基于多变量公钥密码体制的无证书多接收者签密体制

李慧贤[1)] 陈绪宝[1)] 庞辽军[2)] 王育民[2)]

[1)](西北工业大学计算机学院 西安 710072)

[2)](西安电子科技大学综合业务网国家重点实验室 西安 710071)

摘 要 针对基于身份的多接收者签密方案不能抵抗量子攻击以及存在的密钥托管问题,基于多变量公钥密码体制,提出一个多接收者模型下的无证书签密方案.新方案不仅避免了基于身份密码体制的密钥托管问题,而且继承了多变量公钥密码体制的优势,实现了"抗量子攻击"的高安全性.与现有方案相比,新方案无需双线性对操作,具有更少的计算量,更高的计算效率,适用于智能卡等计算能力较小的终端设备.最后,在随机预言模型下,给出了该文方案基于 MQ 困难问题假设和 IP 困难问题假设的安全性证明.分析表明,该文方案具有不可否认性、前向安全性、后向安全性、保护接收者隐私等安全属性.

关键词 多变量公钥密码;无证书签密;多接收者签密;抗量子攻击

中图法分类号 TP309 **DOI 号**: 10.3724/SP.J.1016.2012.01881

Certificateless Multi-receiver Signcryption Scheme Based on Multivariate Public Key Cryptography

LI Hui-Xian[1)] CHEN Xu-Bao[1)] PANG Liao-Jun[2)] WANG Yu-Min[2)]

[1)](*School of Computer Science and Engineering, Northwestern Polytechnical University, Xi'an* 710072)

[2)](*State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an* 710071)

Abstract Aiming at the vulnerability under quantum attacks and the inherent key escrow problem of the existing ID-based multi-receiver signcryption schemes, we propose an efficient certificateless multi-receiver signcryption scheme (CLMSC), which is based on the multivariate public key cryptography (MPKC). The new scheme can not only avoid the inherent key escrow problem in the identity-based cryptographic system, but also have the advantage of MPKC, that is, it can withstand the quantum attack. The proposed scheme does not require any pairing operations in signcrypting a message for any number of receivers. Therefore, compared with the existing signcryption schemes, the proposed scheme is more efficient, and thus it is suitable for terminals which have lower computation capacity like smart card. Finally, we prove its semantic security under the hardness of Multivariate Quadratic (MQ) problem and its unforgeability under the Isomorphism of Polynomials (IP) assumption in the random oracle model respectively. The proposed scheme also has the security properties of non-repudiation, forward security, backward security and the recipient privacy protection.

Keywords multivariate public key cryptography; certificateless signcryption; multi-receiver signcryption; withstanding quantum attack

---

收稿日期:2012-05-15;最终修改稿收到日期:2012-07-10.本课题得到国家自然科学基金(61103178)、高等学校博士学科点专项科研基金(20096102120045)资助.**李慧贤**,女,1977 年生,博士,副教授,主要研究方向为网络与信息安全、多接收者签密及应用. E-mail: lihuixian@nwpu.edu.cn. **陈绪宝**,男,1987 年生,硕士研究生,主要研究方向为多接收者签密. **庞辽军**,男,1978 年生,博士,副教授,中国计算机学会(CCF)高级会员,主要研究方向为密码学、安全协议设计与分析. **王育民**,男,1936 年生,教授,博士生导师,主要研究领域为信息论、密码、编码.

1 引 言

传统的公钥基础设施中,一个可信中心用于管理用户的证书,但它会带来证书管理问题,包括证书的产生、存储、分配及销毁等.为了解决传统公钥密码体制中的证书管理问题,文献[1]提出了基于身份的公钥密码体制,它的主要思想是利用用户的数字身份信息作为它的公钥,同时,系统还需要一个可信的第三方用于计算用户的私钥信息.然而,基于身份的公钥密码体制存在密钥托管问题.

为了解决密钥托管问题,Al-Riyami 等人[2]在 2003 年首次提出无证书密码体制,并立刻成为密码学领域的研究热点.在该体制中,用户的私钥由两部分组成:一部分是由密钥生成中心 KGC(Key Generator Center)生成,另一部分则由用户生成,这样就解决了传统公钥密码体制中的证书管理问题,并消除了基于身份的密码体制中的密钥托管问题.2008 年,Barbosa 等人[3]首次将签密思想引入无证书密码体制.签密技术[4]能够在一个逻辑步内同时实现签名和加密两项功能,而且其计算量和通信开销均大幅低于传统的"先签名后加密"方案,是实现既保密又认证消息传输的理想方法.此后,无证书签密得到学者的广泛研究[5-6].Barbosa 等人[3]的方案利用双线性对运算提出了一种具有前向安全性的无证书签密方案,但没有给出安全性证明.2008 年,Selvi 等人[7]首次在多接收者模型下构建了一个无证书签密方案,但是方案的计算量较大.随后,Selvi 等人研究发现文献[7]的方案在伪造性攻击下是不安全的,并在 2009 年给出一个改进方案①.然而 Miao 等人[8]指出 Selvi 等人的改进方案在内部攻击下依旧是不安全的,并给出了详细的安全分析.2010 年,Li 等人[9]利用双线性对构造了无证书签密方案,并对方案进行了可证明安全分析,但该方案计算效率较低.朱辉等人[10]和 Jing[11]分别基于离散对数问题提出不使用双线性对的无证书签密方案,使计算量进一步降低,并在随机预言机模型下分析了方案的安全性.

随着无线网络和移动终端的快速发展,构建安全、高效的通信是首要解决的问题,然而,移动终端的计算能力低和无线网络的带宽窄,严重制约了包含双线性对等复杂运算的签密方案的应用.迄今为止,几乎所有的无证书签密方案都是基于公钥密码实现的,这些公钥密码的安全性主要基于因式分解和离散对数问题.随着量子计算机的发展,公钥密码所依赖的数学难题将得到解决,现有的无证书签密方案的安全性将会受到威胁②.因此,设计一个抗量子攻击的无证书签密方案成为一项越来越紧迫的任务.多变量公钥密码能够抵抗量子计算机的攻击,被认为是后量子时代的一种安全的密码体制,其安全性是基于有限域上二次方程的难解性,与现有基于身份的密码体制相比,其计算量大大减少,计算效率更高,并且可以在低端设备上实现强安全性的通信.基于多变量密码体制的签名方案得到广泛研究[12-13].

据此,本文利用多变量密码体制对现有的无证书签密方案进行改进,提出一个基于多变量密码体制的多接收者无证书签密方案,新方案不仅具备无证书体制的优势,而且可以以轻量级的计算实现抗量子攻击的高安全性,新方案可以完美地解决上述问题,符合实际需求.最后在随机预言模型下,对新方案进行了详细的安全性证明.此外,该方案还具有前向安全性、后向安全性、不可否认性、保护接收者隐私等安全属性,与现有的其它无证书签密方案相比效率更高.

2 预备知识

2.1 MQ 问题和 IP 问题

本节简要介绍多变量公钥密码学的相关背景知识,包括多变量多项式方程组、MQ 问题和 IP 问题.

选取一个大素数 p,G 是以 p 为阶的有限域.令 n 表示变量的数目,g 为方程的数目,d 表示方程组的全次数.$x_1,x_2,\cdots,x_n$ 是有限域 G 上的 n 个变量.令 P 表示全次数为 d 由 g 个 n 元变量多项式组成的多项式组,即 $P=(p_1,p_2,\cdots,p_g)$,其中 $p_i(i=1,2,\cdots,g)$ 定义如下:

$$p_i(x_1,x_2,\cdots,x_n)=\sum_{1\le j\le k\le n}\gamma_{ijk}x_jx_k+\sum_{j=1}^{n}\beta_{ij}x_j+\alpha_i \tag{1}$$

上式中所有变量 x 和系数 α、β、γ 都在域 G 中.

定义 1. 多变量多项式方程组:令 y_l, y_2,$\cdots$,y_g 是有限域 G 上的元素,p_i 同式(1)定义,那么

$$\begin{cases} y_1=p_1(x_1,x_2,\cdots,x_n)\\ y_2=p_2(x_1,x_2,\cdots,x_n)\\ \quad\cdots\\ y_g=p_g(x_1,x_2,\cdots,x_n) \end{cases} \tag{2}$$

① Selvi S S D, Vivek S S, Rangan C P. A note on the certificateless muli-receiver signcryption scheme. http://eprint.iacr.org/2009/308, 2009

② PQCrypto 2006. http://postquantum.cr.yp.to/pqcrypto-2006record.pdf

就是一个多变量多项式方程组.

当全次数 $d=2$ 时，有限域 G 上的多变量多项式方程组就称为二次多变量方程组.

定义 2. 给定有限域 G 的二次多变量方程组：

$$\begin{aligned} p_1(x_1,x_2,\cdots,x_n)&=p_2(x_1,x_2,\cdots,x_n)\cdots\\ &=p_g(x_1,x_2,\cdots,x_n)\\ &=0 \end{aligned} \tag{3}$$

其中 p_i 的系数和变量均取自有限域 G，求解该方程组的问题称为 MQ 问题(Multivariate Quadratic-Problem).

MQ 问题已经被证明是 NP-困难问题[14]. 多变量公钥密码体制的安全性依赖于 MQ 问题的难解性.

定义 3. 设 P 和 Q 为有限域 G 上两个随机的 n 元 g 个方程的多变量方程组，且 P 和 Q 同构，则有 $P=T\circ Q\circ V$(符号$\circ$表示映射合成)，T 和 V 分别为 G^n 上的两个可逆的仿射变换，这里 G^n 表示有限域 G 的 n(n 为一个正整数)次扩张. 称寻找从 $P\sim Q$ 同构的(T,V)问题为 IP 问题(Isomorphism of Polynomials Problem)，即多项式同构问题.

1996 年，在欧密会上 Patarin 证明了 IP 问题为 NP 困难问题[15]. 因此，可以利用 IP 问题将陷门 T、V 很好地隐藏到公钥 P 中，从而构造多变量公钥密码体制的单向陷门函数.

2.2 多变量公钥密码体制基本结构

公钥：多变量加密结构的公钥为 $P=T\circ Q\circ V$，其中 Q 是选择的中心映射，V 是一个在有限域 G^n 上随机选择的可逆映射，V：$G^n\to G^n$，T 是一个在有限域 G^g 上随机选择的可逆映射，T：$G^g\to G^g$，T 和 V 主要用于隐藏中心映射 Q. Q 是 G^n 到 G^g 的中心映射，它的多项式表达形式为包含 n 个变量 g 个多项式的方程组：

$$\begin{aligned} Q(x_1,x_2,\cdots,x_n)=&(p_1(x_1,x_2,\cdots,x_n),\cdots,\\ &p_g(x_1,x_2,\cdots,x_n)) \end{aligned} \tag{4}$$

私钥：三元组(T,Q,V)为多变量加密结构的私钥.

加密过程：令 x 为明文消息，$x=(x_1,x_2,\cdots,x_n)$，带入公钥多项式，计算 $P(x)$，得到的 $y=(y_1,y_2,\cdots,y_g)$即为加密密文.

解密过程：接收到密文 $y=(y_1,y_2,\cdots,y_g)$，解密密文即计算方程 $P(x)=y$ 的根，$x=P^{-1}(y)$，可以先后计算 $y_T=T^{-1}(y)$，$y_Q=Q^{-1}(y_T)$，$x=V^{-1}(y_Q)$，最终得到明文消息 $x=(x_1,x_2,\cdots,x_n)$.

2.3 算法模型

一个无证书多接收者签密方案由 5 个概率多项式算法组成，包括系统建立算法、部分密钥生成算法、用户密钥生成算法、签密算法和解签密算法[7]. 结合多变量密码体制的特点，本文对无证书多接收者签密方案进行了改进，在部分密钥生成阶段，KGC 生成了通用的系统部分公钥和系统部分私钥.

(1) 系统建立算法(Setup)：该算法由 KGC 运行. 输入秘密参数 s_0，返回系统参数 $params$.

(2) 部分密钥生成算法(Partial Key Extract)：该算法由 KGC 运行. KGC 生成系统主密钥 w，输入系统参数 $params$ 和系统主密钥 w，KGC 输出系统的部分公钥 PP_u 和部分私钥 PS_u，即$\{w,params\}\to\{PP_u,PS_u\}$.

(3) 用户密钥生成算法(Key Extract)：输入公共参数 $params$、PP_u、PS_u 和用户身份 ID_u，用户 U 执行该算法生成自己完整的公钥 PK_u 和私钥 SK_u，即$\{PP_u,PS_u,ID_u,params\}\to\{PK_u,SK_u\}$.

(4) 签密算法(Signcrypt)：签密算法由发送者 *Sender* 执行. 输入 $params$、消息 m、发送者身份 ID_s、发送者私钥 SK_s 以及接收者组 L 的身份和公钥信息，算法最后输出密文 σ，即$\{params,ID_s,SK_s,m,L_0,L_1\}\to\sigma$，其中接收者身份集合 $L_0=\{ID_1,ID_2,\cdots,ID_t\}$，接收者公钥集合 $L_1=\{PK_1,PK_2,\cdots,PK_t\}$.

(5) 解签密算法(De-Signcrypt)：输入 $params$、σ、签密者身份 ID_s、公钥 PK_s、接收者身份 ID_i 及其私钥 SK_i，若验证通过则输出 m，否则解密失败输出 $\perp$. 若正确解签密即有$\{params,\sigma,ID_s,PK_s,ID_i,SK_i\}\to m$.

2.4 安全模型

基于多变量的无证书多接收者签密的安全模型是基于 Selvi 等人[7]所定义的无证书多接收者签密的安全模型，对于无证书密码体制面对两种类型攻击：类型 1 攻击和类型 2 攻击. 对应两类攻击者，分别为 A_1 和 A_2. 在类型 1 攻击中，A_1 可以替换所有用户的公钥，但不能得到 KGC 的主密钥；在类型 2 攻击中，A_2 代表恶意的 KGC，可以知道系统主密钥但是不允许替换任何公钥.

定义 4. 类型 1 攻击下的机密性. 若不存在任何多项式有界敌手 A 以不可忽略优势赢得 IND-CLMSC-CCA2-1 游戏[7]，则称该基于多变量的无证书多接收者签密方案在适应性选择密文攻击下具有不可区分性(Type1-IND-CLMSC-CCA2).

敌手 A 在 IND-CLMSC-CCA2-1 游戏中需遵守以下限制：(1) 不能对系统主密钥进行询问；(2) 不能对挑战者集合中的身份进行私钥提取询问；(3) 不能对挑战密文执行解签密询问.

定义 5. 类型 2 攻击下的机密性. 若不存在任何多项式有界敌手 A 以不可忽略优势赢得 IND-CLMSC-CCA2-2 游戏[7],则称该基于多变量的无证书多接收者签密方案在适应性选择密文攻击下具有不可区分性(Type2-IND-CLMSC-CCA2).

敌手 A 在 IND-CLMSC-CCA2-2 游戏中需遵守以下限制:(1)不能对挑战者集合中的身份进行私钥提取询问;(2)不能进行公钥替换询问;(3)不能对挑战密文执行解签密询问.

定义 6. 类型 1 攻击下的不可伪造性. 若不存在任何多项式有界敌手 A 以不可忽略优势赢得 EUF-CLMSC-CMA-1 游戏[7],则称该基于多变量的无证书多接收者签密方案在适应性选择消息攻击下具有不可伪造性(Type1-EUF-CLMSC-CMA).

敌手 A 在 EUF-CLMSC-CMA-1 游戏中需遵守以下限制:(1)不能对系统主密钥进行询问;(2)不能对挑战者集合中的身份进行私钥提取询问.

定义 7. 类型 2 攻击下的不可伪造性. 若不存在任何多项式有界敌手 A 以不可忽略优势赢得 EUF-CLMSC-CMA-2 游戏[7],则称该基于多变量的无证书多接收者签密方案在适应性选择消息攻击下具有不可伪造性(Type2-EUF-CLMSC-CMA).

敌手 A 在 EUF-CLMSC-CMA-2 游戏中需遵守以下限制:(1)不能对挑战者集合中的身份进行私钥提取询问;(2)不能进行公钥替换询问.

3 新方案

本文提出的基于多变量的无证书多接收者签密方案由 5 个算法组成,分别是系统参数建立算法、部分密钥生成算法、用户密钥生成算法、签密算法和解签密算法. 具体描述如下.

(1)系统参数建立算法(Setup).

输入秘密参数 s_0,KGC 产生大素数 p 和正整数 l,设置特征为 p、阶为 q 的有限域 G,其中 $q=p^l$;选择两个安全的 Hash 函数 $H_1:G^n\times G^n\times G^n\to G^n$,$H_2:G^n\to G^n$,选择一个正整数 g 表示多变量方程组中方程的个数. 最后公开系统参数(G,l,g,n,q,p,H_1,H_2).

(2)部分密钥生成算法(Partial Key Extract).

① KGC 选择安全的多变量加密算法 MES(Multivariate Encryption System),其核心变换 F 为 $G^n\to G^n$ 上的可逆二次变换,并在 $G^n\to G^n$ 上随机选择两个可逆的仿射变换 T 和 V,则 KGC 的系统公钥为 $\overline{F}=T\circ F\circ V$,系统私钥为$(T,F,V)$.

② KGC 在 $G^n\to G^n$ 上随机选择两个可逆的仿射变换 T_0 和 V_0,计算 $\overline{F}_0=T_0\circ\overline{F}\circ V_0$,则部分公钥为 $\overline{F}_0$,部分私钥为$(T_0\circ T,F,V\circ V_0)$. 最后,KGC 通过秘密信道将部分私钥传递给合法用户,KGC 公开自己的系统公钥. 注意:当有用户退出时,KGC 需重新生成系统部分公钥和系统部分私钥;增加新用户则不需改变密钥.

(3)用户密钥生成算法(Key Extract).

① 用户 U 获取 KGC 的部分公钥和部分私钥,随机选择 $G^n\to G^n$ 上的仿射变换 T_u 和 V_u,计算公钥 F_u,$F_u=T_u\circ\overline{F}_0\circ V_u$. 用户 U 的公钥为 F_u,私钥为$(T_u\circ T_0\circ T,F,V\circ V_0\circ V_u)$.

② 用户 U 将公钥 F_u 传递给 KGC.

(4)签密算法(Signcrypt).

身份为 ID_A 的用户 Alice,将签密消息 m 发送给用户组 $L=\{ID_1,ID_2,\cdots,ID_t\}$,首先通过向 KGC 查询得到用户组 L 的公钥信息,然后进行如下计算.

① 选择随机数 $r\in G^n$,并依次计算 $X=\overline{F}(r)$,$Y=H_1(m\parallel ID_A\parallel X)$,$S=F_A^{-1}(Y)$.

② 对于 ID_i,$i=1,2,\cdots,t$,计算 $q_i=H_2(ID_i)$,$W_i=F_i(m\parallel S\parallel X)\oplus(q_i\parallel Y)$.

③ 对于用户组 L,计算 $L'=\overline{F}_0(L)$.

④ 最后生成密文 $\sigma=(S,W_1,W_2,\cdots,W_t,L')$.

(5)解签密算法(De-SignCrypt).

用户 ID_i,$i=1,2,\cdots,t$,收到密文 σ 后,进行如下计算.

① 获取身份列表,$L=\overline{F}_0^{-1}(L')$,提取其对应的密文信息$(S,W_i)$.

② 解密时依次计算 $Y'=F_A(S)$,$q_i=H_2(ID_i)$,$Z=W_i\oplus(q_i\parallel Y')$,$m'\parallel S'\parallel X'=F_i^{-1}(Z)$.

③ 验证等式 $Y'=H_1(m'\parallel ID_A\parallel X')$ 是否成立. 若等式成立则接受密文 σ,否则拒绝并输出 $\perp$.

4 分析与讨论

4.1 正确性分析

定理 1. 新方案解签密阶段的解密和验证过程是正确的.

证明. 用户 ID_i,$i=1,2,\cdots,t$,接收到密文 σ,提取出相应的密文信息(S,W_i),进行如下计算,$Y'=F_A(S)=F_A(F_A^{-1}(Y))=Y$,只有用户 Alice 知道自己的私钥 F_A^{-1},使得上述等式成立. 以及 $q_i=H_2(\mathrm{ID}_i)$,$Z=W_i\oplus(q_i\|Y')=W_i\oplus(q_i\parallel Y)$,则 $m'\parallel S'\parallel X'=\overline{F}_i^{-1}(Z)=m\parallel S\parallel X$,用户 ID_i 利用其私钥计算出消息 m 及 X,进而 $Y'=H_1(m'\parallel ID_A\parallel X')=$

$H_1(m \| ID_A \| X)$成立，说明解签密阶段的计算是正确的.　　证毕.

4.2　安全性分析

4.2.1　保密性

定理 2.　类型 1 攻击下的保密性. 在随机预言模型中，如果存在一个 IND-CLMSC-CCA2-1 敌手 A，能够在多项式时间内以 ε 的优势赢得定义 4 中的游戏(最多进行 q_{H_1} 次 H_1 询问，q_{H_2} 次 H_2 询问，q_{ske} 次私钥提取询问，q_{pke} 次公钥提取询问，q_{pkr} 次公钥替换询问，q_{sc} 次签密询问，q_{dsc} 次解签密询问)，那么存在一个算法 C 能够在多项式时间内以 ε' 优势解决 MQ 问题，其中

$$\varepsilon' > \frac{\varepsilon}{t.q_{sc}+q_{H_1}}\left(1-\frac{q_{sc}.(t.q_{sc}+q_{H_2})}{2^{G_1}}\right)\left(1-\frac{q_{dsc}}{2^{G_1-1}}\right).$$

其中 G_1 表示有限域 G 进行 n 次扩张后的元素大小. 下同.

证明. 算法 C 接收到一个 MQ 问题实例$\langle f(x), Y_0=f(X_0)\rangle$，$C$ 的目标是计算出 X_0. C 把 A 作为子程序并扮演 IND-CLMSC-CCA2-1 游戏中的挑战者.

1) 初始化. C 设置 $\overline{F}=T\circ F\circ V$ 作为系统公钥，在 $G^n \to G^n$ 上随机选择两个可逆的仿射变换 T_0 和 V_0，可得部分私钥为$(T_0\circ T, F, V\circ V_0)$，并计算 $\overline{F}_0=T_0\circ\overline{F}\circ V_0$ 作为部分公钥，一并将公共参数$(G, l, g, n, q, p, H_1, H_2)$发送给 A，C 秘密保存系统主密钥 (T,F,V). 然后 A 输出目标身份集合 $L^*=\{ID_1^*, ID_2^*, \cdots, ID_t^*\}$. 为了保持一致性，$C$ 定义列表 L_1 和 L_2，分别用于记录 A 对预言机 H_1、H_2 的询问以及对私钥提取、公钥提取、公钥替换、签密和解签密的询问.

2) 阶段 1. A 向 C 进行下列询问.

H_1 询问：输入元组(m, ID_i, X, L)，如果表 L_1 中存在相应的记录，那么 C 返回相应的 h_i；否则选择一个随机数 $h_i \in_R G^n$，将记录$(h_i, m, ID_i, X, L, \nabla, \triangle)$加入表 L_1，并返回 h_i. 符号“∇”、“$\triangle$”分别表示用户 ID_i 对消息 m 的签名和加密的信息.

H_2 询问：输入 ID_i，如果表 L_2 中存在相应的记录，那么 C 返回相应的 q_i；否则选择一个随机数 $q_i \in_R G^n$，将记录$(q_i, ID_i, \bigcirc, \square, \diamond, b_i=0)$加入表 L_2，并返回 q_i. 3 个符号“$\bigcirc$”、“$\square$”、“$\diamond$”分别存储该用户的公钥 F_i 和秘密值 T_i、V_i. b_i 是一个标志位，表示该用户的公钥是否被替换.

私钥提取询问：输入 ID_i，如果 $ID_i=ID_j^*$，$j=1,2,\cdots,t$，则 C 丢弃该询问；否则 C 查找 L_2，提取记录$(q_i, ID_i, F_i, T_i, V_i, b_i=0)$. 如果 $b_i=0$，C 返回私钥$(T_i\circ T_0\circ T, F, V\circ V_0\circ V_i)$；如果 $b_i=1$，则该用户的公钥已被替换，C 向 A 询问私钥参数对(T_i, V_i)，C 返回相应的私钥$(T_i\circ T_0\circ T, F, V\circ V_0\circ V_i)$.

公钥提取询问：输入 ID_i，如果表 L_2 中存在相应的记录，那么 C 返回相应的 F_i；否则选择随机数 T_i，$V_i \in_R G^n$，计算 $F_i=T_i\circ\overline{F}_0\circ V_i$，返回 F_i，并更新 L_2 中的记录.

公钥替换询问：输入(ID_i, F_i')，C 搜索表 L_2 中的相应记录$(\cdot, ID_i, F_i, \cdot)$，若存在，则利用 F_i' 替换 F_i，并置 $b_i=1$；若不存在，那么对 ID_i 进行公钥提取询问，再输入(ID_i, F_i')进行替换公钥询问.

签密询问：输入$(m, ID_s, L=\{ID_{R1}, ID_{R2}, \cdots, ID_{Rt}\})$，如果 $ID_s=ID_{Ri}$，$i\in\{1,2,\cdots,t\}$，或者 $ID_{Ri}\in L^*$ 且至少有一个 $ID_{Ri}\in L^*$，$i\in\{1,2,\cdots,t\}$，则丢弃该询问. 若 $ID_s\neq ID_j^*$，$j\in\{1,2,\cdots,t\}$，则 C 知道发送者的私钥，按照签密算法进行计算，并更新表 L_1、L_2 相应的记录信息. 最后返回密文 $\sigma=\langle S, W_1, W_2, \cdots, W_t, L'\rangle$. 若 $ID_s=ID_j^*$，$j\in\{1,2,\cdots,t\}$，那么 C 不知道发送者的私钥，按照如下步骤产生密文.

首先，C 从表 L_2 提取记录$(q_j, ID_s, F_j, T_j, V_j, b_j)$，选择一个随机数 $r\in_R G^n$，计算 $X=F_j(r)$，对(m, ID_s, X, L)执行 H_1 询问，获取 h_{1j}，计算签名 S. 然后，C 随机选择 $q_i\in_R G^n$，从表 L_2 中查询记录$(\cdot, ID_{Ri}, \cdot, b_{Ri})$，计算得到 $y_i=F_i(m \| S \| X)$，$W_i=y_i\oplus(q_i \| h_{1j})$以及 L'，并更新 L_1 中的记录. 若 $b_j=1$，表明该用户的公钥被替换，则向 A 请求(T_i, V_i). 最后，将记录$(q_i, ID_{Ri}, F_i, T_i, V_i, b_i)$添加到表 L_2，如果 L_2 已经存在相应记录，那么 C 签密失败，C 失败的概率至多为 $\frac{t.q_{sc}+q_{H_2}}{2^{G_1}}$. C 将密文 $\sigma=\langle S, W_1, W_2, \cdots, W_t, L'\rangle$ 发送给 A.

解签密询问：输入密文 σ、发送者身份 ID_s 和接收者身份 ID_R，C 从中提取(S, W_i, L). 如果 $ID_R\notin L^*$，则 C 知道接收者 ID_R 的私钥，按照解密算法解密该密文；否则，C 搜索表 L_1，如果没有包含 S、L 的记录，那么 C 拒绝该密文；此外，C 搜索表 L_2，如果不包含记录$\langle q_R, ID_R, F_R, T_R, V_R, b_R\rangle$，则拒绝该密文. 计算 $Y'=F_A(S)$，$Z=W_i\oplus(q_i \| Y')$，$m' \| S' \| X'=F_i^{-1}(Z)$，如果 $S=S'$，则验证通过，返回 m，否则拒绝该密文. 此时一个有效密文被拒绝的概率至多为 $\frac{q_{dsc}}{2^{G_1-1}}$.

3) 挑战阶段. A 输出两个等长消息$\{m_0, m_1\}$，以及发送者身份 $ID_s\notin L^*$，A 希望 C 为其产生一个

挑战密文.C 随机选择一个比特 $b\in_R\{0,1\}$,签密消息 m_b 发送给 $L^*=\{ID_1^*,ID_2^*,\cdots,ID_t^*\}$.$C$ 选择一个随机数 $S^*\in_R G^n$,定义 $X_0=m_b\parallel X^*\parallel S^*$,则密文为 $\sigma^*=\langle S^*,W_1^*,W_2^*,\cdots,W_t^*,L^{*\prime}\rangle$,按如下步骤产生 W_i^*,$i=1,2,\cdots,t$.

C 选择随机数 $y_i\in_R G^n$,$q_i\in_R G^n$,$Y\in_R G^n$,计算 $W_i^*=y_i\oplus(q_i\parallel Y)$,$L^{*\prime}=\overline{F}_0(L^*)$.

4)阶段 2.C 按照阶段 1 的描述模拟 A 的查询,A 不能为接收者 ID_i^*($i=1,2,\cdots,t$)对密文 σ^* 进行解签密询问.

5)猜测阶段.最后 A 输出猜测 b^*,C 忽略 A 的猜测,通过上述分析可知,我们的模拟等同于实际攻击环境,敌手 A 猜测成功,则必须通过询问 H_1 得到 $y_i=F_i(m\parallel X\parallel S)$,$i=1,2,\cdots,t$.$C$ 在 L_1 中随机选择一个记录 $\langle h_i,m,S_i,ID_i,X^*,L,y_i\rangle$,$C$ 以 $\frac{1}{t.q_{sc}+q_{H_1}}$ 的概率(表 L_1 中至多有 $t.q_{sc}+q_{H_1}$ 个元素)选择记录中包含正确的元素 $y_i=F_i(m_b\parallel X^*\parallel S^*)$,$C$ 将 X_0 作为 MQ 问题的解输出.

下面我们分析 C 成功的概率,事件 E 表示 A 输出正确比特 $b^*=b$.

下列任一事件发生则模拟失败.

(1)E_1:对选定的挑战身份进行私钥提取询问.

(2)E_2:模拟失败,因为在某次签密询问中,发送者且至少一个接收者属于挑战者身份集合.

(3)E_3:模拟失败,因为在签密询问时对 H_2 询问出现碰撞.

(4)E_4:C 在解签密时拒绝一个有效密文.

由上可知,$Pr[E]=\varepsilon$,若事件 E 发生,则事件 E_1、E_2 都不发生,即 $\neg E_1\wedge\neg E_2$.通过上述分析可得,$Pr[E_3]\leq\frac{q_{sc}.(t.q_{sc}+q_{H_2})}{2^{G_1}}$,$A$ 总共进行 q_{sc} 次签密询问,表 L_2 中至多有 $t.q_{sc}+q_{H_2}$ 个记录;$Pr[E_4]\leq\frac{q_{dsc}}{2^{G_1-1}}$ 表示一个有效密文被拒绝的概率,$Pr[E_5]\leq\frac{1}{t.q_{sc}+q_{H_1}}$ 表示 C 从 L_1 中选择正确密文的概率.根据上述事件,我们定义 C 成功的优势

$$\varepsilon'=Pr[E\wedge\neg E_1\wedge\neg E_2\wedge\neg E_3\wedge\neg E_4\wedge E_5].$$

因此我们可得

$$\varepsilon'>\frac{\varepsilon}{t.q_{sc}+q_{H_1}}\left(1-\frac{q_{sc}.(t.q_{sc}+q_{H_2})}{2^{G_1}}\right)\left(1-\frac{q_{dsc}}{2^{G_1-1}}\right).$$

证毕.

定理 3. 类型 2 攻击下的保密性.在随机预言模型中,如果存在一个 IND-CLMSC-CCA2-2 敌手 A,能够在多项式时间内以 ε 的优势赢得定义 5 中的游戏(最多进行 q_1 次 H_1 询问,q_2 次 H_2 询问,q_{ske} 次私钥提取询问,q_{pke} 次公钥提取询问,q_{sc} 次签密询问,q_{dsc} 次解签密询问),那么存在一个算法 C 能够在多项式时间内以 ε' 优势解决 MQ 问题.其中

$$\varepsilon'>\frac{\varepsilon}{t.q_{sc}+q_{H_1}}\left(1-\frac{q_{sc}.(t.q_{sc}+q_{H_2})}{2^{G_1}}\right)\left(1-\frac{q_{dsc}}{2^{G_1-1}}\right).$$

在第 2 类攻击类型下,攻击者可以获得系统主密钥信息,但不能替换用户公钥,参照定理 2,我们可以很容易证明定理 3 成立.

4.2.2 不可伪造性

定理 4. 类型 1 攻击下的不可伪造性.在随机预言模型中,如果存在一个 EUF-CLMSC-CMA-1 敌手 A,能够在多项式时间内以 ε 的优势赢得定义 6 中的游戏(最多进行 q_{H_1} 次 H_1 询问,q_{H_2} 次 H_2 询问,q_{ske} 次私钥提取询问,q_{pke} 次公钥提取询问,q_{pkr} 次公钥替换询问,q_{sc} 次签密询问,q_{ver} 次验证询问),那么存在一个算法 C 能够在多项式时间内以 ε' 优势解决 IP 问题.其中

$$\varepsilon'>\frac{\varepsilon}{t(t.q_{sc}+q_{H_2})}\left(1-\frac{q_{sc}.(t.q_{sc}+q_{H_2})}{2^{G_1}}\right)\left(1-\frac{q_{dsc}}{2^{G_1-1}}\right).$$

证明. 算法 C 接收到一个 IP 问题实例($F_S=T_S\circ\overline{F}_0\circ V_S,\overline{F}_0$),$C$ 的目标是计算出(T_S,V_S).C 把 A 作为子程序并扮演 EUF-CLMSC-CMA-1 游戏中的挑战者.

1)初始化.C 设置 $\overline{F}=T\circ F\circ V$ 作为系统公钥,在 $G^n\to G^n$ 上随机选择两个可逆的仿射变换 T_0 和 S_0,可得部分私钥为($T_0\circ T,F,V\circ V_0$),并计算 $\overline{F}_0=T_0\circ\overline{F}\circ V_0$ 作为部分公钥,一并将公共参数(G,l,g,n,q,p,H_1,H_2)发送给 A,秘密保存系统主密钥(T,F,V).然后 A 输出目标身份集合 $L^*=\{ID_1^*,ID_2^*,\cdots,ID_t^*\}$.为了保持一致性,$C$ 定义列表 L_1 和 L_2,分别用于记录 A 对预言机 H_1、H_2 的询问,以及对私钥提取、公钥提取、公钥替换、签密和验证的询问.

2)攻击.A 向 C 进行下列询问.

H_1 询问:输入元组(m,ID_i,X,L),如果表 L_1 中存在相应的记录,那么 C 返回相应的 h_i;否则选择一个随机数 $h_i\in G^n$,将记录($h_i,m,ID_i,X,L,\nabla,\triangle$)加入表 L_1,并返回 h_i.符号“∇”,“$\triangle$”分别表示用户 ID_i 对消息 m 的签名和加密的信息.

H_2 询问:输入 ID_i,如果表 L_2 中存在相应的记录,那么 C 返回相应的 q_i;否则选择一个随机数 $q_i\in_R G^n$,将记录($q_i,ID_i,\bigcirc,\square,\diamond,b_i=0$)加入表 L_2,并返回 q_i.3 个符号“$\bigcirc$”,“$\square$”,“$\diamond$”分别存储该用户的公钥 F_i 和秘密值 T_i、V_i.b_i 是一个标志位,表示该用户的公钥是否被替换.

私钥提取询问：输入 ID_i，如果 $ID_i=ID_j^*$，$j=1,2,\cdots,t$，则 C 丢弃该询问；否则 C 查找 L_2，提取记录$(q_i,ID_i,F_i,T_i,V_i,b_i=0)$. 如果 $b_i=0$，C 返回私钥$(T_i\circ T_0\circ T,F,V\circ V_0\circ V_i)$；如果 $b_i=1$，则该用户的公钥已被替换，C 向 A 询问私钥参数对(T_i,V_i)，C 返回相应的私钥$(T_i\circ T_0\circ T,F,V\circ V_0\circ V_i)$.

公钥提取询问：输入 ID_i，如果表 L_2 中存在相应的记录，那么 C 返回相应的 F_i；否则选择随机数 T_i，$V_i\in_R G^n$，计算 $F_i=T_i\circ\overline{F}_0\circ V_i$，返回 F_i，并更新 L_2 中记录.

公钥替换询问：输入(ID_i,F_i')，C 搜索表 L_2 中的相应记录$(\cdot,ID_i,F_i\cdot)$，若存在，则利用 F_i'替换 F_i，并置 $b_i=1$；若不存在，那么对 ID_i进行公钥提取询问，再输入(ID_i,F')进行替换公钥询问.

签密询问：输入$(m,ID_s,L=\{ID_{R1},ID_{R2},\cdots,ID_{Rt}\})$，如果 $ID_s=ID_{Ri}$，$i\in\{1,2,\cdots,t\}$，或者 $ID_s\in L^*$ 且至少有一个 $ID_{Rj}\in L^*$，$j\in\{1,2,\cdots,t\}$，则丢弃该询问. 若 $ID_s\neq ID_j^*$，$j\in\{1,2,\cdots,t\}$，则 C 知道发送者的私钥，按照签密算法进行计算，并更新表 L_1、L_2 相应的记录信息. 最后返回密文 $\sigma=\langle S,W_1,W_2,\cdots,W_t,L'\rangle$. 若 $ID_s=ID_j^*$，$j\in\{1,2,\cdots,t\}$，那么 C 不知道发送者的私钥，按照如下步骤产生密文.

首先，C 从表 L_2 提取记录$(q_j,ID_s,F_j,T_j,V_j,b_j)$，选择一个随机数 $r\in_R G^n$，计算 $X=F_j(r)$，对(m,ID_s,X,L)执行 H_1 询问，获取 h_{1j}，计算签名 S. 然后，C 随机选择 $q_i\in_R G^n$，从表 L_2 中查询记录$(\cdot,ID_{Ri},\cdot,b_{Ri})$，计算得到 $y_i=F_i(m\parallel S\parallel X)$，$W_i=y_i\oplus(q_i\parallel h_{1j})$以及 L'，并更新 L_1 中的记录. 若 $b_j=1$，表明该用户的公钥被替换，则向 A 请求(T_i,V_i). 最后，将记录$(q_i,ID_{Ri},F_i,T_i,V_i,b_i)$添加到表 L_2，如果 L_2 已经存在相应记录，那么 C 签密失败，C 失败的概率至多为 $\frac{t.q_{sc}+q_{H_2}}{2^{G_1}}$. C 将密文 $\sigma=\langle S,W_1,W_2,\cdots,W_t,L'\rangle$ 发送给 A.

验证询问：输入密文 $\sigma=\langle S,W_1,W_2,\cdots,W_t,L'\rangle$，发送者身份 ID_s 和接收者身份 ID_R，C 从中提取(S,W_i,L)，如果 $ID_R\notin L^*$，则 C 知道接收者 ID_R 的私钥，按照解签密算法解密该密文；否则，C 搜索表 L_1，如果没有包含 S、L 的记录，那么 C 拒绝该密文；此外，C 搜索表 L_2，如果不包含记录$\langle q_R,ID_R,F_R,T_R,S_R,b_R\rangle$，则拒绝该密文. 计算 $Y'=F_A(S)$，$Z=W_i\oplus(q_i\parallel Y')$，$m'\parallel S'\parallel X'=F_i^{-1}(Z)$，如果 $S=S'$ 成立，那么验证通过，否则验证失败. 此时一个有效密文验证失败的概率至多为 $\frac{q_{dsc}}{2^{G_1-1}}$.

3）伪造. 进行多项式有界次上述询问后，A 输出伪造密文 $\sigma^*=\langle S^*,W_1^*,W_2^*,\cdots,W_t^*,L^{*\prime}\rangle$（对于 $L=\{ID_{R1},ID_{R2},\cdots,ID_{Rt}\}$，至少有一个 $ID_{Ri}\notin L^*$），发送者身份 $ID_s\in L^*$.

通过上述分析可知，我们的模拟等同于实际攻击环境，敌手 A 伪造成功，则必须通过询问 H_2 得到(T_S,V_S). C 在 L_2 中随机选择一个记录$\langle q_i,ID_s,F_i,T_i,V_i,b_i\rangle$，$C$ 以 $\frac{1}{t.q_{sc}+q_{H_2}}$ 的概率（表 L_2 中至多有 $t.q_{sc}+q_{H_2}$ 个元素，ID_s 被选中的概率为 $1/n$）选择的记录中包含正确的数对(T_S,V_S)，C 将其作为 IP 问题的解输出.

下面我们分析 C 成功的概率，事件 E 表示 A 伪造的密文 σ^* 验证通过.

下列任一事件发生则模拟失败.

（1）E_1：对选定的挑战身份进行私钥提取询问.

（2）E_2：模拟失败，因为在某次签密询问中，发送者且至少一个接收者属于挑战者身份集合.

（3）E_3：模拟失败，因为在签密询问时对 H_2 询问出现碰撞.

（4）E_4：C 在验证时拒绝一个有效密文.

由上可知，$Pr[E]=\varepsilon$，若事件 E 发生，则事件 E_1、E_2 都不发生，即 $\neg E_1\wedge\neg E_2$. 通过上述分析可得，$Pr[E_3]\leq\frac{q_{sc}.(t.q_{sc}+q_{H_2})}{2^{G_1}}$，$A$ 总共进行 q_{sc} 次签密询问，表 L_2 中至多有 $t.q_{sc}+q_{H_2}$ 个记录；$Pr[E_4]\leq\frac{q_{dsc}}{2^{G_1-1}}$，表示一个有效密文验证未通过的概率，$Pr[E_5]\leq\frac{1}{t.q_{sc}+q_{H_2}}$ 表示 C 从 L_2 中选择正确密文的概率. 根据上述事件，我们定义 C 成功的优势

$$\varepsilon'=Pr[E\wedge\neg E_1\wedge\neg E_2\wedge\neg E_3\wedge\neg E_4\wedge E_5].$$

因此我们可得

$$\varepsilon'>\frac{\varepsilon}{t(t.q_{sc}+q_{H_2})}\left(1-\frac{q_{sc}.(t.q_{sc}+q_{H_2})}{2^{G_1}}\right)\left(1-\frac{q_{dsc}}{2^{G_1-1}}\right).$$

证毕.

定理 5.　类型 2 攻击下的不可伪造性. 在随机预言模型中，如果存在一个 EUF-CLMSC-CMA-2 敌手 A，能够在多项式时间内以 ε 的优势赢得定义 7 中的游戏（最多进行 q_1 次 H_1 询问，q_2 次 H_2 询问，q_{ske} 次私钥提取询问，q_{pke} 次公钥提取询问，q_{sc} 次签密询问，q_{ver} 次验证询问），那么存在一个算法 C 能够在多项式时间内以 ε' 优势解决 IP 问题. 其中

$$\varepsilon'>\frac{\varepsilon}{t(t.q_{sc}+q_{H_2})}\left(1-\frac{q_{sc}.(t.q_{sc}+q_{H_2})}{2^{G_1}}\right)\left(1-\frac{q_{dsc}}{2^{G_1-1}}\right).$$

在第 2 类攻击类型下，攻击者可以获得系统主

密钥信息,但不能替换用户公钥,参照定理 4,我们可以很容易证明定理 5 成立.

4.2.3 前向安全性

签密者每次发送消息,都要选择随机数 $r\in G^n$,即便发送相同的消息,最后形成的密文 $\sigma=(S,W_1,W_2,\cdots,W_t,L')$也是不同的.因此,攻击者获得 Alice 的密钥也无法生成之前签密时的 $X=\overline{F}(r)$,也就无法获得传输的消息 m.因此,本方案满足前向安全性.

4.2.4 后向安全性

在本文方案中,当有用户退出时,KGC 会重新计算用户组的部分私钥,组内用户生成新的密钥,这样退出的用户即便接收到密文消息,也无法解密出正确的明文消息.因此,本方案满足后向安全性.

4.2.5 不可否认性

由定理 4、定理 5 可知,本文方案是不可伪造的,若 Alice 确实签密过一个消息 m,那么她就不能对自己的行为进行否认.因此本方案具有不可否认性.

4.2.6 保护接收者隐私

由于通信信道是公开的,那么攻击者就可以窃听获取传输的密文信息.签密阶段的步骤 3)对用户组列表 L 进行加密操作,$L'=\overline{F}_0(L)$,如果外部攻击者通过密文获取用户组成员信息,则需要求解 MQ 问题,这在计算上是不可行的,因此,本文方案能够保护用户组成员隐私.

4.3 性能分析

对于本方案的效率分析,只考虑计算量大的签密和解签密阶段操作,分析如下.

签密阶段,需要$(t+1)$次 Hash 运算,$(2t+3)$次加密运算和 1 次异或运算.解密验证阶段,每一个用户只需进行 3 次解密运算,1 次异或运算和 2 次 Hash 运算.整个操作不涉及线性对运算、指数运算、群上的点乘运算,计算量为 $O(2t+3)$.生成的密文大小为$(2t+1)G_1$,其中,t 表示接收者的人数,G_1 表示有限域 G 的 n 次扩张后元素的大小.与同为多接收者模型下具有代表性的无证书签密方案[7]相比,新方案不包含复杂的线性对运算和指数运算,具备计算量小、计算效率高、密文短小的特点.单接收者模型下的无证书签密方案[9-11],为了向 t 个接收者签密消息 m,需重复执行 t 次.所以本方案的计算量与文献[9-11]中的方案比较起来具有很大的优势,具体比较结果如表 1 所示.

随着无线传感器网络的快速发展,实现控制端和智能前端的认证和保密的数据通信,在某些机密的领域显得尤为重要.智能终端对在涉密环境中采集的敏感信息,首先通过加密技术防止敏感信息被侦听、破解,然后发送给控制端,控制端根据接收到的信息,可以实时地组播发送控制指令,调整智能终端的工作状态,出于安全考虑智能终端需对控制指令的发送者——控制终端进行身份认证.本文方案可以较好地解决上述问题,符合智能终端功耗低、计算能力偏小、通信带宽窄的特点.新方案避免了密钥托管带来的危害,同时又能实现认证和抗量子攻击的具有高安全性的数据通信.

表 1 方案效率比较

方案	双线性对运算	指数运算	Hash 运算	密文大小
Selvi 等人方法[7]	2	$2t+2$	$t+7$	$(2t+1)\|Z_q\|+\|I\|$
Li 等人方法[9]	2	$t+1$	$2t+2$	$2t\|I\|+t\|m\|$
Zhu 等人方法[10]	0	$3t+4$	$3t+3$	$2t\|I\|+t\|m\|$
Jing 等人方法[11]	0	$3t+2$	$2t+2$	$2t\|I\|+t\|m\|$
新方案	0	0	$n+3$	$(2t+1)\ G_1$

注:表中,t 表示接收者人数,$|Z_q|$表示有限域 Z_q 元素的大小,$|I|$表示循环群 I 元素的大小,$|m|$表示消息 m 的大小,G_1 表示有限域 G 的 n 次扩张后元素的大小.

5 结 论

随着对量子计算理论研究的日益成熟,后量子密码越来越得到人们的重视,多变量公钥密码作为能够抵抗量子攻击的主要备选密码体制之一,已得到学者的广泛研究.在现有无证书签密体制的基础上,提出一个基于多变量的多接收者无证书签密方案,新方案继承了多变量密码体制的安全性,能够抵抗量子攻击.基于 MQ 难题和 IP 难题在随机预言模型下分析了方案的安全性,新方案在适应性选择密文攻击下具有不可区分性并在适应性选择消息攻击下具有不可伪造性.此外,本方案还具有前向安全性、后向安全性、不可否认性和保护接收者隐私等安全属性.

参 考 文 献

[1] Shamir A. Identity-based cryptosystem and signature scheme//Proceedings of the CRYPTO 1984. California, USA, 1984: 47-53

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

[3] Barbosa M, Farshim P. Certificateless signcryption//Proceedings of the ACM Symposium on Information, Computer and Communications Security (ASIACCS). New York, USA, 2008: 369-372

[4] Zheng Y. Digital signcryption or how to achieve cost (signature & encryption)≪cost (signature)+cost (encryption)// Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology. London, UK, 1997: 165-179

[5] Barreto P L, Deusajute A M, Cruz E C, et al. Toward efficient certificateless signcryption from (and without) bilinear pairings//Proceedings of the 2008 Brazilian Symposium on Information and Computer System Security (SBSeg 2008). Gramado, Brazil, 2008: 115-125

[6] Li Fagen, Masaaki S, T suyoshi T. Certificateless hybrid signcryption//Feng Bao. Information Security Practice and Experience 2009. LNCS 5451. Berlin: Springer-Verlag, 2009: 112-123

[7] Selvi S S D, Vivek S S, Shukla D, et al. Efficient and provably secure certificateless multi-receiver signcryption//Joonsang Baek. Provable Security 2008. LNCE 5324. Berlin: Springer-Verlag, 2008: 52-67

[8] Miao Songqin, Zhang Futai, Zhang Lei. Cryptanalysis of a certificateless multi-receiver signcryption scheme//Proceedings of the International Conference on Multimedia Information Networking and Security. Nanjing, China, 2010: 593-597

[9] Li Peng-Cheng, He Ming-Xing, Li Xiao, et al. Efficient and provably secure certificateless signcryption from bilinear pairings. Journal of Computational Information Systems, 2010, 6(11): 3643-3650

[10] Zhu Hui, Li Hui, Wang Yun-Min. Certificateless signcryption on scheme without pairing. Journal of Computer Research and Development, 2010, 47(9): 1587-1594(in Chinese)
(朱辉，李晖，王育民. 不使用双线性对的无证书签密方案. 计算机研究与发展，2010，47(9)：1587-1594)

[11] Jing Xiao-Fei. Provably secure certificateless signcryption scheme without pairing//Proceedings of the International Conference on Electronic and Mechanical Engineering and Information Technology. Harbin, China, 2011: 4753-4756

[12] Tao Yu, Yang Ya-Tao, Li Zi-Chen, et al. Multivariate group signature scheme withstanding conspiracy attacks. Journal of University of Science and Technology of China, 2011, 41(7): 615-618(in Chinese)
(陶羽，杨亚涛，李子臣等. 抗合谋攻击的多变量群签名方案. 中国科学技术大学学报，2011，41(7)：615-6187)

[13] Wang Xin, Liu Jing-Mei, Wang Xin-Mei. Improvement on multivariate signature scheme model. Journal of Beijing University of Posts and Telecommunications, 2009, 32(5): 124-127(in Chinese)
(王鑫，刘景美，王新梅. 多变量签名模型的改进. 北京邮电大学学报，2009，32(5)：124-127)

[14] Patarin J, Goubin L. Trapdoor one-way permutations and multivariate polynomials//Proceedings of the first International Conference on Information and Communications Security. Beijing, China, 1997: 356-368

[15] Patarin J. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric//Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques. Saragossa, Spain, 1996: 33-48

LI Hui-Xian, born in 1977, Ph. D., associate professor. Her research interests include Internet and information security and multi-receiver encryption/signcryption.

CHEN Xu-Bao, born in 1987, M. S. candidate. His research interest focuses on multi-receiver encryption/signcryption.

PANG Liao-Jun, born in 1978, Ph. D., associate professor. His research interests include cryptography, design and analysis of secure protocols.

WANG Yu-Min, born in 1936, professor, Ph. D. supervisor. His research interests include information theory, cryptography and coding.

Background

Secure multicast holds great promise in reducing the network bandwidth required for the transmission of multimedia information such as video and audio data. It has become a hot spot in information security field. The multi-receiver signcryption scheme is considered as one of the most efficient approaches to implement secure multicast, and it has become a new branch of information security. In the recent years, some multi-receiver signcryption schemes based on pairing operations have been proposed, but most of them cannot resist the quantum attack and have high computation cost, which makes them not applicable to low-end devices, such as mobile terminals.

The contribution of this paper is designing an efficient certificateless multi-receiver signcryption scheme based on the multivariate public key cryptography to support the development and application of the secure multicast. The new scheme can not only avoid the inherent key escrow problem in identity-based cryptographic systems and cumbersome certificate management in the public key infrastructure, but also can withstand the quantum attack. In addition, our scheme does not require pairing operations in signcrypting a message for any number of receivers. Compared with the existing multi-receiver signcryption schemes in the computational complexity, ciphertext size and security, the proposed scheme is more efficient and secure and thus suits for terminals which have lower computation capacity.

This research is supported by the National Natural Science Foundation of China under Grant No. 61103178, and the Research Fund for the Doctoral Program of Higher Education of China under Grant No. 20096102120045.