計算論的に健全な形式的再暗号化

川本 裕輔† 櫻田 英樹‡ 萩谷 昌己†‡

†東京大学 ‡NTT コミュニケーション科学基礎研究所

2008 / 03 / 08

目次

- 背景
- 再暗号化可能な暗号方式
- 形式的モデル
- 解釈
- 健全性
- 結論

背景 (1/2)

- セキュリティプロトコル検証の分野において，
  形式的検証手法が 計算論的視点から見て
  妥当であることを示す研究が行われてきた．
  ([Abadi-Rogaway00], [Abadi-Jürjens01], [Micciancio-Warinschi04])

- 解釈 $[\![\cdot]\!]$:
  Dolev-Yao 項 を受け取り，ビット列確率分布を返す関数．

- 健全性定理:

$$m \cong m' \implies [\![m]\!] \approx [\![m']\!]$$

背景 (2/2)

- **従来の計算論的健全性の研究では，主に強い安全性を持つ比較的単純な暗号方式だけが扱われてきた．**
  - IND-CCA2 **安全な公開鍵暗号方式**,
  - EUF-CMA **安全な電子署名方式**,
  - oracle indistinguishable **なハッシュ方式**,

    …

概要 (1/2)

- 再暗号化可能な暗号方式に関する計算論的健全性の議論.
- 再暗号化可能な暗号方式とは，暗号文を復号することなく，暗号化に使われた乱数を，別の乱数に置き換えることのできるような暗号方式.

概要 (2/2)

- **再暗号化可能な暗号方式の新しい形式化を提案する．**
  - [Herzog05] **の形式化を拡張する．**

    ([Herzog05]: “A computational interpretation of Dolev-Yao adversaries”)
  - Abadi-Rogaway **流のパターンにおいて，乱数の合成を扱う新しい方法を導入する．**
- **この形式化の計算論的健全性を示す．**
  - IND-RCCA **安全性** [Canetti et.al. 02]
  - **乱数合成の安全性**

目次

- 背景
- **再暗号化可能な暗号方式**
- 形式的モデル
- 解釈
- 健全性
- 結論

再暗号化可能な暗号方式

定義 1
次のアルゴリズムの組を再暗号化可能な暗号方式という．

- 鍵生成アルゴリズム $\mathcal{G}$: $Param \times Random \to PubKey \times SecKey$
- 暗号化アルゴリズム $\mathcal{E}$: $PubKey \times String \times Random \to Cipher \cup \{\bot\}$
- 復号アルゴリズム $\mathcal{D}$: $SecKey \times String \to Plaintext \cup \{\bot\}$
- 再暗号化アルゴリズム $\mathcal{R}$: $PubKey \times String \times Random \to Cipher \cup \{\bot\}$
- 乱数合成アルゴリズム $\mathcal{CMP}$: $FMulti(Random) \to Random$

再暗号化可能な暗号方式

定義 1 (続)

- $\mathcal{D}(sk, \mathcal{E}(pk, x, r)) = \begin{cases} x & (\text{if } x \in \mathit{Plaintext}) \\ \bot & (\text{otherwise}) \end{cases}$
- $\mathcal{R}(pk, \mathcal{E}(pk, x, r), r') = \mathcal{E}(pk, x, \mathcal{CMP}(\{ r, r' \}))$
- **乱数の合成結果は，合成の順序に依らず，一意に定まる．**
  （乱数の合成は，乱数の多重集合で表すことができる．）

IND-RCCA 安全性 [Canetti et.al. 02]

定義 2 （任意のセキュリティパラメータ η と任意の PPT 攻撃者 A に対し，）次で定義する $Adv^{\mathrm{RCCA}}_{\mathcal{RE},\,A}$ が無視できるとき，再暗号化可能な暗号方式 $\mathcal{RE}$ が IND-RCCA **安全**であるという．

$$Adv^{\mathrm{RCCA}}_{\mathcal{RE},\,A}(\eta) = \Pr\ [\ (pk, sk) \leftarrow \mathcal{G}(1^{\eta});$$

$$m_0, m_1 \leftarrow A^{D_1(\cdot)}(pk);\ \ (m_0 \neq m_1 \text{ and } |m_0| = |m_1|)$$

$$r \leftarrow Random; \qquad b \leftarrow \{0, 1\};$$

$$c \leftarrow \mathcal{E}(pk,\ m_b,\ r);$$

$$b' \leftarrow A^{D_2(\cdot)}(c) :\ \ b' = b \qquad\qquad] - \frac{1}{2},$$

$$D_1(x) = \mathcal{D}(sk, x) \quad \text{and} \quad D_2(x) = \begin{cases} \mathcal{D}(sk, x) & (\mathcal{D}(sk, x) \neq m_0,\ m_1) \\ test & (\text{otherwise}) \end{cases}$$

乱数性を保存する合成 [Xue-Feng07] とほぼ同じ

定義 3
任意のビット列 $r \in Random$ に対し，次が成り立つとき，乱数合成アルゴリズム CMP が乱数性を保存するという．

ビット列集合 $Random$ 上の，任意の独立な一様乱数 x_0 に対し，
$CMP(\{ x_0, r \})$ が $Random$ 上で一様かつ独立に分布する．

ちなみに，このようなとき，

ある乱数 $r \in R$ が独立かつ一様である

$\Longrightarrow CMP(R)$ が独立かつ一様である

乱数性を保存する合成 [Xue-Feng07] とほぼ同じ

定義 3
任意のビット列 $r \in Random$ に対し，次が成り立つとき，乱数合成アルゴリズム CMP が乱数性を保存するという．

ビット列集合 $Random$ 上の，任意の独立な一様乱数 x_0 に対し，
$CMP(\{ x_0, r \})$ が $Random$ 上で一様かつ独立に分布する．

ちなみに，このようなとき，

ある乱数 $r \in R$ が独立かつ一様である

$\Longrightarrow CMP(R)$ が独立かつ一様である

目次

- 背景
- 再暗号化可能な暗号方式
- **形式的モデル**
- 解釈
- 健全性
- 結論

Dolev-Yao モデル

- [Herzog05] の Dolev-Yao モデルとほぼ同じ部分：
  - 適応的能動的攻撃者と正規参加者.
  - プロトコル実行:
    攻撃者のメッセージ q_i と正規参加者のメッセージ r_i を交互に並べた列: $r_0, q_1, r_1, \cdots, r_{n-1}, q_n, r_n$.
  - 攻撃者のメッセージ q_i は，$r_0, r_1, \cdots, r_{i-1}$ と (平文用の) ノンスと (暗号化用の) 乱数 から導出できなければならない．

項 (1/2)

- 乱数記号の多重集合
  - $Rand$: すべての 乱数記号 の集合
  - $FMulti(Rand)$: 乱数記号の非空有限多重集合全体の集合
  - 多重集合 $R \in FMulti(Rand)$ は，
    R に含まれるすべての乱数の合成を表す．

    （多重集合 R に含まれるすべての乱数を合成した結果
    が一意に定まることを仮定．）
  - $Rand = Rand_{uni} \uplus Rand_{adv}$.

項 (1/2)

- 乱数記号の多重集合
  - $Rand$: すべての 乱数記号 の集合
  - $FMulti(Rand)$: 乱数記号の非空有限多重集合全体の集合
  - 多重集合 $R \in FMulti(Rand)$ は，
    R に含まれるすべての乱数の合成を表す．

    （多重集合 R に含まれるすべての乱数を合成した結果
    が一意に定まることを仮定．）
  - $Rand = Rand_{uni} \uplus Rand_{adv}$.

項 (2/2)

- 項

$Term \ni m ::= c \mid k_{pub} \mid k_{sec} \mid n \mid R \mid \langle m, m \rangle \mid \{\!|\, m \,|\!\}^{R}_{k_{pub}} \mid (\!|\, m \,|\!)^{R}_{k_{pub}}$

(c: 定数記号, k_{pub}: 公開鍵記号, k_{sec}: 秘密鍵記号, n: ノンス記号,

$R \in FMulti(Rand)$: 乱数記号の空でない有限多重集合.)

- $\langle m_1, m_2 \rangle$: m_1 と m_2 の対.
- $\{\!|\, m \,|\!\}^{R}_{k_{pub}}$: 公開鍵 k_{pub} と合成乱数 R を用いた m の暗号化
- $(\!|\, m \,|\!)^{R}_{k_{pub}}$: 公開鍵 k_{pub} と合成乱数 R を用いた m の再暗号化

Abadi-Rogaway 流パターン (1/5)

- パターン $pattern(m, T)$ の直観的な意味:

  秘密鍵記号の集合 T を持つ**形式的攻撃者**から見た,

  項 m に対応する**ビット列確率分布**を**形式化**したもの.

  （あくまでも**記号的表現**）

Abadi-Rogaway 流パターン (2/5)

定義 4 パターン全体の集合 *Pattern* を次で定義する:

$$Pattern \ni m ::= c \mid k_{pub} \mid k_{sec} \mid n \mid R \mid \langle m, m \rangle$$

$$\mid \ \{\!|m|\!\}^{R}_{k_{pub}} \mid (\!|m|\!)^{R}_{k_{pub}} \mid \square^{\{\!|type(m)|\!\}^{R}_{k_{pub}}}$$

(c: 定数記号, k_{pub}: 公開鍵記号, k_{sec}: 秘密鍵記号, n: ノンス記号,

$R \in FMulti(Rand)$)

パターン $\square^{\{\!|type(m)|\!\}^{R}_{k_{pub}}}$ **は，攻撃者から見て，暗号文** $\{\!|m|\!\}^{R}_{k_{pub}}$ **と区別できないようなランダムなメッセージを表す．**

($R \cap Rand_{uni} \neq \emptyset$).

Abadi-Rogaway 流パターン (3/5)

定義 5 $pat : Term \times \mathcal{P}(K_{sec}) \to Pattern$.

- $pat(m, T) = m$

  (if $m \in Const \cup K_{pub} \cup K_{sec} \cup Nonce \cup FMulti(Rand)$)

- $pat(\langle m_1, m_2 \rangle, T) = \langle pat(m_1, T), pat(m_2, T) \rangle$

- $$pat(\{\!|\, m \,|\!\}^R_{k_{pub}}, T) = \begin{cases} \{\!|\, pat(m, T) \,|\!\}^R_{k_{pub}} & (\text{if } \overline{k_{pub}} \in T \\ & \text{or } R \in FMulti(Rand_{adv})) \\ \square^{\{\!|\, type(m) \,|\!\}^R_{k_{pub}}} & (\text{otherwise}) \end{cases}$$

ただし，$\overline{k_{pub}}$ は k_{pub} に対応する秘密鍵記号.

Abadi-Rogaway 流パターン (4/5)

定義 5 (続)

- $pat(\{\!|\, m \,|\!\}^{R'}_{k_{pub}}\ |\!\}^{R}_{k_{pub}}, T) = pat(\{\!|\, m \,|\!\}^{R \uplus R'}_{k_{pub}}, T)$ if $m \in Term$ holds.
- $pat(\{\!|\, \{\!|\, m \,|\!\}^{R'}_{k_{pub}}\ |\!\}^{R}_{k_{pub}}, T) = pat(\{\!|\, m \,|\!\}^{R \uplus R'}_{k_{pub}}, T)$ if $m \in Reenc_{k_{pub}}$ holds.
- $pat(\{\!|\, m \,|\!\}^{R}_{k_{pub}}, T) = \{\!|\, pat(m, T) \,|\!\}^{R}_{k_{pub}}$ Otherwise.

ただし，$m \in Reenc_{k_{pub}}$ は，ある公開鍵記号 k_{pub} に対し，

$\{\!|\, \cdots, \{\!|\, m'' \,|\!\}^{R_1}_{k_{pub}} \cdots |\!\}^{R_2}_{k_{pub}}\ |\!\}^{R_m}_{k_{pub}}$ の形をした暗号文であるものとする．

Abadi-Rogaway 流パターン (4/5)

定義 5 (続)

- $pat(\{\!|\, m \,|\!\}^{R'}_{k_{pub}}\ \}^{R}_{k_{pub}}, T) = pat(\{\!|\, m \,|\!\}^{R \uplus R'}_{k_{pub}}, T)$ if $m \in Term$ holds.
- $pat(\{\!|\{\!|\, m \,|\!\}^{R'}_{k_{pub}}\ \}^{R}_{k_{pub}}, T) = pat(\{\!|\, m \,|\!\}^{R \uplus R'}_{k_{pub}}, T)$ if $m \in Reenc_{k_{pub}}$ holds.
- $pat(\{\!|\, m \,|\!\}^{R}_{k_{pub}}, T) = \{\!|\, pat(m, T) \,|\!\}^{R}_{k_{pub}}$ Otherwise.

ただし，$m \in Reenc_{k_{pub}}$ は，ある公開鍵記号 k_{pub} に対し，

$\{\!|\cdots, \{\!|\, m'' \,|\!\}^{R_1}_{k_{pub}} \cdots \}^{R_2}_{k_{pub}}\ \}^{R_m}_{k_{pub}}$ の形をした暗号文であるものとする．

Abadi-Rogaway 流パターン (5/5)

定義 5 (続) $pattern : Term \times \mathcal{P}(K_{sec}) \to Pattern$

- $pattern(m, T) = pat(m, recoverable(m, T))$.

  where $recoverable : Term \times \mathcal{P}(K_{sec}) \to \mathcal{P}(K_{sec})$

（形式的な）乱数使用仮定 (1/4)

乱数使用仮定 (1)

- いかなる正規参加者も，異なるメッセージを
  同じ合成乱数 (を表す多重集合) R で暗号化/再暗号化しない．
- いかなる正規参加者も，一様乱数記号 $r \in Rand_{uni}$ を
  暗号化/再暗号化に用いる乱数以外の目的で使わない．

（形式的な）乱数使用仮定 (2/4)

乱数使用仮定 (2)

- 正規参加者の暗号化/再暗号化に用いられるすべての多重集合 R は，少なくともひとつ独立かつ一様な乱数記号 r を含む.

この仮定 (2) より，多重集合 $R \in FMulti(Rand) \setminus FMulti(Rand_{adv})$ で表される合成乱数を，ひとつの独立かつ一様な乱数と見なせる.
（乱数合成が乱数性を保存するから）

（形式的な）乱数の独立性

定義 6

一様乱数記号 $r \in Rand_{uni}$ が項の集合 S において独立であるとは，次を満たす $R \in FMulti(Rand_{uni})$ が唯一存在することをいう．

- **多重集合 R がある項 $m \in S$ に現れ，かつ**
- **一様乱数記号 r が R のみに含まれる.**

E.g. $S = \{ \{\!| c_1 |\!\}_k^{\{r_1\}}, \{\!| c_1 |\!\}_k^{\{r_1, r_2\}}, \{\!| c_2 |\!\}_k^{\{r_3\}}, (\{\!| c_2 |\!\}_k^{\{r_3\}})_k^{\{r_4\}} \}$ $(r_i \in Rand_{uni})$

- r_2, r_3, r_4 **は，S において独立である．**
- r_1 **は，S において独立でない．**

（形式的な）乱数の独立性

定義 6

一様乱数記号 $r \in Rand_{uni}$ が項の集合 S において独立であるとは，次を満たす $R \in FMulti(Rand_{uni})$ が唯一存在することをいう．

- **多重集合 R がある項 $m \in S$ に現れ，かつ**
- **一様乱数記号 r が R のみに含まれる.**

E.g. $S = \{ \{\!| c_1 |\!\}_k^{\{r_1\}}, \{\!| c_1 |\!\}_k^{\{r_1, r_2\}}, \{\!| c_2 |\!\}_k^{\{r_3\}}, (\{\!| c_2 |\!\}_k^{\{r_3\}})_k^{\{r_4\}} \}$ $(r_i \in Rand_{uni})$

- **r_2, r_3, r_4 は，S において独立である．**
- **r_1 は，S において独立でない．**

（形式的な）乱数使用仮定 (3/4)

（例）次の項は，乱数使用仮定を満たさ**ない**．

- $\langle \{\!|\, c_1 \,|\!\}_k^{\{r_1\}}, \{\!|\, c_2 \,|\!\}_k^{\{r_1\}} \rangle$
- $\{\!|\, r_1 \,|\!\}_k^{\{r_2\}}$
- $\langle \{\!|\, c_1 \,|\!\}_k^{\{r_1\}}, \{\!|\, c_1 \,|\!\}_k^{\{r_1, r_2\}} \rangle$
- $\langle \{\!|\, c_1 \,|\!\}_k^{\{r_1\}}, \{\!|\, c_1 \,|\!\}_k^{\{r_1, r_{adv}\}} \rangle$

$(c_i \in Const,\ k \in K_{pub},\ r_i \in Rand_{uni},\ r_{adv} \in Rand_{adv},\ R_i \in FMulti(Rand))$

（形式的な）乱数使用仮定 (4/4)

（例）次の項は，乱数使用仮定を満たす．

- $\langle \{\!|\, c \,|\!\}_k^{\{ r_1 \}}, \{\!|\, c \,|\!\}_k^{\{ r_1 \}} \rangle$,
- $\langle \{\!|\, c \,|\!\}_k^{\{ r_1 \}}, (\!| \{\!|\, c_1 \,|\!\}_k^{\{ r_1 \}} |\!)_k^{\{ r_2 \}} \rangle$,
- $\langle \{\!|\, c \,|\!\}_k^{\{ r_1, r_2 \}}, \{\!|\, c \,|\!\}_k^{\{ r_1, r_3 \}} \rangle$.

$(c \in Const,\ k \in K_{pub},\ r_i \in Rand_{uni})$

- 以後，乱数使用仮定を満たし，key-cycle を持たない項のみを扱う．

（形式的な）観測同値 (1/2)

定義 7
項 m と m' が観測同値である（$m \cong m'$）とは，
ある名前換え σ に対し，

$$pattern(m,\ K_{adv}) = \sigma\, pattern(m',\ K_{adv})$$

が成り立つことをいう．

（形式的な）観測同値 (2/2)

例 1

$k \in K_{pub} \setminus \overline{K_{adv}}$, $r_i \in Rand_{uni}$, $r_{adv} \in Rand_{adv}$.

(1) **暗号文の再暗号化，合成乱数を用いた暗号化**

- $\{\!|\, m \,|\!\}_k^{\{r_1\}} \cong \{\!|\, m \,|\!\}_k^{\{r_1, r_2\}} \cong (\!(\{\!|\, m \,|\!\}_k^{\{r_2\}})\!)_k^{\{r_1\}}$

- $\{\!|\, m \,|\!\}_k^{\{r_1\}} \cong \{\!|\, m \,|\!\}_k^{\{r_1, r_{adv}\}} \cong (\!(\{\!|\, m \,|\!\}_k^{\{r_{adv}\}})\!)_k^{\{r_1\}}$

（形式的な）観測同値 (2/2)

例 1

$k \in K_{pub} \setminus \overline{K_{adv}}$, $r_i \in Rand_{uni}$.

(2) **メッセージのコピーを識別**

- $\{\!|\, m \,|\!\}_k^{\{r_1\}} \cong \{\!|\, m \,|\!\}_k^{\{r_2\}}$

  but

- $\langle \{\!|\, m \,|\!\}_k^{\{r_1\}}, \{\!|\, m \,|\!\}_k^{\{r_1\}} \rangle \ncong \langle \{\!|\, m \,|\!\}_k^{\{r_1\}}, \{\!|\, m \,|\!\}_k^{\{r_2\}} \rangle$

目次

- 背景
- 再暗号化可能な暗号方式
- 形式的モデル
- **解釈**
- 健全性
- 結論

$$\textbf{if } m \in Dom(e),$$

$$\textbf{then} \quad [\![m]\!]_{\eta}^{e,t} = e(m)$$

$$\textbf{else} \quad [\![c]\!]_{\eta}^{e,t} = \langle C(c), \text{“Const”} \rangle$$

$$[\![k_{pub}]\!]_{\eta}^{e,t} = \langle fst(\mathcal{G}(\eta, t(k_{pub}))), \text{“PubKey”} \rangle$$

$$[\![k_{sec}]\!]_{\eta}^{e,t} = \langle snd(\mathcal{G}(\eta, t(\overline{k_{sec}}))), \text{“SecKey”} \rangle$$

$$[\![n]\!]_{\eta}^{e,t} = \begin{cases} \langle D_{nonce}(\mathcal{N}(\eta, t(n))), \text{“Nonce”} \rangle & (\text{if } n \in Nonce_{adv}) \\ \langle \mathcal{N}(\eta, t(n)), \text{“Nonce”} \rangle & (\text{otherwise}) \end{cases}$$

$$[\![\{ r \}]\!]_{\eta}^{e,t} = \begin{cases} \langle D_{rand}(t(r)), \text{“Rand”} \rangle & (\text{if } r \in Rand_{adv}) \\ \langle t(r), \text{“Rand”} \rangle & (\text{otherwise}) \end{cases}$$

$$[\![R]\!]_{\eta}^{e,t} = \langle \mathcal{CMP}(\{ fst([\![\{ r \}]\!]_{\eta}^{e,t}) \mid r \in R \}), \text{“Rand”} \rangle$$

$$[\![\langle m_1, m_2 \rangle]\!]_{\eta}^{e,t} = \langle \langle [\![m_1]\!]_{\eta}^{e,t}, [\![m_2]\!]_{\eta}^{e,t} \rangle, \text{“pair”} \rangle$$

$$[\![\{\!| m |\!\}_k^R]\!]_{\eta}^{e,t} = \langle \mathcal{E}(fst([\![k]\!]_{\eta}^{e,t}), [\![m]\!]_{\eta}^{e,t}, fst([\![R]\!]_{\eta}^{e,t})), \text{“enc”} \rangle$$

$$[\![(\!| c |\!)_k^R]\!]_{\eta}^{e,t} = \langle \mathcal{R}(fst([\![k]\!]_{\eta}^{e,t}), fst([\![c]\!]_{\eta}^{e,t}), fst([\![R]\!]_{\eta}^{e,t})), \text{“enc”} \rangle$$

$$[\![\square^{\{\!| type(m) |\!\}_k^R}]\!]_{\eta}^{e,t} = \langle \mathcal{E}(fst([\![k]\!]_{\eta}^{e,t}), \mathcal{T}(type(m)), fst([\![R]\!]_{\eta}^{e,t})), \text{“enc”} \rangle$$

目次

- 背景
- 再暗号化可能な暗号方式
- 形式的モデル
- 解釈
- **健全性**
- 結論

Abadi-Rogaway RCCA 識別不能性

定義 8

- $T \subseteq K_{sec}$
- $M,\ M'$: $M \cong M'$ と乱数使用仮定を満たし，key-cycle を持たない項

$[\![M]\!]_\eta \approx_{O^{M, M', T}_{\eta, t}} [\![M']\!]_\eta$ であるとは，（任意のセキュリティパラメータ η と任意の PPT 攻撃者 A に対し，）次で定義される $Adv^{\mathrm{AR-RCCA}}_{\mathcal{RE}, A}$ が無視できることをいう．

$$
\begin{aligned}
Adv^{\mathrm{AR-RCCA}}_{\mathcal{RE}, A}(\eta) \quad &= \Pr[t \leftarrow Coins(M),\ d := [\![M]\!]^t_\eta :\ A^{O^{M, M', T}_{\eta, t}(\cdot,\cdot)}(d,\ \eta) = 1] \\
&\quad - \Pr[t \leftarrow Coins(M'),\ d := [\![M']\!]^t_\eta :\ A^{O^{M, M', T}_{\eta, t}(\cdot,\cdot)}(d,\ \eta) = 1]
\end{aligned}
$$

Abadi-Rogaway RCCA 識別不能性

定義 8 (続)

$$O^{M,M',T}_{\eta,\,t}(pk,\,x) = \begin{cases} \mathcal{D}(\overline{pk},\,x) & (\text{if (i) } pk \in PubKey \text{ and} \\ & \quad \text{(ii) either } pk \in [\![\, K \,]\!]^t_\eta \text{ for } K \in \overline{T}, \\ & \quad\quad \text{or (a) } pk \in [\![\, K \,]\!]^t_\eta \\ & \quad\quad\quad \text{for } K \in \{\, M,\ M' \,\}|_{K_{pub}} \setminus \overline{T}, \\ & \quad\quad\quad \text{(b) } \langle pk,\ \mathcal{D}(\overline{pk},\,x)\rangle \notin forbid_{\eta,t}(M,\ T), \\ & \quad\quad\quad \text{and} \\ & \quad\quad\quad \text{(c) } \langle pk,\ \mathcal{D}(\overline{pk},\,x)\rangle \notin forbid_{\eta,t}(M',\ T)) \\ \bot & (\text{if } pk \notin PubKey) \\ test & (\text{otherwise}) \end{cases}$$

Abadi-Rogaway RCCA 識別不能性

定義 8 (続)

$blob_\tau$ を次頁で定義するアルゴリズムとする．

$forbid_{\eta,t}(M, T)$ を次の集合で定義する．

$$\left\{ \langle pk, \mathcal{D}(\overline{pk}, y)\rangle, \langle pk, Type(\mathcal{D}(\overline{pk}, y))\rangle \;\middle|\; \begin{array}{l} y \in blob_{[\![T]\!]_\eta^t}([\![M]\!]_\eta^t), \\ pk = \mathcal{PK}(y) \end{array} \right\}.$$

algorithm $blob_\tau(\mu)$

Set B, $B' := \{ \mu \}$;

do

$B := B'$; $B' := \emptyset$;

for each $b \in B$

if $b = \langle b_1, b_2, \text{“pair”} \rangle$

then $B' := B' \cup \{ b_1, b_2 \}$;

if $b = \langle c, \text{“enc”} \rangle$ **and** $\mathcal{PK}(c) \in \overline{\tau}$

then $B' := B' \cup \{ \overline{\mathcal{D}(\mathcal{PK}(c), c)} \}$;

if $b = \langle c, \text{“enc”} \rangle$ **and** $\langle \overline{\mathcal{PK}(c)}, \text{“SecKey”} \rangle \in B$

then $B' := B' \cup \{ \overline{\mathcal{D}(\mathcal{PK}(c), c)} \}$;

otherwise

$B' := B' \cup \{ b \}$;

while $B' \neq B$;

return B;

健全性定理 (1/5)

定理 1

M, M': 乱数使用仮定を満たし，key-cycle を持たない任意の項

$$M \cong M' \text{ implies } [\![M]\!]_\eta \approx^{M, M', K_{adv}}_{O_{\eta, t}} [\![M']\!]_\eta .$$

健全性定理 (2/5)

証明の概要:
ある名前換え σ に対して,

$$
\begin{aligned}
[\![M]\!]_\eta &\approx {O^{M, M', K_{adv}}_{\eta, t}}[\![pattern(M, K_{adv})]\!]_\eta \\
&= [\![\sigma\, pattern(M', K_{adv})]\!]_\eta \\
&= [\![pattern(M', K_{adv})]\!]_\eta \\
&\approx {O^{M', M', K_{adv}}_{\eta, t}}[\![M']\!]_\eta
\end{aligned}
$$

□

補題 1 は [Abadi-Rogaway] **と同様のやり方で示せる.**

健全性定理 (3/5)

補題 1

$$[\![M]\!]_\eta \approx_{O_{\eta, t}^{M, M', K_{adv}}} [\![pattern(M, K_{adv})]\!]_\eta$$

これら 2 つの確率分布を識別できる PPT 攻撃者 A が存在するものと仮定する．

このとき，A を用いて，暗号方式の IND-RCCA 安全性を破る攻撃者 A_0 を構成する．

IND-RCCA 安全性 [Canetti et.al. 02]

定義 9

次で定義する $Adv^{\mathrm{RCCA}}_{\mathcal{RE},\,A}$ が無視できるとき，再暗号化可能な暗号方式 $\mathcal{RE}$ が IND-RCCA 安全であるという．

$$Adv^{\mathrm{RCCA}}_{\mathcal{RE},\,A}(\eta) = \Pr\ [\ (pk, sk) \leftarrow \mathcal{G}(1^{\eta});$$

$$m_0, m_1 \leftarrow A^{D_1(\cdot)}(pk);\ (m_0 \neq m_1 \text{ and } |m_0| = |m_1|)$$

$$r \leftarrow Random;\quad b \leftarrow \{0, 1\};$$

$$c \leftarrow \mathcal{E}(pk, m_b, r);$$

$$b' \leftarrow A^{D_2(\cdot)}(c) :\ b' = b\ ] - \frac{1}{2},$$

$$D_1(x) = \mathcal{D}(sk, x) \text{ and } D_2(x) = \begin{cases} \mathcal{D}(sk, x) & (\mathcal{D}(sk, x) \neq m_0, m_1) \\ test & \text{(otherwise)} \end{cases}$$

健全性定理 (4/5)

補題 1

$$[\![M]\!]_\eta \approx_{O^{M, M', K_{adv}}_{\eta, t}} [\![pattern(M, K_{adv})]\!]_\eta$$

- IND-RCCA ゲームにおける暗号文 c を生成するために，
  正規参加者の合成乱数を使うことができる．
  （∵ 乱数使用仮定，乱数性を保存する合成）

健全性定理 (5/5)

証明の概要:
ある名前換え σ に対して，

$$
\begin{aligned}
[\![M]\!]_{\eta} &\approx {O^{M,\, M',\, K_{adv}}_{\eta,\, t}}[\![pattern(M,\ K_{adv})]\!]_{\eta} \\
&= [\![\sigma\, pattern(M',\ K_{adv})]\!]_{\eta} \\
&= [\![pattern(M',\ K_{adv})]\!]_{\eta} \\
&\approx {O^{M',\, M',\, K_{adv}}_{\eta,\, t}}[\![M']\!]_{\eta}
\end{aligned}
$$

□

名前換え σ の計算論的正当化．
（乱数使用仮定，乱数性を保存することから導かれる．）

目次

- 背景
- 再暗号化可能な暗号方式
- 形式的モデル
- 解釈
- 健全性
- **結論**

結論

- Abadi-Rogaway **流のパターンを用いて，**
  再暗号化可能な暗号方式を形式化した．
- IND-RCCA **安全性と乱数性を保存する合成を用いて，**
  計算論的健全性を示した．

今後の課題

- **本研究の健全性は** [Abadi-Rogaway] **流だが，**
  [Micciancio-Warinschi] **流の健全性（**Mapping Lemma**）**
  を示したい．
- **本研究では，乱数合成操作が結合律と交換律を満たす暗号方式のみを扱っているが，そうでないものも扱いたい．**
- **より複雑な暗号方式に対して，計算論的に健全な形式化を与えたい．**

Thank you for your attention.