1ZA-2

ID ベース暗号と ID ベース署名を用いた配達証明付きデータ送信方式

西浦 翔平† 白石 善明† 土井 洋†† 毛利 公美‡ 福田 洋治‡‡ 岩田 彰†

名古屋工業大学† 情報セキュリティ大学院大学†† 岐阜大学‡ 愛知教育大学‡‡

1. はじめに

通信事実を確かめることができないネットワークでは否認が容易である．否認を防ぐには，送ったデータが相手に届けられたことを証明すればよい．その手段の一つに受領書によって証明する方法がある．受領書による配達証明ではデータと受領書を公平に交換しなければならない．

これまでに公開鍵基盤(PKI)を用いた交換方式が提案されているが，PKI では送信者は通信相手の公開鍵証明書を取得し管理しなければならず，通信相手が増えると多くの証明書を扱うことになる．低スペックな送信端末を利用する場合，証明書によるデータの増加は望ましくない．そこで本稿では，任意の ID 情報を公開鍵とすることができる ID ベース暗号(Identity-Based Encryption: IBE)と ID ベース署名(Identity-Based Signature: IBS)を用いて，送信端末で証明書不要な Optimistic 型の配達証明付きデータ送信方式を提案する．

2. 公平な交換

公平な交換(Fair Exchange)とは，「互いに目的のものを手に入れるか，どちらも手に入らない」ことを保証した交換[1]であり，次の二種類に大別される．一つは交換する情報を 1 ビット単位に分割して徐々に交換することにより，たとえプロトコルが打ち切られても両者の持つ情報の差が高々 1 ビット分に過ぎないようにする段階的秘密交換と呼ばれる方式[2]で，もう一つは中立的な信頼機関(Trusted Third Party: TTP)を仲介者としてデータを交換する方式である．また後者における TTP の利用方法については二種類のタイプがあり，必ず TTP が通信に介入するタイプを On-line 型[3]，どちらかが不公平な状況になった場合に TTP を利用して解決するタイプを Optimistic 型[4]という．

TTP の仮定を必要とするが，公平性や効率性の観点から TTP を利用する交換がより実用的である．また On-line 型に比べて Optimistic 型では通信のボトルネックや TTP 依存が軽減できる．これらの理由から提案方式では TTP を利用した Optimistic 型の方式に注目する．

3. 配達証明付きデータ送信のための要件

配達証明付きデータ送信のセキュリティ要件は配達証明付き電子メールに求められる性質[5]とする．以下にその要件を示す．

公平性：利用者は自身だけが目的のものを得るようにプロトコルを中断または不正することができない．

秘匿性：仲介人を含む第三者がデータの内容を読むことはできない．

非拒否性：前に行った行動を取り消すことができない．

完全性：データの内容が不正に書き換えられていない．

認証：通信相手が目的の相手であるとわかる．

4. 提案方式

4.1 提案方式に用いる IBE と IBS

IBE は Boneh,Franklin の方式[6]，IBS は Cha,Cheon の方式[7]を用いる．BF 方式は，[8]で標準化されており，ランダムオラクルモデルにおいて CBDH 仮定のもとで IND-ID-CCA 安全が証明されている．CC 方式は，[9]で標準化されており，ランダムオラクルモデルにおいて CDH 仮定のもとで EUF-ID-CMA 安全が証明されている．

4.2 エンティティ

“送信者”，“受信者”，“仲介者”，“鍵発行機関”で構成される．

[送信者／受信者]

信頼される組織によって ID 情報が登録された利用者であり，秘密情報を漏えいしない．

[仲介者]

信頼される組織によって ID 情報が登録されており，利用者の依頼によって利用者と通信を行う．プロトコルを遵守し，秘密情報を漏えいせず，利用者と結託しない．

[鍵発行機関]

BF 方式，CC 方式のパラメータを公開しており，利用者に依頼され ID 情報に対する秘密鍵を発行する．プロトコルを遵守し，秘密情報を漏えいせず，いかなる不正も行わない．

利用者と仲介者，鍵発行機関の通信は信頼できる通信路（情報の漏えい，欠損，改ざんがない）を用いて行うものとする．

4.3 アルゴリズム

提案方式を構成するアルゴリズムを示す．

PKG.Setup：

セキュリティパラメータ1^kを入力とし，次のように動作する
1.(G, G_T, e, q, P)を生成する
2.$s \xleftarrow{U} Z_q^*$を生成し，$P_{pub} := sP$を求める
3.ハッシュ関数として，$H_1 : \{0,1\}^* \to G, H_2 : G_T \to \{0,1\}^n$,
$H_3 : \{0,1\}^n \times \{0,1\}^n \to Z_q^*, H_4 : \{0,1\}^n \to \{0,1\}^n, H_5 : \{0,1\}^* \to Z_q^*$
を定める
公開パラメータ$pp := (G, G_T, e, q, n, P, P_{pub}, H_1, H_2, H_3, H_4, H_5)$,
マスター秘密鍵$msk := s$を出力する

PKG.Ext：

送信者，受信者，仲介者のID情報ID_S, ID_R, ID_Tを入力とし，次のように動作する
1.$Q_{ID_S} := H_1(ID_S), Q_{ID_R} := H_1(ID_R), Q_{ID_T} := H_1(ID_T)$,を求める
2.$d_S := sQ_{ID_S}, d_R := sQ_{ID_R}, d_T := sQ_{ID_T}$を計算する
d_S, d_R, d_Tをそれぞれの秘密鍵として出力する

CKEnc：

メッセージM,セッション鍵$K \in \{0,1\}^k$を入力とし，
暗号文$Enc_K(M)$を出力する（共通鍵暗号）

R.Enc：

受信者のID情報ID_R,セッション鍵Kを入力とし，
次のように動作する
1.$t_1 \xleftarrow{U} \{0,1\}^n$を選ぶ
2.$r_1 := H_3(t_1, K)$を計算する
3.$C_1 := (c_0, c_1, c_2) = (r_1 P, t_1 \oplus H_2(e(Q_{ID_R}, P_{pub})^{r_1}), K \oplus H_4(t_1))$
を暗号化されたセッション鍵として出力する

T.Enc：

送信者，受信者，仲介者のID情報ID_S, ID_R, ID_T,暗号化されたセッション鍵C_1を入力とし,次のように動作する
1.$t_2 \xleftarrow{U} \{0,1\}^n$を選ぶ
2.$r_2 := H_3(t_2, (ID_S \| ID_R \| C_1))$を計算する
3.$C_2 := (c_3, c_4, c_5)$
$= (r_2 P, t_2 \oplus H_2(e(Q_{ID_T}, P_{pub})^{r_2}), (ID_S \| ID_R \| C_1) \oplus H_4(t_2))$
を二重に暗号化されたセッション鍵として出力する

S.Sig：

送信者，受信者のID情報ID_S, ID_R,暗号文$Enc_K(M)$,二重に暗号化されたセッション鍵C_2,送信者の秘密鍵d_Sを入力とし，次のように動作する
1.$u_1 \xleftarrow{U} \{0,1\}^n$を選ぶ
2.$U_1 := u_1 Q_{ID_S}$を計算する
3.$h_1 := H_5((ID_R \| Enc_K(M) \| C_2), U_1)$を計算する
4.$\sigma_S := (U_1, V_1) = (u_1 Q_{ID_S}, (u_1 + h_1) d_S)$を送信者の署名として出力する

S.Ver：

送信者のID情報ID_S,暗号文$Enc_K(M)$,二重に暗号化されたセッション鍵C_2,送信者の署名σ_Sを入力とし，
$e(P_{pub}, U_1 + h_1 Q_{ID_S}) = e(P, V_1)$ならば1を，そうでなければ0を出力する

R.Sig：

受信者のID情報ID_R,送信者の署名σ_S,受信者の秘密鍵d_Rを入力とし，
1.$u_2 \xleftarrow{U} \{0,1\}^n$を選ぶ
2.$U_2 := u_2 Q_{ID_R}$を計算する
3.$h_2 := H_5(\sigma_S, U_2)$を計算する
4.$\sigma_R := (U_2, V_2) = (u_2 Q_{ID_R}, (u_2 + h_2) d_R)$を受信者の署名として出力する

An ID-Based Certified Data Sending Scheme

†Shohei NISHIURA and Yoshiaki SHIRAISHI and Akira IWATA・Nagoya Institute of Technology

††Hiroshi DOI・Institute of Information Security

‡Masami MOHRI・Gifu University

‡‡Youji FUKUTA・Aichi University of Education

R.Ver：

受信者のID情報$\mathrm{ID_R}$,受信者の署名σ_Rを入力とし，
$e(P_{pub}, U_2 + h_2 Q_{\mathrm{ID_R}}) \equiv e(P, V_2)$ならば1を，そうでなければ0を出力する

R.Dec：

暗号化されたセッション鍵C_1,受信者の秘密鍵d_Rを入力とし，次のように動作する
1.$t_1' := H_2(e(d_\mathrm{R}, c_0)) \oplus c_1$
2.$K' := H_4(t_1') \oplus c_2$
3.$r_1' := H_3(t_1', K')$
4.$r_1'P = c_0$であればK'を出力し，そうでなければ⊥を出力する

CKDec：

K',暗号文$Enc_K(M)$を入力とし，メッセージMを出力する（共通鍵暗号）

T.Dec：

二重に暗号化されたセッション鍵C_2,仲介者の秘密鍵d_Tを入力とし，
1.$t_2' := H_2(e(d_\mathrm{T}, c_3)) \oplus c_4$
2.$(\mathrm{ID_S} \| \mathrm{ID_R} \| C_1)' := H_4(t_2') \oplus c_5$
3.$r_2' := H_3(t_2', (\mathrm{ID_S} \| \mathrm{ID_R} \| C_1)')$
4.$r_2'P = c_3$であれば$\mathrm{ID_S'}, \mathrm{ID_R'}, C_1'$を出力し,そうでなければ⊥を出力する

提案方式の流れを図1，2に示す.

5. 安全性

3.で示した要件について考える.

公平性：公平性が崩れるということは，受信者だけが目的のものを得る，または送信者だけが目的のものを得るということである．受信者の目的のものはメッセージであり，送信者の目的のものは受領書である．ただし，メッセージMは共通鍵で暗号化されているため，共通鍵暗号が計算量的に安全であると仮定すると受信者の目的のものはセッション鍵Kとなる．公平性を崩す攻撃者は受信者または送信者であり，3つの攻撃モデルが考えられる．

・攻撃モデル1

受信者が二重に暗号化されたセッション鍵C_2から部分復号されたセッション鍵C_1を得る．つまり受信者による T.Enc に対しての攻撃である．

・攻撃モデル2

受信者が仲介者の検証に通るような送信者の署名σ_Sを偽造し，リカバリ時のプロトコルを行い，セッション鍵C_1を得る．この際，受信者は偽造した署名に対しての署名を仲介者へ送るため，送信者が手に入れる受領書は正規のものではない．これはつまり受信者による S.Sig に対しての攻撃である．

・攻撃モデル3

送信者が受信者の署名σ_Rを偽造し，受領書を得る．つまり送信者による R.Sig に対しての攻撃である．

攻撃モデル 1 については，敵 A（受信者）を T.Enc に対する IND-ID-CCA の敵とし，敵 B を BF 方式の IND-ID-CCA におけるシミュレータに対しての敵とすると，敵 A は仲介者の秘密鍵だけ得られない以外は，BF 方式の IND-ID-CCA におけるシミュレータから得られる情報をもつ敵 B と同等に考えることができる．よって BF 方式の安全性より，T.Enc において IND-ID-CCA を破る敵 A は存在しない．攻撃モデル 2 については，敵 A（受信者）を S.Sig に対する EUF-ID-CMA の敵とし，敵 B を CC 方式の EUF-ID-CMA におけるシミュレータに対しての敵とすると，敵 A は CC 方式におけるシミュレータから得られる情報をもつ敵 B と同等に考えることができる．よって CC 方式の安全性により，S.Sig において EUF-ID-CMA を破る敵 A は存在しない．攻撃モデル 3 については，攻撃モデル 2 と同様に CC 方式の安全性に帰着させることで，R.Sig が EUF-ID-CMA 安全であることを示すことができる．以上より，3 つの攻撃モデルに対しての安全性が示されたので，公平性は満たされる．

秘匿性：秘匿性が崩れるということは，仲介人を含む第三者がメッセージを得ることである．ただし，公平性と同様の仮定とすると，攻撃者の目標はメッセージではなくセッション鍵を得ることになる．ここでは 1 つの攻撃モデルが考えられる．

・攻撃モデル4

仲介者を含む第三者が部分復号されたセッション鍵C_2から

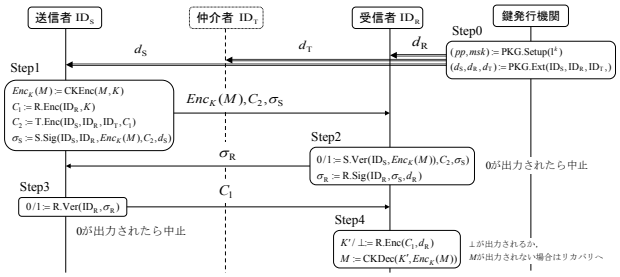

図1　提案方式の流れ（通常時）

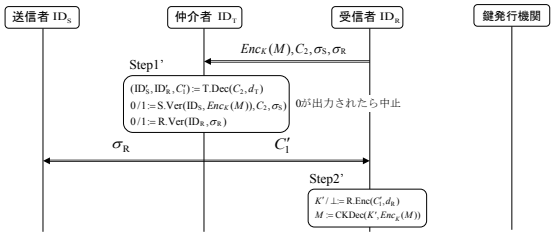

図2　提案方式の流れ（リカバリ時）

セッション鍵Kを得る．つまり仲介者を含む第三者による R.Enc に対する攻撃である．

攻撃モデル 4 は，攻撃モデル 1 と同様に BF 方式の安全性に帰着させることで，R.Enc が IND-ID-CCA 安全であることを示すことができる．攻撃モデル 4 に対しての安全性が示されたので，秘匿性は満たされる．

非拒否性：送信者の署名σ_Sは受信者の ID 情報，暗号文，暗号化されたセッション鍵に対しての署名であり，送信者は送信事実を否定できない．受信者の署名σ_Rは送信者の署名に対しての署名であり，受信者は受信事実を否定できない．

完全性：Step1 で暗号文に対して署名されているので，通信途中で不正な改ざんが起こったとしても署名σ_Sの検証により検知できる．

認証：送信者，受信者，仲介者は署名の検証により通信相手の認証ができる．

6. おわりに

本稿では，BF 方式と CC 方式を用いた送信端末で公開鍵証明書が不要な Optimistic 型の配達証明付きデータ送信方式を提案した．セキュリティ要件について，BF 方式，CC 方式の安全性に帰着させ満たすことを確認した．

参考文献

[1]M. K. Franklin, M. K. Reiter: Fair Exchange with a Semi-Trusted Third Prty, Proc. 4th ACM Conf. on Computer and Communication Security, April 1997.
[2]S. Even, O. Goldreich and A. Lempel: A Randomized Protocol for Signing Contracts, Communications of the ACM, Vol.28, No.6, pp. 637-647, 1985.
[3]J. Zhou, D. Gllmann: Observations on Non-repudiation, Proceedings of ASIACRYPT'96, LNCS 1163, pp.133-144, Springer-Verlag, 1997.
[4]N. Asokan, M. Schunter, M. Waidner: Optimistic Protocols for Fair Exchange, 4th ACM Conference on Computer and Communication Security, pp.6-17, 1997.
[5]今本健二，櫻井幸一：配達仲介人を利用した配達証明付き電子メールの改良，情報処理学会論文誌，Vol.44，No8, pp.2085-2092 2003.
[6]D. Boneh, M. Franklin: Identity-Based Encryption from the Weil Pairing, CRYPTO 2001, LNCS 2139, Springer Verlag, pp. 213-229, 2001.
[7]J. C. Cha, J. H. Cheon: An Identity-Based Signature from Gap Diffie-Hellman Groups, Proceedings of PKC 2002, LNCS 2567, Springer-Verlag, pp. 18-30, 2002.
[8]X. Boyen, L. Martin: Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems, Request for Comments: 5091, IETF, 2007.
[9]ISO/IEC 14888-3: Information technology-Security techniques-Digital Signatures with appendix-Part 3: Discrete logarithm based mechanisms, 2006.