一种侧信道攻击Rainbow签名的算法

易海博

(深圳职业技术学院计算机工程学院 广东 深圳 518055)

【摘要】Rainbow是一种数字签名方案，它基于多元多项式结构构造，属于多变量密码体系。相比现有的签名方案，如RSA和ECC方案，Rainbow的特点是能够抵御量子计算机攻击，被认为是下一代签名方案的重要候选。基于Rainbow的重要性，该文对Rainbow的硬件安全进行了分析，提出了一种基于差分能量分析和故障分析的侧信道分析算法，将Rainbow作为目标，实施侧信道攻击。实现了Rainbow签名电路，并进行功耗采集，对采集的2 000条功耗曲线进行分析和计算，获取了Rainbow所有的密钥。

关 键 词 差分能量分析; 故障分析; 多变量公钥密码; Rainbow签名; 侧信道攻击
中图分类号 TN918.4 **文献标志码** A doi:10.3969/j.issn.1001-0548.2018.06.015

An Algorithm for Side Channel Attacks on Rainbow Signature

YI Hai-bo

(School of Computer Engineering, Shenzhen Polytechnic Shenzhen Guangdong 518055)

Abstract Rainbow is a digital signature scheme. It is based on multivariate polynomials, which belongs to multivariate public key cryptography. Compared with the existing signature schemes, e.g. rivest-shamir-adleman (RSA) and ellipse curve cryptography (ECC), Rainbow can resist quantum computer attacks, which is a candidate of the signature schemes of the next generation. According to the importance of Rainbow, in this paper, we present techniques to exploit differential power analysis (DPA) and fault analysis attacks for analyzing the effectiveness of side channel attacks on Rainbow signature. We implement a naive Rainbow scheme on hardware and propose a successful side channel attack on the implementation. Experimental results show that our attack successfully obtains all the pieces from the private keys of the Rainbow scheme and they clearly demonstrate that we need to protect Rainbow against side channel attacks.

Key words differential power analysis; fault analysis; multivariate public key cryptography; Rainbow signature; side channel attack

随着量子计算机的不断发展，RSA和ECC等公钥密码面临着潜在威胁。文献[1]提出的一种在多项式时间内解决大整数因子分解和离散对数问题的量子算法表明量子计算机有能力破解RSA和ECC等公钥密码。但在公钥密码中存在少数几类密码算法不能被量子计算机攻破，它们是格密码(Lattice-based cryptography)、哈希密码(Hash-based cryptography)、基于编码的密码(code-based cryptography)以及多变量密码(MQ cryptography)[2]，被统称为后量子密码(post-quantum cryptography)。

在后量子密码中，多变量密码基于的数学困难问题是求解一组有限域上的多变量二次(multivariate quadratic, MQ)方程组，它被证明是NP(non-deterministic polynomial)困难问题，并且目前量子计算机并无较好的求解方法。多变量密码最早起源于20世纪80年代，第一种多变量密码算法是MI(Matsumoto Imai)加密算法。在数字签名算法方面，UOV(unbalanced oil-vinegar signature)、Rainbow、TTS(Tame transformation signature)等签名被认为是具有代表性的多变量签名算法[3-5]。

由于UOV、Rainbow、TTS等签名算法的抗量子计算攻击能力，它们的软件和硬件实现成为后量子密码领域研究的热点[6-12]。密码算法的硬件实现可以广泛运用于芯片领域，它除了要防御数学攻击，还同时需要防御侧信道攻击。侧信道攻击基于密码算法的硬件实现中泄露的信息进行破解，如能量消耗、电磁泄露、时间信息、声音等。相应的，常用的侧信道攻击方法包括时间攻击[13]、能量攻击[14]、电磁

收稿日期：2017－09－12；修回日期：2017－10－09
基金项目：广东省自然科学基金(2018A030310030)；广东省普通高校青年创新人才项目(2017GkQNCX059)
作者简介：易海博(1987－)，男，博士，主要从事信息安全方面的研究.

攻击[15]、故障攻击[16]等。

在侧信道攻击方法中，故障攻击的原理是尝试改变密码系统运行的环境，如电压、时钟、温度、光亮等，从而在密码运算过程中造成故障，观测相关变化，以达到破解密钥的目的。一种常用的故障攻击方法是对某一个寄存器使用激光束，导致寄存器的部分比特产生翻转，即从0变成1或从1变成0。故障攻击已经成功在攻击RSA签名中实施[17]。

能量攻击是常用的侧信道攻击方法，基于观测密码系统的能量变化而实现攻击。常用的能量攻击方法包括简单能量攻击SPA(simple power analysis)[18]和差分能量攻击DPA(differential power analysis)[19]。原始DPA(mono-bit DPA)针对寄存器单个比特进行观测，被扩展为multi-bit DPA，可以对某个中间运算结果的一组比特进行观测[20]。文献[20]对DPA进行再次扩展，即可以同时观测多个运算结果的功耗，这种方法被称为高阶DPA攻击。DPA攻击需要基于能量模型实现，如汉明重量模型和汉明距离模型[21]。一般来说，汉明距离模型更适合CMOS (complementary metal oxide semiconductor)密码系统攻击。

这些侧信道攻击方法被证明对不少对称密码系统有效，如DES(data encryption standard)、AES(advanced encryption standard)等[22]。但是，在侧信道攻击研究领域，针对多变量公钥密码进行侧信道攻击的成功例子很少，只有侧信道攻击方法[23-24]、多变量公钥密码的一种故障攻击方法[25]，且都只关注攻击理论的研究和讨论，并未涉及多变量密码的核心结构的攻击，还需要在真实环境下进一步论证。分析多变量签名算法的侧信道安全性对发现算法的漏洞，提高算法的安全性有重要价值。本文将多变量签名Rainbow作为目标，实施侧信道攻击。

1 Rainbow签名硬件实现

在多变量公钥密码中，Rainbow签名是油醋签名家族的一员，可以被看成多层的UOV签名。

1.1 Rainbow方案的选择

在Rainbow的所有安全方案中，本文选取了一种常用的方案Rainbow(10,10,4,3,10)作为硬件实现方案。它的安全级别达到2^{80}，在多项式时间内无法被数学分析攻击。Rainbow(10,10,4,3,10)由4层油醋结构组成。本文选定的Rainbow签名方案的参数如表1所示。签名生成包括第一次仿射变换、中心映射变换和第二次仿射变换，如图1所示。

表1 Rainbow签名方案

名目	内容
有限域	$GF(2^8)$
散列长度/字节	27
签名长度/字节	37
层数	4
每层的醋变量	10,20,24,27
每层的油变量	10,4,3,10
私钥	L_1, L_2, F
公钥	$L_1 \circ F \circ L_2$

假定消息的散列值是$y(y_0, y_1, \cdots, y_{26})$，它的长度是27字节，其中$y_0, y_1, \cdots, y_{26}$是GF($2^8$)的元素。而且，签名是$x(x_0, x_1, \cdots, x_{36})$，它的长度是37字节，其中$x_0, x_1, \cdots, x_{36}$是GF($2^8$)的元素。

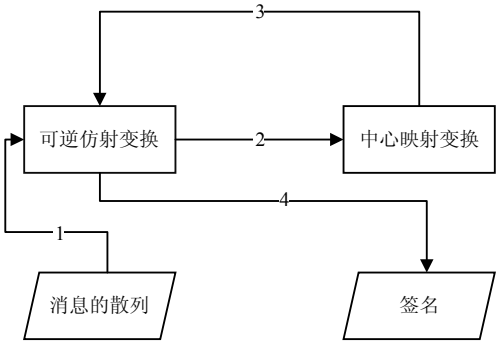

图1 Rainbow签名生成过程

为了对消息的散列值$y(y_0, y_1, \cdots, y_{26})$签名，需要进行如下计算：

$$F \circ L_2(x_0, x_1, \cdots, x_{36}) = L_1^{-1}(y_0, y_1, \cdots, y_{26})$$

式中，F是一个中心映射变换；L_1和L_2是两个可逆的仿射变换。

首先计算可逆仿射L_1的逆变换：

$$\overline{y} = L_1^{-1}(y_0, y_1, \cdots, y_{26})$$

$\overline{y}(\overline{y}_0, \overline{y}_1, \cdots, \overline{y}_{26})$是可逆仿射变换的结果，$\overline{y}$的长度是27字节。$L_1$的逆变换$L_1^{-1}$的形式为：

$$\overline{y} = \boldsymbol{A}y + \boldsymbol{b}$$

式中，$\boldsymbol{A}$是规模为27×27的矩阵；$\boldsymbol{b}$是维度为27的向量，$\boldsymbol{A}$和$\boldsymbol{b}$都被当作密钥来运算。

求解F的逆变换，$\overline{x} = F^{-1}(\overline{y}_0, \overline{y}_1, \cdots, \overline{y}_{26})$，获得$\overline{x}(\overline{x}_0, \overline{x}_1, \cdots, \overline{x}_{26})$的数值，$\overline{x}$的长度是27字节。

中心映射变换F由27个多变量多次多项式$(f_0, f_1, \cdots, f_{26})$组成，它有如下形式：

$$F(\overline{x}_0, \overline{x}_1, \cdots, \overline{x}_{36}) = (f_0, f_1, \cdots, f_{26})$$

将$\overline{y}(\overline{y}_0, \overline{y}_1, \cdots, \overline{y}_{26})$代入中心映射的变换中，它变成如下形式：

$$\overline{y}(\overline{y}_0, \overline{y}_1, \cdots, \overline{y}_{26}) = f(f_0, f_1, f_2, \cdots, f_{26})$$

中心映射F是4层的油醋结构，由27个多变量多

次多项式组成，即 $(f_0,f_1,\cdots,f_{26})$ 被分成4层：

$f_i\,|\,i=0,1,\cdots,9$，共10个多项式；

$f_i\,|\,i=10,11,12,13$，共4个多项式；

$f_i\,|\,i=14,15,16$，共3个多项式；

$f_i\,|\,i=17,18,\cdots,26$，共10个多项式。

F的27个多变量多次多项式 $(f_0,f_1,\cdots,f_{26})$ 的定义为：

$$f(O_0,O_1,\cdots,O_{26})=\sum\alpha_{ij}O_iV_j+\sum\beta_{ij}V_iV_j+\sum\gamma_iV_i+\sum\delta_iO_i+\eta$$

式中，V_i 是醋变量；O_i 是油变量；O_iV_j 是油变量和醋变量的组合；V_iV_j 是醋变量和醋变量的组合；α_{ij}、β_{ij}、γ_i、δ_i 和 η 是多变量多次多项式的系数，被当作私钥使用，η 是常数。

多变量多次多项式包括5项，最高次数不超过二次，若将醋变量的数值代入多变量多次多项式，它将变换成关于油变量的一次多项式。通过4层的多项式系数求值和求解线性方程组，计算获得 $\overline{x}(\overline{x}_0,\overline{x}_1,\cdots,\overline{x}_{36})$。

最后，将 $\overline{x}(\overline{x}_0,\overline{x}_1,\cdots,\overline{x}_{36})$ 的37个元素代入 L_2 的逆变换 L_2^{-1}，计算逆变换得 $x(x_0,x_1,x_2,\cdots,x_{36})$，$x=L_2^{-1}(\overline{x}_0,\overline{x}_1,\cdots,\overline{x}_{36})$。$L_2^{-1}$ 的形式是 $x=\boldsymbol{C}\overline{x}+\boldsymbol{d}$。这里，$\boldsymbol{C}$ 是一个规模为 37×37 的矩阵，$\boldsymbol{d}$ 是一个维度为37的向量，$\boldsymbol{C}$ 和 $\boldsymbol{d}$ 都被当作私钥来运算。所以 $x(x_0,x_1,x_2,\cdots,x_{36})$ 是 $y(y_0,y_1,\cdots,y_{26})$ 的签名。

1.2　Rainbow签名实现

为了攻击的普遍性，Rainbow签名实现基于原始方案，不采用优化手段。本文利用状态机的方式实现Rainbow签名设计，使用硬件描述语言Verilog作为编程语言，Xilinx公司开发的FPGA(field-programmable gate array)工具ISE(integrated software environment)9.1作为编程工具，实现平台选取的是Xilinx FPGA。在FPGA测试通过后，将Verilog代码加载至Synopsis Design Compiler，签名所需时间为102.8 μs，等效门数约为15 490。

Rainbow签名的仿射变换由矩阵向量乘法和向量加法组成，中心映射变换由求解线性方程组和多项式系数求值组成。

下面是有限域加法、乘法、求逆和高斯消元运算的具体实现细节。

选择的有限域是 $\mathrm{GF}(2^8)$，域的不可约多项式是 $f(x)=x^8+x^6+x^3+x^2+1$；有限域加法使用 $\mathrm{GF}(2^8)$ 的加法运算；有限域乘法使用多项式基的一般乘法。假定 $a(x)$ 和 $b(x)$ 是 $\mathrm{GF}(2^8)$ 的元素，那么 $c(x)=(a(x)\times b(x))\bmod f(x)$ 是两者的乘积，其中 $f(x)$ 是 $\mathrm{GF}(2^8)$ 的不可约多项式。计算多项式相乘的结果，即 $s_0,s_1,\cdots,s_{14}$：

$$s_0=a_0b_0$$
$$s_1=a_1b_0+a_0b_1$$
$$s_2=a_2b_0+a_1b_1+a_0b_2$$
$$s_3=a_3b_0+a_2b_1+a_1b_2+a_0b_3$$
$$s_4=a_4b_0+a_3b_1+a_2b_2+a_1b_3+a_0b_4$$
$$s_5=a_5b_0+a_4b_1+a_3b_2+a_2b_3+a_1b_4+a_0b_5$$
$$s_6=a_6b_0+a_5b_1+a_4b_2+a_3b_3+a_2b_4+a_1b_5+a_0b_6$$
$$s_7=a_7b_0+a_6b_1+a_5b_2+a_4b_3+\cdots+a_3b_4+a_2b_5+a_1b_6+a_0b_7$$
$$s_8=a_7b_1+a_6b_2+a_5b_3+a_4b_4+a_3b_5+a_2b_6+a_1b_7$$
$$s_9=a_7b_2+a_6b_3+a_5b_4+a_4b_5+a_3b_6+a_2b_7$$
$$s_{10}=a_7b_3+a_6b_4+a_5b_5+a_4b_6+a_3b_7$$
$$s_{11}=a_7b_4+a_6b_5+a_5b_6+a_4b_7$$
$$s_{12}=a_7b_5+a_6b_6+a_5b_7$$
$$s_{13}=a_7b_6+a_6b_7$$
$$s_{14}=a_7b_7$$

模运算为：

$$c_7=s_7+s_9+s_{11}+s_{12}$$
$$c_6=s_6+s_8+s_{10}+s_{11}$$
$$c_5=s_5+s_{10}+s_{11}+s_{12}+s_{14}$$
$$c_4=s_4+s_9+s_{10}+s_{11}+s_{14}+s_{14}$$
$$c_3=s_3+s_8+s_9+s_{10}+s_{12}+s_{13}+s_{14}$$
$$c_2=s_2+s_8+s_{13}+s_{14}$$
$$c_1=s_1+s_9+s_{11}+s_{13}+s_{14}$$
$$c_0=s_0+s_8+s_{10}+s_{12}+s_{13}$$

$c(x)(c_7,c_6,c_5,\cdots,c_0)$ 是 $a(x)$ 和 $b(x)$ 的乘积，本文采用了基于费马小定理的求逆方法，假定 β 是 $\mathrm{GF}(2^8)$ 的元素，求逆过程如下：

$$\beta^{-1}=\beta^{2^8-2}=\beta^{254}$$
$$2^8-2=2+2^2+2^3+2^4+2^5+2^6+2^7$$
$$\beta^{-1}=\beta^2\beta^4\beta^8\beta^{16}\beta^{32}\beta^{64}\beta^{128}$$

计算 $\beta^2,\beta^4,\beta^8,\beta^{16},\beta^{32},\beta^{64}$ 和 β^{128} 可以并行进行，β^{-1} 是它们的乘积；需要求解4个线性方程组，这些方程组的系数矩阵的规模分别是 10×10、4×4、3×3 和 10×10。本文采取有限域的高斯消元法作为求解线性方程组的方法：

在主元所在列选择一个非零元素作为主元；交换当前行与主元所在行的所有的元素，若当前行是主元所在行则不交换；对当前行所有的元素做归一操作；对当前行下面所有的元素做消元操作；结束

本次迭代，重新选取下一列开始下一轮迭代；直到所有迭代完成，系数矩阵成为一个等效的上三角矩阵；接着使用回溯替代的方法对增广矩阵进行替代；完成回溯替代后，增广矩阵的最右一列(即常数项组成的向量)是线性方程组的解。

2 Rainbow签名侧信道攻击

2.1 总体方案

现有技术中，较少对Rainbow签名进行侧信道安全性分析，在一定程度上阻碍了Rainbow签名的广泛应用。针对Rainbow的侧信道分析可以分为对仿射变换 L_1、中心映射变换 F、仿射变换 L_2 的分析。

仿射变换 L_1：差分能量分析；中心映射变换 F：故障分析结合差分能量分析；仿射变换 L_2：差分能量分析。图2对Rainbow的分析方法基于差分能量分析和故障分析。

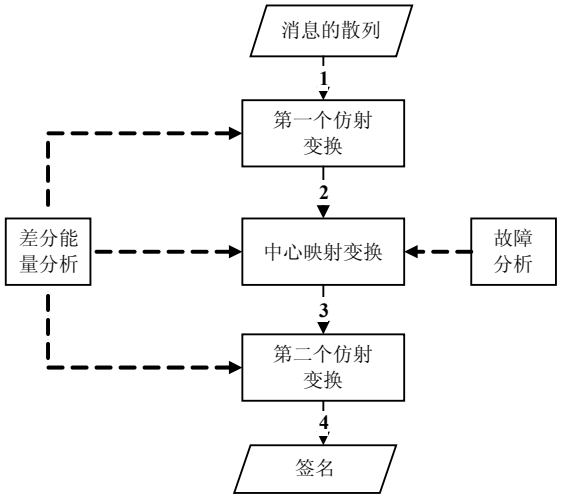

图2 Rainbow分析过程

2.2 分析第一个仿射变换

对于第一个仿射变换，采用差分能量分析。假定 $y(y_0,y_1,\cdots,y_{m-1})$ 是待签名的消息，$\overline{y}(\overline{y}_0,\overline{y}_1,\cdots,\overline{y}_{m-1})$ 是仿射变换 $\overline{y}=\boldsymbol{A}y+\boldsymbol{b}$ 的结果，$\boldsymbol{A}$ 是 $m\times m$ 的矩阵，$\boldsymbol{b}$ 是长度为 m 的向量，$\boldsymbol{A}$ 和 $\boldsymbol{b}$ 是密钥。以计算 $a'_{ij}=a_{ij}\times y_i$ 为例，a_{ij} 是 $\boldsymbol{A}$ 第 i 行第 j 列的元素(密钥)，y_i 是 y 第 i 个元素(消息)，a'_{ij} 是有限域乘法结果，均是有限域 GF(2^k) 的元素。建立基于汉明距离的多比特差分能量分析模型(以下简称汉明距离模型)，那么攻击 a_{ij} 的思路如下：

输入 N 个不同的消息，获得 N 条功耗曲线。令 $D=y_i$，$R=a'_{ij}$，$E=a_{ij}$，开始猜测密钥，范围是 GF(2^k) 所有的元素。因为 E 是密钥的猜测值(已知)，D 是消息的一个元素(已知)，R 可以通过 $R=E\times D$ 计算获得。基于 D 和 R 之间的汉明距离 $H(D\oplus R)$，把 N 条功耗曲线分成两组：

$$T_0=\{t_i,|H_i(D\oplus R)<(k/2)\}$$
$$T_1=\{t_i,|H_i(D\oplus R)\geqslant(k/2)\}$$

对于每个猜测值计算 $\Delta=\frac{\sum_{T_0}t_i}{|T_0|}-\frac{\sum_{T_1}t_i}{|T_1|}$，$|T_0|$ 和 $|T_1|$ 分别是 T_0 和 T_1 中功耗曲线的数量。Δ_i 是对应猜测值 E_i 的曲线，用 $\max_i$ 标记第 i 条曲线的最大值(绝对值)。如果 $(\max_0,\max_1,\cdots)$ 集合的最大值是 $\max_j$，那么它对应的猜测值是密钥的正确值。矩阵 $\boldsymbol{A}$ 其他的元素可以用相同的方法攻击获得。

向量 $\boldsymbol{b}$ 的攻击方法也可以采用汉明距离模型，以计算 $b'_i=y'_i+b_i$ 为例，向量 $\boldsymbol{y}'$ 是 $\boldsymbol{y}'=\boldsymbol{A}y$ 的运算结果，y'_i 是 $\boldsymbol{y}'$ 的第 i 个元素(可以计算得出)，b_i 是向量 $\boldsymbol{b}$ 的第 i 个元素(密钥)，b'_i 是有限域加法结果。攻击 b_i 的思路如下：

令 $D=y'_i$，$R=b'_i$，$E=b_i$，开始猜测密钥。因为 E 是密钥的猜测值(已知)，D 是与消息相关的运算结果(已知)，R 可以通过 $R=E\times D$ 计算。对功耗曲线进行差分运算。对于密钥的每个猜测值 E_i，计算曲线 Δ_i，用 $\max_i$ 标记第 i 条曲线的最大值。如果 $(\max_0,\max_1,\cdots)$ 集合中的最大值是 $\max_j$，则它对应的猜测值 E_j 是密钥的正确值。向量 $\boldsymbol{b}$ 其他的元素可以采用相同的方法攻击获得。

2.3 分析中心映射变换

对于中心映射变换，建立基于故障分析的模型。假定 $x_0,x_1,\cdots,x_{n-1}$ 是Rainbow在中心映射变换时需要随机生成的变量，使用强光或涡流，基于BSR(bit set or reset)方法引入故障，使这些变量固定成预设值 $c_0,c_1,\cdots,c_{n-1}$，即 $x_o\to c_0,x_1\to c_1,\cdots,x_{n-1}\to c_{n-1}$。这样，签名在每次运行时，产生的随机变量是预设值。

中心映射变换 $\overline{x}=F^{-1}(\overline{y}_0,\overline{y}_1,\cdots,\overline{y}_{m-1})$，$\overline{y}(\overline{y}_0,\overline{y}_1,\cdots,\overline{y}_{m-1})$ 是仿射变换 $\overline{y}=\boldsymbol{A}y+\boldsymbol{b}$ 的结果。中心映射 F 是由多个多变量多项式组成的方程 $\sum\alpha_{ij}V_jO_i+\sum\delta_iO_i+\sum\beta_{ij}V_iV_j+\sum\gamma_iV_i+\eta=\overline{y}_k$，将通过运算简化成关于 O 的一次多项式，O 和 V 是两类变量，α_{ij}、β_{ij}、γ_i、δ_i 和 η 是系数(密钥)。攻击思路如下：

对于密钥 α_{ij} 和运算 $V'_j=\alpha_{ij}V_j$，令 $D=V_j$，$R=V'_j$，$E=\alpha_{ij}$，通过故障攻击，将 V_j 固定为预设值，再基于 $H(D\oplus R)$ 采用汉明距离模型分析密钥；

对于密钥 δ_i 和运算 $V_j''=\alpha_{ij}V_j+\delta_i$，因为 $V_j'=\alpha_{ij}V_j$，令 $D=V_j'$，$R=V_j''$，$E=\delta_i$，通过故障攻击，将 V_j 固定为预设值，再基于 $H(D\oplus R)$ 采用汉明距离模型分析密钥；

对于密钥 β_{ij} 和运算 $V_i'=\beta_{ij}V_i$，令 $D=V_i$，$R=V_i'$，$E=\beta_{ij}$，通过故障攻击，将 V_i 固定为预设值，再基于 $H(D\oplus R)$ 采用汉明距离模型分析密钥；

对于密钥 γ_i 和运算 $V_i''=\gamma_iV_i$，令 $D=V_i$，$R=V_{ii}''$，$E=\gamma_i$，通过故障攻击，将 V_i 固定为预设值，再基于 $H(D\oplus R)$ 采用汉明距离模型分析密钥；

对于密钥 η 和运算 $\overline{y}_k'=\eta+\overline{y}_k$，令 $D=\overline{y}_k$，$R=\overline{y}_k'$，$E=\eta$，通过输入不同的消息，计算 $\overline{y}_k$ 的值，再基于 $H(D\oplus R)$ 采用汉明距离模型分析密钥。

根据上述分析，中心映射变换通过建立故障分析模型，固定随机变量，结合差分能量分析，攻击获得全部密钥。

2.4　分析第二个仿射变换

对于第二个仿射变换，采用差分能量分析。$L_2^{-1}(x_0,x_1,\cdots,x_{n-1})=(\overline{x}_0,\overline{x}_1,\cdots,\overline{x}_{n-1})$ 是第二个仿射变换，$\overline{x}(\overline{x}_0,\overline{x}_1,\cdots,\overline{x}_{n-1})$ 是中心映射变换结果，$x(x_0,x_1,\cdots,x_{n-1})$ 是签名。仿射变换 L_2 的形式是 $x=\boldsymbol{C}\overline{x}+\boldsymbol{d}$，$\boldsymbol{C}$ 是 $n\times n$ 的矩阵，$\boldsymbol{d}$ 是长度为 n 的向量，$\boldsymbol{C}$ 和 $\boldsymbol{d}$ 是密钥。

以计算 $c_{ij}'=c_{ij}\times\overline{x}_i$ 为例，c_{ij} 是 $\boldsymbol{C}$ 第 i 行第 j 列的元素(密钥)，$\overline{x}_i$ 是 $\overline{x}$ 第 i 个元素(可以计算得)，c_{ij}' 是有限域乘法结果，均是有限域 GF(2^k) 的元素。攻击 c_{ij} 的思路如下：

令 $D=\overline{x}$，$R=c_{ij}'$，$E=c_{ij}$，开始猜测密钥。因为 E 是密钥的猜测值(已知)，D 是已经计算完成的运算结果(已知)，R 可以通过 $R=E\times D$ 计算。对功耗曲线进行差分运算。对于密钥的每个猜测值 E_i，计算曲线 Δ_i，用 $\max_i$ 标记第 i 条曲线的最大值。如果 $(\max_0,\max_1,\cdots)$ 集合中的最大值是 $\max_j$，则它对应的猜测值 E_j 是密钥的正确值。矩阵 $\boldsymbol{C}$ 其他的元素可以用相同的方法攻击获得。

向量 $\boldsymbol{d}$ 的攻击方法也可以采用汉明距离模型，以计算 $d_i'=x_i'+d_i$ 为例，向量 $\boldsymbol{x}'$ 是 $\boldsymbol{x}'=\boldsymbol{C}\overline{x}$ 的运算结果，x_i' 是 $\boldsymbol{x}'$ 的第 i 个元素(可以计算得出)，d_i 是向量 $\boldsymbol{d}$ 的第 i 个元素(密钥)，d_i' 是有限域加法结果。攻击 d_i 的思路如下：

令 $D=x_i'$，$R=d_i'$，$E=d_i$，开始猜测密钥。因为 E 是密钥的猜测值(已知)，D 是与消息相关的运算结果(已知)，R 可以通过 $R=E\times D$ 计算。对功耗曲线进行差分运算。对于密钥的每个猜测值 E_i，计算曲线 Δ_i，用 $\max_i$ 标记第 i 条曲线的最大值。如果 $(\max_0,\max_1,\cdots)$ 集合中的最大值是 $\max_j$，则它对应的猜测值 E_j 是密钥的正确值。向量 $\boldsymbol{d}$ 其他的元素可以采用相同的方法攻击获得。

至此，完成了所有密钥的分析。

3　实　验

1) 依据第2节描述的Rainbow签名算法，使用Verilog编程语言实现了签名电路，通过Xilinx的FPGA EDA工具ISE软件，下载至Xilinx FPGA开发板上验证签名过程。

2) 在FPGA测试通过后，将Verilog代码加载至安装在Redhat操作系统上的Synopsis Design Compiler编译环境，编译运行。

3) 将Synopsis Design Compiler生成的电路文件加载至ModelSim(Mentor的VHDL和Verilog混合评估器)仿真，PrimeTime(Synopsys的电路功耗评估工具)评估功耗。

通过输入2 000条消息，进行Rainbow签名，使用ModelSim仿真，通过PrimeTime进行功耗采集，获得2 000条功耗曲线。然后，基于侧信道攻击模型，采用计算机集群，建立分布式功耗分析平台并分析功耗。首先，构建4个集合：功耗曲线集合、密钥运算集合、密钥时间集合、密钥猜测值集合。再基于密钥时间集合将功耗曲线集合中的曲线分成多个时间段，每个时间段应包含尽可能少的密钥运算，每个时间段的曲线各自组成一个集合；基于密钥运算集合，为每个时间段曲线集合限定参与运算的密钥；为每个密钥在密钥猜测值集合内猜测一个的值，基于汉明距离模型分析功耗，若猜测值在最后计算的曲线对应位置出现尖峰，则将该值记录为该密钥的分析结果。

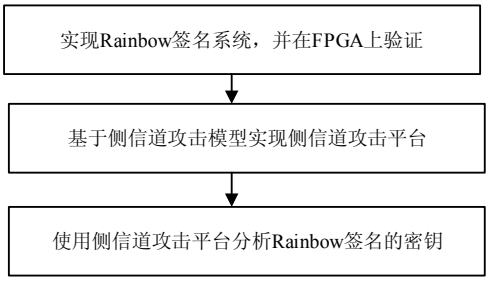

图3　实验过程

通过以上方法，使用分布式功耗分析平台分析

获得Rainbow的所有密钥的分析结果，经过验证全部正确，证明本文的实验能够完全攻破Rainbow签名。实验流程如图3所示。

4 结 束 语

本文提出了一种基于差分能量分析和故障分析的侧信道分析算法，将Rainbow作为目标，实施侧信道攻击。故障分析用于固定Rainbow的中心映射变换的随机变量，结合差分能量分析可攻击Rainbow所有的密钥。实现了Rainbow签名电路，然后使用Synopsis Prime Time进行功耗采集，对采集的2 000条功耗曲线进行分析和计算，获取了所有的密钥。实验结果表明了需要对Rainbow进行侧信道攻击保护。在未来的工作中，将设计基于掩码或隐藏的方法对Rainbow进行保护。

本文的研究工作得到了深圳市知识创新计划基础研究项目(JCYJ20170306144219159)，深圳市战略新兴和未来产业发展资金产业服务体系扶持计划项目(20170502142224600)，深圳职业技术学院校级科研项目(601722K20018)的资助，在此表示感谢！

参 考 文 献

[1] SHOR P. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM Review, 1999, 41(2): 303-332.
[2] DING J, GOWER J E, SCHMIDT D S. Multivariate public key cryptosystems[M]. Berlin: Springer, 2006.
[3] THOMAE E, WOLF C. Solving underdetermined systems of multivariate quadratic equations revisited[C]//PKC 2012. Berlin: Springer, 2012.
[4] PETZOLDT A, BULYGIN S, BUCHMANN J. Selecting parameters for the Rainbow signature scheme[C]// PQCrypto 2010. Darmstadt, Germany: Springer, 2010.
[5] MOH T. A public key system with signature and master key functions[J]. Communications in Algebra. 1999, 27(5): 2207-2222.
[6] TANG S, YI H, DING J, et al. High-speed hardware implementation of Rainbow signature on FPGAs[C]// PQCrypto 2011. Taipei, Taiwan, China: Springer, 2011.
[7] BALASUBRAMANIAN S, CARTER H W, BOGDANOV A, et al. Fast multivariate signature generation in hardware: the case of Rainbow[C]//ASAP 2008. Leuven, Belgium: IEEE, 2008.
[8] YANG B Y, CHEN J M, CHEN Y H. TTS: High-speed signatures on a low-cost smart card[C]//CHES 2004. Cambridge, MA, USA: Springer, 2004.
[9] CHEN I T, CHEN M S, CHEN T R, et al. SSE implementation of multivariate PKCs on modern x86 CPUs[C]//CHES 2009. Lausanne, Switzerland: Springer, 2009.
[10] YI H, TANG S. Very small FPGA processor for multivariate signatures[J]. Computer Journal, 2016(7): 1091-1101.
[11] BOGDANOV A, EISENBARTH T, RUPP A, et al. Time-area optimized public-key engines: MQ-cryptosystems as replacement for elliptic curves?[C]// CHES 2008. Washington, D.C. USA: Springer, 2008.
[12] YANG B Y, CHENG C M, CHEN B R, et al. Implementing minimized multivariate PKC on low-resource embedded systems[C]//SPC 2006. York, UK: Springer, 2006.
[13] KOCHER P C. Timing attacks on implementations of die-hellman, RSA, DSS, and other systems[C]//CRYPTO 96. Santa Barbara, California, USA: Springer, 1996.
[14] KOCHER P, JAE J, JUN B. Differential power analysis. [C]//CRYPTO 99. Santa Barbara, California, USA: Springer, 1999.
[15] QUISQUATER J J, SAMYDE D. Electro-magnetic analysis (EMA): Measures and countermeasures for smart cards[C]//E-smart 2001. Cannes, France: Springer, 2001.
[16] SKOROBOGATOV S P, ANDERSON R J. Optical fault induction attacks[C]//CHES 2002. Redwood Shores, CA, USA: Springer, 2002.
[17] JOYE M, LENSTRA A K, QUISQUATER J J. Chinese remaindering based cryptosystems in the presence of faults [J]. Journal of Cryptology, 1998, 12(4): 241-245.
[18] MAYER-SOMMER R. Smartly analyzing the simplicity and the power of simple power analysis on smartcards [C]//CHES 2000. MA, USA: Springer, 2000.
[19] MESSERGES T S, DABBISH E A, SLOAN R H. Examining smart-card security under the threat of power analysis attacks[J]. IEEE Transactions on Computers, 2002, 51(5): 541-552.
[20] MESSERGES T S. Using second-order power analysis to attack DPA resistant software[C]//CHES 2000. MA, USA: Springer, 2000.
[21] BRIER E, CLAVIER C, OLIVIER F. Correlation power analysis with a leakage model[C]//CHES 2004. Cambridge, MA, USA: Springer, 2004.
[22] MANGARD S, PRAMSTALLER N, OSWALD E. Successfully attacking masked AES hardware implementations[C]//CHES 2005. Edinburgh, UK: Springer, 2005.
[23] AKKAR M L, COURTOIS N T, DUTEUIL R, et al. A fast and secure implementation of SFLASH[C]//PKC 2003. Miami, FL, USA: Springer, 2003.
[24] OKEYA K, TAKAGI T, VUILLAUME C. On the importance of protecting δ in SFLASH against side channel attacks[C]//ITCC 2004. Las Vegas, Nevada, USA: IEEE, 2004.
[25] HASHIMOTO Y, TAKAGI T, SAKURAI K. General fault attacks on multivariate public key cryptosystems[C]// PQCrypto 2011. Taipei, Taiwan, China: Springer, 2011.

编 辑 漆 蓉