基于多线性映射的环签密广播公钥方案

于志敏[1] 景征骏[1,2] 古春生[1,3]
(江苏理工学院计算机工程学院 常州 213001)[1] (南京邮电大学计算机学院 南京 210003)[2]
(中国科学技术大学计算机科学与技术学院 合肥 230027)[3]

摘 要 提出了基于多线性映射的环签密广播方案,环成员代表环群体匿名签密并广播给多个接收者。其具有两个用户群之间环签密通信的功能。该方案满足环签密广播的安全要求,能够保证签密所传输消息的保密性、签密的不可伪造性、签密者的匿名性。在随机预言模型下,把方案的安全性归约到分级 Diffie-Hellman 判定问题(GDDH)进行求解。

关键词 环签密,多线性映射,保密性,不可伪造性,匿名性,GDDH
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.3.022

Ring Signcryption Broadcasting Scheme Based on Multilinear Maps

YU Zhi-min[1] JING Zheng-jun[1,2] GU Chun-sheng[1,3]
(School of Computer Engineering, Jiangsu University of Technology, Changzhou 213001, China)[1]
(College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)[2]
(School of Computer Science and Technology, University of Science and Technology of China, Hefei 230027, China)[3]

Abstract We proposed a ring signcryption scheme based on multilinear maps. Each ring member can represent ring group to generate anonymous signcryption and broadcast it to multiple recipients. Ring signcryption can be communicated between two ring groups. The scheme meets the security requirements of ring signcryption broadcasting like the confidentiality of messages, unforgeability and anonymity. In the random oracle model, the security of the scheme is reduced to grading decisional Diffie-Hellman problem (GDDH) to solve.

Keywords Ring signcryption, Multilinear maps, Confidentiality, Unforgeability, Anonymity, GDDH

1 引言

伴随着互联网的发展,现代的公钥加密系统不仅要解决单一用户之间信息的安全交换,还要面对越来越多的多发送者和多接收者的应用场景。2001 年 Rivest、Shamir 和 Tauman 提出环签名的概念[1],环中有多个用户,每个用户拥有自己的公钥和私钥,每个用户可以代表环匿名地对消息签名,验证者可以验证签名是否由环用户签署,但具体的签名者无法确定。

Rivest 等人考虑了如下场景[1]:内阁成员中的一位深喉要泄露有关国家元首一个非常重要和丰富的信息给新闻界。他/她将以匿名的方式泄露秘密,否则泄密人在内阁将有污点记录。但是新闻媒体不会接受该信息,除非它能确定消息是由内阁成员之一签发。在这里,信息非常敏感,不应该被泄露,我们要匿名加密发送以保护泄密的内阁成员,在拥有阅读权限人收到它之前,信息都是保密的。上述场景除了需要消息加密外,还需要对消息进行环签名以保证发送者环成员身份可认证并且保证匿名性。进一步扩展该实例,泄密者把消息同时泄露给多家新闻媒体,这是一个典型的把加密和环签名处理后的密文进行广播的应用场景。

如果要降低常见的加密+签名模式所需的计算量和通讯开销,可以遵循由 Zheng 首先提出的签密[2]思想把加密和签名高效结合起来,环签名和加密有机结合起来称为“环签密”。环用户能代表环生成一个签密并发送,接收者能够使用自己的私钥解密并能够验证签密确为环成员发送,但具体哪个成员发送是匿名的。目前,研究人员已经提出多种环签密方案[3-7]。为了满足签密广播应用需要,密码学者构造了多接收者签密方案[8-11],这些方案从接收者身份公开到匿名接收,从接收者协作接收到各自独立接收等多个角度进行了设计和尝试。

上述与签密有关的公钥方案,无论是环签密方案还是多接收者签密方案,绝大多数是基于双线性对的,这些方案的签

到稿日期:2014-04-28 返修日期:2014-06-25 本文受江苏省普通高校研究生科研创新计划(CXZZ13_0493),江苏省属高校自然科学基金(13KJB520005),江苏省“青蓝工程”(KYQ14004),江苏理工学院面上项目(KYY14007),常州市云计算与智能信息处理重点实验室 2014 年开放基金项目资助。

于志敏(1973-),男,硕士,讲师,CCF 会员,主要研究方向为网络与信息安全;景征骏(1978-),男,硕士,讲师,主要研究方向为网络与信息安全;古春生(1971-),男,博士,副教授,主要研究方向为网络与信息安全。

密文中所包含群元素个数与用户人数呈线性关系，加解密需要对运算和幂运算，计算开销和数据传输的开销都比较大。更重要的是，大整数分解、离散对数等传统数论问题已经有量子算法破解[12]。后量子时代需要基于新的问题难度假设设计公钥密码原语。2003 年 Boneh 等提出了理想的多线性映射模型[13]，其一度被认为是替代双线性映射的理想工具，但是，如何构造现实的多线性映射一直是公开问题，直到最近才出现了一个近似的多线性映射模型[14]。

基于文献[14]的多线性映射，首次提出环签密广播方案。在该方案中，不仅实现了环签密，还能够把环签密同时广播给多个用户。集合 S 包括发送环所有成员，每个成员都能够利用环中成员的公钥和自己的私钥代表整个群匿名生成签密发送给接收者。集合 R 包含所有环签密接收者，接收者使用各自私钥解密并验证环签密的合法性。多线性映射良好的特性，使得方案能够很好地保证发送者匿名性、环签密不可伪造以及消息的保密性。签密包含的群元素个数固定，不会随着发送环人数或接收人数增加而线性增长。每个接收者使用自己的私钥解密，无需多个接收者共同组装解密私钥，能够保证接收的公平性。显然，集合 S 和集合 R 的角色可以互换，也就是说本文方案具有多个用户集合相互的环签密通信能力，所以，下文称两个集合为发送环 S 和接收环 R。

在计算复杂性上，本文方案除通用哈希函数外都是在多项式环上计算，所以各种算法只需大约 $|R|+|S|$ 次多项式乘法，无需复杂的双线性对运算和幂运算，计算复杂性较低，$|R|$ 和 $|S|$ 分别代表发送环人数和接收环人数。当然，与其它基于格的公钥方案类似，多线性映射需要较大的公钥存储空间，这需要进一步研究来减小公钥尺寸。

作为环签密公钥方案，在安全性方面应该满足：1）签密所传输消息的保密性；2）签密的不可伪造性；3）签密者具有匿名性。在随机预言模型下将方案的上述安全性归约到分级的 Diffie-Hellman 判定问题（GDDH）进行求解。

本文第 2 节给出预备知识；第 3 节设计环签密广播公钥方案；第 4 节证明环签密广播公钥方案的安全性；最后总结全文。

2 预备知识

2.1 符号说明

为了描述方便，首先对本文中用到的相关符号做出说明。设 n 为 2 的幂，多项式环 $R=Z[X]/(X^n+1)$。$u\in R$ 是一个度至多为 $n-1$ 的整系数多项式，其系数构成的 n 维向量也用 u 表示，两者等同视之。哈希函数 $h(\cdot)\in\{0,1\}^n$ 作为 R 上系数为 $\{0,1\}$ 的多项式参与多项式运算。设环 $R_q=R/qR=Z_q[X]/(X^n+1)$，这里 q 为较大整数。对于元素 $g\in R$，令 $\langle g\rangle$ 表示 R 中由 g 生成的主理想 I，商环 R/I 中的向量 e 的陪集标识为 $e+I$，下文出现的陪集都指理想 I 的某个陪集。

设 λ 为安全参数，正整数 n，t 为 λ 多项式大小，即 $poly(\lambda)$。给定整数 t，设集合 $[t]=\{1,2,\cdots,t\}$。对整数 t 和 p，符号 $\langle t\rangle_p$ 表示 t 模以 p 在区间 $[-p/2,p/2)$ 的取值。类似地，$\langle u\rangle_p$ 表示对向量 u 的每个整系数模以 p。A^{T} 表示矩阵 A 的转置。$a\|b$ 表示 a，b 的比特串联接。对于集合 S，$|S|$ 表示集合的元素个数。

2.2 多线性映射

Boneh 等在 2003 年首次提出了理想化的多线性映射模型[13]，其定义可描述为：若 G_1 和 G_2 是两个阶相同的循环群（阶为素数）且 G_1 上的离散对数问题是难解的，那么一个多线性映射 $e:G_1^n\to G_2$ 应具有以下特性：（1）如果 $a_1,\cdots,a_n\in\mathbb{Z}$ 且 $x_1,\cdots,x_n\in G_1$，则 $e(x_1^{a_1},\cdots,x_n^{a_n})=e(x_1,\cdots,x_n)^{\prod_{i\in[n]}a_i}$；（2）映射 e 是非退化的。也就是说，当 g 是群 G_1 的生成元时，$e(g,\cdots,g)$ 则是群 G_2 的生成元。虽然借助该模型可以实现更为高效的密码原语，但是如何实例化一个多线性映射一直是公开问题。直到最近，Gentry 等基于理想格实现了一个近似多线性映射实例，也称为分级的编码模式，即在一个 k 级编码系统中，只要 $i+j\leqslant k$，在 i 级的编码和在第 j 级的编码就可以进行乘法运算形成第 $(i+j)$ 级上的编码。显然，k 个 1 级编码累乘就可以得到一个 k 级编码。

定义 1（多线性映射） 对于具有相同阶 p 的循环群 G_1，G_T，一个 k 阶多线性映射 $e:G_1\times\cdots\times G_1\to G_T$ 满足：$e(\alpha_1 g,\alpha_2 g,\cdots,\alpha_k g)=\prod_{i=1}^{k}\alpha_i e(g,g,\cdots,g)$，其中 $g\in G_1$ 为群的生成元。

它与双线性对的主要区别是元素 α 的编码 $\alpha\cdot g$ 具有随机噪声，只有计算多重线性映射的函数 $e(\alpha_1\cdot g,\alpha_2\cdot g,\cdots,\alpha_k\cdot g)$ 是 α_i 的确定函数。该结构具有固定的编码级数 k，它是安全参数的多项式。此外，多级编码系统中，多线性群的 g_i^a 运算表示元素 $a\in R$ 在第 i 级上的编码。环 R 的 n 级编码集合为 $S=\{S_i^a\subset\{0,1\}^*:i\in[0,n],a\in R\}$，其中 S_i^a 为 a 在 i 级编码的集合。多级编码系统主要包括以下算法：

（1）系统初始化 $InstGen(1^\lambda,1^k)$。给定安全参数 λ 和最高编码级数 k，该算法输出多级编码系统的公共参数 $params=\{n,q,y,\{x_i\}_i,s\}$ 和 p_{zt}，其中 y 是陪集 $1+I$ 在第 1 级的编码，$\{x_i\}_i$ 表示大量陪集 $0+I$ 的 i 级编码，而 p_{zt} 和 s 分别是在 k 级零测试和强随机提取时用的参数。

（2）0 级采样编码 $samp(params)$。该算法随机输出一个陪集 $a+I$ 在 0 级的编码 d，即 $d\in S_0^a$。

（3）i 级编码 $enc(params,i,d)$。输入系统参数 $params$，$i\in[n]$ 和一个 0 级编码 $d\in S_0^a$，该算法通过将编码 d 乘上 y^i 得到 $a+I$ 的第 i 级编码 $u\in S_i^a$。

（4）编码随机化 $reRand(params,i,u)$。输入系统参数 $params$，$i\in[n]$ 和元素 $a+I$ 在第 i 级的编码 $u\in S_i^a$，该算法通过将参数 $params$ 中的第 i 级上 $0+I$ 的编码 $\{x_i\}_i$ 与编码 u 相加，得到元素 $a+I$ 在同一级上的另一个编码 $u^*\in S_i^a$，编码 u 和 u^* 的概率分布相同。

（5）加运算 $add(params,u_1\in S_i^\alpha,u_2\in S_i^\beta)$。对于同在 i 级上的元素 α 和 β 的编码 u_1、u_2，该算法 u_1 与 u_2 的和 $u=u_1+u_2=S_i^{\alpha+\beta}$。也就是说，两个不同元素的同级编码和等于两元素的和在该级上的编码，满足加法运算同态，前提是满足 $\|\alpha+\beta\|_\infty\ll q$。

（6）乘运算 $mult(params,u_1\in S_i^\alpha,u_2\in S_j^\beta)$。对于元素 α 的 i 级编码 u_1 和元素 β 的 j 级编码 u_2，当 $i+j\leqslant k$ 时，该算法

输出元素 α 和 β 乘积的第 $i+j$ 级编码，即 $u=u_1 \cdot u_2=S_{i+j}^{\alpha \times \beta}$。如果 α 和 β 都足够小，满足 $\|\alpha \cdot \beta\|_\infty \ll q$，那么乘法同态也满足。

(7)零元素编码测试 $isZero(params, p_{zt}, u \in S_k^\alpha)$。输入系统参数 $params$、k 级测试参数 p_{zt} 以及 k 级编码 u，如果 $\|\langle p_{zt} \cdot u \rangle_q\|_\infty < q^{3/4}$，那么认为编码 $u \in 0+I$，该算法输出 1，否则输出 0。

(8)提取算法 $ext(params, p_{zt}, u \in S_k^\alpha)$。输入系统参数 $params$、k 级参数 p_{zt} 以及编码 u，该算法输出 $b \in \{0,1\}^\lambda$ 来表示环元素 α。如果 u_1 和 u_2 均为元素 α 的 k 级编码，则 $ext(params, p_{zt}, u_1 \in S_k^\alpha)=ext(params, p_{zt}, u_2 \in S_k^\alpha)$。另外，提取算法输出的 λ 位二元值在 $\{0,1\}^\lambda$ 上均匀分布。

相同陪集的两个 k 级编码 u_1 和 u_2 之差显然是 0 陪集的 k 级编码，所以调用理想零元素编码测试算法有 $\|\langle p_{zt}(u_1-u_2)\rangle_q\|_\infty < q^{3/4}$。可以看出，一个 k 级编码与 p_{zt} 乘积系数的高 $(\log q)/4$ 位比特的值取决于这个 k 级编码所属的陪集，而不依赖于某个具体的陪集元素。

3 环签密广播公钥方案

假定发送环 S 包含所有环签密成员，其中任何成员都能够利用环中成员的公钥和自己的私钥代表整个群匿名生成签密发送给接收者。接收环 S 的每个成员的公钥和私钥用符号 $(spk_i, ssk_i)(i \in [|S|])$ 表示。假定接收环 R 包含了所有签密接收者，接收者使用各自私钥解密并验证签密的合法性，他们所拥有的公钥和私钥用符号 $(rpk_i, rsk_i)(i \in [|R|])$ 表示。在 k 级编码系统中，要求发送环人数 $|S|$ 和接收环人数 $|R|$ 满足 $2|S|+|R|-2 \leqslant k$。首先讨论 $2|S|+|R|-2=k$ 的情况，然后讨论如何处理 $2|S|+|R|-2<k$ 的情况。文中用公钥来指代相关用户。

环签密广播公钥方案包含 3 个概率多项式时间算法：密钥生成算法 KG、签密算法 B-Signcrypt 和解签密算法 B-DeSigncrypt。

3.1 方案构造

1. 密钥生成算法 KG

输入系统安全参数 λ、发送环人数 $|S|$ 和接收环人数 $|R|$。

(1)调用初始化算法 $InstGen(1^\lambda, 1^k)$ 生成参数 $params=(n, q, y, \{x_i\}_i, s)$、$p_{zt}$ 和 k，并选择安全防碰撞哈希函数 $h(\cdot) \in \{0,1\}^n$，公共参数 $pub=\{params, p_{zt}, k, h(\cdot)\}$。

(2)每个发送环成员生成密钥。以第 i 个发送环成员为例，随机选取 $sd_{i,j} \leftarrow samp(params), j \in \{0,1\}$，计算 1 级编码 $su_{i,j} \leftarrow enc(params, 1, sd_{i,j}), j \in \{0,1\}$，并随机化处理 $sw_{i,j} \leftarrow reRand(y, 1, su_{i,j}), j \in \{0,1\}$。该用户的私钥 $ssk_i=(sd_{i,0}, sd_{i,1})$，公钥 $spk_i=(sw_{i,0}, sw_{i,1})$。

(3)每个接收环成员生成密钥。以第 i 个接收环成员为例，随机选取 $rd_{i,j} \leftarrow samp(params), j \in \{0,1\}$，计算 1 级编码 $ru_{i,j} \leftarrow enc(params, 1, rd_{i,j}), j \in \{0,1\}$，并随机化处理 $rw_{i,j} \leftarrow reRand(y, 1, ru_{i,j}), j \in \{0,1\}$。该用户的私钥 $rsk_i=(rd_{i,0}, rd_{i,1})$，公钥 $rpk_i=(rw_{i,0}, rw_{i,1})$。

(4)输出公共参数 $pub=\{params, p_{zt}, k, h(\cdot)\}$ 和各方公钥集 $\{(sw_{j,0}, sw_{j,1}), j \in [|S|]\} \cup \{(rw_{j,0}, rw_{j,1}), j \in [|R|]\}$。

2. 签密算法 B-Signcrypt

假定公钥 $spk_i=(sw_{i,0}, sw_{i,1})$，私钥 $ssk_i=(sd_{i,0}, sd_{i,1})$ 的发送环成员对消息 m 签密，过程如下：

(1)随机选取 $r \xleftarrow{R} \{0,1\}^{80}$，计算 $s_0=h(m \| r) sd_{i,0} \cdot sd_{i,1}$，$s_1=\prod_{j \neq i} sw_{j,0} \prod_{j \neq i} sw_{j,1}, j \in [|S|]$；

(2)计算 $s_2=enc(params, 1, s_0) \cdot s_1$；

(3)计算 $c_1=reRand(params, 2|S|-1, s_2)$；

(4)计算 $s_3=(s_0 \cdot s_1) \prod_{j \in [|R|]} rw_{j,0}$；

(5)计算 $c_2=ext(params, p_{zt}, s_3) \oplus (m \| r)$；

(6)输出签密 $c=(c_1, c_2)$。

3. 解签密算法 B-DeSigncrypt

假定接收环成员私钥 $rsk_i=(rd_{i,0}, rd_{i,1})$，公钥 $rpk_i=(rw_{i,0}, rw_{i,1})$，输入签密 $c=(c_1, c_2)$。解签密过程如下：

(1)计算 $f_1=c_1 \cdot rd_{i,0} \prod_{j \neq i} rw_{j,0}, j \in [|R|]$；

(2)计算 $m'=ext(params, p_{zt}, f_1) \oplus c_2$；

(3)计算 $f_2=c_1 \cdot y^{k-2|S|+1} - h(m') \prod_{i \in [|S|]} (sw_{i,0} \cdot sw_{i,1}) \cdot y^{k-2|S|}$。调用函数 $isZero(params, p_{zt}, f_2)$ 判断 f_2 是否为 0 陪集的 k 级编码，如果是，则继续执行下一步骤，否则，拒绝密文，输出 $\perp$；

(4)接受明文 m' 并去掉 m' 末尾随机添加的 r 得到 m。

3.2 方案正确性分析

定理 1 上述方案每个接收环成员使用自己的私钥能够正确解密，得到明文后，能够验证签密是否为发送环成员签发。

证明：从环签密过程可知，$2|S|-1$ 级编码 $c_1 \in h(m \| r) \prod_{i \in [|S|]} (sd_{i,0} \cdot sd_{i,1}) + I$，$k$ 级编码 $s_3 \in h(m \| r) \prod_{i \in [|S|]} (sd_{i,0} \cdot sd_{i,1}) \prod_{j \in [|R|]} rd_j + I$。而 k 级编码 $f_1 \in h(m \| r) \prod_{i \in [|S|]} (sd_{i,0} \cdot sd_{i,1}) \prod_{j \in [|R|]} rd_j + I$。所以 k 级编码 s_3 和 f_1 同属一个陪集，应用提取算法后的结果相同，从而保证了解密的正确性。$c_1 \cdot y^{k-2|S|+1}$ 是陪集 $h(m \| r) \prod_{i \in [|S|]} (sd_{i,0} \cdot sd_{i,1}) + I$ 的 k 级编码，解密得到明文 m' 后，计算 $h(m') \prod sw_{j,k} \cdot y^{k-2|S|}$ 得到陪集 $h(m') \prod_{i \in [|S|]} (sd_{i,0} \cdot sd_{i,1}) + I$ 的 k 级编码。如果 $m \| r=m'$，意味着 k 级编码 $f_2 \in 0+I$，那么调用 $isZero(params, p_{zt}, f_2)$ 返回值为 1。通过这种方法，接收者正确解密后能够验证发送者是否属于发送环成员。

3.3 方案的计算复杂性分析

签密过程只需 $O(k)$ 次多项式环上的乘法，解签密过程所需计算与签密过程基本相同。与现有的多接收者方案比较，因为不需要双线性对计算和指数运算，本文方案计算复杂性更低。

3.4 特殊情况的讨论

如果 $2|S|+|R|-2 \neq k$，而是 $2|S|+|R|-2<k$，那么密钥生成算法 KG 额外生成一组密钥，私钥 $psk=(prd_0, prd_1)$，公钥 $ppk=(prw_0, prw_1)$。在执行上述签密和解签密算法中，公钥 ppk 参与运算 $k-(2|S|+|R|-2)$ 次，把相关编码补足到 k 级编码即可。因为接收环成员不需要 psk 解签

密，所以私钥 psk 不需要保存。

只要满足 $|S|+2|R|-2\leqslant k$，就可以把发送环和接收环的角色互换，两个用户群之间仍然可进行环签密通信。

4 安全性分析

参照 Zheng 对签密公钥方案安全性的定义[2]并结合环签密的特性，环签密广播方案在安全方面需要满足：1)消息的保密性；2)签密的不可伪造性；3)签密者具有匿名性。首先给出多级 Diffie-Hellman 判定问题(GDDH)的定义，并把环签密广播方案的安全性归约到 GDDH 问题进行求解。

4.1 方案的难度假设

首先给出 GDDH 问题的定义。

定义 2(GDDH 问题[14]) 考虑下述过程，参数 $params=(n,q,y,\{x_i\}_i,s)$公开。

(1)$(params,p_{sk})\leftarrow InstGen\ (1^\lambda,1^k)$；

(2)$e_j\leftarrow samp\ (params),j\in\{0\}\cup[k]$；//随机取 $k+1$ 个 0 级编码

(3)令 $u_j\leftarrow rRand(y,1,enc(params,1,e_j)),j\in\{0\}\cup[k]$；//对 $k+1$ 个 0 级编码 1 级编码并随机化

(4)$f\leftarrow samp\ (params)$；//随机取一个 0 级编码

(5)令 $v=e_0\prod_{i=1}^{k}u_i,v'=f\prod_{i=1}^{k}u_i$。

对于多级 Diffie-Hellman 判定问题(GDDH)是如何区分 v 和 v'的，更正式的定义是区分分布 $D_{GDDH}=\{(y,\{x_i\}_i,p_{sk}),u_0,\cdots,u_k,v\}$与 $D_{RAND}=\{(y,\{x_i\}_i,p_{sk}),u_0,\cdots,u_k,v'\}$。

4.2 安全性证明

4.2.1 消息保密性证明

消息保密性通过在选择明文攻击情况下密文具有不可区分性来证明。

定理 2 对于随机预言模型的环签密广播公钥方案，如果存在具有不可忽略优势 ε 的概率多项式时间攻击算法 A，则存在求解多级 Diffie-Hellman 判定问题(GDDH)的概率多项式时间算法 B。B 成功的概率接近 1，运行时间可以用 $1/\varepsilon$，λ 和 A 运行时间的多项式表示。如果多级 Diffie-Hellman 判定问题(GDDH)是难解的，那么上述签密方案满足语义安全。

证明：根据定义 2，给定的 GDDH 问题实例$((y,\{x_i\}_i,p_{sk}),u_0,\cdots,u_k,v)$要求判定 $v=e_0\prod_{i=1}^{k}u_i$ 还是 $v=f\prod_{i=1}^{k}u_i$。因为 $v=e_0\prod_{i=1}^{k}u_i$ 与 $v=f\prod_{i=1}^{k}u_i$ 分布相同，无法直接区分。虽然已知 $u_0\leftarrow enc(params,1,e_0)$，但是由 u_0 求解 e_0 是理想格问题，目前为止是难解的。假定存在能够有效攻击环签密广播方案的攻击算法 A，算法 B 借助 A 求解 GDDH 问题的步骤如下：

Step1 B 作为模拟者根据给定实例构造加密方案的密钥。B 首先随机选取 $k+1$ 个较短向量 $d_i\xleftarrow{R}\{0,1\}^n,0\leqslant i\leqslant k$，令 $w_i\leftarrow reRand(y,1,d_iu_i),0\leqslant i\leqslant k$，$(w_0,w_1,\cdots,w_k)\rightarrow(sw_{1,1},sw_{2,0},sw_{2,1},\cdots,sw_{|S|,0},sw_{|S|,1},rw_{1,0},rw_{2,0},\cdots,rw_{|R|,0})$。然后，采样 0 级编码 $sd\leftarrow samp(params)$，令 $reRand(y,1,enc(params,1,sd))\rightarrow sw_{1,0}$。最后 B 把公共参数 $params=(n,q,y,\{x_i\}_i,s)$和公钥$(sw_{1,0},sw_{1,1},sw_{2,0},sw_{2,1},\cdots,sw_{|S|,0},sw_{|S|,1},rw_{1,0},rw_{2,0},\cdots,rw_{|R|,0})$输入给攻击算法 A。(sd)保密。

Step2 A 可以询问随机预言机 q_H 次。A 向随机预言机输入一组元素 $M_i(i=1,\cdots,q_H)$。B 通过列表 $H\text{-}list(M_j,h_j)$来保存返回给 A 的值。如果列表中存在 M_j，则返回 h_j；否则，随机选择比特串 $h_j\in\{0,1\}^\ell$ 返回，并将(M_j,h_j)保存到列表中。

Step3 A 对 B 进行签密询问。A 向 B 输入一组信息 m_i $(i=1,\cdots,q_s)$，要求 B 对这些信息签密。不失一般性，假定 B 指定公钥为$(sw_{1,0},sw_{1,1})$的环用户对给定消息环签密。B 随机选取 $r\xleftarrow{R}\{0,1\}^{80}$，计算 $s_0=h(m\parallel r)sd\cdot sw_{1,1}$；计算 $s_1=s_0\prod_{j>1}sw_{j,0}\prod_{j>1}sw_{j,1},j\in[|S|]$，令 $c_1=reRand(params,2|S|-1,s_1)$；计算 $s_2=h\ (m\parallel r)sd\cdot v,c_2=ext(params,p_{sk},s_2)\oplus(m\parallel r)$，输出环签密 $c=(c_1,c_2)$给 A。

Step4 挑战。A 选择等长消息(m_0,m_1)发送给 B。B 随机选取 $b\xleftarrow{R}\{0,1\}$和 $r\xleftarrow{R}\{0,1\}^{80}$，采用 Step3 的方法计算 m_b 的环签密 $c=(c_1,c_2)$提交给 A。

Step5 A 输出对 b 的猜测 b'。

Step6 B 重复上述过程(即 Step1－Step5)$poly(\lambda)/\varepsilon$ 次并统计 A 成功猜测 b 的次数。如果统计结果表明 A 成功猜测出 b 的优势是不可忽略的，那么 B 判定 $v=e_0\prod_{i=1}^{k}u_i$，反之，B 判定 $v=f\prod_{i=1}^{k}u_i$。

分析：B 在构造密钥的过程中，选取的 $d_i\xleftarrow{R}\{0,1\}^n,0\leqslant i\leqslant k$向量长度很短，所以 d_iu_i 与 u_i 的分布基本相同。B 计算给定明文环签密过程中，采用 v 替换了 $e_0\prod_{i=1}^{k}u_i$，如果 $v=e_0\prod_{i=1}^{k}u_i$ 成立，上述过程就是正确的环签密过程，按照假定，A 将以不可忽略的优势 ε 判断出 b 值。反之，如果 $v=f\prod_{i=1}^{k}u_i$，那么 B 提供给 A 的密文近似为随机分布的数据，并不是一组合法的签密文，所以 A 正确判断出 b 的优势是可忽略的。B 调用 A 的攻击过程 $poly(\lambda)/\varepsilon$ 次并统计 A 成功的次数，就能够以不可阻挡的概率区分 $v=e_0\prod_{i=1}^{k}u_i$ 或 $v=f\prod_{i=1}^{k}u_i$，也就求解了 GDDH 问题。

综上，B 调用 A 攻击过程 $poly(\lambda)/\varepsilon$ 次能够以接近 1 的概率求解 GDDH 问题，B 的运行时间可以用 $1/\varepsilon$，λ 和 A 运行时间的多项式表示。如果 GDDH 是难解的，那么上述环签密广播公钥方案随机预言模型下消息保密性满足语义安全。

4.2.2 环签密的不可伪造性证明

定理 3 对于随机预言模型的环签密广播公钥方案，如果存在概率多项式时间敌手 F 能够在时间 τ 内(最多进行 q_H 次 Hash 函数询问，q_s 次环签密询问)以不可忽略的优势 ε 赢得对给定明文 M^* 伪造签密的攻击游戏，则存在一个算法 B 能够解决 GDDH 问题，成功的概率接近 1，运行时间可以用 $1/\varepsilon$，λ 和 F 运行时间 τ 的多项式表示。如果多级 Diffie-Hellman 判定问题(GDDH)难解，那么上述签密方案具有不可伪造性。

证明：给定 GDDH 的问题实例$((y,\{x_i\}_i,p_{sk}),u_0,\cdots,$

$u_k, v)$，要求判定 $v=e_0\prod_{i=1}^{k}u_i$ 或者 $v=f\prod_{i=1}^{k}u_i$。

Step1　B 作为模拟者根据给定 GDDH 的问题实例生成发送环成员和接收环成员的密钥过程以及 F 询问随机预言机 q_H 次的过程与定理 2 证明相同。B 把公共参数 $params=(n,q,y,\{x_i\}_i,s)$ 和所有公钥输入给敌手 F。假定要求攻击者伪造明文 M^* 的环签密（M^* 包含了实际明文和填充的随机串）。

Step2　F 向 B 输入一组信息 $m_i(i=1,\cdots,q_s)$ 进行环签密询问，B 对信息环签密并发送给 F，环签密的方法与定理 2 证明相同。

Step3　伪造。敌手 F 生成 M^* 的一个签密 $c^*=(c_1^*, c_2^*)$。

Step4　B 验证签密是否合法。首先采用解签密算法验证 c_1^* 的合法性，然后判断 $ext(params, p_{\pi}, h(M^*)v)\oplus M^*$ 与 c_2^* 是否相等，如果两者都满足，那么环签密伪造成功，反之伪造不成功。

Step5　B 重复上述过程（即 Step1－Step4）$poly(\lambda)/\varepsilon$ 次并统计 F 成功伪造签密的次数。如果统计结果表明 F 成功伪造签密的优势是不可忽略的，则 B 判定 $v=e_0\prod_{i=1}^{k}u_i$，反之，B 判定 $v=f\prod_{i=1}^{k}u_i$。

分析：与定理 2 证明类似，B 采用 v 替换 $e_0\prod_{i=1}^{k}u_i$ 来计算环签密。如果 $v=e_0\prod_{i=1}^{k}u_i$ 成立，生成的是合法的环签密，而且步骤 4 也能正确验证环签密的合法性。这种情况下 F 将以不可忽略的优势 ε 成功伪造签密。反之，如果 $v=f\prod_{i=1}^{k}u_i$，那么 B 提供给 F 的密文近似为随机分布的数据，并不是一个合法的签密，所以 F 成功伪造签密的优势是可忽略的，B 在步骤 4 验证签密合法的概率可以忽略。B 调用 F 的攻击过程 $poly(\lambda)/\varepsilon$ 次并统计 F 成功的次数，就能够以不可阻挡的概率区分 $v=e_0\prod_{i=1}^{k}u_i$ 或 $v=f\prod_{i=1}^{k}u_i$，也就求解了 GDDH 问题。

综上，如果 F 能够以不可忽略的优势 ε 伪造给定信息 M^* 的签密，那么 B 能以不可阻挡的概率解决给定 GDDH 问题。所以，如果 GDDH 问题难解，那么签密具有不可伪造性。

4.2.3　签密具有匿名性

定理 4　签密者具有发送匿名性，真实签密者能成功证明其他成员是签密者的优势是可忽略的。

证明：从环签密算法可以看出，任何环用户生成消息 m 的环签密 $c=(c_1,c_2)$ 中 c_2 是分布均匀的比特串，而任何环签密的 $c_1\in h(m\|r)\prod_{i\in[|S|]}(sd_{i,0}\cdot sd_{i,1})+I$，这样有效地隐藏了环用户的身份，所以签密者具有发送匿名性。同理，真实签密者无法证明其他成员是签密者。

结束语　本文基于多线性映射构建了环签密广播方案。接收者在得到明文后可以验证发送者的发送环成员身份，但无法知道确切的发送者。基于 GDDH 问题假设，在随机预言模型下，我们证明了方案满足信息保密性、签密在选择消息攻击下的不可伪造性和发送者匿名性。尽管基于多线性映射已经构造出多种密码原语[15,16]，但这些密码原语效率都较低。为此，我们下一步将研究如何减小多线性映射公钥的尺寸，节约存储空间，使方案更具实用性，以及研究设计基于多线性映射的新的密码原语。

参 考 文 献

[1] Rivest R L, Shamir A, Tauman Y. How to leak a secret[C]// Advances in Cryptology-ASIACRYPT 2001. Berlin: Springer-Verlag, 2001: 552-565

[2] Zheng Yu-liang. Digital signcryption or how to achieve cost (signature&encryption)<<cost(signature)+cost(encryption) [C]// Advances in Cryptology-CRYPTO'97. Berlin: Springer-Verlag, 1997: 165-179

[3] 孙华，王爱民，郑雪峰. 标准模型下可证安全的基于身份的门限环签密方案[J]. 计算机科学，2013，40(5)：131-135

[4] Huang X Y, Zhang F T, Wu W. Identity-based ring signcryption scheme[J]. Tien Tzu Hsueh Pao/Acta Electronica Sinica, 2006, 34(2): 263-266

[5] Selvi S S D, Vivek S S, Rangan C P. On the security of identity based ring signcryption schemes [C]// Information Security, 12th International Conference(ISC 2009). Berlin: Springer-Verlag, 2009: 310-325

[6] Deng Lun-zhi, Liu Cheng-lian, Wang Xiang-bin. An Improved Identity-Based Ring Signcryption Scheme[J]. Information Security Journal: A Global Perspective, 2013, 22(1): 46-54

[7] Sharmila D S S, Sree V S, Pandu R C. Identity based ring signcryption schemes revisited[J]. Journal of Math-for-Industry, 2011, 3(A3): 33-46

[8] Zhang Bo, Xu Qiu-liang. An ID-based anonymous signcryption scheme for multiple receivers secure in the standard model: Advances in Computer Science and Information Technology[C]// AST/UCMA/ISA/ACN 2010 Conferences. Berlin: Springer-Verlag, 2010: 15-27

[9] 鲁力，胡磊. 基于 Weil 对的多接收者公钥加密方案[J]. 软件学报，2008，19(8)：2159-2166

[10] 庞辽军，高璐，裴庆祺，等. 基于身份公平的匿名多接收者签密方案[J]. 通信学报，2013，34(8)：161-168

[11] 李慧贤，陈绪宝，巨龙飞，等. 改进的多接收者签密方案[J]. 计算机研究与发展，2013，50(7)：1418-1425

[12] Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM J Comput, 1997, 26(5): 1484-1509

[13] Boneh D, Silverberg A. Applications of multilinear forms to cryptography[J]. Contemporary Mathematics, 2003, 324: 71-90

[14] Garg S, Gentry C, Halevi S. Candidate multilinear maps from ideal lattices [C]// Advances in Cryptology (EUROCRYPT 2013). Berlin: Springer-Verlag, 2013: 1-17

[15] Coron J-S, de Lepoint T, Tibouchi M. Practical multilinear maps over the integers [C]// Advances in Cryptology (CRYPTO 2013). Berlin: Springer-Verlag, 2013: 476-493

[16] Hohenberger S, Sahai A, Waters B. Full domain hash from (leveled) multilinear maps and identity-based aggregate signatures [EB/OL]. 2013-7. http://eprint.iacr.org/2013/434.pdf