标准模型下基于证书的加密方案的通用构造

陆 阳[1,2] 李继国[2] 肖军模[1]
(中国人民解放军理工大学通信工程学院电子信息工程系 南京 210007)[1]
(河海大学计算机及信息工程学院 南京 210098)[2]

摘 要 主要研究标准模型下基于证书的加密方案(certificate-based encryption,简称CBE)的通用构造,并给出了两个实现方案。首先,以IND-CCA2安全的公钥加密方案、IND-ID-CCA安全的基于身份的加密方案以及强一次性签名方案这3种密码学原型为组件提出了第一个CBE方案的通用构造,并在标准模型下证明了其安全性;其次,针对强一次性签名方案存在的一些问题,以强一次性消息认证码代替一次性签名方案,提出了另一个通用构造。与前者相比,第二个通用构造的性能得到了明显的优化。

关键词 基于证书的加密方案,通用构造,标准模型
中图分类号 TP309.7 **文献标识码** A

Generic Construction of Certificate-based Encryption Scheme in the Standard Model

LU Yang[1,2] LI Ji-guo[2] XIAO Jun-mo[1]
(Institute of Communication Engineering, PLA Univ. of Sci. & Tech., Nanjing 210007, China)[1]
(College of Computer and Information Engineering, Hohai University, Nanjing 210098, China)[2]

Abstract The certificate-based encryption (CBE) is a new PKC paradigm which combines public-key encryption (PKE) and identity based encryption (IBE) while preserving their features. CBE provides an efficient implicit certification mechanism for a PKI and allows a form of automatic certificate revocation, while it is not subjected to the private key escrow problem and secret key distribution problem inherent in IBE. This paper firstly proposed a generic construction of CBE scheme based on three general primitives: IBE, PKE and strong one-time signature (SOTS) scheme and proved it to be secure in the standard model. Then, it described how to use message authentication code (MAC) to replace the SOTS scheme to further improve the efficient of the first generic CBE scheme and to achieve another generic CBE scheme. These two generic constructions show that CBE scheme can be constructed in a more general and efficient way.

Keywords Certificate-based encryption scheme, Generic construction, Standard model

在Eurocrypt 2003上,Gentry[1]提出了基于证书的公钥密码体制(certificate-based public key cryptography,简称CB-PKC),有效克服了基于身份的公钥密码体制和传统公钥密码体制存在的缺陷,并保留了两者的优点。一方面,CB-PKC解决了传统PKI系统中证书的撤销问题和对证书状态的第三方询问问题,能够用于构造高效的PKI,减少公钥证书的管理和维护所需的计算、通信和存储开销。另一方面,CB-PKC消除了基于身份的公钥密码体制中固有的密钥托管问题以及KGC与用户之间的密钥分发问题。因此,CB-PKC是一种性能优良、便于应用的公钥密码体制。自提出基于证书的公钥密码系统概念以来,相继公开发表一些基于具体代数假设的基于证书的加密(certificate-based encryption,简称CBE)方案。与此同时,基于一些密码学原型(primitive)来通用构造CBE方案的方法也得到了关注。遗憾的是,这些方法[2-4]相继被指出要么是不安全的[5],要么是错误的[6]。最近,本文作者指出了文献[2,3]中通用构造安全缺陷产生的根本原因,并基于Fujisaki-Okamoto变换[7,8]给出了相应的安全增强组件[15],提出了CBE方案的两类通用构造[16],并在随机预言模型(random oracle model)[9]中证明了其安全性。

本文研究标准模型下CBE方案的通用构造,以公钥加密方案PKE(public key encryption)、基于身份的加密方案IBE(identity-base encryption)等密码学原型为组件分别提出了两个安全可证的CBE方案的通用构造。其基本思想是以一个选择密文安全的IBE方案和一个选择密文安全的PKE方案来对消息进行双重加密,生成消息的密文;同时以一个强一次性签名方案(或消息认证码)来生成消息密文的签名(或认证码),并与消息密文组成CBE方案的最终密文。这一方法有效保证了方案密文的有效性,使得文献[5]中的攻击者无法借

到稿日期:2008-07-22 返修日期:2008-10-13 本文受国家高技术研究发展计划(863计划)项目(No. 2007AA01Z409),国家自然科学基金项目(No. 60673070)资助。

陆 阳(1977-),男,博士生,讲师,CCF会员,主要研究方向为网络信息安全,E-mail:luyangnsd@163.com;李继国(1970-),男,博士,副教授,硕士生导师,主要研究方向为信息安全、密码学;肖军模(1947-),男,教授,博士生导师,主要研究方向为网络信息安全。

助于解密 Oracle 对本文通用构造所生成的 CBE 方案实施有效的攻击。

1 基于证书的加密方案

本节简要介绍 CBE 方案及其安全模型的形式化定义[1,4]。

定义 1 一个基于证书的加密方案由 5 个多项式时间算法构成，即 *Setup*：输入安全参数 k、输出 CA 的主密钥 sk_{CA} 和系统公开参数集 *params*，该算法通常由 CA 运行；*SetKeyPair*：输入 *params*，输出为用户的公钥/私钥对 $\langle upk, usk\rangle$；*Certify*：输入 $(sk_{CA}, params, \tau, id, upk)$，输出身份标识为 id 的用户在 τ 期间内的有效证书 $Cert_{id,\tau}$；*Enc*：输入 $\langle params, \tau, id, upk, M\rangle$，输出消息 M 的密文 C；*Dec*：输入 $\langle params, Cert_{id,\tau}, usk, C\rangle$，若 $Cert_{id,\tau}$ 和 C 有效，算法则计算并输出 C 的明文 M；否则输出 $\perp$。

CBE 方案标准的并且是最强的安全性概念为 IND-CBE-CCA[1,4]，其形式化定义如下：

定义 2 对任一 CBE 方案 $(Setup, SetKeyPair, Certify, Enc, Dec)$，如果任意的多项式时间敌手 A_1 和 A_2 攻击成功的优势 $Adv(A_1)=2|\Pr[(sk_{CA}, params)\leftarrow Setup(1^k), (M_0, M_1, \tau, id, upk, usk, s)\leftarrow B_1^{O_1}(params), b\leftarrow\{0,1\}, C=Enc(\tau, id, upk, M_b): B_2^{O_2}(params, \tau, id, upk, usk, M_0, M_1, C, s)=b]-1/2|$ 和 $Adv(A_2)=2|\Pr[(sk_{CA}, params)\leftarrow Setup(1^k), \langle upk, usk\rangle\leftarrow SetKeyPair(params), (M_0, M_1, \tau, id, s)\leftarrow C_1^{O_3}(params, sk_{CA}, upk), b\leftarrow\{0,1\}, C=Enc(\tau, id, upk, M_b): C_2^{O_4}(params, sk_{CA}, \tau, id, upk, usk, M_0, M_1, C, s)=b]-1/2|$ 都是可忽略的，则称该方案是 IND-CBE-CCA 安全的，并称该方案对敌手 A_1 是 Type I IND-CBE-CCA 安全的，对敌手 A_2 是 Type II IND-CBE-CCA 安全的。其中，敌手 $A_1=(B_1, B_2)$ 和 $A_2=(C_1, C_2)$ 都是 2 阶段攻击者；O_1 和 O_2 分别表示敌手 A_1 可以询问证书 Oracle 和解密 Oracle，而 O_3 和 O_4 分别表示敌手 A_2 可以询问解密 Oracle。

2 通用构造 I

2.1 通用构造的组件

通用构造 1 的组件包括 3 类密码学原型，分别为 IND-ID-CCA 安全的 IBE 方案、IND-CCA2 安全的 PKE 方案以及强一次性签名方案。受篇幅限制，下面仅介绍强一次性签名方案的定义。IBE 方案和 PKE 方案的定义及其安全性概念，请参见文献[10]和文献[11]。

定义 3 一个签名方案由 3 个多项式时间算法组成，即 *KeyGen*：输入为安全参数 k，输出为一签名/验证密钥对 $\langle sk, vk\rangle$；*Sign*：输入为消息 M 和签名密钥 sk，输出为消息 M 的签名 s；*Verify*：输入为消息 M、签名 s 以及验证密钥 vk，若 s 是 M 的有效签名，则输出 1，否则输出 0。

当一个签名方案满足存在性不可伪造，抗一次性选择消息攻击的安全性时，称之为强一次性签名方案[12]，其形式化定义如下：

定义 4 对任一签名方案 $(KeyGen, Sign, Verify)$，如果任意的多项式时间敌手 A 攻击成功的概率 $Succ_A=|\Pr[\langle sk, vk\rangle\leftarrow KeyGen(1^k), M\leftarrow A(1^k, vk), s=Sign(sk, M), \langle M', s'\rangle\leftarrow A(M, s, vk): \langle M', s'\rangle\neq\langle M, s\rangle \wedge Verify(vk, M', s'=1]$ 是可忽略的，则称该签名方案为强一次性签名方案（strong one time signature，简称 SOTS）。

2.2 通用构造的描述

假设 IBE=(Setup, Extract, Enc, Dec) 是一个 IBE 方案，PKE=(KeyGen, Enc, Dec) 是一个 PKE 方案，以及 S=(KeyGen, Sign, Verify) 是一个签名方案；并且假设方案 IBE 和 PKE 的密文空间是相容的，即方案 PKE 的密文空间是方案 IBE 的密文空间的子集，则一个 CBE 方案 Generic-CBE=(Setup, SetKeyPair, Certify, Enc, Dec) 可以通用构造如下。

Setup：输入安全参数 k，算法运行 IBE. Setup 算法生成一主密钥 msk 和公开参数集 *params*，CA 的主密钥 sk_{CA} 置为 msk。

SetKeyPair：算法同 PKE. KeyGen 算法。

Certify：输入 $\langle msk, params, \tau, id, upk\rangle$，该算法以 $\tau||id||upk$ 和 msk 作为输入运行 IBE. Extract 算法，并且将 IBE. Extract 算法的输出作为用户 id 在 τ 期间内的证书 $Cert_{id,\tau}$。

Enc：输入 $\langle params, \tau, id, upk, M\rangle$，算法首先执行 S. KeyGen 算法，生成签名/验证密钥对 $\langle sk, vk\rangle$；然后分别计算 $c_1=$ PKE. Enc$(upk, M||vk)$，$c_2=$ IBE. Enc$(\tau||id||upk, c_1)$ 和 $s=$ OTS. Sign(sk, c_2)；最后输出密文 $C=\langle c_2, s, vk\rangle$。

Dec：输入 $\langle params, Cert_{id,\tau}, usk, C\rangle$，其中 $C=\langle c, s, vk\rangle$。算法首先计算 S. Verfify$(vk, s, c)$ 是否为 0。如果成立，则输出 $\perp$ 并终止解密；否则，分别计算 $c_1=$ IBE. Dec$(Cert_{id,\tau}, c)$ 和 $M||vk'=$ PKE. $Dec(usk, c_1)$。如果 $vk'\neq vk$，则输出 $\perp$，否则输出 M。

2.3 安全性证明

引理 1 若方案 IBE 是 IND-ID-CCA 安全的并且 S 是一个强一次性签名方案，则方案 Generic-CBE 是 Type I IND-CBE-CCA 安全的。

证明：假设 A_1 为 Generic-CBE 的 Type I IND-CBE-CCA 敌手，并假设 A_1 在 IND-CBE-CCA 游戏的挑战阶段的输出为 $\langle \tau_{ch}, id_{ch}, upk_{ch}, usk_{ch}, M_0, M_1\rangle$，返回的挑战密文为 $C_{ch}=\langle c_{ch}, s_{ch}, vk_{ch}\rangle$，其中 c_{ch} 为 $M_b\in\{M_0, M_1\}$ 的密文，s_{ch} 为 c_{ch} 的一次性签名，vk_{ch} 为一次性签名的验证密钥。下面证明敌手 A_1 获胜的优势是可忽略的。

定义如下事件。(1) 事件 Forge：敌手 A_1 对 $\langle \tau, id, upk, usk, C\rangle$ 作过解密查询，其中 $C=\langle c, s, vk_{ch}\rangle$ 是有效的密文，即 s 是 c 的有效签名，并且 $\langle c, s\rangle\neq\langle c_{ch}, s_{ch}\rangle$。(2) 事件 A_1 wins：敌手 A_1 对 b 的猜测 b' 是正确的。

根据 IND-CBE-CCA 敌手获胜优势的定义，有

$$
\begin{aligned}
Adv(A_1) &= 2|\Pr[A_1 \text{ wins}]-1/2| \\
&= 2|\Pr[A_1 \text{ wins}|\text{Forge}]\cdot\Pr[\text{Forge}]-\Pr[\text{Forge}]/2+\Pr[A_1 \text{ wins}|\neg\text{Forge}]\cdot\Pr[\neg\text{Forge}]+\Pr[\text{Forge}]/2-1/2| \\
&\leqslant \Pr[\text{Forge}]+2|\Pr[A_1 \text{ wins}|\neg\text{Forge}]\cdot\Pr[\neg\text{Forge}]+\Pr[\text{Forge}]/2-1/2|
\end{aligned}
$$

易见，如果能够证明 $\Pr[\text{Forge}]$ 和 $|\Pr[A_1 \text{ wins}|\neg\text{Forge}]\cdot\Pr[\neg\text{Forge}]+\Pr[\text{Forge}]/2-1/2|$ 都是可忽略的，那么也就证明了 A_1 获胜的优势是可忽略的。

首先，$\Pr[\text{Forge}]$ 显然是可忽略的。根据事件 Forge 的定义可知，事件 Forge 的发生将意味着敌手 A_1 成功地伪造了方案 S 一个有效的消息/签名对，这就与方案 S 的强一次安全性

发生了矛盾。

其次，证明 $|\Pr[A_1 \text{ wins}|\neg\text{Forge}]\cdot\Pr[\neg\text{Forge}]+\Pr[\text{Forge}]/2-1/2|$ 也是可忽略的。下面由 A_1 来构造一个 IND-ID-CCA 敌手 B 攻击方案 IBE。记 B 所在的 IND-ID-CCA 游戏的挑战者为 X，X 运行 IBE. Setup 算法，生成一主密钥 msk 和公开参数集 $params$，并将 $params$ 输出给 B，同时允许 B 询问密钥生成 Oracle 和解密 Oracle。B 首先运行 S. KeyGen 算法，生成签名/验证密钥对 $\langle vk_{ch}, sk_{ch}\rangle$，然后将 params 输出给 A_1，并模仿方案 Generic-CBE 的挑战者与 A_1 进行如下交互。

证书询问：假设 $\langle\tau, id, upk, usk\rangle$ 是由 A_1 作出的证书询问，则 B 以向其挑战者 X 对 $\langle\tau||id||upk\rangle$ 做密钥生成询问，并将返回结果作为证书 $Cert_{id,\tau}$ 输出给 A_1。

解密询问：假设 $\langle\tau, id, upk, usk, C=\langle c, s, vk\rangle\rangle$ 是由 A_1 作出的解密询问，(1)如果事件 Forge 发生，则 B 直接进入其 IND-ID-CPA 游戏的挑战阶段，随机输出 $b\in\{0,1\}$ 作为其对挑战密文的猜测并退出游戏；(2)否则，B 首先计算 S. Verfify (vk, s, c) 是否为 0，如果成立，则输出 $\perp$ 并终止解密；然后借助于其挑战者 X 计算 $M||vk'=\text{PKE. Dec}(usk, \text{IBE. Dec}(Cert_{id,\tau}, c))$，如果 $vk'\neq vk$，则输出 $\perp$；否则输出 M。

挑战询问：假设 $\langle\tau_{ch}, id_{ch}, upk_{ch}, usk_{ch}, M_0, M_1\rangle$ 是由 A_1 作出的挑战询问，B 处理如下：(1)分别计算 $c_0=\text{PKE. Enc}(upk_{ch}, M_0||vk_{ch})$ 和 $c_1=\text{PKE. Enc}(upk_{ch}, M_1||vk_{ch})$；(2)将 $\langle\tau_{ch}||id_{ch}||upk_{ch}, c_0, c_1\rangle$ 提交给挑战者 X 作为其 IND-ID-CPA 游戏的挑战。X 随机选择比特 $b\in\{0,1\}$，返回挑战密文 $c_{ch}=\text{IBE. Enc}(\tau_{ch}||id_{ch}||upk_{ch}, c_b)$ 给 B。(3)计算 $s_{ch}=\text{OTS. Sign}(usk_{ch}, c_{ch})$，并输出挑战密文 $C_{ch}=\langle c_{ch}, s_{ch}, vk_{ch}\rangle$ 给 A_1。

A_1 收到挑战密文后，继续作出一系列的询问，但限制是：(1)$\langle\tau_{ch}, id_{ch}, upk_{ch}, usk_{ch}\rangle$ 不能作为证书询问的对象；(2)$\langle\tau_{ch}, id_{ch}, upk_{ch}, usk_{ch}, C_{ch}\rangle$ 不能作为解密询问的对象。最终，A_1 向 B 给出对 b 的猜测 $b'\in\{0,1\}$，而 B 将 b' 提交给 X 作为其对 b 的猜测。

由 B 的模拟过程可以看出，B 与 A_1 交互过程完全模拟了 A_1 真实攻击方案 Generic-CBE 的环境，因此在事件 Forge 不发生的前提下，B 获胜的概率等于 A_1 获胜的概率，即 $\Pr[B \text{ wins}|\neg\text{Forge}]=\Pr[A_1 \text{ wins}|\neg\text{Forge}]$。而在事件 Forge 发生的前提下，B 获胜的概率显然等于 1/2，即 $\Pr[B \text{ wins}|\text{Forge}]=1/2$。

由 B 获胜的优势 $Adv(B)=|\Pr[B \text{ wins}]-1/2|$，可知

$$\begin{aligned}Adv(B)&=|\Pr[B \text{ wins}|\text{Forge}]\cdot\Pr[\text{Forge}]+\Pr[B \text{ wins}|\neg\text{Forge}]\cdot\Pr[\neg\text{Forge}]-1/2|\\&=|\Pr[\text{Forge}]/2+\Pr[A_1 \text{ wins}|\neg\text{Forge}]\cdot\Pr[\neg\text{Forge}]-1/2|\end{aligned}$$

由于方案 IBE 是 IND-ID-CCA 安全的，因此 A 获胜的优势是可忽略的，从而证明了 $|\Pr[\text{Forge}]/2+\Pr[A_1 \text{ wins}|\neg\text{Forge}]\cdot\Pr[\neg\text{Forge}]-1/2|$ 是可忽略的。

综上，A_1 获胜的优势 $\text{Adv}(A_1)$ 是可忽略的。引理 1 证明完毕。

引理 2 若方案 PKE 是 IND-CCA2 安全的并且 S 是一个强一次性签名方案，则方案 Generic-CBE 是 Type II IND-CBE-CCA 安全的。

引理 2 的证明方法与引理 1 类似，不同之处在于 Type II IND-CBE-CCA 敌手拥有 CA 的主密钥 sk_{CA}，并且在 IND-CBE-CCA 游戏的一开始就被指定了一个固定挑战公钥 upk_{ch}，即 IND-CCA2 敌手的挑战公钥。受文章篇幅限制，本文略去引理 2 的证明过程。

由引理 1 和引理 2 可得如下定理：

定理 1 若方案 IBE 是 IND-ID-CCA 安全的、方案 PKE 是 IND-CCA2 安全的并且方案 S 是一个强一次性签名方案，则方案 Generic-CBE 是 IND-CBE-CCA 安全的。

3 通用构造 II

文献[14]指出，现有的两类 SOTS 方案存在着如下的缺陷：(1)基于单向函数的 SOTS 方案尽管计算效率高，但生成的验证密钥和签名过长；(2)基于数论假设的 SOTS 方案尽管验证密钥和签名较短，但计算效率却比较差。因此，本节引入了更为高效的消息认证码 MAC(message authentication code)来代替 SOTS 方案，提出了一个性能优化的通用构造。

3.1 消息认证码

首先介绍消息认证码及其安全性的定义[14]。

定义 5 一个消息认证码由两个多项式时间算法组成，Mac：输入为待认证信息 M 和一个随机密钥 $mk\in\{0,1\}^k$，其中 $\{0,1\}^k$ 为 MAC 的密钥空间，k 为安全参数，输出为 MAC 标记 $tag=Mac(mk,M)$；$Verify$：输入为信息 M、标记 tag 以及密钥 mk，若 tag 是 M 的有效标记，即 $tag=Mac(mk,M)$，则输出 1；否则输出 0。

一般地，消息认证码应具有抗一次性选择消息攻击(against a one-time chosen-message attack)的安全性，形式化定义如下：

定义 6 对任一消息认证码 $(Mac, Verify)$，如果任意的多项式时间敌手 A 攻击成功的概率 $Succ_A=|\Pr[mk\leftarrow\{0,1\}^k, M\leftarrow A(1^k), tag=Mac(mk,M), \langle M', tag'\rangle\leftarrow A(M,tag): \langle M', tag'\rangle\neq\langle M, tag\rangle\wedge Verify(mk, M', tag')=1]$ 是可忽略的，则称该信息认证码是抗一次性选择消息攻击安全的。

通常，抗一次性选择消息攻击安全的消息认证码也称为强一次性消息认证码。

3.2 通用构造的描述

假设 MAC = (Mac, Verify)是一个信息认证码，其它条件同通用构造 1，则一个通用的 CBE 方案 Generic-CBE′ = (Setup′, SetKeyPair′, Certify′, Enc′, Dec′)可以构造如下：

Setup′：同 Generic-CBE. Setup 算法。

SetKeyPair′：同 Generic-CBE. SetKeyPair 算法。

Certify′：同 Generic-CBE. Certify 算法。

Enc′：输入为 $\langle\tau, id, upk, M\rangle$，算法执行过程如下：生成 MAC 的一个随机密钥 $mk\in\{0,1\}^{k'}$，其中 $\{0,1\}^{k'}$ 为 MAC 的密钥空间，k' 为安全参数；分别计算 $c_1=\text{PKE. Enc}(upk, M||mk)$，$c_2=\text{IBE. Enc}(\tau||id||upk, c_1)$ 和 $tag=\text{MAC. Mac}(mk, c_2)$；输出密文 $C=\langle c_2, tag\rangle$。

Dec：输入为 $\langle Cert_{id,\tau}, usk, C\rangle$，其中 $C=\langle c, tag\rangle$，算法依次计算 $M||mk=\text{PKE. Dec}(usk, \text{IBE. Dec}(Cert_{id,\tau}, c))$ 和 $b=\text{MAC. Verify}(c, tag, mk)$。如果 $b=0$，则输出 $\perp$；否则输出 M。

经对比，方案 Generic-CBE′ 的性能明显优于方案 Gener-

ic-CBE。首先，由于使用了计算性能更好的 MAC 来代替 SOTS 方案作为组件，因此加/解密效率要优于方案 Generic-CBE；其次，密文长度也大大短于方案 Generic-CBE 的密文长度。方案 Generic-CBE'的密文由消息的密文和密文的消息认证码组成，而方案 Generic-CBE 的密文则由密文、密文的签名及签名的验证密钥组成。在具体实现中，方案 Generic-CBE'使用 CBC-MAC 来产生密文的消息认证码可以短至 128bit；而方案 Generic-CBE 在使用 BLS 短签名[13]的前提下，密文的签名也有 170bit 左右。但方案 Generic-CBE'的不足之处是无法在完全解密前对密文的有效性进行验证，即使密文是无效的。

最后，方案 Generic-CBE'的安全性有如下的结论：

定理 2 若方案 IBE 是 IND-ID-CCA 安全的、方案 PKE 是 IND-CCA2 安全的并且方案 MAC 是一个强一次性信息认证码，则方案 Generic-CBE'是 IND-CBE-CCA 安全的。

定理 2 的证明方法与定理 1 几乎相同。不同之处是需要将事件 Forge 定义为 IND-CBE-CCA 敌手 A 对$\langle \tau, id, upk, usk, C=\langle c, tag\rangle\rangle$ 作过解密查询，其中 $C=\langle c, tag\rangle$是有效的密文，$\langle c, tag\rangle \neq \langle c_{ch}, tag_{ch}\rangle$，并且 c 和 c_{ch} 解密后获得的 MAC 标记的验证密钥相同，即 $mk=mk_{ch}$。由 MAC 的抗一次性选择消息攻击安全性，Pr[Forge]显然是可忽略的。

结束语 由于基于一般密码学原型而非具体的代数假设，能够最大程度地保留其组件的优点，公钥密码体制的通用构造近年来得到了广泛的关注。本文以 IND-CCA2 安全的公钥加密方案、IND-ID-CCA 安全的基于身份的加密方案以及强一次性签名方案等密码学原型为组件提出了两个 CBE 方案的通用构造，并在标准模型下证明了其安全性。

下一步的工作主要是对本文的通用构造做一步改进，探讨是否存在对组件的安全性要求更低的通用构造，以期提出更高效的构造方案。此外，目前还未见有标准模型下安全可证的基于证书的签名方案的通用构造，因此这方面的研究也将是下一步的工作重点。

参 考 文 献

[1] Gentry C. Certificate-based Encryption and the Certificate Revocation Problem[C]// Proceedings, Advances in Cryptology-EUROCRYPT 2003. Warsaw, Poland, 2003

[2] Yum D H, Lee P J. Identity-based Cryptography in Public Key Management[C]// Proceedings, EuroPKI 2004. Samos Island, Greece, 2004

[3] Yum D H, Lee P J. Generic Construction of Certificateless Encryption[C]// Proceedings, EuroPKI2004 International Conference on Computational Science and Its Applications-ICCSA 2004. Assisi, Italy, 2004

[4] Al-Riyami S, Paterson K G. CBE from CL-PKE: A Generic Construction and Efficient Schemes[C]// Proceedings, Public Key Cryptography-PKC 2005. Les Diablerets, Switzerland, 2005

[5] Galindo D, Morillo P, Ràfols C. Breaking Yum and Lee Generic Constructions of Certificateless and Certificate-based Encryption Schemes[C]// Proceedings, EuroPKI 2006. Turin, Italy, 2006

[6] Kang B G, Park J H. Is It Possible to Have CBE from CL-PKE? Cryptology ePrint Archive[R]. 2005/431. http://eprint.iacr.org/, 2005

[7] Fujisaki E, Okamoto T. How to Enhance the Security of Public Key Encryption at Minimum Cost[C]// Proceedings, Public Key Cryptography-PKC'99. Kamakura, Japan, 1999

[8] Fujisaki E, Okamoto T. Secure Integration of Asymmetric and Symmetric Encryption Schemes[C]// Proceedings, Advances in Cryptology-CRYPTO'99. California, USA, 1999

[9] Bellare M, Rogaway P. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols[C]// Proceedings, ACM CCS 1993. Virginia, USA, 1993

[10] Bellare M, Desai A, Pointcheval D, et al. Relations Among Notions of Security for Public Key Encryption Schemes[C]// Proceedings, Advances in Cryptology-CRYPTO'98. California, USA, 1998

[11] Boneh D, Franklin M. Identity-based Encryption from the Weil Pairing[C]// Proceedings, Advances in Cryptology -CRYPTO 2001. California, USA, 2001

[12] Canetti R, Halevi S, Katz J. Chosen-ciphertext Security from Identity-based Encryption[C]// Proceedings, Advances in Cryptology-Eurocrypt 2004. Interlaken, Switzerland, 2004

[13] Boneh D, Lynn B, Shacham H. Short Signatures from the Weil Pairing[C]// Proceedings, Asiacrypt 2001. Gold Coast, Australia, 2001

[14] Boneh D, Katz J. Improved Efficiency for CCA-Secure Cryptosystems Built Using Identity Based Encryption[C]// Proceedings, RSA — Cryptographers' Track 2005. California, USA, 2005

[15] Lu Yang, Li Jiguo, Xiao Junmo. Applying the Fujisaki-Okamoto Conversion to Certificate-based Encryption[C]// Proceedings, 2008 International Symposium on Electronic Commerce and Security-ISECS 2008. Guangdong, China, 2008

[16] Lu Yang, Li Jiguo, Xiao Junmo. Generic Construction of Certificate-based Encryption[C]// Proceedings, 9th International Conference for Young Computer Scientists-ICYCS 2008. Zhangjajie, China, 2008

(上接第 74 页)

[4] 张学，陆桑璐，等. 无线传感器网络的拓扑控制[J]. 软件学报，2007(4)：943-954

[5] 张重庆，李明禄，等. 数据收集传感器网络的负载平衡网络构建方法[J]. 软件学报，2007(5)：1110-1121

[6] 李捷，刘先省，韩志杰. 基于 ARMA 的无线传感器网络流量预测模型的研究[J]. 电子与信息学报，2007(5)：1224-1227

[7] Manjeshwar A, Agrawal D P. TEEN: A protocol for enhanced efficiency in wireless sensor networks[C]// Int'l Proc. of the 15th Parallel and Distributed Processing Symp. San Francisco: IEEE Computer Society, 2001: 2009-2015