■1 群（信号・システム）- 3 編（暗号理論）

5 章 公開鍵暗号

（執筆者：花岡悟一郎）

■概要■

【本章の構成】

■1 群 - 3 編 - 5 章

5-1 公開鍵暗号の概要と利点

（執筆者：花岡悟一郎）[2008 年 11 月 受領]

インターネットのような不特定多数の利用者が存在するネットワークでは，通信相手と交信するための秘密情報をあらかじめ共有しておくことは困難であるため，共通鍵暗号のみによって安全な通信を行うことは容易ではない．公開鍵暗号を用いた場合，暗号化に必要となるすべての情報は公開することができ，受信者と事前に秘密情報を共有することなく，誰でも暗号化を行うことができる．一方，作成された暗号文は，（秘密に保管されている）復号鍵を用いない限り復号することができない．したがって，公開鍵暗号を利用することで，より簡便に安全な通信路を確立することが可能となる．また，暗号文の受信者は，送信者が誰であったとしても単一の復号鍵のみで復号処理を行うことができることも大きい利点といえる．

■1 群 - 3 編 - 5 章

5-2 公開鍵暗号のモデル

（執筆者：花岡悟一郎）[2008 年 11 月 受領]

定義 1 (公開鍵暗号) 公開鍵暗号方式 Π は，**鍵生成アルゴリズム** GEN，**暗号化アルゴリズム** ENC，**復号アルゴリズム** DEC の三つのアルゴリズムの組として定義される．

GEN: 1^k を入力とし，復号鍵と公開鍵のペア (sk, pk) を出力する確率的アルゴリズム．ここで，k はセキュリティパラメータとする．

ENC: 平文 $m \in M$ と公開鍵 pk を入力とし，暗号文 c を出力する確率的アルゴリズム（もしくは，確定的アルゴリズム）．

DEC: 暗号文 c と復号鍵 sk を入力とし，平文 m（もしくは，失敗を表すシンボル “⊥”）を出力する確定的アルゴリズム．

受信者は GEN により鍵ペアを生成し，また，このうち公開鍵 pk を周知にする．送信者は ENC により平文を受信者の公開鍵 pk で暗号化し，受信者に送信する．受信者は DEC により，復号鍵 sk を用いて受信した暗号文の復号を行う．

■1 群 - 3 編 - 5 章

5-3 選択平文攻撃に対して安全な方式

（執筆者：花岡悟一郎）[2008 年 11 月 受領]

5-3-1 選択平文攻撃に対する安全性

公開鍵暗号方式において，暗号化された文書の不正解読を試みる攻撃者は，公開鍵を自由に得ることができるため，任意の平文の暗号化を行うことができる．すなわち，攻撃者に与えられる攻撃環境として**選択平文攻撃（chosen plaintext attack）**が，最低でも保証される．そのため，選択平文攻撃に対して，平文の完全な解読を許さないこと（すなわち**一方向性（one-wayness）**をもつこと）が公開鍵暗号の安全性に関する最も基本的な要件であると考えられる．また，同様の攻撃に対して，平文の一切の部分解読を許さないこと（すなわち**強秘匿性（semantic security）**をもつ）が，それに次ぐ基本的要件とみなされる．

定義 1 (一方向性) 任意の多項式時間アルゴリズム $\mathcal{A}$ に対して，$\Pi = (\mathsf{GEN}, \mathsf{ENC}, \mathsf{DEC})$ が次式を満足するとき，Π は**一方向（one-way）**であるという．

$$\Pr[(sk, pk) \leftarrow \mathsf{GEN}(1^k);\ m \leftarrow_R M; c \leftarrow \mathsf{ENC}(m, pk);\ m' \leftarrow \mathcal{A}(c, pk) | \ m' = m] < \epsilon$$

ここで，ϵ は，無視できる値とする．また，M は平文空間とする．

定義 2 (強秘匿性) 任意の多項式時間アルゴリズム $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ に対して，$\Pi = (\mathsf{GEN}, \mathsf{ENC}, \mathsf{DEC})$ が次式を満足するとき，Π は**強秘匿（semantically secure）**であるという[9]．

$$|\Pr[\mathbf{Exp}_{\Pi,\mathcal{A}}^{ind-1} = 1] - \Pr[\mathbf{Exp}_{\Pi,\mathcal{A}}^{ind-0} = 1]| < \epsilon$$

ここで，ϵ は無視できる値とし，また，$\mathbf{Exp}_{\Pi,\mathcal{A}}^{ind-b}$ は，$b \in \{0, 1\}$ に対し，次のように定義される試行とする:

$$\mathbf{Exp}_{\Pi,\mathcal{A}}^{ind-b} : [(sk, pk) \leftarrow \mathsf{GEN}(1^k);\ (m_0, m_1, s) \leftarrow \mathcal{A}_1(pk);$$
$$c \leftarrow \mathsf{ENC}(m_b, pk);\ b' \leftarrow \mathcal{A}_2(m_0, m_1, c, pk, s); \mathsf{return}\ b']$$

5-3-2 RSA 暗号

RSA 暗号（RSA cryptosystem）[11]は現在最も広く利用されている公開鍵暗号方式といえる．ただし，RSA 暗号の基本部分をそのまま実装しただけでは，様々な攻撃に対してぜい弱であることがよく知られており，実用上は，OAEP[2]などの安全性を高める工夫が施されている．

(a) RSA 暗号[11]

鍵生成: 入力 1^k に対し，二つの素数 p, q を生成し，$n = pq$ を計算する．ここで，$|p|$ と $|q|$ は，ほぼ等しい値とする．また，$\lambda(n) = lcm(p-1, q-1)$ を計算する．更に，適当な $e \in \mathbb{Z}_{\lambda(n)}$, $gcd(e, \lambda(n)) = 1$ を定め，$ed = 1 \bmod \lambda(n)$ となるような d を導出する．復号鍵，公開鍵のペアとして次のように (sk, pk) を出力する: $sk = (d, n)$, $pk = (e, n)$.

暗号化: 入力 $m \in \mathbb{Z}_n$ 及び pk に対し，次式により暗号文 c を得る: $c = m^e \bmod n$．ここで，m は暗号化の対象となる平文とする．

復号: 入力 $c \in \mathbb{Z}_n$ 及び sk に対し，次式により復号を行う: $m = c^d \bmod n$.

RSA 暗号は一方向性を満足するものと考えられているが，それを支える根拠は，それを破る具体的な攻撃方法が過去 30 年に渡って示されていないことそのものであり，それ自体の難しさの仮定に基づいているといっていい．

定義 3 (RSA 問題) RSA 暗号の公開鍵 (e, n) と，ランダムな $y \in \mathbb{Z}_n$ が与えられたとき，$x = y^{1/e} \bmod n$ を満たす x を求める問題を **RSA 問題（RSA inversion problem）**という．

いかなる確率的多項式時間アルゴリズムを用いたとしても RSA 問題を解く確率が無視できると仮定できるとき，RSA 暗号は一方向性を満たす．なお，RSA 問題の困難性の仮定は，**RSA 仮定（RSA assumption）**とよばれている．

定理 1 RSA 仮定が成立するとき，RSA 暗号は一方向性を満足する．

n の素因数分解を行う確率的多項式時間アルゴリズムの存在性は，RSA 問題を解く確率的多項式時間アルゴリズムの存在性の十分条件であるが，それらのギャップについてはまだよく分かっていない．現在のところは，RSA 暗号の一方向性を破るための最も有効な手段は，n の素因数分解を解くことであると考えてよい．

5-3-3 ElGamal 暗号

ElGamal 暗号（ElGamal cryptosystem）[8]は，離散対数問題の困難性に依拠した公開鍵暗号であり，RSA 暗号とは異なる様々な性質を有している．特に，強秘匿で，しかも，準同型暗号であるため多彩な拡張が可能である．また，位数が既知の群を用いて構成できることも重要な性質といえる．

(a) ElGamal 暗号[8]

鍵生成: 入力 1^k に対し，位数 p の群 $\mathbb{G}$ を作成する（p は素数）．次に，$g \in \mathbb{G}$ を選び，また，$x \in_R \mathbb{Z}_p$ を選択し，$y = g^x$ を計算する．復号鍵，公開鍵のペアとして次のように (sk, pk) を出力する: $sk = (x, \mathbb{G}), pk = (y, \mathbb{G}, g)$.

暗号化: 入力 $m \in \mathbb{G}$ 及び pk に対し，次式により暗号文 c を得る: $r \in_R \mathbb{Z}_p$, $c_1 = g^r$, $c_2 = m \cdot y^r$, $c = (c_1, c_2)$．ここで，m は暗号化の対象となる平文とする．

復号: 入力 $c(= (c_1, c_2))$ 及び sk に対し，次式により復号を行う: $m = c_2 \cdot c_1^{-x}$.

1976 年の提案以降，Diffie-Hellman 鍵配送[6]の安全性について深く検討をなされてきたが，これまでに本質的な問題点は指摘されておらず，Diffie-Hellman 鍵配送は安全であると考えられている．ElGamal 暗号の安全性は，Diffie-Hellman 鍵配送の安全性に密接に関係している．

定義 4 (CDH 問題) 群 $\mathbb{G}$ とその三つの元 $(g_1, g_2, g_3) \in \mathbb{G}^3$ が与えられたとき, $\log_{g_1} g_2 = \log_{g_3} h$

を満たす $h \in \mathbb{G}$ を求める問題を群 $\mathbb{G}$ に関する **CDH 問題（computational Diffie-Hellman problem）**という．

定義 5 (DDH 問題) 群 $\mathbb{G}$ とその四つの元 $(g_1, g_2, g_3, g_4) \in \mathbb{G}^4$ が与えられたとき，$\log_{g_1} g_2 = \log_{g_3} g_4$ が成立するかを判定する問題を群 $\mathbb{G}$ に関する **DDH 問題（decisional Diffie-Hellman problem）**という．

ここで, CDH 問題が困難であるとは, h を導出する確率が無視できる場合をいう．DDH 問題が困難であるとは, (g_1, g_2, g_3, g_4) が二つの分布 $\mathcal{D} := \{(\alpha, \beta, \gamma, \delta) | (\alpha, \beta, \gamma, \delta) \in \mathbb{G}^4, \log_\alpha \beta = \log_\gamma \delta\}$ 及び $\mathcal{R} := \{(\alpha, \beta, \gamma, \delta) | (\alpha, \beta, \gamma, \delta) \in \mathbb{G}^4\}$ のうちどちらか一方から確率 1/2 で選び出されるとき，たかだか $1/2 + \epsilon$ の確率でしか，どちらの分布から選び出されたのかを判定できない場合をいう．ここで，ϵ は無視できる値とする．CDH 問題（もしくは，DDH 問題）の困難性の仮定は **CDH 仮定（CDH assumption）**（もしくは，**DDH 仮定（DDH assumption）**）と呼ばれる．ElGamal 暗号の安全性は，これらの仮定を用いて次のように根拠付けられる．

定理 2 群 $\mathbb{G}$ に関して CDH 仮定が成立するとき，ElGamal 暗号は一方向性を満足する．また，群 $\mathbb{G}$ に関して DDH 仮定が成立するとき，ElGamal 暗号は強秘匿性を満足する．

■1 群 - 3 編 - 5 章

5-4 選択暗号文攻撃に対して安全な方式

（執筆者：花岡悟一郎）［2008 年 11 月 受領］

5-4-1 選択暗号文攻撃に対する安全性

上述のとおり，（選択平文攻撃に対する）一方向性や強秘匿性は公開鍵暗号に求められる最も基礎的な安全性上の要件と考えられるが，実用システムへの導入を考慮すると，更に高い安全性が要求されることになる．すなわち，実用的な情報通信システムにおいては，暗号文の不正な解読を試みる攻撃者が，解読の対象となる暗号文に巧妙に手を加えたうえで，それを正規受信者に復号させ，その復号結果を攻撃者に返信させることが可能となる状況もありうる．事実，Bleichenbacher は，広く利用されていた実用システムにおける，そのような状況の実例と，その状況を利用した具体的な解読方法を示している[3]．そのため，近年では**選択暗号文攻撃に対する強秘匿性（IND-CCA: semantic security against chosen-ciphertext attacks）**が証明可能であることが，実用的公開鍵暗号に求められている．

選択暗号文攻撃に対する強秘匿性は，その定義自体が非常に強い安全性を直接的に意味しているが，そのほかにも（選択暗号文攻撃に対する）**頑強性（non-malleability）**をも自動的に保証するものとなっている点も重要である．頑強性とは，攻撃の対象となる暗号文に対する平文について，いかなる攻撃者であっても，その平文と意味のある関係を満足するような別の平文に対する暗号文を作成することができないような安全性を指す．

定義 1 (選択暗号文攻撃に対する強秘匿性) 任意の多項式時間アルゴリズム $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ に対して，$\Pi = (\mathrm{GEN}, \mathrm{ENC}, \mathrm{DEC})$ が次式を満足するとき，Π は**選択暗号文攻撃に対して強秘匿（IND-CCA: semantically secure against chosen-ciphertext attacks）**であるという[10, 7]．

$$|\Pr[\mathbf{Exp}_{\Pi,\mathcal{A}}^{ind-1} = 1] - \Pr[\mathbf{Exp}_{\Pi,\mathcal{A}}^{ind-0} = 1]| < \epsilon$$

ここで，ϵ は無視できる値とし，また，$\mathbf{Exp}_{\Pi,\mathcal{A}}^{ind-b}$ は，$b \in \{0, 1\}$ に対し，次のように定義される試行とする:

$$\mathbf{Exp}_{\Pi,\mathcal{A}}^{ind-b} : [(sk, pk) \leftarrow \mathrm{GEN}(1^k);\ (m_0, m_1, s) \leftarrow \mathcal{A}_1^{\mathcal{O}}(pk);$$
$$c \leftarrow \mathrm{ENC}(m_b, pk);\ b' \leftarrow \mathcal{A}_2^{\mathcal{O}}(m_0, m_1, c, pk, s); \text{return } b'].$$

なお，$\mathcal{O}$ は復号オラクルであり，$\mathcal{A}$ は $\mathcal{O}$ に対して c 以外の任意の暗号文を問い合わせることが許されており，それのような問い合せに関して $\mathcal{O}$ は復号鍵 sk による正当な復号結果を返答する．$\mathcal{O}$ に対し，任意の順序で任意の（多項式）回数の問い合せを行うことができる．

5-4-2 RSA-OAEP

前述のとおり，RSA 暗号を直接的に実装しただけでは，実用に耐えうるレベルの安全性は得られないため **OAEP（optimal asymmetric encryption padding）**[2]という変換を施し，**RSA-OAEP** と呼ばれる実装形態にてしばしば利用されることになる．RSA-OAEP はランダムオラクルモデル[1]において，選択暗号文攻撃に対する強秘匿性をもつことが証明されている．

（a）RSA-OAEP[2)]

鍵生成: 通常の RSA 暗号と同様の手順で n, e, d を計算し，また，二つのハッシュ関数 $G : \{0,1\}^k \to \{0,1\}^{|n|-k}$，$H : \{0,1\}^{|n|-k} \to \{0,1\}^k$ をランダムに選択する．復号鍵，公開鍵のペア (sk, pk) を次のように出力する: $sk = (d, n, G, H)$, $pk = (e, n, G, H)$.

暗号化: 平文 $m \in \{0,1\}^{|n|-2k}$ 及び pk に対し，次式により暗号文 c を得る: 乱数 $r \in \{0,1\}^k$ を選び，次の手順にて m を m' に変換する．

$$\begin{aligned} m'_0 &\leftarrow (m\|0^k) \oplus G(r) \\ m'_1 &\leftarrow r \oplus H(m'_0) \\ m' &\leftarrow (m'_0\|m'_1) \end{aligned}$$

なお，上記の m から m' への変換が OAEP と呼ばれる．最後に，（二進表現である）m' を $\mathbb{Z}_n$ 上の値に変換したうえで，$c = m'^e \bmod n$ により暗号文 c を作成する．

復号: 入力 $c \in \mathbb{Z}_n$ 及び sk に対し，次式により復号を行う: まず，$m' = c^d \bmod n$ を計算し，また m' を二進表現に戻したうえで，次のように m を m' に変換する．

$$\begin{aligned} (m'_0\|m'_1) &\leftarrow m' \qquad (\text{ただし，} |m'_1| = k) \\ r &\leftarrow m'_1 \oplus H(m'_0) \\ (m\|\alpha) &\leftarrow m'_0 \oplus G(r) \qquad (\text{ただし，} |\alpha| = k) \end{aligned}$$

もし，$\alpha = 0^k$ であれば，m を復号結果として出力する．そうでなければ，復号失敗を表すシンボルを出力する．

RSA-OAEP は，ハッシュ関数 G 及び H を理想的なランダム関数（すなわちランダムオラクル）と仮定したうえで，安全性の証明が可能となる．そのような仮定は非常に強く，様々な問題が指摘されていることに注意が必要である（例えば，参考文献 4) を参照のこと）．

定理 3 RSA 仮定が成立し，G と H がランダムオラクルとみなせるとき，RSA-OAEP は選択暗号文攻撃に対する強秘匿性を満足する．

5-4-3 Cramer-Shoup 暗号

上述のとおり，RSA-OAEP はランダムオラクルモデルにおいて選択暗号文攻撃に対して強秘匿であることが証明可能ではあるが，現実にはランダムオラクルは存在し得ないため，実装された RSA-OAEP が実際にはどのような安全性をもっているかはよく分かっていない．ランダムオラクルモデルに依存することなく選択暗号文攻撃に対する強秘匿性を証明可能となり，しかも，実用的効率性を併せもつような公開鍵暗号の構成方法としては Cramer-Shoup 暗号がよく知られている．Cramer-Shoup 暗号は ElGamal 暗号の（非自明な）拡張と考えることができる．

（a）Cramer-Shoup 暗号[5)]

鍵生成: 入力 1^k に対し，位数 p の群 $\mathbb{G}$ を作成する（p は素数）．次に，$(g,h) \in_R \mathbb{G}^2$ を選び，また，$(x_{00},x_{01},x_{10},x_{11},x_{20},x_{21}) \in_R \mathbb{Z}_p^6$ を選択し，$y_i = g^{x_{i0}}h^{x_{i1}}$ $(0 \le i \le 2)$ を計算する．また，ターゲット衝突困難なハッシュ関数 H をランダムに選択する*．復号鍵，公開鍵のペアとして次のように (sk, pk) を出力する: $sk = (x_{00},x_{01},x_{10},x_{11},x_{20},x_{21},\mathbb{G},H)$, $pk = (y_0,y_1,y_2,\mathbb{G},g,h,H)$.

暗号化: 入力 $m \in \mathbb{G}$ 及び pk に対し，次式により暗号文 c を得る: $r \in_R \mathbb{Z}_p$, $c_1 = g^r$, $c_2 = h^r$, $c_3 = m \cdot y_0^r$, $c_4 = (y_1 y_2^{H(c_1,c_2,c_3)})^r$, $c = (c_1,c_2,c_3,c_4)$．ここで，m は暗号化の対象となる平文とする．

復号: 入力 $c(=(c_1,c_2,c_3,c_4))$ 及び sk に対し，次のように復号を行う: まず，

$$c_4 = (c_1^{x_{10}}c_2^{x_{11}})(c_1^{x_{20}}c_2^{x_{21}})^{H(c_1,c_2,c_3)}$$

が成立しているか確認する．等号が成り立っていないとき，復号失敗を表すシンボルを出力する．等号が成立しているならば $m = c_3 \cdot c_1^{-x_{00}} \cdot c_2^{-x_{01}}$ を計算し，m を出力する．

ElGamal 暗号と同様に Cramer-Shoup 暗号も DDH 問題の困難性を安全性の根拠としている．

定理 4 群 $\mathbb{G}$ に関して DDH 仮定が成立し，なおかつ H がターゲット衝突困難なハッシュ関数であるとき，Cramer-Shoup 暗号は選択暗号文攻撃に対する強秘匿性を満足する．

Cramer-Shoup 暗号はランダムオラクルに依存しておらず，したがって，上記の RSA-OAEP に比べて，より確固とした安全性が根拠付けられているといえる．

■参考文献

1) M. Bellare and P. Rogaway, “Random oracles are practical: A paradigm for designing efficient protocols,” Proc. of CCS’93, ACM, pp.62-73, 1993.
2) M. Bellare and P. Rogaway, “Optimal asymmetric encryption,” Proc. of EUROCRYPT’94, LNCS 950, Springer-Verlag, pp.92-111, 1995.
3) D. Bleichenbacher, “Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1,” Proc. of CRYPTO’98, LNCS 1462, Springer-Verlag, pp.1-12, 1998.
4) R. Canetti, O. Goldreich, and S. Halevi, “The random oracle methodology, revisited,” Proc. of STOC’98, ACM, pp.209-218, 1998.
5) R. Cramer and V. Shoup, “A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack,” Proc. of CRYPTO’98, LNCS 1462, Springer-Verlag, pp.13-25, 1998.
6) W. Diffie and M. Hellman, “New directions in cryptography,” IEEE Trans. on Inform. Theory, IT-22, 6, pp.644-654, 1976.
7) D. Dolev, C. Dwork, and M. Naor, “Non-malleable cryptography,” Proc. of STOC’91, ACM, pp.542-552, 1991.

* 関数 H の定義域よりランダムに選ばれた値 x が与えられたとき，$H(x) = H(x')$ となる $x'(\neq x)$ を導出するのが困難であるとき，H はターゲット衝突困難であるという．

8) T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” IEEE Trans. on Inform. Theory, vol.IT-31, no.4, pp.469-472, 1985.
9) S. Goldwasser and S. Micali, “Probabilistic encryption,” J. Comput. Syst. Sci., vol.28, no.2, pp.270-299, 1984.
10) C. Rackoff and D.R. Simon, “Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack,” Proc. of CRYPTO’91, LNCS 576, Springer-Velag, pp.433-444, 1992.
11) R.L. Rivest, A. Shamir and L.M. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” Commun. ACM, vol.21, no.2, pp.120-126, 1978.