SCIS 2004 The 2004 Symposium on Cryptography and Information Security
Sendai, Japan, Jan.27-30, 2004
The Institute of Electronics, Information and Communication Engineers

ハイブリッド暗号の安全性について
On the Security of Hybrid Public-Key Encryption

長尾 若* 真鍋 義文*† 岡本 龍明*‡
Waka Nagao Yoshifumi Manabe Tatsuaki Okamoto

あらまし 公開鍵暗号を用いて秘密鍵暗号のための鍵配送を行い，その秘密鍵を用いてデータの暗号化を行なう方式は従来用いられていたが，Shoupはこの方式を鍵共有(KEM)とデータの暗号化(DEM)を組み合わせたハイブリッド暗号というフレームワークで定式化を行ない，現在ではこれが広く認められつつある．このような背景や暗号の重要性を踏まえ，ISOでは暗号に関して理論的安全性を考慮しつつ標準化を進めている．KEMにおける理論的安全性に関しては，今まで強秘匿(IND)性のみが研究され，頑強(NM)性に関しては研究がされていない．そこで本稿では，公開鍵暗号において定義されている3つのNM性に対応した形で，KEMにおいて新たなNM性を定義する．そして，新たに定義した3つのNM性が等価であることを証明し，KEMにおけるIND-CCA2とNM-CCA2との等価性を証明する．

キーワード KEM, DEM, ハイブリッド暗号, IND, NM

1 はじめに

現在の情報化社会においてハイブリッド暗号は広く使われているが，公開鍵暗号を鍵配送に特化した鍵共有(KEM)とデータの暗号化(DEM)という2つのフレームワークからなるハイブリッド暗号系がShoupによって定式化され，新たに提案されている．そして，ISOを中心にこのフレームワークでのハイブリッド暗号系の標準化が進められており[1]，欧州連合(EU)の暗号評価プロジェクトNESSIEにおいてもKEMに基づく方式が採用されている[2]．ハイブリッド暗号の安全性はKEMとDEMの安全性により定義されるが，KEMは公開鍵暗号を鍵配送に特化したものであるため，公開鍵暗号の安全性と同様に定式化される．公開鍵暗号の安全性は一般に暗号系に対する攻撃の種類と暗号系が耐えうる安全性レベルの組によってなされ，攻撃には受動的な攻撃法(CPA)と能動的な攻撃法(CCA1およびCCA2)などがあり，安全性レベルには一方向(OW)性，強秘匿(IND)性，頑強(NM)性[3]~[5]が定義されている．現在，KEMにおいてはOWおよびINDのみが定義され，NMに該当するものが定義されていない．そこで，本稿では公開鍵暗号において定義されている3つのNM性に対応した，KEMにおける3つのNM性を新たに定義し，それらが等価であることを証明する．また，公開鍵暗号系と同じく，KEMにおいてもIND-CCA2とNM-CCA2とが等価であることを証明する．

2 ハイブリッド暗号

公開鍵暗号方式には，暗号化・復号化に非常に長い時間がかかるというデメリットがある．これに対し共通鍵暗号方式には高速に暗号化・復号化が行えるというメリットがある．これらを考慮して公開鍵暗号方式を鍵配送のみに利用し，共通鍵暗号方式をデータの送受信に利用する仕組みが考えられた．これがハイブリッド暗号である．ハイブリッド暗号はRSA暗号などの各暗号系で独自に構築されてきたが，Shoup[1]によりKEMとDEMによるハイブリッド暗号が新たに提案され，広く認められつつある．KEMは鍵共有における初めての定式化であり，ハイブリッド暗号のみならずハイブリッドメッセージ認証，ハイブリッド相手認証等への応用も含めた鍵共有の一般的な定式化となっている．つまり，KEMはDEMと全く独立な概念であり(DEMの存在可能性などに全く関係なく)，鍵共有の一般的な定式化となっている．KEMとDEMによるフレームワークはKEMおよびDEMの望ましい安全性を満足すれば暗号系が異なってもそれらを組み合わせて安全なハイブリッド暗号を構築可能であることを意味する．以下では，ISOにおけるKEMの定義とその安全性を紹介する．

* 京都大学大学院情報学研究科社会情報学専攻〒606-8501 京都市左京区吉田本町 Department of Social Informatics, Graduate School of Informatics, Kyoto University Yoshidahonmachi, Sakyo-ku, Kyoto-shi, Japan, w-nagao@lab7.kuis.kyoto-u.ac.jp
† NTTサイバースペース研究所〒239-0847 横須賀市光の丘1-1 NTT Cyber Space Laboratories 1-1 Hikarinooka, Yokosuka-shi, Japan, manabe.yoshifumi@lab.ntt.co.jp
‡ NTT情報流通プラットフォーム研究所〒239-0847 横須賀市光の丘1-1 NTT Information Sharing Platform Laboratories 1-1 Hikarinooka, Yokosuka-shi, Japan, okamoto@sucaba.isl.ntt.co.jp

2.1 KEM

KEMとは二者X,Yの間において鍵Kを共有するために公開鍵暗号を鍵配送に特化させた手法である．ISOではKEMのスキームΠ_Kを以下のように定義している．

1. 鍵生成アルゴリズム$KEM.KeyGen()$により，公開鍵PKと秘密鍵SKとのペア(PK, SK)を生成する
2. 暗号化アルゴリズム$KEM.Encrypt()$はPKを入力として，共有するための鍵Kとその暗号文C_0のペア(K, C_0)を出力する
3. 復号化アルゴリズム$KEM.Decrypt()$はSKと暗号文C_0を入力として鍵K，もしくは$\perp$を出力する($\perp$は正しい暗号文ではないことを表す)

鍵Kを共有する二者X,Yの間で，XからYへと鍵Kを配送するものとする．まず事前にYは公開鍵と秘密鍵のペア(PK_Y, SK_Y)を$KEM.KeyGen()$により生成し，PK_Yを公開しておく．Yに鍵配送をしたい場合には，Xが公開されているPK_Yを入力とし，$KEM.Encrypt()$を用いて(K, C_0)を出力する．XはKを所有し，C_0をYへと配送する．YはC_0と自身の秘密鍵SK_Yを入力とする$KEM.Decrypt(SK_Y, C_0)$により鍵Kを得る．このように二者X,Y間において鍵Kを共有することが出来る．

KEMにおいて定義されているIND-CCA2の安全性は，攻撃者Aに対して次のゲームを考えて定義される．まず，$KEM.KeyGen()$により公開鍵と秘密鍵のペア(PK, SK)を生成する．このPKにより攻撃者以外の第三者(暗号化オラクル)が$KEM.Encrypt(PK)$を用いて鍵K^*とその暗号文C_0^*のペア(K^*, C_0^*)を作成する．暗号化オラクルは鍵K^*と同じ長さの偽の鍵$\widetilde{K}$も生成する．ここで，二つの鍵のどちらか一方を暗号化オラクルが選択し，暗号文C_0^*とのペアをAに与える．さらにAにはPKが与えられている．攻撃者Aは次に暗号文を復号化する復号化オラクルにC_0^*ではない暗号文$C[i](i = 1, 2, \cdots, n)$を送る．復号化オラクルはそれらを復号化し，平文$P[i]$をAに返す．Aはこの情報をもとに，暗号化オラクルがどちらの鍵を選択したのかをあてる．

3 Non-Malleable

Non-Malleable(NM)性とは公開鍵暗号系において定義された安全性の一つであり頑強性と呼ばれる．公開鍵暗号系においてNM性を持つとは，二つの平文xとx'間で成り立つある非自明な関係$R(x, x')$があり，これに対してxの暗号文Cから$R(x, x')$を満足するx'の暗号文C'を生成することが困難であることをいう(自明とは例えばxとx'の長さが等しいなどがある)．関係Rにはビット反転などがある．もし，このNM性が満たされなければ，攻撃者がネットワーク上に流れる暗号文を改ざんし，特定の関係を持つ暗号文を生成することが可能である．例えば，送信者が重要な契約書にYesという内容の返事を暗号化して送信した時，攻撃者がNoという内容の暗号文に改ざんして受信者に送ることができる．以上は公開鍵暗号についての危険性であるが，KEMにおいてNM性が満足されていない場合にも，鍵を書き換える事が出来るので，特定の関係を持つ鍵に改ざんされる可能性があり，何らかの危険性を生じる恐れがある．よって，KEMにおけるNM性を定義することは非常に重要なことである．

公開鍵暗号系では，Dolev，Dwork，Naorによる NM性[3](以下，SNM-PKEと呼ぶ)，Bellare，Desai，Pointcheval，Rogawayによる NM性[5](以下，CNM-PKEと呼ぶ)，Bellare，Sahaiによる Parallel attackを用いたNM性[4](以下，PNM-PKEと呼ぶ) が定義され，それらの間に等価性が成り立つことが証明されている．

本稿では，ハイブリッド暗号のKEMにおいて新たなNM性を公開鍵暗号の定義に対応した形で3つ定義し，それらにおいて等価性が成り立つことを証明する．各定義はISOにおけるKEMのスキームΠ_Kをもとに定義している．さらに攻撃の種類atkは選択平文攻撃(cpa)，選択暗号文攻撃(cca1)，適応的選択暗号文攻撃(cca2)のいずれかを示し，cpa,cca1,cca2の各攻撃にパラレル攻撃[4]を加えた時の攻撃をそれぞれpa0,pa1,pa2で表す．ここでパラレル攻撃とは，復号化オラクルに対して一度だけ暗号文を送ることができる攻撃法である．定義では，攻撃者やシミュレータの復号化オラクルをO_1, O_2で表し，その復号化アルゴリズム$KEM.Decrypt(SK, \cdot)$は$D_{sk}(\cdot)$で表す．またεは復号化オラクルを参照しないことを表す．次に，セキュリティパラメータをz，平文と暗号文ベクトルにおける関係をRで表し，鍵空間を$\mathcal{K}$，状態情報をsとする．

以下で，SNM-PKEの考えに対応したKEMにおけるNM性(以下，SNM-KEMと呼ぶ)，CNM-PKEの考えに対応したKEMにおけるNM性(以下，CNM-KEMと呼ぶ)，PNM-PKEの考えに対応したKEMにおけるNM性(以下，PNM-KEMと呼ぶ)の3つの定義を示す．

3.1 SNM-KEM

図1に定義を示す．Π_Kにおける攻撃者を$A = (A_1, A_2)$，シミュレータを$S = (S_1, S_2)$とするとき，攻撃者AにおけるSNM-KEMの安全性は，アドバンテージ$Adv^{snm-atk}_{A,S,\Pi_K}(R, z)$で定義される．全ての多項式で表される攻撃アルゴリズムの実行時間$p(z)$において，全ての関係Rと全ての攻撃者Aに対して$Adv^{snm-atk}_{A,S,\Pi_K}(R, z)$が無視できるくらい小さくなるSが存在するとき，SNM-KEMは安全であるという．$Adv^{snm-atk}_{A,S,\Pi_K}(R, z)$は暗号文$C_0^*$を受け取る攻撃者のアルゴリズム$Expt^{snm-atk}_{A,\Pi_K}(R, z)$

図 1: SNM-KEM Definition

$$
\begin{aligned}
Adv^{snm-atk}_{A,S,\Pi_K}(R,z) &\equiv \Pr[Expt^{snm-atk}_{A,\Pi_K}(R,z)=1] \\
&- \Pr[Expt^{snm-atk}_{S,\Pi_K}(R,z)=1]
\end{aligned}
$$

---

where

$Expt^{snm-atk}_{A,\Pi_K}(R,z)$

$$
\begin{aligned}
(pk,sk) &\leftarrow KEM.KeyGen(1^z) \\
(\mathcal{K},s_1) &\leftarrow A_1^{O_1}(pk) \\
(K^*,C_0^*) &\leftarrow KEM.Encrypt(pk) \ \wedge \ K^*\in\mathcal{K} \\
(\boldsymbol{C}_{\mathrm{o}},s_2) &\leftarrow A_2^{O_2}(s_1,C_0^*) \\
\boldsymbol{K} &\leftarrow KEM.Decrypt(sk,\boldsymbol{C}_{\mathrm{o}})
\end{aligned}
$$

return 1 iff $(C_0^* \notin \boldsymbol{C}_{\mathrm{o}}) \ \wedge \ R(K^*,\boldsymbol{K},\mathcal{K},s_2)$

$Expt^{snm-atk}_{S,\Pi_K}(R,z)$

$$
\begin{aligned}
(pk,sk) &\leftarrow KEM.KeyGen(1^z) \\
(\mathcal{K},s_1) &\leftarrow S_1^{O_1}(pk) \\
K^* &\leftarrow \mathcal{K} \\
(\boldsymbol{C}_{\mathrm{o}},s_2) &\leftarrow S_2^{O_2}(s_1) \\
\boldsymbol{K} &\leftarrow KEM.Decrypt(sk,\boldsymbol{C}_{\mathrm{o}})
\end{aligned}
$$

return 1 iff $R(K^*,\boldsymbol{K},\mathcal{K},s_2)$
and
If $atk = cpa$ then $O_1=\varepsilon$ and $O_2=\varepsilon$.
If $atk = cca1$ then $O_1=D_{sk}(\cdot)$ and $O_2=\varepsilon$.
If $atk = cca2$ then $O_1=D_{sk}(\cdot)$ and $O_2=D_{sk}(\cdot)$.

が成功する時の確率とそれを受け取れないシミュレータのアルゴリズム $Expt^{snm-atk}_{S,\Pi_K}(R,z)$ が成功する時の確率の差である．ただし，$\boldsymbol{K}$ は $\perp$ を含まない．SNM-PKE との違いは，$A_2^{O_2}$ と $S_2^{O_2}$ の出力に状態情報を出力させる点とシミュレータ S に復号化オラクルを利用できるようにした点である．

3.2 CNM-KEM

図2に定義を示す．Π_K における攻撃者を $A=(A_1, A_2)$ とするとき，CNM-KEM の安全性はアドバンテージ $Adv^{cnm-atk}_{A,\Pi_K}(z)$ で定義される．全ての多項式で表される攻撃アルゴリズムの実行時間 $p(z)$ において，$Adv^{cnm-atk}_{A,\Pi_K}(z)$ が無視できるくらい小さくなるとき，CNM-KEM は安全であるという．$Adv^{cnm-atk}_{A,\Pi_K}(z)$ は鍵 K^* の暗号文 C_0^* を受け取る攻撃者のアルゴリズム $Expt^{cnm-atk}_{A,\Pi_K}(z)$ が成功する時の確率と鍵 K^* ではない鍵 $\widetilde{K}$ の暗号文 $\widetilde{C_0}$ を受け取る攻撃者のアルゴリズム $\widetilde{Expt}^{cnm-atk}_{A,\Pi_K}(z)$ が成功する時の確率の差である．ただし，$\boldsymbol{K}$ は $\perp$ を含まない．

図 2: CNM-KEM Definition

$$
\begin{aligned}
Adv^{cnm-atk}_{A,\Pi_K}(z) &\equiv \Pr[Expt^{cnm-atk}_{A,\Pi_K}(z)=1] \\
&- \Pr[\widetilde{Expt}^{cnm-atk}_{A,\Pi_K}(z)=1]
\end{aligned}
$$

---

where

$Expt^{cnm-atk}_{A,\Pi_K}(z)$

$$
\begin{aligned}
(pk,sk) &\leftarrow KEM.KeyGen(1^z) \\
(\mathcal{K},s) &\leftarrow A_1^{O_1}(pk) \\
(K^*,C_0^*) &\leftarrow KEM.Encrypt(pk) \ \wedge \ K^*\in\mathcal{K} \\
(R,\boldsymbol{C}_{\mathrm{o}}) &\leftarrow A_2^{O_2}(s,C_0^*) \\
\boldsymbol{K} &\leftarrow KEM.Decrypt(sk,\boldsymbol{C}_{\mathrm{o}})
\end{aligned}
$$

return 1 iff $(C_0^* \notin \boldsymbol{C}_{\mathrm{o}}) \ \wedge \ R(K^*,\boldsymbol{K})$

$\widetilde{Expt}^{cnm-atk}_{A,\Pi_K}(z)$

$$
\begin{aligned}
(pk,sk) &\leftarrow KEM.KeyGen(1^z) \\
(\mathcal{K},s) &\leftarrow A_1^{O_1}(pk) \\
K^* &\leftarrow \mathcal{K} \\
(\widetilde{K},\widetilde{C_0}) &\leftarrow KEM.Encrypt(pk) \ \wedge \ \widetilde{K}\in\mathcal{K} \\
(R,\widetilde{\boldsymbol{C}_{\mathrm{o}}}) &\leftarrow A_2^{O_2}(s,\widetilde{C_0}) \\
\widetilde{\boldsymbol{K}} &\leftarrow KEM.Decrypt(sk,\widetilde{\boldsymbol{C}_{\mathrm{o}}})
\end{aligned}
$$

return 1 iff $(\widetilde{C_0} \notin \widetilde{\boldsymbol{C}_{\mathrm{o}}}) \ \wedge \ R(K^*,\widetilde{\boldsymbol{K}})$
and
If $atk = cpa$ then $O_1=\varepsilon$ and $O_2=\varepsilon$.
If $atk = cca1$ then $O_1=D_{sk}(\cdot)$ and $O_2=\varepsilon$.
If $atk = cca2$ then $O_1=D_{sk}(\cdot)$ and $O_2=D_{sk}(\cdot)$.

3.3 PNM-KEM

図3に定義を示す．Π_K における攻撃者を $A=(A_1, A_2)$ とするとき，PNM-KEM の安全性はアドバンテージ $Adv^{pnm-atk}_{A,\Pi_K}(z)$ で定義され，これが多項式で表される，A による攻撃アルゴリズムの実行時間 $p(z)$ において無視できるくらい小さいとき，PNM-KEM は安全であるという．定義において攻撃者 $A=(A_1,A_2)$，$A_2=(A_{2,q},A_{2,g})$ を考える．攻撃者 A_1 は，鍵空間 $\mathcal{K}$ と状態情報 s_1 を出力する．s_1 は $A_{2,q}$ へと渡す情報である．

$KEM.Encrypt(pk)$ は鍵 K^* とその暗号文 C_0^* のペア (K^*,C_0^*)(ただし，K^* は $\mathcal{K}$ の要素である) を出力する．

図 3: PNM-KEM Definition

$$Adv^{pnm-atk}_{A,\Pi_K}(z) \equiv \Pr[Expt^{pnm-atk}_{A,\Pi_K}(z)=1] - \frac{1}{2}$$

---

where
$Expt^{pnm-atk}_{A,\Pi_K}(z)$

$$\begin{aligned}
(pk, sk) &\leftarrow KEM.KeyGen(1^z)\\
(\mathcal{K}, s_1) &\leftarrow A_1^{O_1}(pk)\\
(K^*, C_0^*) &\leftarrow KEM.Encrypt(pk) \ \wedge \ K^* \in \mathcal{K}\\
\widetilde{K} &\leftarrow \mathcal{K}\\
b &\leftarrow \{0,1\}\\
X &\leftarrow \begin{cases} (K^*, C_0^*) \text{ if } b=0 \\ (\widetilde{K}, C_0^*) \text{ if } b=1 \end{cases}\\
(\boldsymbol{C}_{\rm o}, s_2) &\leftarrow A_{2,q}^{O_2}(s_1, X)\\
\boldsymbol{K} &\leftarrow KEM.Decrypt(sk, \boldsymbol{C}_{\rm o})\\
g &\leftarrow A_{2,g}^{O_2}(\boldsymbol{K}, s_2)
\end{aligned}$$

return 1 iff $(C_0^* \notin \boldsymbol{C}_{\rm o}) \ \wedge \ (g=b)$
and
If $atk = pa0$ then $O_1 = \varepsilon$ and $O_2 = \varepsilon$.
If $atk = pa1$ then $O_1 = D_{sk}(\cdot)$ and $O_2 = \varepsilon$.
If $atk = pa2$ then $O_1 = D_{sk}(\cdot)$ and $O_2 = D_{sk}(\cdot)$.

次に，$\mathcal{K}$ の要素であるもう一つの鍵 $\widetilde{K}$ を生成する．そして，ランダムに $b = \{0,1\}$ の値を選び，$b=0$ のとき (K^*, C_0^*) のペアを，$b=1$ のとき $(\widetilde{K}, C_0^*)$ のペアを X として出力する．$A_{2,q}$ は s_1 と X を受け取り，状態情報 s_2 と暗号文ベクトル $\boldsymbol{C}_{\rm o}$ を出力する．$A_{2,g}$ は s_2 と復号化オラクル $KEM.Decrypt(sk, \boldsymbol{C}_{\rm o})$ により出力される復号文ベクトル $\boldsymbol{K}$ を受け取り，g の値を出力する．ここで，暗号文ベクトル $\boldsymbol{C}_{\rm o}$ の中に C_0^* が含まれず，なおかつ $g=b$ であるとき，この攻撃者は攻撃に成功すると定義する．

攻撃者が以上のような振舞いで攻撃を行う時にアルゴリズム $Expt^{pnm-atk}_{A,\Pi_K}(z)$ が成功する確率と $\frac{1}{2}$ との差が無視できるくらい小さいとき，PNM-KEM は安全であるという．

4 各定義の等価性証明

前章では KEM における 3 つの新たな NM 性を定義したが，ここではそれらの間で成り立つ以下の定理について述べる．

定理 1 *CNM-KEM* $\Rightarrow$ *SNM-KEM*

定理 2 *SNM-KEM* $\Rightarrow$ *PNM-KEM*

定理 3 *PNM-KEM* $\Rightarrow$ *CNM-KEM*

それぞれの定理について，以下で証明を与える．

4.1 CNM-KEM ⇒SNM-KEM

SNM-KEM が安全でないと仮定して CNM-KEM が安全でないことを示す．SNM-KEM における攻撃者を $A = (A_1, A_2)$，シミュレータを $S = (S_1, S_2)$，CNM-KEM における攻撃者を $B = (B_1, B_2)$ とする．まず $Expt^{cnm-atk}_{B,\Pi_K}(z)$ が $Expt^{snm-atk}_{A,\Pi_K}(R,z)$ をシミュレートすることができることを示し，次に $Expt^{snm-atk}_{S,\Pi_K}(R,z)$ と $\widetilde{Expt}^{cnm-atk}_{B,\Pi_K}(z)$ のアルゴリズムが等しくなることを証明する．図 4 に $B_1^{O_1}$，$B_2^{O_2}$，$S_1^{O_1}$，$S_2^{O_2}$ の構成を示す．$B_1^{O_1}, B_2^{O_2}$ がそれ

図 4: CNM-KEM ⇒SNM-KEM

$Algorithm B_1^{O_1}(pk)$

$$(\mathcal{K}, s_1) \leftarrow A_1^{O_1}(pk)$$

return $(\mathcal{K}, (\mathcal{K}, s_1))$

$Algorithm B_2^{O_2}((\mathcal{K}, s_1), C_0^*)$

$$(\boldsymbol{C}_{\rm o}, s_2) \leftarrow A_2^{O_2}(s_1, C_0^*)$$

Define R' by $R'(a, \boldsymbol{b}) = 1$

iff $R(a, \boldsymbol{b}, \mathcal{K}, s_2) = 1$

return $(R', \boldsymbol{C}_{\rm o})$

$Algorithm S_1^{O_1}(pk)$

$$(\mathcal{K}, s_1) \leftarrow A_1^{O_1}(pk)$$

return $(\mathcal{K}, s_1)$

$Algorithm S_2^{O_2}(s_1)$

$$\begin{aligned}
(\widetilde{K}, \widetilde{C_0}) &\leftarrow KEM.Encrypt(pk) \ \wedge \ \widetilde{K} \in \mathcal{K}\\
(\widetilde{\boldsymbol{C}_{\rm o}}, s_2) &\leftarrow A_2^{O_2}(s_1, \widetilde{C_0})
\end{aligned}$$

return $(\widetilde{\boldsymbol{C}_{\rm o}}, s_2)$

ぞれ $A_1^{O_1}, A_2^{O_2}$ を用いることにより，$Expt^{cnm-atk}_{B,\Pi_K}(z)$ が $Expt^{snm-atk}_{A,\Pi_K}(R,z)$ をシミュレートすることができる．次に，$S_1^{O_1}, S_2^{O_2}$ を図 4 のように構成した時，$Expt^{snm-atk}_{S,\Pi_K}(R,z)$ と $\widetilde{Expt}^{cnm-atk}_{B,\Pi_K}(z)$ が等しくなる．

よって，

$$Adv^{cnm-atk}_{B,\Pi_K}(z) \geq Adv^{snm-atk}_{A,S,\Pi_K}(R,z)$$

が成り立つ．

4.2 SNM-KEM ⇒PNM-KEM

PNM-KEMが安全でないと仮定してSNM-KEMが安全でないことを示す．SNM-KEMにおける攻撃者を$A=(A_1,A_2)$，PNM-KEMにおける攻撃者を$B=(B_1,B_2)$，$B_2=(B_{2,q},B_{2,g})$とする．まず$Expt^{snm-atk}_{A,\Pi_K}(R,z)$が$Expt^{pnm-atk}_{B,\Pi_K}(z)$をシミュレートすることができることを示し，次に$Expt^{snm-atk}_{S,\Pi_K}(R,z)$が成功する時の確率が最大でも$\frac{1}{2}$となることを証明する．図5に$A_1^{O_1}$，$A_2^{O_2}$，Rの構成を示す．図5から$A_1^{O_1},A_2^{O_2}$，Rは$B$を用いて表すこ

図 5: SNM-KEM ⇒ PNM-KEM

$Algorithm A_1^{O_1}(pk)$

$$\begin{aligned}(\mathcal{K},t_1) &\leftarrow B_1^{O_1}(pk)\\ K_1 \leftarrow \mathcal{K} \;;\; K_2 &\leftarrow \mathcal{K}\\ \mathcal{K}' &= \{K_1,K_2\}\end{aligned}$$

Let $s_1=(\mathcal{K}',t_1,pk)$.
return $(\mathcal{K}',s_1)$

$Algorithm A_2^{O_2}(s_1,C_0^*)$ where $s_1=(\mathcal{K}',t_1,pk)$

$$\begin{aligned}X &\leftarrow (K_1,C_0^*)\\ (\boldsymbol{C}_{\rm o},t_2) &\leftarrow B_{2,q}^{O_2}(t_1,X)\end{aligned}$$

Choose random coins σ for $B_{2,g}$.

$$s_2 \leftarrow (t_2,\sigma)$$

return $(\boldsymbol{C}_{\rm o},s_2)$

$Relation R(K^*,\boldsymbol{K},\mathcal{K},s_2)$ where $s_2=(t_2,\sigma)$
Let $b\in 0,1$.
If $K^*=K_1$, then $b=0$. Otherwise, $b=1$.
return 1 iff $B_{2,g}^{O_2}(\boldsymbol{K},t_2;\sigma)=b$

とができ，$Expt^{snm-atk}_{A,\Pi_K}(R,z)$が$Expt^{pnm-atk}_{B,\Pi_K}(z)$をシミュレートすることができる．次に，$Expt^{snm-atk}_{S,\Pi_K}(R,z)$が成功する確率が最大でも$\frac{1}{2}$となることを証明する．$Expt^{pnm-atk}_{B,\Pi_K}(z)$の第三者が選択する$b$の値に対して，$Expt^{snm-atk}_{S,\Pi_K}(R,z)$がbを出力する確率を$p_b$とする．$p_b$は$Expt^{snm-atk}_{S,\Pi_K}(R,z)$と$Expt^{pnm-atk}_{B,\Pi_K}(z)$が独立であるので，$p_0+p_1\leq 1$である．$Expt^{snm-atk}_{S,\Pi_K}(R,z)$が成功する確率は，

$$\begin{aligned}&\Pr[Expt^{snm-atk}_{S,\Pi_K}(R,z)=1]\\ &= (p_0\times\Pr[b=0]+p_1\times\Pr[b=1])\\ &\leq (p_0\times\frac{1}{2}+p_1\times\frac{1}{2})\\ &\leq (p_0+p_1)\times\frac{1}{2}\\ &\leq \frac{1}{2}\end{aligned}$$

となる．

よって，$Adv^{snm-atk}_{A,S,\Pi_K}(R,z)$と$Adv^{pnm-atk}_{B,\Pi_K}(z)$との間の関係は以下のようになる．

$$\begin{aligned}Adv^{pnm-atk}_{B,\Pi_K}(z) &= \Pr[Expt^{pnm-atk}_{B,\Pi_K}(z)=1]-\frac{1}{2}\\ &\leq \Pr[Expt^{snm-atk}_{A,\Pi_K}(R,z)=1]\\ &\quad -\frac{1}{2}+\epsilon(z)\\ &\leq \Pr[Expt^{snm-atk}_{A,\Pi_K}(R,z)=1]\\ &\quad -\Pr[Expt^{snm-atk}_{S,\Pi_K}(R,z)=1]\\ &\quad +\epsilon(z)\\ &\leq Adv^{snm-atk}_{A,S,\Pi_K}(R,z)+\epsilon(z)\end{aligned}$$

$\epsilon(z)$は無視できる程小さいので，

$$Adv^{snm-atk}_{A,S,\Pi_K}(R,z)\geq Adv^{pnm-atk}_{B,\Pi_K}(z)$$

が成り立つ．

4.3 PNM-KEM ⇒CNM-KEM

CNM-KEMが安全でないと仮定してPNM-KEMが安全でないことを示す．PNM-KEMにおける攻撃者を$A=(A_1,A_2),A_2=(A_{2,q},A_{2,g})$，CNM-KEMにおける攻撃者を$B=(B_1,B_2)$とする．図6に$A_1^{O_1}$，$A_{2,q}^{O_2}$，$A_{2,g}^{O_2}$の構成を示す．$Expt^{pnm-atk}_{A,\Pi_K}(z)$におけるXにおいて，第3者がb=0を選択すると，Xは鍵K^*とその暗号文C_O^*のペア(K^*,C_O^*)となる．このとき，CNM-KEMの$Expt^{cnm-atk}_{B,\Pi_K}(z)$のアルゴリズムと対応する．また，b=1のとき，XはK^*ではない鍵$\widetilde{K}$と暗号文C_O^*のペア$(\widetilde{K},C_O^*)$となり，CNM-KEMでは$(\widetilde{K},C_O^*)$のように鍵と暗号文のペアが対応していない$\widetilde{Expt}^{cnm-atk}_{B,\Pi_K}(z)$に相当するアルゴリズムになる．ゆえに，図6のように構成することにより，$Expt^{pnm-atk}_{A,\Pi_K}(z)$は$Expt^{cnm-atk}_{B,\Pi_K}(z)$と$\widetilde{Expt}^{cnm-atk}_{B,\Pi_K}(z)$の両方をシミュレートすることができる．よって，$\Pr[Expt^{pnm-atk}_{A,\Pi_K}(z)=1]$は，

$$\begin{aligned}&\Pr[Expt^{pnm-atk}_{A,\Pi_K}(z)=1]\\ &= \Pr[b=0]\times\Pr[b=0\wedge g=0]\\ &\quad +\Pr[b=1]\times\Pr[b=1\wedge g=1]\\ &= \frac{1}{2}\times\{\Pr[Expt^{cnm-atk}_{B,\Pi_K}(z)=1]\times 1\\ &\quad +(1-\Pr[Expt^{cnm-atk}_{B,\Pi_K}(z)=1])\times\frac{1}{2}\}\\ &\quad +\frac{1}{2}\times\{\Pr[\widetilde{Expt}^{cnm-atk}_{B,\Pi_K}(z)=1]\times 0\end{aligned}$$

図 6: PNM-KEM ⇒CNM-KEM

$Algorithm A_1^{O_1}(pk)$

$$(\mathcal{K}, t) \leftarrow B_1^{O_1}(pk)$$
$$s_1 \leftarrow (\mathcal{K}, t)$$

return $(\mathcal{K}, s_1)$

$Algorithm A_{2,q}^{O_2}(s_1, X)$ where $s_1 = (\mathcal{K}, t)$

$$(R, \boldsymbol{C}_{\rm o}) \leftarrow B_2^{O_2}(t, C_0^*)$$
$$s_2 \leftarrow (R, X, \boldsymbol{C}_{\rm o})$$

return $(\boldsymbol{C}_{\rm o}, s_2)$

$Algorithm A_{2,g}^{O_2}(\boldsymbol{K}, s_2)$

where $s_2 = (R, X, \boldsymbol{C}_{\rm o})$

If $(C_0^* \notin \boldsymbol{C}_{\rm o}) \ \wedge \ R(K^*, \boldsymbol{K})$

$$\text{then } g \leftarrow 0$$
$$\text{else } g \leftarrow \{0,1\}$$

return g

$$+(1-\Pr[\widetilde{Expt}_{B,\Pi_K}^{cnm-atk}(z)=1])\times\frac{1}{2}\}$$
$$= \frac{1}{4}(\Pr[Expt_{B,\Pi_K}^{cnm-atk}(z)=1] - \Pr[\widetilde{Expt}_{B,\Pi_K}^{cnm-atk}(z)=1]) + \frac{1}{2}$$

となる．よって，

$$\Pr[Expt_{A,\Pi_K}^{pnm-atk}(z)=1] - \tfrac{1}{2} = \frac{1}{4}(\Pr[Expt_{B,\Pi_K}^{cnm-atk}(z)=1] - \Pr[\widetilde{Expt}_{B,\Pi_K}^{cnm-atk}(z)=1])$$

と変形し，

$$Adv_{A,\Pi_K}^{pnm-atk}(z) = \frac{1}{4} Adv_{B,\Pi_K}^{cnm-atk}(z)$$

が成り立つ．

以上のように，定理1∼3が証明される．よって，SNM-KEM，CNM-KEM，PNM-KEMは互いに等価であることが証明される．また，公開鍵暗号においてはIND-CCA2-PKEとNM-CCA2-PKEは等しいことが証明されているが，KEMにおいても以下の定理が成り立つ．

定理 4 *IND-CCA2-KEM ⇔ NM-CCA2-KEM*

これは，まずPNM-CCA2-KEMとIND-CCA2-KEMが各定義から等しくなり，次に4章で証明した各定義の等価性によりNM-CCA2-KEMとIND-CCA2-KEMは等しくなる．

5 おわりに

ISOを中心として新たにハイブリッド暗号に関する標準化案が議論されている．現在，KEMに対してはIND性のみが定義されていたが，本稿ではNM性について3つの定義を新たに定義した．そして，それらの間に等価性が成り立つことを証明し，IND-CCA2-KEMとNM-CCA2-KEMが等しいことを述べた．今後はハイブリッド暗号におけるもう一つのフレームワークであるDEMに関するNM性に関しても検討を行う．

参考文献

[1] V.Shoup, “A Proposal for an ISO Standard for Public Key Encryption (version 2.1), ”manuscript, December 20, 2001.

[2] NESSIE, http://cryptonessie.org.

[3] D.Dolev, C.Dwork, and M.Naor, “Non-Malleable Cryptography, ”Proceedings of the 23rd Annual Symposium on Theory of Computing, ACM, 1991. Also Technical Report CS95-27, Weizmann Institute of Science, 1995.

[4] M.Bellare and A.Sahai, “Non-Malleable Encryption: Equivalence between Two Notions, and an Indistinguishability-Based Characterization, ”Advances in Cryptology-Crypt’99 Proceedings, Lecture notes in computer science Vol.1666, M.Winer ed., Springer-verlag, 1999.

[5] M.Bellare, A.Desai, D.Pointcheval, and P.Rogaway, “Relations Among Notions of Security for Public-Key Encryption Schemes, ”Advances in Cryptology-Crypt’98 Proceedings, Lecture notes in computer science Vol. 1462, H.Krawczyk ed., Springer-verlag, 1998.