2E-4

紛失通信プロトコルの解析のための可能世界意味論に基づく形式体系*

小黒 博昭 †　　萩原 茂樹 †　　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

Bhery らは Dolev-Yao の記号論的な手法を基に，暗号メッセージから得られる部分情報を推論可能な演繹体系 (Judgment-Deduction System; JD 体系) を提案した [1]．さらに，萩原らは JD 体系に対し，確率的多項式時間チューリング機械を用いた計算論に基づく意味を与え，その意味論に対する健全性および完全性を示した [3]．これらの研究の流れを汲み，著者らはこれまでに，暗号プロトコルの基本要素としてよく利用される 1-out-of-2 型の Oblivious Transfer (OT; 紛失通信) プロトコルに着目し，同プロトコルの一実現形態である EGL85 プロトコル [2] の性質を記号論的に解析するための形式体系を提案している [4]．しかしながら，[4] で提案された形式体系には構文に対する直観的な意味しか与えられておらず，形式的な意味論が与えられていなかった．

本稿では，[4] で提案された形式体系に対し，可能世界モデルに基づく意味論を与え，その意味論における推論規則の健全性を示す．

2 構文

EGL85 を記号論的に解析するために用いるメッセージを定義する．

定義 1 (メッセージ) $\mathcal{B} = \{0, 1\}$ をビットを表す定数記号の集合，$\mathcal{R} = \{r, s\}$ をランダムビットを表す定数記号の集合，k を送信者の公開鍵を表す定数記号，k^{-1} をその私有鍵を表す定数記号，$\mathcal{M} = \{M_0, M_1\}$ をデータを表す定数記号の集合，$\mathcal{X} = \{x, m_0, m_1\}$ を乱数データを表す定数記号の集合とする．このとき，B を $\mathcal{B}$ の要素を表すメタ変数，R を $\mathcal{R}$ の要素を表すメタ変数，M を $\mathcal{M}$ の要素を表すメタ変数，X を $\mathcal{X}$ の要素を表すメタ変数として，メッセージ T を以下のように帰納的に定義する．

$$\begin{array}{rcl} B & ::= & \mathsf{B} \mid \mathsf{R} \mid (B_1 \oplus B_2) \\ X & ::= & \mathsf{X} \\ T & ::= & B \mid X \mid k \mid k^{-1} \mid \mathsf{M} \mid C(X_1, X_2, B) \\ & & \mid E_k(T) \mid D_{k^{-1}}(T) \\ & & \mid (T_1 \boxplus_k T_2) \mid (\boxminus_k T) \mid \langle T_1, T_2 \rangle \end{array}$$

ここで，$(B_1 \oplus B_2)$ は二つのビットの排他的論理和を表すメッセージである．$C(X_1, X_2, B)$ は B により X_1 または X_2 のどちらかを表すメッセージである．$E_k(T)$ は公開鍵 k により T を暗号化したメッセージである．$D_{k^{-1}}(T)$ は私有鍵 k^{-1} により T を復号したメッセージである．$(T_1 \boxplus_k T_2)$ は公開鍵 k により定まる有限体上で加算した結果を表すメッセージである．$(\boxminus_k T)$ は公開鍵 k により定まる有限体上の逆元を表すメッセージである．$\langle T_1, T_2 \rangle$ は T_1 および T_2 の対を表すメッセージである．

定義 2 (式) T, T_1, T_2 をメッセージを表すメタ変数，Γ をメッセージの集合とするとき，式 F を以下のように定義する．

$$\begin{array}{rcl} P & ::= & T_1 = T_2 \mid T_1 \neq T_2 \\ F & ::= & P \mid \Gamma \models T \mid \Gamma \models P \end{array}$$

ここで，P の型の式を関係情報，$\Gamma \models T$ の型の式をメッセージ認識文，$\Gamma \models P$ の型の式を判定文と呼ぶ．

定義 3 (代数法則) メッセージの値がいかなる値でも常に等価性が成立する代数法則を *[4]* のように定義する．(例えば，B_1, B_2, B_3 をビットを表すメッセージのメタ変数とするとき，$((B_1 \oplus B_2) \oplus B_3) = (B_1 \oplus (B_2 \oplus B_3))$ は代数法則の一つである．)

代数法則を公理とみなし，公理および等号付き一階述語論理の推論規則を用いて，仮定 $P_1, \ldots, P_n$ から P が演繹されるとき，$P_1, \ldots, P_n \vdash P$ と記述する．特に，仮定なしで P が演繹されるとき，$\vdash P$ と記述する．

定義 4 (メッセージ認識規則) メッセージ認識文が導出される推論規則を以下のように定義する．

(B1) $\dfrac{}{\Gamma \models \mathsf{0}}$　　*(B2)* $\dfrac{}{\Gamma \models \mathsf{1}}$

(B3) $\dfrac{}{\Gamma \models T}\ (T \in \Gamma)$　　*(B4)* $\dfrac{\Gamma \models B_1 \qquad \Gamma \models B_2}{\Gamma \models (B_1 \oplus B_2)}$

(B5) $\dfrac{\Gamma \models X_1 \qquad \Gamma \models X_2 \qquad \Gamma \models B}{\Gamma \models C(X_1, X_2, B)}$

(B6) $\dfrac{\Gamma \models X_1 \qquad \Gamma \models X_2 \qquad \Gamma \models C(X_1, X_2, B)}{\Gamma \models B}$ *(ただし X_1 と X_2 は異なる記号)*

(B7) $\dfrac{\Gamma \models k \qquad \Gamma \models T}{\Gamma \models E_k(T)}$　　*(B8)* $\dfrac{\Gamma \models k^{-1} \qquad \Gamma \models T}{\Gamma \models D_{k^{-1}}(T)}$

(B9) $\dfrac{\Gamma \models k \qquad \Gamma \models T_1 \qquad \Gamma \models T_2}{\Gamma \models (T_1 \boxplus_k T_2)}$

(B10) $\dfrac{\Gamma \models k \qquad \Gamma \models T}{\Gamma \models (\boxminus_k T)}$　　*(B11)* $\dfrac{\Gamma \models T_1 \qquad \Gamma \models T_2}{\Gamma \models \langle T_1, T_2 \rangle}$

(B12) $\dfrac{\Gamma \models \langle T_1, T_2 \rangle}{\Gamma \models T_1}$　　*(B13)* $\dfrac{\Gamma \models \langle T_1, T_2 \rangle}{\Gamma \models T_2}$

(B14) $\dfrac{\Gamma \models T_1 \qquad T_1 = T_2}{\Gamma \models T_2}$ *(ただし $T_1 = T_2$ は仮定なしで代数法則のみから導出される式)*

(B15) $\dfrac{\Gamma \models T_1 \quad \Gamma \models T_2 \quad \Gamma \models T[T_1] \quad T_1 = T_2}{\Gamma \models T[T_2/T_1]}$ *(ただし $T_1 = T_2$ は仮定および代数法則から導出される式)*

定義 5 (JD-推論規則) 定義 *4* に示されるメッセージ認識規則に，判定文が導出される以下の推論規則を追加した規則群を JD-推論規則と定義する．

(C1) $\dfrac{T_1 = T_2}{\Gamma \models T_1 = T_2}$ *(ただし $T_1 = T_2$ は仮定なしで代数法則のみから導出される式)*

(C2) $\dfrac{T_1 \neq T_2}{\Gamma \models T_1 \neq T_2}$ *(ただし $T_1 \neq T_2$ は仮定なしで代数法則のみから導出される式)*

* Formal System Based on Possible World Semantics for Analysis of Oblivious Transfer Protocols. †Hiroaki Oguro, Shigeki Hagihara, Naoki Yonezaki, Department of Computer Science, Graduate School of Information Science and Engineering, Tokyo Institute of Technology.

(C3) $\dfrac{\Gamma \models T_1 \qquad \Gamma \models T_2 \qquad T_1 = T_2}{\Gamma \models T_1 = T_2}$ *(ただし $T_1 = T_2$ は仮定および代数法則から導出される式)*

(C4) $\dfrac{\Gamma \models T_1 \qquad \Gamma \models T_2 \qquad T_1 \neq T_2}{\Gamma \models T_1 \neq T_2}$ *(ただし $T_1 \neq T_2$ は仮定および代数法則から導出される式)*

(C5) $\dfrac{\Gamma \models P_1 \ \cdots \ \Gamma \models P_n \qquad \begin{matrix} P_1, \ldots, P_n \\ \vdots \\ P \end{matrix}}{\Gamma \models P}$ *(ただし，前提の P は，仮定 $P_1, \ldots, P_n$ のみを仮定して代数法則および述語計算から導出される式)*

定義 6 (JD-導出) S をメッセージ認識文 $\Gamma \models T$ または判定文 $\Gamma \models P$ とする．このとき，関係情報 $P_1, \ldots, P_n$ を仮定して，JD-推論規則を用いて S が演繹されるとき，$P_1, \ldots, P_n \vdash_{JD} S$ と記述し，演繹不可能のとき，$P_1, \ldots, P_n \nvdash_{JD} S$ と記述する．

3 意味論

定義 7 (メッセージ代数) メッセージ代数は組 $\mathcal{A} = \langle A, pk, sk, xor, choose, enc, dec, add, inv, pair \rangle$ で定義される．ここで，A はビット列の集合の部分集合である．pk は送信者の公開鍵を表すビット列である．sk はその私有鍵を表すビット列である．$xor : \{0,1\} \times \{0,1\} \to \{0,1\}$ は以下のように定義される関数である．

$$xor(b_1, b_2) = \begin{cases} 0 & ((b_1, b_2) = (0,0)\, or\, (1,1)) \\ 1 & ((b_1, b_2) = (0,1)\, or\, (1,0)) \end{cases}$$

$choose : A \times A \times \{0,1\} \to A$ は以下のように定義される関数である．

$$choose(d_1, d_2, b) = \begin{cases} d_1 & (b = 0) \\ d_2 & (b = 1) \end{cases}$$

$enc : \{pk\} \times A \to A$ は公開鍵およびビット列からビット列を返す関数である．$dec : \{sk\} \times A \to A$ は私有鍵およびビット列からビット列を返す関数である．ここで，enc, dec は以下を満足するものとする．

$$\forall d \in A\, (dec(sk, enc(pk, d)) = enc(pk, dec(sk, d)) = d)$$

$add : \{pk\} \times A \times A \to A$ は二つのビット列に加法を適用したビット列を返す関数である．$inv : \{pk\} \times A \to A$ はビット列からその逆元のビット列を返す関数である．ここで，add, inv は以下を満足するものとする．

$$\forall d_1 \forall d_2 \forall d_3 \in A\, (add(pk, add(pk, d_1, d_2), d_3) = add(pk, d_1, add(pk, d_2, d_3)))$$

$$\forall d \in A\, (add(pk, d, 0) = d)$$

$$\forall d \in A\, (add(pk, d, inv(pk, d) = 0)$$

$$\forall d_1 \forall d_2 \in A\, (add(pk, d_1, d_2) = add(pk, d_2, d_1))$$

$pair$ は二つの任意のビット列からビット列の対を返す関数であり，以下を満足するものとする．

$$\forall d_1 \forall d_2 \forall d_3 \forall d_4 \in A\, (pair(d_1, d_2) = pair(d_3, d_4) \Rightarrow d_1 = d_3 \wedge d_2 = d_4)$$

$\mathcal{A}$ をメッセージ代数とする．$m : \mathcal{B} \cup \mathcal{R} \cup \mathcal{M} \cup \mathcal{X} \to A$ を意味関数とし，$I = (m, \mathcal{A})$ を解釈とする．このとき，メッセージに以下のビット列を割り当てる．

- $[\![\mathtt{0}]\!]_I = m(\mathtt{0}) = 0$, $[\![\mathtt{1}]\!]_I = m(\mathtt{1}) = 1$
- $[\![r]\!]_I = m(r)$, $[\![s]\!]_I = m(s)$
- $[\![(B_1 \oplus B_2)]\!]_I = xor([\![B_1]\!]_I, [\![B_2]\!]_I)$
- $[\![x]\!]_I = m(x)$, $[\![m_0]\!]_I = m(m_0)$, $[\![m_1]\!]_I = m(m_1)$
- $[\![k]\!]_I = m(k) = pk$, $[\![k^{-1}]\!]_I = m(k^{-1}) = sk$
- $[\![M_0]\!]_I = m(M_0)$, $[\![M_1]\!]_I = m(M_1)$
- $[\![C(X_1, X_2, B)]\!]_I = choose([\![X_1]\!]_I, [\![X_2]\!]_I, [\![B]\!]_I)$
- $[\![E_k(T)]\!]_I = enc([\![k]\!]_I, [\![T]\!]_I)$
- $[\![D_{k^{-1}}(T)]\!]_I = dec([\![k^{-1}]\!]_I, [\![T]\!]_I)$
- $[\![(T_1 \boxplus_k T_2)]\!]_I = add([\![k]\!]_I, [\![T_1]\!]_I, [\![T_2]\!]_I)$
- $[\![(\boxminus_k T)]\!]_I = inv([\![k]\!]_I, [\![T]\!]_I)$
- $[\![\langle T_1, T_2 \rangle]\!]_I = pair([\![T_1]\!]_I, [\![T_2]\!]_I)$

ただし，乱数データを表す定数記号 x, m_0, m_1 には，上記すべてのメッセージのビット列と異なるビット列が割り当てられるとする．

メッセージ T を基にし，そこから新たに計算可能なメッセージに関して分かることのすべてを表すために用いる閉包を定義する．

定義 8 (閉包) Y をメッセージの集合とする．このとき，Y の閉包 $cl(Y)$ は以下を満足する最小集合 U である．

1. $\{\mathtt{0}, \mathtt{1}\} \subset U$
2. $Y \subseteq U$
3. $B_1, B_2 \in U \Rightarrow (B_1 \oplus B_2) \in U$
4. $X_1, X_2, B \in U \Rightarrow C(X_1, X_2, B) \in U$
5. $X_1, X_2, C(X_1, X_2, B) \in U \Rightarrow B \in U$
6. $k, T \in U \Rightarrow E_k(T) \in U$
7. $k^{-1}, T \in U \Rightarrow D_{k^{-1}}(T) \in U$
8. $k, T_1, T_2 \in U \Rightarrow (T_1 \boxplus_k T_2) \in U$
9. $k, T \in U \Rightarrow (\boxminus_k T) \in U$
10. $T_1, T_2 \in U \Rightarrow \langle T_1, T_2 \rangle \in U$
11. $\langle T_1, T_2 \rangle \in U \Rightarrow T_1, T_2 \in U$
12. $\vdash T_1 = T_2$ のとき，$T_1 \in U \Rightarrow T_2 \in U$
13. $T_1, T_2, T[T_1] \in U \Rightarrow T[T_2/T_1] \in U$

式の意味（真偽値 t または f）は以下のように定義される．

- $[\![T_1 = T_2]\!]_I = t \iff [\![T_1]\!]_I = [\![T_2]\!]_I$
- $[\![T_1 \neq T_2]\!]_I = t \iff [\![T_1]\!]_I \neq [\![T_2]\!]_I$
- $[\![\Gamma \models T]\!]_I = t \iff \forall I'\, (I \approx_\Gamma I' \Rightarrow [\![T]\!]_I = [\![T]\!]_{I'})$, ここで，$I \approx_\Gamma I'$ *iff* $\forall T\, (T \in cl(\Gamma) \Rightarrow [\![T]\!]_I = [\![T]\!]_{I'})$
- $[\![\Gamma \models P]\!]_I = t \iff \forall I'\, (I \approx_\Gamma I' \Rightarrow [\![P]\!]_{I'})$

JD-推論規則の健全性は以下を示すことにより証明される．

1. $P_1, \ldots, P_n \vdash P \Rightarrow \forall I\, (\bigwedge_{i=1}^n ([\![P_i]\!]_I = t) \Rightarrow [\![P]\!]_I = t)$
2. $P_1, \ldots, P_n \vdash_{JD} \Gamma \models T \Rightarrow \forall I\, (\bigwedge_{i=1}^n ([\![P_i]\!]_I = t) \Rightarrow [\![\Gamma \models T]\!]_I = t)$
3. $P_1, \ldots, P_n \vdash_{JD} \Gamma \models P \Rightarrow \forall I\, (\bigwedge_{i=1}^n ([\![P_i]\!]_I = t) \Rightarrow [\![\Gamma \models P]\!]_I = t)$

4 まとめ

本稿では，[4] で提案された，EGL85 プロトコルの性質を記号論的に解析するための形式体系に対し，可能世界モデルに基づく意味論を与え，その意味論における推論規則の健全性を示した．

今後の課題は，本稿で提案した意味論における完全性の証明，および確率的多項式時間チューリング機械による計算論的な意味付けとの比較である．

参考文献

[1] Bhery, A., Hagihara, S., Yonezaki, N.: A Formal System for Analysis of Cryptographic Encryption and Their Security Properties. ISSS 2003, LNCS, vol. 3233, pp. 87–112. Springer (2004)

[2] Even, S., Goldreich, O., Lempel, A.: A Randomized Protocol for Signing Contracts. Communications of the ACM, vol. 28, no. 6, pp. 637–647 (1985)

[3] 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 回大会論文集 (2007)

[4] 小黒博昭，萩原茂樹，米崎直樹：記号論的暗号解析を用いた Oblivious Transfer プロトコルの解析，電子情報通信学会論文誌 Vol.J92-D(5), pp. 596–607 (2009)