2Z-6

Web ベースファイル送受信システムのための部分的に二重暗号化する ID ベース暗号方式

佐藤　誠[†]　毛利　公美[‡]　土井　洋[††]　白石　善明[†]　野口　亮司[‡‡]

†名古屋工業大学　‡岐阜大学　††情報セキュリティ大学院大学　‡‡（株）豊通システムズ

1. はじめに

企業や研究機関等で，内容を秘匿してファイルの送受信を行いたいというニーズがある．公開鍵基盤(PKI)を用いた秘匿通信では，受信者は自身が生成した公開鍵に対して，事前に信頼できる機関である認証局(CA)から公開鍵証明書の発行を受け，公開鍵を送信者に通知する必要がある．

受信者の公開情報をもとに暗号文を作成でき，公開鍵証明書が不要な ID ベース暗号(IBE)では，復号鍵発行サーバ(PKG)が任意の受信者宛の暗号文を復号できる．よってファイルを暗号化する機密ファイル送受信システムに IBE を利用する場合，PKG はファイルの内容を見ることができる．すでに我々は，次の要件を満たす IBE を用いた機密ファイル送受信システム[1]を提案している．(i)システム利用者が行う作業は最低限の作業のみである(ii)情報授受の当事者（送信者と受信者）のみがファイルの中身を知ることができる(iii)ソフトウェアのインストールの必要性をなくすため，Web ベースのシステムである(iv)送受信者がともにオンラインでなくても利用できる．

文献[1]の方式は，送受信者以外に PKG，平文の情報を含む暗号文成分（以降，メッセージ成分）の復号（部分復号）を担うメッセージ成分供託サーバ(MCD)，平文の情報を含まない暗号文成分（以降，乱数成分）の部分復号を担う乱数成分供託サーバ(RCD)の 3 つのサーバで構成される．送信者は 1 回目に受信者の公開情報で平文を暗号化し，2 回目に，1 回目の暗号化により生成された暗号文のうち，乱数成分を RCD の公開鍵を用いて，メッセージ成分を MCD の公開鍵を用いて暗号化することから二重暗号化 ID ベース方式(DEIBE)と呼んでいる．DEIBE を用いて機密ファイル送受信システムを構成する場合，PKG，MCD，RCD をそれぞれ別の 3 つの組織が運用する必要があり，導入が難しい．

本稿では，乱数成分を暗号化せず，メッセージ成分のみを二重暗号化する ID ベース暗号方式を提案する．乱数成分の二重暗号化処理をなくすことで，RCD が不要になる．そして，既存の暗号方式との比較を行い，提案方式を構成するメッセージ成分保管サーバ(MCD)と PKG のうち一方が攻撃者と結託した場合にも受動的な攻撃に対して安全であることを示す．

2. 準備

[双線形写像]　$\mathbb{G}_1, \mathbb{G}_2$を素数位数$q$の巡回群とする．双線形写像 $\hat{e}: \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ は任意の$P, Q \in \mathbb{G}_1$，$a, b \in \mathbb{Z}_q^*$に対して，以下の性質を満たす．

双線形性：$\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$.

非縮退性：$\hat{e}(P, Q) = 1$ ならば $P = 0$ または$Q = 0$.

計算可能性：$\hat{e}(P, Q)$を効率的に計算できる．

[$\mathbb{G}_1$上の CDH 問題]　$P \in \mathbb{G}_1$，$a, b \in \mathbb{Z}_q^*$に対して，$< P, aP, bP >$ からabPを求める問題のことである．$\mathbb{G}_1$上の CDH 問題が困難であるという仮定を$\mathbb{G}_1$上の CDH 仮定という．

3. 提案方式

提案方式は DEIBE と同様に，Dan Boneh，Matthew Fraklin らが提案した ID ベース暗号方式[2]（以降，BF 方式）をもとに構成する．送信者は BF 方式の BasicIdent による 1 回目の暗号化後，BF 方式に対して新たに追加した MCD の公開鍵を用いてメッセージ成分をさらに暗号化する．2 回目の暗号化のアルゴリズムは楕円 ElGamal 暗号をもとにしている．

3.1. モデル

提案方式を構成する主体を以下に示す．

[送信者]　受信者の公開情報である ID と MCD の公開鍵を用いて暗号文を作成する．公開通信路を用いて，乱数成分を受信者に，メッセージ成分を MCD に送信する．乱数成分は MCD を経由して送信することも可能である．

[受信者]　MCD と PKG から認証を受ける．認証後，送信者から乱数成分を，MCD からメッセージ成分を受信し，PKG から受け取った復号鍵によって暗号文を復号する．

[PKG]　自身が秘匿するマスター秘密鍵を用いて，受信者の ID に対する復号鍵を生成する．暗号化通信路を用いて，受信者に復号鍵を配布する．

[MCD]　自身が秘匿する秘密鍵によって，送信者から受信したメッセージ成分の部分復号を行い，暗号化通信路を用いて受信者に送信する．部分復号で生成したメッセージ成分を安全に保管し，外部に漏らさない．

3.2. アルゴリズム

提案方式は以下の 7 つのアルゴリズムから構成される．処理の流れを図 1 に示す．

PKG.Setup：セキュリティパラメータ$k \in \mathbb{Z}^+$ を入力として，

Step.1　素数q，素数位数qの群$\mathbb{G}_1, \mathbb{G}_2$と双線形写像$\hat{e}: \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$を出力する．ランダムに生成元$P \in \mathbb{G}_1$を選択する．

Step.2　ランダムに$s \in \mathbb{Z}_q^*$を選択し，$P_{pub} = sP$を計算する．

Step.3　ハッシュ関数

$H_1: \{0,1\}^* \to \mathbb{G}_1^*$，$H_2: \mathbb{G}_2 \to \{0,1\}^n$，$H_M: \mathbb{G}_1 \to \{0,1\}^n$を選択する．

システムの公開パラメータ

$params = < q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, P, P_{pub}, H_1, H_2, H_M >$，マスター秘密鍵 $msk = s$を出力する．平文空間$\mathcal{M} = \{0,1\}^n$，暗号文空間 $\mathcal{C} = \mathbb{G}_1^* \times \{0,1\}^n$と定める．

PKG.Ext：任意のID $\in \{0,1\}^*$，mskを入力とし，

Step.1　$Q_{\mathrm{ID}} = H_1(\mathrm{ID}) \in \mathbb{G}_1^*$を計算する．

Step.2　IDに対する秘密鍵$d_{\mathrm{ID}} = sQ_{ID}$を計算する．

復号鍵d_{ID}を出力する．

MCD.KG：$params$を入力とし，ランダムに$b \in \mathbb{Z}_q^*$を選び，$(\mathrm{MCD.PK}, \mathrm{MCD.SK}) = (bP, b)$ を出力する．ここで，MCD.PK, MCD.SKはそれぞれ MCD の公開鍵と秘密鍵である．

Enc：公開パラメータ$params$, 平文$M \in \{0,1\}^n$，ID $\in \{0,1\}^*$を入力とし，

Step.1　$Q_{\mathrm{ID}} = H_1(\mathrm{ID}) \in \mathbb{G}_1^*$を計算する．

Step.2　$r \in \mathbb{Z}_q^*$をランダムに選ぶ．

Step.3　暗号文$< C_R, C_M > = < rP, M \oplus H_2(\hat{e}(Q_{\mathrm{ID}}, P_{pub})^r) >$を生成する．

暗号文$C = < C_R, C_M >$を出力する．

MCD.Enc（メッセージ成分の 2 回目の暗号化）：**Enc** によって出力されたメッセージ成分C_Mを入力とし，

Step.1　$a \in \mathbb{Z}_q^*$をランダムに選び，$C'_{M1} = aP$とする．

Step.2　$H_M(abP)$を計算し，$C'_{M2} = C_M \oplus H_M(abP)$とする．

$C'_M = < C'_{M1}, C'_{M2} >$を出力する．

MCD.Dec（メッセージ成分の部分復号）：**MCD.Enc** で生成した

Partly Doubly Encrypted ID-based Encryption for Web-based File Transmission System

† Makoto SATO and Yoshiaki SHIRAISHI・Nagoya Institute of Technology

‡ Masami MOHRI・Gifu University

†† Hiroshi DOI・Institute of Information Security

‡‡ Ryoji NOGUCHI・Toyotsu System Corp.

C'_Mと$MCD.SK = b$を入力とし，$C_M = C'_{M2} \oplus H_M(bC'_{M1})$を計算し，$C_M$を出力する．

Dec：公開パラメータ$params$，**Enc** によって生成された乱数成分C_R，**MCD.Dec** で部分復号されたメッセージ成分C_M，復号鍵d_{ID}を入力とし，$M = C_M \oplus H_2(\hat{e}(d_{\mathrm{ID}}, C_R))$を計算し，$M$を出力する．

4. 安全性

提案方式のもとになった DEIBE の安全性要件は「少なくとも 1 つのサーバを信頼できれば安全」というものである．ここで信頼できるとは，PKG，MCD，RCD の各サーバがアルゴリズムによって定められた以外の処理を行わず，秘匿情報を漏らさないということである．DEIBE には受動的な攻撃に対する安全性が示されたアルゴリズムと，そのアルゴリズムを変更し，能動的な攻撃に対する安全性が示されたアルゴリズムの 2 種類がある．提案方式は前者をもとにしたアルゴリズムで構成した，受動的な攻撃に対して安全な方式であることを示す．受動的な攻撃では，攻撃者は自分で選んだ平文に対する暗号文を得ることができる．

表 1 に示す攻撃モデルを考えることで，提案方式が DEIBE と同様の「PKG と MCD のうち少なくとも 1 つのサーバを信頼できれば安全」という安全性要件を満たすことを確認する．

攻撃モデル 1 では，PKG が攻撃者と結託することを考える．このモデルでは，攻撃者は暗号文$< C_R, C'_M >$，PKG のマスター秘密鍵msk，公開パラメータ$params$，MCD の公開鍵 MCD.PK を取得できる．

攻撃者は **PKG.Ext** にしたがって受信者の復号鍵d_{ID}を生成し，C'_MからC_Mを求められれば，**Dec** にしたがって$< C_R, C_M >$を復号することで，攻撃に成功する．ここで，$C_M = C'_{M2} \oplus H_M(bC'_{M1})$について，$\mathbb{G}_1$上の CDH 仮定より，$< P, aP(= C'_{M1}), bP(= \mathrm{MCD.PK}) >$から$abP = (bC'_{M1})$を求めることは困難である．

攻撃モデル 2 では MCD が攻撃者と結託することを考える．このモデルでは，攻撃者は暗号文$< C_R, C_M >$，公開パラメータ$params$，MCD の公開鍵と秘密鍵である MCD.PK，MCD.SK を取得できる．

攻撃者は$< C_R, C_M >$を復号することができれば攻撃に成功するが，MCD.SK はメッセージ成分の部分復号に利用する情報であり，$< C_R, C_M >$の復号には一切利用できない．よって提案方式の攻撃モデル 2 における安全性は BF 方式の BasicIdent の安全性に帰着する．

以上より，提案方式は PKG と MCD のどちらか一方が攻撃者と結託しても受動的な攻撃に対して安全である．

5. 既存の暗号方式との比較

DEIBE の処理の流れを図 2 に示す．DEIBE では，提案方式のアルゴリズムに加えて，乱数成分を二重暗号化する．そのため，乱数成分の部分復号を担うサーバとして乱数成分供託サーバ(RCD)が必要である．そして，部分復号によって生成されたC_Rは暗号化通信路を用いて受信者に送信する．C_Rを公開通信路を用いて送信し，MCD と PKG が攻撃者と結託することを考えた場合，RCD を信頼できても，攻撃者に暗号文を復号されてしまう．

また DEIBE では，RCD が乱数成分を部分復号するが，入力となる暗号文は平文のサイズに依存せず一定である．さらに部分復号処理自体も積，ハッシュ値，排他的論理和の計算一度ずつのみで構成されており，この処理を担うためだけにサーバを設けることは非効率的である．

提案方式は，乱数成分を暗号化しないので，送信者が行う暗号化処理が DEIBE と比べて少ない．また，部分復号を担うサーバは MCD1 つである．C_Rを公開通信路を用いて送信しても安全性要件を満たすことができるので，方式を構成する暗号化通信路を 3 つから 2 つに減らすことができた．

また，文献[3]では，IBE における PKG の復号権限を分散する方法として，閾値暗号を用いて，PKG のマスター秘密鍵 msk からシェアと呼ばれるマスター秘密鍵の一部を生成し，複数の PKG に配布する方式が検討されている．各 PKG は自身のシェアを用いて復号鍵の一部を生成し，受信者に送信する．受信者は受け取った複数の復号鍵の一部から復号鍵を生成する．この方式では各 PKG は自身の持つシェアだけでは復号鍵全体を生成できず，暗号文を復号できない．(k,n)閾値暗号では，全部で n 個存在する PKG のうち，k 個以上の PKG のシェアが復号鍵の生成に必要である．

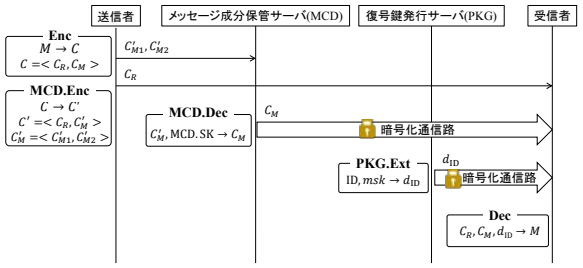

図 1　提案方式の処理の流れ

表 1　攻撃モデル

	攻撃者が得られる情報	帰着する仮定
攻撃モデル 1（PKG が攻撃者と結託する）	$C_R, C'_M, msk, params,$ MCD.PK	$\mathbb{G}_1$上のCDH 仮定
攻撃モデル 2（MCD が攻撃者と結託する）	$C_R, C_M, params,$ MCD.PK, MCD.SK	BF 方式 BasicIdent の安全性（IND-ID-CPA 安全）

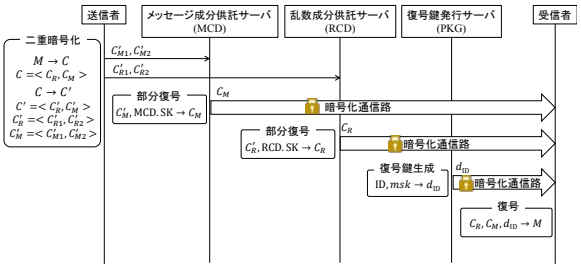

図 2　DEIBE の処理の流れ

(2,2)閾値暗号を用いて提案方式と同様に PKG が暗号文を復号できない IBE 方式を構成することを考えると，提案方式の MCD の代わりに PKG を用いることになる．まず，利用者（受信者）の認証回数は，閾値暗号と提案方式のいずれの場合でも等しい．次に鍵の生成に関しては，閾値暗号では 2 つの PKG と受信者が行う．提案方式では，MCD と PKG が鍵を生成し，受信者は鍵を受け取るのみである．最後に鍵の配布に関して，閾値暗号では 2 つの PKG がそれぞれ行うが，提案方式では PKG のみが配布を行う．以上より鍵の生成と配布に関して，提案方式は閾値暗号より効率が良い．また，閾値暗号の適用が自明でない IBE も存在するが，提案方式は暗号文が乱数成分と平文成分に分かれる任意の IBE に対して適用が可能である．

6. まとめ

本稿では，ファイル送受信システムに用いるための部分的に二重暗号化する ID ベース暗号方式を提案した．提案方式は BF 方式の BasicIdent による暗号化後，生成された暗号文の一部を楕円 ElGamal 暗号をもとにしたアルゴリズムによって二重暗号化する．方式を構成する 2 つのサーバ（メッセージ成分保管サーバ，復号鍵発行サーバ）のうち一方が攻撃者と結託した場合にも受動的攻撃に対して安全であることを示し，閾値暗号を用いて IBE 方式を構成する場合と比較して，鍵の生成と配布の面で効率が良いことと，より多くの IBE に対して適用可能であることを確認した．今後は提案方式の安全性を厳密に証明することを目標とする．

参考文献

[1] 川村舞，伴拓也，白石善明，土井洋，毛利公美，福田洋治，岩田彰，野口亮司：ID ベース暗号を用いた複数サーバによる機密情報伝送システム，SCIS2012，4C1-3　(2012).

[2] Boneh, D. and Franklin, M.: Identity-Based Encryption from the Weil Pairing, SIAM J. of Computing, Vol.32, No.3, pp.586-615 (2003).

[3] Kate, A. and Goldberg, I.: Distributed Private-Key Generators for Identity-Based Cryptography, Proc. 7thConference on Security and Cryptography for Networks (SCN), pp.436-453 (2010).