秘密分散法に於ける確率論的秘匿

竹内泉　足立智子

2011年3月7日

本研究の内容

・確率論的秘匿の定式化

・確率論的秘匿を証明できるような形式的論理体系の設計

確率論的秘匿の定式化

→暗号通信に於ける秘匿を議論するには、確率論的議論が不可欠

形式的論理体系の設計

→確率ホーア論理に対して健全な体系

→確率ホーア論理は暗黙の規則が多く煩雑なのに対し

　議論を抽象化し、必要な規則を明確にした簡明な公理化

事例として秘密分散法を採り上げる

秘密分散法

n **：参加者の数**

t **：閾値、**$1 \leq t \leq n$

F **：有限体**

$g \in F$ **：位数** $\geq n$

$n \times t$ **行列**

$$\begin{pmatrix} 1 & \cdots & 1 & \cdots & 1 \\ \vdots & & \vdots & & \vdots \\ 1 & \cdots & g^{(i-1)(j-1)} & \cdots & g^{(i-1)(t-1)} \\ \vdots & & \vdots & & \vdots \\ 1 & \cdots & g^{(n-1)(j-1)} & \cdots & g^{(n-1)(t-1)} \end{pmatrix}$$

ファンデルモンド行列：任意の部分 t **次正方行列が退化しない**

$m \in F$ **：平文**

$x_1, x_2, ..., x_{t-1}$ **：乱数**

$y_1, y_2, ..., y_n$ **：各参加者に配られる値**

$$\begin{pmatrix} y_1 \\ \vdots \\ y_i \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} 1 & \cdots & 1 & \cdots & 1 \\ \vdots & & \vdots & & \vdots \\ 1 & \cdots & g^{(i-1)(j-1)} & \cdots & g^{(i-1)(t-1)} \\ \vdots & & \vdots & & \vdots \\ 1 & \cdots & g^{(n-1)(j-1)} & \cdots & g^{(n-1)(t-1)} \end{pmatrix} \begin{pmatrix} m \\ x_1 \\ \vdots \\ x_{j-1} \\ \vdots \\ x_{t-1} \end{pmatrix}$$

$y_1, y_2, ..., y_n$ **の中から** t **ヶ以上知れば、**m **が分かる**

$y_1, y_2, ..., y_n$ の中から t ヶ以上知れば、m が分かる

乱数 $x_1, x_2, ..., x_{t-1}$ の分布に偏りがあれば、

t ヶ未満からでも、m を 推測することが出来る

$t = 2$ の場合

y_i だけを知っている

$\mathbf{Pr}(x_1 = \bar{x}_1) > 1/|F|$

m の推測値 $\bar{m}$ は $y_i = \bar{m} + g^{i-1}\bar{x}_1$ を解いて

$\bar{m} = y_i - g^{i-1}\bar{x}_1$

この推測が当たる確率は

$\mathbf{Pr}(m = \bar{m}) = \mathbf{Pr}(y_i - g^{i-1}x_1 = y_i - g^{i-1}\bar{x}_1)$

$= \mathbf{Pr}(x_1 = \bar{x}_1) > 1/|F|$

$t = 3$ の場合

y_i、$y_{i'}$ だけを知っている

$\mathbf{Pr}(x_2 = \bar{x}_2) > 1/|F|$

m の推測値 $\bar{m}$ は

$y_i = \bar{m} + g^{i-1}x_1 + g^{2(i-1)}\bar{x}_2$

$y_{i'} = \bar{m} + g^{i'-1}x_1 + g^{2(i'-1)}\bar{x}_2$

を解いて

$$\bar{m} = \frac{\begin{vmatrix} y_i - g^{2(i-1)}\bar{x}_2 & g^{i-1} \\ y_{i'} - g^{2(i'-1)}\bar{x}_2 & g^{i'-1} \end{vmatrix}}{\begin{vmatrix} 1 & g^{i-1} \\ 1 & g^{i'-1} \end{vmatrix}} = \frac{\begin{vmatrix} y_i & g^{i-1} \\ y_{i'} & g^{i'-1} \end{vmatrix} - \begin{vmatrix} g^{2(i-1)} & g^{i-1} \\ g^{2(i'-1)} & g^{i'-1} \end{vmatrix} \bar{x}_2}{\begin{vmatrix} 1 & g^{i-1} \\ 1 & g^{i'-1} \end{vmatrix}}$$

$= C_0 + C_1\bar{x}_2 \quad (C_1 \neq 0)$

この推測が当たる確率は

$\mathbf{Pr}(m = \bar{m}) = \mathbf{Pr}(C_0 + C_1x_2 = C_0 + C_1\bar{x}_2)$

$= \mathbf{Pr}(x_2 = \bar{x}_2) > 1/|F|$

$t = 3$ の場合

y_i だけを知っている

$\mathbf{Pr}(\xi = g^{i-1}x_1 + g^{2(i-1)}x_2) > 1/|F|$

m の推測値 $\bar{m}$ は

$y_i = \bar{m} + \xi$

を解いて

$\bar{m} = y_i - \xi$

この推測が当たる確率は

$\mathbf{Pr}(m = \bar{m}) = \mathbf{Pr}(y_i - \xi = y_i - g^{i-1}x_1 - G^{2(i-1)}x_2)$

$= \mathbf{Pr}(\xi = g^{i-1}(x_1 + g^{i-1}x_2)) > 1/|F|$

$x_1, ..., x_{t-1}$ の中の k ヶの分布に偏りがある時、

$y_1, y_2, ..., y_n$ の中から $t - k$ ヶ知れば、m が確率的に分かることがある

形式的体系による証明の目標：

$x_1, ..., x_k$ の分布に偏りがない時、

$y_1, y_2, ..., y_n$ の中から k ヶしか知らなければ、m は確率的に分からない

本質を保った特殊事例として

$x_1, ..., x_k$ の分布に偏りがない時、

$y_1, ..., y_k$ から m を確率的に知ることは出来ない

を問題にする

$x_1, ..., x_k$ の分布に偏りがない時、
$y_1, y_2, ..., y_k$ しか知らなければ、m は確率的に知ることは出来ない

《 $x_1, ..., x_k$ の分布に偏りがない》とは
$x_1, ..., x_k$ が互いに独立、かつ他の $x_{k+1}, ..., x_{t-1}$ と独立であり、
任意の $\bar{x}_1, ..., \bar{x}_k \in F$ に対して

$$\mathbf{Pr}(x_1 = \bar{x}_1, ..., x_k = \bar{x}_k) = 1/|F|^k$$

《確率的に知ることは出来ない》とは
攻撃者の機能を $f(y_1, ..., y_k, p)$ と置く　但し p は攻撃者の使う確率オラクル
任意の m に対して $Pr(m = f(y_1, ..., y_k, p)) > 1/|F|$
となることはない
即ち
ある m があって $Pr(m = f(y_1, ..., y_k, p)) \leq 1/|F|$

行列 G をこのように置く

$$G = \begin{pmatrix} 1 & \cdots & 1 & \cdots & 1 \\ \vdots & & \vdots & & \vdots \\ g^{i-1} & \cdots & g^{(i-1)j} & \cdots & g^{(i-1)k} \\ \vdots & & \vdots & & \vdots \\ g^{k-1} & \cdots & g^{(k-1)j} & \cdots & g^{(k-1)k} \end{pmatrix}$$

これの逆行列を行列 H と置き、各成分を h_{ij} と書く
即ち

$$G^{-1} = H = \begin{pmatrix} h_{11} & \cdots & h_{1j} & \cdots & h_{1k} \\ \vdots & & \vdots & & \vdots \\ h_{i1} & \cdots & h_{ij} & \cdots & h_{jk} \\ \vdots & & \vdots & & \vdots \\ h_{k1} & \cdots & h_{kj} & \cdots & h_{kk} \end{pmatrix}$$

$H(y_1, ..., y_k)^T$

$$= H \begin{pmatrix} 1 & \cdots & 1 & \cdots & 1 \\ \vdots & & \vdots & & \vdots \\ 1 & \cdots & g^{(i-1)(j-1)} & \cdots & g^{(i-1)(t-1)} \\ \vdots & & \vdots & & \vdots \\ 1 & \cdots & g^{(k-1)(j-1)} & \cdots & g^{(k-1)(t-1)} \end{pmatrix} \begin{pmatrix} m \\ \vdots \\ x_{j-1} \\ \vdots \\ x_{t-1} \end{pmatrix}$$

$$= \begin{pmatrix} \sum_j h_{1j} & 1 & & 0 & \cdots \\ \vdots & & \ddots & & \cdots \\ \sum_j h_{kj} & 0 & & 1 & \cdots \end{pmatrix} \begin{pmatrix} m \\ x_1 \\ \vdots \\ x_k \\ \vdots \end{pmatrix}$$

$$= \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} + L \begin{pmatrix} m \\ x_{k+1} \\ \cdots \\ x_{t-1} \end{pmatrix} = (x_1 + l_1(m, x_{k+1}, ..., x_{t-1}), ..., x_k + l_k(m, x_{k+1}, ..., x_{t-1}))$$

但し L は行列、各 $l_j(\ )$ は線形函数、G と H から定まる

攻撃者の機能を表す函数 $f(\ )$ に対して、函数 $f'(\ )$ を

$$f'(z_1, ..., z_k, p) = f(\left(G \begin{pmatrix} z_1 \\ \vdots \\ z_k \end{pmatrix} \right)^T, p)$$

と置く

即ち

$$f(y_1, ..., y_k, p) = f'(\left(H \begin{pmatrix} y_1 \\ \vdots \\ y_k \end{pmatrix} \right)^T, p)$$

$$= f'(\begin{pmatrix} x_1 + l_1(m, x_{k+1}, ..., x_{t-1}) \\ \vdots \\ x_k + l_k(m, x_{k+1}, ..., x_{t-1}) \end{pmatrix}^T, p)$$

$$= f'(x_1 + l_1(m, x_{k+1}, ..., x_{t-1}), \cdots, x_k + l_k(m, x_{k+1}, ..., x_{t-1}), p)$$

確率変数 x_i の分布が他の x_j に対して偏りがないことを $\mathbf{Rand}(x_i)$ と書く

穴のある論理式 $P(\ )$ 及び項 T が確率変数 x_i に依存していない時、以下が成り立つ

$$\mathbf{Rand}(x_i) \supset \mathbf{Pr}(P(x_i + T)) = \mathbf{Pr}(P(x_i))$$

これを用いると

$$\mathbf{Rand}(x_1) \wedge ... \wedge \mathbf{Rand}(x_k) \supset \mathbf{Pr}(m = f(y_1, ..., y_k, p)) = \mathbf{Pr}(m = f'(x_1, ..., x_k, p))$$

故に

$$\mathbf{Rand}(x_1) \wedge ... \wedge \mathbf{Rand}(x_k) \wedge (\forall m \in F.\, \mathbf{Pr}(m = f(y_1, ..., y_k, p)) > 1/|F|) \supset \forall m \in F.\, \mathbf{Pr}(m = f'(x_1, ..., x_k, p)) > 1/|F|$$

一方で

$$(\forall m \in F.\, \mathbf{Pr}(m = f'(x_1, ..., x_k, p) > 1/|F|)) \supset \textstyle\sum_{m \in F} \mathbf{Pr}(m = f'(x_1, ..., x_k, p)) > 1$$

かつ

$$\neg \textstyle\sum_{m \in F} \mathbf{Pr}(m = f'(x_1, ..., x_k, p)) > 1$$

故に

$$\neg \forall m \in F.\, \mathbf{Pr}(m = f'(x_1, ..., x_k, p) > 1/|F|)$$

結論として

$$\mathbf{Rand}(x_1) \wedge ... \wedge \mathbf{Rand}(x_k) \supset \neg \forall m \in F.\, \mathbf{Pr}(m = f(y_1, ..., y_k, p)) > 1/|F|$$

以上は非形式的な議論
この議論を形式的論理体系の上で形式化する

一般の F に対して形式化し証明するのは、論理体系が体の一般理論を含まなければならず
煩雑である
特定の F に対して形式化し、証明する

ある体 F を取り、固定する
言語
- 非決定性変数：$m, ... \in V_N$
- 確率変数：$x, y, ... \in V_P$
- 変数：$V = V_N \coprod V_P$
- 定数：$\bar{e}$ 但し $e \in F$
- 函数記号：$+$、$-$、$\times$、inv( ) 及び不定函数 $f, f', ...$
- 項：$T, U, ...$、変数と定数から函数記号によって作られる
- 述語：$=$、$\mathsf{R}(x; x', ...)$
- 論理式：$P ::= T = U \mid \mathsf{R}(x; x', ...) \mid \neg P \mid P \wedge P \mid \forall V_N P \mid \mathsf{A}P \mid \mathsf{M}P$

$\mathsf{M}P$ は、P の確率が $1/|F|$ より大きいことを表す
$\mathsf{A}P$ は、P の確率が 1 であることを表す
A、M は確率変数を束縛する
$\mathsf{R}(x; x', x'', ...)$ は、「x は x'、x'' …に対し偏りがない」ということを表す
$\supset$、$\supset\subset$ は $\neg$ と $\wedge$ から定義する

意味論

$w_N : V_N \to F$: 非決定性変数への割当

$w_P : V_P \to F$: 確率変数への割当

w_F : n 引数変数 f に対し $w_F(f) : F^n \to F$: 不定函数記号への割当

$\mu : F^{V_P} \to [0,1]$: 確率変数の値の組合せに対する確率分布

$\sum_{w \in F^{V_P}} \mu(w) = 1$

$[\![\bar{e}]\!](w_N, w_P, w_F) = e,\ e \in F$

$[\![m]\!](w_N, w_P, w_F) = w_N(m),\ m \in V_N$

$[\![x]\!](w_N, w_P, w_F) = w_P(x),\ x \in V_P$

$[\![T + U]\!](w_N, w_P, w_F) = [\![T]\!](w_N, w_P, w_F) + [\![U]\!](w_N, w_P, w_F)$

$-$、$\times$ についても同様

$[\![\mathsf{inv}(T)]\!](w_N, w_P, w_F) = ([\![T]\!](w_N, w_P, w_F))^{-1}$ 但し $[\![T]\!](w_N, w_P, w_F) \neq 0$

$[\![\mathsf{inv}(T)]\!](w_N, w_P, w_F) = 0$ 但し $[\![T]\!](w_N, w_P, w_F) = 0$

$[\![f(T_1, ...)]\!](w_N, w_P, w_F) = e_F(f)([\![T_1]\!](w_N, w_P, w_F), ...)$

$[\![T = U]\!](w_N, w_P, w_F, \mu) = 1$ 但し $[\![T]\!](w_N, w_P, w_F, \mu) = [\![U]\!](w_N, w_P, w_F, \mu)$

$[\![T = U]\!](w_N, w_P, w_F, \mu) = 0$ 上記以外

$[\![\mathsf{R}(x; x', x'', ...)]\!](w_N, w_P, w_F, \mu) = 1$

但し μ の許では x の分布は $x', x'', ...$ に対し偏りがない

$[\![\mathsf{R}(x; x', x'', ...)]\!](w_N, w_P, w_F, \mu) = 0$ 上記以外

$[\![\neg P]\!](w_N, w_P, w_F, \mu) = 1 - [\![P]\!](w_N, w_P, w_F, \mu)$

$[\![P \wedge Q]\!](w_N, w_P, w_F, \mu) = [\![P]\!](w_N, w_P, w_F, \mu) \cdot [\![Q]\!](w_N, w_P, w_F, \mu)$

$[\![\forall m P]\!](w_N, w_P, w_F, \mu) = \prod_{e \in F} P(w_N[e/m], w_P, w_F, \mu)$

$[\![\mathsf{A}mP]\!](w_N, w_P, w_F, \mu) = 1$ 但し $\sum_w \mu(w) \cdot [\![P]\!](w_N, w, w_F, \mu) = 1$
$[\![\mathsf{A}mP]\!](w_N, w_P, w_F, \mu) = 0$ 上記以外

$[\![\mathsf{M}mP]\!](w_N, w_P, w_F, \mu) = 1$ 但し $\sum_w \mu(w) \cdot [\![P]\!](w_N, w, w_F, \mu) > 1/|F|$
$[\![\mathsf{M}mP]\!](w_N, w_P, w_F, \mu) = 0$ 上記以外

$\models P$ とは、任意の (w_N, w, w_F, μ) に対して $[\![P]\!](w_N, w_P, w_F, \mu) = 1$

公理系

分離規則：$\dfrac{P \supset Q \quad P}{Q}$　　一般化規則：$\dfrac{P}{\forall mP}$　　必然性規則：$\dfrac{P}{\mathsf{A}P}$

始式：

1. トートロジー
2. 等号に関する始式　2.1. $T = T$　2.2. $T = U \supset P[T/x] \supset P[U/x]$
3. 量化に関する始式
   3.1. $(\forall mP) \supset P[T/m]$　3.2. $\forall m(P \supset Q) \supset P \supset \forall Q$ 但し $m \notin FV(P)$
4. 体 F の理論
5. 確率に関する始式
   5.1 $P \supset\subset \mathsf{A}P$ 但し $V_P \cap FV(P) = \emptyset$
   5.2. $\mathsf{A}P \supset \mathsf{M}P$　5.3. $\mathsf{A}(P \supset Q) \supset \mathsf{A}P \supset \mathsf{A}Q$　5.4. $\mathsf{A}(P \supset Q) \supset \mathsf{M}P \supset \mathsf{M}Q$
   5.5. $\neg\forall m\mathsf{M}(m = T)$ 但し $m \notin FV(T)$
   5.6. $\mathsf{R}(x; x', x'', ...) \supset (\mathsf{M}P \supset\subset \mathsf{M}P[x + T/x])$
   　　但し $FV(P) \subset \{x, x', x'', ...\}$ 、$FV(T) \subset \{x', x'', ...\}$

確率論的秘匿とは

$$\neg\forall m \mathsf{M}(m = f(y_1, y_2, ..., y_k, p))$$

$y_1, y_2, ..., y_k$ は攻撃者が知り得る情報、p は攻撃者が使う確率オラクル

函数記号 f を全称束縛する構文はないが、
意味論的には論理式の一番外側で束縛されるので、
「任意の f に対してある m があって $\neg\mathsf{M}(m = f(y_1, y_2, ..., y_k))$」
という意味になる

m、x_1、… x_{t-1} から y_1、… y_n を定める計算は

$$y_i = m + g^{i-1}x_1 + g^{2(i-1)}x_2 + \ldots + g^{(t-1)(i-1)}x_{t-1}$$

この計算を表す論理式を P_1 と置く
即ち

$$P_1 \equiv \bigwedge_{i=1,...,n} y_i = m + \overline{g^{i-1}}x_1 + \overline{g^{2(i-1)}}x_2 + \ldots + \overline{g^{(t-1)(i-1)}}x_{t-1}$$

この議論の仮定は、$x_1, ..., x_k$ の分布に偏りがないことである
この性質を表す論理式を P_2 と置く
即ち

$$P_2 \equiv \bigwedge_{i=1,...,k} \mathsf{R}(x_i; x_{k+1}, ..., x_{t-1})$$

先の非形式的な議論から、ある項 $T(z_1, ..., z_k, p)$、$L_i(m, x_{k+1}, ..., x_{t-1})$ があって

$\vdash P_1 \supset$

$f(y_1, ..., y_k) = T(x_1 + L_1(m, x_{k+1}, ..., x_{t-1}), ..., x_k + L_k(m, x_{k+1}, ..., x_{t-1}), p)$

かつ

$FV(T(z_1, ..., z_k, p) = \{z_1, ..., z_k, p\}$

$FV(L_i(m, x_{k+1}, ..., x_{t-1})) = \{m, x_{k+1}, ..., x_{t-1}\}$

等号に関する始式、確率に関する始式より

$\vdash \mathsf{A}P_1 \supset \mathsf{M}(m = f(y_1, ..., y_k)) \supset$

$\mathsf{M}(m = T(x_1 + L_1(m, x_{k+1}, ..., x_{t-1}), ..., x_k + L_k(m, x_{k+1}, ..., x_{t-1}), p))$

確率に関する始式より

$\vdash P_2 \supset (\mathsf{M}(m = T(x_1, ..., x_k) \supset\subset$

$\mathsf{M}(m = T(x_1 + L_1(m, x_{k+1}, ..., x_{t-1}), ..., x_k + L_k(m, x_{k+1}, ..., x_{t-1}), p)))$

故に　$\vdash \mathsf{A}P_1 \supset P_2 \supset \mathsf{M}(m = f(y_1, ..., y_k, p)) \supset \mathsf{M}(m = T(x_1, ..., x_k))$

$\vdash \mathsf{A}P_1 \supset P_2 \supset \mathsf{M}(m = f(y_1, ..., y_k, p)) \supset \mathsf{M}(m = T(x_1, ..., x_k))$

故に

$\vdash \mathsf{A}P_1 \supset P_2 \supset \forall m\mathsf{M}(m = f(y_1, ..., y_k, p)) \supset \forall m\mathsf{M}(m = T(x_1, ..., x_k))$

所で $m \notin FV(T(x_1, ..., x_k))$ であるから

$\vdash \neg\forall m\mathsf{M}(m = T(x_1, ..., x_k))$

故に

$\vdash \mathsf{A}P_1 \supset P_2 \supset \neg\forall m\mathsf{M}(m = f(y_1, ..., y_k, p))$