改进的无双线性对的无证书签密方案

周才学 王飞鹏
(九江学院信息科学与技术学院 九江 332005)

摘 要 对一个无双线性对的无证书签密方案进行了密码学分析,指出该方案不满足机密性和不可伪造性,并指出其安全证明中的错误之处,然后对其进行了改进。在随机预言机模型中,基于计算 Diffie-Hellman 问题和离散对数问题,证明了改进方案具有机密性和不可伪造性。效率分析表明,改进方案是高效的。

关键词 无证书签密,保密性,不可伪造性,双线性对,随机预言机模型
中图法分类号 TP309 **文件标识码** A

Improved Certificateless Signcryption Scheme without Pairing

ZHOU Cai-xue WANG Fei-peng
(School of Information Science and Technology, University of Jiujiang, Jiujiang 332005, China)

Abstract A certificateless signcryption scheme without pairing was analyzed. This paper showed the scheme can not achieve confidentiality and unforgeability. The mistakes in the security proofs were pointed out, and an improved scheme was proposed. The improved scheme was proved to be confidential under the computational diffie-hellman(CDH) assumption and existentially unforgeable under the discrete logarithm(DL) assumption in random oracle model(ROM). Performance analysis shows the improved scheme is of high efficiency.

Keywords Certificateless signcryption, Confidentiality, Unforgeability, Bilinear pairings, Random oracle model

1 引言

1984年,Shamir[1]提出了基于身份的密码体制,即用户的公钥可通过用户的身份信息直接计算,公钥不需要证书,从而简化了公钥的管理。但基于身份的密码体制天生就具有密钥托管的问题,为了克服这种缺陷,2003年 AI-Riyami 和 Paterson[2]提出了无证书公钥密码系统。在无证书体制中,用户的私钥由两部分组成,一部分由 KGC(Key Generation Center)产生,另一部分由用户自己掌握,这样就解决了密钥托管问题,同时公钥也不需要证书,因此这种密码体制具有巨大的优越性。无证书体制自被提出后,立即成为密码学界的研究热点,人们对其进行了广泛的研究[3,4]。

2008年,Barbosa 和 Farshim[5]首次将无证书体制推广到签密[6]并给出了一个具体方案。同一年,Aranha 等人[7]、Wu 等人[8]基于双线性对也各提出一个方案,但 Selvi 等人[9]于2009年指出文献[5,7,8]都是不安全的,他们给出了具体的攻击方法并提出一个不使用双线性对的无证书签密方案。此后,人们又提出了多接收者无证书签密[10-12]、无证书混合签密[13-15]、标准模型下的无证书签密[16-18]、无证书广播签密[19]等。2011年,刘文浩等人[20]提出一个不使用双线性对的无证书签密方案并给出了内部攻击模型下的安全性证明。

本文对文献[20]进行了密码学分析,分析表明该方案达不到保密性和不可伪造性的目的。指出了其安全证明中的错误之处,对原方案给出了几种攻击方法,并对原方案进行了改进,对改进后的方案进行了内部攻击模型下的安全性证明并对效率进行了分析,分析表明改进方案具有较高的效率。

2 一些基本概念

2.1 无证书签密的形式化定义

一个无证书签密方案由以下7个算法组成:

(1)系统建立(Setup):输入安全参数 k,输出系统参数 $Params$ 和主密钥 x,保密主密钥 x;

(2)部分密钥生成(Partial-Key-Extract):输入 $Params$、主密钥 x 和一个用户身份 ID,输出该用户的部分私钥 d_{ID} 和部分公钥 p_{ID};

(3)设置秘密值(Set-Secret-Value):输入 $Params$ 和一个用户身份 ID,输出一个秘密值 s_{ID};

(4)设置公钥(Set-Public-Key):输入 $Params$、一个用户的部分公钥 p_{ID} 和他的秘密值 s_{ID},输出该用户的公钥 pk_{ID};

(5)设置私钥(Set-Private-Ket):输入 $Params$、一个用户的部分私钥 d_{ID} 和他的秘密值 s_{ID},输出用户的完整私钥 sk_{ID};

(6)签密(Signcrypt):输入 $Params$、发送者的身份 ID_S、发送者的私钥 sk_{ID_S}、接收者的身份 ID_R、接收者的公钥 pk_{ID_R} 和消息 m,输出签密文 σ;

(7)解签密(Unsigncrypt):输入 $Params$、发送者身份 ID_S、发送者公钥 pk_{ID_S}、接收者身份 ID_R、接收者私钥 sk_{ID_R} 和

到稿日期:2012-12-08 返修日期:2013-03-12
周才学(1966—),男,硕士,副教授,CCF会员,主要研究方向为密码学与网络信息安全,E-mail:charlesjjjx@126.com;王飞鹏(1982—),男,硕士,讲师,主要研究方向为软件技术。

签密文 σ，假如密文合法，输出 m，否则输出“失败”。

上述算法要满足 $Signcrypt(Params, m, ID_S, sk_{ID_S}, ID_R, pk_{ID_R}) = \sigma, Unsigncrypt(\sigma, Params, ID_S, pk_{ID_S}, ID_R, sk_{ID_R}) = m$。

2.2 无证书签密的安全模型

在无证书密码体制中，因为没有证书来对用户的公钥进行认证，这样攻击者就可以把用户的公钥替换为自己任意选定的值，所以无证书密码体制存在两类攻击者[2]：第Ⅰ类攻击者 A_I，他不知道系统主密钥，但是他可以替换任意用户的公钥；第Ⅱ类攻击者 A_{II}，他知道系统主密钥，所以他可以计算出每个用户的部分私钥，但是他不可以替换用户的公钥。在实际应用中 A_I 模拟的是除 KGC 之外的攻击者，A_{II} 模拟的是恶意 KGC 的非法攻击。

无证书签密方案在第Ⅰ类攻击者 A_I 和第Ⅱ类攻击者 A_{II} 下都需要满足机密性和不可伪造性。下面分别以游戏的方式直观给出无证书签密方案的安全模型。

定义 1(类型Ⅰ攻击下的保密性) 若不存在任何多项式有界的敌手 A_I 以不可忽略的优势在以下游戏中获胜，则称该无证书签密方案在适应性选择密文攻击下具有不可区分性(IND-CLSC-CCA2)。

1. 初始化，挑战者 C 输入安全参数 k，运行 Setup，并输出系统参数 $Params$ 给敌手 A_I，保密主密钥。

2. 寻找阶段，敌手 A_I 可以适应性地执行多项式有界次的以下提问：

(1)Hash 提问：A_I 可以对任何输入进行 Hash 提问。

(2)部分密钥生成提问：A_I 输入一个身份 ID，挑战者 C 计算身份 ID 的部分私钥 d_{ID} 和部分公钥 p_{ID} 并输出 d_{ID} 给 A_I。

(3)私钥生成提问：A_I 选择一个身份 ID，挑战者 C 计算相应的私钥 sk_{ID} 并返回给 A_I。如果相应的公钥被替换，则不允许询问该预言机，这是因为挑战者不知道相应的秘密值所以不能提供完整私钥。

(4)公钥提问：A_I 输入身份 ID，挑战者 C 计算相应的公钥 pk_{ID}。

(5)替换公钥提问：在任何时间，A_I 选择一个新的值 pk_{ID}' 替换原来的公钥 pk_{ID}。

(6)签密提问：A_I 选择身份 ID_a，ID_b 和明文 m，设 sk_a 为 ID_a 的私钥，pk_b 为 ID_b 的公钥，C 计算 $\sigma = Signcrypt(m, sk_a, pk_b)$ 并将结果 σ 发送给 A_I。假如 ID_a 的公钥被替换，为了产生正确的回答，要求 A_I 另外提供 ID_a 的秘密值给 C。

(7)解签密提问：A_I 选择身份 ID_a，ID_b 和密文 σ，设 sk_b 为 ID_b 的私钥，pk_a 为 ID_a 的公钥，C 计算 $Unsigncrypt(\sigma, pk_a, sk_b)$，最后发送结果明文 m 或“失败”给 A_I。如果 ID_b 的公钥被替换，为了产生正确的回答，要求 A_I 另外提供 ID_b 的秘密值给 C。

3. 挑战阶段，A_I 生成两个相同长度的明文 m_0, m_1 和希望挑战的两个身份 ID_a^*，ID_b^*，但不能对 ID_b^* 执行部分密钥生成提问或私钥生成提问(如果是外部安全模型，则要求不能对 ID_a^*，ID_b^* 执行部分密钥生成提问或私钥生成提问)，C 随机选择 $j \in \{0,1\}$，计算 $\sigma^* = Signcrypt(m_j, sk_a, pk_b)$，把 σ^* 输出给 A_I。

4. 在猜测阶段，A_I 可以像寻找阶段一样执行多项式有界次的适应性的提问，但不能对 ID_b^* 执行部分密钥生成或私钥生成提问，也不能对密文 σ^*、发送者 ID_a^* 和接收者 ID_b^* 执行 Unsigncrypt 提问，除非 ID_a^* 或 ID_b^* 的公钥被替换。

5. 最终，A_I 输出 j' 作为对 j 的猜测，若 $j' = j$，则 A_I 获胜。

注：在文献[5]中，作者定义了一类类型 I′攻击者，它与类型Ⅰ攻击者的区别是：类型 I′攻击者在任何时候都不能对 ID_b^* 执行部分密钥生成提问，而类型Ⅰ攻击者是若 ID_b^* 的公钥在挑战密文发布之前已经被替换则不能对 ID_b^* 执行部分密钥生成提问。文献[5]的引理 1 证明，一个无证书签密方案如果在类型 I′和类型Ⅱ下是内部攻击模型下安全的，则也是类型Ⅰ内部攻击模型下安全的，所以定义 1 中要求任何时候都不能对 ID_b^* 执行部分密钥生成提问，这一点与文献[20]相同。

定义 2(类型Ⅱ攻击下的保密性) 若不存在任何多项式有界的敌手 A_{II} 以不可忽略的优势在以下游戏中获胜，则称该无证书签密方案在适应性选择密文攻击下具有不可区分性(IND-CLSC-CCA2)。

1. 初始化，挑战者 C 输入安全参数 k，运行 Setup 算法，并输出 $Params$ 和主密钥 x 给敌手 A_{II}；

2. 在寻找阶段，敌手 A_{II} 可以执行定义 1 中除“公钥替换提问”和“部分密钥生成提问”以外的所有提问，提问方法同定义 1；

3. 挑战阶段，A_{II} 生成两个相同长度的不同明文 m_0, m_1 和希望挑战的两个身份 ID_a^*，ID_b^*，但不能对 ID_b^* 执行私钥生成提问，C 随机选择 $j \in \{0,1\}$，计算 $\sigma^* = Signcrypt(m_j, sk_a, pk_b)$ 并把 σ^* 输出给 A_{II}。

4. 在猜测阶段，A_{II} 像寻找阶段一样适应性地执行多项式有界次的提问，但不能对 ID_b^* 执行私钥生成提问，也不能对密文 σ^*、发送者 ID_a^* 和接收者 ID_b^* 执行 Unsigncrypt 提问。

5. 最终，A_{II} 输出 j' 作为对 j 的猜测，若 $j' = j$，则 A_{II} 获胜。

定义 3(类型Ⅰ攻击下的不可伪造性) 若不存在任何多项式有界的敌手 A_I 以不可忽略的优势在以下游戏中获胜，则称该无证书签密方案在适应性选择消息攻击下具有不可伪造性(EUF-CLSC-CMA)。

1. 初始化和寻找阶段同定义 1；

2. A_I 输出某发送者 ID_a(对应接收者为 ID_b)对某消息 m 的签密 σ，且 (σ, ID_a, ID_b) 不是签密预言机产生的，也未对 ID_a 进行过部分密钥生成提问或私钥生成提问，若 $Unsigncrypt(\sigma, pk_a, sk_b)$ 的结果不是“错误”，则 A_I 获胜。

定义 4(类型Ⅱ攻击下的不可伪造性) 若不存在任何多项式有界的敌手 A_{II} 以不可忽略的优势在以下游戏中获胜，则称一个无证书签密方案在适应性选择消息攻击下具有不可伪造性(EUF-CLSC-CMA)。

1. 初始化和寻找阶段同定义 2；

2. A_{II} 输出某发送者 ID_a(对应接收者为 ID_b)对某消息 m 的签密 σ，且 (σ, ID_a, ID_b) 不是签密预言机产生的，也未对 ID_a 进行过私钥生成提问，若 $Unsigncrypt(\sigma, pk_a, sk_b)$ 的结果不是“错误”，则 A_{II} 获胜。

3 对刘文浩等人方案的安全性分析及改进

3.1 原方案描述

1. 系统参数建立。输入参数 k，产生两个大素数 p 和 q，

且 $q|p-1$，P 为椭圆曲线上的循环群 G 中任意一阶为 q 的生成元，选取安全的 Hash 函数，$H_1:\{0,1\}^* \times G \rightarrow Z_q^*$，$H_2:\{0,1\}^* \rightarrow Z_q^*$，$H_3:G \rightarrow \{0,1\}^*$，明文消息 m 为任意比特长。KGC 随机选取一个主密钥 $z \in Z_q^*$，计算 $y=zP$，公开参数 $\{p,q,P,y,H_1,H_2,H_3\}$，保密主密钥 z。

2. 用户密钥的生成。给定用户身份 ID_i，KGC 随机选取 $r_i \in Z_q^*$，计算 $R_i=r_iP$，$D_i=r_i+zH_1(ID_i,R_i)$，通过安全渠道返回 D_i 给用户 ID_i，并作为其部分私钥，$R_i=r_iP$ 为用户部分公钥。

用户 ID_i 随机选取秘密值 $x_i \in Z_q^*$ 作为其长期私钥，生成对应的私钥 (x_i,D_i)，计算 $X_i=x_iP$，生成公钥 (X_i,R_i)。因此，用户 A 的私钥 $SK_A=(x_A,D_A)$，公钥 $PK_A=(X_A,R_A)$。用户 B 的私钥 $SK_B=(x_B,D_B)$，公钥 $PK_B=(X_B,R_B)$。

用户 ID_i 可以通过计算等式 $R_i+H_1(ID_i,R_i)y=D_iP$ 是否成立来判断 KGC 分配给自己的部分私钥是否有效。

3. 签密。当 Alice 要发送消息 m 给 Bob 时，Alice 进行以下操作：

(1)随机选取 $a \in Z_q^*$，计算 $T_A=aP$，$h_1=H_1(ID_B,R_B)$，$h=H_2(T_A \| ID_A \| m)$，$s=a/(x_A+D_A+h)$，$V_A=a(R_B+X_B+h_1y)$，$c=H_3(V_A) \oplus m$，发送消息 $\sigma=(h,s,c)$ 给 Bob。

4. 解签密。收到密文 σ 后，Bob 进行以下操作：

(1)计算 $h_1'=H_1(ID_A,R_A)$，$V_B=s(x_B+D_B)(X_A+R_A+h_1'y+hP)$，恢复消息 $m=H_3(V_B) \oplus c$；

(2)若 $H_2(s(X_A+R_A+h_1'y+hP) \| ID_A \| m)=h$ 成立，则 Bob 接收消息 m。

将 (h,s,m) 提交给第三方进行公开验证，验证等式 $H_2(s(X_A+R_A+h_1'y+hP) \| ID_A \| m)=h$ 是否成立。

3.2 对原方案的攻击

1. 对原方案的伪造性攻击。

这里考虑的是内部攻击者即接收者 ID_B 的伪造攻击，伪造步骤如下：

接收者 B 得到一个发送者为 ID_A，接收者为 ID_B 的签密文 $\sigma=(h,s,c)$，B 如下处理：

(1)先解密，计算 $h_1'=H_1(ID_A,R_A)$，$V_B=s(x_B+D_B)(X_A+R_A+h_1'y+hP)$，$m=H_3(V_B) \oplus c$；

(2)若 $H_2(s(X_A+R_A+h_1'y+hP) \| ID_A \| m)=h$ 成立，则 B 确信 $\sigma=(h,s,c)$ 为合法签密；否则，终止；

(3)任取一身份 ID_c，作 ID_c 的私钥生成询问，得到 $SK_c=(x_c,D_c)$；

(4)计算 $V_c'=s(x_c+D_c)(X_A+R_A+h_1'y+hP)$，$c'=H_3(V_c') \oplus m$；

(5)则 $\sigma'=\{h,s,c'\}$ 是发送者 ID_A，接收者 ID_c 的签密文伪造成功。

这里给出一种实例：设 Alice 是卖电子飞机票的公司，Bob 是客户，当 Bob 获得 Alice 的关于电子飞机票的签名后，他可以把票卖给他的朋友如 Carol，这样 Bob 和 Carol 都可以登机。

2. 对原方案保密性的攻击。

攻击方法 1　对原方案不可区分性选择明文攻击：设发送者是 ID_S，接收者是 ID_R，攻击者 A 选择两个等长不同明文 m_0,m_1。经过签密预言机产生 $\sigma^*=(h^*,s^*,c^*)$。A 计算 $h_1'=H_1(ID_A,R_A)$，验证等式 $H_2(s^*(X_A+R_A+h_1'y+h^*P) \| ID_A \| m_0)=h^*$ 是否成立，若成立，则 $\sigma^*=(h^*,s^*,c^*)$ 是对 m_0 的签密，否则是对 m_1 的签密。

攻击方法 2　这里考虑的是内部攻击者即发送者 ID_S 的攻击，攻击步骤如下：

给定挑战密文 $\sigma^*=(h^*,s^*,c^*)$，发送者 ID_S 的私钥 $SK_S=(x_S,D_S)$ 和接收者 ID_R 的公钥 $PK_R=(X_R,R_R)$，攻击者 A 计算 $h_1=H_1(ID_B,R_B)$，$a^*=s^*(x_S+D_S+h^*)$，$V_S=a^*(R_R+X_R+h_1y)$，$m_b=H_3(V_S) \oplus c^*$。

攻击方法 3　设 $\sigma^*=(h^*,s^*,c^*)$ 是发送者为 A、接收者为 B 对消息 m_b 的挑战密文。考虑内部攻击者即发送者 A，A 任取一身份 ID_c，作 ID_c 的私钥询问得到 $SK_C=(x_C,D_C)$，先作任意猜测 m_b 为 m_0，计算 $h_1'=H_1(ID_B,R_B)$，$T_A'=s^*(X_A+R_A+h_1'y+h^*P)$，$h'=H_2(T_A' \| ID_C \| m_0)$，$s'=s^*(x_A+D_A+h^*)/(x_C+D_C+h')$，要求挑战者解密 $\sigma'=(h',s',c^*)$，显然 $\sigma'=(h',s',c^*)$ 是发送者为 ID_c、接收者为 ID_b 的密文，挑战者要么返回 m_0，要么返回 $\perp$，如果返回 m_0 则 σ^* 是 m_0 对应的签密密文，否则是 m_1 对应的签密密文。

3.3 对原方案的改进

步骤 1、2 同原方案；增加 $H_4:G \rightarrow Z_q^*$。

3. 签密。Alice 要发送消息 m 给 Bob 时，进行以下操作：

(1)随机选取 $a \in Z_q^*$，计算 $T=aP$，$h_1=H_1(ID_B,R_B)$，$V_A=a(R_B+X_B+h_1y)$，$U=H_4(V_A)P$，$h=H_2(T \| U \| X_A \| X_B \| ID_A \| ID_B \| m)$，$s=a/(x_A+D_A+h+H_4(V_A))$，$C=H_3(V_A) \oplus (m \| s)$，发送消息 $\sigma=(T,C,U)$ 给 Bob。

4. 解签密。收到密文 σ 后，Bob 进行以下操作：

(1)计算 $V_B=(x_B+D_B)T$，恢复消息 $m \| s=H_3(V_B) \oplus C$；

(2)计算 $h=H_2(T \| U \| X_A \| X_B \| ID_A \| ID_B \| m)$，$h_1'=H_1(ID_A,R_A)$，验证 $s(X_A+R_A+h_1'y+hP+U)=T$ 是否成立，成立则输出 m，否则输出 $\perp$。

将 (T,U,s,m) 提交给第三方进行公开验证，计算 $h=H_2(T \| U \| X_A \| X_B \| ID_A \| ID_B \| m)$，$h_1'=H_1(ID_A,R_A)$，验证等式 $s(X_A+R_A+h_1'y+hP+U)=T$ 是否成立。

注：把原方案的 $h=H_2(T_A \| ID_A \| m)$ 改为 $h=H_2(T \| U \| X_A \| X_B \| ID_A \| ID_B \| m)$，这样签名 s 就与特定接收者 ID_b 绑定了，这是为了防止本文给出的伪造性攻击。签名 s 中加入 $H_4(V_A)$，由于对内部攻击者 A 来说，$H_4(V_A)$ 是个未知量，若他还想通过保密性攻击方法 2 从 s 中求出 a，那么一个方程两个未知数无法求出，从而可以有效防止保密性攻击方法 2。在计算密文 C 时，对 $m \| s$ 进行加密，使得最后的签密文 σ 中不用公布 s，从而验证等式中有未知量 s，可以有效防止保密性攻击方法 1，同时也使得密文 C 与特定的发送者 ID_A 进行了绑定，可以有效防止保密性攻击方法 3。

4 方案分析

4.1 安全性分析

刘文浩等人的安全性证明中存在如下漏洞。在刘文浩等人的定理一中，Q 是一个 CDH 困难问题的解决者，其困难问题的输入为 (uP,vP)，其目标是计算出 uvP。首先，Q 设置 $y=uP$。在挑战阶段，参看刘文浩等人的原文第 5 页 36 行至第 6 页第 2 行。最后，Q 输出 $((V'-x_BT')-(r_BT'))\times(1/k)=auP$ 作为 CDH 问题的答案，其中 $V'=s^*(x_B+D_B)(R_A+$

$X_A+h_1'y+h^*P$)。注意到此处 a 的值对 Q 是已知的，因此 auP 可以直接计算，CDH 问题是知道(uP,vP)，要求计算出 uvP，u、v 对 Q 是未知的。另外，挑战身份 ID_B 的部分私钥 D_B 对 Q 是未知的，所以 V' 无法求出。定理一中的缺陷在定理二中同样存在。定理三的证明中同样存在一个漏洞。原文如下"Q 输出 $u=(a-s^*(r_A+x_A+h^*))/h_1's^*$ 作为解决 DL 困难问题的回答"，注意这里 Q 并不知道 a 的值，所以无法计算 u 的值。定理三的缺陷在定理四中同样存在。下面给出改进方案的安全证明。

定理 1(类型 I 攻击下的保密性)　在 ROM 中，若存在一个(IND-CLSC-CCA2)敌手 A_1 能够在概率多项式时间内以 ε 的优势在定义 1 中的游戏中获胜(最多 q_i 次 H_i 提问($i=1,2,3,4$)，q_s 次签密提问，q_{un} 次解签密提问)，那么存在一个区分者 Q 能够在概率多项式时间内以 $Adv^{IND\text{-}CCA2}(A_1)\geqslant(\varepsilon/q_1(q_3+q_4))(1-q_s(q_2+q_s)/2^k)(1-q_{un}/2^k)$ 的优势解决 CDH 问题。

证明：设 Q 是一个 CDH 问题的解决者，输入为(uP,vP)，其目标是计算 uvP。首先，Q 设 $y=uP$，Q 以 A_1 为子程序并充当(IND-CLSC-CCA2)游戏中的挑战者。游戏开始后，Q 发送(p,q,P,y,H_1,H_2,H_3,H_4)给 A_1，并维持表 L_1，L_2，L_3，L_4，L_d，L_{sk}，L_{pk} 分别用于跟踪 A_1 对预言机 H_1、H_2、H_3、H_4、部分私钥提取、私钥提取、公钥提取提问，另外设置表 L_{rec} 用于记录挑战身份的一些参数，开始每个表均为空。

H_1 提问：表 L_1 的格式为(ID,R,h_1,c)。当 Q 收到 A_1 对 $H_1(ID,R)$ 提问时，若(ID,R)在表 L_1 中存在，则输出 h_1 给 A_1；否则，Q 随机选择 $c\in\{0,1\}$，其中 $\Pr[c=1]=\delta$。当 $c=0$ 时，Q 随机选择 $h_1\in Z_q^*$，并将(ID,R,h_1,c) 加入表 L_1 中，输出 h_1；当 $c=1$ 时，令 $h_1=k$，输出 k 给 A_1，并将(ID,R,h_1,c)加入表 L_1 中。

H_2 提问：表 L_2 的格式为($T,U,X_A,X_B,ID_A,ID_B,m,h_2$)。当 Q 收到 A_1 对 $H_2(T\|U\|X_A\|X_B\|ID_A\|ID_B\|m)$ 提问时，若表 L_2 中已经存在，则输出 h_2 给 A_1；否则，Q 随机选择 $h_2\in Z_q^*$，将($T,U,X_A,X_B,ID_A,ID_B,m,h_2$)加入表 L_2 中，输出 h_2 给 A_1。

H_3 提问：表 L_3 的格式为(V,h_3)。当 Q 收到 A_1 对 $H_3(V)$ 提问时，若表 L_3 中已经存在，则输出 h_3 给 A_1；否则，Q 随机选择 $h_3\in\{0,1\}^*$，并将(V,h_3)加入表 L_3 中，输出 h_3 给 A_1。

H_4 提问：表 L_4 的格式为(V,h_4)。当 Q 收到 A_1 对 $H_4(V)$ 提问时，若表 L_4 中已经存在，则输出 h_4 给 A_1；否则，Q 随机选择 $h_4\in Z_q^*$，并将(V,h_4)加入表 L_4 中，输出 h_4 给 A_1。

部分私钥提取提问：表 L_d 的格式为(ID,D,R)。Q 先在表 L_1 查询(ID,R,h_1,c)，若 $c=1$，则输出失败并终止；否则，若(ID,D,R)在表 L_d 中存在，则输出(D,R)给 A_1；否则，Q 随机选择 $D,h_1\in Z_q^*$，计算 $R=DP-h_1y$，将(ID,D,R)加入表 L_d 中，(ID,R,h_1,c)加入表 L_1 中，输出(D,R)给 A_1。

私钥提取提问：表 L_{sk} 的格式为(ID,D,x)。Q 先在表 L_1 查询(ID,R,h_1,c)，若 $c=1$，则输出失败并终止；否则，若(ID,D,x)在表 L_{sk} 中存在，则输出(D,x)给 A_1；否则，Q 作部分私钥提取提问得 D，随机选择 $x\in Z_q^*$，把(ID,D,x)加入表 L_{sk} 中，并输出(D,x)给 A_1。

公钥提取提问：表 L_{pk} 的格式为(ID,R,X)。当 Q 收到 A_1 对身份 ID 的公钥提问时，若表 L_{pk} 中已经存在，则输出(R,X)给 A_1；否则，Q 先查询表 L_d 和 L_{sk}，若表中存在，则分别得到 R 和 x，计算 $X=xP$，将(ID,R,X)加入表 L_{pk} 中，并输出(R,X)给 A_1。若表 L_d 和 L_{sk} 中不存在，则查询表 L_1：若 $c=1$，则 Q 随机选择 $r,x\in Z_q^*$，计算 $R=rP,X=xP$，将(ID,R,X)加入表 L_{pk} 中，输出(R,X)并记录 r,x 到 L_{rec}(ID,r,x,c)中；若 $c=0$，则运行部分私钥提取提问，获得(D,R)，Q 随机选择 $x\in Z_q^*$，把(ID,D,x)加入表 L_{sk} 中，计算 $X=xP$，将(ID,R,X)加入列表 L_{pk} 中，并输出(R,X)。

公钥替换：签名者的身份为 ID，A_1 可以选择一个新的公钥替换原有公钥。

签密提问：发送者为 ID_A，接收者为 ID_B，消息为 m。Q 先在列表 L_1 查询(ID_A,R_A)，若 $c=0$，由于知道 ID_A 的完整私钥，Q 可以按正常方式完成签密；否则，$c=1$，Q 随机选 s，$h\in Z_q^*$，$U\in G$，在 L_1 中查询(ID_A,R_A,h_1,c)得 h_1，在 L_{pk} 中查询(ID,R,X)得 R_A 和 X_A，计算 $T=s(X_A+R_A+h_1y+hP+U)$，把($T,U,X_A,X_B,ID_A,ID_B,m,h$)加入到表 L_2 中，在 L_{sk} 中查询 ID_B 得 D_B,x_B，计算 $V_A=(x_B+D_B)T$，在 L_3 中查询 V_A 得 h_3，计算 $C=h_3\oplus(m\|s)$，输出 $\sigma=(T,C,U)$给 A_1。

解签密提问：发送者为 ID_A，接收者为 ID_B，密文为 $\sigma=(T,C,U)$。Q 先在表 L_1 查询(ID_B,R_B)：①若 $c=0$，由于知道 ID_B 的完整私钥，Q 可以按正常方式完成解签密；②若 $c=1$，则遍历 L_3 中的条目(V,h_3)，计算 $m\|s=h_3\oplus C$，在 L_1 中查询(ID_A,R_A,h_1')得 h_1'，在 L_{pk} 中查询(ID_A,R_A,X_A)得 R_A 和 X_A，在 L_2 中查询($T,U,X_A,X_B,ID_A,ID_B,m,h_2$)得 h_2，令 $h=h_2$，验证 $s(X_A+R_A+h_1'y+hP+U)=T$ 是否成立，若成立则输出 m，否则移到 L_3 中下一条目重新开始。若遍历完 L_3 中条目还没有消息返回，则输出$\perp$。

经过概率多项式次数上述提问后，A_1 输出两个希望接收挑战的身份(ID_A,ID_B)和两个等长的不同明文(m_0,m_1)。Q 先在表 L_1 查询(ID_B,R_B)，若 $c=0$，则失败并终止模拟；否则，Q 先作 ID_B 的公钥提问，以确保 x_B 和 r_B 被保存在 L_{rec} 中。然后，Q 随机选择 $C^*\in\{0,1\}^*$，$U^*\in G$，并设 $T^*=vP$，将挑战密文 $\sigma^*=(T^*,C^*,U^*)$发给 A_1。第二阶段的询问同第一阶段，最后 A_1 输出他的猜测。A_1 不知道 $\sigma^*=(T^*,C^*,U^*)$ 不是一个正确的密文除非他用 $V'=v(R_B+X_B+h_1y)$作 H_3 或 H_4 提问。如果这种情况发生，则 CDH 问题的候选答案将被保存在 L_3 或 L_4 中，Q 忽略 A_1 的猜测，随机从 L_3 或 L_4 中选取 V'，输出$((V'-x_BT^*)-(r_BT^*))\times(1/k)=vuP$ 作为 CDH 问题的答案，其中 x_B,r_B,T^*,V'对 Q 均已知。

下面求 Q 成功的概率。ID_B 被选为挑战身份的概率为 $1/q_1$，ID_B 被选为挑战身份蕴含着 A_1 没有对 ID_B 进行部分私钥或私钥提取提问[21]；Q 从 L_3 或 L_4 中随机选取 V'作为 CDH 问题的候选答案，成功的概率为 $1/(q_3+q_4)$；在进行签密提问时，由于 H_2 碰撞，挑战者中止行为的概率 $\Pr_1\leqslant q_s(q_2+q_s)/2^k$；在游戏中，挑战者拒绝有效密文的概率 $\Pr_2\leqslant q_{un}/2^k$。所以，$Q$ 解决 CDH 困难问题的优势：$Adv^{IND\text{-}CCA2}(A_1)\geqslant(\varepsilon/q_1(q_3+q_4))(1-q_s(q_2+q_s)/2^k)(1-q_{un}/2^k)$。

定理 2(类型 II 攻击下的保密性)　在 ROM 中，若存在一个(IND-CLSC-CCA2)敌手 A_2 能够在概率多项式时间内以 ε 的优势在定义 2 中的游戏中获胜(最多 q_i 次 H_i 提问($i=1,2,3,4$))，那么存在一个区分者 Q 能够在概率多项式时间内

以 $\varepsilon/q_1(q_3+q_4)$ 的优势解决 CDH 问题。

证明：CDH 问题的输入为 (uP,vP)，其目标是计算 uvP。敌手 A_2 除了知道定理 1 中所给定的条件以外，还知道系统主密钥 z。A_2 可以进行除定理 1 中“公钥替换”和“部分私钥提取”之外的所有提问，除“公钥提取提问”外，其它提问方法同定理 1。

公钥提取提问：表 L_{pk} 的格式为 (ID,R,X)。当 Q 收到 A_2 对身份 ID 的公钥提问时，若表 L_{pk} 中已经存在，则输出 (R,X) 给 A_2；否则，Q 先查询表 L_d 和 L_{sk}，若表中存在，则分别得到 R 和 x，计算 $X=xP$，将 (ID,R,X) 加入表 L_{pk} 中，并输出 (R,X) 给 A_2。若表 L_d 和 L_{sk} 中不存在，则查询表 L_1：若 $c=1$，则 Q 随机选择 $x\in Z_q^*$，设 $R=uP$，计算 $X=xP$，将 (ID,R,X) 加入表 L_{pk} 中，输出 (R,X) 并记录 x 到 $L_{mc}(ID,-,x,c)$ 中；若 $c=0$，则运行部分私钥提取提问，获得 (D,R)，Q 随机选择 $x\in Z_q^*$，把 (ID,D,x) 加入表 L_{sk} 中，计算 $X=xP$，将 (ID,R,X) 加入表 L_{pk} 中，并输出 (R,X)。

经过概率多项式次数上述提问后，A_2 输出两个希望接收挑战的身份 (ID_A,ID_B) 和两个等长不同明文 (m_0,m_1)。Q 先在表 L_1 查询 (ID_B,R_B)，若 $c=0$，则失败并终止模拟；否则，Q 先作 ID_B 的公钥提问，以确保 x_B 被保存下来。然后，Q 随机选择 $C^*\in\{0,1\}^*$，$U^*\in G$，并设 $T^*=vP$，将挑战密文 $\sigma^*=(T^*,C^*,U^*)$ 发给 A_2。第二阶段的提问同第一阶段，最后 A_2 输出他的猜测。A_2 不知道 $\sigma^*=(T^*,C^*,U^*)$ 不是一个正确的密文除非他用 $V'=v(R_B+X_B+h_1y)$ 作 H_3 或 H_4 提问。如果这种情况发生，则 CDH 问题的候选答案将被保存在 L_3 或 L_4 中，Q 忽略 A_2 的猜测，随机从 L_3 或 L_4 中选取 V'，输出 $((V'-x_BT^*)-(kzT^*))=vuP$ 作为 CDH 问题的答案，其中 x_B,k,z,T^*,V' 对 Q 均已知。

下面求 Q 成功的概率。ID_B 被选为挑战身份的概率为 $1/q_1$；Q 从 L_3 或 L_4 中随机选取 V' 作为 CDH 问题的候选答案，成功的概率为 $1/(q_3+q_4)$。所以，Q 解决 CDH 困难问题优势：$\varepsilon/q_1(q_3+q_4)$。

定理 3(类型 I、II 攻击下的不可伪造性)　在 ROM 中，若存在一个(EUF-CLSC-CMA)敌手 A_1(或 A_2)能够在概率多项式时间内以 $\varepsilon\geqslant 10(q_s+1)(q_s+q_2)/2^k$ 的优势在定义 3(或定义 4)的游戏中获胜(最多 q_i 次 H_i 提问($i=1,2,3,4$)，q_s 次签密提问)，那么存在一个区分者 Q 能够在概率多项式时间内以 $1/9q_1$ 的优势解决 DL 问题。

证明：设 Q 是一个 DL 问题的解决者，输入为 (P,uP)，其目标是计算出 u。若是类型 I 攻击者 A_1，则 Q 设置 $y=uP$，若是类型 II 攻击者 A_2，则 Q 设置 $y=zP$(z 的值已知)，Q 以 A_1(或 A_2)为子程序并充当(EUF-CLSC-CMA)游戏中的挑战者。

若是类型 I 攻击者 A_1，则执行定理 1 中的所有提问；若是类型 II 攻击者 A_2，则执行定理 2 中的所有提问。

经过概率多项式次数上述提问后，最终，A_1(或 A_2)输出一个伪造的密文 $\sigma^*=(T^*,C^*,U^*)$，发送者是 ID_A，接收者是 ID_B，消息是 m^*。Q 首先在表 L_{pk} 查询 ID_A，若 $c=0$，则失败并终止模拟；否则 $c=1$，由于可以得到 ID_B 的完整私钥，Q 计算 $V_B^*=(x_B+D_B)T^*$，对 V_B^* 作 H_3 提问得 h_3^*，作 H_4 提问得 h_4^*。Q 用 h_3^* 解密 C^* 得 m^* 和 s^*，如果 A_1(或 A_2)的伪造正确，则由分叉引理[22]可以得到两个合法签名 $(m^*,ID_A,ID_B,T^*,h_4^*,h_2,s_1)$ 和 $(m^*,ID_A,ID_B,T^*,h_4^*,h_2',s_2)$，其中 $h_2\neq h_2'$，于是可得：

$T^*=aP=s_1(x_A+D_A+h_2+h_4^*)$，$P=s_2(x_A+D_A+h_2'+h_4^*)P$

$s_1(x_A+D_A+h_2+h_4^*)=s_2(x_A+D_A+h_2'+h_4^*)$

对于类型 I 攻击者即是：

$s_1(x_A+r_A+uk+h_2+h_4^*)=$

$\quad s_2(x_A+r_A+uk+h_2'+h_4^*)$

其中，$k=h_1=H_1(ID_A,R_A)$，此式中只有 u 未知，于是可求出 u。

对于类型 II 攻击者即是：

$s_1(x_A+r_A+zk+h_2+h_4^*)=s_2(x_A+r_A+zk+h_2'+h_4^*)$

其中，$k=h_1=H_1(ID_A,R_A)$，此式中只有 r_A 未知，于是可求出 r_A 即 u 的值，因为“公钥提取提问”中已经设置 $R=r_AP=uP$。

下面求 Q 成功的概率。ID_A 被选为挑战身份的概率为 $1/q_1$；采用预言重放技术[22]产生两个或以上有效密文时，Q 失败的概率小于 1/9。因此，Q 解决 DL 困难问题的优势：$1/9q_1$。

4.2　效率分析

考虑计算开销和密文长度是影响效率的两个主要方面。在计算开销方面，主要考虑双线性对运算、G_1 中的点乘运算和 G_2 中的指数运算。表 1 给出了改进方案与其它一些方案的比较，其中 e 表示指数运算、m 表示点乘运算、p 表示双线性对运算。根据文献[23]的结论，双线性对和指数运算的计算量分别是标量乘运算的约 20 倍和 3 倍。从表 1 可以看出，文献[8,15]都需要双线性对运算，文献[9,21]的运算量大于本文改进方案，只有原方案的运算量小于本文改进方案。在密文长度方面，本文改进方案比文献[8,9]短，比文献[15,21]和原方案长。

表 1　无证书签密方案之间的比较

方案	密文长度	签密			解签密		
		e	m	p	e	m	p
文献[8]	3|G1|+|m|+|q|	4	3	1	4	0	3
文献[9]	2|p|+2|q|+|m|	5	0	0	7	0	0
文献[15]	|q|+2|m|	0	1	1	0	1	1
文献[20]	2|q|+|m|	0	3	0	0	4	0
文献[21]	|p|+|q|+|m|	6	0	0	8	0	0
改进方案	2|G1|+|q|+|m|	0	4	0	0	4	0

本文改进方案与原方案相比效率有所下降。改进方案比原方案多了一次点乘运算，密文长度多出 $2|G_1|-|q|$，这主要是在改进安全缺陷的过程中增加了一些计算量和通信量，但却能有效克服原方案的安全缺陷。综上所述，本文改进方案具有较高的效率。

结束语　本文对一个无双线性对的无证书签密方案进行了密码学分析，指出其不满足机密性和不可伪造性，并指出其安全证明中的错误之处，然后对其进行了改进。在 ROM 模型中基于 CDH 困难问题和 DL 困难问题，对改进方案的安全性进行了证明。效率分析表明，改进方案是高效的。无证书体制有效克服了基于身份体制的密钥托管的缺陷，并省去了公钥证书，具有广阔的应用前景，我们期待着更多安全高效的方案出现。

(下转第 154 页)

models from concurrent programs[M]. NASA Formal Methods, Springer Berlin Heidelberg, 2011:500-505

[9] 肖美华,薛锦云. 基于 SPIN/Promela 的并发系统验证 [J]. 计算机科学,2004,31(8):201-203

[10] Witkowski T, Blanc N, Kroening D, et al. Model checking concurrent linux device drivers[C]// Proceedings of the Twenty-second IEEE/ACM International Conference on Automated Software Engineering. ACM, 2007:501-504

[11] Grov G, Michaelson G, Ireland A. Formal verification of concurrent scheduling strategies using TLA[C]// Parallel and Distributed Systems, 2007 International Conference on. IEEE, 2007, 2:1-6

[12] Apt K R, De Boer F S, Olderog E R. Verification of sequential and concurrent programs[M]. Springer, 2010

[13] Feng X, Shao Z, Dong Y, et al. Certifying low-level programs with hardware interrupts and preemptive threads[C]// PLDI'08: Conference on Programming Language Design and Implementation. ACM, 2008:170-182

[14] Feng X, Shao Z, Vaynberg A, et al. Modular verification of assembly code with stack-based control abstractions[C]// PLDI'06: Conference on Programming Language Design and Implementation. ACM, 2006:401-414

[15] Stephan V S, Cristiano C, Bertrand M. Verifying Executable Object-Oriented Specifications with Separation Logic[C]// 24th European Conference. Maribor, Slovenia, June 2010:21-25

[16] Aquinas H, Andrew W A, Francesco Z N. Oracle Semantics for Concurrent Separation Logic[C]// ESOP. April 2008

[17] Alexey G, Honseok Y. Modular verification of Preemptive OS Kernels[C]// ICEP'11. 2011

[18] O'Hearn P W. Resources, concurrency and local reasoning[C]// Gardner P, Yoshida N, eds. CONCUR, volume 3170 of Lecture Notes in Computer Science. Springer, 2004:49-67

[19] Yu S W. Formal verification of concurrent programs[D]. Durham University, 1999

[20] Brookes S. A semantics for concurrent separation logic [J]. Theor. Computer Science, 2007, 375:227-270

[21] Hayman J, Winskel G. Independence and concurrent separation logic[C]// LICS 2006. 2006:147-156

(上接第 143 页)

参 考 文 献

[1] Shamir A. Identity-based cryptosystems and signature schemes [C]// Proceeding of Crypto'84. LNCS 196, Berlin: Springer-Verlag, 1984:47-53

[2] Al-Riyami S S, Paterson K G. Certificateless public key cryptography[C]// Proceeding of ASIACRYPT 2003. LNCS 2894, Berlin: Springer-Verlag, 2003:452-473

[3] 于刚,韩文报. 具有代理解签密功能的无证书签密方案[J]. 计算机学报,2011,34(7):1291-1299

[4] Yang Guo-min, Tan C H. Certificateless cryptography with KGC trust level 3[J]. Theoretical Computer Science, 2011, 412(39): 5446-5457

[5] Barbosa M, Farshim P. Certificateless signcryption[C]// Proceeding of ASIACCS'2008. ACM, 2008:369-372

[6] Zheng Yu-liang. Digital signcryption or how to achieve cost(signature and encryption)<<cost(signature)+cost(encryption) [C]// Proceeding of CRYPTO'1997. LNCS 1294, Berlin: Springer-Verlag, 1997:165-179

[7] Aranha D, Castro R, Lopez J, et al. Efficient certificateless signcryption [EB/OL]. http://sbseg2008.inf.ufrgs.br/anais/data/pdf/st03_01_resumo.pdf, 2009-03-21

[8] Wu Chen-huang, Chen Zhi-xiong. A new efficient certificateless signcryption scheme[C]// Proceedinf of ISISE'2008. IEEE, 2008:661-664

[9] Selvi S S D, Vivek S S, Rangan C P. Cryptanalysis of certificateless signcryption schemes and an efficient construction without pairing[C]// Proceeding of Inscrypt 2009. LNCS 6151, Berlin: Springer-Verlag, 2010:75-92

[10] Selvi S S D, Vivek S S, Shukla D, et al. Efficient and provably secure certificateless multi-receiver signcryption[C]// Proceeding of ProvSec 2008. LNCS 5324, Berlin: Springer-Verlag, 2008:52-67

[11] Selvi S S D, Vivek S S, Rangan C P. A note on the certificateless multi-receiver signcryption scheme[EB/OL]. http://eprint.iacr.org/2009/308, 2009-6-26

[12] Miao Song-qin, Zhang Fu-tai, Zhang Lei. Cryptanalysis of a certificateless multi-receiver signcryption scheme[C]// Proceeding of MIMES 2010. IEEE, 2010:593-597

[13] Li Fa-gen, Shirase M, Takagi T. Certificateless hybrid signcryption[C]// Proceeding of ISPEC 2009. LNCS 5451, Berlin: Springer-Verlag, 2009:112-123

[14] Selvi S S D, Vivek S S, Rangan C P. Certificateless KEM and hybrid signcryption schemes revisited[C]// Proceeding of ISPEC 2010. LNCS 6047, Berlin: Springer-Verlag, 2010:294-307

[15] 孙银霞,李晖. 高效无证书混合签密[J]. 软件学报,2011,22(7):1690-1698

[16] Liu Zhen-hua, Hu Yu-pu, Zhang Xiang-song, et al. Certificateless signcryption scheme in the standard model[J]. Information Sciences, 2010, 180(3):452-464

[17] Weng Jian, Yao Guo-xiang, Deng R H, et al. Cryptanalysis of a certificateless signcryption scheme in the standard model[J]. Information Sciences, 2011, 181(3):661-667

[18] Jin Zheng-ping, Wen Qiao-yan, Zhang Hua. A supplement to Liu et al.'s Certificateless signcryption scheme in the standard model[EB/OL]. http://eprint.iacr.org/2010/252, 2010-05-03

[19] Luo Ming, Zou Chun-hua, Xu Jian-feng. Certificateless Broadcast Signcryption with Forward Secrecy[C]// Conference on Computational Intelligence and Security. 2011:910-914

[20] 刘文浩,许春香. 无双线性配对的无证书签密方案[J]. 软件学报,2011,22(8):1918-1926

[21] Xie Wen-jian, Zhang Zhang. Certificateless Signcryption without Pairing[EB/OL]. http://eprint.iacr.org/2010/187, 2010-06-20

[22] Pointcheval D, Stern J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3): 361-396

[23] Chen L, Cheng Z, Smart N P. Identity-based key agreement protocols from pairings[J]. International Journal Information Security, 2007, 6(4):213-241