软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2018,29(2):456−472 [doi: 10.13328/j.cnki.jos.005258]

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

一种混合多变量签名方案*

李慧贤[1], 王凌云[1], 庞辽军[2]

[1](西北工业大学 计算机学院,陕西 西安 710072)

[2](综合业务网国家重点实验室(西安电子科技大学),陕西 西安 710071)

通讯作者: 李慧贤, E-mail: lihuixian@nwpu.edu.cn

摘 要: RGB(red-green-blue)方案是一个可以抵抗已知代数攻击的混合多变量签名方案,但是和其他多变量公钥方案一样,它也具有公钥量大的缺点.针对RGB方案这一不足,采用循环公钥的思想对RGB方案进行优化,提出了一个新的方案——CyclicRGB混合多变量签名方案.与RGB方案相比,CyclicRGB方案在降低公钥大小的同时,还具有更快的签名验证过程.通过该方案和RGB方案的实验比较,结果表明:该方案的公钥大小约为RGB方案公钥大小的40%,CyclicRGB方案签名验证所需时间为RGB方案签名验证所需时间的60%.

关键词: 多变量公钥密码系统;混合多变量签名方案;Red-Green-Blue多项式;循环公钥

中图法分类号: TP309

中文引用格式: 李慧贤,王凌云,庞辽军.一种混合多变量签名方案.软件学报,2018,29(2):456−472. http://www.jos.org.cn/1000-9825/5258.htm

英文引用格式: Li HX, Wang LY, Pang LJ. Mixed multivariate signature scheme. Ruan Jian Xue Bao/Journal of Software, 2018, 29(2):456−472 (in Chinese). http://www.jos.org.cn/1000-9825/5258.htm

Mixed Multivariate Signature Scheme

LI Hui-Xian[1], WANG Ling-Yun[1], PANG Liao-Jun[2]

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

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

Abstract: RGB is one of the mixed multivariate signature schemes. It can resist the current known algebraic attacks against multivariate schemes. However, similar to other MPKC (multivariate public key cryptosystem) schemes, it suffers from large public key size. In order to reduce the public key size of RGB, this study extends the idea of cyclic public key to the RGB signature scheme and proposes a new scheme—CyclicRGB mixed multivariate signature system. In comparison with the original scheme, the new scheme has smaller public key size, and it is also possible to speed up the verification process. Furthermore, experiments demonstrate that it is feasible to reduce the size of public key. The public key size of the new scheme is about 40% of that for the RGB scheme. The time required for the signature verification in CyclicRGB scheme is about 60% of the time required for the RGB scheme.

Key words: multivariate public key cryptosystem (MPKC); mixed multivariate signature scheme; red-green-blue polynomial; cyclic public key

自量子计算机被提出以来,量子计算机在最近几十年里已经成为世界各国战略竞争的焦点.各国研究人员对量子计算机的研究从未间断.与此同时,研究人员也一直在寻找未知的算法,这些算法可以应用于量子计算

* 基金项目: 国家自然科学基金(61103178, 61473214); 陕西省自然科学基础研究计划(2015JM6294, 2016JM6002); 中央高校基本科研业务费专项资金(3102015JSJ0003)

Foundation item: National Natural Science Foundation of China (61103178, 61473214); Natural Science Basic Research Plan in Shaanxi Province of China (2015JM6294, 2016JM6002); Fundamental Research Funds for the Central Universities (3102015JSJ0003)

收稿时间: 2016-10-03; 修改时间: 2016-11-17; 采用时间: 2017-01-19; jos在线出版时间: 2017-03-24

CNKI网络优先出版: 2017-03-24 17:09:35, http://kns.cnki.net/kcms/detail/11.2560.TP.20170324.1709.013.html

机,并且利用量子计算机来解决当前传统计算机所不能解决的困难问题.这一类算法也被称为量子算法.例如,目前已经提出解决 RSA 所基于的数学困难问题的量子算法[1].这预示着,如果量子计算机研制成功,将严重威胁目前网络数字通信中数据的安全性.因此,与之对应的抗量子密码算法的研究成为目前密码学学者关注的一个热点,目的是为将来量子计算机时代提供安全的密码算法.

多变量公钥密码体制、基于格的密码算法、基于编码问题的密码算法以及基于 Hash 的密码算法都是抗量子密码学的研究热点.多变量公钥密码体制作为抗量子密码算法的研究热点之一,其主要优点体现在多变量公钥密码体制的计算效率高、功耗小,可以应用于存储和计算能力有限的设备上.

最早的多变量公钥密码方案在 1988 年由 Matsumoto 等人提出,即著名的 Matsumoto-Imai(MI)[2]加密方案.这是多变量公钥密码发展史上一个具有里程碑意义的方案.1995 年,Patarin 利用线性化方程攻破了 MI 多变量加密方案,并且 Patarin 等人在 MI 体制的基础上又提出了隐藏域方程(hidden field equation,简称 HFE)多变量公钥密码体制[3],HFE 密码体制是将 MI 体制中的多变量单变元单项式方程变成单变元多项式方程.然而,HFE 方案很快被 Kipnis 等人[4]攻破.随后,更多的多变量加密方案和多变量签名方案相继被提出.

在随后的方案中,密码学研究者主要通过以下几种方法来提出新方案:一种是通过寻找和设计新的、安全的中心映射来构造新的多变量公钥密码方案;另一种方法是通过一定的手段对已有方案进行改进,比如,比较有名的改进多变量方案的方法有扰动方法、加方法、减方法;亦或将已有的几个方案结合起来形成新的方案,使之达到抵抗已知攻击的目的.随后出现的有名的多变量方案包括油醋(oil and vinegar,简称 OV)[5]、不平衡油醋(unbalanced oil and vinegar,简称 UOV)[6]多变量签名方案、SFLASH[7].在 UOV 的基础上,Ding 等人[8]设计了彩虹(rainbow)签名方案.采用扰动方法、加方法、减方法对已有方案进行改进得到的方案有 PMI(perturbed Matsumoto-Imai)[9],PMI$^+$(perturbed Matsumoto-Imai-plus)[10]等.然而,绝大多数多变量公钥密码方案已被证明是不安全的.目前,新的安全的多变量方案有 ZHFE(Zhuang-Zi hidden field equation)[11]、ABC(simple matrix encryption scheme)[12]、cubic-ABC(cubic simple matrix encryption scheme)[13]、SRP(square Rainbow plus)[14]方案.ZHFE 方案是使用两个高阶的 HFE 多项式来构造中心映射.ABC,cubic-ABC 方案是通过构造新的中心映射结构来设计多变量加密方案,其优点是高效的加密和解密算法.SRP 方案是 Yasuda 等人提出的一个新的多变量加密方案,SRP 就是将 Square 加密方案、Rainbow 签名方案以及 Plus 方法这 3 种多变量密码技术相结合而形成的一个多变量加密方案.这几个方案在目前来说是安全的,它们的安全性还需进一步分析.

一方面,密码学研究者不断设计更安全、更实用的多变量公钥加密、签名体制;另一方面,虽然与传统的公钥密码体制相比,多变量公钥密码体制具有计算效率高的优点,但同时,它也存在密钥量大的缺点.因此,对于多变量公钥密码体制的研究还体现在如何设计密钥量小的公钥密码方案,使得多变量公钥密码方案密钥的存储空间尽可能地小.

Petzoldt 等人提出了 CyclicRainbow 方案[15],主要方法是在 Rainbow 的公钥麦考利矩阵中插入特殊的循环结构,使得公钥大小降低了 62%.更重要的是,CyclicRainbow 的签名验证与 Rainbow 方案的签名验证相比,可以减少 30%的模乘运算,这意味着可以提高签名验证效率.Petzoldt 等人[16]在 2013 年的后量子密码会议上详细说明了采用循环公钥的 UOV 和 Rainbow 方案.2016 年,Duong 等人又将循环公钥的思想运用于 SRP 方案,提出了 CyclicSRP[17],使得 SRP 的公钥大小降低了 54%.同时,在加密过程中减少了 50%的模乘运算.更重要的是,这样的结构并没有削弱原始 SRP 的安全性.文献[17]指出:通过这样的方法,使得 CyclicSRP 成为第 1 个减小公钥大小的多变量公钥加密方案.这种特殊结构的 SRP 方案的公钥仅为 ABC,ZHFE 方案公钥的一半,同时,加密过程所需的时间也仅为其他方案的一半.

2015 年,Shen 等人[18]提出一个混合类型的多变量公钥签名 RGB(red-green-blue)方案.RGB 方案是在 UOV 方案的基础上提出的.RGB 方案最大的特点就是它属于一个混合类型的多变量签名方案,在其中心映射中,消息值与其他变量可以更好地混合在一起,因此,该方案生成的签名难以伪造.RGB 方案在选择合适参数的情况下,可以抵抗已知的代数攻击.与其他方案(如 UOV,Quartz,Rainbow,RSA-1024)相比,RGB 方案在安全性和效率方面性能更佳.RGB 适合于计算能力有限的设备,例如 RFID 设备、掌上设备、无线传感器网络等.但是和其他多变

量方案一样,RGB 方案也存在公钥量大的缺点.

本文通过分析 RGB 方案的结构特性,将循环公钥的方法与 RGB 混合多变量公钥密码方案相结合,提出了本文方案.通过采用循环公钥的思想,利用 RGB 中心映射系数矩阵和公钥系数矩阵的关系,构造了 CyclicRGB 多变量混合签名方案.新方案 CyclicRGB 的公钥具有更加紧凑的结构,从而降低 RGB 的公钥大小.进一步地,利用公钥的特殊结构来提高 RGB 签名方案在进行签名验证时的效率.本文方案将更有利于 RGB 方案在低端设备上的应用.

本文第 1 节介绍多变量公钥签名方案,包括 UOV 方案和 RGB 混合多变量签名方案.第 2 节在分析 RGB 混合多变量签名方案的基础上具体设计 CyclicRGB 混合多变量签名方案中的签名验证算法.同时介绍 CyclicRGB 签名方案,并对方案的正确性予以证明.第 3 节对方案的安全性予以说明.第 4 节对 RGB 方案和 CyclicRGB 方案的公钥大小和验证签名的效率进行比较.第 5 节采用 C++对 RGB 方案和 CyclicRGB 方案进行实现,并对签名验证的实验结果进行比较.第 6 节总结全文.

1 RGB 混合多变量签名方案介绍及其分析

多变量公钥密码方案是后量子密码时代保证网络数字信息安全通信的重要手段之一.多变量公钥密码基于的数学困难问题是解有限域上多变量多项式方程组的困难性(MQ 问题)以及 IP(isomorphism of polynomial)问题.其基本思想是:选择有限域的一个可逆多变量多项式方程组 F 作为中心映射(这里的可逆是指可以通过某种方式较容易地求出前像值);同时,选择两个可逆仿射变换 L_1,L_2 来隐藏中心映射的结构.这种结构下,多变量公钥密码方案的私钥为(F,L_1,L_2),公钥为 $P=L_2\circ F\circ L_1$.在私钥未知、公钥已知的情况下,想通过公钥求解私钥是不可行的.

使用多变量公钥密码方案对消息 m 的哈希值 $h=H(m)$进行签名时,使用私钥分别进行如下计算: $u=L_2^{-1}(h)$, $v=F^{-1}(u)$,最后得到消息签名值 $x=L_1^{-1}(v)$.

1.1 UOV多变量签名方案

创建可逆的多变量二次系统的一种方法就是采用不平衡油醋方案(UOV).UOV 方案由 Kipnis 等人[6]提出,UOV 方案是对 OV 方案的扩展.UOV 公钥形式为 $P=F\circ L$.

假设 K 为有限域,o 和 v 为两个正整数,并且 $v>o,n=o+v$.设整数集合为 $V=\{1,2,...,v\}$,$O=\{v+1,v+2,...,n\}$.在 n 个变量 $x_1,x_2,...,x_n$ 中,前 v 个变量 $x_1,...,x_v$ 称为醋变量,后 o 个变量 $x_{v+1},...,x_n$ 称为油变量.UOV 中心映射是由 o 个多变量多项式方程构成的方程组 $F=(f^{(1)}(x_1,...,x_n),...,f^{(o)}(x_1,...,x_n))$,其中,每个多变量多项式方程形式如下:

$$f^{(k)}(x_1,...,x_n)=\sum_{i=1}^{v}\sum_{j=1}^{v}a_{ij}x_ix_j+\sum_{i=1}^{v}\sum_{j=1}^{o}b_{ij}x_ix_{v+j}+\sum_{i=1}^{o}c_ix_{v+i}+\sum_{j=1}^{v}d_jx_j+e(k=1,...,o).$$

映射 $F=(f^{(1)}(x_1,...,x_n),...,f^{(o)}(x_1,...,x_n))$可以通过以下方式求逆:首先,随机选择 v 个醋变量值 $x_1,...,x_v$,将这 v 个值代入多变量多项式方程组,得到关于 o 个变量 $x_{v+1},...,x_n$ 的线性方程组;通过高斯消元可以求出这 o 个变量的值,如果无解,则重新选择醋变量来求解线性方程组,直至求得 o 个变量的值;再将随机选择的 v 个醋变量的值和求得的 o 个油变量的值代入 L 的逆,即得到消息的 UOV 签名.

1.2 RGB混合多变量签名方案的介绍及其分析

1.2.1 RGB 多变量公钥签名方案

Shen 等人[18]在 UOV 方案的基础上提出一个混合多变量签名方案 RGB.该方案中,首先定义了一个特殊结构的多项式,称为三色多项式(RGB 多项式).与 UOV 方案相比,RGB 多项式包括 3 种类型的变量,并且每个 RGB 多变量多项式方程的二次项系数组成的相关对称矩阵的表示形式与比色法中的三色模型结构相似,因此将这种特殊结构的多项式称为 RGB 多项式,这就是 RGB 多项式名称的由来.

具体地,设 K 是特征值为 p 的有限域,并且阶为 $q=p^k$(k 是一个正整数).RGB 中有 3 类变量(分别标记为 *Red* 变量、*Green* 变量、*Blue* 变量),设正整数 r,g,b 分别表示 *Red* 变量、*Green* 变量、*Blue* 变量的个数,并且整数

$n=r+g+b$.3 类变量具体表示为 *Red* 变量 $x_1,...,x_r$,*Green* 变量 $x_{r+1},...,x_{r+g}$,*Blue* 变量 $x_{r+g+1},...,x_n$,并且 $S_1:K^r\to K^r$, $S_2:K^{g+b}\to K^{g+b}$,$S_3:K^g\to K^g$ 均为在有限域上随机选取的可逆仿射变换.定义 RGB 多变量二次多项式方程:

$$f^{(k)}(x_1,...,x_n)=\sum_{i=1}^{r}\sum_{j=1}^{r}A_{ij}^{(k)}x_ix_j+\sum_{i=1}^{r}\sum_{j=1}^{g}B_{ij}^{(k)}x_ix_{r+j}+\sum_{i=1}^{r}\sum_{j=1}^{b}C_{ij}^{(k)}x_ix_{r+g+j}+\sum_{i=1}^{g}\sum_{j=1}^{b}D_{ij}^{(k)}x_{r+i}x_{r+g+j}+$$

$$\sum_{i=1}^{b}\sum_{j=1}^{b}E_{ij}^{(k)}x_{r+g+i}x_{r+g+j}+\sum_{i=1}^{r}G_i^{(k)}x_r+\sum_{i=1}^{g}H_i^{(k)}x_{r+i}+\sum_{i=1}^{b}L_i^{(k)}x_{r+g+i}+R^{(k)}(k=1,...,g),$$

其中, $A_{ij}^{(k)},B_{ij}^{(k)},C_{ij}^{(k)},D_{ij}^{(k)},E_{ij}^{(k)},G_i^{(k)},H_i^{(k)},L_i^{(k)},R^{(k)}\in K$. RGB 混合多变量公钥密码方案的中心映射 $F:K^n\to K^g$ 为

$$F(x_1,...,x_n)=(f^{(1)}(x_1,...,x_n),\ldots,f^{(g)}(x_1,...,x_n)).$$

RGB 多变量签名方案由 3 种多项式时间的算法组成,即密钥生成算法 Kg、签名生成算法 Sign 以及签名验证算法 Verify.

密钥生成算法 Kg.

这一多项式时间算法主要是系统根据适当的安全参数为用户生成相应的 RGB 方案的公钥和私钥.RGB 混合多变量方案的公钥为 $P=S_3\circ F\circ(S_1\times S_2)$,对应的私钥为$(S_1,S_2,S_3,F)$.然后,用户使用自己的私钥对消息进行签名.

签名生成算法 Sign.

生成的签名为 $X\leftarrow Sign(S_1,S_2,F,M)$.

该算法输入签名者的私钥和待签名消息值 $M=(x_1,...,x_r)$,生成对应的消息签名.签名算法需要执行以下步骤,生成消息的签名 $X=(x_{r+1},...,x_n)$.

(1) 计算 $\tilde{M}=S_1(M)=S_1(x_1,...,x_r)=(x_1',...,x_r')$.

(2) 随机选择 $(x_{r+g+1}',...,x_n')\in K^b$ 的值,将这些随机选择的值与步骤(1)中的 $\tilde{M}$ 值代入中心映射 F,得到一个线性方程组.该方程组是由关于 g 个未知量 $(x_{r+1}',...,x_{r+g}')\in K^g$ 的 g 个线性方程组成的,具有如下形式:

$$\begin{cases}f^{(1)}(x_1',...,x_r',x_{r+1}',...,x_{r+g}',x_{r+g+1}',...,x_n')=0\\ \vdots\\ f^{(g)}(x_1',...,x_r',x_{r+1}',...,x_{r+g}',x_{r+g+1}',...,x_n')=0\end{cases}.$$

对这个线性方程组采用高斯消元,可以求得方程组的解,从而求得 g 个变量 $(x_{r+1}',...,x_{r+g}')$ 的值.需要注意的是,如果线性方程组无解,则重新选择 $(x_{r+g+1}',...,x_n')\in K^b$ 的值,重复步骤(2)中的运算,直到可以求出 g 个变量 $(x_{r+1}',...,x_{r+g}')$ 的值为止.

(3) 结合步骤(2)求得的 g 个变量 $(x_{r+1}',...,x_{r+g}')$, 假设 $X'=(x_{r+1}',...,x_{r+g}',x_{r+g+1}',...,x_n')$, 然后计算:

$$X=S_2^{-1}(X')=S_2^{-1}(x_{r+1}',...,x_{r+g}',x_{r+g+1}',...,x_n')=(x_{r+1},...,x_{r+g},x_{r+g+1},...,x_n).$$

最后,X 即为消息 M 的签名值.

签名验证算法 Verify.

对于签名的验证,验证者为了验证签名是否有效,执行签名验证算法 Verify.验证者使用签名者的公钥对接收到的消息 M 以及消息的签名 X 进行验证:

$$P(M,X)=P(x_1,...,x_r,x_{r+1},...,x_{r+g},x_{r+g+1},...,x_n)\stackrel{?}{=}0.$$

如果上式成立,则认为 X 是对消息 M 的合法签名,并且验证算法返回 1;否则,签名无效,输出⊥.

1.2.2 对 RGB 签名方案的分析

RGB 方案是 UOV 方案的改进,如果把 RGB 混合多变量多项式方程中的 *Red* 变量和 *Blue* 变量看作醋变量,把 *Green* 变量看作油变量,RGB 多变量多项式就是 OV 多项式.在这一部分,我们简单分析 RGB 方案公钥结构、公钥大小以及签名验证的具体计算过程,这些分析是进一步设计 CyclicRGB 方案的基础.

RGB 方案的公钥是以下 3 部分的复合.

$$P=S_3\circ F\circ(S_1\times S_2),$$

其中, $(S_1 \times S_2)(\bar{x}_1,...,\bar{x}_r,\bar{x}_{r+1},...,\bar{x}_n)$ 表示两线性映射运算结果的级联,即 $S_1(\bar{x}_1,...,\bar{x}_r) \| S_2(\bar{x}_{r+1},...,\bar{x}_n)$. 我们假设矩阵 S_0 由 $S_1 \times S_2$ 组成且表示为 $S_0 = \begin{pmatrix} S_1 & 0 \\ 0 & S_2 \end{pmatrix}$, $(S_1 \times S_2)(\bar{x}_1,...,\bar{x}_r,\bar{x}_{r+1},...,\bar{x}_n)$ 就可表示为 $S_0(\bar{x}_1,...,\bar{x}_r,\bar{x}_{r+1},...,\bar{x}_n)$. 并且由于 $S_1 \times S_2$ 为可逆仿射变换,那么 S_0 的逆也可以通过 $S_1 \times S_2$ 的逆运算求得.因此,RGB 的公钥可以表示为

$$P=S_3 \circ F \circ S_0.$$

上述结构形式与多变量方案的一般模型相同,接下来,我们利用上述公钥组织结构中的符号做进一步的分析与设计.具体地,可以将 RGB 多变量公钥的每个多项式表示成如下形式:

$$p^{(k)}(x_1,...,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(k)} x_i x_j + \sum_{i=1}^{n} q_i^{(k)} x_r + r^{(k)} (k = 1,...,g).$$

RGB 多变量签名方案的公钥由关于 $n(n=r+g+b)$个变量的 g 个多变量多项式方程组成,公钥的大小为

$$g \cdot \frac{(n+2)(n+1)}{2}.$$

假设 RGB 多变量公钥的系数矩阵为 Pm,在验证消息 $M=(x_1,...,x_r)$和给定消息的签名 $X=(x_{r+1},...,x_{r+g},x_{r+g+1},\ldots,x_n)$是否有效时,需要将消息值和签名值进行一定的运算,然后将这些值代入 RGB 多变量公钥中进行验证.具体步骤如下.

- 首先,计算向量值 $ver = (x_1^2,...,x_r x_n,...,x_n^2,x_1,...,x_r,x_{r+1},...,x_{r+g},x_{r+g+1},...,x_n,1)$.
- 然后,将向量 vec 与签名者的公钥进行计算:

$$P(M,X) = Pm \times vec^T = \begin{pmatrix} Pm[1] \cdot vec^T \\ Pm[2] \cdot vec^T \\ \vdots \\ Pm[g] \cdot vec^T \end{pmatrix},$$

其中,$Pm[i]$是公钥系数矩阵的第 i 行向量.

- 最后,根据上述公式的计算结果判定签名的有效性.

从上述分析可以看出,Rainbow 方案的公钥与多变量公钥密码方案的一般模型相吻合.接下来对公钥方程 $P=S_3 \circ F \circ S_0$ 进行优化,设计具有部分循环结构的 RGB 公钥来降低公钥大小;再由于采用循环结构,可以进一步优化其签名验证的计算步骤,降低签名验证的步骤中模乘运算量,从而提高签名验证效率.

2 CyclicRGB 混合多变量签名方案

2.1 RGB多变量方案的结构特性

本节我们将描述如何构建具有部分循环公钥的 RGB 混合多变量公钥签名方案.下面我们分析在给定公钥方程组以及可逆仿射变换 S_3 和 S_0 的情况下,可以确定中心映射 F.

首先分析 RGB 方案中公钥和私钥的关系.通过第 1.2.2 节中的分析,RGB 多变量公钥可以表示为 3 部分的复合运算:

$$P=S_3 \circ F \circ S_0.$$

中心映射 F 是关于 n 个变量的 g 个二次方程组成的方程组.对于 F 中每个多变量二次方程,假设 Fm 为该方程组的系数矩阵,并且用 $FM[k](k=1,...,g)$表示方程组中对应第 k 个方程的系数矩阵,假设 $Q=F \circ S_0$.由于 F 为多变量二次多项式方程组,S_0 为可逆仿射变换.所以 Q 也为多变量二次多项式方程组,并且 Q 中方程的系数可以通过以下方程求得:

$$Qm = F \circ S_0 = \begin{cases} S_0^T \times FM[1] \times S_0 \\ \vdots \\ S_0^T \times FM[g] \times S_0 \end{cases},$$

其中,Qm 为 Q 的系数矩阵,×表示矩阵相乘,S_0^T 表示矩阵 S_0 的转置矩阵.

Petzoldt 等人在文献[15,16]中指出:在给定可逆仿射变换 S_0 和 Q 的情况下,Q 和 F 的系数矩阵之间存在线性关系 $Qm=Fm\times A$(其中,矩阵 A 是关于 S_0 元素的一个矩阵).但是文献[15,16]中没有给出具体的证明,本文附录 A 将给出详细的说明.

公钥方程组为 $P=S_3\circ F\circ S_0=S_3\circ Q$,公钥 P 的系数矩阵为可逆仿射变换 S_3 与 Q 的系数矩阵的乘积:

$$Pm=S_3\times Qm \tag{1}$$

因此,如果给定公钥方程组的系数矩阵以及可逆仿射变换 S_3 和 S_0,就可以通过下面的计算,达到确定中心映射 F 的目的:

$$Qm=S_3^{-1}\times Pm, Fm=Qm\times A^{-1} \tag{2}$$

2.2 CyclicRGB签名验证算法的设计

首先,RGB 公钥的每个多项式方程可以写成如下结构:

$$p^{(k)}(x_1,\ldots,x_n)=\sum_{i=1}^{r}\sum_{j=i}^{n}\alpha_{ij}^{(k)}x_ix_j+\sum_{i=r+1}^{r+g}\sum_{j=i}^{n}\beta_{ij}^{(k)}x_ix_j+\sum_{i=r+g+1}^{n}\sum_{j=i}^{n}\gamma_{ij}^{(k)}x_ix_j+\sum_{i=1}^{n}\eta_i^{(k)}x_r+\lambda^{(k)}(k=1,\ldots,g),$$

其中,$\alpha_{ij}^{(k)}$ 表示 *Red* 变量分别与 *Red* 变量、*Green* 变量、*Blue* 变量相乘构成的二次项的系数,$\beta_{ij}^{(k)}$ 表示 *Green* 变量分别与 *Green* 变量、*Blue* 变量相乘构成的二次项的系数,$\gamma_{ij}^{(k)}$ 表示 *Blue* 变量与 *Blue* 变量相乘构成的二次项的系数,$\eta_i^{(k)}$ 为一次项系数,$\lambda^{(k)}$为常数项.将上述多变量方程的系数表示为上三角矩阵形式如下:

$$PM[k]=\begin{pmatrix}
\alpha_{11}^{(k)} & \alpha_{12}^{(k)} & \alpha_{13}^{(k)} & \alpha_{14}^{(k)} & \cdots & \alpha_{1r}^{(k)} & \alpha_{1(r+1)}^{(k)} & \cdots & \alpha_{1(r+g-1)}^{(k)} & \alpha_{1(r+g)}^{(k)} & \alpha_{1(r+g+1)}^{(k)} & \cdots & \alpha_{1n}^{(k)} & \eta_1^{(k)}\\
0 & \alpha_{22}^{(k)} & \alpha_{23}^{(k)} & \alpha_{24}^{(k)} & \cdots & \alpha_{2r}^{(k)} & \alpha_{2(r+1)}^{(k)} & \cdots & \alpha_{2(r+g-1)}^{(k)} & \alpha_{2(r+g)}^{(k)} & \alpha_{2(r+g+1)}^{(k)} & \cdots & \alpha_{2n}^{(k)} & \eta_2^{(k)}\\
0 & 0 & \alpha_{33}^{(k)} & \alpha_{34}^{(k)} & \cdots & \alpha_{3r}^{(k)} & \alpha_{3(r+1)}^{(k)} & \cdots & \alpha_{3(r+g-1)}^{(k)} & \alpha_{3(r+g)}^{(k)} & \alpha_{3(r+g+1)}^{(k)} & \cdots & \alpha_{3n}^{(k)} & \eta_3^{(k)}\\
0 & 0 & 0 & \alpha_{44}^{(k)} & \cdots & \alpha_{4r}^{(k)} & \alpha_{4(r+1)}^{(k)} & \cdots & \alpha_{4(r+g-1)}^{(k)} & \alpha_{4(r+g)}^{(k)} & \alpha_{4(r+g+1)}^{(k)} & \cdots & \alpha_{4n}^{(k)} & \eta_4^{(k)}\\
 & \vdots & & \ddots & & \vdots & & & & & & & \vdots & \vdots\\
0 & 0 & 0 & 0 & \cdots & \alpha_{rr}^{(k)} & \alpha_{r(r+1)}^{(k)} & \cdots & \alpha_{r(r+g-1)}^{(k)} & \alpha_{r(r+g)}^{(k)} & \alpha_{r(r+g+1)}^{(k)} & \cdots & \alpha_{rn}^{(k)} & \eta_r^{(k)}\\
0 & 0 & 0 & 0 & \cdots & 0 & \beta_{(r+1)(r+1)}^{(k)} & \cdots & \beta_{(r+1)(r+g-1)}^{(k)} & \beta_{(r+1)(r+g)}^{(k)} & \beta_{(r+1)(r+g+1)}^{(k)} & \cdots & \beta_{(r+1)n}^{(k)} & \eta_{r+1}^{(k)}\\
 & \vdots & & & & & & & \ddots & & \vdots & & \vdots & \vdots\\
0 & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & \beta_{(r+g)(r+g)}^{(k)} & \beta_{(r+g)(r+g+1)}^{(k)} & \cdots & \beta_{(r+g)n}^{(k)} & \eta_{r+g}^{(k)}\\
0 & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \gamma_{(r+g+1)(r+g+1)}^{(k)} & \cdots & \gamma_{(r+g+1)n}^{(k)} & \eta_{r+g+1}^{(k)}\\
 & \vdots & & & & & & & & & & \ddots & & \vdots\\
0 & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & \gamma_{nn}^{(k)} & \eta_n^{(k)}\\
0 & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & \lambda^{(k)}
\end{pmatrix}.$$

消息 $M=(x_1,\ldots,x_r)$和消息的签名为 $X=(x_{r+1},\ldots,x_{r+g},x_{r+g+1},\ldots,x_n)$,定义由它们组成的扩展向量为

$$ver=(x_1,\ldots,x_r,x_{r+1},\ldots,x_{r+g},x_{r+g+1},\ldots,x_n,1).$$

在验证 RGB 签名时,可以用公钥方程的系数矩阵、扩展向量 ver 进行以下运算:

$$ver\cdot PM[k]\cdot ver^T\stackrel{?}{=}0(k=1,\ldots,g).$$

如果采用上述形式对 RGB 方案进行签名验证,我们就可以设计具有部分循环公钥的 RGB 多变量混合签名方案.假设公钥方程 P 的系数矩阵表示为 $Pm=(V|U|W|C)$,Pm 为 $g\times\frac{(n+1)(n+2)}{2}$ 的矩阵.我们将 Pm 分为 4 部分:矩阵 V,U,W 是由公钥方程组的 g 个方程中二次项系数构成的矩阵,C 是由公钥方程组 g 个方程中的一次项系数和常数项组成的矩阵.具体地,Pm 中的第 k 行向量 $Pm[k]=(V[k]|U[k]|W[k]|C[k])$是由第 k 个公钥方程的系数组成.对应地,$V[k]$为矩阵 V 的第 k 行,它表示第 k 个公钥方程中由 *Red* 变量构成的相关二次项的系数,对应 $PM[k]$矩阵

中的系数 $\alpha_{ij}^{(k)}$. $W[k]$表示第 k 个公钥方程中由 *Blue* 变量与 *Blue* 变量相乘组成的二次项的系数,即对应 $PM[k]$矩阵中的系数 $\gamma_{ij}^{(k)}$. 同理,$U[k]$表示第 k 个公钥方程中由 *Green* 变量分别与 *Green* 变量、*Blue* 变量相乘组成的二次项的系数,对应系数矩阵 $PM[k]$中的 $\beta_{ij}^{(k)}$. $C[k]$由系数矩阵 $PM[k]$中的一次项系数 $\eta_i^{(k)}$ 和常数项$\lambda^{(k)}$组成.我们对于每个公钥方程的系数 $V[k]$,$W[k]$使用特殊结构的序列生成.

首先,假设随机选择的向量 $v\in K^{r(n+g+b+1)/2}$,$w\in K^{b(b+1)/2}$,v,w 的维度分别为公钥系数矩阵行向量 $Pm[k]$的子向量 $V[k]$中元素的个数、子向量 $W[k]$中元素的个数.将 v,w 这两个向量通过特定运算插入到 RGB 的公钥多项式中,使得 V,W 分别是由 v,w 生成的结构化的矩阵:

$$V[k]=\Delta^{k-1}(v),W[k]=\Delta^{k-1}(w)(k=1,\ldots,g) \tag{3}$$

其中,$\Delta^k(v)$表示将 v 向量循环右移 k 个位置.因此,矩阵 V 的第 k 行由向量 v 循环右移 k–1 个元素得到.采用类似的方法,可以用向量 w 生成矩阵 W.如果采用上述方法生成公钥方程的对应系数,那么在存储公钥时只需要存储向量 v,w 就可以恢复公钥系数矩阵的 V,W 部分,从而降低公钥的大小.

在 CyclicRGB 中,由于公钥方程中部分系数采用上述特殊结构生成,使得 CyclicRGB 多变量公钥多项式方程组中相邻两个方程的系数存在特定关系,具体如下:

$$\alpha_{ij}^{(k)}=\alpha_{i(j-1)}^{(k-1)},i=1,\ldots,r,\ j=i+1,\ldots,n,k=2,\ldots,g,$$

$$\gamma_{ij}^{(k)}=\gamma_{i(j-1)}^{(k-1)},i=r+g+1,\ldots,n,\ j=i+1,\ldots,n,k=2,\ldots,g.$$

因此,利用上述系数间的关系,在验证消息签名时,RGB 多变量公钥多项式方程中第 k 个方程的计算和第 k–1 个方程的计算存在以下关系:

$$(ver_1,\ldots,ver_i)\begin{pmatrix}\alpha_{1j}^{(k)}\\ \alpha_{2j}^{(k)}\\ \vdots\\ \alpha_{ij}^{(k)}\end{pmatrix}=(x_1,\ldots,x_i)\begin{pmatrix}\alpha_{1(j-1)}^{(k-1)}\\ \alpha_{2(j-1)}^{(k-1)}\\ \vdots\\ \alpha_{i(j-1)}^{(k-1)}\end{pmatrix},\ \begin{matrix}i=1,\ldots,r\\ j=i+1,\ldots n,\\ k=2,\ldots,g\end{matrix}$$

$$(ver_{r+g+1},\ldots,ver_{r+g+i})\begin{pmatrix}\gamma_{(r+g+1)j}^{(k)}\\ \gamma_{(r+g+2)j}^{(k)}\\ \vdots\\ \gamma_{(r+g+i)j}^{(k)}\end{pmatrix}=(x_{r+g+1},\ldots,x_{r+g+i})\begin{pmatrix}\gamma_{(r+g+1)(j-1)}^{(k-1)}\\ \gamma_{(r+g+2)(j-1)}^{(k-1)}\\ \vdots\\ \gamma_{(r+g+i)(j-1)}^{(k-1)}\end{pmatrix},\ \begin{matrix}i=1,\ldots,b\\ j=i+1,\ldots n.\\ k=2,\ldots,g\end{matrix}$$

与此同时,利用上述事实,在给定消息值和签名值后,我们可以设计 CyclicRGB 方案签名验证步骤来提高 RGB 多变量公钥签名的验证效率.下面给出验证签名算法.

1. 首先,将由消息值和签名值组成的扩展向量 ver 代入公钥方程组中的第 1 个多项式方程,即计算 $ver\cdot PM[1]\cdot ver^T$:先将扩展向量 ver 与第 1 个公钥方程的系数矩阵 $PM[1]$相乘,得到乘积 $ver\cdot PM[1]$,这部分的运算又可以具体地分为以下几部分的运算.

a) 我们假设用 sum_i 表示 ver 与 $PM[1]$中第 i 列相乘得到的结果,那么 ver 分别与 $PM[1]$中第 n 列、第 n+1 列相乘得到的结果分别为

$$sum_n=\sum_{j=1}^{r}\alpha_{jn}^{(1)}ver_j+\sum_{j=r+1}^{r+g}\beta_{jn}^{(1)}ver_j+\sum_{j=r+g+1}^{n}\gamma_{jn}^{(1)}ver_j,$$

$$sum_{n+1}=\sum_{j=1}^{n}\eta_j^{(1)}ver_j+\lambda^{(1)}.$$

b) 将系数矩阵 $PM[1]$中由特殊向量 v,w 生成的系数与扩展向量 ver 对应元素进行运算,并保存运算结果.

首先,系数矩阵 $PM[1]$的第 i 列($1\leqslant i\leqslant n-1$)的前 r 行元素分别与 ver 对应元素进行运算,假设运算结果用 $col1_i$ 进行保存:

$$col1_i=\sum_{j=1}^{\min(i,r)}\alpha_{ji}^{(1)}ver_j.$$

将这部分运算结果用 $col1_i$ 进行保存,目的是利用第 2 个公钥方程系数矩阵中的系数 $\alpha_{ij}^{(2)}$ 与第 1 个公钥方程系数矩阵中的系数 $\alpha_{i(j-1)}^{(1)}$ 之间的关系,在将扩展向量 ver 代入第 2 个公钥方程计算时,在第 1 个公钥方程计算

过程中得到的 $col1_i$ 可直接用于第 2 个公钥方程签名验证的计算,从而节省计算量.

将系数矩阵 $PM[1]$的第 i 列($r+g+1\leqslant i\leqslant n-1$)中的第 j 行($r+g+1\leqslant j\leqslant i$)元素分别与 ver 对应元素进行运算,假设运算结果用 $col2_i$ 进行保存:

$$col2_i=\sum_{j=r+g+1}^{i}\gamma_{ji}^{(1)}ver_j.$$

与保存 $col1_i$ 的目的类似,保存第 1 个公钥方程在签名验证时的部分中间计算结果 $col2_i$,也主要是利用第 2 个公钥方程的系数矩阵中的系数 $\gamma_{ij}^{(2)}$ 与第 1 个公钥方程系数矩阵中的系数 $\gamma_{i(j-1)}^{(1)}$ 的关系,在将 ver 代入第 2 个公钥方程计算时可以直接利用这部分的计算结果,节省签名验证计算过程的模乘运算.

c) 结合步骤 b)中的计算结果,求 ver 分别与系数矩阵 $PM[1]$的前 $n-1$ 列相乘得到的结果,并将运算结果保存在 sum_i 中.那么有:

- ver 与系数矩阵 $PM[1]$的第 i 列(其中,$1\leqslant i\leqslant r$)运算结果:$sum_i=col1_i$;
- ver 与系数矩阵 $PM[1]$的第 i 列(其中 $r+1\leqslant i\leqslant r+g$)运算结果: $sum_i=col1_i+\sum_{j=r+1}^{i}\beta_{ji}^{(1)}ver_j$;
- ver 与系数矩阵 $PM[1]$的第 i 列(其中,$r+g+1\leqslant i\leqslant n-1$)运算结果: $sum_i=col1_i+col2_i+\sum_{j=r+1}^{r+g}\beta_{ji}^{(1)}ver_j$.

将上述步骤中的计算结果 $sum_i(i=1,...,n+1)$与扩展向量 ver 的转置相乘,得到消息值、签名值代入第 1 个公钥方程的计算结果 h_1:

$$h_1=ver\cdot PM[1]\cdot ver^T=\sum_{j=1}^{n+1}sum_j ver_j.$$

2. 这一步中,将消息和签名的扩展向量 ver 代入公钥方程组的其他多项式方程中进行计算.下面说明将 ver 代入第 $f(2\leqslant f\leqslant g)$个公钥方程的计算流程.

a) 由于 $PM[f]$中第 $n+1$ 列不具有特殊结构,ver 与第 $n+1$ 列相乘的运算与步骤 1 中相同,均为

$$sum_{n+1}=\sum_{j=1}^{n}\eta_j^{(f)}ver_j+\lambda^{(f)}.$$

对于 $PM[f]$中第 n 列,有 $\alpha_{in}^{(f)}=\alpha_{i(n-1)}^{(f-1)}(i=1,...,r),\gamma_{in}^{(f)}=\gamma_{i(n-1)}^{(f-1)}(i=r+g+1,...,n-1)$,因此,可以利用上一个方程的中间计算结果 $col1_{n-1},col2_{n-1}$ 来求 sum_n:

$$(ver_1,...,ver_r)\begin{pmatrix}\alpha_{1n}^{(f)}\\ \vdots\\ \alpha_{rn}^{(f)}\end{pmatrix}=(ver_1,...,ver_r)\begin{pmatrix}\alpha_{1(n-1)}^{(f-1)}\\ \vdots\\ \alpha_{r(n-1)}^{(f-1)}\end{pmatrix}=col1_{n-1},$$

$$(ver_{r+g+1},...,ver_{n-1})\begin{pmatrix}\gamma_{(r+g+1)n}^{(f)}\\ \vdots\\ \gamma_{(n-1)n}^{(f)}\end{pmatrix}=(ver_{r+g+1},...,ver_{n-1})\begin{pmatrix}\gamma_{(r+g+1)(n-1)}^{(f-1)}\\ \vdots\\ \gamma_{(n-1)(n-1)}^{(f-1)}\end{pmatrix}=col2_{n-1},$$

$$sum_n=col1_{n-1}+\sum_{j=r+1}^{r+g}\beta_{jn}^{(f)}ver_j+col2_{n-1}+\gamma_{nn}^{(f)}ver_n.$$

b) 计算第 f 个公钥方程系数矩阵 $PM[f]$中前 $n-1$ 列与扩展向量 ver 相乘的结果.在计算的过程中,利用上一个公钥方程计算时保存的结果 $col1_i,col2_i$.同时,对 $col1_i,col2_i$ 的值进行更新.

具体地,首先,依次从第 $n-1$ 列到第 $r+g+2$ 列进行计算,同样与步骤 a)中类似,由于公钥方程系数的特殊结构,可以得到以下方程:

$$col1_i=col1_{i-1},$$

$$col2_i=col2_{i-1}+\gamma_{ii}^{(f)}ver_i,$$

$$sum_i=col1_i+col2_i+\sum_{j=r+1}^{r+g}\beta_{ji}^{(f)}ver_j(i=r+g+2,...,n-1).$$

对于第 $r+g+1$ 列,$col2_{r+g+1}$ 需进行新的计算求得 $col2_{r+g+1}=\gamma_{(r+g+1)(r+g+1)}^{(f)}ver_{r+g+1}$. $col1_{r+g+1}$ 仍可利用上一个多项式方程的计算结果:$col1_{r+g+1}=col1_{r+g}$.因此, $sum_{r+g+1}=col1_{r+g+1}+col2_{r+g+1}+\sum_{j=r+1}^{r+g}\beta_{j(r+g+1)}^{(f)}ver_j$.

接下来,将第 $r+g$ 列~第 $r+1$ 列分别与扩展向量 ver 相乘:

$$col1_i = col1_{i-1},$$

$$sum_i = col1_i + \sum_{j=r+1}^{i} \beta_{ji}^{(f)} ver_j (i = r+1,...,r+g).$$

将第 r 列到第 2 列分别与扩展向量 ver 相乘,有:

$$col1_i = col1_{i-1} + \alpha_{ii}^{(f)} ver_i,$$

$$sum_i = col1_i (i = 2,...,r).$$

最后,对于第 1 列的计算有:

$$col1_1 = \alpha_{11}^{(f)} ver_1,$$

$$sum_1 = col1_1.$$

将上述步骤中计算结果 $sum_i(i=1,...,n+1)$与扩展向量 ver 的转置相乘,得到消息值、签名值代入第 f 个公钥方程的计算结果:

$$h_f = ver \cdot PM[f] \cdot ver^T = \sum_{j=1}^{n+1} sum_j ver_j.$$

3. 最后,验证这 g 个计算结果:

$$h_f=0, \forall f \in \{1,\ldots,g\}.$$

如果上式成立,则签名有效;否则,签名无效.

附录 B 的算法 B1 给出签名验证的伪代码,对应上述验证流程.

2.3 CyclicRGB混合多变量签名方案

在具体分析了 CyclicRGB 的签名验证之后,我们就可以设计 CyclicRGB 混合多变量签名方案.CyclicRGB 混合多变量签名方案由 3 种多项式时间算法组成,分别为密钥生成算法、签名生成算法和签名验证算法.

密钥生成算法. (Key Generation):$(pk,sk) \leftarrow KeyGeneration(1^{\lambda})$.

输入:安全参数λ.

输出:用户的公钥 pk、私钥 sk.

RGB 公钥方程组中的每个方程的系数矩阵以及中心映射 F 的每个方程的系数矩阵都可以表示为$(n+1)\times(n+1)$的上三角矩阵形式,均为第 2.2 节中 $PM[k]$矩阵表示形式.不同的是,在中心映射 F 的每一个方程的系数矩阵中,表示 *Green* 变量与 *Green* 变量乘积的二次项系数全部为 0;相反地,对应的公钥方程的系数矩阵中,表示 *Green* 变量与 *Green* 变量乘积的二次项系数需要由私钥求得.

在密钥生成过程中,首先生成公钥方程组系数矩阵中的二次项系数部分,利用公钥方程组的系数矩阵与中心映射的系数矩阵的线性关系,求得中心映射系数矩阵的二次项系数.当中心映射系数矩阵的二次项系数确定以后,再为中心映射 F 随机选取一次项系数和常数项系数.最后,由中心映射 F 和可逆仿射变换 S_0,S_3 确定最终公钥方程.具体密钥生成过程如下.

1. 随机选择两个向量 $v \in K^{r(n+g+b+1)/2}, w \in K^{b(b+1)/2}$.随机选择 3 个可逆仿射变换 $S_1:K^r \to K^r, S_2:K^{g+b} \to K^{g+b}, S_3:K^g \to K^g$.通过第 1.2.2 节中的方法,由 S_1,S_2 求出 S_0.并使用附录 A 中的方法,由 S_0 求得矩阵 A.
2. 使用 v,w,按照公式(3)循环右移生成每个公钥方程系数矩阵中对应的二次项系数.即生成公钥系数矩阵 $Pm=(V|U|W|C)$中的矩阵 V 和 W.
3. 公钥系数矩阵中除了 V 和 W 表示二次项系数之外,U 也表示二次项系数,并且 U 表示 *Green* 变量分别与 *Green* 变量、*Blue* 变量构成的二次项乘积的系数矩阵.对于这一部分系数,我们将 U 中表示 *Green* 变量与 *Green* 变量组成的二次项的系数全部设置为 0.公钥系数矩阵中的这一部分值最终由中心映射的一次项系数和常数项系数确定以后求得.
4. 另外,为 U 中表示 *Green* 变量与 *Blue* 变量组成的二次项的系数随机选取值.
5. 通过上述步骤,可以确定公钥方程组中二次项的系数,即 V,U,W.根据公钥方程组的系数矩阵与中心映射系数矩阵的线性关系,通过公式(2)可以得到中心映射 F 的二次项系数.
6. 随机选择中心映射 F 的一次项系数以及常数项系数,根据 $P=S_3 \circ F \circ S_0$ 求得公钥方程的系数矩阵 $Pm=$

$(V|U|W|C)$.CyclicRGB 方案的公钥为 $pk=(v,U,w,C)$,私钥 $sk=(S_1,S_2,S_3,F)$.

7. 输出密钥对(pk,sk).

签名生成算法. (Signature Generation):$X\leftarrow Sign(S_1,S_2,F,M)$.

该算法由签名者执行,签名者根据自己的私钥(S_1,S_2,F)、消息值 $M=(x_1,...,x_r)$.生成相应的消息签名 $X\in K^{g+b}$.具体签名过程如下.

1. 计算 $\tilde{M}=S_1(M)=S_1(x_1,...,x_r)=(x'_1,...,x'_r)$.

2. 随机选择 Blue 变量 $(x'_{r+g+1},...,x'_n)\in K^b$,将这些随机选择的 Blue 变量值与 $\tilde{M}$ 一同代入中心映射 F.使用高斯消元求解未知量 $(x'_{r+1},...,x'_{r+g})\in K^g$ 的值,具有如下形式:

$$\begin{cases} f^{(1)}(x'_1,...,x'_r,x'_{r+1},...,x'_{r+g},x'_{r+g+1},...,x'_n)=0 \\ \vdots \\ f^{(g)}(x'_1,...,x'_r,x'_{r+1},...,x'_{r+g},x'_{r+g+1},...,x'_n)=0 \end{cases}.$$

如果上述线性方程组无解,则重复步骤(2)中的运算过程,即重新选择 *Blue* 变量的值进行运算,直到可以求出 g 个变量 $(x'_{r+1},...,x'_{r+g})$ 的值为止.

3. 将步骤 2 中随机选择的 *Blue* 变量 $(x'_{r+g+1},...,x'_n)\in K^b$ 和步骤 2 中求得的 g 个变量 $(x'_{r+1},...,x'_{r+g})$ 代入 S_2 的逆中,

$$X=S_2^{-1}(X')=S_2^{-1}(x'_{r+1},...,x'_{r+g},x'_{r+g+1},...,x'_n)=(x_{r+1},...,x_{r+g},x_{r+g+1},...,x_n).$$

最后,运算结果 X 即对消息 M 的签名.

签名验证算法. (Signature Verification):{ACCEPT,⊥}←*Verify*(*pk*,*M*,*X*).

该算法由验证者执行,来验证消息签名是否有效.

输入:验证者的公钥 *pk*,消息值 M 以及消息的签名 X.

输出:如果签名有效,返回 ACCEPT;否则签名无效,返回⊥.

为了验证 $X=(x_{r+1},...,x_{r+g},x_{r+g+1},\ldots,x_n)\in F^{g+b}$ 是否为 $M=(x_1,...,x_r)\in F^r$ 的签名,使用第 2.2 节中的验证算法(即算法 B1)对消息和签名进行验证:

$$pk(M,X)=pk(x_1,\ldots,x_r,x_{r+1},...,x_{r+g},x_{r+g+1},\ldots,x_n)=0.$$

若采用算法 B1 的验证结果为“ACCEPT”,则消息签名合法,算法返回 1;否则,消息的签名不合法,算法返回⊥.

2.4 方案正确性证明

CyclicRGB 混合签名方案的正确性可以通过下式加以证明.

$$\begin{aligned} pk(M,X)=0 &\Leftrightarrow S_3\circ F\circ S_0(M,X)=0 \\ &\Leftrightarrow F(S_1(M),S_2(X))=0 \\ &\Leftrightarrow F(\tilde{M},S_2\circ S_2^{-1}(X'))=0 \\ &\Leftrightarrow F(\tilde{M},X')=0 \\ &\Leftrightarrow F(x'_1,...,x'_r,x'_{r+1},...,x'_{r+g},x'_{r+g+1},...,x'_n)=0. \end{aligned}$$

如果消息值和签名值合法,上式一定成立.

3 安全性分析及参数的选择

目前,针对多变量公钥密码方案存在大量的攻击方法.这些攻击方法包括有强力搜索、直接攻击、最小秩攻击、高秩攻击、Patarin 线性关系(线性化方程攻击)、差分攻击、分离“油”“醋”变量攻击、Rainbow Band Seperation 攻击等.下面就 CyclicRGB 方案的安全性进行分析.

由于原始的 RGB 方案是 UOV 方案的改进,本文方案 CyclicRGB 基于原始的 RGB 方案进行改进,在降低

RGB 方案的公钥大小的同时,提高签名验证效率.原始 RGB 方案与本文 CyclicRGB 方案都不是多层次结构的方案,这就使得作用于 Rainbow,CyclicRainbow 等多层次复杂结构方案的攻击方法不能用来攻击 RGB,CyclicRGB 方案.这些攻击方法包括秩攻击、Rainbow Band Separation 等攻击.

本文主要采用循环公钥的方法来降低 RGB 多变量混合签名方案的公钥量.与原方案 RGB 相比,改进后的方案并没有降低原方案的安全性,因此,不能作用于 RGB 方案的攻击方法也不能作用于 CyclicRGB 方案.同时,新方案的安全性也和 RGB 方案一样,可以通过选择合适的参数来抵抗代数攻击.

3.1 穷举攻击

穷举攻击可以作用于任何的密码方案.穷举攻击的方式有两种:一种是穷举密钥空间,通过找到一个等价密钥确定该方法是否可行,这种攻击方法的时间复杂度较高;另一种是对明文直接攻击,通过找到有效的明文的概率来确定这种穷举攻击方法是否可行.明文长度大于 64 比特的方案可以抵抗对明文的穷举攻击.因此,当有限域选择 $GF(2^8)$时,在 CyclicRGB 中表示 *Red* 变量的个数 r,当 $r\geqslant 8$ 时,方案可以抵抗穷举攻击.

3.2 分离油、醋变量的攻击

分离油醋攻击是 Kipnis 等人[19]在 1998 年对 OV 体制进行攻击时提出的攻击方法.文献[6]中指出:当醋变量个数多余油变量个数或者两者个数近似相等时,油醋分离攻击方法的时间复杂度为 $q^{(v-o)-1}\cdot o^4$(其中,v,o 分别为 OV 体制中醋变量的个数和油变量的个数).RGB,CyclicRGB 多变量混合签名方案实质上是对 UOV 签名方案的改进,前两者的中心映射结构与 UOV 方案相同.当将 RGB,CyclicRGB 方案中心映射中的 *Red* 变量和 *Blue* 变量看作醋变量、*Green* 变量看作油变量时,分离油醋攻击方法对于 CyclicRGB 方案的攻击复杂度为 $q^{r+b-g-1}\cdot o^4$.当有限域选择 $GF(2^8)$时,只要 $r+g-b\geqslant 14$,CyclicRGB 的安全级别就将大于 2^{100}.

3.3 Patarin线性关系攻击

Patarin 线性关系攻击最初是针对 MI 多变量公钥密码方案提出的,Patarin 线性攻击方法是对公钥多项式方程进行等价变形,试图使用足够多的明文和密文对得到关于明文变量和密文变量(或者公钥多项式)间的线性关系,最后,攻击者利用这个线性关系达到攻破方案的目的.但是文献[18]中指出,RGB 方案的中心映射不是双射的.因此,线性化方程的攻击方法不使用 RGB;同理,Patarin 线性攻击也不适用于 CyclicRGB.

4 CyclicRGB 与 RGB 公钥大小及签名验证效率的比较

RGB 混合多变量签名方案的公钥大小为

$$g\frac{(n+1)(n+2)}{2}=g\times\frac{r(n+g+b+1)}{2}+g\times\frac{g(2b+g+1)}{2}+g\times\frac{b(b+1)}{2}+g\times(n+1) \tag{4}$$

CyclicRGB 混合多变量签名方案的公钥由向量 v,w 和矩阵 U,C 构成,因此,CyclicRGB 混合多变量签名方案的公钥大小为

$$\frac{r(n+g+b+1)}{2}+\frac{b(b+1)}{2}+g\left[\frac{g(2b+g+1)}{2}+n+1\right]=\frac{r(n+g+b+1)}{2}+g\times\frac{g(2b+g+1)}{2}+\frac{b(b+1)}{2}+g\times(n+1) \tag{5}$$

用公式(4)减去公式(5)得到 $(g-1)\times\frac{r(n+g+b+1)+b(b+1)}{2}$.因此,RGB 的公钥大小比 CyclicRGB 的公钥大 $(g-1)\times\frac{r(n+g+b+1)+b(b+1)}{2}$ 个元素,即 CyclicRGB 方案的公钥大小小于原始方案的公钥大小.

文献[18]对 RGB 方案各部分的时间复杂度进行了分析(包括公钥、私钥的生成,签名的生成和验证),其中包括有限域上的模加法和模乘法运算.但是,有限域上模乘运算的时间复杂度高于有限域上模加法运算的时间复杂度,因此,下面我们主要分析算法中有限域上模乘运算的复杂度.CyclicRGB 验证签名效率的提高主要通过第 2.2 节中签名验证算法得以体现,附录 B 中算法 B1 即为 CyclicRGB 签名验证的伪代码.下面我们就附录 B 中算法 B1 伪代码中用到的模乘运算的个数进行分析.

- 算法 B1 第 1 行~第 3 行需要执行的模乘运算为 $\frac{r(r+1)}{2}+r(g+b-1)$;
- 第 4 行~第 6 行需要执行的模乘运算为 $\frac{b(b-1)}{2}$;
- 第 11 行执行完第 7 行的循环体需要执行的模乘运算数为 $\frac{g(g+1)}{2}$;
- 第 13 行执行完第 7 行的循环体需要执行的模乘运算数为 $g(b-1)$;
- 第 15 行需要执行的模乘运算数为 n;
- 第 16 行需要执行的模乘运算数为 n;
- 第 17 行需要执行的模乘运算数为 $n+1$;
- 从算法 B1 的第 18 行开始的循环语句:
  - 第 19 行需要执行的模乘运算数为 n;
  - 第 20 行需要执行的模乘运算数为 $g+1$;
  - 执行第 21 行的 for 循环中,第 23 行需要执行的模乘运算数为$(b-2)$;
  - 执行第 21 行的 for 循环中,第 24 行需要执行的模乘运算数为 $g(b-2)$;
  - 第 27 行需要执行的模乘运算数为 1;
  - 第 28 行需要执行的模乘运算数为 g;
  - 执行第 29 行的 for 循环中,第 31 行总共执行的模乘运算数为 $\frac{g(g+1)}{2}$;
  - 执行第 33 行的 for 循环中,第 34 行总共执行的模乘运算数为 $r-1$;
  - 第 37 行需要执行的模乘运算数为 1;
  - 第 39 行需要执行的模乘运算数为 $n+1$.

因此,CyclicRGB 混合多变量签名方案的签名验证总共需要执行模乘运算为

$$\frac{n(n+5)}{2}+1+(g-1)\left[\frac{(2b+g)(g+1)}{2}+r+2n+1\right];$$

RGB 混合签名方案在签名验证时所需要执行的模乘运算数为

$$\frac{n(n+1)}{2}+g\times\frac{(n+1)(n+2)-2}{2}.$$

如果有限域 K 选取 $GF(2^8)$,并且选择参数$(r,g,b)=(20,24,10)$,CyclicRGB 混合多变量签名方案在签名验证时所需要的模乘运算仅为 RGB 签名方案模乘运算的 45%.可以看出:CyclicRGB 方案比 RGB 方案签名验证时需要执行的模乘运算数少,验证签名时效率较高.

5 实 验

为了验证 CyclicRGB 签名方案的效率,我们使用 C++对 RGB 签名方案和 CyclicRGB 方案在两组参数情况下进行实现.实验结果见表 1.

实验对两种方案公钥大小、签名验证所消耗时间以及签名验证进行的有限域上的主要模运算时间进行统计.需要说明的是,其中,CyclicRGB 签名验证时间为两部分:括号中的时间主要为签密验证过程中有限域上模运算的总时间;括号外的时间为整个签名验证的时间,这个时间不仅包括签名验证过程中有限域上模运算的时间,还包括使用循环公钥恢复公钥方程对应系数矩阵的时间.在参数相同的情况下,RGB 与 CyclicRGB 所采用的消息、消息的长度以及得到的签名长度都是相同的.例如,在参数取有限域 $GF(2^8)$,$r=20$,$g=24$,$b=10$ 的实验中,消息的大小均为 20B,对消息的签名的大小也均为 34B.不同的是,在参数相同的情况下,我们可以看到,CyclicRGB 签名方案的验证效率高于 RGB 签名方案的验证效率.CyclicRGB 方案与 RGB 方案相比,采用部分循环公钥的方法来设计公钥时,CyclicRGB 方案在签名验证时所需时间约为 RGB 方案签名验证时间的 60%,本文方案可以达到

提高后者签名验证效率的目的.同时,CyclicRGB 方案的公钥大小不超过 RGB 方案公钥大小的 40%,达到了降低公钥大小的目的.

Table 1 Performance comparison of RGB and CyclicRGB

表 1 RGB 方案与 CyclicRGB 方案实现性能比较

方案	RGB(256,20,24,10)	CyclicRGB(256,20,24,10)	RGB(256,28,28,28)	CyclicRGB(256,28,28,28)
公钥大小(KB)	36.09	14.87	99.94	37.19
私钥大小(KB)	31.20	31.20	93.52	93.52
消息长度(B)	20	20	28	28
签名长度(B)	34	34	56	56
密钥生成(s)	10.990 6	10.878 1	46.571 9	46.107 8
签名时间(s)	0.137 6	0.135 9	0.359	0.375
签名验证时间(s)	0.077 8	0.047(0.031 6)	0.219	0.109(0.075 1)

6 结 论

在本文中,我们采用循环公钥的方法对 RGB 方案进行改进,设计了新的混合多变量签名方案——CyclicRGB 方案,并且具体设计了 CyclicRGB 签名验证算法.新的混合多变量签名方案在签名验证时所需要的时间为原始的 RGB 方案签名验证消耗时间的 60%,新方案的公钥大小也仅为 RGB 方案的 40%.我们也采用 C++对有限域 $GF(2^8)$上不同参数情况下的两种方案的签名效率进行了实验比较.实验结果表明:CyclicRGB 的签名方案在验证签名时,可以在很大程度上提高签名验证的效率.

References:

[1] Shor PW. Polynomial-Time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Review, 1999,41(2):303−332. [doi: 10.1137/S0036144598347011]

[2] Matsumoto T, Imai H. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In: Günther CG, ed. Proc. of the Workshop on the Theory and Application of of Cryptographic Techniques. Davos: Springer-Verlag, 1988. 419−453. [doi:10.1007/3-540-45961-8_39]

[3] Partarin J. Hidden field equations (HFE) and isomorphism of polynomial (IP): Two new families of asymmetric algorithms. In: Maurer U, ed. Proc. of the Advances in Cryptology—EUROCRYPT'96. LNCS 1070, Berlin, Heidelberg: Springer-Verlag, 1996. 33−48. [doi: 10.1007/3-540-68339-9_4]

[4] Kipnis A, Shamir A. Cryptanalysis of the HFE public key cryptosystem by relinearization. In: Wiener M, ed. Proc. of the Advances in Cryptology—CRYPTO'99. Springer-Verlag, 1999. 19−30. [doi:10.1007/3-540-48405-1_2]

[5] Ding J, Gower JE, Schmidt DS. Oil-Vinegar signature schemes. In: Ding J, Gower JE, Schmidt DS, eds. Proc. of the Multivariate Public Key Cryptosystems, Vol.25. Springer-Verlag, 2006. 63−97. [doi: 10.1007/978-0-387-36946-4_3]

[6] Kipnis A, Patarin J, Goubin L. Unbalanced oil and vinegar signature schemes. In: Stern J, ed. Proc. of the Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Prague: Springer-Verlag, 1999. 206−222. [doi: 10.1007/3-540-48910-X_15]

[7] Patarin J, Courtois N, Goubin L. Flash, a fast multivariate signature algorithm. In: Naccache D, ed. Proc. of the Cryptographers' Track at the RSA Conf. San Francisco: Springer-Verlag. 2001. 298−307. [doi: 10.1007/3-540-45353-9_22]

[8] Ding J, Schmidt D. Rainbow, a new multivariable polynomial signature scheme. In: Ioannidis J, ed. Proc. of the Int'l Conf. on Applied Cryptography and Network Security. New York: Springer-Verlag, 2005. 164−175. [doi: 10.1007/11496137_12]

[9] Ding J. A new variant of the Matsumoto-Imai cryptosystem through perturbation. In: Bao F, ed. Proc. of the Int'l Workshop on Public Key Cryptography. Singapore: Springer-Verlag, 2004. 305−318. [doi: 10.1007/978-3-540-24632-9_22]

[10] Ding J, Gower JE. Inoculating multivariate schemes against differential attacks. In: Yung M, ed. Proc. of the Int'l Workshop on Public Key Cryptography. New York: Springer-Verlag, 2006. 290−301. [doi: 10.1007/11745853_19]

[11] Porras J, Baena J, Ding J. ZHFE, a new multivariate public key encryption scheme. In: Mosca M, ed. Proc. of the Int'l Workshop on Post-Quantum Cryptography. Waterloo: Springer Int'l Publishing, 2014. 229−245. [doi: 10.1007/978-3-319-11659-4_14]

[12] Tao C, Diene A, Tang S, Ding J. Simple matrix scheme for encryption. Lecture Notes in Computer Science, 2013,7932:231−242.

[13] Ding J, Petzoldt A, Wang L. The cubic simple matrix encryption scheme. In: Mosca M, ed. Proc. of the Int'l Workshop on Post-Quantum Cryptography. Waterloo: Springer Int'l Publishing, 2014. 76–87. [doi: 10.1007/978-3-319-11659-4_5]

[14] Yasuda T, Sakurai K. A multivariate encryption scheme with rainbow. In: Qing SH, ed. Proc. of the Int'l Conf. on Information and Communications Security. Beijing: Springer Int'l Publishing, 2015. 236–251. [doi: 10.1007/978-3-319-29814-6_19]

[15] Petzoldt A, Bulygin S, Buchmann J. CyclicRainbow—A multivariate signature scheme with a partially cyclic public key. In: Gong G, ed. Proc. of the Int'l Conf. on Cryptology in India. Hyderabad: Springer-Verlag, 2010. 33–48. [doi: 10.1007/978-3-642-17401-8_4]

[16] Petzoldt A, Bulygin S, Buchmann J. Fast verification for improved versions of the UOV and rainbow signature schemes. In: Gaborit P, ed. Proc. of the Int'l Workshop on Post-Quantum Cryptography. Limoges: Springer-Verlag, 2013. 188–202. [doi: 10.1007/978-3-642-38616-9_13]

[17] Duong DH, Petzoldt A, Takagi T. Reducing the key size of the SRP encryption scheme. In: Liu JK, ed. Proc. of the Australasian Conf. on Information Security and Privacy. Melbourne: Springer Int'l Publishing, 2016. 427–434. [doi: 10.1007/978-3-319-40367-0_27]

[18] Shen W, Tang S. RGB, a mixed multivariate signature scheme. The Computer Journal, 2016,59(4):439–451. [doi: 10.1093/comjnl/bxv056]

[19] Kipnis A, Shamir A. Cryptanalysis of the oil and vinegar signature scheme. In: Krawczyk H, ed. Proc. of the Annual Int'l Cryptology Conf. Springer-Verlag, 1998. 257–266. [doi: 10.1007/BFb0055733]

附录 A

下面证明:在已知多变量二次多项式方程 Q 和可逆仿射变换 S_0 的情况下,Q 和 F 的系数矩阵之间存在线性关系.由本文第 2 节可知,

$$Qm = F \circ S_0 = \begin{cases} S_0^T \times FM[1] \times S_0 \\ \vdots \\ S_0^T \times FM[g] \times S_0 \end{cases}, \ Q = F \circ S_0.$$

这里假设 $S_0 = \begin{pmatrix} s_{11}, s_{12}, ..., s_{1n} \\ s_{21}, s_{22}, ..., s_{2n} \\ \vdots \\ s_{n1}, s_{n2}, ..., s_{nn} \end{pmatrix}, FM[k] = \begin{pmatrix} f_{11}^{(k)}, f_{12}^{(k)}, ..., f_{1n}^{(k)} \\ f_{21}^{(k)}, f_{22}^{(k)}, ..., f_{2n}^{(k)} \\ \vdots \\ f_{n1}^{(k)}, f_{n2}^{(k)}, ..., f_{nn}^{(k)} \end{pmatrix}$. 假设 $QM[k]$为 Q 中第 k 个方程的系数矩阵,则 $QM[k] = S_0^T \times FM[k] \times S_0$, 并且

$$\begin{aligned} QM[k] &= \begin{pmatrix} q_{11}^{(k)}, q_{12}^{(k)}, ..., q_{1n}^{(k)} \\ q_{21}^{(k)}, q_{22}^{(k)}, ..., q_{2n}^{(k)} \\ \vdots \\ q_{n1}^{(k)}, q_{n2}^{(k)}, ..., q_{nn}^{(k)} \end{pmatrix} \\ &= \begin{pmatrix} s_{11}, s_{12}, ..., s_{1n} \\ s_{21}, s_{22}, ..., s_{2n} \\ \vdots \\ s_{n1}, s_{n2}, ..., s_{nn} \end{pmatrix}^T \times \begin{pmatrix} f_{11}^{(k)}, f_{12}^{(k)}, ..., f_{1n}^{(k)} \\ f_{21}^{(k)}, f_{22}^{(k)}, ..., f_{2n}^{(k)} \\ \vdots \\ f_{n1}^{(k)}, f_{n2}^{(k)}, ..., f_{nn}^{(k)} \end{pmatrix} \times \begin{pmatrix} s_{11}, s_{12}, ..., s_{1n} \\ s_{21}, s_{22}, ..., s_{2n} \\ \vdots \\ s_{n1}, s_{n2}, ..., s_{nn} \end{pmatrix} \\ &= \begin{pmatrix} s_{11}, s_{21}, ..., s_{n1} \\ s_{12}, s_{22}, ..., s_{n2} \\ \vdots \\ s_{1n}, s_{2n}, ..., s_{nn} \end{pmatrix} \times \begin{pmatrix} f_{11}^{(k)}, f_{12}^{(k)}, ..., f_{1n}^{(k)} \\ f_{21}^{(k)}, f_{22}^{(k)}, ..., f_{2n}^{(k)} \\ \vdots \\ f_{n1}^{(k)}, f_{n2}^{(k)}, ..., f_{nn}^{(k)} \end{pmatrix} \times \begin{pmatrix} s_{11}, s_{12}, ..., s_{1n} \\ s_{21}, s_{22}, ..., s_{2n} \\ \vdots \\ s_{n1}, s_{n2}, ..., s_{nn} \end{pmatrix}. \end{aligned}$$

那么, $q_{ij}^{(k)}$ 为矩阵 $S_0^T \times FM[k]$ 乘积结果的第 i 行与 S_0 的第 j 列相乘的结果.S_0 第 j 列可以表示为 $(s_{1j}, s_{2j}, \ldots, s_{nj})^T$,

而矩阵 $S_0^T \times FM[k]$ 乘积结果的第 i 行第 c 列(c=1,...,n)的元素由 S_0^T 的第 i 行元素分别与 $FM[k]$的第 c 列对应元素乘积之和得到.又因为 S_0^T 为 S_0 的转置矩阵,因此, S_0^T 的第 i 行就为 S_0 的第 i 列,即$(s_{1i},s_{2i},\ldots,s_{ni})^T$.可以求得 $q_{ij}^{(k)}$ 为

$$
\begin{aligned}
q_{ij}^{(k)} &= (s_{1i},s_{2i},...,s_{ni})\times\begin{pmatrix} f_{11}^{(k)},f_{12}^{(k)},...,f_{1n}^{(k)} \\ f_{21}^{(k)},f_{22}^{(k)},...,f_{2n}^{(k)} \\ \vdots \\ f_{n1}^{(k)},f_{n2}^{(k)},...,f_{nn}^{(k)} \end{pmatrix}\times\begin{pmatrix} s_{1j} \\ s_{2j} \\ \vdots \\ s_{nj} \end{pmatrix} \\
&= \begin{pmatrix} s_{1i}f_{11}^{(k)}+s_{2i}f_{21}^{(k)}+...+s_{ni}f_{n1}^{(k)} \\ s_{1i}f_{12}^{(k)}+s_{2i}f_{22}^{(k)}+...+s_{ni}f_{n2}^{(k)} \\ \vdots \\ s_{1i}f_{1n}^{(k)}+s_{2i}f_{2n}^{(k)}+...+s_{ni}f_{nn}^{(k)} \end{pmatrix}^T\times\begin{pmatrix} s_{1j} \\ s_{2j} \\ \vdots \\ s_{nj} \end{pmatrix} \\
&= (s_{1i}s_{1j}f_{11}^{(k)}+s_{2i}s_{1j}f_{21}^{(k)}+...+s_{ni}s_{1j}f_{n1}^{(k)})+(s_{1i}s_{2j}f_{12}^{(k)}+s_{2i}s_{2j}f_{22}^{(k)}+...+s_{ni}s_{2j}f_{n2}^{(k)})+...+ \\
&\quad (s_{1i}s_{nj}f_{1n}^{(k)}+s_{2i}s_{nj}f_{2n}^{(k)}+...+s_{ni}s_{nj}f_{nn}^{(k)}) \\
&= \sum_{r=1}^{n}\sum_{c=1}^{n}s_{ri}s_{cj}f_{rc}^{(k)} \\
&= (f_{11}^{(k)},...,f_{1n}^{(k)},f_{21}^{(k)},...,f_{2n}^{(k)},...,f_{n1}^{(k)},...,f_{nn}^{(k)})\times(s_{1i}s_{1j},...,s_{1i}s_{nj},s_{2i}s_{1j},...,s_{2i}s_{nj},...,s_{ni}s_{1j},...,s_{ni}s_{nj})^T.
\end{aligned}
$$

因此,可以得到如下关系:

$$
\begin{aligned}
Qm &= \begin{pmatrix} q_{11}^{(1)}\ q_{12}^{(1)}...\ q_{1n}^{(1)}\ q_{21}^{(1)}...\ q_{2n}^{(1)}...\ q_{n1}^{(1)}...\ q_{nn}^{(1)} \\ \vdots \\ q_{11}^{(k)}\ q_{12}^{(k)}...\ q_{1n}^{(k)}\ q_{21}^{(k)}...\ q_{2n}^{(k)}...\ q_{n1}^{(k)}...\ q_{nn}^{(k)} \end{pmatrix} \\
&= \begin{pmatrix} f_{11}^{(1)}\ f_{12}^{(1)}...\ f_{1n}^{(1)}\ f_{21}^{(1)}...\ f_{2n}^{(1)}...\ f_{n1}^{(1)}...\ f_{nn}^{(1)} \\ \vdots \\ f_{11}^{(k)}\ f_{12}^{(k)}...\ f_{1n}^{(k)}\ f_{21}^{(k)}...\ f_{2n}^{(k)}...\ f_{n1}^{(k)}...\ f_{nn}^{(k)} \end{pmatrix}\times\begin{pmatrix} s_{11}s_{11}\ \ s_{11}s_{12}\cdots s_{11}s_{1n}\ \ s_{12}s_{11}\cdots s_{12}s_{1n}\cdots\ s_{1n}s_{11}\cdots s_{1n}s_{1n} \\ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots \\ s_{11}s_{n1}\ s_{11}s_{n2}\cdots s_{11}s_{nn}\ \ s_{12}s_{n1}\cdots s_{12}s_{nn}\cdots\ s_{1n}s_{n1}\cdots s_{1n}s_{nn} \\ s_{21}s_{11}\ s_{21}s_{12}\cdots s_{21}s_{1n}\ \ s_{22}s_{11}\cdots s_{22}s_{1n}\cdots\ s_{2n}s_{11}\cdots s_{2n}s_{1n} \\ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots \\ s_{21}s_{n1}\ s_{21}s_{n2}\cdots s_{21}s_{nn}\ \ s_{22}s_{n1}\cdots s_{22}s_{nn}\cdots\ s_{2n}s_{n1}\cdots s_{2n}s_{nn} \\ s_{n1}s_{11}\ s_{n1}s_{12}\cdots s_{n1}s_{1n}\ \ s_{n2}s_{11}\cdots s_{n2}s_{1n}\cdots\ s_{nn}s_{11}\cdots s_{nn}s_{1n} \\ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots \\ s_{n1}s_{n1}\ s_{n1}s_{n2}\cdots s_{n1}s_{nn}\ \ s_{n2}s_{n1}\cdots s_{n2}s_{nn}\cdots\ s_{nn}s_{n1}\cdots s_{nn}s_{nn} \end{pmatrix} \\
&= Fm\times A.
\end{aligned}
$$

多变量多项式方程组 Q 的系数矩阵和 F 的系数矩阵之间存在线性关系,即 Qm=Fm×A.这里,A 为关于 S_0 的元素的矩阵.

附录 B

- CyclicRGB 签名验证算法

算法 B1. CyclicRGB 签名的验证.

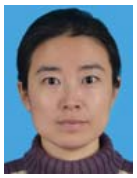
1. for i=1 to n−1 //将扩展向量 ver 代入公钥方程组中第 1 个多项式方程计算
2. $\quad col1_i = \sum_{j=1}^{\min(i,r)}\alpha_{ji}^{(1)}ver_j$
3. end for
4. for i=r+g+1 to n−1
5. $\quad col2_i = \sum_{j=r+g+1}^{i}\gamma_{ji}^{(1)}ver_j$
6. end for

7. for i=1 to n−1
8. if $i \leqslant r$
9. $sum_i = col1_i$
10. else if $i \leqslant r+g$
11. $sum_i = col1_i + \sum_{j=r+1}^{i} \beta_{ji}^{(1)} ver_j$
12. else
13. $sum_i = col1_i + col2_i + \sum_{j=r+1}^{r+g} \beta_{ji}^{(1)} ver_j$
14. end for
15. $sum_n = \sum_{j=1}^{r} \alpha_{jn}^{(1)} ver_j + \sum_{j=r+1}^{r+g} \beta_{jn}^{(1)} ver_j + \sum_{j=r+g+1}^{n} \gamma_{jn}^{(1)} ver_j$
16. $sum_{n+1} = \sum_{j=1}^{n} \eta_j^{(1)} ver_j + \lambda^{(1)}$
17. $h_1 = \sum_{j=1}^{n+1} sum_j ver_j$
18. for f=2 to g //将消息和签名的扩展向量 ver 代入公钥方程组中其余多项式方程计算
19. $sum_{n+1} = \sum_{j=1}^{n} \eta_j^{(f)} ver_j + \lambda^{(f)}$
20. $sum_n = col1_{n-1} + \sum_{j=r+1}^{r+g} \beta_{jn}^{(f)} ver_j + col2_{n-1} + \gamma_{nn}^{(f)} ver_n$
21. for i=n−1 to r+g+2
22. $col1_i = col1_{i-1}$
23. $col2_i = col2_{i-1} + \gamma_{ii}^{(f)} ver_i$
24. $sum_i = col1_i + col2_i + \sum_{j=r+1}^{r+g} \beta_{ji}^{(f)} ver_j$
25. end for
26. $col1_{r+g+1} = col1_{r+g}$
27. $col2_{r+g+1} = \gamma_{(r+g+1)(r+g+1)}^{(f)} ver_{r+g+1}$
28. $sum_{r+g+1} = col1_{r+g+1} + col2_{r+g+1} + \sum_{j=r+1}^{r+g} \beta_{j(r+g+1)}^{(f)} ver_j$
29. for i=r+g to r+1
30. $col1_i = col1_{i-1}$
31. $sum_i = col1_i + \sum_{j=r+1}^{i} \beta_{ji}^{(1)} ver_j$
32. end for
33. for i=r to 2
34. $col1_i = col1_{i-1} + \alpha_{ii}^{(f)} ver_i$
35. $sum_i = col1_i$
36. end for
37. $col1_1 = \alpha_{11}^{f} ver_1$
38. $sum_1 = col1_1$
39. $h_f = \sum_{j=1}^{n+1} sum_j ver_j$
40. end for
41. if h_f=0,$\forall f \in \{1,\ldots,g\}$
42. return “ACCEPT”
43. else
44. return “⊥”

45. end if

- 算法 B1 的工作流程

算法 B1 是将消息和签名构成的扩展向量 *ver* 代入循环结构公钥方程组的每个方程中进行计算的过程.其中,第 1 行~第 17 行是将 *ver* 代入公钥方程组中第 1 个方程的运算过程,即 $ver{\cdot}Pm[1]{\cdot}ver^T.sum$ 保存 $ver{\cdot}Pm[1]$的计算结果.同时,由于公钥方程组中方程系数矩阵 $PM[k]$的α,γ部分分别由向量 v,w 循环右移生成,因此在计算的过程中,将这部分的计算结果保存在 $col1_i,col2_i$ 中,用于下一步 $ver{\cdot}Pm[2]$的计算.算法的第 18 行~第 40 行是将 *ver* 代入剩下的 $g-1$ 个方程进行验证的过程.例如,当 $f=2$ 时,对多变量公钥方程组中的第 2 个方程进行计算.在这一步计算过程中,我们利用了上一步计算结果的 $col1_i,col2_i$,这样就可以节省一些模乘运算,提高验证效率.计算过程中,根据现有公钥方程系数矩阵对 $col1_i,col2_i$ 值进行更新,目的是用于下一个多项式方程的计算.CyclicRGB 方案的签名验证就是通过这些值在第 2 个~第 g 个公钥方程计算的过程中的重复利用来降低签名验证的计算代价,从而提高了签名验证效率.对于 $f=2$,算法第 18 行~第 38 行对应 $ver{\cdot}Pm[2]$的计算.第 39 行为公钥方程组中第 2 个方程的计算结果 $ver{\cdot}Pm[2]{\cdot}ver^T$.当 $f=2$ 到 $f=g$ 循环全部结束时,CyclicRGB 验证签名的计算结束.最后,第 41 行~第 45 行判断签名的有效性,并返回判断结果.



李慧贤(1977－),女,内蒙古乌兰浩特人,博士,副教授,主要研究领域为信息安全,多变量公钥密码,安全协议设计与分析.

庞辽军(1978－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为密码学,信息安全.

王凌云(1991－),男,硕士,主要研究领域为多变量公钥密码,安全协议设计与分析.