M-090

2者間暗号通信における鍵交換の計算コスト・通信コスト削減

Reduction of Computational Cost and Communicational Overhead for Key Exchange Protocol over Two-Party Cryptographic

榎木 康二 † 贄田 里詩 † 梅澤 克之 ‡ 平澤 茂一 †
Koji Enoki Satoshi Nieda Katsuyuki Umezawa Shigeichi Hirasawa

1. はじめに

暗号通信は，一般に，公開鍵暗号によって鍵交換を行い，送信する情報を共通鍵暗号によって暗号化することで達成される．しかし，鍵交換には計算コストが大きいという問題があるため，現在まで様々なアルゴリズムが開発されている．

2者間通信において計算コスト・通信コストに優れた公開鍵暗号の概念として，Signcryption [1] があるが，同じ鍵で異なる文書を暗号化すると，受信者の秘密鍵を容易に算出できる性質がある．そのため，同じ相手に別の情報を次々と暗号化して送信する際には，その都度，鍵を再交換する必要があり，結果的にコストが増大する．

そこで本研究では，Signcryption を利用しながら，以後の通信を共通鍵暗号によって暗号化することで，複数回の暗号通信においてもコストを削減できる方式を提案し，Signcryption に比べて有効であることを示す．また，この際に安全性が損なわれていないことを示す．

2. 準備

2.1 鍵交換の概念

ある主体 X が持つ公開鍵 y_X と秘密鍵 x_X による平文 M の暗号化を $E_{y_X}(M)$, $E_{x_X}(M)$ と表記する．一般的な鍵交換では，以下の C を送信者 A から受信者 B に送ることで共通鍵暗号の鍵 k の交換が達成できる．

$$C = E_{y_B}(M), \quad M = (k, s), \quad s = E_{x_A}(k). \qquad (1)$$

C を正しく M に復号できるのは鍵 x_B を持つ受信者 B だけであり，署名情報 s から鍵 y_A によって k を復号できれば，送信相手が A であることが証明できる．

一般に，このような手順で共有した k を鍵とする共通鍵暗号によって，暗号通信を行うことができる．

2.2 暗号理論における安全性 [2]

暗号理論では，攻撃条件と耐性の組み合わせによって9種類の安全性が定義できる．

(1) 攻撃条件：攻撃者の知り得る情報
- (1, a) 公開情報のみ知り得る．
  CPA (Chosen Plaintext Attack)
- (1, b) (1, a) に加えて，予め用意した暗号文に対して，ペアとなる平文を知り得る．
  CCA1 (Chosen Ciphertext Attack)
- (1, c) (1, b) を適応的に知り得る．
  CCA2 (Adaptive CCA)

(2) 暗号の耐性
- (2, a) 平文を完全には解読させない．
  OW (One-Way)：一方向性
  秘密鍵を知ることができない．
- (2, b) 平文を部分解読させない．
  SS (Semantic Security)：強秘匿性
  暗号文から，平文に関する情報を全く知ることが出来ない．
  IND (Indistinguishability)：判別不可能性
  任意の2つの平文と一方の暗号文が与えられたとき，どちらの平文か判別できない．
- (2, c) 暗号文を改竄させない．
  NM (Non-Malleability)：頑健性
  暗号文から，元の平文を改竄した新たな暗号文を作成できない．

攻撃条件 (1, c) に対して耐性が (2, b) または (2, c) であるとき，最も高い安全性を持つ．そのため，暗号の安全性を論じる際には，IND-CCA2 または IND-NM であるかどうかを検討する必要がある．

3. Signcryption [1]

Signcryption は，Y. Zheng によって 1997 年に考案された新しい公開鍵暗号の概念である．鍵交換に必要である，署名と暗号化を同時処理 (signcrypt) することで，計算コスト・通信コストを削減できる．

3.1 Signcryption の手順

Signcryption の一方式である SCS1 アルゴリズム [1] について，送信者 A から受信者 B へ平文 M を signcrypt して暗号化する手順，および暗号文から M を unsigncrypt して復号する手順を示す．

[**ノーテーション**]
素数：p, q（ただし，$q|p-1$）
生成元：$g \in Z_q{}^* = \{1, 2, \cdots, q-1\}$
主体 X の秘密鍵：x_X , 公開鍵：$y_X = g^{x_X} \bmod p$
ハッシュ関数：$h(\cdot)$，鍵付ハッシュ関数：$KH.(\cdot)$
暗号化，復号アルゴリズム：$E.(\cdot)$, $D.(\cdot)$

S1）signcrypt

(1) A は乱数 $n \in Z/qZ$ を生成し，鍵 k を計算する．

$$k = (k_1, k_2) = h({y_B}^n \bmod q). \qquad (2)$$

(2) A は平文 M に対して以下の (c, r, s) を計算し，B に送信する．

$$\begin{aligned} r &= KH_{k_2}(M), \\ s &= n/(r + x_A) \bmod q, \\ c &= E_{k_1}(M). \end{aligned} \qquad (3)$$

†早稲田大学 大学院 理工学研究科 経営システム工学専攻
‡早稲田大学 大学院 理工学研究科 経営システム工学専攻,
（株）日立製作所 システム開発研究所

S2）unsigncrypt

(1) B は鍵情報 k を算出する．

$$k = (k_1, k_2) = h((y_A \cdot g^r)^{s \cdot x_B} \bmod p). \quad (4)$$

(2) B は平文 M を算出する．

$$M = D_{k_1}(c). \quad (5)$$

(3) $KH_{k_2}(M) = r$ ならば，B は M を受理する．

3.2 Signcryption の安全性

定理 1

Signcryption は，以下の (1) 仮定，(2) 条件で鍵の長さが十分に長いとき，IND-CCA2 である [3].

(1) Gap Diffie-Hellman 問題が計算困難である．

(2) アルゴリズム中で用いる共通鍵暗号が IND-CPA の安全性を持つ． □

4. 提案方式

4.1 Signcryption の問題点

Signcryption は同一の乱数 n を異なる平文に適用した場合，送信者の秘密鍵 x_A を容易に算出できるという性質を持つ [4]．そのため，異なる平文を送信する度に，鍵 k の再生成のための signcrypt 処理を行う必要がある．

一方，一般的な鍵交換の手法を用いる場合，一度十分に長い鍵を送受信者間で共有すれば，その鍵による暗号通信を何度でも行うことができる．

すなわち，Signcryption によって複数回の暗号通信を行う場合，コストが小さいという利点が生かされないといえる．

4.2 提案方式

Signcryption を複数回の暗号通信で利用するために，共通鍵暗号と併用することを考える．3.1 節の平文 M に対して秘密情報 k^* を付加した平文 $M^* = (M, k^*)$ を定義し，signcrypt して送信する．

$$\begin{aligned} r^* &= KH_{k_2}(M^*) = KH_{k_2}(M, k^*), \\ s^* &= n/(r^* + x_A) \bmod q, \\ c^* &= E_{k_1}(M^*) = E_{k_1}(M, k^*). \end{aligned} \quad (6)$$

以上のように M^* および (r^*, s^*, c^*) を定義することにより，正当な受信者 B だけが k^* を得ることができる．2 回目以降の暗号通信では，k^* を鍵とした共通鍵暗号による暗号通信を行うことで，SCS1 とほぼ同じ計算コストで複数回の暗号通信を行うことができる．

5. 評価および考察

5.1 計算コストの評価

提案方式の有効性を示すため，計算コストを評価する．Signcryption，共通鍵暗号の計算コストをそれぞれ C_{sc}, C_{ck} とすると，N 回の暗号通信に要する SCS1，提案方式の総計算コストは次のようになる．

- SCS1：$N\ C_{sc}$
- 提案方式：$C_{sc} + (N-1)C_{ck}$

一般に $C_{sc} \gg C_{ck}$ となるため，提案方式は計算コストにおいて SCS1 よりも優れていることが分かる．

5.2 通信コストの評価

本節では，鍵交換に必要な通信コストであるオーバーヘッド，すなわち暗号文以外に送信しなければならない情報ビット数について評価する．

SCS1 と提案方式について，N 回の暗号通信に要する鍵交換の回数と総通信コスト，同一の安全性を仮定した場合の総通信コスト比率を表 1 に示す．ただし整数 X に対して，$|X| = \lceil \log_2 X \rceil$ とする．

表 1: 通信コストの比較

	SCS1 [1]	提案方式
鍵交換回数	N	1
総通信コスト	$N(\|KH.(\cdot)\|+\|q\|)$	$\|KH.(\cdot)\|+\|q\|+\|k^*\|$
比率	$1.00 \times N$	$1.53\ (< 2)$

また，各パラメータに代入した値は以下の通り [1].
$|p|=1024$, $|q|=160$, $|KH.(\cdot)|=80$, $|k^*|=128$.

よって，$N \geq 2$ の場合で，提案方式は通信コストにおいて SCS1 よりも優れていることが分かる．

5.3 安全性に関する考察

3.2 節の定理 1 より，以下の系が導かれる．

系 1

下記 (1), (2) が与えられたとしても，c_α の平文が M_1, M_2 のどちらであるか判別できない．

(1) 2 つの平文：$M_1 = (M, m_1),\ M_2 = (M, m_2)$.

(2) どちらかの暗号文：$c_\alpha = E_k(M_\alpha),\ \alpha \in \{1, 2\}$. □

このとき，系 1 における $m_\alpha = k_\alpha{}^*$ とすると，提案方式における平文 M^* となる．従って上記より，提案方式において攻撃者は秘密情報の有無および変化を認識できない．そのため，提案方式は Signcryption と同等の安全性を持つと考えられる．

6. まとめと今後の課題

2 者間通信における鍵交換について，Signcryption と共通鍵暗号を併用することで，複数回の暗号通信において計算コスト・通信コストを削減する方式を提案した．また，その際に安全性が損なわれていないことを示した．

今後の課題として，サイドチャネル攻撃に対する耐性評価が挙げられる．

文献

[1] Y. Zheng, “Digital Signcryption or How to Achieve Cost(Signature & Encryption) ≪ Cost(Signature) + Cost(Encryption),” *CRYPTO’97*, vol.1294 of LNCS, pp.165–179, 1997.

[2] 多田 充, “暗号プロトコルの安全性に関する研究,” 電気通信普及財団研究報告書, No.15, pp.430–437, 2000.

[3] J. Baek, R. Steinfeld, and Y. Zheng,, “Formal Proofs for the Security of Signcryption,” *Proc. PKC’02*, vol.2274 of LNCS, pp.80–98, 2002.

[4] T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” *IEEE Trans. Inform. Theory*, vol.30, pp.469–472, 1985.