软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2011,22(8):1918−1926 [doi: 10.3724/SP.J.1001.2011.03891]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

无双线性配对的无证书签密方案*

刘文浩+, 许春香

(电子科技大学 计算机科学与工程学院,四川 成都 611731)

Certificateless Signcryption Scheme Without Bilinear Pairing

LIU Wen-Hao+, XU Chun-Xiang

(School of Computer Science and Engineering, University of Electronic Science and Technology, Chengdu 611731, China)

+ Corresponding author: E-mail: whl819_819@163.com

Liu WH, Xu CX. Certificateless signcryption scheme without bilinear pairing. *Journal of Software*, 2011,22(8): 1918−1926. http://www.jos.org.cn/1000-9825/3891.htm

Abstract: Only six certificateless signcryption schemes have been proposed in recent years. Most of them cannot provide confidentiality and authentication. Even if some of them are secure, all of them need pairing operations. In order to solve the above-mentioned problems, a pairing-free certificateless signcryption scheme is proposed, and its security has proven to be in the random oracle model (ROM) under the computational Diffie-Hellman (CDH) assumption and the hardness of discrete logarithm problem (DLP). This scheme eliminates pairing operations and is the most efficient certificateless signcryption scheme.

Key words: signcryption; certificateless; ROM (random oracle model); CDH (computational Diffie-Hellman) assumption

摘 要: 近几年,仅提出了 6 个无证书签密方案,其中大部分不能提供保密性和不可伪造性.即使有些签密方案是安全的,它们也都需要双线性对运算.为了解决上述问题,提出了一个无需对运算的无证书签密方案,并在随机预言模型下,基于计算 Diffie-Hellman 假设和离散对数困难问题证明了其保密性和认证性.该方案无需双线性对操作.到目前为止,它是已知最有效的无证书签密方案.

关键词: 签密;无证书;随机预言模型;计算 Diffie-Hellman 假设

中图法分类号: TP309 **文献标识码**: A

保密性和认证性是通信的两个基本安全要求.传输的消息保密通过加密来完成,消息的认证通过数字签名来实现.1997 年,Zheng[1]首先提出了签密的概念.它开创了消息保密和认证同步高效进行的先河,但文献[1]中并没有给出其安全证据.在 2003 年的亚密会上,Al-Riyami 和 Paterson[2]第一次提出了无证书公钥密码学概念.它减少了对密钥生成中心的信任.在无证书密码学体制中,由可信密钥生成中心生成用户的部分私钥和部分公钥;同时,用户选择一个秘密值和部分私钥相结合,生成自己独立的私钥和公钥.这样,它克服了基于身份密码学中用户密钥托管问题,也消除了基于传统公钥基础设施中公钥证书的复杂性管理问题,并合并了这两者的优势,大大提高了系统的运行效率.随着签密技术的发展,仅有的 6 个无证书签密方案[3−8]先后由不同的研究者提出来.

* 基金项目: 国家高技术研究发展计划(863)(2009AA01Z415)
收稿时间: 2010-01-25; 定稿时间: 2010-05-17

2008 年,Barbosa 等人[3]首次提出了无证书签密方案.该方案使用的是先加密后签名方式,它并不能抗扩展不可伪造攻击.同年,Diego 等人[4]提出了一个有效的无证书签密方案,Wu 等人[5]提出了一个新的有效的无证书签密方案.这两个无证书签密方案被 Sharmila 等人[6]攻破,并提出了具体攻击方法,前者不能提供保密性和认证性,后者不能提供保密性.Barreto[7]首次提出了签密和解签密均不需要双线性对操作的无证书签密方案,但该方案在生成公钥时需要双线性对操作;同时,该方案也不能保证发送消息的保密性和不可否认性.2009 年,Li[8]提出了一种无证书混合签密方案,并在随机谕示模型下证明了其安全性.但由于运用了对运算和指数运算,计算开销很大.到目前为止,所有已知的无证书签密方案都采用了对操作,比较指数运算和点乘运算,在有限域中,对操作仍然是比它们更为耗时的运算.按照文献 MIRACL[9],执行一个 512 位 Tate pairing 需要花费 20ms,而一个 1 024 位素数模指数操作却只需要 8.80ms.运行一次双线性对操作的时间至少是椭圆曲线上点乘运算的 20 倍以上[10].因此,不用双线性对运算和指数运算的安全签密方案具有更大的效率优势.基于以上情况,我们提出了一个无需对运算和指数运算的无证书签密方案.在整个通信过程中,无需对运算和指数运算.因此,它是目前已知无证书签密方案中计算复杂度最低的.

1 有关困难问题及其假设

计算性 Diffie-Hellman 问题(computational diffie-hellman problem,简称 CDHP):设 G 是阶为 q 的一个加法循环群,P 是它的一个生成元,给定 $aP,bP\in G$,对任意未知 $a,b\in Z_q^*$,计算 abP.

在概率多项式时间(probabilistic polynomial time,简称 PPT)内,算法 A 在解决 CDH 问题的优势定义如下:

$$Adv^{CDH}(A)=\Pr[A(aP,bP)=abP \mid a,b\in Z_q^*].$$

CDH 假设:对任意 PPT 算法 A,$Adv^{CDH}(A)$是可以忽略的.

离散对数问题(discrete logarithm problem,简称 DLP):设 G 是阶为 q 的一个循环群,P 是它的一个生成元,给定 $P,aP\in G$,对任意未知 $a\in Z_q^*$,计算 a.

在概率多项式时间内,算法 A 在解决 DLP 问题的优势定义如下:

$$Adv^{DLP}(A)=\Pr[A(P,aP)=a \mid a\in Z_q^*].$$

DLP 假设:对任意 PPT 算法 A,$Adv^{DLP}(A)$是可以忽略的.

2 形式化安全定义

无证书签密方案有 3 个合法参与者:密钥生成中心(KGC)、签密者 ID_i、接收者 ID_j.无证书签密方案方案由 7 种算法构成:

(1) 系统参数建立算法:输入安全参数 k,KGC 返回系统公开参数 $params$、保密系统主密钥 z.

(2) 用户部分密钥生成算法:输入给定用户身份 ID_i、系统参数 $params$ 和主密钥 z,KGC 输出身份 ID_i 用户的部分私钥 D_i,并通过安全渠道返回 D_i 给用户 ID_i.

(3) 用户秘密值生成算法:输入给定用户身份 ID_i、系统参数 $params$,用户 ID_i 输出其秘密值 $x_i\in Z_q^*$ 作为其长期密钥.

(4) 用户私钥生成算法:输入给定用户身份 ID_i、系统参数 $params$、ID_i 用户的部分私钥 D_i 及其长期私钥 x_i,返回用户 ID_i 私钥 $SK_i=(x_i,D_i)$.

(5) 用户公钥生成算法:输入给定用户身份 ID_i、系统参数 $params$、ID_i 用户的部分公钥 P_i 及其长期私钥 x_i,返回用户 ID_i 公钥 PK_i.

(6) 签密算法(Signcrypt):输入 $params$、消息 m、签密者身份 ID_i 及其私钥 SK_i、接收者 ID_j 及其公钥 PK_j,返回密文 σ.

(7) 解密验证算法(Unsigncrypt):输入 $params$、σ、签密者身份 ID_i 及其公钥 PK_i、接收者 ID_j 及其私钥 SK_j,如果验证通过,则用户输出明文消息 m;否则,返回出错消息,拒绝接收消息 m.

参照 Huang[11]定义的敌手类型,无证书签密方案面临两种类型的敌手攻击:

- 类型 1:攻击者可以查询用户公钥或替换合法用户的公钥,但不知道系统主密钥;
- 类型 2:攻击者可以获得系统主密钥,但不能同时替换合法用户公钥或查询用户公钥.

定义 1(类型 1 攻击下的保密性). 在类型 1 敌手攻击下,在概率多项式时间内,如果攻击者没有不可忽略的优势在如下游戏中获胜,则称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) 挑战者 C 输入安全参数 k,运行"系统参数建立"算法,获得系统主密钥和系统公共参数 $params$,将 $params$ 发送给敌手 A,保密系统主密钥.

(2) 查询阶段,A 执行如下操作:

- Hash 查询:A 可以查询任意输入的 Hash 值;
- 部分私钥生成查询:A 选择一个身份 ID,根据系统参数 $params$ 和主密钥,挑战者 C 计算用户部分私钥 D_{ID},并发送给敌手 A;
- 私钥生成查询:A 选择一个身份 ID,挑战者 C 根据用户密钥生成算法生成用户 ID 的私钥 SK_{ID},并发送给敌手 A;
- 公钥生成查询:A 选择一个身份 ID,C 根据用户公钥生成算法生成用户 ID 的公钥 PK_{ID},并发送给敌手 A;
- 用户公钥替换:对任意身份 ID,A 可以选择一个新的秘密值,计算新公钥,并用新公钥来替换身份为 ID 用户的原有公钥 PK_{ID};
- 签密查询:A 选择身份 ID_i,ID_j 和明文 m,C 分别对 ID_i 进行私钥生成查询和对 ID_j 进行公钥生成查询.计算 $\sigma=Signcrypt(ID_i,ID_j,m,SK_i,PK_j)$,将 σ 发送给敌手 A;
- 解密验证查询:A 选择身份 ID_i,ID_j 和密文 σ,C 分别对 ID_j 进行私钥生成查询和对 ID_i 进行公钥生成查询.计算 $Unsigncrypt(ID_i,ID_j,\sigma,SK_j,PK_i)$,发送明文 m 或"出错"给 A.

(3) A 选择两个等长的明文 m_0,m_1 和希望挑战的两个身份 ID_i^*,ID_j^*,但 ID_j^* 不是执行过部分私钥查询或私钥查询的用户身份,C 随机选择 $b\in\{0,1\}$,计算 $\sigma^* = Signcrypt(m_b,ID_j^*,SK_{ID_i^*},PK_{ID_j^*})$,将 σ^* 发送给敌手 A.

(4) 猜测阶段.A 和查询阶段一样,执行多项式有界次数查询,但不允许对 ID_j^* 执行部分私钥生成查询和私钥生成查询,也不能对 σ^* 执行解密验证查询.

(5) 游戏最后,A 输出一个 b' 作为对 b 的猜测,若 $b'=b$,A 在此游戏中获胜.A 在此游戏中获胜的优势为

$$Adv^{IND\text{-}CCA2}(A)=|2\Pr[b'=b]-1|.$$

定义 2(类型 2 攻击下的保密性). 在类型 2 敌手攻击下,在概率多项式时间内,如果攻击者没有不可忽略的优势在如下游戏中获胜,则称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) 挑战者 C 输入安全参数 k,运行"系统参数建立"算法,并发送 $params$ 和系统主密钥给类型 2 的敌手 A;

(2) 查询阶段,A 执行定义 1 中除"用户公钥替换"外的所有查询.

阶段(3)~阶段(5)同上述阶段(3)~阶段(5)过程.

定义 3(类型 1 攻击下的不可伪造性). 在类型 1 敌手攻击下,在概率多项式时间内,如果攻击者没有不可忽略的优势在如下游戏中获胜,则称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:

阶段(1)、阶段(2)同定义 1 中的阶段(1)、阶段(2).

(3) 输出:最后,A 输出一个新的三元组 (σ^*,ID_i^*,ID_j^*) (这个三元组不是签密预言产生的).我们说 A 在这个游戏中获胜,当且仅当 A 没有对身份为 ID_i 用户进行部分私钥查询和私钥查询且 $Unsigncrypt(\sigma^*,ID_i^*,SK_{ID_j^*},PK_{ID_i^*})$ 的结果不是"出错".

定义 4(类型 2 攻击下的不可伪造性). 在类型 2 敌手攻击下,在概率多项式时间内,如果攻击者没有不可忽略的优势在如下游戏中获胜,则称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:

阶段(1)、阶段(2)同定义 2 中的阶段(1)、阶段(2).

(3) 输出:最后,A 输出一个新的三元组 $(\sigma^*, ID_i^*, ID_j^*)$ (这个三元组不是签密预言产生的).我们说 A 在这个游戏中获胜,当且仅当 A 没有对身份为 ID_i 用户进行部分私钥查询和私钥查询且 $Unsigncrypt(\sigma^*, ID_i^*, SK_{ID_j^*}, PK_{ID_i^*})$ 的结果不是“出错”.

3 新的无证书签密方案

(1) 系统参数的建立

输入安全参数 k,产生两个大素数 p,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,选择安全 Hash 函数: $H_1:\{0,1\}^*\times G\to Z_q^*, H_2:\{0,1\}^*\to Z_q^*, H_3:G\to\{0,1\}^*$,明文消息 m 为任意比特长,KGC 随机选择主密钥 $z\in Z_q^*$,计算 $y=zP$,公开系统参数 (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 随机选择 $r_i\in Z_q^*$,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,$R_i=r_iP$ 作为用户 ID_i 的部分公钥.

用户 ID_i 随机选择秘密值 $x_i\in Z_q^*$ 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 $SK_A=(D_A,x_A)$,公钥 $PK_A=(R_A,X_A)$.用户 B 的私钥 $SK_B=(D_B,x_B)$,公钥 $PK_B=(R_B,X_B)$.

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) 签密过程

用户 A 随机选取 $a\in Z_q^*$,计算 $T_A=aP, h_1=H_1(ID_B,R_B), h=H_2(T_A\|ID_A\|m), s=a/(x_A+D_A+h)$,生成签名 (h,s).$V_A=a(R_B+X_B+h_1y), C=H_3(V_A)\oplus(m)$(完成加密),发送消息 $\sigma=(h,s,C)$ 给用户 B.

(4) 解密验证过程

当收到密文 σ 后,用户 B 执行如下操作:

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 $m=C\oplus H_3(V_B)$(完成解密).

若 $H_2(s(R_A+X_A+h_1'y+hP)\|ID_A\|m)=h$ 成立,则用户 B 接受消息 m.

验证签名的正确性:

$$\begin{aligned}s(R_A+X_A+h_1'y+hP)&=(a/(D_A+x_A+h))\times(r_AP+x_AP+zh_1'P+hP)\\&=(a/(D_A+x_A+h))\times(D_A+x_A+h)P\\&=aP\\&=T_A.\end{aligned}$$

只要将 (h,s,m) 提交第三方,它就可通过检验 $H_2(s(R_A+X_A+h_1'y+hP)\|ID_A\|m)=h$ 是否成立来公开验证签名者的身份.若此等式成立,签名者的身份就得到了公开验证.

验证消息的正确性:

$$\begin{aligned}m&=H_3(s(D_B+x_B)(X_A+R_A+h_1'y+hP))\oplus C\\&=H_3((a/(D_A+x_A+h))(D_B+x_B)(x_AP+r_AP+h_1'zP+hP))\oplus C\\&=H_3((x_B+D_B)aP)\oplus C\\&=H_3(a(x_BP+r_BP+h_1y))\oplus C\\&=H_3(a(R_B+X_B+h_1y))\oplus C\\&=H_3(V_A)\oplus C\\&=m.\end{aligned}$$

4 安全证明

4.1 保密性证明(安全证明参照文献[12]中证明方法)

定理 1(类型 1 攻击下的保密性). 在 ROM 中,若存在一个敌手 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(假设最多进行 q_i 次 H_i 查询,i=1,2,3,最多 q_s 次签密查询,最多 q_{un} 次解签密查询),那么存在一个可区分者 Q,能够在概率多项式时间内以 $Adv^{IND-CCA2}(A_1) \geqslant (\varepsilon/q_1^2 q_2 q_3)(1-q_s(2q_2+q_3+2q_s)/2^k)(1-q_{un}/2^k)$ 的优势解决 CDH 困难问题.

证明:假设 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 $y=uP$,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)给 A_1,并维持列表 L_1,L_2,L_3,L_D,L_{SK},L_{PK},L_S,L_U 分别用于跟踪 A_1 对预言机 H_1,H_2,H_3、部分私钥提取、私钥提取、公钥提取、签密和解签密的查询,开始每个列表均为空.

- H_1 查询:列表 L_1 中每一项格式为(ID,R,h_1,c),当 Q 收到 A_1 对 $H_1(ID_i,R_i)$查询时,若(ID,R,h_1)在列表 L_1 中存在,则返回相应的值给 A_1;否则,Q 随机选择 $c\in\{0,1\}$,其中,Pr[c=1]=δ.当 c=0 时,Q 随机选择 $h_1 \in Z_q^*$,并将(ID,R,h_1,c)加入列表 L_1 中,返回 h_1;当 c=1 时,令 $h_1=k$,返回 k 给 A_1.
- H_2 查询:列表 L_2 中每一项格式为(m,ID,T,h_2),当 Q 收到 A_1 对 $H_2(m||ID||T)$查询时,若(m,ID,T,h_2)在列表 L_2 中存在,则返回相应的值给 A_1;否则,Q 随机选择 $h_2 \in Z_q^*$,将(m,ID,T,h_2)加入列表 L_2 中,返回 h_2 给 A_1.
- H_3 查询:列表 L_3 中每一项格式为(V,h_3),当 Q 收到 A_1 对 $H_3(V_i)$查询时,若(V_B,h_3)在列表 L_3 中存在,则返回相应的值给 A_1;否则,Q 随机选择 $h_3 \in Z_q^*$,并将(V_B,h_3)加入列表 L_3 中,返回 h_3 给 A_1.
- 部分私钥提取查询:若(ID,D,R)在列表 L_D 中存在,则返回相应的值给 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)加入列表 L_D 中,(ID,R,h_1)加入列表 L_1 中,返回(R,D)给 A_1.
- 私钥提取查询:若(ID,D,x)在列表 L_{SK} 中存在,则返回相应的值给 A_1;否则,Q 查询列表 L_D 得到 D,随机选择 $x \in Z_q^*$,把(ID,D,x)加入列表 L_{SK} 中.
- 公钥提取查询:列表 L_{PK} 中每一项格式为(ID,R,X,c),当 Q 收到 A_1 对身份 ID 的公钥查询时,若(ID,R,X)在列表 L_{PK} 中存在,则返回相应的值给 A_1;否则,Q 先查询列表 L_D 和 L_{SK},计算 $X_i=x_iP$,将(ID,R,X)加入列表 L_{PK} 中,并返回(R,X)给 A_1.若列表 L_D 和 L_{SK} 中不存在,则查询列表 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,c)加入列表 L_{PK} 中,并返回(R,X);若 c=0,则运行部分私钥提取查询,获得(R,D),Q 随机选择 $x \in Z_q^*$,把(ID,D,x)加入列表 L_{SK} 中,将(ID,R,X,c)加入列表 L_{PK} 中,并返回(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.
- 签密查询:Q 先在列表 L_{PK} 查询(ID_B,R_B,X_B,c),若 c=1,则放弃;否则,查询列表(ID_A,D_A,x_A),随机选 $a \in Z_q^*$,计算 $T_A=aP$,$h_1=H_1(ID_B,R_B)$,$h=H_2(T_A||ID_A||m)$,$s=a/(x_A+D_A+h)$,$V=a(R_B+X_B+h_1y)$,$C=H_3(V)\oplus(m)$,返回消息 $\sigma=(h,s,C)$给 A_1.
- 解签密的查询:Q 先在列表 L_{PK} 查询 ID_A:① 若存在且 c=0,则在列表 L_{SK} 查询(ID_B,D_B,x_B),在列表 L_1 中查询 (ID_A,R_A,h_1'),计算 $V=s(x_B+D_B)(X_A+R_A+h_1'y+hP)$,$m=H_3(V)\oplus C$, $T'=s(R_A+X_A+h_1'y+hP)$,若 $H_2(T'||ID_A||m)=h$ 成立,则返回 m,否则终止模拟;② 若存在且 c=1,则在 L_1 中查询 (ID_A,R_A,h_1'),若存在 $(m,ID_A,T',h_2)\in L_2$,$(V,h_3)\in L_3$ 则返回 m,否则终止模拟;③ 如果列表 L_{PK} 中不存在(公钥被替换掉),那么在列表 L_1 中查询 (ID_A,R_A,h_1'),若存在$(m,ID_A,T',h_2)\in L_2$,$(V,h_3)\in L_3$,则返回 m,否则终止模拟.

经过概率多项式次数上述查询后,A_1 输出两个希望接收挑战的身份(ID_A,ID_B)和两个等长度的明文(m_0,m_1).若 c=0,则终止模拟;否则,Q 随机选择 $a,h^* \in Z_q^*$,$b\in\{0,1\}$,并计算 $s^*=a/(D_A+x_A+h^*)$,$V=a(R_B+X_B+h_1y)$,$C^*=H_3(V)\oplus m_b$,将挑战密文 $\sigma^*=(h^*,s^*,C^*)$发给 A_1.A_1 经过概率多项式次数查询后,输出 b'作为对 b 的猜想,若 $b'=b$,则 Q 输出 $((V'-x_BT')-(r_BT'))\times(1/k)=auP$ 作为 CDH 问题的答案,其中,

$$V'=s^*(x_B+D_B)(R_A+X_A+h_1'y+h^*P),T'=s^*(R_A+X_A+h_1'y+h^*P);$$

否则,Q 没有解决 CDH 问题.

若 A_1 对 ID_B 进行过部分私钥或私钥提取查询,则 Q 失败,它不进行这种查询的概率至少为 $1/q_1^2$;若 A_1 对 T' 进行过 H_2 或对 V' 进行过 H_3 查询,则 Q 失败,它不进行这种查询的概率大于 $1/q_2q_3$.在进行签密查询时,由于 H_2,H_3 碰撞,挑战者中止行为的概率 $Pr_1\leqslant q_s(2q_2+q_3+2q_s)/2^k$;在游戏中,挑战者拒绝有效的密文的概率 $Pr_2\leqslant q_{un}/2^k$.根据以上情况,我们可以得出 Q 解决 CDH 困难问题优势:

$$Adv^{IND\text{-}CCA2}(A_1)\geqslant(\varepsilon/q_1^2q_2q_3)(1-q_s(2q_2+q_3+2q_s)/2^k)(1-q_{un}/2^k).$$ □

定理 2(类型 2 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(假设最多进行 q_i 次 H_i 查询,i=1,2,3),那么存在一个可区分者 Q,能够在概率多项式时间内,以 $\varepsilon/(q_1^2q_2q_3)$ 的优势解决 CDH 困难问题.

证明:敌手 A_2 不能进行公钥替换攻击,除了知道定理 1 中所给定的条件以外,还知道系统主密钥.

A_2 可以进行定理 1 中除了“解签密”和“公钥替换”之外的所有查询,查询方法同定理 1,现在只讨论解签密查询.

解签密查询:Q 先在列表 L_{PK} 查询 ID_A:① 若存在且 c=0,则在列表 L_{SK} 中查询(ID_B,D_B,x_B),在列表 L_1 中查询 (ID_A,R_A,h_1'),计算 $V=s(x_B+D_B)(X_A+R_A+h_1'y+hP)$,$m=H_3(V)\oplus C$, $T'=s(R_A+X_A+h_1'y+hP)$,若 $H_2(T'||ID_A||m)=h$ 成立则返回 m,否则终止模拟;② 若存在且 c=1,则在 L_1 中查询 (ID_A,R_A,h_1'),若存在$(m,ID_A,T',h_2)\in L_2$,$(V,h_3)\in L_3$ 则返回 m,否则终止模拟;③ 如果列表 L_{PK} 中不存在(公钥被替换掉),那么在列表 L_1 中查询 (ID_A,R_A,h_1'),若存在 $(m,ID_A,T',h_2)\in L_2$,$(V,h_3)\in L_3$,则返回 m,否则终止模拟.

经过概率多项式次数上述查询后,A_2 输出两个希望接收挑战的身份(ID_A,ID_B)和两个等长度的明文(m_0,m_1).若 c=0,则终止模拟;否则,随机选择 $a,h^*\in Z_q^*$,$b\in\{0,1\}$,并计算 $s^*=a/(D_A+x_A+h^*)$,$V=a(R_B+X_B+h_1y)$,$C^*=H_3(V)\oplus m_b$,将挑战密文 $\sigma^*=(h^*,s^*,C^*)$发给 A_2.其中,Q 知道系统主私钥 u.A_2 经过概率多项式次数查询后,输出 b'作为对 b 的猜想,若 $b'=b$,则 Q 输出 $V'-x_BT'-uh_1T'=ar_BP$ 作为 CDH 问题的答案,其中,

$$V'=s^*(x_B+D_B)(R_A+X_A+h_1'y+h^*P),T'=s^*(R_A+X_A+h_1'y+h^*P);$$

否则,Q 没有解决 CDH 问题.

若 A_2 对 ID_B 进行过部分私钥或私钥查询,则 Q 失败,它不进行这种查询的概率至少是 $1/q_1^2$;若 A_2 对 T'进行过 H_2 或对 V'进行过 H_3 查询,则 Q 失败,它不进行这种查询的概率大于 $1/q_2q_3$.因此,Q 解决 CDH 问题的优势:

$$Adv^{IND\text{-}CCA2}(A_2)\geqslant\varepsilon/q_1^2q_2q_3.$$ □

4.2 不可伪造性证明

定理 3(类型 1 攻击下的不可伪造性). 在 ROM 中,若存在一个(EUF-CLSC-CMA)敌手 A_1,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 中的游戏中获胜(假设最多进行 q_i 次 H_i 查询,i=1,2),那么存在一个可区分者 Q,能够在概率多项式时间内,以 $1/(9q_1^2q_2)$ 的优势解决 DL 困难问题.

证明:假设 Q 是一个 DL 困难问题的解决者,其困难问题的输入为(P,uP),其目标是计算出 u.首先,Q 设置 $y=uP$,Q 以 A_1 为子程序并充当(EUF-CLSC-CMA)游戏中的挑战者.游戏开始后,Q 发送(p,q,P,y,H_1,H_2)给 A_1,并维持列表 L_1,L_2,L_D,L_{SK},L_{PK},L_S,L_V 分别用于跟踪 A_1 对预言机 H_1,H_2、部分私钥提取、私钥提取、公钥提取、签名和校验签名查询,开始每个列表为空.

- H_1 查询:列表 L_1 中每一项格式为(ID,R,h_1),当 Q 收到 A_1 对 $H_1(ID_i,R_i)$查询时,若(ID,R,h_1)在列表 L_1 中存在,则返回相应的值给 A_1;否则,Q 随机选择 $h_1\in Z_q^*$,并将(ID,R,h_1)加入列表 L_1 中.
- H_2 查询:列表 L_2 中每一项格式为(m,ID,T,h_2,c),当 Q 收到 A_1 对 $H_2(m||ID||T)$查询时,若(m,ID,T,h_2)在列表 L_2 中存在,则返回相应的值给 A_1;否则,Q 随机选择 $c\in\{0,1\}$,其中,Pr[c=1]=δ.当 c=0 时,随机选择 $h_2\in Z_q^*$,返回 h_2 给 A_1,并将(m,ID,T,h_2,c)加入列表 L_2 中;当 c=1 时,令 $h_1=\perp$,返回$\perp$给 A_1.

- 部分私钥提取查询:若(ID,D,R)在列表 L_D 中存在,则返回相应的值给 A_1;否则,Q 随机选择 $D,h_1 \in Z_q^*$,计算 $R=DP-yh_1$,将(ID,D,R)加入列表 L_D 中,(ID,R,h_1)加入列表 L_1 中,返回(R,D)给 A_1.
- 私钥提取查询:若(ID,D,x)在列表 L_{SK} 中存在,则返回相应的值给 A_1;否则,Q 查询列表 L_D 得到 D,随机选择 $x \in Z_q^*$,把(ID,D,x)加入列表 L_{SK} 中.
- 公钥提取查询:若(ID,R,X)在列表 L_{PK} 中存在,则返回相应的值给 A_1;否则,Q 先查询列表 L_D 和 L_{SK},计算 $X=xP$,将(ID,R,X)加入列表 L_{PK} 中,并返回(R,X)给 A_1;若列表 L_D 和 L_{SK} 中不存在,则查询列表 L_2.若 $c=1$,Q 随机选择 $r,x \in Z_q^*$,计算 $R=rP,X=xP$,将(ID,R,X,c)加入列表 L_{PK} 中,并返回(R,X);若 $c=0$,运行部分私钥提取查询,获得(R,D),Q 随机选择 $x \in Z_q^*$,把(ID,D,x)加入列表 L_{SK} 中,将将(ID,R,X,c)加入列表 L_{PK} 中,并返回(R,X).
- 公钥替换:签名者的身份为 ID,A_1 可以任意选择一个新的 x' 替换原来的 x,并用新的公钥 R' 替换原来的 R 参与计算.
- 签名查询:Q 先在列表 L_{PK} 查询(ID_B,R_B,X_B,c),若 $c=1$,则放弃;否则查询列表(ID_A,D_A,x_A),随机选 $a \in Z_q^*$,计算 $T=aP$, $h_1' = H_1(ID_A,R_A)$, $h=H_2(T\|ID_A\|m)$, $s=a/(x_A+D_A+h)$,返回消息$\sigma=(h,s)$给 A_1.
- 校验签名查询:Q 先在列表 L_{PK} 查询 ID_A:① 若存在且 $c=0$,则在列表 L_1 中查询 (ID_A,R_A,h_1'),计算 $T'=s(R_A+X_A+h_1'y+hP)$,若 $H_2(T'\|ID_A\|m)=h$ 成立,则返回“通过”,否则终止模拟;② 若存在且 $c=1$,则在 L_1 中查询 (ID_A,R_A,h_1'),若存在$(m,ID_A,T',h)\in L_2$,返回“通过”,否则终止模拟;③ 如果列表 L_{PK} 中不存在(公钥被替换掉),那么在列表 L_1 中查询 (ID_A,R_A,h_1'),若存在$(m,ID_A,T',h)\in L_2$,返回“通过”,否则终止模拟.

经过概率多项式次数上述查询后,A_1 随机选择 $a,s^* \in Z_q^*$,计算 $T=aP$,$h^*=H_2(ID_A\|T\|m)$, $h_1' = H_1(ID_A,R_A)$,输出对 m 的有效伪签名$\sigma^*=(h^*,s^*)$,Q 知道被替换掉的公钥.若伪造签名成功,则 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;否则,Q 没有解决 DL 困难问题.若 A_1 对 ID_A 进行过部分私钥或私钥查询,则 Q 失败,它不进行这种查询的概率至少是 $1/q_1^2$;若 A_1 对 T' 进行过 H_2 查询,则 Q 失败,它不进行这种查询的概率大于 $1/q_2$;采用预言重放技术[13]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:

$$Adv^{EUF\text{-}CMA}(A_1) \geqslant 1/9q_1^2q_2.$$ □

定理 4(类型 2 攻击下的不可伪造性). 在 ROM 中,若存在一个(EUF-CLSC-CMA)敌手 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 4 中的游戏中获胜(假设最多进行 q_i 次 H_i 查询,$i=1,2$),那么存在一个可区分者 Q,能够在概率多项式时间内,以 $1/(9q_1^2q_2)$ 的优势解决 DL 困难问题.

证明:假设 Q 是一个 DL 困难问题的解决者,其困难问题输入为(P,vP),其目标是计算出 v.首先,Q 设置 $y=uP$,Q 以 A_1 为子程序并充当(EUF-CLSC-CMA)游戏中的挑战者.游戏开始后,Q 发送(p,q,P,y,H_1,H_2)给 A_2.A_2 知道系统主密钥 u,但不能进行公钥替换攻击.其他条件及目标均同定理 3 中给定的.

A_2 可以进行定理 3 中的除“校验签名”和“公钥替换”之外的所有查询.

校验签名查询:Q 先在列表 L_{PK} 查询 ID_A:① 若存在且 $c=0$,则在列表 L_1 中查询 (ID_A,R_A,h_1'),计算 $T'=s(R_A+X_A+h_1'y+hP)$,若 $H_2(T'\|ID_A\|m)=h$ 成立,则返回“通过”,否则终止模拟;② 若存在且 $c=1$,则在 L_1 中查询 (ID_A,R_A,h_1'),若存在$(m,ID_A,T',h)\in L_2$,返回“通过”,否则终止模拟;③ 如果列表 L_{PK} 中不存在(公钥被替换掉),那么在列表 L_1 中查询 (ID_A,R_A,h_1'),若存在$(m,ID_A,T',h)\in L_2$,返回“通过”,否则终止模拟.

经过概率多项式次数上述查询后,A_2 随机选择 $a,s^* \in Z_q^*$,计算 $T=aP$,$h^*=H_2(ID_A\|T\|m)$, $h_1' = H_1(ID_A,R_A)$,输出对 m 的有效伪签名$\sigma^*=(h^*,s^*)$,Q 知道系统主密钥 u.若伪造签名成功,则 Q 输出 $r_A=(a-s^*(uh_1'+x_A+h^*))/s^*$ 作为解决 DL 困难问题的回答;否则,Q 没有解决 DL 困难问题.若 A_2 对 ID_A 进行过部分私钥或私钥查询,则 Q 失败,它不进行这种查询的概率至少是 $1/q_1^2$;若 A_2 对 T' 进行过 H_2 查询,则 Q 失败,它不进行这种查询的概率大于 $1/q_2$;采用预言重放技术[13]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:

$$Adv^{EUF\text{-}CMA}(A_2) \geqslant 1/9q_1^2q_2.$$ □

5 性能比较

新方案无需双线性对运算和指数运算,在通信过程中,签密者只需进行 3 次椭圆曲线上的点乘运算,解签校验者也只需进行 3 次点乘运算.到目前为止,它是已知无证书签密方案中效率最高的.文献[3–5,7]的方案都存在安全上的缺限,要么无保密性,要么不能抗不可否认性,要么同时存在这两方面的缺限.除了文献[7]的方案以外,上述的所有方案都需要对运算,效率比新方案要低得多.尽管文献[7]的方案在签密和解签密过程中没有使用对操作,但使用了几次指数操作,而且在生成公钥过程中也使用了对操作,其效率也比新方案低;同时,该方案也不能保证发送消息的保密性和不可否认性.计算机复杂度比较见表 1.其中,P 表示双线性对运算,E 表示指数运算,M 表示椭圆曲线上的点乘运算.由表 1 可以看出,新方案与本文提到的其他无证书签密方案相比,有明显的效率优势.

Table 1 Comparing the complexity of computer

表 1 计算复杂度比较

Scheme	Signcryption	Unsigncryption
Barbosa[3]	1P+1E+4M	5P+0E+0M
Diego[4]	1P+1E+4M	3P+0E+1M
Wu[5]	1P+4E+3M	3P+4E+0M
Barreto[7]	0P+1E+0M	0P+4E+0M
Li[8]	1P+1E+4M	5P+0E+1M
New scheme	0P+0E+3M	0P+0E+3M

6 结 论

新方案无需双线性对操作和指数运算,它具有比其他安全无证书密钥协商方案更高的效率.只要 CDH 假设和 DLP 假设成立,新方案就是安全的.如何设计标准模型下不需要双线性对运算的无证书签密方案,将是下一步值得深入研究的新课题.

致谢 感谢外审专家的精心评审,感谢各位编缉的辛勤劳动!

References:

[1] Zheng YL. Digital signcryption or how to achieve *cost*(*signature* & *encryption*)<<*cost*(*signature*)+*cost*(*encryption*). In: Jr Kaliski BS, ed. Proc. of the CRYPTO'97. LNCS 1294, Heidelberg: Springer-Verlag, 1997. 165−179. [doi: 10.1007/BFb0052234]

[2] Al-Riyami SS, Paterson KG. Certificateless public key cryptography. In: Laih CS, ed. Proc. of the Advances in Cryptology—Asiacrypt 2003. LNCS 2894, Heidelberg: Springer-Verlag, 2003. 452−473. [doi: 10.1007/978-3-540-40061-5_29]

[3] Barbosa M, Farshim P. Certificateless signcryption. In: Proc. of the ACM Symp. on Information, Computer and Communications Security (ASIACCS 2008). ACM, 2008. 369−372. [doi: 10.1145/1368310.1368364]

[4] Aranha D, Castro R, Lopez J, Dahab R. Efficient certificateless signcryption. 2008. http://sbseg2008.inf.ufrgs.br/proceedings/data/pdf/st03_01_resumo.pdf

[5] Wu CH, Chen ZX. A new efficient certificateless signcryption scheme. In: Proc. of the ISISE 2008. 2008. 661−664. [doi: 10.1109/ISISE.2008.206]

[6] Sharmila DS, Vivek SS, Pandu RC. On the security of certificateless signcryption schemes. Cryptology ePrint Archive: Report 2009/298. 2009. http://eprint.iacr.org/2009/298

[7] da Silva RR. Toward efficient certificateless signcryption from (and without) bilinear pairings. 2008. http://sbseg2008.inf.ufrgs.br/proceedings/data/pdf/st03_03_artigo.pdf

[8] Li FG, Shirase M, Takagi T. Certificateless hybrid signcryption. In: Proc. of the ISPEC 2009. LNCS 5451, Berlin, Heidelberg: Springer-Verlag, 2009. 112−123. [doi: 10.1007/978-3-642-00843-6_11]

[9] MIRACL. Multiprecision integer and rational arithmetic C/C++ Library. 2004. http://indigo.ie/mscott/

[10] Chen L, Cheng Z, Smart NP. Identity-Based key agreement protocols from pairings. Int'l Journal of Information Security, 2007, 6(4):213−241. [doi: 10.1007/s10207-006-0011-9]

[11] Huang Q, Wong DS. Generic certificateless encryption in the standard model. In: Miyaji A, Kikuchi H, Rannenberg K, eds. Proc. of the IWSEC 2007. LNCS 4752, Heidelberg: Springer-Verlag, 2007. 278−291. [doi: 10.1007/978-3-540-75651-4_19]

[12] Zhang L, Zhang FT. A method to construct a class of certificateless signature schemes. Chinese Journal of Computers, 2009,32(5): 940−945 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2009.00940]

[13] Pointcheval D, Stern J. Security arguments for digital signatures and blind signatures. Journal of Cryptology, 2000,13(3):361−396. [doi: 10.1007/s001450010003]

附中文参考文献:

[12] 张磊,张福泰.一类无证书签名方案的构造方法.计算机学报,2009,32(5):940−945. [doi: 10.3724/SP.J.1016.2009.00940]

刘文浩(1974－),男,湖北孝感人,博士,主要研究领域为信息安全,密码学.

许春香(1965－),女,博士,教授,博士生导师,主要研究领域为信息安全,密码学.