形式手法の計算論的健全性

川本 裕輔

LIX, École Polytechnique & INRIA Saclay, France

概 要

形式手法の「計算論的健全性」とは，形式手法を用いて安全性が証明された暗号プロトコルは，計算量理論の観点からも安全であるという性質である．

1 形式手法の計算論的健全性

[数理的技法による情報セキュリティの検証]（p.244）でも述べたように，暗号プロトコルの安全性の解析には「形式手法」と「計算論的手法」がある．形式手法による解析は，計算論的手法による解析と異なり，プロトコルの部品として用いる暗号方式に対する攻撃の確率を考慮しない．このため，形式手法を用いて安全性が確かめられたプロトコルに対し，暗号の脆弱性に基づく攻撃が存在する可能性がある．

一方，暗号を破る攻撃の確率が十分小さい場合，形式手法の計算論的健全性（すなわち，形式手法を用いて安全だと証明されたプロトコルは，計算論的手法における計算量的安全性を満たすという性質）を示せる．計算論的健全性は，暗号方式の安全性の種類，検証したいプロトコルの安全性の種類，想定する攻撃者の種類に応じて，様々な結果が知られている．

2 受動的攻撃者のもとでの計算論的健全性

まず，受動的攻撃者（通信内容を傍受できるが，改竄できない攻撃者）を想定する場合の計算論的健全性 [1] を説明する．本節では逐次的にメッセージを送受信するだけのプロトコルを考える．プロトコル実行は，通信路上のメッセージの連結で表現される．

2.1 構文論と記号的等価性

メッセージを項（記号表現）で表す．項として，鍵記号 K，ビット 0 と 1，項の連結 (M, N)，項 M の鍵 K による暗号文 $\{M\}_K$ を記述できる．ここでは対称鍵暗号のみを扱う．項 M から読み取れる情報を表現するために，パターン $pat(M)$ を定義する．

$$p(M,T) = M \qquad (M \in \mathbf{K} \cup \{0,1\} \text{ のとき})$$

$$p((M,N),T) = (p(M,T), p(N,T))$$

$$p(\{M\}_K, T) = \begin{cases} \{p(M,T)\}_K & (K \in T \text{ のとき}) \\ \square & (K \notin T \text{ のとき}) \end{cases}$$

$$pat(M) = p(M, \{K \in \mathbf{K} \mid M \vdash K\})$$

ただし，$\mathbf{K}$ は全ての鍵記号の集合，$\square$ は解読できない暗号文，$\{K \in \mathbf{K} \mid M \vdash K\}$ は項 M から導出できる全ての鍵記号の集合を表す．例えば，

$$\{K \in \mathbf{K} \mid (\{\{0\}_{K_1}\}_{K_2}, K_2) \vdash K\} = \{K_2\}$$

より，$pat((\{\{0\}_{K_1}\}_{K_2}, K_2)) = (\{\square\}_{K_2}, K_2)$．

次に，項の間の記号的等価性 $\cong$ を定義する．項 N に現れる各鍵記号 K を $\sigma(K)$ で置き換えたものを $N\sigma$ と書く．項 M，N に対し，$\mathbf{K}$ 上の全単射 σ が存在し，$pat(M) = pat(N\sigma)$ のとき，$M \cong N$ と書く．例えば，$(\{0\}_{K_1}, \{1\}_{K_2}) \cong (\{1\}_{K_3}, \{0\}_{K_1})$．

2.2 計算論的意味論と計算量的識別不能性

以下では，記号列としての項に対し，ビット列の確率分布の族を対応付ける「解釈」を定義する．

対称鍵暗号方式 Π を，鍵生成，暗号化，復号アルゴリズムの三つ組 $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ と定義し，自然数 η をセキュリティ・パラメータ，τ を乱数テープとする．

項 M に対応するビット列 $[\![M]\!]^\tau_{\Pi,\eta}$ を，

$$[\![K]\!]^\tau_{\Pi,\eta} = \langle k, \text{“}key\text{”} \rangle$$
$$[\![i]\!]^\tau_{\Pi,\eta} = \langle i, \text{“}bool\text{”} \rangle \quad (i \in \{0,1\})$$
$$[\![(M,N)]\!]^\tau_{\Pi,\eta} = \langle [\![M]\!]^\tau_{\Pi,\eta}, [\![N]\!]^\tau_{\Pi,\eta}, \text{“}pair\text{”} \rangle$$
$$[\![\{M\}_K]\!]^\tau_{\Pi,\eta} = \langle \mathcal{E}_\tau([\![M]\!]^\tau_{\Pi,\eta}, [\![K]\!]^\tau_{\Pi,\eta}), \text{“}enc\text{”} \rangle$$

で定める．k は τ の乱数と $\mathcal{K}$ で生成される鍵とし，$\mathcal{E}$ は τ の乱数を用いて暗号化する．末尾の

タグでメッセージの種別を表す．τ をランダムに選んだときのビット列 $[\![M]\!]^{\tau}_{\Pi,\eta}$ の確率分布を $[\![M]\!]_{\Pi,\eta}$ とし，確率分布族 $\{[\![M]\!]_{\Pi,\eta}\}_{\eta\in\mathbb{N}}$ を M の解釈 $[\![M]\!]_{\Pi}$ とする．

確率分布族 $D=\{D_\eta\}_{\eta\in\mathbb{N}}$ と $D'=\{D'_\eta\}_{\eta\in\mathbb{N}}$，任意の確率的多項式時間（PPT）アルゴリズム $\mathcal{A}$ に対し，次の関数 ε が無視できる[1]とき，D と D' が計算量的に識別不能であるといい，$D\approx D'$ と書く．

$$\varepsilon(\eta)=\Big|\Pr\left[x\leftarrow D_\eta\colon \mathcal{A}(x)=1\right] - \Pr\left[x\leftarrow D'_\eta\colon \mathcal{A}(x)=1\right]\Big|$$

2.3 記号的等価性の計算論的健全性

ビット列 m の鍵 k による暗号文を受信した受動的攻撃者が，m や k についていかなる情報も多項式時間で得られないとき，type-0 安全であるという．

項 $\{K\}_K$ や $\{\{K_1\}_{K_2}\}_{K_1}$ のように，暗号化に用いる対称鍵が暗号化されるメッセージの中に含まれることを鍵循環という．

定理 1 *M と N を鍵循環を含まない項とし，対称鍵暗号方式 Π が type-0 安全であるとする．$M\cong N$ ならば $[\![M]\!]_{\Pi}\approx[\![N]\!]_{\Pi}$ である．*

二つのプロトコル実行を表す項の間の記号的等価性を示しさえすれば，定理 1 より，計算論的手法における受動的攻撃者のもとでの計算量的安全性（プロトコル実行の間の計算量的識別不能性）が導かれる．

3 能動的攻撃者のもとでの計算論的健全性

次に，能動的攻撃者（メッセージの改竄や順序の入れ替えもできる攻撃者）を考える．Cortier と Warinschi の研究 [5] に基づき，公開鍵暗号の場合について述べる．

3.1 記号モデル

記号モデルでは項として，i 番目の参加者の名前 a_i，a_i の公開鍵 $\mathsf{pk}(a_i)$ と秘密鍵 $\mathsf{sk}(a_i)$，ノンス n_j，鍵 $\mathsf{pk}(a_i)$ による t の暗号文 $\{t\}^{l}_{\mathsf{pk}(a_i)}$ を扱う．ラベル l は，同じ平文と鍵による暗号文の区別に用いる．

攻撃者の動作として，参加者の集合 $\overline{a}$ による新しいセッションの生成 $new(\overline{a})$ と，セッション s への項 t の送信とそれに対するの応答の受信 $send(s,t)$ を扱う．攻撃者は，受信した項の集合 H から導出できる項のみを送信する．H から項 t が導出できるとき，攻撃者のラベル l を用いて $\{t\}^{l}_{\mathsf{pk}(a_i)}$ を導出できる．H から $\{t\}^{l}_{\mathsf{pk}(a_i)}$ と $\mathsf{sk}(a_i)$ を導出できるとき，t を導出できる．受信した項の集合 H_j と攻撃者の動作 E_j の列 $H_0\xrightarrow{E_0}H_1\cdots\xrightarrow{E_{n-1}}H_n$ で記号トレースを定義する．秘密鍵を含むメッセージを参加者が送信しないようなプロトコル Π を考える．Π を実行した記号トレース全体の集合を Exe^{s}_{Π} と書く．

3.2 計算論的モデル

計算論的モデルでも，攻撃者の動作 new と $send$ を扱うが，項の代わりにビット列を扱う．攻撃者は，受信ビット列の集合 H から PPT 計算可能なビット列を送信する．受信ビット列集合と攻撃者の動作の列で計算論的トレースを定義する．PPT 攻撃者 $\mathcal{A}$ のもとでプロトコル Π を実行した計算論的トレースは，ノンスと鍵の生成や暗号化の乱数により確率的に定まる．セキュリティ・パラメータ η に対し，計算論的トレースの確率分布を $Exe^{c}_{\Pi,\mathcal{A}}(\eta)$ で表す．

3.3 マッピング補題と計算論的健全性

マッピング補題（mapping lemma）は，計算論的トレースに対して記号トレースが対応しない確率が無視できるという性質である．ビット列集合から項集合への部分関数 c に対し，計算論的トレース tr^c に現れる各ビット列 m を $c(m)$ で置き換えたものを $c(tr^c)$ と書く．単射な部分関数 c が存在し，$c(tr^c)$ が記号トレース tr^s であるとき，$tr^s\preceq tr^c$ と書く．

補題 2 *公開鍵暗号が IND-CCA2 安全[2]のとき，任意の PPT 攻撃者 $\mathcal{A}$ に対し，次が無視できる．*

$$Pr\left[tr^c\leftarrow Exe^{c}_{\Pi,\mathcal{A}}(\eta)\colon\ \forall tr^s\in Exe^{s}_{\Pi}\ \ tr^s\not\preceq tr^c\right]$$

プロトコル Π の安全性を，望ましいトレースの集合で表す．Π が記号トレースの集合 P^s で表される安全性を満たすことを $Exe^{s}_{\Pi}\subseteq P^s$ で定

[1] 自然数から実数への関数 ε が，$\forall c>0\ \exists N\ \forall\eta\geq N\ \varepsilon(\eta)\leq\eta^{-c}$ を満たすとき，ε が無視できるという．

[2] 能動的攻撃者のもとでの安全性定義のひとつ

義する．Πが計算論的トレースの集合 P^c で表される安全性を満たすことを任意の PPT アルゴリズム $\mathcal{A}$ に対し，$\Pr\left[tr^c \leftarrow Exe^c_{\Pi,\mathcal{A}}(\eta)\colon tr^c \notin P^s\right]$ が無視できることとする．P^s が P^c に対応する（$c^{-1}(P^s) \subseteq P^c$ である）とき，補題 2 から次が導かれる．

定理 3 Π が記号モデルで安全性 P^s を満たすならば，Π は計算論的モデルで安全性 P^c を満たす．

つまり，記号モデルで Π の安全性を示せば，定理 3 により，Π の計算論的実行の安全性が導かれる．

同様の考え方で，汎用的結合可能性での安全性が記号的安全性から導かれることが示されている [2].

4　その後の計算論的健全性の研究

匿名性のように，等価性で表せてもトレース集合で表せない安全性は，定理 3 を適用できない．能動的攻撃者のもとでの等価性の計算論的健全性は，2.3 項の等価性の健全性と 3.3 項のマッピング補題を発展させた議論で導かれる [3, 4].

参考文献

[1] M. Abadi and P. Rogaway. Reconciling two views of cryptography (the computational soundness of formal encryption). *Journal of Cryptology*, 15(2), pp.103 – 127, 2002.

[2] R. Canetti and J. Herzog. Universally composable symbolic analysis of mutual authentication and key-exchange protocols. In *Proc. TCC'06*, Springer *Lecture Notes in Computer Science*, Vol. 3876, pp.380–403, 2008.

[3] H. Comon-Lundh and V. Cortier. Computational soundness of observational equivalence. In *Proc. ACM CCS'08*, pp.109–118, 2008.

[4] H. Comon-Lundh, M. Hagiya, Y. Kawamoto and H. Sakurada. Computational soundness of indistinguishability properties without computable parsing. In Proc. *ISPEC'12*, Springer *Lecture Notes in Computer Science*, Vol. 7232, pp.63–79, 2012.

[5] V. Cortier and B. Warinschi. Computationally sound, automated proofs for security protocols. In *Proc. ESOP'05*, Springer *Lecture Notes in Computer Science*, Vol. 3444, pp.157–171, 2005.