第41卷 第6A期 2014年6月
计 算 机 科 学
Computer Science
Vol. 41 No. 6A June 2014

多变量公钥密码体制扩展方案的改进

罗文俊 弓守朋
(重庆邮电大学计算机科学与技术学院 重庆 400065)

摘 要 多变量公钥密码扩展方案是一种新型的多变量公钥加密算法,它通过引入Tame变换,增加冗余变量来增强原始公钥加密体制的安全性。然而聂旭云等人声称该加密方案存在安全漏洞,并且给出了针对Tame变换中对角矩阵D的具体破解方法。针对方案中存在的漏洞,作者对原始算法中的矩阵D和冗余明文进行了两处改进,并证明了经过改进后的方案不存在聂旭云等人提出的安全漏洞,从而进一步增强了原始方案的安全性。

关键词 多变量公钥密码,Tame变换,改进
中图法分类号 TP309 **文献标识码** A

Improvement of Extended Multivariate Public Key Cryptosystem

LUO Wen-jun GONG Shou-peng
(Department of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)

Abstract Extended Multivariable Public Key Cryptosystem (EMC) is a new kind of public key cryptosystem. It introduces a transformation and increases some redundant variables to enhance security of original scheme. However, Xunyun Nie and his partners declare that there are some security vulnerabilities in EMC, and crack the diagonal matrix D in Tame. We changed the structure of matrix D and sequence of redundant variables. What's more, we also proved that there are no security vulnerabilities in EMC after the changing. The level of security of EMC is higher.

Keywords Multivariate public key cryptosystem, Transformation tame, Change

1 相关工作

多变量公钥密码是抗量子密码算法领域的研究热点,多变量公钥密码体制根据中心映射的不同大致可以分为3类:MI体制、HFE体制、油醋体制[1]。

虽然提出新的体制对研究者来说是一个巨大的诱惑,但关于新体制的研究成果近年来并不多见。所以多变量公钥密码领域的研究热点大多围绕怎样增强这3种体制的安全性展开,如对MI体制的内部扰动方法[2]、油醋体制中的Rainbow签名体制[3]、对HFE体制的内部扰动方法[4]。但是利用上述方法的加密方案都被相继攻克,学者们进一步根据不同的加密方案研究了不同的破解方案,最常用的破解算法有F_4,F_5算法[5,6],线性攻击法[7],差分攻击法[8],其中最常用的就是线性攻击和差分攻击。在此基础之上,不断出现了许多新的研究成果。虽然现有的一些方案仍有很多的不足之处,但是无论在安全性还是效率上都比早期的体制有了不小的进步。

2 多变量公钥密码扩展方案的介绍

多变量公钥密码方案是王后珍等人在2010年提出的[9],该方案的核心思想是将已知Hash函数和已知明文生成冗余变量,引入Tame变换来对冗余变量和原始变量进行转换,进而利用冗余变量带来的影响来最大限度地增强加密的安全性。

设原始的多变量公钥密码体制的公钥为:$Y=T\circ F\circ U=(f_1(x_1,x_2,\cdots,x_n),\cdots,f_n(x_1,x_2,\cdots,x_n))$,变量均在有限域内,首先应该明确的一点是这里的方程的个数和变量的个数是相等的,王后珍等人正是对这种体制进行的改进,他们首先引入了一个特殊的Tame变换,该变换原本被当作中心映射的一种,但是由于其本身结构的特殊性,使得明文和密文之间蕴含线性关系,因此不再适合作为中心映射,但仍有类似Tame变换的加密方案至今仍被认为是安全的[10]。设F_q是有限域,王后珍等人利用Tame变换L的结构如下:

$$L:F_q^{n+\partial}\to F_q^n$$

$$\begin{pmatrix}h_1\\ \vdots\\ h_{n-\partial}\end{pmatrix}=A\begin{pmatrix}x_1\\ \vdots\\ x_{n-\partial}\end{pmatrix}+\alpha_1$$

$$\begin{pmatrix}h_{n-\partial+1}\\ \vdots\\ h_n\end{pmatrix}=\begin{pmatrix}x_{n-\partial+1}\\ \vdots\\ x_n\end{pmatrix}+D\begin{pmatrix}x_{n+1}\\ \vdots\\ x_{n+\partial}\end{pmatrix}+B\begin{pmatrix}x_1\\ \vdots\\ x_{n-\partial}\end{pmatrix}+\partial_2$$

其中,A为$(n-\partial)\times(n-\partial)$可逆矩阵,$\partial_1$为$n-\partial$维常量矩阵,$D$为$\partial\times\partial$的对角矩阵,$B$是任意的$\partial\times(n-\partial)$矩阵,$\alpha_2$为$\partial$维常量矩阵,而扩展变量为$x_{n+i}(1\leqslant i\leqslant\partial)$,它们是前面的已知变量的Hash值,即:

本文受重庆市教委基金(Grant KJ120513),科委项目(cstc2011jjA40037)资助。
罗文俊(1966—),男,博士,教授,主要研究方向为信息安全,E-mail:luowj@cqupt.edu.cn;弓守朋(1989—),男,研究生,主要研究方向为信息安全。

$x_{n+i}=H_k(x_1\|x_2\|\cdots\|x_{n-\partial+i-1}),1\leqslant i\leqslant\partial$

可以看出 L 不是可逆的，但引入后加解密时间不会受太大的影响，此时公钥方程的形式就变成了如下形式：$Y=T\circ F\circ U\circ L$，此时的公钥变为 $n+\partial$ 个输入、n 个输出的不定方程组。加解密过程如下：

加密：对于明文变量 $(x_1,x_2,\cdots,x_n)$，首先利用安全 Hash 函数计算出扩展变量 $x_{n+i},1\leqslant i\leqslant\partial$，然后把明文变量和扩展变量带入到公钥方程中。首先把这些得到的变量利用方程组 L 进行转换，接着把得到的结果代入到方程组 U 和 F 中，具体过程如下：

$(t_1,\cdots,t_n)=F\circ U\circ L(x_1,\cdots x_{n+\partial})$

从这个等式中可以看到，此时方程组中方程的个数为 n，王后珍等人在此处又增加了方程的个数，他们从有限域中随机选取了 u 个多项式，即：

$(t_{n+1},t_{n+2},\cdots,t_u)=(f_{n+1},f_{n+2},\cdots,f_{n+u}),1\leqslant u\leqslant\partial$

随后又选取了新的可逆矩阵 T'，并利用它对计算结果进行转换，得到了最终加密结果：$(y_1,y_2,\cdots,y_{n+u})$，可以看出此时公钥方程组是 $n+\partial$ 个输入，$n+u$ 个输出。

解密：对于一组合法的密文 $(y_1,y_2,\cdots,y_{n+u})$，首先利用 T'^{-1} 求得 $t_1,\cdots,t_{n+u}$，然后去掉后面多余的 u 个值，再依次利用 F^{-1},U^{-1},L^{-1} 求得最终的合法明文 $(x_1,x_2,\cdots,x_n)$。

3 破解方法介绍

然而在 2013 年 6 月，聂旭云等人针对此加密算法提出王后珍等人的加密方案并没有增强原始方案的安全性，并且扩展方案中的随机增加多项式的方法并不能增强原始密码体制的安全性[11]。他们对只含有扩展变量的公钥方程组进行了分析，指出如果存在一个能够破解原始密码体制的算法 A，并且找到一种能够消除扩展变量影响的方法，那么就能够破解王后珍等人的方案，破解过程如下：

首先，利用公钥 $Y=T\circ F\circ U\circ L$ 方程组得到不含扩展变量的公钥方程 $Y'=T\circ F\circ U\circ L'$，此方程组很容易得到，只要使含有扩展变量的系数为零即可，即让对角矩阵 D 的元素全部为零。此时这两个公钥方程组的唯一不同之处是 L,L'，我们也可以容易地得到 L' 的结构：

$$\begin{pmatrix}h_1\\\vdots\\h_{n-\partial}\end{pmatrix}=A\begin{pmatrix}x_1\\\vdots\\x_{n-\partial}\end{pmatrix}+\alpha_1$$

$$\begin{pmatrix}h_{n-\partial+1}\\\vdots\\h_n\end{pmatrix}=\begin{pmatrix}x_{n-\partial+1}\\\vdots\\x_n\end{pmatrix}+B\begin{pmatrix}x_1\\\vdots\\x_{n-\partial}\end{pmatrix}+\alpha_2$$

可以看出 L' 是可逆的，那么 $U\circ L'$ 仍是可逆的，也就是说可以利用算法 A 很容易地破解 Y'，只要解出 L，王后珍等人的方案将不再安全。

接着，破解方随机选择一组合法的明文利用公钥进行加密。即 $Y=T\circ F\circ U\circ L(x_1',x_2',\cdots,x_n')$，得到密文 $(y_1',y_2',\cdots,y_n')$，利用得到的合法密文和算法 A，求解出在公钥 $Y'=T\circ F\circ U\circ L'$ 下的明文 $(x_1'',\cdots x_n'')$。

利用 $D[i][i]=(x''_{n-\partial+i}-x'_{n-\partial+i})/x'_{n+i}$，其中 $1\leqslant i\leqslant\partial$，扩展变量可以根据已知的 Hash 函数和初始的合法明文得到。通过这个等式我们可以很容易地求出对角矩阵 D。

最后，在获得矩阵 D 后，对于任意一组的合法密文 $(y_1',y_2',\cdots,y_n')$，求其合法的明文时，首先利用算法 A 求得在 Y' 的明文 $(x_1'',\cdots,x_n'')$，再根据合法明文和求得的明文之间的关系，可以先求得部分合法的明文，即：$x_i'=x_i'',1\leqslant i\leqslant n-\partial$，对于后面没有得到的明文，首先利用哈希函数和得到的部分合法明文求得扩展变量，即：$x'_{n+i}=H_k(x_1'\|x_2'\|\cdots\|x'_{n-\partial+i-1}),1\leqslant i\leqslant\partial$。在得到扩展变量后，没有得到的明文可以利用如下等式得到：$x'_{n-\partial+i}=x''_{n-\partial+i}-D[i][i]x'_{n+i}$。至此王后珍等人的加密方案被破解。

4 改进方法及证明

我们在研究了聂旭云等人的破解方案后发现，他们之所以能够解出矩阵 D，是因为找到了这样的一个线性关系式：$x'_{n-\partial+i}=x''_{n-\partial+i}-D[i][i]x'_{n+i}$，之所以存在这个线性关系是因为矩阵 D 的结构比价特殊，它是对角矩阵，聂旭云等人很好地利用了这个性质，我们从这个线性关系中寻找改进方案的方法。

首先，我们把这个线性关系做一般化的处理：

$$x'_{n-\partial+i}+\begin{bmatrix}a_{11},a_{12},\cdots,a_{1\partial}\\\vdots\\a_{\partial1},a_{\partial2},\cdots,a_{\partial\partial}\end{bmatrix}\begin{pmatrix}x'_{n+1}\\\vdots\\x'_{n+\partial}\end{pmatrix}=x'_{n-\partial+i}\qquad(1)$$

其中，$1\leqslant i\leqslant\partial$，可以看出利用对角阵的性质能以很容易地写出通项表达式，因为只有对角线上的元素不为零，其他全部为零，因此也就无法破解出王后珍等人的加密方案。所以我们主要的工作就是利用改进的对角矩阵 D 和扩展变量来解除这个线性关系。

从结构上我们看出，可以从两个部分进行改进。第一，如果我们在加密的初始，得到扩展变量后，适当调整扩展变量的输入顺序，可以消除这个线性关系。证明如下：

我们假设得到扩展变量后，将其按照它相反的顺序 $(x'_{n+\partial},x'_{n+\partial-1},\cdots,x'_{n+1})$ 和明文共同输入到公钥方程中，破解者不知道这个顺序。如果 D 仍是对角阵，那么在计算矩阵 D 时利用的关系式为：$D[i][i]=(x''_{n-\partial+i}-x'_{n-\partial+i})/x'_{n-i+1}$，其中，$1\leqslant i\leqslant\partial$，与原来的元素顺序正好相反，更进一步地，如果扩展变量调整顺序后看起来不再有序，那么破解者不得不花费一定的时间找到这个顺序后才能得到矩阵 D。可以知道，扩展变量的全排列可以有 $\partial!$ 种，如果 ∂ 取适当的值，那么就可以进一步增强方案的安全程度。

第二，矩阵 D 也采取了类似的方法。先来分析一下王后珍等人为什么要让矩阵 D 为对角矩阵的原因，主要有两点：一是加密效率的考虑，D 中零元素的个数应该尽可能地多，这样才能最大限度增加加密的速度。二是 D 与扩展变量计算后，应该保证全部扩展变量的系数不为零，这样才能够发挥扩展变量的全部影响。对角矩阵很好地满足了这两个要求。但是由于其结构的特殊性存在不小的安全隐患，我们对原始的对角矩阵进行了行变换，并且发现经过行变换后的矩阵 D，结构更具一般性，原来的线性结构不再存在，证明如下：

在式(1)中，我们取一个实例，假设 $i=1$，则可以得到如下关系式：

$$x'_{n-\partial+1}+a_{11}x'_{n+1}+a_{12}x'_{n+2}\cdots+a_{1\partial}x'_{n+\partial}=x''_{n-\partial+1}$$

当 D 为对角阵时，除 a_{11} 外，其余的系数全部为零，其实我们也可以有其他的选择，只要保证这些系数中有一个不为零即

（下转第 373 页）

参 考 文 献

[1] 郑博,张衡阳,等. 航空自组网贪婪地理路由协议研究[J]. 传感器与微系统,2012,31(5):23-25

[2] Al-Riyami S S,Paterson K. Certificateless public key cryptography [C] // Asiacrypt' 2003 (LNCS 2894). Springer-Verlag, 2003:452-473

[3] Wu C H,Chen Z X. A new efficient certificateless signcryption scheme[C]//Preceedings of the ISISE2008. 2008:661-664

[4] Yuan Y M, Li D, Tian L W, et al. Certificateless signature scheme without random oracles[C]//Park J H,et al. eds. Proc. of the ISA2009 (LNCS5576). Heidelberg: Springer-Verlag, 2009:31-40

[5] 张福泰,孙银霞,等. 无证书公钥密码体制研究[J]. 软件学报, 2011,22(6):1317-1332

[6] Lippold G, Boyd C, Gonzalez NJM. Strongly secure certificateless key agreement[C]//Shacham H, Waters B, eds. Proc. of the Pairing-Based Cryptography-Pairing 2009. LNCS5671, Heidelberg: Springer-Verlag, 2009:206-230

[7] Gao Meng, Zhang Fu-tai. Key-compromise impersonation attacks on some certificateless key agreement protocols and two improved protocols[C]// Proc. of the 1st International Workshop on Education Technology and Computer Science. 2009:62-66

[8] MIRACL. Multiprecision integer and rational arithmetic C/C++ library[OL]. http://indigo.ie/mscott/

[9] 刘文浩,许春香. 无证书两方密钥协商方案[J]. 软件学报,2011, 22(11):2843-2852

[10] 候爱琴,高宝建,等. 基于椭圆曲线的一种高效率数字签名[J]. 计算机应用与软件,2009,26(2):58-71

[11] Andrew C, Zhao Y L. Digital signatures from challenge-divided sigma-protocols[OL]. Proc. of the IACR Cryptology ePrint Archive, 2012

(上接第 362 页)

可,在这个关系式中,除了 a_{11} 外,我们还有 $\partial-1$ 种选择。对于整个矩阵来说,就是对矩阵 D 进行行变换后的结果。经过行变换后的矩阵,破解者很难确定矩阵中每一行上哪一项不为零,这样就从根本上消除了原始方案中的线性关系。

考虑到安全性,这两种措施应该同时采取,这样的改进工作不会对解密效率带来任何的影响,因为我们的工作主要是围绕者扩展变量展开的,而这些工作对合法的解密者来说却是透明的。每一次加密都要对矩阵 D 进行行变换,对扩展变量进行顺序调整。

总的来说,改进的关键之处就在于利用全排列的方法对对角矩阵和扩展变量进行了扰动,改变了变量的排列顺序,使破解者无法利用变量之间的顺序关系破解原有密码体制。

5 目的矩阵 D 的生成算法

我们需要对矩阵 D 的行变换设计专门的算法才能保证加密的要求。如果对矩阵 D 进行行变换应该有 ∂ !种,但如果 ∂ 较大,那么用来存储行变换结构的空间对整个加密过程来说会变得难以承受,所以我们在这里设计了一种类似的计算 ∂ !的算法。该算法并没有存储全部的行变换的结果,只是返回给调用程序一种行变换的结果。结果如下:

1. 初始化数组 $a[\partial]=\{1,2,\cdots,\partial\}$。

2. 生成 $[0,\partial-i)$ 之间的一个随机数 $subcript$,其中 $0\leqslant i<\partial$。

3. 将数组中下标为 $subcript$ 的元素输出,原数组将该元素删除

4. 将 i 加 1,然后返回步骤 2,直至原数组中元素为空。输出的元素序列即是 ∂ 个元素全排列的一种,即矩阵 D 行变换的一种。

此方法同样适用于对扩展变量的顺序调整,这里不再一一赘述。

结束语 聂旭云等人分析了多变量公钥密码扩展方案,并且发现了方案中的安全漏洞,但并未对其进行改进,我们从他们的破解方法中找到了改进方案的方法,并且给出了相关的证明。多变量公钥密码是抗量子攻击的一个重要组成部分,一旦量子计算机出现,该加密体制一定会有更广泛的应用前景和更高的学术价值。未来的工作是多变量公钥密码体制在云环境下[12]的应用范围。

参 考 文 献

[1] Ding Jin-tai, Schmidt D. Multivariable public-key cryptosystems [J]. Advances in Information Security, 2006, 3494(10): 288-304

[2] Ding Jin-tai. A new Variant of Matsumoto-Imai Cryptosystem through Perturbation[J]. Public Key Cryptography-PKC, 2004, 2947(12): 305-318

[3] Ding Jin-tai, Schmidt D. Rainbow a new Multivariable Polynomial Signature[J]. Applied Cryptography and Network Security, 2005, 3531(14): 164-175

[4] Ding Jin-tai, Schmidt D. Cryptanalysis of HFEv and Internal Perturbation of HFE[J]. Public key Cryptography-PKC, 2005, 3386(5): 288-301

[5] Faugere J C. A new efficient algorithm for computing Grobner bases(F4)[J]. Journal of Pure and Applied Algebra, 2009 (139): 61-88

[6] Yang Bo-yin. Public-Key Cryptography from New Multivariate Quadratic Assumptions[J]. Informa tion Security, 2010(5): 193-241

[7] Ding Jin-tai, Hu Lei, Nie Xun-yun, et al. High Order Linearization Equition (HOLLE) Attack on Multivariable Public Key [J]. Advances in Information Security, 2010(9): 126-134

[8] Fouque P A, Granboulan L, Stern J. Differential Cryptanalysis for Multivariate Scheme[J]. Advance In Cryptology EUROCRYPT, 2005, 3494(9): 341-353

[9] 王后珍,张焕国,王张宜,等. 一类具有安全加密功能的扩展 MQ 公钥加密体制[J]. 中国科学,2011,41(11):1297-1309

[10] Yang Bo-yin, Chen Jiun-ming. Building Secure Tame-like Multivariate Public-Key Cryptosystems The New TTS[J]. Information Security and Privacy, 2005, 354(7): 518-531

[11] 聂旭云,徐赵虎,廖永建,等. 多变量公钥密码扩展方案的安全性分析[J]. 计算机学报,2013,36(6):1177-1182

[12] 李乔,郑啸. 云计算研究现状综述[J]. 计算机科学,2011,38(4): 32-37