一个高效的基于证书的加密方案

陆 阳[1,2] 李继国[1] 肖军模[2]
(河海大学计算机及信息工程学院 南京 210098)[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)[2]

摘 要 基于证书的公钥密码体制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中存在缺陷,成为一种颇受关注的公钥体制。以SK-IBE方案和ElGamal公钥加密方案作为构件,提出了一个高效的基于线对和基于证书的加密方案,并在随机预言模型下给出了安全性证明。在 p-BDHI 假设下,该方案被证明是IND-CBE-CCA安全的。在效率方面,该方案仅在解密时计算一个线对,因此方案的总体性能是高效的,经对比分析,优于现有的其它CBE方案。

关键词 基于证书的加密方案,线对,IND-CBE-CCA,随机预言模型
中图法分类号 TP309.7 **文献标识码** A

Efficient Certificate-based Encryption Scheme

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

Abstract The certificate-based encryption (CBE) is a new PKC paradigm which combines traditional 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 presented an efficient pairing-based CBE scheme and proved it to be IND-CBE-CCA secure in the random oracle model based on the hardness of the p-BDHI problem. Compared with other existing CBE schemes, this scheme has obvious advantage in the computation performance.

Keywords Certificate-based encryption, Pairing, IND-CBE-CCA, Random oracle 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),该体制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中存在的缺陷。与已有的公钥密码体制相比,CB-PKC的优点在于:(1)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;(2)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密钥分发需要安全信道的问题;(3)避免了无证书公钥密码体制容易遭受公钥替换攻击和拒绝解密攻击的问题。因此,CB-PKC是一种性能优良、便于应用的公钥密码体制。

本文主要研究高效的基于证书的加密(Certificate-Based Encryption,简称CBE)方案。作为CB-PKC的重要组成部分,可证安全的CBE方案的设计与实现是当前研究的热门问题。现有的已被证明安全的CBE方案[1-3]都需要使用双线性对(Bilinear Pairing)运算。双线性对被成功运用于安全协议的设计[5]以来,由于其独特的数学特性,已成为加密、签名方案和协议设计中不可或缺的数学工具。然而,相对于其它常用的运算(如模指数运算等),双线性对运算的缺陷在于高昂的计算开销。例如,在MIRACL[14]中,一个512比特的Tate对的计算开销需要20ms,而一个1024比特的指数运算仅需8.8 ms。尽管最近在实现技术上取得了一些进展[13],但是并没有从根本上解决双线性对运算这一固有的问题。目前,无线对CBE方案的设计仍是一个困难问题,因此在基于线对的CBE方案的设计中,如何尽可能少地使用线对计算成为值得关注的问题。在此背景下,本文以SK-IBE方案[6,7]和ElGamal公钥加密方案[9]作为构件,提出了一个高效的基于线对的CBE方案,并在随机预言模型下[12]证明其是选择密文安全的。在线对计算方面,本文方案仅在解密时计算一个线对。经对比分析,方案的总体性能是高效的,优于其它现有的CBE方案[1-3]。

1 预备知识

设 G_1 和 G_2 是阶为 q 的加法循环群,G_T 是阶为 q 的乘法

到稿日期:2008-10-15 返修日期:2008-12-30 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. 60842002),河海大学自然科学基金项目(No. 2008428611)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 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 男,教授,博士生导师,主要研究方向为网络信息安全。

循环群，q 是一个大素数；P_1 和 P_2 分别为群 G_1 和群 G_2 的生成元；映射 $\varphi: G_2 \to G_1$ 为群 G_2 到群 G_1 的同态且满足 $\varphi(P_2)=P_1$。若映射 $e: G_1 \times G_2 \to G_T$ 具有如下性质，则称之为可接受的双线性映射：(1)双线性：对于任意的 $P \in G_1, Q \in G_2, a, b \in Z$ 有 $e(aP,bQ)=e(P,Q)^{ab}$。(2)非退化性：$e(P_1,P_2) \neq 1_{G_T}$。(3)可计算性：对于任意的 $P \in G_1, Q \in G_2$，存在高效的算法计算 $e(P,Q)$。

本文 CBE 方案的安全性基于如下的 p-BDHI(p-Bilinear Diffie-Hellman Inversion)假设[7,8]。

定义 1(p-BDHI 假设) 设 G_1 和 G_2 是阶为素数 q 的加法循环群，G_T 是阶为素数 q 的乘法循环群，P_1 和 P_2 分别为 G_1 和 G_2 的生成元且满足 $\varphi(P_2)=P_1$，则给定整数 $p>0$，对任意的 $x \in Z_q^*$，由 $(P_1, P_2, xP_2, x^2P_2, \cdots, x^pP_2)$ 计算 $e(P_1,P_2)^{1/x}$ 是困难的。

文献[7]证明了 1-BDHI 假设和标准的 BDH(Bilinear Diffie-Hellman)假设是多项式时间等价的。

2 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 2 一个基于证书的加密方案由 5 个多项式时间算法构成。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 $params$；SetKeyPair：输入 $params$，输出为用户的私钥/公钥对 $\langle usk, upk\rangle$；Certify：输入 $\langle sk_{CA}, params, \tau, id, upk\rangle$，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 $\perp$。

上述算法应满足一致性约束，即对于任意的 M，$Dec(Cert_{id,\tau}, usk, Enc(\tau, id, upk, M))=M$，其中 $Cert_{id,\tau}=Certify(sk_{CA}, \kappa\tau, id, upk)$，$\langle usk, upk\rangle$ 为有效的私钥/公钥对。

CBE 方案最强安全性概念为 IND-CBE-CCA，其定义如下：

定义 3 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。

在上述定义中，若 O_1 和 O_2 分别表示敌手 A_1 可以询问证书 Oracle，O_3 和 O_4 为空，则可以得到 CBE 方案 IND-CBE-CPA 安全性的定义。

3 方案的描述

本节首先构造一个 IND-CBE-CPA 安全的 CBE 方案 BasicCBE；然后在此基础之上构造 IND-CBE-CCA 安全的完全方案 FullCBE。

3.1 BasicCBE

方案 BasicCBE 由如下 5 个多项式时间算法组成。

Setup：输入为安全参数 $k \in Z^+$，算法执行如下：(1)产生大素数 q，并生成 q 阶加法循环群 G_1 和 G_2，q 阶乘法循环群 G_T，使得存在可接受的双线性映射 $e: G_1 \times G_2 \to G_T$；(2)生成 G_2 到 G_1 的同态 $\varphi: G_2 \to G_1$，随机选择群 G_2 的生成元 P_2，置 $P_1=\varphi(P_2)$，并计算 $g=e(P_1,P_2)$；(3)随机选择 $s \in Z_q^*$，计算 $P_{pub}=sP_1$；(4)选择两个 Hash 函数 $H_1: \{0,1\}^* \to Z_q^*$ 和 $H_2: G_T \times G_T \to \{0,1\}^n$，其中 $n \in Z^+$。算法输出为系统的公开参数集 $params=\{q, G_1, G_2, G_T, \varphi, e, n, P_1, P_2, g, P_{pub}, H_1, H_2\}$，CA 的主密钥 s，明文空间 $\coprod=\{0,1\}^n$，以及密文空间 $\coprod=G_1^* \times \{0,1\}^n$。

SetKeyPair：算法随机选择 $x \in Z_q^*$ 并计算 g^x，输出 $\langle x, g^x\rangle$ 作为用户的私钥/公钥对 $\langle usk, upk\rangle$。

Certify：输入为 $\langle s, \tau, id, upk\rangle$，算法计算并输出用户 id 在 τ 期间内的短期证书 $Cert_{id,\tau}=\frac{1}{H_1(\tau||id||upk)+s}P_2$。

Enc：输入为 $\langle \tau, id, upk, M\rangle$，算法随机选择 $r \in Z_q^*$，置 $Q_{id}=H_1(\tau||id||upk)P_1+P_{pub}$，计算并输出密文 $C=\langle U, V\rangle=\langle rQ_{id}, M \oplus H_2(g^r, upk^r)\rangle$。

Dec：输入为 $\langle Cert_{id,\tau}, usk, C=\langle U, V\rangle\rangle$，算法计算并输出明文 $M=V \oplus H_2(e(U, Cert_{id,\tau}), e(U, Cert_{id,\tau})^{usk})$。

不难验证 $e(U, Cert_{id,\tau})=g^r$，因此方案 BasicCBE 中的算法显然是满足一致性要求的。

3.2 FullCBE

对方案 BasicCBE 应用 Fujisaki-Okamoto 变换[11]，得到方案 FullCBE，方案描述如下：

Setup：在 BasicCBE. Setup 算法基础上，额外选择一个 Hash 函数 $H_3: \{0,1\}^* \to Z_q^*$。算法输出为公开参数集 $params=\{q, G_1, G_2, G_T, \varphi, e, n, P_1, P_2, g, P_{pub}, H_1, H_2, H_3\}$，CA 的主密钥 s，明文空间 $\coprod=\{0,1\}^{n-k_0}$，以及密文空间 $\coprod=G_1^* \times \{0,1\}^n$，其中 $k_0 \in Z^+$。

SetKeyPair：同 BasicCBE. SetKeyPair 算法。

Certify：同 BasicCBE. Certify 算法。

Enc：输入为 $\langle \tau, id, upk, M\rangle$，算法随机选择 $\sigma \in \{0,1\}^{k_0}$，置 $r=H_3(M||\sigma||\tau||id||upk)$，$Q_{id}=H_1(\langle \tau||id||upk\rangle)P_1+P_{pub}$，计算并输出密文 $C=\langle U, V\rangle=\langle rQ_{id}, (M||\sigma) \oplus H_2(g^r, upk^r)\rangle$。

Dec：输入为 $\langle Cert_{id,\tau}, SK, \langle U, V\rangle\rangle$，算法依次计算 $g=e(U, Cert_{id,\tau})$，$M||\sigma=V \oplus H_2(g, g^{usk})$ 和 $r=H_3(M||\sigma||\tau||id||upk)$。若 $U=r(H_1(\langle \tau||id||upk\rangle)P_1+P_{pub})$ 成立，则输出 M；否则输出 $\perp$。

4 安全性证明

首先证明方案 BasicCBE 的安全性。

定理 1 若 Hash 函数 H_1 和 H_2 为随机预言，则在 p-BDHI 假设下，方案 BasicCBE 是 Type I IND-CBE-CPA 安全

的;在 1-BDHI 假设下,BasicCBE 是 Type II IND-CBE-CPA 安全的。

由于篇幅限制,以及上述定理两个部分的证明思路具有相似性,因此下文仅给出定理第二部分的证明,即在 1-BDHI 假设下,方案 BasicCBE 是 Type II IND-CBE-CPA 安全的。该部分的证明需经两次安全规约,具体过程如下。

证明:若对方案 BasicCBE 存在 Type II IND-CBE-CPA 敌手 A_2,且 A_2 的优势至少为 ε,对 H_1 最多作了 q_1 次不同询问,则存在针对如下公钥加密方案 BasicPub 的 IND-CPA 敌手 B,其优势至少为 ε/q_1。

方案 BasicPub 由如下 3 个多项式时间算法组成。

Keygen:输入为安全参数 $k\in Z^+$,算法执行如下:(1)生成参数集$\{q,G_1,G_2,G_T,\varphi,e,n,P_1,P_2,g\}$,其中各参数同 BasicCBE;(2)随机选择 $s,x,h_0\in Z_q^*$,并分别计算 $P_{pub}=sP_1$ 和 $upk=g^x$;(3)选择 Hash 函数 $H_2:G_T\times G_T\to\{0,1\}^n$,其中 $n\in Z^+$。算法输出公钥为 $K_{pub}=\{q,G_1,G_2,G_T,\varphi,e,n,P_1,P_2,g,s,P_{pub},upk,h_0,H_2\}$,私钥为 $K_{pri}=x$,明文空间为 $\coprod:=\{0,1\}^n$,密文空间为 $\coprod=G_1^*\times\{0,1\}^n$。

Encrypt:对明文 M 加密,算法随机选择 $r\in Z_q^*$,计算并输出密文 $C=\langle U,V\rangle=\langle r(h_0P_1+P_{pub}),M\oplus H_2(g^r,upk^r)\rangle$。

Decrypt:对密文 $C=\langle U,V\rangle$ 解密,算法计算并输出明文 $M=V\oplus H_2(e(U,\frac{1}{h_0+s}P_2),(e(U,\frac{1}{h_0+s}P_2))^{K_{pri}})$。

下面由敌手 A_2 构造针对方案 BasicPub 的 IND-CPA 敌手 B。记敌手 B 所攻击方案 BasicPub 的挑战者为 X,X 运行 BasicPub. Keygen 算法生成一公钥/私钥对 $K_{pub}=\{q,G_1,G_2,G_T,\varphi,e,n,P_1,P_2,g,s,P_{pub},upk_{ch},h_0,H_2\}$ 和 $K_{pri}=x_{ch}$,并将 K_{pub} 输出给 B。敌手 B 模仿方案 BasicCBE 的 Type II IND-CBE-CPA 挑战者与 A_2 进行如下交互以实现对方案 BasicPub 的 IND-CPA 攻击。

Setup:B 首先选择一索引值 $I(1\leqslant I\leqslant q_1)$,然后将$\{q,G_1,G_2,G_T,\varphi,e,n,P_1,P_2,g,P_{pub},H_1,H_2\}$作为方案 BasicCBE 的公开参数集、$s$ 作为 CA 的主密钥以及 upk_{ch} 作为挑战公钥输出给 A_2,其中 H_1 为 B 所控制的随机预言。B 按如下方式应答 A_2 对 H_1 的询问:

H_1-query:B 构造并维持一列表 H_1^{list},该列表初始为空,列表中每一项的形式为元组$\langle(\tau||id||upk_{ch})_i,h_i\rangle$,其索引为$(\tau||id||upk_{ch})_i$。当 A_1 对$(\tau||id||upk_{ch})_i$ 作 H_1-query 时,B 处理如下:若$(\tau||id||upk_{ch})_i$ 已经存在于某一项$\langle(\tau||id||upk_{ch})_i,h_i\rangle$中,则 B 应答 $H_1((\tau||id||upk_{ch})_i)=h_i$;若$(\tau||id||upk_{ch})_i$ 不在任何一项中,并且$(\tau||id||upk_{ch})_i$ 是第 I 个不同的 H_1-query 输入,则 B 应答 $H_1((\tau||id||upk_{ch})_i)=h_0$,并且在列表 H_1^{list} 中添加新项$\langle(\tau||id||upk_{ch})_I,h_0\rangle$;否则,$B$ 随机选择 $h_i\in Z_q^*$,应答 $H_1((\tau||id||upk_{ch})_i)=h_i$,并在列表 H_1^{list} 中添加新项$\langle(\tau||id||upk_{ch})_i,h_i\rangle$。

Challenge:A_2 输出$\langle\tau_{ch},id_{ch},M_0,M_1\rangle$进行挑战,$B$ 应答如下:若列表 H_1^{list} 的第 I 项为空,即 A_2 未曾作过第 I 个 H_1-query,则 B 将列表 H_1^{list} 的第 I 项置为$\langle\tau_{ch}||id_{ch}||upk_{ch},h_0\rangle$;否则,若 $\tau_{ch}||id_{ch}||upk_{ch}\neq(\tau||id||upk_{ch})_I$,则 B 终止并退出游戏(该事件记为 Event 1),否则,B 将$\langle M_0,M_1\rangle$提交给挑战者 X 作为其 IND-CPA 游戏的挑战。X 随机选择比特 $b\in\{0,1\}$,运行算法 BasicPub. Encrypt 对 M_b 加密,并将结果 C_{ch} 输出给 B。B 将 C_{ch} 作为挑战密文输出给 A_2。

Guess:最终,A_2 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。

由以上的交互过程可以看出 B 对 H_1-query 的应答在 Z_q^* 中是随机均匀分布的,与 A_2 攻击方案 BasicCBE 的真实环境一致,所以在 B 模拟期间不终止的情况下,有 $Adv(A_2)\geqslant\varepsilon$。

下面求 B 在模拟期间不会异常终止的概率。由上述过程可知,B 在模拟期间异常终止当且仅当事件 Event 1 发生(记为 H_1),即 A_2 在挑战阶段的输出为$\langle\tau_{ch},id_{ch},M_0,M_1\rangle$,但 $\tau_{ch}||id_{ch}||upk_{ch}\neq(\tau||id||upk_{ch})_I$。因此,若记 B 在模拟期间没有终止的事件为 H,那么有 $\Pr[H]=\Pr[\neg H_1]=1/q_1$。

易见,B 获胜的优势 $Adv(B)=Adv(A_2)\cdot\Pr[H]\geqslant\varepsilon/q_1$。

下面证明若存在针对方案 BasicPub 的 IND-CPA 敌手 B,优势为 ε',且对 H_2 最多作 q_2 次不同询问,则存在一个多项式时间算法 A 可以求解 1-BDHI 问题,其优势至少为 ε'/q_2。

假定算法 A 输入的随机 1-BDHI 实例为$\langle q,G_1,G_2,G_T,\varphi,e,P_1,P_2,xP_2\rangle$,其中 x 为 Z_q^* 的一个随机元素。算法 A 以如下的方式与 B 进行交互以获得该 1-BDHI 实例的解 $e(P_1,P_2)^{1/x}$:

Setup:算法 A 模拟方案 BasicPub. Keygen 算法生成一公钥并输出给敌手 B,过程如下:置 $Q_2=xP_2$,分别计算 $Q_1=\varphi(Q_2)=xP_1$ 和 $g=e(Q_1,Q_2)$;随机选择 $s,h_0,y\in Z_q^*$,分别计算 $P_{pub}=sQ_1$ 和 $upk=e(P_1,P_2)^y=e(Q_1,Q_2)_{x^2}^y$。最终,$A$ 将 $K_{pub}=\{q,G_1,G_2,G_T,\varphi,e,n,Q_1,Q_2,g,s,P_{pub},upk,h_0,H_2\}$作为方案 BasicPub 的公钥输出给 B,其中 H_2 是由 A 所控制的随机预言。易见公钥 K_{pub} 对应的私钥为 $K_{pri}=\frac{y}{x^2}$,但 K_{pri} 不为 A 所知。由于 $e(h_0Q_1+P_{pub},\frac{1}{h_0+s}Q_2)=e(Q_1,Q_2)$,因此 K_{pub} 是方案 BasicPub 的一个有效公钥。

H_2-query:为了应答 B 对 H_2 的询问,A 构造并维持一列表 H_2^{list},该列表初始为空,列表中每一项为元组$\langle\gamma_1,\gamma_2,\zeta\rangle$。当 B 对$\langle\gamma_1,\gamma_2\rangle$作 H_2-query 时,A 处理如下:若$\langle\gamma_1,\gamma_2\rangle$已经存在于 H_2^{list} 的某一项$\langle\gamma_1,\gamma_2,\zeta\rangle$中,则 A 应答 $H_2(\gamma_1,\gamma_2)=\zeta$。否则,$A$ 随机选择 $\zeta\in\{0,1\}^n$,应答 B 为 $H_2(\gamma_1,\gamma_2)=\zeta$,同时在列表 H_2^{list} 中插入新项$\langle\gamma_1,\gamma_2,\zeta\rangle$。

Challenge:敌手 B 输出两个等长的明文 M_0 和 M_1 给 A 进行挑战。A 随机选择 $R\in\{0,1\}^n$ 和 $r\in Z_q^*$,计算挑战密文为 $C_{ch}=\langle U,V\rangle=\langle r(h_0P_1+sP_1),R\rangle=\langle\frac{r}{x}(h_0Q_1+P_{pub}),R\rangle$,并输出给 B。显然,对 C_{ch} 的解密应为 $V\oplus H_2(e(U,\frac{1}{h_0+s}P_2),e(Q_1,Q_2)_{x^2}^{y\cdot\frac{r}{x}})$。

Guess:当敌手 B 向 A 给出其对 b 的猜测 $b'\in\{0,1\}$ 后,A 则在 H_2^{list} 中随机选择一项$\langle\gamma_1,\gamma_2,\zeta\rangle$,计算并返回 $\gamma_2^{\frac{1}{y}}$。注意,如果 $\gamma_2=e(Q_1,Q_2)_{x^2}^{y\cdot\frac{r}{x}}$,那么 $\gamma_2^{\frac{1}{y}}=e(P_1,P_2)^{\frac{1}{x}}$。

由 A 的模拟过程可以看出,A 与交互过程完全模拟了 B 攻击方案 BasicPub 的真实环境,因此有 $Adv(B)\geqslant\varepsilon'$。

下面分析 A 输出上述 1-BDHI 实例的正确解 $e(P_1,P_2)^{1/x}$ 的优势。记 H 为 B 在上述模拟期间询问过 $H_2(*,e$

$(Q_1, Q_2)^{\frac{r}{x}\cdot\frac{r}{x}}$)的事件，由于 H_2 是随机预言，因此 B 在事件 H 未发生的前提下获胜的概率为 $\Pr[B\ wins\ |\neg H]=1/2$，又 $\Pr[B\ wins]\leqslant\Pr[H]+\frac{1}{2}(1-\Pr[H])=\frac{1}{2}+\frac{1}{2}\Pr[H]$，$\Pr[B\ wins]\geqslant\Pr[B\ wins\ |\neg H]\Pr[\neg H]=\frac{1}{2}(1-\Pr[H])=\frac{1}{2}-\frac{1}{2}\Pr[H]$，因此 $\Pr[H]\geqslant|2\Pr[B\ wins]-1|=Adv(B)\geqslant\varepsilon$。由于 B 对 H_2 最多作了 q_2 次不同询问，因此在事件 H 发生的前提下，A 输出 q_1-BDHI 实例的正确解 $e(P_1,P_2)^{1/x}$ 的概率为 $1/q_2$。

易见，A 获胜的优势 $Adv(A)=Adv(B)\cdot\Pr[H]\geqslant\varepsilon'/q_2$。

综上，若存在针对 BasicCBE 的 Type II IND-CBE-CPA 敌手，则必然存在一个多项式时间算法可以求解 1-BDHI 问题，这与 p-BDHI 假设相矛盾，因此 BasicCBE 是 Type II IND-CBE-CPA 安全的。

对于方案 FullCBE 的安全性，有如下结论。

定理 2 若 H_3 为随机预言，且 BasicCBE 是 IND-CBE-CPA 安全的，则方案 FullCBE 是 IND-CBE-CCA 安全的。

由于方案 FullCBE 是在方案 BasicCBE 的基础之上应用 Fujisaki-Okamoto 变换[11]获得的，文献[10]已证明了 Fujisaki-Okamoto 变换能够将 IND-CBE-CPA 安全的 CBE 方案的安全性增强为 IND-CBE-CCA 安全的，因此定理 2 显然是成立的。

5 性能评价

表 1 给出了该方案与已有 CBE 方案[1-3]的性能对比，其中 p，e，m 和 h 分别表示线对运算、指数运算、乘运算以及 Hash 运算；r 表示加密中所使用的随机数。可以看出，该方案的总体性能，尤其是加密算法，要优于已有的 CBE 方案。

表 1 本文方案与其它方案的性能比较

方案	加密	解密	密文长度
文献[1]	2p+1m+1e+4h	1p+1m+3h	$\|M\|+\|r\|+\|G_1\|$
文献[2]	3m+2e+2h+S+MAC	3p+2m+2h+R+MAC	$\|M\|+3\|G_1\|+\|com\|+\|tag\|$
文献[3]	3m+2e+3h+sig	3p+2m+1h+vfy	$\|M\|+3\|G_1\|+\|vk\|+\|s\|$
本文方案	2m+2e+3h	1p+1m+1e+2h	$\|M\|+\|r\|+\|G_1\|$

结束语 提出了一个高效的基于线对的 CBE 方案，并在随机预言模型中给出了安全性证明。在 p-BDHI 假设下，该方案被证明是 IND-CBE-CCA 安全的。在方案效率上，本文方案仅在解密时计算一个线对，将方案的线对计算的次数降至最少，而已有的其它方案都需要 3 个线对计算，因此本文方案是高效的，其总体性能要优于现有的其它方案。

无线对 CBE 方案的设计目前仍是一个公开问题，因此这方面的研究将是下一步的工作重点。此外，标准模型下安全的高效 CBE 方案的构造也将是另一研究重点。

参 考 文 献

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

[2] Morillo P, Râfols C. Certificate-based Encryption without Random Oracles[R]. Cryptology ePrint Archive, 2006/12

[3] Galindo D, Morillo P, Râfols C. Improved Certificate-based Encryption in the Standard Model [J]. Journal of System and Software, 2008, 81(7): 1218-1226

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

[5] Joux A. A One Round Protocol for Tripartite Diffe-Hellman[C]// Proceedings Fourth International Symposium on Algorithmic Number Theory. Leiden, Netherlands, 2000

[6] Sakai R, Kasahara M. ID Based Cryptosystems with Pairing on Elliptic Curve[R]. Cryptology ePrint Archive, 2003/054

[7] Chen L Q, Cheng Z H. Security Proof of Sakai-Kasahara's Identity-based Encryption Scheme[R]. Cryptology ePrint Archive, 2005/226

[8] Boneh D, Boyen X. Efficient Selective-ID Secure Identity Based Encryption without Random Oracles. Proceedings[C]// Advances in Cryptology - EUROCRYPT 2004. Interlaken, Switzerland, 2004

[9] ElGamal T E. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. Proceedings[C]// Advances in Cryptology -CRYPTO'84. California, USA, 1985

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

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

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

[13] Barreto P S L M, Kim H Y, Lynn B, et al. Efficient Algorithms for Pairing-based Cryptosystems. Proceedings[C]// Advances in Cryptology - CRYPTO 2002. California, USA, 2002

[14] MIRACL, Multiprecision Integer and Rational Arithmetic C/C++ Library. http://indigo.ie/mscott/

(上接第 20 页)

[52] Chrabakh W, Wolski R. GridSAT: A Chaff-based Distributed SAT Solver for the Grid[C]// Proceedings of the ACM/IEEE Conference on Supercomputing. Phoenix, 2003: 1-13

[53] Chrabakh W, Wolski R. GrADSAT: A Parallel SAT Solver for the Grid[R]. UCSB 2003-05 (pdf). http://www.cs.ucsb.edu/~chrabakh/

[54] Wolfgang B, Wolfgang W, Wolfgang K, et al. ZetaSAT - Boolean Satisfiability solving on Desktop Grids [C]// International Symposium on Cluster Computing and the Grid. Cardiff, 2005: 1079-1086

[55] Tobias S, Bernd B. PICHAFF2 - A Hierarchical Parallel SAT Solver [C]// International Workshop on Microprocessor Test and Verification. Austin, 2004: 56-61

[56] Tobias S, Matthew L, Bernd B. PaMira - a Parallel SAT Solver with Knowledge Sharing[C]// International Workshop on Microprocessor Test and Verification. Austin, 2005: 29-36

[57] Matthew L, Tobias S, Bernd B. Multithreaded SAT Solving[C]// The 12th Asia and South Pacific Design Automation Conference. Yokohama, 2007: 926-931