

RSA-CRT 密码防御算法的故障注入攻击

孔凡玉¹, 乔咏², 刘蓬涛³, 刘晓东¹, 周大水¹

(1. 山东大学网络信息安全研究所, 山东 济南 250100;

2. 中标软件有限公司, 北京 100190;

3. 山东政法学院网络空间安全学院, 山东 济南 250014)

摘要: RSA 密码是在 TLS、SSL、IPSec 等网络安全协议中广泛使用的密码算法, 其安全性至关重要。在 FDTC 2014 会议上, Rauzy 和 Guilley 提出了改进的基于中国剩余定理的 RSA 密码实现算法, 用于抵抗故障注入攻击。针对 Rauzy 和 Guilley 的两个 RSA-CRT 安全防御算法, 提出了相应的故障注入攻击方法, 在 RSA 密码运算过程中注入一个永久性错误, 并利用错误的 RSA 运算结果, 计算出 RSA 私钥。此攻击表明, Rauzy 和 Guilley 的两个 RSA 安全实现算法不能抵抗故障注入攻击。

关键词: RSA 密码; 中国剩余定理; 侧信道攻击; 故障注入攻击

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2019004

Fault-injection attack on countermeasure algorithms of RSA-CRT cryptosystem

KONG Fanyu¹, QIAO Yong², LIU Pengtao³, LIU Xiaodong¹, ZHOU Dashui¹

1. Institute of Network Security, Shandong University, Jinan 250100, China

2. China Standard Software Co., Ltd., Beijing 100190, China

3. School of Cyberspace Security, Shandong University of Political Science and Law, Jinan 250014, China

Abstract: As a widely-applied public-key cryptosystem in TLS, SSL and IPSec protocols, the security of RSA cryptosystem is of great importance. At FDTC 2014, Rauzy and Guilley proposed several improved countermeasure algorithms of RSA implementation based on Chinese remainder theorem, which were used to defeat fault-injection attacks. New fault-injection attacks on two of their countermeasure algorithms are proposed. During the RSA computation process, a permanent fault is injected and then a faulty RSA signature result is induced. The RSA private key can be obtained by using the faulty RSA signature and the correct result. Therefore, Rauzy and Guilley's two countermeasure algorithms cannot resist our fault-injection attack.

Key words: RSA cryptosystem, Chinese remainder theorem, side channel attack, fault-injection attack

收稿日期: 2018-11-28; 修回日期: 2018-12-28

通信作者: 孔凡玉, fangyukong@sdu.edu.cn

基金项目: 国家自然科学基金项目资助 (No.61602275)

Foundation Item: The National Natural Science Foundation of China (No.61602275)

论文引用格式: 孔凡玉, 乔咏, 刘蓬涛, 等. RSA-CRT 密码防御算法的故障注入攻击[J]. 网络与信息安全学报, 2019, 5(1): 30-36.
KONG F Y, QIAO Y, LIU P T, et al. Fault-injection attack on countermeasure algorithms of RSA-CRT cryptosystem [J]. Chinese Journal of Network and Information Security, 2019, 5(1): 30-36.

1 引言

自 Diffie 和 Hellman 提出第一个公钥密码体制——Diffie-Hellman 密钥协商协议^[1]以来, 公钥密码体制在数字签名、密钥协商等方面发挥了越来越重要的作用。RSA 密码算法^[2]是最早提出的几个公钥密码体制之一, 其安全性基于大整数分解困难问题, 可用于公钥加密和数字签名等功能, 是几十年以来应用最广泛的公钥密码体制之一。近年来, 基于椭圆曲线的 SM2 密码算法标准和美国的 ECDSA 数字签名标准逐渐推广, 但在 IPsec 协议、TLS/SSL 协议以及浏览器等互联网环境中, RSA 密码体制的实际应用依然很广泛, 其安全性分析非常重要。

长期以来, 密码攻击者主要从数学计算的角度分析一个密码算法的安全性, 如通过大整数分解等方法攻击 RSA 密码体制。但是, Kocher 等学者提出的侧信道攻击^[3-5]拓展了传统密码分析的思路, 能够利用密码算法实际执行时泄露的运算时间、电量消耗等信息恢复部分甚至整个秘密密钥。被动式的侧信道攻击通过测量密码运算的执行时间、电量消耗等信息分析密钥, 不影响密码运算的正常执行; 主动式的侧信道攻击则可以改变密码运算的执行过程, 使其产生对密码分析有用的信息, 故障注入攻击是一种主动式攻击方法。

Dan Boneh 首次提出了故障注入攻击^[4]的概念, 并提出了针对 RSA 密码的中国剩余定理实现 (RSA-CRT) 的攻击方法: 当其中一个模幂运算发生错误时, 可以通过错误的 RSA 签名结果恢复 RSA 私钥。Shamir^[6]通过在 RSA 运算过程中引入一个随机数 r 来判断两次模幂的结果是否存在错误, 如果检测到错误, 则只返回错误提示, 不返回错误的 RSA 签名值, 因此避免攻击者使用错误的签名值恢复私钥。Joye

等学者^[7]进一步改进、细化了 Shamir 的方法, 使用 d_p 和 d_q 替代私钥指数 d 。Aumüller 等^[8]指出, 在 Shamir 的方法中, 如果计算两次模幂的过程中不出错, 而是在中国剩余定理的结果合成运算中注入错误, 使其中一个模幂结果出错, 则仍然能够成功攻击。Yen 等^[9]详细分析了 Shamir 的方法和 Aumüller 的改进方法, 对 RSA-CRT 的故障注入攻击方法进行了系统的论述。

在 FDTC 2014 会议上, Rauzy 和 Guilley^[10]对基于检测和基于感染计算的两类故障注入防御算法进行了分析, 并提出了多个抵抗故障注入攻击的算法。2016年, Battistello 和 Giraud^[11]对 Rauzy 和 Guilley 提出的感染计算的防御算法进行了分析, 证明其不能抵抗故障注入攻击。关于 RSA-CRT 密码算法的故障注入攻击和防御措施, 可以参见相关参考文献^[12-22]。

本文针对 Rauzy 和 Guilley 提出的两个基于检测的 RSA-CRT 安全防御算法, 进行故障注入攻击, 在 RSA 密码运算过程中注入一个永久性错误, 使防御算法不能检测到错误的发生, 然后利用错误的 RSA 签名运算结果, 计算出 RSA 私钥。此攻击表明, Rauzy 和 Guilley 的 RSA 安全实现算法不能抵抗故障注入攻击。

2 RSA-CRT 密码算法和故障注入攻击

本节介绍 RSA 密码算法的中国剩余定理实现, 以及针对 RSA-CRT 实现的故障注入攻击和防御措施。

2.1 RSA 密码和中国剩余定理实现

RSA 密码算法^[2]是基于整数分解困难问题的公钥密码体制, 其公钥包括模数 N 和公钥指数 e , 其中 $N=pq$, 为了保证安全性, 要求 p 和 q 为 512 bit 以上长度的素数。RSA 密码的私钥为 p 、 q 和私钥指数 d , 满足 $e \cdot d \equiv 1 \pmod{\phi(N)}$, 其中, $\phi(N)=(p-1) \cdot$

$(q-1)$ 是欧拉函数。

RSA 加密或验证签名的过程,即计算模幂 $M^e \bmod N$; RSA 解密或签名的过程,即计算模幂 $M^d \bmod N$ 。为了提高加密和验签的速度,一般选择比较短的公钥指数 e ,如 $e=65\ 537$,私钥指数 d 是与模 N 长度相同或接近的整数, RSA 私钥运算 $S=M^d \bmod N$ 的时间复杂性为 $O(\log^3(N))$ 。

采用中国剩余定理可以提高 RSA 私钥运算的速度(简称 RSA-CRT),即先计算两个模幂 $S_p=M^{d_p} \bmod p$ 和 $S_q=M^{d_q} \bmod q$,然后组合成最后的计算结果。

$S=\text{CRT}(S_p, S_q)=S_q+((S_p-S_q)(q^{-1} \bmod p) \bmod p) \cdot q$
其中, $d_p=d \bmod (p-1)$, $d_q=d \bmod (q-1)$ 。由于素数 p 和 q 的长度为模 N 的一半,因此每次 S_p 或 S_q 的计算量约为计算 $S=M^d \bmod N$ 的 $\frac{1}{8}$,所以采用中国剩余定理能够提高约 4 倍速度。

2.2 RSA-CRT 密码的故障注入攻击

当 RSA-CRT 运算中的一个模幂运算 $S_p=M^{d_p} \bmod p$ 发生错误,即得到错误的模幂结果 S'_p ,那么最后的 RSA-CRT 运算结果为

$$S'=\text{CRT}(S'_p, S_q)=S_q+((S'_p-S_q)(q^{-1} \bmod p) \bmod p) \cdot q$$

根据 RSA-CRT 的正确运算结果 S 和错误结果 S' ,可以通过欧几里得算法计算出素数 q ,即计算^[4]

$$q=\text{GCD}((S-S') \bmod N, N)$$

或者由 RSA-CRT 的错误结果 S' ,直接计算出素数 q ,即计算

$$q=\text{GCD}((S'^e-M) \bmod N, N)$$

存在两大类抵抗故障注入攻击的 RSA-CRT 实现算法:一类是 Shamir^[6]提出的基于错误检测的方法,随机选择一个随机数 r ,用于盲化素数 p 和 q ,先计算模 pr 和 qr 的模幂,然后通过模 r 运算判断两次模幂的结果是否存在错误,

如果判断没有错误,则正常计算并返回结果 RSA 签名 S ,否则,返回计算失败;另一类是基于感染计算的方法^[12],即不管是否存在模幂运算错误,都返回 RSA 签名结果,但利用错误的 RSA 签名结果不能计算出秘密素数 p 或 q 。文献[10,17]对 RSA-CRT 密码的故障注入攻击和防御方法进行了详细论述。

3 Rauzy 等提出的 RSA-CRT 密码防御算法

Rauzy 和 Guilley 在 FDTC 2014 会议上的论文^[10]系统地分析了基于检测和基于感染计算的两类故障注入防御算法,指出这两类算法之间可以通过一定的方法相互转化。Rauzy 和 Guilley^[10]认为,基于感染计算的抵御算法比基于检测的算法更好,因为它避免了分支判断,减少了故障注入的可能性,同时提出了多个抵抗故障注入攻击的算法。但 Battistello 和 Giraud^[11]对 Rauzy 和 Guilley 提出的两个感染计算的防御算法进行了分析,表明其不能抵抗故障注入攻击。

本文主要对 Rauzy 和 Guilley 提出的基于检测的防御算法^[10]进行分析,一个被称为“一种直接的防御算法”(原文中的 Algorithm 9),另一个是改进的 Shamir 方法(原文中的 Algorithm 10)。下面分别对这两个算法进行简要描述。

3.1 一种直接的 RSA-CRT 防御算法

Rauzy 和 Guilley 提出的“一种直接的防御算法”(参考文献[10]中的 Algorithm 9)是对模幂 S_p 、 S_q 和 CRT 绑定结果均进行验证,并被证明能够抵抗一阶故障注入攻击,其算法描述如下。

算法 1 一种直接的 RSA-CRT 防御算法^[10]

输入: 消息 M , 密钥 (p, q, d_p, d_q, i_q)

输出: RSA 签名值 $M^d \bmod N$, 或返回失败

Begin

Step 1 $S_p = M^{dp \bmod \phi(p)} \bmod p$;
Step 2 if $S_p \neq M^{dp} \bmod p$ then return error;
Step 3 $S_q = M^{dq \bmod \phi(q)} \bmod q$;
Step 4 if $S_q \neq M^{dq} \bmod q$ then return error;
Step 5 $S = \text{CRT}(S_p, S_q) = S_q + q \cdot (i_q \cdot (S_p - S_q) \bmod p)$;
Step 6 if $((S \neq S_p \bmod p) \text{ or } (S \neq S_q \bmod q))$
 then return error;
Step 7 return S ;
 End

3.2 改进的 Shamir 防御算法

Rauzy 和 Guilley 提出的改进的 Shamir 方法 (参考文献[10]中的 Algorithm 10) 对原来的 Shamir 方法进行了修改, 并被认为是能够抵抗故障注入攻击, 其算法描述如下。

算法 2 RSA-CRT 实现的改进 Shamir 防御算法^[10]

输入: 消息 M , 密钥 (p, q, d_p, d_q, i_q)
 输出: RSA 签名值 $M^d \bmod N$, 或返回失败
 Begin
Step 1 选择一个小的随机数 r ;
Step 2 $p' = p \cdot r$;
Step 3 $q' = q \cdot r$;
Step 4 if $((p' \neq 0 \bmod p) \text{ or } (q' \neq 0 \bmod q))$
 then return error;
Step 5 $S'_p = M^{d \bmod \phi(p')} \bmod p'$;
Step 6 $S'_q = M^{d \bmod \phi(q')} \bmod q'$;
Step 7 if $S'_p \neq S'_q \bmod r$ then return error;
Step 8 $S_p = S'_p \bmod p$;
Step 9 $S_q = S'_q \bmod q$;
Step 10 $S = \text{CRT}(S_p, S_q) = S_q + q \cdot (i_q \cdot (S_p - S_q) \bmod p)$;
Step 11 if $((S \neq S'_p \bmod p) \text{ or } (S \neq S'_q \bmod q))$
 then return error;
Step 12 return S ;
 End

4 针对 Rauzy 等的 RSA-CRT 防御算法的攻击

Yen 等^[9]将故障注入攻击中发生的错误分为两类: 一类是暂时性的错误, 即仅在这一次运算时某个数据临时出错, 之后恢复原来的正确值; 另一类是永久性的错误, 即在某个时间点修改了某个数据后, 这个错误值将一直保持到整个 RSA 运算过程结束。对 RSA-CRT 密码算法的故障注入攻击方法, 包括在 RSA 运算过程中的哪个时间点注入错误, 以及注入的是临时性错误还是永久性错误。根据注入错误的次数, 可以分为一阶故障注入攻击、二阶故障注入攻击等, 分别表示攻击者能够在 RSA 运算过程中注入一个、两个以及更多的错误。

本文主要对 Rauzy 和 Guilley 提出的基于检测的防御算法的故障注入攻击, 采用了一阶故障注入攻击方法, 产生的是一个永久性错误, 并能够顺利通过防御算法的错误检测流程, 从而导致产生、输出一个错误的 RSA 签名结果, 以用于求解 RSA 私钥。下面分别对这两个算法的攻击方法进行描述。

4.1 对算法 1 的故障注入攻击

Rauzy 和 Guilley 提出的“一种直接的防御算法”(算法 1), 分别在 Step 2 和 Step 4 对模幂 S_p 、 S_q 结果进行错误检测, 在 Step 5 进行 CRT 组合运算, 然后在 Step 6 检测 CRT 组合运算结果是否有错误。

本文提出的故障注入攻击方法是在 Step 5 计算过程中, 对 S_p 注入一个永久性错误, 攻击方法描述如下。

攻击方法 1 针对算法 1 的故障注入攻击

输入: 消息 M , 密钥 (p, q, d_p, d_q, i_q)
 输出: RSA 签名值 $M^d \bmod N$, 或返回失败
 Begin
Step 1 $S_p = M^{dp \bmod \phi(p)} \bmod p$;
Step 2 if $S_p \neq M^{dp} \bmod p$ then return error;
Step 3 $S_q = M^{dq \bmod \phi(q)} \bmod q$;
Step 4 if $S_q \neq M^{dq} \bmod q$ then return error;
Step 5 $S = \text{CRT}(S_p, S_q) = S_q + q \cdot (i_q \cdot (S_p - S_q) \bmod p)$;
Step 6 if $((S \neq S_p \bmod p) \text{ or } (S \neq S_q \bmod q))$
 then return error;
 End

Step 2 if $S_p \neq M^{d_p} \bmod p$ then return error;
Step 3 $S_q = M^{d_q \bmod \varphi(q)} \bmod q$;
Step 4 if $S_q \neq M^{d_q} \bmod q$ then return error;
Step 5 对 S_p 注入一个永久性错误, 即将其修改为 S'_p , 计算:

$$S' = \text{CRT}(S'_p, S_q) = S_q + q \cdot (i_q \cdot (S'_p - S_q) \bmod p);$$

Step 6 if $((S' \neq S'_p \bmod p) \text{ or } (S' \neq S_q \bmod q))$ then return error;

Step 7 return S' ;

End

下面说明故障注入攻击方法 1 能够成功恢复 RSA 私钥。

首先, 本文的攻击方法不改变 Step1~Step4 的运算, 因此 Step1~Step4 能够顺利执行, 不会返回错误。然后, 在 Step 5 中, 对 S_p 注入一个永久性错误, 即将其修改为 S'_p , 并计算 $S' = \text{CRT}(S'_p, S_q)$ 。因为 S'_p 是一个永久性错误, CRT 组合运算只是按照上面的运算公式计算 S' , 其结果 S' 依然满足 $S' = S'_p \bmod p$ 和 $S' = S_q \bmod q$, 因此 Step 6 并不能检测到 S'_p 的错误, Step 7 会返回一个错误的 RSA 签名值 S' 。根据错误的 RSA 签名值 S' , 容易计算出素数 $q = \text{GCD}((S'^e - M) \bmod N, N)$, 从而恢复 RSA 私钥。

4.2 对算法 2 的故障注入攻击

Rauzy 和 Guilley 提出的改进的 Shamir 方法 (算法 2), 在 Step 4 检测 p' 和 q' 的正确性, 在 Step 7 检测模幂 S'_p 、 S'_q 的正确性, 在 Step 10 进行 CRT 组合运算, 然后在 Step 11 检测 CRT 组合运算结果是否存在错误。

本文提出的故障注入攻击方法是在 Step 8 计算过程中, 对 S'_p 注入一个永久性错误, 攻击方法描述如下。

攻击方法 2 针对算法 2 的故障注入攻击

输入: 消息 M , 密钥 (p, q, d_p, d_q, i_q)

输出: RSA 签名值 $M^d \bmod N$, 或返回失败

Begin

Step 1 选择一个小的随机数 r ;

Step 2 $p' = p \cdot r$;

Step 3 $q' = q \cdot r$;

Step 4 if $((p' \neq 0 \bmod p) \text{ or } (q' \neq 0 \bmod q))$ then return error;

Step 5 $S'_p = M^{d \bmod \varphi(p')} \bmod p'$;

Step 6 $S'_q = M^{d \bmod \varphi(q')} \bmod q'$;

Step 7 if $S'_p \neq S'_q \bmod r$ then return error;

Step 8 对 S'_p 注入一个永久性错误, 即将其修改为 S'^*_p , 计算: $S'^*_p = S'^*_p \bmod p$;

Step 9 $S_q = S'_q \bmod q$;

Step 10 $S^* = \text{CRT}(S'^*_p, S_q) = S_q + q \cdot (i_q \cdot (S'^*_p - S_q) \bmod p)$;

Step 11 if $((S^* \neq S'^*_p \bmod p) \text{ or } (S^* \neq S'_q \bmod q))$ then return error;

Step 12 return S^* ;

End

下面说明故障注入攻击方法 2 能够成功恢复 RSA 私钥。

首先, 本文的攻击方法不改变 Step1~Step7 的运算过程, 因此不会返回错误。然后, 在 Step 8 中, 对 S'_p 注入一个永久性错误, 即将其修改为 S'^*_p , 并计算出一个错误的模幂值 $S'^*_p = S'^*_p \bmod p$ 。在 Step 10 中, CRT 组合运算将错误的模幂 S'^*_p 和正确的模幂 S_q 进行组合计算, 得到错误的 S^* 。因为在 Step 8 中, S'^*_p 是由 S'_p 模 p 计算出来的, 因此 Step 11 中的 S^* 满足 $S^* = S'^*_p \bmod p$ 和 $S^* = S'_q \bmod q$ 。所以, Step 12 会返回一个错误的 RSA 签名值 S^* 。根据错误的 RSA 签名值 S^* , 容易计算出素数 $q = \text{GCD}((S'^*_e - M) \bmod N, N)$, 从而恢复 RSA 私钥。

不管在硬件还是软件实现中, S_p 和 S'_p 等大整数都是以数组的形式存储在内存或寄存器中, 如在 Intel CPU 中, 可以是以 32 或 64 比特为单

位的数组进行存储。所以,本文提出的故障注入攻击,只要对 S_p 和 S'_p 等数据的某一个 32 或 64 比特存储单位进行修改,就可以实现相应的故障注入攻击。

5 结束语

故障注入攻击等侧信道攻击方法表明,一个密码算法的正确、安全实现与其安全性密切相关。针对 RSA-CRT 密码实现的故障注入攻击是一种很强大的攻击技术,仅需要一次模幂出现错误即可攻击成功,因此必须采用安全的实现算法以抵抗故障注入攻击。

本文对 Rauzy 和 Guilley 提出的两个故障注入攻击算法进行了分析,提出了一阶故障注入攻击算法,表明这两个算法不能抵抗故障注入攻击。如何在抵抗故障注入攻击的同时,提高 RSA-CRT 密码实现的速度,并分析在手机、物联网、车联网等移动环境下的实际攻击技术,是下一步需要研究的方向。

参考文献:

- [1] DIFFIE W, HELLMAN M E. New directions in cryptography[J]. IEEE Trans Inform Theory, 1976, 22(6): 644-654.
- [2] RIVEST R L, SHAMIR A, ADLEMAN M. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120-126.
- [3] KOCHER P. Timing attacks on implementations of Diffie-Hellmann, RSA, DSS, and other systems[C]//Advances in Cryptology-CRYPTO'96. 1996: 104-113.
- [4] BONEH D, DEMILLO R A, LIPTON R J. On the importance of checking cryptographic protocols for faults[C]//Advances in Cryptology - EUROCRYPT 1997. 1997: 37-51.
- [5] KOCHER P, JAFFE J, JUN B. Differential power analysis[C]//Advances in Cryptology - CRYPTO'99. 1999: 388-397.
- [6] SHAMIR A. Method and apparatus for protecting public key schemes from timing and fault attacks [P]. 1999.
- [7] JOYE M, PAILLER P, YEN S M. Secure evaluation of modular functions[C]//2001 International Workshop on Cryptology and Network Security. 2001: 227-229.
- [8] AUMÜLLER C, BIER P, FISCHER W, et al. Fault attacks on RSA with CRT: concrete results and practical countermeasures [C]//Cryptographic Hardware and Embedded Systems-CHES 2002. 2002: 260-275.
- [9] YEN S M, MOON S J, HA J. Hardware fault attack on RSA with CRT revisited[C]//Information Security and Cryptology-ICISC 2002. 2002: 374-388.
- [10] RAUZY P, GUILLEY S. Countermeasures against high-order fault-injection attacks on CRT-RSA [C]//Fault Diagnosis and Tolerance in Cryptography 2014. 2014: 68-82.
- [11] BATTISTELLO A, GIRAUD C. Lost in translation: fault analysis of infective security proofs[C]//The Workshop on Fault Diagnosis & Tolerance in Cryptography. 2016: 45-53.
- [12] YEN S M, KIM S, LIM S, et al. Moon. RSA speedup with Chinese remainder theorem immune against hardware fault cryptanalysis[J]. IEEE Transactions on Computers, 2003, 52(4): 461-472.
- [13] YEN S M, KIM D, MOON S. Cryptanalysis of two protocols for RSA with CRT based on fault infection[C]//Fault Diagnosis and Tolerance in Cryptography 2006. 2006: 53-61.
- [14] WAGNER D. Cryptanalysis of a provably secure CRT-RSA algorithm[C]//ACM Conference on Computer and Communications Security 2004. 2004: 92-97.
- [15] GIRAUD C. An RSA implementation resistant to fault attacks and to simple power analysis[J]. IEEE Transactions on Computers, 2006, 55(9): 1116-1120.
- [16] VIGILANT D. RSA with CRT: a new cost-effective solution to thwart fault attacks[C]//Cryptographic Hardware and Embedded Systems - CHES 2008. 2008: 130-145.
- [17] JOYE M, TUNSTALL M. Fault analysis in cryptography[M]. Berlin Heidelberg: Springer, 2012.
- [18] LEE S, CHOI D, CHOI Y. Improved Shamir's CRT-RSA algorithm: revisit with the modulus chaining method [J]. ETRI Journal, 2014, 36.3: 469-478.
- [19] 王红胜, 纪道刚, 张阳, 等. 针对 RSA-CRT 数字签名的光故障攻击研究[J]. 电子设计工程, 2015, 23(6): 12-5.
WANG H S, JI D G, ZHANG Y, et al. Optical fault attack on RSA-CRT signatures[J]. Electronic Design Engineering, 2015, 23(6): 12-15.
- [20] 李增局. 一种关于 CRT-RSA 算法的差分错误注入攻击[J]. 密码学报, 2016, 3(6): 546-554.
LI Z J. Differential fault attack on CRT-RSA [J]. Journal of Cryptologic Research, 2016, 3(6): 546-554.
- [21] KISS A, KRMER J, RAUZY P, et al. Algorithmic countermeasures against fault attacks and power analysis for RSA-CRT [C]//Intern-

tional Workshop on Constructive Side-Channel Analysis and Secure Design. 2016: 111-129.

- [22] KONG F, ZHOU D S, JIANG Y L, et al. Fault attack on an improved CRT-RSA algorithm with the modulus chaining method [C]//International Conference on Computational Science and Engineering (CSE) 2017. 2017: 866-869.

[作者简介]



孔凡玉 (1978-), 男, 山东莱芜人, 博士, 山东大学副教授, 主要研究方向为密码学与信息安全。



刘蓬涛 (1980-), 女, 山东蓬莱人, 山东政法学院副教授, 主要研究方向为密码学。



刘晓东 (1975-), 男, 山东寿光人, 博士, 山东大学讲师, 主要研究方向为密码学。



乔咏 (1977-), 男, 北京人, 中标软件有限公司高级工程师, 主要研究方向为系统与软件安全。



周大水 (1963-), 男, 山东潍坊人, 山东大学教授, 主要研究方向为网络系统安全。