对 pSFLASH 扰动公钥密码的一个实际攻击

孙思维[1)] 胡 磊[1)] 蒋 鑫[1),2)]

[1)](中国科学院研究生院信息安全国家重点实验室 北京 100049)

[2)](中国航天科技集团公司第九研究院第七零四研究所 北京 100076)

摘 要 通过对 SFLASH 的中心映射进行扰动,最近 Wang 等人提出了一个新的多变量公钥系统 pSFLASH. pSFLASH的设计者认为,扰动后的中心映射可以破坏 SFLASH 公钥潜在的数学结构,从而抵抗针对 SFLASH 的差分代数攻击[2-3]. 然而对于以(T^{-1},U^{-1},β,γ)为私钥的任一 pSFLASH 实例,一定存在一个可逆仿射变换 $\tilde{U}$,使它变成一个以(T^{-1},$\tilde{U}^{-1}$)为私钥的 SFLASH 实例,因此利用对 SFLASH 的差分代数攻击[2-3],在几秒钟的时间内可以实际地伪造出任意消息的合法的 pSFLASH 签名.

关键词 多变量公钥密码;SFLASH;线性化方程攻击;差分代数攻击

中图法分类号 TP309 **DOI 号**: 10.3724/SP.J.1016.2011.01284

A Practical Attack on the pSFLASH Public Key Cryptosystem

SUN Si-Wei[1)] HU Lei[1)] JIANG Xin[1),2)]

[1)](*State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences, Beijing* 100049)

[2)](*Research Institute 704 of China Academy of Aerospace Electronics Technology, Beijing* 100076)

Abstract Recently, a new multivariate public key cryptosystem named pSFLASH is proposed by Wang in 2010 by inserting a perturbation into the central map of the SFLASH cryptosystem. The designers of pSFLASH claim that the potential mathematical structure of the public key of SFLASH will be destroyed, if the central map is perturbed in such a way. Therefore, pSFLASH could resist the differential algebraic attack[2-3]. This paper points out that, for every pSFLASH instance with private key (T^{-1},U^{-1},β,γ), there must exist a SFLASH instance with private key (T^{-1},$\tilde{U}^{-1}$), such that the pSFASH instance can be converted into that sFLASH instance. As a result, by applying the differential algebraic attack on SFLASH[2-3], we can practically forge a valid pSFLASH signature in seconds.

Keywords multivariate public key cryptosystem; SFLASH; linearization attack; differential algebraic attack

1 引 言

公钥密码已经成为现代信息社会中保护数据通信的一种重要工具. 经典的公钥密码算法主要基于大整数分解(如 RSA 算法)和离散对数(如 ElGmal 算法和椭圆曲线公钥算法)这两个数学难题. 然而在 1994 年,Shor 等人[4]给出了一种可以用于分解大整数的多项式时间的量子算法. 这表明,一旦实用的量子计算机能成功制造出来,那些基于大整数分解和离散对数的公钥系统就会受到致命的威胁. 所以,构造新的可以抵抗量子攻击的公钥密码系统就变的非

收稿日期:2010-05-07;最终修改稿收到日期:2011-06-13. 本课题得到国家自然科学基金(61070172,10990011)、国家"九七三"重点基础研究发展规划项目基金(2007CB311201)资助.**孙思维**,男,1985 年生,博士研究生,主要研究方向为密码分析与网络安全. E-mail: sunsiwei08@mails.gucas.ac.cn. **胡 磊**,男,1967 年生,博士生导师,主要研究领域为密码学与网络安全. **蒋 鑫**,男,1984 年生,博士,主要研究方向为密码学与网络安全.

常有意义.

研究者们在此方向上进行了各种努力与尝试，构造了一些新的公钥算法. 一些著名的例子包括基于一般线性码译码问题的 McEliece 公钥算法[5]、基于格问题的 NTRU 公钥算法[6]和基于有限域上多项式方程组求解问题的多变量公钥系统 MI[7]. 这些新提出的公钥算法所基于的数学问题，至今没有找到有效的量子多项式时间算法.

多变量公钥密码被认为是一类很有前途的可以抵抗量子计算机攻击的公钥系统. 近年来各种新的多变量公钥系统的构造方法层出不穷[8-10]，同时在对多变量公钥系统的攻击方面，研究者也积累了大量的经验. 一些著名的攻击包括线性化方程攻击[11]、高阶线性化方程攻击[12]、小秩攻击[13]和差分代数攻击[2-3]等等. 其中差分代数攻击成功攻破了 SFLASH 多变量公钥系统. 最近，一些研究者研究了如何修复 SFLASH 公钥系统，文献[14]将 SFLASH 密码系统的消息空间定义在一个超平面上，以挫败差分代数攻击[2-3]中所利用的差分对称性质. 而在文献[1]中，设计者试图通过对 SFLASH 算法的中心映射 F 进行扰动，设计出抵抗差分代数攻击的新的多变量公钥密码.

第 2 节介绍原始 SFLASH 多变量公钥系统以及文献[1]设计的扰动 SFLASH——pSFLASH；在第 3 节中，我们简要描述对 SFLASH 的线性化方程攻击和差分代数攻击；在第 4 节中，我们证明 pSFLASH 系统等价于原始的 SFLASH 系统，并给出对 pSFLASH 的实际攻击.

2　SFLASH 和 pSFLASH 多变量公钥系统

SFLASH 是一个用于签名的多变量公钥系统，它是 2003 年 NESSIE 推荐的 3 个签名算法之一，SFLASH 算法的签名速度很快，并且适合在一些轻量级设备(如 RFID 智能卡)上实现，下面我们给出 SFLASH 的描述.

2.1　MI 和 SFLASH 多变量公钥系统

设 k 是一个有 q 个元素且特征为 2 的有限域，而 $K=k[x]/g(x)$ 是 k 的一个 n 次扩域，其中 $g(x)$ 是 $k[x]$ 上的 n 次不可约多项式. 令 $\phi: K\to k^n$ 是 K 与 k^n 的自然同构，即

$$\phi(a_0+a_1x+\cdots+a_{n-1}x^n)=(a_0,a_1,\cdots,a_{n-1}),\ a_i\in k$$

Matsumoto-Imai(MI)型多变量公钥系统[7]的公钥 $P: k^n\to k^n$ 为

$$P=T\circ\phi\circ F\circ\phi^{-1}\circ U.$$

而 SFLASH 型多变量公钥系统的公钥 $P_{\Pi}: k^n\to k^{n-r}$ 为

$$P_{\Pi}=\Pi_{n-r}\circ T\circ\phi\circ F\circ\phi^{-1}\circ U,$$

其中，U，T 是 k^n 到 k^n 上的可逆仿射变换；Π_{n-r} 的作用是 n 个坐标到它前 $n-r$ 个坐标的投影. 因此，SFLASH 是一个“减”版本的 MI 系统[15]. 以下记 $\Pi_{n-r}\circ T$ 为 T_{Π}. F 是 K 到 K 上的一个可逆变换，我们称其为中心映射，按如下的方式定义

$$F(X):=X^{q^{\theta}+1}=X^{q^{\theta}}X,$$

其中 $\gcd(q^{\theta}+1,q^{\theta}-1)=1$. 因为 $\tau: X\mapsto X^{q^{\theta}}$ 是 K 到 K 上的 k-线性映射，所以 SFLASH 系统的公钥可以写成一组 k 上的二次多项式，形如

$$y_i=\sum_{0\le j\le k\le n}\xi_{ijk}x_jx_k+\sum_{0\le j\le n}\delta_{ij}x_j+\rho_i,\quad i=0,1,\cdots,n-r-1.$$

注意，虽然这组多项式是公开的，但 U 和 T 是保密的，U^{-1} 和 T^{-1} 作为 SFLASH 系统的私钥.

对于消息 $\boldsymbol{y}=(y_0,y_1,\cdots,y_{n-r-1})^{\mathrm{T}}\in k^{n-r}$，签名的过程为：首先任取 r 个 k 上的元素，把 $\boldsymbol{y}$ 补成一个 n 维向量 z，然后计算

$$\boldsymbol{x}=T^{-1}\circ\phi\circ F^{-1}\circ\phi^{-1}\circ U^{-1}(\boldsymbol{z}).$$

$\boldsymbol{x}$ 即为消息 $\boldsymbol{y}$ 的签名. 签名的验证过程为：计算 $\boldsymbol{\omega}=P_{\Pi}(\boldsymbol{x})$，然后比较 $\boldsymbol{\omega}$ 是否与 $\boldsymbol{y}$ 相同，如果相同，签名验证通过. 由于 P 是公开的，所以任何人都可以执行签名验证这个操作. 但只有私钥拥有者，才能通过 U^{-1} 和 T^{-1} 来计算签名.

对于一个想要伪造消息 $\boldsymbol{y}$ 的签名的攻击者，伪造签名最直接的方式就是解如下由公钥 P 得到的多项式方程组

$$\begin{cases}y_0=f_0(x_0,x_1,\cdots,x_{n-1})\\ y_1=f_1(x_0,x_1,\cdots,x_{n-1})\\ \vdots\\ y_{n-r-1}=f_{n-r-1}(x_0,x_1,\cdots,x_{n-1}).\end{cases}$$

若得到一个解 $\boldsymbol{x}$，从而 $P_{\Pi}(\boldsymbol{x})=\boldsymbol{y}$. 然而，解一个有限域上的一般的多项式方程组通常是困难的.

虽然通过直接解上述方程组来攻击 SFLASH 是困难的，但 Dubois 等人利用 SFLASH 公钥差分的结构攻破了该系统[2-3]. 为了抵抗这种差分攻击，文献[1]提出了一个新的用于签名的多变量公钥系统 pSFLASH. 下面给出 pSFLASH 的具体构造.

2.2 pSFLASH 多变量公钥系统

pSFLASH 的构造思想是，对原始的 SFLASH 系统的中心映射 F 进行所谓的“噪声扰动”，从而破坏公钥的差分结构.

定义 1. 定义二元运算$\otimes: K\times K\to K$ 为 $a\otimes b=\phi^{-1}(a_0\ b_0, a_1\ b_1, \cdots, a_{n-1}\ b_{n-1})$，其中 $(a_0, a_1, \cdots, a_{n-1})=\phi(a)$，$(b_0, b_1, \cdots, b_{n-1})=\phi(b)$. 文献[1]称其为噪声运算.

定义 2. 称 $\langle PG, \otimes\rangle=\{\beta: \beta\in K, \phi^{-1}(\beta)\in (k^*)^n\}$ 为 SFLASH 系统的噪声群，其中 k^* 表示有限域 k 的乘法群.

从 SFLASH 的噪声群中任意取两个元素 β, γ，令 $F_d: K\to K$ 为

$$F_d(X)=(\beta\otimes X+\gamma)^{q^\theta+1}.$$

现在我们用 F_d 替换 SFLASH 的中心映射 F，其它运算保持不变，便得到了 pSFLASH 系统，即 pSFLASH 的公钥为

$$Q_\Pi=\Pi_{n-r}\circ T\circ\phi\circ F_d\circ\phi^{-1}\circ U.$$

在以后的讨论中，我们记 $T\circ\phi\circ F_d\circ\phi^{-1}\circ U$ 为 Q. 因此，$Q_\Pi=\Pi_{n-r}\circ Q$.

文献[1]认为，SFLASH 的中心映射经过这样的“噪声扰动”，就可以避免差分代数攻击，下面两节的分析指出，事实上并非如此.

3 对 SFLASH 的攻击

3.1 MI 系统的线性化方程攻击

$$P(x)=T\circ\phi\circ F\circ\phi^{-1}\circ U \tag{1}$$

由 $Y=F(X)=X^{q^\theta+1}$ 可以得到

$$Y^{q^\theta-1}=X^{q^{2\theta}-1}.$$

两边同乘 XY，有

$$XY^{q^\theta}=X^{q^{2\theta}}Y.$$

而对 K 上的元素进行 q^θ 和 $q^{2\theta}$ 次幂，都是 K 上的 k-线性映射，所以对于任意的满足 $\boldsymbol{y}=P(\boldsymbol{x})$ 的 $\boldsymbol{x}$ 和 $\boldsymbol{y}$，其分量一定满足一些形如

$$\sum_{i,j}a_{ijk}x_iy_j+\sum_i b_{ik}x_i+\sum_j c_{jk}y_j+d_k=0 \tag{2}$$

的多项式方程.

文献[11]的分析表明，对于 MI 系统任意给定的公钥，一定可以找到足够多的、相互独立的形如式(2)的多项式方程. 这样，当攻击者想恢复 $\boldsymbol{y}=P(\boldsymbol{x})$ 的原象时，他并不需要去解由 $\boldsymbol{y}=P(\boldsymbol{x})$ 对应的多项式方程组，而是将 $\boldsymbol{y}$ 代入形如式(2)的多项式方程组，此时便得到了一个关于 x_i 的线性方程组，解这个线性方程组便可以得到 $\boldsymbol{y}$ 在 P 下的原象 $\boldsymbol{x}$. 这种恢复原象的过程，就是著名的线性化方程攻击[7].

为了避免上述线性化方程攻击，SFLASH 的设计者在 MI 系统的中心映射 P 的基础上加入了一个投影映射 Π_{n-r}，即隐藏了由 $P(\boldsymbol{x})$ 导出的多项式方程组的最后 r 个多项式. 文献[15]的分析表明，攻击者无法直接利用这样处理后所得到的公钥多项式组，找到足够多的、相互独立的形如式(2)的多项式方程组，从而线性化方程攻击对 SFLASH 失效.

3.2 SFLASH 的差分代数攻击

由上一小节的分析可知，如果我们能克服 SFLASH 系统中投影变换 Π_{n-r} 的作用，便有可能利用线性化方程攻击来伪造 SFLASH 系统的合法签名. 而 SFLASH 系统公钥差分的对称性质，使得攻击者可以达到这一目的[2-3].

为了叙述方便，下面不再显式地写出自然同构映射 ϕ，当运算需要时，我们认为所考虑的元素或向量被自然地同构映射或逆映射到相应的向量或域元素. 另外，假设所有可逆仿射变换为可逆线性变换，这并不影响分析，具体细节参考文献[16-18].

首先，引入差分算子 $D: Df(a,x)=f(a+x)-f(a)-f(x)+f(0)$，则对于 SFLASH 系统的中心映射 F，有

$$DF(a,x)=ax^{q^\theta}+a^{q^\theta}x.$$

对于 $\forall\xi\in K$，可以得到

$$DF(\xi\cdot a,x)+DF(a,\xi\cdot x)=(\xi+\xi^{q^\theta})\cdot DF(a,x) \tag{3}$$

这是 MI 系统中心映射的差分具备的一个重要的对称性质.

令 $P=T\circ\phi\circ F\circ\phi^{-1}\circ U$，则由 $DP(a,x)=T\circ DF(U(a),U(x))$ 与式(3)可以得到

$$\begin{aligned}&T\circ DF(\xi\cdot U(a),U(x))+T\circ DF(U(a),\xi\cdot U(x))=\\&\quad T\circ(\xi+\xi^{q^\theta})\cdot DF(U(a),U(x))=\\&\quad T\circ(\xi+\xi^{q^\theta})\cdot T^{-1}(DP(a,x)).\end{aligned}$$

用 M_ξ，$M_{L(\xi)}$ 和 N_ξ 分别表示映射 $M_\xi: x\mapsto\xi\cdot x$，$M_{L(\xi)}: x\mapsto(\xi+\xi^{q^\theta})\cdot x$ 和 $N_\xi: x\mapsto U^{-1}\circ M_\xi\circ U(x)$. 将 Π_{n-r} 作用到上式，得到

$$\begin{aligned}&DP_\Pi(N_\xi(a),x)+DP_\Pi(a,N_\xi(x))=\\&\qquad\Lambda(L(\xi))(DP_\Pi(a,x))\end{aligned} \tag{4}$$

其中 $\Lambda(L(\xi))$ 表示映射 $T_\Pi\circ M_{L(\xi)}\circ T^{-1}$. 当 U 固定时，$\{N_\xi: \xi\in K\}$ 是一个由线性变换组成的 n 维 k-线性空间，它是由全体线性变换组成的 n^2 维 k-线性空间的一个子空间. 而一般的线性变换并不满足上式，由此可以用简单的线性代数很容易地计算出这个子

空间，请参考文献[2-3]. 实际上，由这个子空间还可以计算出 U 的一部分信息，见文献[19]，不过下面的分析并不需要这一点.

注意，在复合映射

$$P_{\Pi}(\boldsymbol{x}) = \Pi_{n-r} \circ T \circ \phi \circ F \circ \phi^{-1} \circ U(\boldsymbol{x})$$

式中，T 的作用实质上是通过对 $\phi \circ F \circ \phi^{-1} \circ U(\boldsymbol{x})$ 的分量多项式进行新的线性组合得到一组新的分量多项式. 如果能在 $T_{\Pi} = \Pi_{n-r} \circ T$ 的复合之前引入一个新的线性变换，则很可能得到一些与 P_{Π} 所对应的多项式组线性独立的多项式，从而得到与 MI 系统等价的公钥多项式，进而利用线性化方程攻击，就可以伪造出 SFLASH 系统的合法签名. 注意到

$$\begin{aligned} P_{\Pi} \circ N_{\xi} &= T_{\Pi} \circ F \circ U \circ (U^{-1} \circ M_{\xi} \circ U) \\ &= T_{\Pi} \circ M_{\xi^{q^{\theta}+1}} \circ F \circ U, \end{aligned}$$

由于 $T_{\Pi} \circ M_{\xi^{q^{\theta}+1}}$ 与 $\Pi_{n-r} \circ T$ 一般是线性独立的线性变换，所以利用 $P_{\Pi} \circ N_{\xi}$，就可以得到所需的与 P_{Π} 所对应的多项式组线性独立的公钥多项式. 实验证明，这种方法是完全可行的[2-3].

4　对 SFLASH 及 pSFLASH 的攻击

4.1　理论分析

对于 pSFLASH 系统的中心映射 F_d，我们有

$$DF_d(a,x) = \beta \otimes a \cdot (\beta \otimes x)^{q^{\theta}} + (\beta \otimes a)^{q^{\theta}} \cdot \beta \otimes x.$$

pSFLASH 的设计者认为，由于 β 是未知的，所以上述差分攻击对 SFLASH 无效. 我们指出，pSFLASH 公钥系统与 SFLASH 系统实质上是等价的.

定理 1.　对于任意给定的 $\beta, \gamma \in \langle PG, \otimes \rangle$，一定存在仿射变换 $\widetilde{U}$，使得对任意的 $x \in k^n$，有

$$T_{\Pi} \circ \phi \circ F \circ \phi^{-1} \circ \widetilde{U}(\boldsymbol{x}) = Q_{\Pi}(\boldsymbol{x}),$$

其中 Q_{Π} 是 pSFLASH 系统的公钥映射.

证明.　设可逆仿射变换 U 为 $U(\boldsymbol{x}) := \boldsymbol{A}\boldsymbol{x} + \boldsymbol{b}$，其中 $\boldsymbol{A}$ 是 k 上 $n \times n$ 可逆矩阵，$\boldsymbol{b}$ 为 k 上的 n 维常向量. 令 $\boldsymbol{A}\boldsymbol{x} + \boldsymbol{b} = \boldsymbol{u} = (u_0, u_1, \cdots, u_{n-1})^{\mathrm{T}}$，

$$\boldsymbol{M} = \begin{bmatrix} \beta_0 & & & \\ & \beta_1 & & \\ & & \ddots & \\ & & & \beta_{n-1} \end{bmatrix},$$

并令

$$\widetilde{U}(\boldsymbol{x}) = \boldsymbol{M}\boldsymbol{A}\boldsymbol{x} + \boldsymbol{M}\boldsymbol{b} + \boldsymbol{\gamma} = \boldsymbol{M}(\boldsymbol{A}\boldsymbol{x} + \boldsymbol{b}) + \boldsymbol{\gamma},$$

可见 $\widetilde{U}$ 仍然是一个可逆的仿射变换. 此时，我们有

$$\widetilde{P}(\boldsymbol{x}) = T \circ \phi \circ F \circ \phi^{-1} \circ \widetilde{U}(\boldsymbol{x}) =$$

$$T(\phi((\phi^{-1}(\widetilde{U}(\boldsymbol{x})))^{q^{\theta}+1})) =$$

$$T(\phi((\phi^{-1}(\boldsymbol{M}\boldsymbol{A}\boldsymbol{x} + \boldsymbol{M}\boldsymbol{b} + \boldsymbol{\gamma}))^{q^{\theta}+1})).$$

它进一步等于

$$\widetilde{P} = T\left(\phi\left(\left(\phi^{-1}\left(\begin{bmatrix} \beta_0 & & & \\ & \beta_1 & & \\ & & \ddots & \\ & & & \beta_{n-1} \end{bmatrix} \boldsymbol{A}\boldsymbol{x} + \boldsymbol{M}\boldsymbol{b} + \boldsymbol{\gamma}\right)\right)^{q^{\theta}+1}\right)\right) =$$

$$T(\phi((\phi^{-1}(\beta_0 u_0 + \beta_1 u_1 + \cdots + \beta_{n-1} u_{n-1}))^{q^{\theta}+1})) =$$

$$T(\phi((\boldsymbol{\beta} \otimes \boldsymbol{u} + \boldsymbol{\gamma})^{q^{\theta}+1})) =$$

$$T(\phi((\boldsymbol{\beta} \otimes (\boldsymbol{A}\boldsymbol{x} + \boldsymbol{b}) + \boldsymbol{\gamma})^{q^{\theta}+1})) =$$

$$Q(\boldsymbol{x}).$$

上述等式两边同时作用投影映射 Π_{n-r}，得到

$$T_{\Pi} \circ \phi \circ F \circ \phi^{-1} \circ \widetilde{U}(\boldsymbol{x}) = Q_{\Pi}(\boldsymbol{x}) \quad \text{证毕.}$$

也就是说，只要把 pSFLASH 系统中的秘密仿射变换 U 换成 $\widetilde{U}$，并去掉 pSFLASH 对 SFLASH 系统中心映射 F 的扰动，则 pSFLASH 系统变成 SFLASH 系统. 由前一节的分析可以看出，对 SFLASH 的差分攻击与仿射变换 U 的选取无关.

4.2　实验数据

下面给出伪造 pSFLASH 消息 $\boldsymbol{y} \in k^{n-r}$ 的签名的具体步骤并给出相应的实验结果.

1. 把 pSFLASH 的公钥多项式组 Q_{Π} 看成一组 SFLASH 系统对应的公钥多项式. 利用差分攻击，求出相应的线性空间 $\{N_{\xi} : \xi \in K\}$. 它是线性变换的集合.

2. 从 $\{N_{\xi} : \xi \in K\}$ 中任选一线性变换，计算 $Q_{\Pi} \circ N_{\xi}(\boldsymbol{x})$，从而得到 $n-r$ 个多项式，从这 $n-r$ 个多项式中随机选取 r 个，加入到由 $Q_{\Pi}(\boldsymbol{x})$ 对应的公钥多项式组中去，记新得到的公钥多项式组为 $\widetilde{Q}(\boldsymbol{x})$.

3. 对 $\widetilde{Q}(\boldsymbol{x})$ 实施线性化方程攻击，得到 $\boldsymbol{x}$，验证 $Q_{\Pi}(\boldsymbol{x}) = \boldsymbol{y}$ 是否成立，如果成立，签名伪造成功，否则重复步 2.

因为 SFLASH 两个推荐版本的参数为：SFLASHv2—$q = 2^7$，$n = 37$，$\theta = 11$，$r = 11$；SFLASHv3—$q = 2^7$，$n = 67$，$\theta = 33$，$r = 11$，所以我们选取的攻击目标的参数都与上述参数相同或相近，在一台内存为 3.25GB，主频为 2.83GHz，Intel (R) Core(TM)2 Quad CPU 的计算机上，我们用 Magma 代数系统实现了上述攻击（只用了单核），实验结果见表 1，另外我们在附录中给出了一个小规模的例子. 其中表 1 中预计算耗时一行中显示的是恢复 $\{N_{\xi} : \xi \in K\}$ 的时间与恢复 r 个缺失多项式所用时间之和.

表 1　实验数据

q	n	θ	r	预计算耗时/s	伪造签名耗时/s
2^7	36	8	11	68+5	4
2^7	37	11	11	100+23	2
2^7	40	8	12	121+17	1
2^7	44	12	13	140+56	4
2^7	67	33	11	3523+812	3
2^7	128	33	13	2210+513	1

实验表明,在各种典型的参数下,对一个给定的 pSFLASH 系统,通过最多两个小时的预计算后(此预计算对一个给定的公钥是一次性的),对任意消息 $\boldsymbol{y}$,我们可以在几秒钟内伪造一个合法的 pSFLASH 签名.从而,文献[1]中的扰动方法对原始算法安全性的加强是无效的.

5 结束语

在本文中,我们证明了 pSFLASH 系统与 SFLASH 系统在不考虑公钥中的两个可逆仿射变换的意义下是等价的,因此利用差分攻击和线性化方程攻击可以给出一个对 pSFLASH 的实际攻击,pSFLASH 系统是完全不安全的.实际上,通过简单的扰动来增强类似于 SFLASH 这样的公钥系统的安全性是相当困难的问题[20-21],这方面的研究仍然是一个公开课题.

参 考 文 献

[1] Wang Hou-Zhen, Zhang Huan-Guo, Guan Hai-Ming, Han Hai-Qing. A new perturbation algorithm and enhancing security of SFLASH signature scheme. Science in China, Information Sciences, 2010, 53(4): 700-708

[2] Dubois V, Fouque A, Shamir A et al. Practical cryptanalysis of SFLASH//Proceedings of the Crypto 2007. Santa Barbara, California, USA, 2007: 1-12

[3] Dubois V, Fouque A, Stern J. Cryptanalysis of SFLASH with slightly modified parameters//Proceedings of the Eurocrypt 2007. Barcelona, Spain, 2007: 264-275

[4] Shor P W. Algorithm for quantum computation: Discrete log and factoring//Proceedings of the 35th Symposium on Foundations of Computer Science. Washington, DC, USA, 1994: 124-134

[5] McEliece R. A public key cryptosystem based on algebraic coding theory. DSN Progress Report: 42-44, 1987

[6] Hoffstein J, Pipher J, Silverman J H. NTRU: A ring based public key cryptosystem//Buhler J. Proceedings of the ANTS III. LNCS 1423. Berlin: Springer-Verlag, 1998: 267-288

[7] Matsumoto T, Imai H. Public quadratic polynomial-tuples for efficient signature verification and message encryption//Guenther C. Advances in Eurocrypt 1988. Davos, Switzerland. LNCS 330. Berlin: Springer, 1988: 419-453

[8] Patarin J, Courtois N, Goubin L. SFLASH, a fast multivariate signature algorithm//Proceedings of the CT-RSA 2001. San Francisco, CA, USA, 2001: 297-370

[9] Akkar M, Courtois N, Duteuil R et al. A fast and secure implementation of SFLASH//Proceedings of the PKC 2003. Miami, Florida, USA, 2003: 267-278

[10] Patarin J. Hidden field equations (HFE) and isomorphism of polynomials (IP): Two new families of asymmetric algorithms//Proceedings of the Eurocrypt 1996. Saragossa, Spain, 1996: 33-48

[11] Patarin J. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88//Proceedings of the Crypto 1995. Santa Barbara, California, USA, 1995: 248-261

[12] Ding Jin-Tai, Hu Lei, Nie Xu-Yun, Li Jian-Yu, Wagner J. High order linearization equation (HOLE) attack on multivariate public key cryptosystems//Proceedings of the PKC2007. Tsinghua University, Beijing, 2007: 233-248

[13] Nicolas T. The security of hidden field equations (HFE)//Naccache D. Proceedings of the ASIACRYPT 2001. LNCS. Heidelberg: Springer, 2001: 402-421

[14] Ding Jin-Tai, Dubois V, Yang Bo-Yin. Could SFLASH be repaired?//Proceedings of the ICALP 2008. Reykjavik, Iceland, 2008: 691-701

[15] Patarin J, Goubin L, Courtois N. C^{*}_{+-} and HM: Variations around two schemes of T. Matsumoto and H. Imai//Proceedings of the Asiacrypt 1998. Beijing, China, 1998: 35-49

[16] Geiselmann W, Steinwandt R, Beth T. Attacking the affine parts of SFLASH//Cryptography and Coding, 8th IMA International Conference Proceedings. Cirencester, UK, 2008: 355-362

[17] Geiselmann W, Steinwandt R, Beth T. Revealing 441 key bits of SFLASH^{v2}//Workshop Record of the 3rd NESSIE Workshop, 2002

[18] Geiselmann W, Steinwandt R, Beth T. Revealing affine parts of SFLASH^{v1}, SFLASH^{v2}, and FLASH. Actas de la VII Reunisn Espaqola de Criptologma y Seguridad de la Informacisn, 2002, 7: 305-314

[19] Billet O, Macario-Rat G. Cryptanalysis of the square cryptosystem//Proceedings of the ASIACRYPT 2009. Tokyo, Japan, 2009: 451-468

[20] Ding Jin-Tai. A new variant of the Matsumoto-Imai cryptosystem through perturbation//Proceedings of the PKC 2004. LNCS 2947. Springer, 2004: 305-318

[21] Ding Jin-Tai, Jason E. Inoculating multivariate schemes against differential attacks//Proceedings of the PKC 2006. Singapore, 2006: 290-301

[22] Ding Jin-Tai, Gower Jason E, Schmidt Dieter S. Multivariate public key cryptosystems//Yung M. Advances in Information Security. Berlin: Springer, 2006, 25

附录. 小规模 pSFLASH 实例及其分析.

令 $k=GF(2)$，$K=k[x]/(x^2+x+1)$，且 α 满足 $\alpha^2+\alpha+1=0$. 我们选取参数 $q=4$，$n=5$，$\theta=3$，且 $r=1$，某一 pSFLASH 实例的公钥多项式组为

$$\begin{cases} y_1=\alpha x_2+x_3+x_4+x_5+\alpha x_1^2+\alpha x_1x_2+\alpha^2x_1x_3+\\ \quad \alpha x_1x_4+x_2^2+\alpha x_2x_3+\alpha x_2x_5+\alpha^2x_3^2+\alpha x_3x_4+\\ \quad \alpha x_3x_5+\alpha x_4^2+\alpha x_4x_5+x_5^2\\ y_2=\alpha+\alpha^2x_4+x_5+\alpha x_1^2+\alpha^2x_1x_3+\alpha^2x_1x_4+x_1x_5+\\ \quad x_2^2+\alpha^2x_2x_3+\alpha x_3x_4+x_4^2+\alpha^2x_4x_5+x_5^2\\ y_3=1+\alpha^2x_1+\alpha x_2+\alpha^2x_3+x_4+\alpha^2x_5+\alpha^2x_1^2+x_1x_4\\ \quad \alpha^2x_1x_5+\alpha^2x_2^2+x_2x_4+x_2x_5+\alpha^2x_3^2+\alpha x_3x_4+\\ \quad \alpha x_3x_5+\alpha^2x_4x_5+\alpha^2x_5^2\\ y_4=1+\alpha^2x_1+x_2+\alpha^2x_3+\alpha^2x_1^2+\alpha x_1x_2+\alpha^2x_1x_3+\\ \quad \alpha^2x_1x_4+\alpha^2x_1x_5+x_2^2+\alpha^2x_2x_4+\alpha x_2x_5+x_3^2+\\ \quad \alpha^2x_3x_4+\alpha x_3x_5+\alpha^2x_4x_5+x_5^2 \end{cases}$$

私钥为(注意 pSFLASH 中的扰动可以和仿射变换合并成一个仿射变换)：

$$T^{-1}=\begin{bmatrix}\alpha^2&\alpha&\alpha^2&1&1\\0&0&\alpha^2&\alpha^2&1\\\alpha&\alpha&1&\alpha^2&1\\\alpha&\alpha^2&0&\alpha&1\\0&0&\alpha&\alpha&1\end{bmatrix}\begin{bmatrix}y_1-\alpha^2\\y_2-\alpha^2\\y_3\\y_4-1\\y_5\end{bmatrix},$$

$$T^{-1}=\begin{bmatrix}\alpha^2&1&\alpha^2&0&1\\\alpha&1&\alpha&1&\alpha\\0&\alpha^2&\alpha&\alpha&0\\\alpha&1&1&\alpha&\alpha\\0&1&0&\alpha&\alpha^2\end{bmatrix}\begin{bmatrix}y_1-1\\y_2\\y_3-\alpha^2\\y_4-\alpha^2\\y_5-\alpha^2\end{bmatrix}.$$

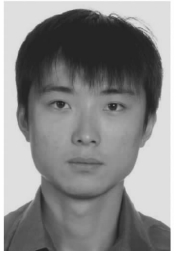
不难验证，对于消息$(\alpha^2,\alpha,\alpha^2,0,1)$的签名为$(1,1,\alpha,\alpha,\alpha)$. 对于该系统，我们可以计算相应的线性空间为$\{x\boldsymbol{N}:x\in K\}$，其中

$$\boldsymbol{N}=\begin{bmatrix}\alpha&1&\alpha^2&0&1\\1&0&\alpha&\alpha^2&1\\\alpha&\alpha&1&\alpha^2&1\\\alpha^2&\alpha&0&\alpha&0\\0&1&\alpha^2&\alpha&1\end{bmatrix}.$$

利用该矩阵，我们可以恢复公钥中缺失的多项式，从而完整的多项式组为

$$\begin{cases} y_1=\alpha x_2+x_3+x_4+x_5+\alpha x_1^2+\alpha x_1x_2+\alpha^2x_1x_3+\\ \quad \alpha x_1x_4+x_2^2+\alpha x_2x_3+\alpha x_2x_5+\alpha^2x_3^2+\alpha x_3x_4+\\ \quad \alpha x_3x_5+\alpha x_4^2+\alpha x_4x_5+x_5^2\\ y_2=\alpha+\alpha^2x_4+x_5+\alpha x_1^2+\alpha^2x_1x_3+\alpha^2x_1x_4+x_1x_5+\\ \quad x_2^2+\alpha^2x_2x_3+\alpha x_3x_4+x_4^2+\alpha^2x_4x_5+x_5^2\\ y_3=1+\alpha^2x_1+\alpha x_2+\alpha^2x_3+x_4+\alpha^2x_5+\alpha^2x_1^2+x_1x_4\\ \quad \alpha^2x_1x_5+\alpha^2x_2^2+x_2x_4+x_2x_5+\alpha^2x_3^2+\alpha x_3x_4+\\ \quad \alpha x_3x_5+\alpha^2x_4x_5+\alpha^2x_5^2\\ y_4=1+\alpha^2x_1+x_2+\alpha^2x_3+\alpha^2x_1^2+\alpha x_1x_2+\alpha^2x_1x_3+\\ \quad \alpha^2x_1x_4+\alpha^2x_1x_5+x_2^2+\alpha^2x_2x_4+\alpha x_2x_5+x_3^2+\\ \quad \alpha^2x_3x_4+\alpha x_3x_5+\alpha^2x_4x_5+x_5^2\\ y_5=\alpha^2+\alpha^2x_1+\alpha x_5+\alpha x_1^2+\alpha x_1x_2+x_1x_4+\alpha x_2^2+\\ \quad x_2x_3+x_2x_4+\alpha^2x_2x_5+\alpha x_3^2+\alpha x_3x_4+x_3x_5+\\ \quad \alpha x_5^2 \end{cases}$$

这显然是一个 MI 系统，利用线性化方程攻击机可以直接伪造签名[22].



SUN Si-Wei, born in 1985, Ph. D. candidate. His main research interests include cryptanalysis and network security.

HU Lei, born in 1967, Ph. D., professor, Ph. D. supervisor. His main research interests include information security and cryptography.

JIANG Xin, born in 1984, Ph. D.. His current research interests include information security and cryptography.

Background

Public key cryptography is an important tool for nowadays information society. Unfortunately, the security of public key schemes used in practice relies on a rather small number of problems: either factoring (RSA) or discrete logarithms (ECC). Both problems are currently considered to be hard. It is widely believed that research on new schemes based on other classes of problems is necessary. Such work provides greater diversity and hence forces cryptanalysts to spend additional effort concentrating on completely new types of problems. This way, we make sure that not all "crypto-eggs" are in one basket. To strengthen the necessity for new schemes, we want to point out that important results on the potential weaknesses of existing public key schemes are emerging. In particular techniques for factorization and solving discrete logarithm improve continually. For example, polynomial time quantum algorithms can be used to solve both problems. Therefore, the existence of quantum computers in the range of 1000 bits would be a real-world threat to

systems based on factoring or the discrete logarithm problem. This stresses the importance of research into new algorithms for asymmetric cryptography.

One proposal for secure post-quantum public key schemes is based on the NP-hard problem of solving system of multivariate equations over finite field. Such systems are called multivariate public key cryptosystem (MPKC). Recently, a new multivariate public key cryptosystem named pSFLASH is proposed by Wang by inserting a perturbation into the central map of the SFLASH cryptosystem (An efficient MPKC accepted by NESSIE which was broken by Dubois V, Fouque A and Shamir A in 2007 with algebraic differential attack). The designers of pSFLASH claim that the potential mathematical structure of the public key of SFLASH will be destroyed, if the central map is perturbed in such a way. Therefore, pSFLASH could resist the differential algebraic attack. In this paper we point out that, for every pSFLASH instance there must exist a SFLASH instance, such that the pSFASH instance can be converted into that sFLASH instance. As a result, by applying the differential algebraic attack on SFLASH, we can practically forge a valid pSFLASH signature in seconds, and the attack presented in this paper is experimentally verified.