日本ソフトウェア科学会第 27 回大会 (2010 年度) 講演論文集

紛失通信プロトコルを解析する形式体系の意味論

小黒 博昭　萩原 茂樹　米崎 直樹

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．しかしながら，従来の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，従来の形式体系に対し，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す．

1 はじめに

暗号および暗号プロトコルの安全性を記号論的に解析する研究は，Dolev-Yao [7] に始まり，BAN 論理 [3]，等式書き換え [10]，プロセス代数 CSP [11][17][18]，定理証明 [14]，確率 Hoare 論理 [5]，確率プロセス計算 [2]，タスク構造を持つ確率 I/O オートマトン (task-PIOA) [4]，Protocol Composition Logic (PCL) [6]，知識の論理 [12] などの様々なアプローチにより，多くの研究がなされてきた．

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 [9]．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 [8] 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 [13]．しかしながら，[13] 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，[13] 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．

本稿の以降の構成は以下の通りである．2 節で OT プロトコルを説明する．3 節で OT の性質を解析するための形式体系の構文を示し，4 節で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．5 節でまとめと今後の課題を述べる．

2 Oblivious Transfer (紛失通信)

本節では，OT の一種である 1-out-of-2 OT が達成すべき二つの基本性質，1-out-of-2 OT の実現例である EGL85 プロトコル，および [13] で独自に定義

Semantics of a Formal System for the Analysis of an Oblivious Transfer Protocol.

Hiroaki Oguro, 東京工業大学大学院情報理工学研究科計算工学専攻 / (株)NTT データ 技術開発本部 IT アーキテクチャ＆セキュリティ技術センタ, Dept. of Computer Science, Graduate School of Information Science and Engineering, Tokyo Institute of Technology / IT Architecture & Security Center, Research and Development Headquarters, NTT DATA Corporation.

Shigeki Hagihara, Naoki Yonezaki, 東京工業大学大学院情報理工学研究科計算工学専攻, Dept. of Computer Science, Graduate School of Information Science and Engineering, Tokyo Institute of Technology.

された追加性質を説明する．

2.1 OT_2^1 の基本性質

OT とは，送信者が受信者へメッセージを送るとき，1/2 の確率で受信者へ伝わることが保証され，伝わったかどうかを送信者は知ることができないという性質を持つ通信である [15]．

OT が暗号プロトコルの一構成要素として実際に利用される際は，1-out-of-2 OT (OT_2^1) の形態で利用されることが多い．OT_2^1 の安全性を議論するとき，送信者および受信者は互いに相手に対する攻撃者としてモデル化される．ここで，本稿で想定する攻撃者は受信者および送信者のみとし，通信路上の盗聴者による攻撃は考察の対象外とする．攻撃者は，その振る舞いにより以下のようにモデル化される．

- **Honest**: プロトコルに従った動作しかしない．
- **Semi-honest**: 攻撃者は通信相手に対してはプロトコルに従って動作し，それにより得た情報を基に解析を行う．
- **Dishonest**: 送信するメッセージの順序および構成はプロトコルに従うが，メッセージの生成時に課せられた条件に違反する．

送信者および受信者のプライバシの観点から，OT_2^1 が達成すべき基本性質は以下の二つである [8]．

- **基本性質 1 (受信排他性；送信者のプライバシ)**
  送信者が Honest，受信者が Semi-honest であるとき，受信者は，送信者が送信しようとする二つのメッセージ†1のどちらか一方の内容しか認識することができない．
- **基本性質 2 (送達確認不能性；受信者のプライバシ)**
  送信者が Semi-honest，受信者が Honest であるとき，送信者は，受信者が二つのメッセージのどちらを認識できたのか分からない．

†1 [13] では二つのメッセージが異なることを前提として基本性質 1 が定義されたが，本稿ではこの前提を取り除く立場をとる．

2.2 EGL85 プロトコル

Even, Goldreich, Lempel は，落とし戸付き一方向性置換 (One-Way Trapdoor Permutation) を直接的に公開鍵暗号として利用する公開鍵暗号系を利用して，OT_2^1 プロトコルの実現例 (EGL85 プロトコル；以降，単に EGL85 と呼ぶ) を示した [8]．EGL85 を図 1 に示す． ここで，pk, sk はそれぞれ送信者の公開鍵および私有鍵を表す．$\boldsymbol{Z}_n = \{0, 1, \ldots, n-1\}$ はメッセージ空間を表す．置換の性質が反映されるため，暗号化関数 $E_{pk} : \boldsymbol{Z}_n \to \boldsymbol{Z}_n$ および復号関数 $D_{sk} : \boldsymbol{Z}_n \to \boldsymbol{Z}_n$ に関して以下が成り立つ．

$\forall x \in \boldsymbol{Z}_n \ (D_{sk}(E_{pk}(x)) = E_{pk}(D_{sk}(x)) = x)$.

$x \leftarrow S$ は確率空間 S から要素を一様な確率でランダムに選択し x へ割り当てることを表す．$\oplus$ は 2 を法とする加算を表す．$\boxplus$ および $\boxminus$ は以下の 3 条件を満足する写像 $\boldsymbol{Z}_n \times \boldsymbol{Z}_n \mapsto \boldsymbol{Z}_n$ である．

1. $\forall x \in \boldsymbol{Z}_n$ について，写像 $y \mapsto x \boxplus y$ が $\boldsymbol{Z}_n$ 上の置換となる．
2. $\forall y \in \boldsymbol{Z}_n$ について，写像 $x \mapsto x \boxplus y$ が $\boldsymbol{Z}_n$ 上の置換となる．
3. $\forall x \forall y \in \boldsymbol{Z}_n$ について $(x \boxplus y) \boxminus y = x$.

公開鍵暗号として教科書的 RSA 暗号 [16] を利用する場合，$\boxplus$ および $\boxminus$ として，その RSA 暗号系のモジュラス n を法とする加算および減算を採用することができる．EGL85 は以下のように実行される．

Protocol $\mathrm{OT}_2^1(S, R, M_0, M_1)$

Step 1: 送信者 S はメッセージ $M_0, M_1 \in \boldsymbol{Z}_n$，公開鍵 pk，私有鍵 sk，乱数 $m_0, m_1 \leftarrow \boldsymbol{Z}_n$ $(m_0 \neq m_1)$ および乱数 $s \leftarrow \{0,1\}$ を生成し，pk, m_0 および m_1 を受信者 R へ送信する．

Step 2: R は乱数 $r \leftarrow \{0,1\}$ および乱数 $x \leftarrow \boldsymbol{Z}_n$ を生成し，$q_r = E_{pk}(x) \boxplus m_r$ を S へ送信する．

Step 3: S は $y_{r,0} = D_{sk}(q_r \boxminus m_0)$ および $y_{r,1} = D_{sk}(q_r \boxminus m_1)$ を求め，$c_{r,0} = M_0 \boxplus y_{r,s}$, $c_{r,1} = M_1 \boxplus y_{r,s\oplus 1}$ および s を R へ送信する．

Step 4: R は $M_{r\oplus s} = c_{r,r\oplus s} \boxminus x$ を計算する．$(r,s) = (0,0)\, or\, (1,1)$ のときは M_0 が得られる．$(r,s) = (0,1)\, or\, (1,0)$ のときは M_1 が得られる．

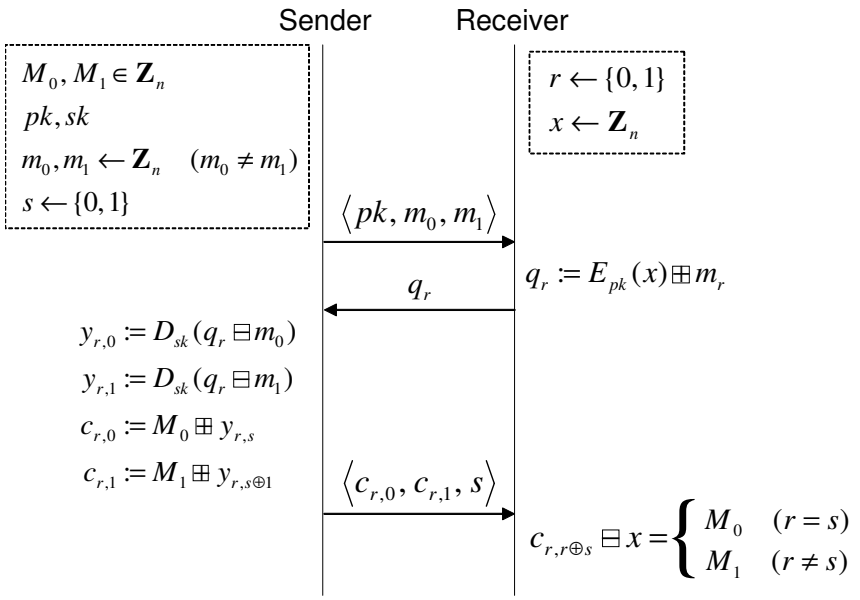

図 1 Even らによる 1-out-of-2 Oblivious Transfer の実現例 [8]

2.3 OT_2^1 が満足すべき追加性質

本節では，OT_2^1 を実現しようとするプロトコルが実際のアプリケーションに導入される際に，OT_2^1 の基本性質に加えて満足すべき追加性質として，[13] で定義された追加性質の一つを説明する．

今，OT_2^1 の機能を直接的に利用するサービスの要件として，送信者は受信者にとって価値のある二つの異なるデータを準備する義務がある場合を考える．もし，受信者が OT_2^1 を一回のみ実行可能という制約がある場合，Dishonest な送信者は，受信者にとって価値のあるデータを一つしか保持していなくても，$M_0 = M_1$ として OT_2^1 を実行することにより，受信者にその事実を悟られずにサービスを提供しようとする可能性がある．そのような状況を考慮して導入された追加性質は以下である．

- **追加性質 (獲得メッセージと非獲得メッセージの同一性の検出) [13]**
  送信者が Dishonest，受信者が Honest であるとき，受信者は，送信者が送信しようとする二つのメッセージが同じであること (すなわち，$M_0 = M_1$)，または異なること (すなわち，$M_0 \neq M_1$) を認識できる．

3 構文

本節では，公開鍵暗号として教科書的 RSA 暗号を利用する EGL85 を解析するための形式体系の構文を定義する．

3.1 メッセージ

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

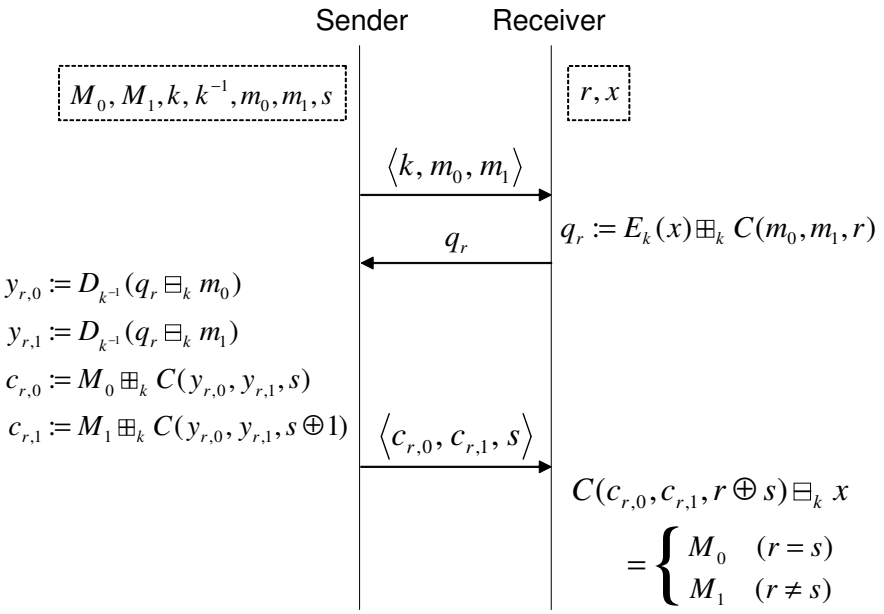

図 2　記号論的な解析のために書き直した EGL85

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．

本稿の以降では，適宜 $(T_1 \boxplus_k (\boxminus_k T_2))$ を $(T_1 \boxminus_k T_2)$ と略記し，公開鍵 k により定まる有限体上で減算した結果を表すメッセージとみなす．

図 1 に示した EGL85 を記号論的に解析するため，定義 1 の構文を用いて図 1 を書き直したプロトコルを図 2 に示す．

3.2　式

メッセージの値に関する等価関係，非等価関係，メッセージの集合からメッセージを新たに構成できる関係，およびメッセージの集合からメッセージの値に関する等価関係および非等価関係の知識が得られる関係を表す式を定義する．

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．

直観的には，式の意味は以下の通りである．関係情報 $T_1 = T_2$ は T_1 と T_2 の値が等しいことを表す．関係情報 $T_1 \neq T_2$ は T_1 と T_2 の値が異なることを表す．メッセージ認識文 $\Gamma \models T$ は，「Γ の要素であるすべてのメッセージの構成およびその値が分かっていて，これらのメッセージから T を生成でき，T の部

分メッセージの値が分かっているかどうかに関係なく，T の構成およびその値が分かる」ということを表す．判定文 $\Gamma \models P$ は,「Γ を知る者は P の真偽を認識できる」ということを表す．

3.3 代数法則

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以下のように定義する．ここで，メッセージを表すメタ変数を T, T_1, T_2, ... , T', T'_1, T'_2, ... , T'', T''_1, T''_2, ... で表す．特に，ビットを表すメッセージのメタ変数を B, B_1, B_2, ... で表し，乱数を表すメッセージのメタ変数を X_1, X_2, ... で表す．$T[T_1,\ldots,T_n/T'_1,\ldots,T'_n]$ は，T の中の $T'_1,\ldots,T'_n$ のすべての出現へ $T_1,\ldots,T_n$ をそれぞれ同時代入したものを表す．等号 *(=)* は反射律 $T = T$，対称律 $T_1 = T_2 \Rightarrow T_2 = T_1$，および推移律 $T_1 = T_2, T_2 = T_3 \Rightarrow T_1 = T_3$ を満足する同値関係である．

(A1) $((B_1 \oplus B_2) \oplus B_3) = (B_1 \oplus (B_2 \oplus B_3))$

(A2) $(B \oplus \mathtt{0}) = B$

(A3) $(B \oplus B) = \mathtt{0}$

(A4) $(B_1 \oplus B_2) = (B_2 \oplus B_1)$

(A5) $(B \oplus \mathtt{1}) \neq B$

(A6) $X_1 \neq X_2$ *(ただし，X_1 と X_2 は異なる記号)*

(A7) $C(X_1, X_2, \mathtt{0}) = X_1$

(A8) $C(X_1, X_2, \mathtt{1}) = X_2$

(A9) $C(X_1, X_2, B_1) = C(X_1, X_2, B_2) \wedge X_1 \neq X_2 \rightarrow B_1 = B_2$

(A10) $D_{k^{-1}}(E_k(T)) = T$

(A11) $E_k(D_{k^{-1}}(T)) = T$

(A12) $((T_1 \boxplus_k T_2) \boxplus_k T_3) = (T_1 \boxplus_k (T_2 \boxplus_k T_3))$

(A13) $(T \boxplus_k \mathtt{0}) = T$

(A14) $(T \boxplus_k (\boxminus_k T)) = \mathtt{0}$

(A15) $(T_1 \boxplus_k T_2) = (T_2 \boxplus_k T_1)$

(A16) $\langle T_1, T_2\rangle = \langle T_3, T_4\rangle \Rightarrow T_1 = T_3 \wedge T_2 = T_4$

(A17) $T_1 = T'_1, \ldots, T_n = T'_n \rightarrow T[T_1,\ldots,T_n/T''_1,\ldots,T''_n] = T[T'_1,\ldots,T'_n/T''_1,\ldots,T''_n]$

代数法則 (A1) および (A12) より，構成子 $\oplus$ および $\boxplus_k$ の結合法則がそれぞれ成立するため，本稿の以降では，$(B_1 \oplus B_2)$ および $(T_1 \boxplus_k T_2)$ のそれぞれの括弧を適宜省略する．

以上の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．

3.4 メッセージ認識規則

メッセージ認識文 $\Gamma \models T$ が導出される推論規則を定義する．

定義 4 (メッセージ認識規則) 式 $\Gamma \models T$ を以下の推論規則を満足する最小の関係と定義する．

(B1) $\dfrac{}{\Gamma \models \mathtt{0}}$

(B2) $\dfrac{}{\Gamma \models \mathtt{1}}$

(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 $X_1 \neq X_2$)*

(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)*

ここで，規則 *(B6)* の $\neq$ は記号が異なることを表す．

直観的には，規則 (B14) は，「メッセージ T_1 を保持し，その構成および値が分かっていて，かつ代数法則のみから $T_1 = T_2$ が導出されるとき，メッセージ T_2 を保持でき，その構成および値を認識できる」ということを意味する．規則 (B15) は，「メッセージ T_1, T_2 を保持し，それらの構成および値が分かっていて，かつ T_1 を部分メッセージとして含むメッセージ T を保持し，T の構成および値も分かっていて，かつ仮定および代数法則から $T_1 = T_2$ が導出されるとき，T における T_1 の出現部分を T_2 に置き換えたメッセージ $T[T_2/T_1]$ を保持でき，その構成および値を認識できる」ということを意味する．

3.5 JD-推論規則

判定文 $\Gamma \models P$ が導出される推論規則を定義する．

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) メッセージ T_1 および T_2 の値を分かっているかどうかに関係なく，仮定なしで代数法則のみから $T_1 = T_2$ が導かれるとき，T_1 および T_2 の値が等しいことを認識できる．

$\dfrac{T_1 = T_2}{\Gamma \models T_1 = T_2}$ *(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) メッセージ T_1 および T_2 の値を分かっているかどうかに関係なく，仮定なしで代数法則のみから $T_1 \neq T_2$ が導かれるとき，T_1 および T_2 の値が異なることを認識できる．

$\dfrac{T_1 \neq T_2}{\Gamma \models T_1 \neq T_2}$ *(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)*

(C3) Γ を保持する者がメッセージ T_1 および T_2 の値が分かっていて，自身が認識していない任意の関係情報を仮定して，それらの仮定に代数法則を用いることにより等価関係 $T_1 = T_2$ が導かれるとき，それらの仮定の下では T_1 および T_2 の値が等しいことを認識できる．

$\dfrac{\Gamma \models T_1 \qquad \Gamma \models T_2 \qquad T_1 = T_2}{\Gamma \models T_1 = T_2}$ *(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) Γ を保持する者がメッセージ T_1 および T_2 の値が分かっていて，自身が認識していない任意の関係情報を仮定して，それらの仮定に代数法則を用いることにより非等価関係 $T_1 \neq T_2$ が導かれるとき，それらの仮定の下では T_1 および T_2 の値が異なることを認識できる．

$\dfrac{\Gamma \models T_1 \qquad \Gamma \models T_2 \qquad T_1 \neq T_2}{\Gamma \models T_1 \neq T_2}$ *(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) Γ を保持する者が，自身が認識していない任意の関係情報を仮定して，それらの仮定の下で判定文 $P_1, \ldots, P_n$ の真偽が分かっていて，$P_1, \ldots, P_n$ のみの仮定の下で代数法則および述語計算を用いて判定文 P が導出されるとき，それらの仮定の下では P の真偽を認識できる．

$$\dfrac{\begin{array}{c} P_1, \ldots, P_n \\ \vdots \\ \Gamma \models P_1 \ \cdots \ \Gamma \models P_n \qquad P \end{array}}{\Gamma \models P}$$

(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)

3.6 JD-導出

JD-推論規則を用いてメッセージ認識文 $\Gamma \models T$ または判定文 $\Gamma \models P$ を演繹できるか否かを表す記述を定義する．

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．

4 意味論

本節では，3 節で定義されたメッセージおよび式に

対し，可能世界モデルに基づく意味論を与える．

4.1 メッセージ代数

メッセージに意味を与える準備として，メッセージ代数を定義する．

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．

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

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

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

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

$pair$ 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．

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

4.2 メッセージの意味

$\mathcal{A}$ 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．

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

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．

4.3 式の意味

本節では，意味関数を拡張し，可能世界意味論により意味づけを行う．その準備として，メッセージと値の対の集合の閉包を定義する．

4.3.1 閉包

メッセージ T の値が d であることが分かっていることを基にし，そこから新たに計算可能なメッセージおよびその値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 をメッセージおよびその値を表すビット列の対 (T, d) 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. $\{(\mathsf{0}, \mathsf{0}), (\mathsf{1}, \mathsf{1})\} \subset U$
2. $Y \subseteq U$

3. $(B_1, b_1), (B_2, b_2) \in U$
$\Rightarrow ((B_1 \oplus B_2), xor(b_1, b_2)) \in U$

4. $(X_1, d_1), (X_2, d_2), (B, b) \in U$
$\Rightarrow (C(X_1, X_2, B), choose(d_1, d_2, b)) \in U$

5. $(X_1, d_1), (X_2, d_2), (C(X_1, X_2, B), d_3) \in U$
$\Rightarrow (B, \texttt{if}\ d_1 = d_3\ \texttt{then}\ 0\ \texttt{else}\ 1) \in U$

6. $(k, pk), (T, d) \in U \Rightarrow (E_k(T), enc(pk, d)) \in U$

7. $(k^{-1}, sk), (T, d) \in U$
$\Rightarrow (D_{k^{-1}}(T), dec(sk, d)) \in U$

8. $(k, pk), (T_1, d_1), (T_2, d_2) \in U$
$\Rightarrow ((T_1 \boxplus_k T_2), add(pk, d_1, d_2)) \in U$

9. $(k, pk), (T, d) \in U \Rightarrow ((\boxminus_k T), inv(pk, d)) \in U$

10. $(T_1, d_1), (T_2, d_2) \in U$
$\Rightarrow (\langle T_1, T_2 \rangle, pair(d_1, d_2)) \in U$

11. $(\langle T_1, T_2 \rangle, pair(d_1, d_2)) \in U$
$\Rightarrow (T_1, d_1), (T_2, d_2) \in U$

12. $\vdash T_1 = T_2$ のとき，$(T_1, d) \in U \Rightarrow (T_2, d) \in U$

13. $(T_1, d), (T_2, d), (T[T_1], d') \in U$
$\Rightarrow (T[T_2/T_1], d') \in U$

4.3.2 式の意味

$\Gamma = \{T_1, T_2, \ldots, T_n\}$ をメッセージの集合とする．このとき，式の真偽値 (t または f) を以下のように定義する．

- $[\![T_1 = T_2]\!]_I = t \iff [\![T_1]\!]_I = [\![T_2]\!]_I$
  すなわち，$T_1 = T_2$ が解釈 I において真であるとは，T_1 の解釈 I によるビット列と T_2 の解釈 I によるビット列が等しいことである．
- $[\![T_1 \neq T_2]\!]_I = t \iff [\![T_1]\!]_I \neq [\![T_2]\!]_I$
  すなわち，$T_1 \neq T_2$ が解釈 I において真であるとは，T_1 の解釈 I によるビット列と T_2 の解釈 I によるビット列が異なることである．
- $[\![\Gamma \models T]\!]_I = t \iff (T, [\![T]\!]_I) \in Cl(\Gamma, I)$
  ここで，$Cl(\Gamma, I)$ は以下で定義される．
  $Cl(\Gamma, I) = cl(\{(T', [\![T']\!]_I) \mid T' \in \Gamma\})$
  すなわち，$\Gamma \models T$ が解釈 I において真であるとは，T の解釈 I によるビット列が，Γ の解釈 I による閉包の要素であることである．
- $[\![\Gamma \models P]\!]_I = t$
  $\iff \forall I'\ (I' \in W(Cl(\Gamma, I)) \Rightarrow [\![P]\!]_{I'} = t)$
  ここで，$W(X)$ は以下で定義される．
  $W(X) = \{I' \mid \forall (T, d) \in X\ ([\![T]\!]_{I'} = d)\}$
  すなわち，$\Gamma \models P$ が解釈 I において真であるとは，Γ の閉包のすべてのメッセージ T について T の解釈 I によるビット列と同じ解釈を持つようなすべての可能世界での解釈 I' において P が真となることである．

4.4 JD-推論規則の健全性

本節では，JD-推論規則の健全性を証明する．証明すべき式は以下となる．

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

[1. の証明]

代数法則 (A1) から (A17) が任意の解釈 I に対して真になることを示せば十分である．(A1) から (A5) は $\oplus$ が *xor* であるため明らかである．(A7) から (A9) は *choose* の定義より明らかである．(A10), (A11) は *enc*, *dec* が満足すべき制約の定義より明らかである．(A12) から (A15) は *add*, *inv* が満足すべき制約の定義より明らかである．(A16) は *pair* の定義より明らかである．(A17) は合同性により明らかである．以上より題意が示される． ■

[2. の証明]

メッセージ認識規則 (B1) から (B15) が閉包の定義にそれぞれ対応することを示せば十分である．(B1), (B2) は閉包の定義の項番 1 に，(B3) は 2 に，(B4) は 3 に，(B5) は 4 に，(B6) は 5 に，(B7) は 6 に，(B8) は 7 に，(B9) は 8 に，(B10) は 9 に，(B11) は 10 に，(B12), (B13) は 11 に，(B14) は 12 に，(B15) は 13 に，それぞれ対応する．以上より題意が示される． ■

[3. の証明]

証明図の構成に関する帰納法で示す．

1. JD-推論規則 (C1)
   $\vdash T_1 = T_2$ より，$\forall I\,([\![T_1]\!]_I = [\![T_2]\!]_I)$ を満たす．

従って，$I' \in W(Cl(\Gamma, I))$ を満たす任意の I' に対しても $[\![T_1]\!]_{I'} = [\![T_2]\!]_{I'}$ を満たす．従って，$[\![\Gamma \models T_1 = T_2]\!]_I = t$ である．

2. JD-推論規則 (C2)

JD-推論規則 (C1) と同様に証明される．

3. JD-推論規則 (C3)

前提 $P_1, \ldots, P_l \vdash_{JD} \Gamma \models T_1$, $Q_1, \ldots, Q_m \vdash_{JD} \Gamma \models T_2$ より，$\forall I\,([\![P_1]\!]_I = t \wedge \cdots \wedge [\![P_l]\!]_I = t \Rightarrow [\![\Gamma \models T_1]\!]_I = t)$, $\forall I\,([\![Q_1]\!]_I = t \wedge \cdots \wedge [\![Q_m]\!]_I = t \Rightarrow [\![\Gamma \models T_2]\!]_I = t) \cdots (1)$ である．さらに，前提 $R_1, \ldots, R_n \vdash T_1 = T_2$ より，$\forall I\ ([\![R_1]\!]_I = t \wedge \cdots \wedge [\![R_n]\!]_I = t \Rightarrow [\![T_1]\!]_I = [\![T_2]\!]_I) \cdots (2)$ を満たす．このとき，$\forall I\ ([\![P_1]\!]_I = t \wedge \cdots \wedge [\![P_l]\!]_I = t \wedge [\![Q_1]\!]_I = t \wedge \cdots \wedge [\![Q_m]\!]_I = t \wedge [\![R_1]\!]_I = t \wedge \cdots \wedge [\![R_n]\!]_I = t \Rightarrow [\![\Gamma \models T_1 = T_2]\!]_I = t)$ を示す．今，I が $[\![P_1]\!]_I = t \wedge \cdots \wedge [\![P_l]\!]_I = t \wedge [\![Q_1]\!]_I = t \wedge \cdots \wedge [\![Q_m]\!]_I = t \wedge [\![R_1]\!]_I = t \wedge \cdots \wedge [\![R_n]\!]_I = t$ を満たすとし，I' が $I' \in W(Cl(\Gamma, I))$ を満たすとする．このとき (1) より，$[\![T_1]\!]_I = [\![T_1]\!]_{I'}$, $[\![T_2]\!]_I = [\![T_2]\!]_{I'}$ を満たす．一方，(2) より，$[\![T_1]\!]_I = [\![T_2]\!]_I$ となる．従って，題意が示される．

4. JD-推論規則 (C4)

JD-推論規則 (C3) と同様に証明される．

5. JD-推論規則 (C5)

$\forall i = \{1, \ldots, n\}(Q^i_1, \ldots, Q^i_{m_i} \vdash \Gamma \models P_i)$ より，$\forall I\,([\![Q^i_1]\!]_I = t \wedge \cdots \wedge [\![Q^i_{m_i}]\!]_I = t \Rightarrow \forall I'\,(I' \in W(cl(\Gamma, I)) \Rightarrow [\![P_i]\!]_{I'} = t) \cdots (1)$ を満たす．さらに，前提 $P_1, \ldots, P_n \vdash P$ より，$\forall I\,([\![P_1]\!]_I = t \wedge \cdots \wedge [\![P_n]\!]_I = t \Rightarrow [\![P]\!]_I = t) \cdots (2)$ を満たす．このとき，$\forall I\,([\![Q^1_1]\!]_I = t \wedge \cdots \wedge [\![Q^1_{m_1}]\!]_I = t \wedge \cdots \wedge [\![Q^n_1]\!]_I = t \wedge \cdots \wedge [\![Q^n_{m_n}]\!]_I = t \wedge [\![P_1]\!]_I = t \wedge \cdots \wedge [\![P_n]\!]_I = t \Rightarrow \forall I'\,(I' \in W(Cl(\Gamma, I)) \Rightarrow [\![P]\!]_{I'} = t))$ を示す．今，I が $[\![Q^1_1]\!]_I = t \wedge \cdots \wedge [\![Q^1_{m_1}]\!]_I = t \wedge \cdots \wedge [\![Q^n_1]\!]_I = t \wedge \cdots \wedge [\![Q^n_{m_n}]\!]_I = t \wedge [\![P_1]\!]_I = t \wedge \cdots \wedge [\![P_n]\!]_I = t$ を満たすとし，I' が $I' \in W(Cl(\Gamma, I))$ を満たすとする．このとき (1) より $\forall i \in \{1, \ldots, n\}\,([\![P_i]\!]_{I'} = t)$ を満たす．これと (2) より，$[\![P]\!]_{I'} = t$ となり，題意が示される． ■

4.5 本体系による記述および証明

本稿で提案した意味論によれば，EGL85 が 2 節で示した追加性質を満足することを保証するためには，Γ_R をプロトコル終了後に受信者が保持するメッセージの集合として，以下を示せば十分となる．

$$M_0 = M_1 \vdash_{JD} \Gamma_R \models M_0 = M_1$$
$$M_0 \neq M_1 \vdash_{JD} \Gamma_R \models M_0 \neq M_1$$

なぜならば，JD-推論規則は意味論に対して健全であるためである．

また，EGL85 が追加性質を満足することの証明図は [13] に与えられている．

5 まとめ

本稿では，[13] 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．

今後の課題は以下の通りである．

- 本稿で提案した意味論における完全性の証明
- 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，およびその意味論と本稿で提案した意味論との比較

参 考 文 献

[1] Bhery, A., Hagihara, S., Yonezaki, N.: A Formal System for Analysis of Cryptographic Encryption and Their Security Properties. In: Software Security — Theories and Systems: Second Mext-NSF-JSPS International Symposium, ISSS 2003, LNCS, vol. 3233, pp. 87–112. Springer, Berlin / Heidelberg (2004)

[2] Blanchet, B., Pointcheval, D.: Automated Security Proofs with Sequences of Games. In: Advances in Cryptology - CRYPTO 2006, LNCS, vol. 4117, pp. 537-554 (2006)

[3] Burrows, M., Abadi, M., Needham, R.: A Logic of Authentication. ACM Trans. on Computer Systems, vol. 8, no. 1, pp. 18–36 (1990)

[4] Canetti, R., Cheung, L., Kaynar, D., Liskov, M., Lynch, N., Pereira, O., Segala, R.: Using Task-Structured Probabilistic I/O Automata to Analyze an Oblivious Transfer Protocol. MIT-CSAIL-TR-2007-011 (2007)

[5] Corin, R., den Hartog, J.: A Probabilistic Hoare-style Logic for Game-Based Cryptographic Proofs. In: Part II of the proceedings of the 33rd International Colloquium on Automata, Languages

and Programming, ICALP 2006, LNCS, vol. 4052, pp. 252–263 (2006)
[6] Datta, A., Derek, A., Mitchell, J. C., Roy, A.: Protocol Composition Logic (PCL). In: Electronic Notes in Theoretical Computer Science 172, pp. 311–358 (2007)
[7] Dolev, D., Yao, C.: On the Security of Public Key Protocols. IEEE Trans. and Information Theory, vol. IT-29, no. 2, pp. 198–208 (1983)
[8] Even, S., Goldreich, O., Lempel, A.: A Randomized Protocol for Signing Contracts. Communications of the ACM, vol. 28, no. 6, pp. 637–647 (1985)
[9] 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)
[10] Kemmerer, R., Meadows, C., Millen, J.: Three Systems for Cryptographic Protocol Analysis. J. Cryptology, vol. 7, no. 2, pp. 79–130 (1994)
[11] Lowe, G.: Breaking and Fixing the Needham-Schroeder Public-Key Protocol Using FDR. In: Proceedings of the Second International Workshop on Tools and Algorithms for Construction and Analysis of Systems, LNCS, vol. 1055, pp. 147–166. Springer-Verlag, London (1996)
[12] van der Meyden, R., Wilke, T.: Preservation of Epistemic Properties in Security Protocol Implementations. In: Proceedings of the 11th Conference on Theoretical Aspects of Rationality and Knowledge, pp. 212–221 (2007)
[13] 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)
[14] Paulson, L. C.: The Inductive Approach to Verifying Cryptographic Protocols. J. Computer Security, vol. 6, no. 1–2, pp. 85–128 (1998)
[15] Rabin, M. O.: How to Exchange Secrets by Oblivious Transfer. Technical report, TR-81, Aiken Computation Laboratory, Harvard Univ. (1981)
[16] Rivest, R. L., Shamir, A., Adleman, L. M.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, vol. 21, no. 2, pp. 120–126 (1978)
[17] Ryan, P., Schneider, S., Goldsmith, M., Lowe, G., Roscoe, B.: The Modelling and Analysis of Security Protocols: the CSP Approach. Addison-Wesley (2001)
[18] Schneider, S.: Security Properties and CSP. In: Proceedings of the 1996 IEEE Symposium on Security and Privacy, pp. 174–187. IEEE Computer Society. Washington, DC (1996)