■1 群（信号・システム）- 3 編（暗号理論）

8 章 ハイブリッド暗号

（執筆者：岡本龍明）［2019 年 1 月 受領］

【本章の構成】

8-1 章ではハイブリッド暗号についてを紹介する．8-2 章では藤崎-岡本変換によるハイブリッド暗号の構成法を紹介する．8-3 章では KEM-DEM ハイブリッド暗号の構成法を紹介する．8-4 章では KEM の構成例を取り上げ、PSEC-KEM を紹介する．

■1 群 - 3 編 - 8 章

8-1 ハイブリッド暗号とは

（執筆者：岡本龍明）[2019 年 1 月 受領]

暗号には大きく共通鍵暗号と公開鍵暗号がある．共通鍵暗号では，暗号通信を行うために，送受信者が事前に安全に鍵を共有（配送）する必要がある．

一方，インターネットのようなオープンなネットワークでは，不特定な（事前に情報の共有のない）送受信者が安全でない（盗聴の可能性がある）通信手段のみを用いて安全な暗号通信を行うことのできる（つまり，事前に鍵共有をする必要のない）暗号方式が求められるようになった．このような要求に答える暗号方式が公開鍵暗号である[2)]．公開鍵暗号は，不特定な送受信者が安全でない通信手段のみを用いて安全に情報を送信する手段を提供する．

それでは，インターネット上で用いられる秘匿目的の暗号機能は公開鍵暗号のみで十分であろうか？　機能的には，公開鍵暗号のみで十分であるが，性能まで考慮すると公開鍵暗号のみでは不十分である．なぜならば最も実用的な公開鍵暗号でも，その処理速度は非常に遅いからである．公開鍵暗号に比べると共通鍵暗号の処理速度は 2 桁から 3 桁高速である．そこで，不特定送受信間での暗号通信を可能とする公開鍵暗号の機能を保持しつつ，共通鍵暗号の高速性を兼ね備えた暗号は構成可能であろうか？　このような問いに答える暗号の構成方法が公開鍵暗号と共通鍵暗号を併用したハイブリッド暗号である．

ハイブリッド暗号では，公開鍵暗号（秘匿通信もしくは鍵共有）は，共通鍵暗号で用いる秘密鍵の共有／配送のために使われ，秘匿通信の対象であるデータの暗号は，（公開鍵暗号で）共有／配送された秘密鍵を用いた共通鍵暗号で行う．

現在，インターネットなどにおける暗号通信は，多くの場合このようなハイブリッド暗号を用いて行われている．例えば，多くのアプリケーションで用いられている暗号ツールである SSL/TLS においては，公開鍵暗号として RSA 暗号や楕円曲線暗号などが使われ，共通鍵暗号としては AES などが用いられている．

ハイブリッド暗号を機能としてみると公開鍵暗号である．したがって，ハイブリッド暗号の安全性は，公開鍵暗号の安全性で定式化できる．公開鍵暗号の望ましい安全性は「選択暗号文攻撃に対して強秘匿（IND-CCA2）」であるため，ハイブリッド暗号で求められる安全性も同様に IND-CCA2 である．

IND-CCA2 安全なハイブリッド暗号方式を構成する方法として，最も弱い安全性（一方向性）しかもたない任意の公開鍵暗号と強秘匿性をもつ任意の共通鍵暗号を用いて IND-CCA2 安全なハイブリッド暗号を構成する汎用的な方法が藤崎-岡本変換と呼ばれている方法である[3)]．これは，ランダムオラクルモデルに基づき安全性が証明されるが，ランダムオラクルの代わりに実用的なハッシュ関数を用いることで極めて実用性の高い方式となる．

ランダムオラクルを用いない標準モデルで IND-CCA2 安全なハイブリッド暗号を構成する方法として黒澤-デスメット（Desmedt）ハイブリッド暗号がある [5)]．これは公開鍵暗号としてクラマー-シュープ（Cramer-Shoup）暗号の変形を用いて，強秘匿性の共通鍵暗号と安全なメッセージ認証および鍵導出関数を組み合わせて構成する．

2001 年に，シュープは，国際標準化機構 ISO における公開鍵暗号の標準化作業の中で，ハイブリッド暗号を実現するための標準的な構成要素として，公開鍵暗号の鍵共有の機能を鍵カプセル化メカニズム（Key Encapsulation Mechanism: 以降 KEM と呼ぶ）として，共通鍵

暗号の機能をデータカプセル化メカニズム（Data Encapsulation Mechanism: DEM）として定式化した[7]．そして，IND-CCA2 安全な（強い安全性の）KEM と IND-CCA2 安全な（強い安全性の）DEM を組み合わせることにより，IND-CCA2 安全なハイブリッド暗号が構成できることを示した[1]．これは，藤崎-岡本変換や黒澤-デスメット暗号が，弱い安全性の公開鍵暗号と共通鍵暗号から IND-CCA2 安全な（強い安全性の）ハイブリッド暗号を構成しようとするものであることとは対照的に，強い安全性の公開鍵暗号と強い安全性の共通鍵暗号から強い安全性のハイブリッド暗号を構成するものである．

■1 群 - 3 編 - 8 章

8-2 藤崎-岡本変換によるハイブリッド暗号の構成法

（執筆者：岡本龍明）[2019 年 1 月 受領]

藤崎-岡本変換は，適当な（最も弱い安全性の）公開鍵暗号（トラップドア一方向性関数）と共通鍵暗号を用いて，IND-CCA2-PKE のハイブリッド暗号に変換する一般的な方式である．

まず，(G,E,D) を公開鍵暗号方式，$(SymE,SymD)$ を共通鍵暗号方式とする．ここで，$E(K,X;R)$ は，公開鍵 K, 平文 X を入力として乱数 R を用いる暗号化演算とする．H_1,H_2 はハッシュ関数であり，ランダムオラクルであるとみなす．これらを用いてハイブリッド暗号 $PKE=\{Gen,Enc,Dec\}$ を構成する．

Gen: 入力として 1^k をとり，$(pk,sk)\leftarrow G(1^k)$ を生成する．公開鍵と秘密鍵を (pk,sk) とする．

Enc: 公開鍵 pk および平文 m を入力として，$r\leftarrow\{0,1\}^*$ を選び，$C_1=E(pk,r;H_2(C_2\,\|\,r))$ および $C_2=SymE(H_1(r),m)$ を求める（つまり，$H_1(r)$ を共通鍵暗号の秘密鍵として用いる）．$C=(C_1,C_2)$ を暗号文として出力する．

Dec: 鍵対 (pk,sk) と暗号文 C を入力とし，$r=D(sk,C_1)$ を求め，$m=SymD(H_1(r),C_2)$ を求める．次に，$C_1=E(pk,r;H_2(C_2\,\|\,r))$ であるかを確認する．もしそうでないならば $\perp$ を出力する．成立するならば m を復号結果として出力する．

藤崎-岡本変換によるハイブリッド暗号の安全性は以下である．

公開鍵暗号 (G,E,D) が OW-CPA 安全（CPA で一方向性）かつ γ 一様性であり，共通鍵暗号 $(SymE,SymD)$ が IND-OT 安全な（ワンタイム強秘匿性）ならば，ハイブリッド暗号 PKE はランダムオラクルモデルにおいて IND-CCA2 安全である．

■1 群 - 3 編 - 8 章

8-3 KEM-DEM ハイブリッド暗号の構成法

（執筆者：岡本龍明）[2019 年 1 月 受領]

8-3-1 KEM

KEM は，公開鍵暗号方式の概念に従い，各利用者 A は公開鍵 P_A と秘密鍵 S_A の対を保有する．KEM と秘匿通信機能の公開鍵暗号方式（以降 PKE（Public-Key Encryption）と呼ぶ）との違いは，PKE の暗号化処理においては，平文 m と受信者 A の公開鍵 P_A を入力として暗号文 C を出力するのに対して，KEM の暗号化処理では，受信者の公開鍵 P_A を入力として暗号文 C と鍵 K を出力する（C は受信者 A に送られるが，K は送信者側で秘密に保有され，以降のデータ暗号処理で利用される）．また，復号処理では，PKE の場合，C と秘密鍵 S_A より，平文 m が復号される．KEM では，C と秘密鍵 S_A より，鍵 K が復号される．

KEM をより正確に述べると，以下の 3 つのアルゴリズムから構成される．

- 鍵サイズなどに関するセキュリティパラメータを入力し公開鍵／秘密鍵の対 (P_A, S_A) を出力する鍵生成アルゴリズム．
- 公開鍵 P_A を（さらに必要に応じてオプション情報を）入力し，鍵 K と暗号文 C の対を出力する暗号化アルゴリズム．
- 秘密鍵 S_A と暗号文 C を入力とし，鍵 K を出力とする復号化アルゴリズム．

PKE で「適応的選択暗号文攻撃に対して識別不可能性（IND-CCA2）」が定義されているように，KEM においても，「適応的選択暗号文攻撃に対して識別不可能性 」が定義されている．ここでは，PKE における IND-CCA2 と区別するため，KEM に対する IND-CCA2 を IND-CCA2-KEM と記述する．（なお，本来，IND-CCA2 は PKE に対して定義された概念である．KEM や DEM に対して類似の定義を与え，いずれも同じ名前（「適応的選択暗号文攻撃に対して識別不可能性（安全）」）を使用することは，シュープらの記述に従っている．ここでは，それらの違いを明確化するために，それぞれ IND-CCA2-PKE, IND-CCA2-KEM, IND-CCA2-DEM, と記することにする．）

以下に，IND-CCA2-KEM の定義を述べる．まず，攻撃者による次のような攻撃シナリオを考える．

Stage 1: 鍵生成アルゴリズムが実行され，公開鍵と秘密鍵の対が生成される．当然，攻撃者は公開鍵のみ得ることができ，秘密鍵は取得できない．

Stage 2: 攻撃者は，一連の質問を復号オラクルに行う．それぞれの質問は，暗号文 C であり，復号オラクルは秘密鍵を用いてそれらを復号し，その復号結果は攻撃者に回答される．もし，復号オラクルが復号できなかった場合でもそのこと (復号結果）が攻撃者に通知される．攻撃者は質問 C をどのように作ってもよく，C に関しては何の制約もない．

Stage 3: 攻撃者は，暗号オラクルを実行させる（必要に応じて，オプション情報を入力する）．暗号オラクルは以下のように動作する．

1. 暗号アルゴリズムを実行し，鍵と暗号文の対 (K^*, C^*) を生成する．
2. K^* と同じ長さのビット列（もしくはオクテット列）$\tilde{K}$ を一様にランダムに生成する．
3. $b \in \{0,1\}$ をランダムに選ぶ．
4. $b = 0$ ならば，(K^*, C^*) を出力し，さもなければ $(\tilde{K}, C^*)$ を出力する．

Stage 4: 攻撃者は，さらに一連の暗号文 C を復号オラクルに質問し続けることができる．ただし，$C \neq C^*$（つまり，C^* だけは質問することができないが，それ以外には何を質問してもよい）．

Stage 5: 攻撃者が，最終的に $\hat{b} \in \{0,1\}$ を出力し，停止する．

以上が，攻撃者の攻撃のシナリオである．

このシナリオにおける 攻撃者 A のアドバンテージ $\mathrm{Advantage}_{KEM}(A)$ は, $2 \cdot \left|\Pr[\hat{b} = b] - 1/2\right|$ で定義される．妥当な時間で実行する全ての攻撃者に対して，$\mathrm{Advantage}_{KEM}(A)$ が（セキュリティパラメータに関して）無視できる（十分に小さい）とき，KEM を「適応的選択暗号文攻撃に対して識別不可能（IND-CCA2-KEM)」（もしくは，単に「安全である」）と呼ぶ．

公開鍵暗号（PKE）では，識別不可能性（IND）よりも定義的により安全性の高い頑強性（NM: non-malleability）が定義されるが，KEM に対しても同様に定義され，公開鍵暗号と同様に IND-CCA2-KEM と NM-CCA2-KEM が等価であることが示されている[6]．

8-3-2 DEM

次に, 共通鍵暗号を定式化したデータカプセル化メカニズム（Data Encapsulation Mechanism: DEM）について述べよう．前に述べたように，DEM に対しても「適応的選択暗号文攻撃に対して識別不可能性」が定義でき IND-CCA2-DEM と記述する．

DEM は共通鍵暗号方式であり，鍵生成と暗号化アルゴリズムおよび復号化アルゴリズムからなる．暗号化アルゴリズムは鍵 K，平文 m を入力とし，暗号文 C を出力するアルゴリズムで，C が送信される．復号化アルゴリズムは，鍵 K と暗号文 C を入力として，平文 m を出力するアルゴリズムである．

DEM の安全性は，IND-CCA2-PKE の定義の DEM 版である IND-CCA2-DEM により定義される．つまり，攻撃者は，同じ長さの 2 つの平文 M_0, M_1 を選び，それを暗号オラクルに送る．暗号オラクルは，ランダムに鍵 K とランダムビット b を選び，M_b と L^* を鍵 K を用いて C^* に暗号化し，それを攻撃者に送る．攻撃者は，$C \neq C^*$ でないような一連の C を復号オラクルに送り，鍵 K を用いて復号した結果をもらう（これは，C^* をもらう前後で何回でも行ってよい）．最終的に，攻撃者は $\hat{b}$ を出力する．$2 \cdot \left|\Pr[\hat{b} = b] - 1/2\right|$ を攻撃者のアドバンテージ $\mathrm{Advantage}_{DEM}(A)$ と定義し，これがセキュリティパラメータに関して十分に小さいとき，DEM は IND-CCA2-DEM であるとする．

KEM-DEM で IND-CCA2 安全なハイブリッド暗号を構成するためには，IND-CCA2-KEM 安全な KEM と IND-CCA2-DEM 安全な DEM があれば十分であり，DEM の安全性としては，IND-CCA2-DEM 安全性のみを考慮すればいいが，それ以外に以下のようなことが知ら

れている．

公開鍵暗号（PKE）や KEM と同様に，DEM においても頑強性（NM: non-malleability）が定義される．ところが意外なことに，DEM においては，PKE および KEM とは状況が異ることが知られている[4]．（ただし，7) では，DEM は確定的暗号として定式化しているが，4) では，DEM を確率的暗号として定式化していることに注意.）

PKE や KEM では，選択平文攻撃（CPA）は，公開鍵を用いて誰でもできるため，受動的な攻撃に分類される．ところが，DEM においては，公開鍵に相当する鍵が存在せず，鍵は秘密の共通鍵のみであるため，暗号化オラクルへの問い合わせである選択平文攻撃（CPA）および復号化オラクルへの問い合わせである選択暗号文攻撃（CCA）は，いずれも能動的攻撃となる．

さて, PKE と KEM においては, 2 種類の能動的攻撃である非適応的選択暗号文攻撃（CCA1）と適応的選択暗号文攻撃（CCA2）との間には攻撃能力に差があり，例えば，IND-CCA2-PKE と IND-CCA1-PKE が異なる（当然，IND-CCA2-PKE の方がより強い安全性を意味する）ことが示されている．しかし，DEM においては，2 種類の能動的攻撃である非適応的選択平文攻撃（CPA1）と適応的選択平文攻撃（CPA2）との間には攻撃能力に差がないことが示されている[4]．

また，PKE と KEM においては，頑強（NM）であることは必ず識別不可能（IND）であることを意味したが，DEM では，能動的攻撃に対して頑強（NM）であっても受動的攻撃に対してすら識別不可能（IND）でない場合が生じることが示されている[4]．

8-3-3 KEM-DEM ハイブリッド暗号の安全性

前に述べたように，国際標準化機構 ISO における公開鍵暗号の標準化作業の中で導入された枠組では，ハイブリッド暗号は，公開鍵暗号の鍵共有の機能を担う KEM と共通鍵暗号の機能を担う DEM を組み合わせることで実現される．そして，IND-CCA2-KEM である KEM を IND-CCA2-DEM である DEM と組み合わせてハイブリッド暗号を構成した場合，IND-CCA2-PKE である PKE が実現される[1]．（ここで，ハイブリッド暗号は，PKE として定義できることに注意.）したがって，ISO における枠組では，IND-CCA2 レベルの安全性を持った KEM と DEM を組み合わせてハイブリッド暗号を構成することが推奨されることになる．個々の KEM や DEM が IND-CCA2 レベルの安全性を保有していれさえすれば，どのような方式の KEM と DEM と組み合わせても安全なハイブリッド暗号が構成できるという意味で，このような推奨方式は ISO のような標準的枠組に適していると思われる．

■1 群 - 3 編 - 8 章

8-4 KEM の構成例：PSEC-KEM

（執筆者：岡本龍明）[2019 年 1 月 受領]

前に述べたように，公開鍵暗号に基づく鍵共有機能が KEM として定式化され，そのコンセプトに基づき，いくつかの方式が設計されている．ここでは，楕円曲線上で KEM を実現した PSEC-KEM を紹介する．PSEC-KEM は，2001 年に NTT により提案された方式であり，楕円ディフィ（Diffie）・ヘルマン（Hellman）鍵共有法とワンパッド暗号に藤崎-岡本変換[3] を用いて KEM として構成したものである（ISO で標準化され，欧州連合の暗号評価プロジェクト NESSIE で公開鍵暗号の第一推薦アルゴリズムとして認定されている）．

【鍵生成】 楕円ディフィ・ヘルマン鍵共有法に基づき，システムパラメータ $\{E(F),G,l\}$（$E(F)$ は有限体 F 上の楕円曲線，G は $E(F)$ 上の点であり，l は G の位数）及び公開鍵 $P_A = x_A G$ と秘密鍵 $x_A \in \{0,\ldots,l-1\}$ のペアを生成する（群演算は加法で表記）．さらに，ハッシュ関数 $H_1 : \{0,1\}^* \to \{0,1\}^{L_h}$ および $H_2 : \{0,1\}^* \to \{0,1\}^{L_g}$（理論的には，理想的ランダム関数と仮定）を公開する．

【暗号化】

乱数 $r \in \{0,1\}^{L_h}$ を生成し，$t||K = H_2(r)$, $\alpha = t \bmod l$, $Q = \alpha P_A$, $C_1 = \alpha G$, $C_2 = r \oplus H_1(C_1||Q)$ を計算し，(C_1,C_2) を暗号文とする．このとき，K が共有鍵となる．

【復号】

$Q' = x_A C_1$, $r' = C_2 \oplus H_1(C_1||Q')$, $t'||K' = H_2(r')$, $\alpha' = t' \bmod l$ を計算し，$C_1 = \alpha' G$ が成立するかどうかを検証し，成立すれば K' を共有鍵として出力する．

PSEC-KEM は，楕円曲線上の計算 DH 問題が困難でありハッシュ関数 H_1 および H_2 が理想的なランダム関数（ランダムオラクル）と仮定すると，（KEM の意味で）適応的選択暗号文攻撃に対して識別不可能（IND-CCA2-KEM）である．

■参考文献

1) Cramer, R. and Shoup, V.: Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack, SIAM Journal of Computing, 33, 1, pp.167–226 (2003).
2) Diffie, W. and Hellman, M.: New Directions in Cryptography,IEEE Trans. on Information Theory, IT-22, 6, pp.644–654 (1976).
3) Fujisaki, E. and Okamoto, T.: Secure Integration of Asymmetric and Symmetric Encryption Schemes, Jouranla of Cryptology, 26, 1, pp.80–101 (2013)
4) Katz, J. and Yung, M.: Complete Characterization of Security Notions for Probabilistic Private-Key Encryption, Proceedings of STOC 2000, ACM, pp.245–254 (2000).
5) Kurosawa, K. and Desmedt, Y.: A New Paradigm of Hybrid Encryption Scheme, Proc. of Crypto'04, Springer-Verlag, LNCS 3152, pp. 426–442 (2004).
6) Nagao, W., Manabe, Y. and Okamoto, T.: On the Equivalence of Several Security Notions of KEM and DEM, IEICE Transactions, 91-A, 1, pp.283–297 (2008)
7) Shoup, V.: A Proposal for an ISO Standard for Public Key Encryption (v.2.1). ISO/IEC JTC1/SC27, N2563, http://shoup.net/papers/ (2001).