6A-2

暗号文間の関係情報認知可能性に関する論理体系

萩原 茂樹　　小黒 博昭　　米崎 直樹
東京工業大学大学院情報理工学研究科計算工学専攻

1 はじめに

敵が獲得可能なメッセージ集合を想定し，その集合から敵が認知できる情報を解析することにより，暗号プロトコルの秘密性を検証することができる．著者らはこれまでに，2 つの暗号メッセージの鍵や内容の関係情報すなわち同値性・非同値性の，認知可能性を解析するための論理体系を提案した [1, 2]．本稿では，その論理体系に対する可能世界意味論を構成し，[2] の公理系がこの意味論に対して健全であることを述べる．

2 暗号文間の関係情報認知可能性の論理体系の構文

定義 1 (メッセージ) (1)（対称）鍵記号 $K \in \mathcal{K}$，公開アトミックメッセージ記号 $I \in \mathcal{I}$，秘密アトミックメッセージ記号 $N \in \mathcal{N}$ はそれぞれメッセージである．(2) T_1 と T_2 がメッセージであるとき，その連結 (T_1, T_2) はメッセージである．(3) T がメッセージであり，$K \in \mathcal{K}$ が鍵記号，$R \in \mathcal{R}$ が乱数値の記号であるとき，T を K で暗号化したメッセージ $\{T\}_K^R$ はメッセージである．$\{T\}_K^R$ を暗号メッセージと呼ぶ．

定義 2 (拡張メッセージ) (1) メッセージ T は拡張メッセージである．(2) E が拡張メッセージであるとき，$content\_of(E)$, $key\_of(E)$ は拡張メッセージである．

E が暗号メッセージを表す場合，$content\_of(E)$ はその内容を，$key\_of(E)$ は E の暗号化に用いられた鍵を表す．E が暗号メッセージを表していない場合，未定義とすることを意図する．

定義 3 (式) (1) T_1, T_2 がメッセージであるとき，$T_1 \geqslant T_2$ は式である．(2) E_1, E_2 が拡張メッセージであるとき，$E_1 \equiv E_2$ と $E_1 \not\equiv E_2$ は式である．(3) φ_1, φ_2 が式であるとき，$\varphi_1 \wedge \varphi_2, \neg\varphi_1$ は式である．(4) T がメッセージ，φ が式であるとき，$T \triangleright \varphi$ は式である．

ここで，$T_1 \geqslant T_2$ は T_1 の値から T_2 の値が構成できることを表し，$E_1 \equiv E_2 (E_1 \not\equiv E_2)$ は E_1 と E_2 の値が定義され，それらが等しい（異なる）ことを表わす．$T \triangleright \varphi$ は T を持っている敵は φ が成り立つことを認知することを表す．$T \triangleright \varphi$ の形の式を様相式とよぶ．

An Epistemic Logic of Relational Information between Ciphertexts, Shigeki Hagihara, Hiroaki Oguro and Naoki Yonezaki, Department of Computer Science, Graduate School of Information Science and Engineering, Tokyo Institute of Technology.

例 1 T, T_1, T_2 がメッセージであるとき，$content\_of(T_1) \equiv T_2$ や $key\_of(T_1) \not\equiv key\_of(T_2)$ は式であり，それぞれ「T_1 は暗号メッセージであり，その内容の値が T_2 の値と等しい」こと，「T_1 と T_2 は暗号メッセージであり，そこで用いられている鍵は異なる」ことを表す．$T \triangleright content\_of(T_1) \equiv T_2$ や $T \triangleright key\_of(T_1) \not\equiv key\_of(T_2)$ は様相式であり，T を持っている敵は上記のことを認知することを表す．

3 可能世界意味論

定義 4 (メッセージ代数) メッセージ代数は組 $\mathcal{A} = \langle A_{key}, A_{pub}, A_{sec}, A_{ct}, A_{pair}, R_{hon}, R_{adv}, pair, enc \rangle$ である．ここで，$A_{key}, A_{pub}, A_{sec}, A_{ct}, A_{pair}$ はそれぞれ鍵データ，公開データ，秘密データ，暗号データ，対データの集合であり，交わりがないとする．$A = A_{key} \cup A_{pub} \cup A_{sec} \cup A_{ct} \cup A_{pair}$ をメッセージデータの集合とよぶ．R_{hon} と R_{adv} は，正当な参加者と敵がそれぞれ用いる乱数データの集合である．$pair : A^2 \to A_{pair}$ は対データ生成関数，$enc : A \times A_{key} \times (R_{hon} \cup R_{adv}) \to A_{ct}$ は暗号化関数である．さらに，enc と $pair$ について，次が成り立つとする．$enc(d, k, r) = enc(d', k', r') \Rightarrow d = d' \wedge k = k' \wedge r = r'$, $pair(d_1, d_2) = pair(d_3, d_4) \Rightarrow d_1 = d_3 \wedge d_2 = d_4$

定義 5 (閉包) U をメッセージデータの集合とする．このとき，U の閉包 $cl(U)$ は以下を満たすメッセージデータの最小集合 X である．(1) $U \subseteq X$ (2) $A_{pub} \subseteq X$ (3) $d_1, d_2 \in X \Rightarrow pair(d_1, d_2) \in X$ (4) $pair(d_1, d_2) \in X \Rightarrow d_1, d_2 \in X$ (5) $d, k \in X, k \in A_{key}, r \in R_{adv} \Rightarrow enc(d, k, r) \in X$ (6) $enc(d, k, r), k \in X \Rightarrow d \in X$

$cl(U)$ は，敵により U から構成されるメッセージデータの集合を表す．

定義 6 (メッセージの意味) $\mathcal{A}$ をメッセージ代数とする．m をアトミックメッセージ記号と乱数値記号に対して，適切な型のメッセージデータや乱数データを割り当てる付値とする．ここで，m は異なる記号には異なるデータを割り当てるものとする．これを用いて，メッセージにメッセージデータを割り当てる付値関数 $[\![\cdot]\!]_{\mathcal{A},m}$ を次のように定義する．

- $[\![K]\!]_{\mathcal{A},m} = m(K)$, $[\![I]\!]_{\mathcal{A},m} = m(I)$, $[\![N]\!]_{\mathcal{A},m} = m(N)$
- $[\![(T_1, T_2)]\!]_{\mathcal{A},m} = pair([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m})$
- $[\![\{T\}_K^R]\!]_{\mathcal{A},m} = enc([\![T]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R))$

定義 7 (メッセージデータの再解釈) $U \subseteq A$ を敵が持つメッセージデータの集合とする．このとき，A から A

への全単射 π が以下の条件をみたすとき，U のもとでの準再解釈という．(1) $d \in A_{key} \cup A_{pub} \cup A_{sec} \Rightarrow \pi(d) = d$ (2) $\pi(pair(d_1, d_2)) = pair(\pi(d_1), \pi(d_2))$ (3) π は暗号データを暗号データへ写像する．(4) $enc(d, k, r)$, $k \in U \Rightarrow \pi(enc(d, k, r)) = enc(\pi(d), k, r)$ (5) $d, k \in U, k \in A_{key}, r \in R_{adv} \Rightarrow \pi(enc(d, k, r)) = enc(\pi(d), k, r)$ (6) $enc(d, k, r), k' \in U$ かつ $k \neq k' \Rightarrow \forall d' \forall r' \pi(enc(d, k, r)) \neq enc(d', k', r')$. π が U のもとでの準再解釈であり，かつ，π^{-1} が $\pi(U)$ のもとでの準再解釈であるとき，π を U のもとでの再解釈という．さらに，$\pi(X) = \{\pi(d) | d \in X\}$ とする．U のもとでの再解釈の集合を $R(U)$ とする．

$\pi(d_1) = d_2$ を満たす U のもとでの再解釈 π が存在することは，U しか持たない敵は d_1 と d_2 の違いを識別できないことを表す．

定義 8 (拡張メッセージの意味) π をメッセージデータの再解釈とする．拡張メッセージにメッセージデータを割り当てる付値関数 $[\![\cdot]\!]^{\pi}_{\mathcal{A},m}$ を次のように定義する．

- $[\![T]\!]^{\pi}_{\mathcal{A},m} = \pi([\![T]\!]_{\mathcal{A},m})$
- $[\![content\_of(E)]\!]^{\pi}_{\mathcal{A},m} = \begin{cases} d & \text{if } [\![E]\!]^{\pi}_{\mathcal{A},m} = enc(d,k,r) \\ \bot & \text{otherwise} \end{cases}$
- $[\![key\_of(E)]\!]^{\pi}_{\mathcal{A},m} = \begin{cases} k & \text{if } [\![E]\!]^{\pi}_{\mathcal{A},m} = enc(d,k,r) \\ \bot & \text{otherwise} \end{cases}$

ここで，$\bot$ は未定義をあらわす特別なデータであり，$\bot \notin A$ とする．$content\_of(E)$ や $key\_of(E)$ の意味を，E に対する付値を π に従って再解釈し，その結果得られるデータが暗号データであるならば，その内容や鍵の値と定義し，そうでないならば，$\bot$ と定義している．

定義 9 (式の意味) $\mathcal{A}$ をメッセージ代数，m をアトミックメッセージ記号にメッセージデータを割り当てる付値，π を再解釈とする．$\mathcal{A}, m, \pi$ で，式 φ が真であることを $\mathcal{A}, m, \pi \models \varphi$ で表し，以下のように定義する．

- $\mathcal{A}, m, \pi \models T_1 \geqslant T_2 \Leftrightarrow [\![T_2]\!]^{\pi}_{\mathcal{A},m} \in cl(\{[\![T_1]\!]^{\pi}_{\mathcal{A},m}\})$
- $\mathcal{A}, m, \pi \models E_1 \equiv E_2 \Leftrightarrow$ $[\![E_1]\!]^{\pi}_{\mathcal{A},m} = [\![E_2]\!]^{\pi}_{\mathcal{A},m} \wedge [\![E_1]\!]^{\pi}_{\mathcal{A},m} \neq \bot$
- $\mathcal{A}, m, \pi \models E_1 \not\equiv E_2 \Leftrightarrow [\![E_1]\!]^{\pi}_{\mathcal{A},m} \neq [\![E_2]\!]^{\pi}_{\mathcal{A},m}$ $\wedge [\![E_1]\!]^{\pi}_{\mathcal{A},m} \neq \bot \wedge [\![E_2]\!]^{\pi}_{\mathcal{A},m} \neq \bot$
- $\mathcal{A}, m, \pi \models \varphi_1 \wedge \varphi_2 \Leftrightarrow \mathcal{A}, m, \pi \models \varphi_1 \ \wedge \ \mathcal{A}, m, \pi \models \varphi_2$
- $\mathcal{A}, m, \pi \models \neg\varphi_1 \Leftrightarrow \mathcal{A}, m, \pi \not\models \varphi_1$
- $\mathcal{A}, m, \pi \models T \triangleright \varphi \Leftrightarrow$ $\forall \pi' \in R(\pi(cl([\![T]\!]_{\mathcal{A},m}))) (\mathcal{A}, m, \pi' \circ \pi \models \varphi)$

$T_1 \geqslant T_2$ が成り立つことを，T_1 の値から T_2 の値を構成できることと意味付けしている．$E_1 \equiv E_2$（$E_1 \not\equiv E_2$）が成り立つことを，E_1 と E_2 の値が定義され，それらが等しい（異なる）ことと意味付けしている．$T \triangleright \varphi$ が成り立つことを，T の値から敵が構成できるメッセージデータの集合のもとでの任意の再解釈において，φ がその再解釈した結果で成り立つことと意味付けしている．即ち，T の値を持つ敵が φ を認知することを，T の値を持つ敵が，メッセージの現付値と違いを識別できない如何なる付値に対しても，φ が成り立つことと意味付けしている．恒等写像を id とする．任意の $\mathcal{A}, m$ において，$\mathcal{A}, m, id \models \varphi$ であるとき，φ は可能世界意味論で恒真であるといい，$\models \varphi$ と記述する．

例 2 ● $\models content\_of(\{N\}^R_K) \equiv N$ である．
● $\models (\{N\}^R_K, K) \triangleright content\_of(\{N\}^R_K) \equiv N$ である．
● $\models \{N\}^R_K \triangleright content\_of(\{N\}^R_K) \equiv N$ ではない．

再解釈を用いて可能世界を表す手法は，[3] により，セキュリティプロトコルの匿名性の検証に用いる知識の論理の意味論で取り入れられた．本稿では，対象とした関係情報認知可能性の論理で用いることできるように，[3] の手法を変更して導入した．

4 演繹体系

[2] において，敵による関係情報の認知可能性を演繹する体系を構成した．この体系は，3 章で定義した可能世界意味論に対して健全である．

定義 10 (JD 体系 [2]) 以下の規則により，式 φ が導出されるとき，$\vdash_{JD} \varphi$ と記述する．

$$\frac{}{T \geqslant T} \quad \frac{}{T \geqslant I} \ (I \in \mathcal{I})$$

$$\frac{T \triangleright T_1 \quad T \geqslant T_1}{T \triangleright (T_1, T_2)} \quad \frac{T \geqslant (T_1, T_2)}{T \geqslant T_1} \quad \frac{T \geqslant (T_1, T_2)}{T \geqslant T_2}$$

$$\frac{T \geqslant \{T_1\}^R_K \quad T \geqslant K}{T \geqslant T_1} \qquad \frac{T \geqslant T_1 \quad T \geqslant K}{T \geqslant \{T_1\}^R_K} \ (R \in \mathcal{R}_{adv})$$

$$\frac{T \geqslant T_1}{T \triangleright T_1 \equiv T_1} \quad \frac{T \geqslant T_1 \quad T \geqslant T_2}{T \triangleright T_1 \not\equiv T_2} \ (T_1 \text{ と } T_2 \text{ は構文的に異なる})$$

$$\frac{T \triangleright \{T_1\}^R_K \equiv \{T_2\}^{R'}_{K'}}{T \triangleright f(\{T_1\}^R_K) \equiv f(\{T_2\}^{R'}_{K'})} \ (f \in \{content\_of, key\_of\})$$

$$\frac{T \geqslant \{T_1\}^R_K \quad T \geqslant K}{T \triangleright content\_of(\{T_1\}^R_K) \equiv T_1} \qquad \frac{T \geqslant \{T_1\}^R_K \quad T \geqslant K}{T \triangleright key\_of(\{T_1\}^R_K) \equiv K}$$

$$\frac{T \geqslant \{T_1\}^R_K \quad T \geqslant T_2}{T \triangleright key\_of(\{T_1\}^R_K) \not\equiv T_2} \ (T_2 \text{ と } K \text{ は構文的に異なる})$$

$$\frac{T \triangleright E_1 \equiv E}{T \triangleright E \equiv E_1} \quad \frac{T \triangleright E_1 \not\equiv E}{T \triangleright E \not\equiv E_1}$$

$$\frac{T \triangleright E \equiv E_2 \quad T \triangleright E_2 \equiv E_1}{T \triangleright E \equiv E_1} \qquad \frac{T \triangleright E \equiv E_2 \quad T \triangleright E_2 \not\equiv E_1}{T \triangleright E \not\equiv E_1}$$

定理 1 (健全性) $\vdash_{JD} \varphi$ ならば，$\models \varphi$ である．

参考文献

[1] Ashraf Bhery, Shigeki Hagihara, and Naoki Yonezaki. A formal system for analysis of cryptographic encryption and their security properties. In *International Symposium on Software Security 2003*, Vol. 3233 of *Lecture Notes in Computer Science*, pp. 87–112, 2004.

[2] 萩原茂樹, 小黒博昭, 米崎直樹. 暗号文から得られる部分情報に関する推論体系とその計算論に基づく意味. 日本ソフトウェア科学会第 24 回大会講演論文集, 2007.

[3] Flavio D. Garcia, Ichiro Hasuo, Wolter Pieters, and Peter van Rossum. Provable anonymity. In *FMSE '05: Proceedings of the 2005 ACM workshop on Formal methods in security engineering*, pp. 63–72, New York, NY, USA, 2005. ACM.