrow \{0,1\}^n;$$
$$\mathbf{r} := prg(\mathbf{seed});$$
$$\{\ \Pr(f(\mathbf{seed}) \in S)) > \epsilon \wedge$$
$$\forall Z.\ \mathrm{H}_\infty(Z) > m - \Delta \rightarrow$$
$$|\Pr(D(\mathbf{r}) = 1 | f(\mathbf{seed}) = a) - \Pr(D(Z) = 1)| > \epsilon\}$$

結論
ある攻撃者*D*と、
β ∈ {0, 1} に対して、

$$\{\epsilon_{prg} < \frac{\epsilon^2}{2^\lambda} - 2^{-\Delta}\}$$
$$\mathbf{seed} \leftarrow \{0,1\}^n;$$
$$\mathbf{r} := prg(\mathbf{seed});\quad \mathbf{z} \leftarrow \{0,1\}^m$$
$$\{\Pr(D(\mathbf{r}) = \beta) - \Pr(D(\mathbf{z}) = \beta) > \frac{\epsilon^2}{2^\lambda} - 2^{-\Delta} > \epsilon_{prg}\}$$

検証対象

- 乱数生成器の性質に関する補題

仮定
ある集合*S*の
任意の元 *a* に対して、
ある攻撃者*D*が存在して、

$$\{\epsilon_{prg} < \frac{\epsilon^2}{2^\lambda} - 2^{-\Delta}\}$$
$$\mathtt{seed} \leftarrow \{0,1\}^n;$$
$$\mathtt{r} := prg(\mathtt{seed});$$
$$\{\ \Pr(f(\mathtt{seed}) \in S)) > \epsilon \wedge$$
$$\forall Z.\ \mathrm{H}_\infty(Z) > m - \Delta \rightarrow$$
$$|\Pr(D(\mathtt{r}) = 1 | f(\mathtt{seed}) = a) - \Pr(D(Z) = 1)| > \epsilon\}$$

我々の枠組みでは
表現できない

結論
ある攻撃者*D*と、
β ∈ {0, 1} に対して、

$$\{\epsilon_{prg} < \frac{\epsilon^2}{2^\lambda} - 2^{-\Delta}\}$$
$$\mathtt{seed} \leftarrow \{0,1\}^n;$$
$$\mathtt{r} := prg(\mathtt{seed});\quad \mathtt{z} \leftarrow \{0,1\}^m$$
$$\{\Pr(D(\mathtt{r}) = \beta) - \Pr(D(\mathtt{z}) = \beta) > \frac{\epsilon^2}{2^\lambda} - 2^{-\Delta} > \epsilon_{prg}\}$$

解決法

- 確率的実行のプログラムが、プログラム変数の確率分布をつくる
- $X := v_1 \oplus_{\rho 1} (X := v_2 \oplus_{\rho 2} (\ldots \oplus_{\rho n} X := v_n) \ldots)$ の形のプログラムにおいて、$v_1,\ldots,v_n$, $\rho_1,\ldots,\rho_n$ に適当な値を代入すれば、xが任意の確率分布に従うようにできる

等価なホーアトリプル

- 乱数生成器の性質に関する補題

仮定
ある集合*S*の
任意の元 *a* に対して、
ある攻撃者*D*が存在して、
任意の$\rho_1,\ldots,\rho_{2m}$に
対して

$$\{\epsilon_{prg} < \frac{\epsilon^2}{2^\lambda} - 2^{-\Delta}\}$$
$$\mathbf{seed} \leftarrow \{0,1\}^n;$$
$$\mathbf{r} := prg(\mathbf{seed});$$
$$\mathbf{z} := 0 \oplus_{\rho_1} (\ldots \oplus_{\rho_{2^m}} (\mathbf{z} := 2^m - 1)\ldots)$$
$$\{\ \Pr(f(\mathbf{seed}) \in S)) > \epsilon \wedge$$
$$\mathrm{H}_\infty(\mathbf{z}) > m - \Delta \rightarrow$$
$$|\Pr(D(\mathbf{r}) = 1 | f(\mathbf{seed}) = a) - \Pr(D(\mathbf{z}) = 1)| > \epsilon\}$$

結論
ある攻撃者*D*と、
β ∈ {0, 1} に対して、

$$\{\epsilon_{prg} < \frac{\epsilon^2}{2^\lambda} - 2^{-\Delta}\}$$
$$\mathbf{seed} \leftarrow \{0,1\}^n;$$
$$\mathbf{r} := prg(\mathbf{seed}); \quad \mathbf{z} \leftarrow \{0,1\}^m$$
$$\{\Pr(D(\mathbf{r}) = \beta) - \Pr(D(\mathbf{z}) = \beta) > \frac{\epsilon^2}{2^\lambda} - 2^{-\Delta} > \epsilon_{prg}\}$$

等価なホーアトリプル

- z が一様分布に従うように, $\rho_1,\ldots\rho_n$を決めると

仮定
ある集合*S*の
任意の元 *a* に対して、
ある攻撃者*D*が存在して、

$$\{\epsilon_{prg} < \frac{\epsilon^2}{2^\lambda} - 2^{-\Delta}\}$$
$$\mathbf{seed} \leftarrow \{0,1\}^n;$$
$$\mathbf{r} := prg(\mathbf{seed});$$
$$\mathbf{z} \leftarrow \{0,1\}^m$$
$$\{\ \Pr(f(\mathbf{seed}) \in S)) > \epsilon\ \wedge \mathrm{H}_\infty(\mathbf{z}) = m \wedge$$
$$\mathrm{H}_\infty(\mathbf{z}) > m - \Delta \rightarrow$$
$$|\Pr(D(\mathbf{r}) = 1 | f(\mathbf{seed}) = a) - \Pr(D(\mathbf{z}) = 1)| > \epsilon\}$$

結論
ある攻撃者*D*と、
β ∈ {0, 1} に対して、

$$\{\epsilon_{prg} < \frac{\epsilon^2}{2^\lambda} - 2^{-\Delta}\}$$
$$\mathbf{seed} \leftarrow \{0,1\}^n;$$
$$\mathbf{r} := prg(\mathbf{seed});\quad \mathbf{z} \leftarrow \{0,1\}^m$$
$$\{\Pr(D(\mathbf{r}) = \beta) - \Pr(D(\mathbf{z}) = \beta) > \frac{\epsilon^2}{2^\lambda} - 2^{-\Delta} > \epsilon_{prg}\}$$

等価なホーアトリプル

- z が一様分布に従うように, ρ1,…ρnを決めると

仮定
ある集合*S*の
任意の元 *a* に対して、
ある攻撃者*D*が存在して、

$$\{\epsilon_{prg} < \frac{\epsilon^2}{2^\lambda} - 2^{-\Delta}\}$$
$$\mathbf{seed} \leftarrow \{0,1\}^n;$$
$$\mathbf{r} := prg(\mathbf{seed});$$
$$\mathbf{z} \leftarrow \{0,1\}^m$$
$$\{\ \Pr(f(\mathbf{seed}) \in S)) > \epsilon\ \wedge \mathrm{H}_\infty(\mathbf{z}) = m \wedge$$
$$\mathrm{H}_\infty(\mathbf{z}) > m - \Delta \rightarrow$$
$$|\Pr(D(\mathbf{r}) = 1 | f(\mathbf{seed}) = a) - \Pr(D(\mathbf{z}) = 1)| > \epsilon\}$$

結論
ある攻撃者*D*と、
β ∈ {0, 1} に対して、

$$\{\epsilon_{prg} < \frac{\epsilon^2}{2^\lambda} - 2^{-\Delta}\}$$
$$\mathbf{seed} \leftarrow \{0,1\}^n;$$
$$\mathbf{r} := prg(\mathbf{seed});\quad \mathbf{z} \leftarrow \{0,1\}^m$$
$$\{\Pr(D(\mathbf{r}) = \beta) - \Pr(D(\mathbf{z}) = \beta) > \frac{\epsilon^2}{2^\lambda} - 2^{-\Delta} > \epsilon_{prg}\}$$

等価なホーアトリプル

- あとは確率を計算することによって、結論に到達できる

仮定
ある集合*S*の
任意の元 *a* に対して、
ある攻撃者*D*が存在して、

$$\{\epsilon_{prg} < \frac{\epsilon^2}{2^\lambda} - 2^{-\Delta}\}$$
$$\mathbf{seed} \leftarrow \{0,1\}^n;$$
$$\mathbf{r} := prg(\mathbf{seed});$$
$$\mathbf{z} \leftarrow \{0,1\}^m$$
$$\{\ \Pr(f(\mathbf{seed}) \in S)) > \epsilon \wedge$$
$$|\Pr(D(\mathbf{r}) = 1 | f(\mathbf{seed}) = a) - \Pr(D(\mathbf{z}) = 1)| > \epsilon\}$$

結論
ある攻撃者*D*と、
β ∈ {0, 1} に対して、

$$\{\epsilon_{prg} < \frac{\epsilon^2}{2^\lambda} - 2^{-\Delta}\}$$
$$\mathbf{seed} \leftarrow \{0,1\}^n;$$
$$\mathbf{r} := prg(\mathbf{seed}); \quad \mathbf{z} \leftarrow \{0,1\}^m$$
$$\{\Pr(D(\mathbf{r}) = \beta) - \Pr(D(\mathbf{z}) = \beta) > \frac{\epsilon^2}{2^\lambda} - 2^{-\Delta} > \epsilon_{prg}\}$$

目次

- 確率的ホーア論理
- 検証(1)　ビットコミットメント
- 検証(2)　ストリーム暗号
- **我々の貢献**
- 結論
- 今後の課題

我々の貢献(1)

- 証明に有用な推論規則を導入した
  - 検証1の安全性証明が形式化できた

(乱択)

$$\frac{\{p\}\ \mathtt{r} := 0; s\ \{q\}, ..., \{p\}\ \mathtt{r} := n; s\ \{q\}}{\{p\}\ \mathtt{r} \leftarrow RND; s\ \{q\}}$$

(独立な式の追加)

$$\frac{\textit{For all procedure } A.\quad \{p\}\ A(e_1, ..., e_n; \mathtt{x})\ \{q\}}{\textit{For all procedure } A'.\quad \{p \wedge I(e_1, e) \wedge ... \wedge I(e_n, e)\} A'(e_1, ..., e_n, e; \mathtt{x}) \{q\}}$$

我々の貢献(1)

{P(true) = 1}
σ ← RND;
s ← RND;
y := P(s) ⇒ F(σ) → σ;
b := b(s);
v := F(y, σ);

σ~ ← RND;
s~ ← RND;
z ← RND;
y~ := P(s~) ⇒ F(σ~) → σ~;
b~ := b(s~);
v~ := F(z, σ~);
{ | P(v = 0) - P(v~ = 0) | < ε_dr}

目的のゲームでは、攻撃者にハードコア述語をインプットする

我々の貢献(1)

{P(true) = 1}
σ ← RND;
s ← RND; d ← BOOL;
y := P(s) ⇒ F(σ) → σ;
b := b(s);
v := F(y, d, σ);

σ~ ← RND;
s~ ← RND; d~ ← BOOL;
z ← RND;
y~ := P(s~) ⇒ F(σ~) → σ~;
b~ := b(s~);
v~ := F(z, d~, σ~);
{ | P(v = 0) - P(v~ = 0) | < ε_dr}

導入した規則(2)を適用

我々の貢献(1)

{P(true) = 1}
σ ← RND;
s ← RND; d ← BOOL;
y := P(s) ⇒ F(σ) → σ;
b := b(s);
v := F(y, b, σ);

σ~ ← RND;
s~ ← RND; d~ ← BOOL;
z ← RND;
y~ := P(s~) ⇒ F(σ~) → σ~;
b~ := b(s~);
v~ := F(z, b~, σ~);
{ | P(v = 0) - P(v~ = 0) | < ε_dr + 2*ε_hc}

ハードコア述語の
仮定より

我々の貢献(2)

- 検証(1) Micali-Reyzinモデルに基づいて
  ビットコミットメントの安全性証明を検証した
  - 漏洩オラクルを形式化した
  - ビットコミットメントの秘匿性を形式化し、
    安全性証明を検証した
    - Natural hardcore bitをもつDurable one-way permutation,
      サイドチャネル攻撃に耐性をもつXOR演算を仮定
      - 従来のプロトコルたちの安全性を得るためには、
        強い仮定が必要であると予想される

我々の貢献(3)

- (検証2)Diembouwski-Pietrzakの
  ストリーム暗号の安全性証明の補題を検証した
  - 「確率変数の量化」は、
    確率的ホーア論理で扱えなかった
  - 非形式的に「等価」だと議論した
    ホーアトリプルを用いた

結論

- 証明の検証に有用な推論規則を導入した
- 確率的ホーア論理を用いて
  - Micali-Reyzinモデルの漏洩オラクルを形式化した
  - Diembowski-Pietrozakのストリーム暗号の安全性証明のための補題を形式化した

今後の課題

- より多くの暗号スキームに対して検証を行い、確率的ホーア論理の有効性を調べていく
  - 必要に応じて拡張する
- 検証に有用な推論規則を検討し導入する
- 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

参照文献

- [Corin-Hartog2006] R. Corin. A probabilistic Hoare-style logic for game-based cryptographic proofs. In *ICALP'06, volume 4052 of LNCS,* pages 252–263. Springer, July 2006.
- [Micali-Reyzin2003] Micali and L. Reyzin. A model for physically observable cryptography. Manuscript, 2003.
- [Dziembowski-Pietrozak2008] Dziembowski, S., Pietrzak, K.: Leakage-Resilient Cryptography. In: The proceedings of FOCS 2008, Philadelphia, USA, pp. 293–302 (October 2008)
- [久保田et al.2009]久保田貴大, 川本裕輔, 萩谷昌己, 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, JSIAM FAIS, 2009年3月

ご静聴ありがとうございました

プログラムの意味

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

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

$$\mathcal{D}((\mathtt{x_1}, ..., \mathtt{x_n}) := (e_1, ..., e_n))(\sum_i \rho_i\sigma_i) = \sum_i \rho_i\sigma_i[\mathtt{x_1} \mapsto \sigma_i(e_1), ..., \mathtt{x_n} \mapsto \sigma_i(e_n)]$$

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

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

$$\mathcal{D}(\textbf{repeat } n \textbf{ times } s \textbf{ end})(\theta) = (\mathcal{D}(s))^n(\theta)$$

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

$$\textit{where } (\mathcal{D}(s))^n(\theta) = \mathcal{D}(s)((\mathcal{D}(s))^{n-1}(\theta)) \quad \textit{and} \quad (\mathcal{D}(s))^0(\theta) = \theta$$

述語の意味

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

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

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

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