单双钥混合体制的选择密文安全性

陈　原　　董庆宽　　肖国镇
(西安电子科技大学 ISN 综合业务网国家重点实验室　西安　710071)

摘　要：该文主要讨论单双钥混合体制的选择密文安全性 IND-CCA 的定义和相关结论。在对两种不同用途的单双钥混合体制及其安全性的研究之后发现它们的 IND-CCA 定义中允许敌手访问的预言机不同，我们将其统一为：对只能询问混合体制整体解密机的敌手的安全性，从而统一了混合体制的安全结论，为正确使用混合体制提供了依据。我们提出了一种混合体制：REACT+，并证明了其 IND-CCA 安全性。

关键词：混合体制，选择密文安全性，密码学
中图分类号：TN918.1　　**文献标识码**：A　　**文章编号**：1009-5896(2005)04-0612-05

Chosen Ciphertext Security of Hybrid Schemes of Symmetric and Asymmetric Encryption

Chen Yuan　　Dong Qing-kuan　　Xiao Guo-zhen
(*National Key Lab of Integrated Service Network* , *Xidian University*, *Xi'an* 710071, *China*)

Abstract　The definition and related conclusions of chosen ciphertext security IND-CCA (INDistinguishability against adaptive-Chosen Ciphertext Attack) of hybrid encryption of symmetric and asymmetric encryption are discussed. Having studied two kinds of hybrid encryptions of different use and their security definitions, it is found that there is a difference in the oracles. Then the definition of IND-CCA is unified as security for the adversaries can only access the whole decryption oracle of hybrid schemes, which makes the unification of security conclusions of hybrid schemes possible, and supplies the ground for proper use of hybrid schemes. A hybrid scheme called REACT+ has been proposed with its security proof.

Key words　Hybrid scheme, Chosen ciphertext security, Cryptology

1　引言

选择密文安全性是现代密码学中的一个重要问题，虽然在一般情况下因为敌手无法询问解密机而无需考虑这一安全性，但是在很多密码学应用环境中高安全水平的体制必须达到该安全性。对适应性选择密文攻击的不可区分性(INDistinguishability against adaptive-Chosen Ciphertext Attack, IND-CCA)被证明是对选择密文安全性的一个良好定义，本文将采用该定义。

单双钥混合体制在实际中有很多应用，本文将考虑这种体制的选择密文安全性。最初采用混合体制的目标是在用单钥体制传输加密数据的同时将密钥发送给数据接收者，即用双钥体制传送单钥体制的密钥，单钥体制用该密钥加密消息。我们把这种用途的混合体制称为混合体制 1。最近文献[1]中提出了混合体制 1 中双钥体制 IND-CCA 保留的安全性定义，并且给出了混合体制 1 的 IND-CCA 定义。为了使双钥加密的消息空间不受限，并且使其达到 IND-CCA，人们也采用单双钥混合的方法，我们把这种用途的混合体制称为混合体制 2。Okamoto 等人提出的 REACT[2]是混合体制 2 的典型范例。我们希望能找到两种混合体制之间的联系。深入研究之后，我们发现两者的 IND-CCA 安全性定义不同：前者允许敌手对分开询问组成混合体制的单双钥体制的解密机，而后者必须是对整体混合体制的解密机询问。在前者中，敌手既然可以单独询问双钥体制的解密机，就可以对其进行选择密文攻击，如果能得到私钥，就可以攻破混合体制 1。因此，我们将混合体制 IND-CCA 安全性统一为攻击者只能询问整体解密机，从而统一与混合体制有关的安全性结论，找到使用混合体制的正确方法。

文中第 2 节将介绍一些基础知识；第 3 节简要介绍两种混合体制、相关定义和结论；第 4 节指出两种混合体制的安全性定义不相同，并统一定义；第 5 节在该定义的基础上给

2003-08-25 收到，2004-07-19 改回
国家部级基金（41001040102）资助课题

出混合体制的一些安全结论和其它有用结果，并提出一种新的方案 REACT+；第 6 节对全文小结并提出需要解决的问题。

2　基础知识

双钥加密方案由 3 个多项式时间算法构成，记为 AS=(AK,AE,AD)： AK (1^k)生成公私钥对 (pk, sk)；加密算法 $\mathrm{AE}_{\mathrm{pk}}(m)$ 加密给定消息 m，得到密文 c；解密算法 $\mathrm{AD}_{\mathrm{sk}}(c)$ 解密密文 c。

本文涉及到的关于双钥体制的安全性有 IND-CCA[3]和对明文检测攻击的单向性(One-Wayness against Plaintext-Checking Attack, OW-PCA)[2]。OW-PCA 比 IND-CCA 弱，这里不做描述。

定义 1　(AS 的 IND-CCA)　m 设 AS= (AK, AE, AD) 是一个双钥加密方案，称 AS 是 IND-CCA 的，如果对于所有合法的多项式时间敌手 $A=(A_1,A_2)$，

$$\mathrm{Adv}^{\text{ind-cca}}_{\mathrm{AS},A}(k)=\Pr[\mathrm{Exp}^{\text{ind-cca-1}}_{\mathrm{AS},A}(k)=1]-\Pr[\mathrm{Exp}^{\text{ind-cca-0}}_{\mathrm{AS},A}(k)=1]$$

都是可忽略的，其中 $\mathrm{Exp}^{\text{ind-cca-}b}_{\mathrm{AS},A}(k)$ 的定义如下：

Experiment $\mathrm{Exp}^{\text{ind-cca-}b}_{\mathrm{AS},A}(k)$

$(\mathrm{pk},\mathrm{sk})\leftarrow \mathrm{AK}(1^k)$；$(x_0,x_1,s)\leftarrow A_1^{\mathrm{AD}_{\mathrm{sk}}(\cdot)}(\mathrm{pk})$；$y\leftarrow \mathrm{AE}_{\mathrm{pk}}(x_b)$；

$d\leftarrow A_2^{\mathrm{AD}_{\mathrm{sk}}(\cdot)}(x_0,x_1,s,y)$；

return d

$|x_0|=|x_1|$，即敌手选择的两个消息同长。s 是状态信息，可以包括 pk。敌手的合法性是指 A_2 不可以向 $\mathrm{AD}_{\mathrm{sk}}(\cdot)$ 询问 y。

单钥加密体制 SS=(SK,SE,SD)由 3 个多项式时间的算法构成：$\mathrm{SK}(1^k)$生成密钥 K，$\mathrm{SE}_K(M)$加密消息 $M\in\{0,1\}^*$ 得到密文 C，　$\mathrm{SD}_K(C)$解密 C 得到 M。

对单钥体制的安全性，我们主要关心对被动攻击的不可区分性（INDistinguishability against passive attack, IND）和 IND-CCA。

定义 2　(SS 的 IND)　设 SS = (SK,SE,SD) 是一个单钥加密方案，称 SS 是 IND 的，如果对于所有多项式时间敌手 $A=(A_1,A_2)$，

$$\mathrm{Adv}^{\text{ind}}_{\mathrm{SS},A}(k)=\Pr[\mathrm{Exp}^{\text{ind-1}}_{\mathrm{SS},A}(k)=1]-\Pr[\mathrm{Exp}^{\text{ind-0}}_{\mathrm{SS},A}(k)=1]$$

都是可忽略的，其中 $\mathrm{Exp}^{\text{ind-}b}_{\mathrm{SS},A}(k)$ 的定义如下：

Experiment $\mathrm{Exp}^{\text{ind-}b}_{\mathrm{SS},A}(k)$

$K\leftarrow \mathrm{SK}(1^k)$；$(x_0,x_1,s)\leftarrow A_1(k)$；$y\leftarrow \mathrm{SE}_K(x_b)$；

$d\leftarrow A_2(x_0,x_1,s,y)$；

return d

其中 $|x_0|=|x_1|$。

单钥体制的 IND-CCA 定义与上类似，但允许敌手询问解密机，询问规则同双钥体制。注意该定义实际上是文献[4]中的 FTG（Find Then Guess）不可区分性，它与文献[1]中使用的 LOR（Left Or Right）不可区分性等价[4]。

3　两种混合体制及安全性定义

3.1 混合体制 1

我们引用文献[1]中对混合体制及其安全性的定义，即

定义 3　(HY1 及其 IND-CCA)　混合体制 1 是由双钥体制 AS=(AK,AE,AD)和单钥体制 SS=(SK,SE,SD)组成的，简记为 HY1=(AS,SS)。称混合体制 1 是 IND-CCA 的，如果对于所有对混合体制 1 的合法多项式时间攻击敌手 $H=(H_1,H_2)$，

$$\mathrm{Adv}^{\text{ind-cca}}_{\mathrm{HY1},H}(k)=\Pr[\mathrm{Exp}^{\text{ind-cca-1}}_{\mathrm{HY1},H}(k)=1]-\Pr[\mathrm{Exp}^{\text{ind-cca-0}}_{\mathrm{HY1},H}(k)=1]$$

都是可忽略的，其中 $\mathrm{Exp}^{\text{ind-cca-}b}_{\mathrm{HY1},H}(k)$ 的定义如下：

Experiment $\mathrm{Exp}^{\text{ind-cca-}b}_{\mathrm{HY1},H}(k)$

$(\mathrm{pk},\mathrm{sk})\leftarrow \mathrm{AK}(1^k)$；　$K\leftarrow \mathrm{SK}(1^k)$；　$C_a\leftarrow \mathrm{AE}_{\mathrm{pk}}(K)$；

$(M_0,M_1)\leftarrow H_1^{\mathrm{SD}_K(\cdot),\mathrm{AD}_{sk}(\cdot)}(\mathrm{pk},C_a)$；　$y\leftarrow \mathrm{SE}_K(M_b)$；

$d\leftarrow H_2^{\mathrm{SD}_K(\cdot),\mathrm{AD}_{\mathrm{sk}}(\cdot)}(\mathrm{pk},C_a,y)$；

return d

敌手的合法性是指不能向 $\mathrm{AD}_{\mathrm{sk}}(\cdot)$ 询问 C_a，不能向 $\mathrm{SD}_K(\cdot)$ 询问 y。我们称 AS 是 IND-CCA 保留的(preserving)，如果对所有 IND-CCA 安全的单钥体制，混合体制 1(AS，SS)在上述定义下是 IND-CCA 的。

该写法与文献[1]不完全相同，原因是直接应用了上述 FTG 和 LOR 不可区分性的等价性。本文主要关心文献[1]中有关双钥体制 IND-CCA 保留的以下结论：

定理 1[1]　在标准模型下，一个双钥体制如果既是密钥可验证的，又是密文可验证的，那么它就一定不是 IND-CCA 保留的。

3.2 混合体制 2

这里介绍 Okamoto 等人为使双钥密码体制达到 IND-CCA 而采用的单双钥混合体制[2,5]，以 REACT[2]为例，其简单描述如下，其中 H 和 G 是 Hash 函数：

$$C=\varepsilon^{\text{asym}}_{\mathrm{pk}}(r),\quad K=G(r),\quad c=\varepsilon^{\text{sym}}_{k}(x),$$

$$\varepsilon_{pk}(x)=C\|c\|H(r,x,C,c)$$

定理 2[2]　如果 REACT 中双钥密码体制是 OW-PCA 的，单钥体制是 IND 的，那么由 REACT 得到的混合体制在随机预言机模型中可证明是 IND-CCA 的。

这里所说的混合体制的 IND-CCA 安全性是指混合体制

2 作为一个双钥体制是 IND-CCA 的，也就是说加解密是整体的，敌手不可以对其中的单双钥体制进行分别询问，否则构造密文合法性测试的 Hash 函数以及与单钥体制的混合就毫无意义。为了比较方便，我们给出混合体制2 的IND-CCA 定义。注意：下面我们将把混合体制 2 加解密的整体分别记为 $\mathrm{HY2E}_{\mathrm{pk}}(\cdot)$ 和 $\mathrm{HY2D}_{\mathrm{sk}}(\cdot)$。

定义 4 (HY2 及 HY2 的 IND-CCA) 混合体制 2 是由双钥体制 AS、单钥体制 SS 和 Hash 函数 H 构成的三元组，简记为 HY2=(AS,SS,H)。称混合体制 2 是 IND-CCA 的，如果对于所有对该体制的合法多项式时间攻击者 $H=(H_1, H_2)$，

$$\mathrm{Adv}^{\text{ind-cca}}_{\mathrm{HY2},H}(k)=\Pr[\mathrm{Exp}^{\text{ind-cca-1}}_{\mathrm{HY2},H}(k)=1]-\Pr[\mathrm{Exp}^{\text{ind-cca-0}}_{\mathrm{HY2},H}(k)=1]$$

都是可忽略的，其中 $\mathrm{Exp}^{\text{ind-cca-}b}_{\mathrm{HY2},H}(k)$ 的定义如下：

Experiment $\mathrm{Exp}^{\text{ind-cca-}b}_{\mathrm{HY2},H}(k)$

$(\mathrm{pk},\mathrm{sk})\leftarrow \mathrm{AK}(1^k)$ ； $(M_0,M_1)\leftarrow H_1^{\mathrm{HY2}D_{\mathrm{sk}}(\cdot)}(\mathrm{pk})$ ；

$y\leftarrow \mathrm{HY2}E(M_b)$；

$d\leftarrow H_2^{\mathrm{HY2Dsk}(\cdot)}(\mathrm{pk},y)$；

return d

这里敌手的合法性是指敌手不能向 $\mathrm{HY2D}_{\mathrm{sk}}(\cdot)$ 询问 y。

虽然混合体制 2 是在随机预言机模型[6]下安全的，混合体制 1 中双钥体制也可能是随机预言机模型的，所以我们可以比较上述两个定义。

4 统一定义

文献[1]中作者指出 Hash ElGamal 双钥体制的 IND-CCA 保留特性与 REACT 等弱双钥体制足以使混合体制 IND-CCA 的结论一致，但是我们可以看到文献[1]中的定义与文献[2]中的并不相同。定义 3 允许敌手对组成的单、双钥体制的解密机分开询问，而定义 4 只允许敌手对混合体制整体的解密机询问。

我们看到，定义 4 如果允许敌手分开询问单、双钥体制的解密机，那么混合体制 2 还是不安全的，因为此时我们不必在意 Hash 函数构造的密文合法性测试，而只要对其中不是 IND-CCA 的双钥体制进行攻击即可。我们知道选择密文攻击成功时，经常是得到双钥体制的私钥，而且双钥体制的密钥对总是一段时期才更换一次，所以攻破了双钥体制可能就攻破了整个混合体制 2。

定义 3 虽然允许敌手的能力较强，但是该安全性仍然不能保证混合体制 1 的安全性，因为既然可以分开询问，那么我们只要攻破其中达不到 IND-CCA 的双钥体制，从而得到单钥体制的密钥 K，即可攻破混合体制 1，即使单钥体制是 IND-CCA 的。我们注意到混合体制 1 中，双钥体制之所以能够保留 IND-CCA 是因为它加密的消息是 K，具有足够的随机性，但是只要得到 sk，那么用相应 pk 加密的 K 就暴露无遗。

为了达到实际中的通常目标，我们把混合体制整体看成是一个双钥体制，将 IND-CCA 定义统一为只允许敌手询问整体的解密机，这样询问的结果只是单钥体制的解密，与双钥体制无关，避开了双钥体制的不安全性。这一要求并不改变定义 4，但是在定义 3 中要将 (H_1,H_2) 可以询问的解密机改为 $\mathrm{HY1}D_{\mathrm{sk}}(\cdot)$。修改后的定义我们记为定义 3*：

定义 3* (统一后 HY1 的 IND-CCA) 与定义 3 相同，只是将其中的 Experiment 替换为

Experiment $\mathrm{Exp}^{\text{ind-cca-}b}_{\mathrm{HY1},H}(k)$

$(\mathrm{pk},\mathrm{sk})\leftarrow \mathrm{AK}(1^k)$； $K\leftarrow \mathrm{SK}(1^k)$； $C_a\leftarrow \mathrm{AE}_{\mathrm{pk}}(K)$；

$(M_0,M_1)\leftarrow H_1^{\mathrm{SD}_K(\cdot),\mathrm{AD}_{\mathrm{sk}}(\cdot)}(\mathrm{pk},C_a)$； $y\leftarrow \mathrm{SE}_K(M_b)$；

$d\leftarrow H_2^{\mathrm{SD}_K(\cdot),\mathrm{AD}_{\mathrm{sk}}(\cdot)}(\mathrm{pk},C_a\|y)$；

return d

定义的统一使我们可以不区分上述两种用途和目标不同的混合体制。而且如果定义的修改没有改变已有的结论，我们就可以把两种混合体制各自的安全结论统一为混合体制的安全结论，从而拓宽整个混合体制的用法和用途。

5 一些有用结论

5.1 有关 IND-CCA 保留性

我们看到统一定义后混合体制 1 之所以能达到 IND-CCA 是因为整体解密机询问只能得到单钥体制的解密结果，而该单钥体制是IND-CCA 安全的，所以混合体制是IND-CCA 的。但这并不表明其中的双钥体制可以没有任何安全性保障，IND-CCA 保留特性就概括了此时双钥体制需要的安全性，所以说 IND-CCA 保留性是一个非常有价值的概念，它为混合体制的安全性提供了保障。

观察文献[1]中关于定理 1 的证明，我们发现定义的修改并没有影响这些证明，因为这些证明中都没有任何对双钥体制解密机的单独询问，而其中对单钥体制加解密的询问我们都可以用混合整体加解密机替代。（注意：此时询问必须是混合体制的整体密文。）也就是说，在定义 3*下，定理 1 仍然成立，即：

定理 1* 在标准模型下，一个双钥体制既是密钥可验证的又是密文可验证的，那么它在定义3*下一定不是 IND-CCA 保留的。

上述结论虽然只是为我们提供了证明一个双钥体制不

是 IND-CCA 保留的方法，但它至少比从定义来证明容易得多，而且该定理将 IND-CCA 保留性与其它安全性联系了起来。

5.2 有关如何正确使用混合体制

单双钥混合的体制不仅能保证单钥加密的正常进行，而且能使低安全的双钥体制达到 IND-CCA。本节考虑混合体制 1 的用途，即双钥体制传输单钥体制的密钥，单钥体制加密真正的消息。

首先，在保证敌手只能询问整体解密机的情况下，我们可以像 REACT 那样，加一个密文合法性的 Hash 验证，这样可以降低对混合体制中双钥体制和单钥体制的安全性要求。

REACT 对其组成部分的双钥体制和单钥体制的要求比较低，尤其是对单钥体制只要求其对被动攻击的 IND。Hash 验证有效地降低了选择密文攻击者成功的概率，使得敌手必须构造合法的密文，否则得不到解密的结果，从而无法攻破。这样我们就可以降低对单双钥体制的要求，但是这并不表明有了 Hash 验证就可以很大限度地降低对单双钥体制的安全性，已经有很多选择密文攻击不需要解密结果，而只需要知道是否解密或解密是否成功，就可以攻破体制。所以，对混合体制中的单双钥体制各自的安全性还是有一定的要求。

对于混合体制 1 的用途，当某单双钥体制达不到要求时，尤其是单钥体制达不到 IND-CCA 时，我们可以采用混合体制 2 的方法达到混合体制的 IND-CCA，只要能满足混合体制 2 对单双钥体制的要求。但是，当混合体制 1 中单钥体制加密的消息是多个分组时，Hash 验证过于繁琐。

其次，当单钥体制是 IND-CCA，而双钥体制不是 IND-CCA 保留时，我们可以采用混合体制 2 的方法使该双钥体制达到 IND-CCA，从而使整个混合体制是 IND-CCA 的，即 HY1= (HY2, SS)，譬如说：AS=(AK,AE,AD)是一个双钥加密体制，它不是 IND-CCA 保留的，但是 OW-PCA 的，SS=(SK,SE,SD)是一个 IND-CCA 的单钥加密体制。我们采用 REACT 的方法使 AS 达到 IND-CCA。假设 $SS'=(SK', SE', SD')$ 是一个 IND 的单钥体制，则

$$C=\mathrm{AE}_{\mathrm{pk}}(r),\quad K'=G(r),\quad c=\mathrm{SE}'_{K'}(K),$$

$$\mathrm{HY2E}_{\mathrm{pk}}(K)=C\|c\|H(r,K,C,c)\ ,$$

$$\begin{aligned}\mathrm{HY1E}_{\mathrm{pk}}(m)&=\mathrm{HY2E}_{\mathrm{pk}}(K)\|\mathrm{SE}_K(m)\\&=C\|\mathrm{SE}'_{K'}(K)\|H(r,K,C,c)\|\mathrm{SE}_K(m)\end{aligned}\qquad(1)$$

因为 IND-CCA 的 SS 一定也是 IND 的，所以我们可以把式(1)中的 SE′ 换成 SE：

$$\mathrm{HY1E}_{\mathrm{pk}}(m)=C\|\mathrm{SE}_{K'}(K)\|H(r,K,C,c)\|\mathrm{SE}_K(m)\qquad(2)$$

将两处的 SE 合并：

$$\mathrm{HY1E}_{\mathrm{pk}}(m)=C\|\mathrm{SE}_{K'}(K)\|\mathrm{SE}_K(m)\|H(r,K,C,c)\qquad(3)$$

因为 HY2 是 IND-CCA 的，所以 K' 是安全的。因为 K 是发送者加密时随机选的，所以可以选 $K=K'$，有

$$\mathrm{HY1E}_{\mathrm{pk}}(m)=C\|\mathrm{SE}_{K'}(K')\|\mathrm{SE}_{K'}(m)\|H(r,K',C,c)\qquad(4)$$

式(4)与 REACT 十分相像，如果我们把 K' 看作是要加密消息的一部分，这就意味着我们只需要对加密消息的一小部分做 Hash 验证，简化了计算。我们把上述方案记为 REACT+，则有：

定理 3　假设 AS=(AK,AE,AD)是一个 OW-PCA 的双钥体制，SS=(SK,SE,SD)是一个 IND-CCA 的单钥体制，则由 REACT+构造的方案不仅对询问 REACT+整体解密机的敌手是 IND-CCA 的，而且对可以分开询问其中 HY2 (REACT)解密机和 SS 的解密机的敌手是 IND-CCA 的。

证明　我们要证明的是 REACT+作为混合体制 1 的 IND-CCA。

因为 REACT+中的一部分 $C\|\mathrm{SE}_{K'}(K')\|H(r,K',C,c)$ 实际上就是一个 REACT 体制，只是将被加密的消息换作 K'，而消息的改变并不影响安全性，所以这部分作为一个双钥体制是 IND-CCA 的。

一个 IND-CCA 的双钥体制和一个 IND-CCA 的单钥体制构成的混合体制 1 对能分别询问单双钥解密的敌手是 IND-CCA 的，而 SS 是一个 IND-CCA 的单钥体制，所以 REACT+对能分别询问单双钥解密的敌手也是 IND-CCA 的。又因为对分别询问单双钥解密的敌手的 IND-CCA 定义显然比对只能询问整体解密机的敌手的 IND-CCA 定义强，所以 REACT+对只能询问整体解密机的敌手也是 IND-CCA。

证毕

可以将式(4)中第二部分的加密消息换作 m 的第一个分组，Hash 函数也做相应变化，但其安全性还有待证明。

5.3 有关使双钥体制达到 IND-CCA 的方法

本节考虑混合体制 2 的用途：使双钥体制达到 IND-CCA。

目前，所有使得双钥体制达到 IND-CCA 的方法，如 OAEP[7]，REACT 和文献[8,9]等中的方法，都是构造密文合法性测试，使得敌手因为无法构造合法的密文而不能攻击成功。前两种方法用 Hash 函数构造该测试，虽然为构造测试增加的计算量可以忽略，但是为了用该测试判断一个密文是否合法，需要很多额外的计算，有时甚至需要再加密。后几种方法则采用零知识证明的方法构造，它们几乎都需要同一消息的两个密文，降低了一半的效率。因此，我们希望存在

不构造密文合法性测试，而使得双钥体制 IND-CCA 的方法。本文为此提供了有力的证据。

由本文的分析可以看出，对于一个达不到 IND-CCA，但是 IND-CCA 保留的双钥体制，只要与一个 IND-CCA 的单钥体制混合，保证敌手只能询问整体解密机，那么混合得到的体制作为一个双钥体制就是 IND-CCA 的。该方法没有用到任何密文合法性测试。所以只要存在 IND-CCA 保留的双钥体制，就存在不构造合法性测试的方法使双钥体制达到 IND-CCA。

6 小结与问题

由于 REACT 的特殊构造，让我们看到混合体制达到 IND-CCA 的新希望，但是它的安全性却取决于敌手只能询问整体解密机，这与我们常用的对混合体制的安全性定义不同。我们对此做了一定的研究之后，将对混合体制 IND-CCA 的定义进行了统一，这为如何正确地使用混合体制提供了基础。我们已经给出一些有用的结论，但还有一些问题需要解决： IND-CCA 保留性与其它双钥体制的安全性定义之间的关系；如何使一般的双钥体制达到 IND-CCA 保留性，而且这些方法应该比使其达到 IND-CCA 代价小得多。

参 考 文 献

[1] Bellare M, Boldyreva A, Palacio A. An uninstantiable random-oracle-model scheme for a hybrid-encryption problem. Cachin C, Camenisch J eds. Advances in Cryptology - Eurocrypt 2004 Proceedings. Berlin: Springer-Verlag, 2004, LNCS Vol. 3027: 171 – 188.

[2] Okamoto T, Pointcheval D. REACT: Rapid enhanced-security asymmetric cryptosystem transform. Advances in Cryptology-Crypto'2001. Berlin: Springer Verlag, 2001, LNCS Vol.2020: 159 – 175.

[3] Bellare M, Desai A, D. Pointcheval, *et al*.. Relations among notions of security for public-key encryption schemes. Advances in Cryptology-Crypt'98. Berlin: Springer-Verlag, 1998, LNCS Vol.1462: 26 – 45.

[4] Bellare M, Sahai A, Jokipii E, *et al*.. A concrete security treatment of symmetric encryption: Analysis of the DES modes of operation. Proceedings of the 38th Symposium on Foundations of Computer Science, IEEE, Miami Beach, Florida, 1997: 394 – 403.

[5] Fujisaki E, Okamoto T. Secure integration of asymmetric and symmetric encrption scheme. Advances in Cryptology-Crypto'99. Berlin: Springer Verlag, 1999, LNCS Vol.1666: 537 – 554.

[6] Bellare M, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols. Proceedings of the First Annual Conference on Computer and Communications Security, New York, ACM, 1993: 62 – 73.

[7] Bellare M, Rogaway P. Optimal asymmetric encryption: How to encrypt with RSA. Advances in Cryptology-Eurocrpt'94. Berlin: Springer Verlag, 1994, LNCS Vol. 950: 92 – 111.

[8] Crammer R, Shoup V. A pratical public key cryptosystem provably secure against adaptive chosen ciphertext attack. H. Krawczyk ed. Advances in Cryptology-Crypto'98 Proceedings, Berlin: Springer Verlag, 1998, LNCS Vol.1462: 13 – 25.

[9] Elkind E, Sahai A. A unified methodology for constructing public-key encryption schemes secure against adaptive chosen-ciphertext attack, available at iacr.org/2002/042.ps.gz. 2002.

陈 原： 女，1978 年生，博士生，主要从事密码学研究.

董庆宽： 男，1973 年生，博士后，主要从事密码学和网络安全研究.

肖国镇： 男，1934 年生，教授，博士生导师，主要从事信息论、编码学和密码学研究.