一种基于模板的RSA-CRT模约减攻击方法

马向亮[1,3],乌力吉[1,2*],王 宏[4],张向民[1,2],黄克振[5],刘玉岭[6,7]

(1. 清华大学集成电路学院,北京 100084;2. 清华大学北京信息科学与技术国家研究中心,北京 100084;3. 北京邮电大学集成电路学院,北京 100876;4. 国家信息技术安全研究中心,北京 100084;5. 中国科学院软件研究所可信计算与信息保障实验室,北京 100190;6. 中国科学院信息工程研究所,北京 100093;7. 中国科学院大学网络安全学院,北京 101408)

摘 要: 目前针对RSA-CRT的建模类攻击研究较少,本文以模约减操作为研究对象,提出了一种针对RSA-CRT实现的模板攻击方法. 该方法的核心是解决了如何由模约减后中间值的汉明重量恢复RSA-CRT私钥的难题. 该方法的特点是基于模约减后中间值的汉明重量模型建模,通过采集选择密文模约减的能量迹进行模板匹配获取模约减后中间值的汉明重量,由汉明重量变化值恢复中间值,进一步恢复RSA-CRT算法的私钥. 另外,该方法的优点在于理想情况下,基于中间值汉明重量模型建立的模板之间可以共用,且对中间值以多少位大小建模没有限制,可以选择字节大小,64位大小,甚至私钥p相同大小,实际环境中可根据泄露信息情况进行选取. 最后,本文选择对中间值的最低字节进行建模,验证了该方法的可行性,并给出了防护建议.

关键词: 模板攻击;RSA-CRT;选择密文;模约减;侧信道攻击

中图分类号: TP309.1 **文献标识码:** A **文章编号:** 0372-2112(2024)03-0689-07

电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20220175

An Attack Method Against the Modular Reduction Within a RSA-CRT Implementation Based on Template Attack

MA Xiang-liang[1,3], WU Li-ji[1,2*], WANG Hong[4], ZHANG Xiang-min[1,2], HUANG Ke-zhen[5], LIU Yu-ling[6,7]

(1. *School of Integrated Circuits, Tsinghua University, Beijing* 100084, *China*;
2. *Beijing National Research Center for Information Science and Technology, Tsinghua University, Beijing* 100084, *China*;
3. *School of Integrated Circuits, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*;
4. *National Research Center for Information Technology Security, Beijing* 100084, *China*;
5. *Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences, Beijing* 100190, *China*;
6. *Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093, *China*;
7. *School of Cyber Security, University of Chinese Academy of Sciences, Beijing* 101408, *China*)

Abstract: At present, there are few researches on profile attacks against RSA-CRT implementation. This paper takes modular reduction operation as the research object, and a template attack method against RSA-CRT implementation is proposed. The core of this method is to solve the difficulty to recover the RSA-CRT private key from the Hamming weight of the intermediate value of ciphertext modular reduction. The characteristic of this method is to build a model based on the Hamming weight of the intermediate value derived from modular reduction. The Hamming weight can be obtained by collecting the power traces of chosen ciphertext modular reduction for template matching, and the intermediate value is recovered from the Hamming weight variation, the private key of the RSA-CRT algorithm can be further inferred based on the intermediate value. In addition, the advantage of this method is that ideally, templates based on the intermediate Hamming weight model can be shared, and there is no limit on the number of bits of the intermediate value for modelling, which can be in byte size, 64 bit size, or even the bit size of p. In the actual environment, it can be selected according to the leaked information. Finally, in this paper, the lowest byte of the intermediate value is selected to model to verify the feasibility of this method, and the defense suggestions are also provided.

Key words: template attack; RSA-CRT; chosen-ciphertext; modular reduction; side channel attack

收稿日期:2022-02-15;修回日期:2022-04-25;责任编辑:梅志强

*通讯作者:乌力吉

1 引 言

Kocher 等研究者创新性地提出了差分能量分析[1],开创了能量分析攻击这一研究领域. 能量分析攻击[2]利用密码设备泄露的能量消耗信息进行攻击,是最常用的一种攻击方式. 能量分析攻击主要分为两类,一类是建模类攻击,如模板攻击[3,4],另一类是非建模类攻击,如相关能量分析[5~7]. 其中,模板攻击成立的前提是能量消耗依赖于正在处理的数据. 使用模板攻击一般需要两个步骤,其一是使用多元正态分布对已拥有权限的训练设备采集的能量迹的特征进行刻画;其二是使用目标设备的能量迹进行匹配恢复算法使用的密钥. 由于模板攻击具有极强的现实威胁性,分析者对其进行了深入研究,并将其用于破解各种密码算法工程实现,恢复密码算法使用的密钥. 到目前为止,模板攻击的密码算法涵盖了SM4、DES和AES算法等,但尚没有基于模板的RSA[8]算法模约减攻击.

RSA算法是一种被广泛应用的公钥密码算法,对其进行能量分析攻击一直是分析者研究的热点. Messees等分析者提出了针对模幂运算的三种差分能量攻击方法[9]:单指数多数据、多指数单数据和零指数多数据攻击,并分析了这三种方法的使用条件. Novak通过判断Garner重组运算中模p运算中是否执行加p运算,提出了选择可适应密文的简单能量分析攻击[10]. Yen等分析者提出了一种选择明文的简单能量分析攻击方法[11],当k是奇数时,计算$(n-1)^k \equiv n-1 (\mathrm{mod}\, n)$. 当$k$是偶数时,计算$(n-1)^{2\times\frac{k}{2}} \equiv 1 (\mathrm{mod}\, n)$,通过观察能量迹中的能量消耗信息可以直接获得RSA算法使用的私钥. Witteman利用了RSA-CRT重组运算中近似相等关系,提出了逐字节猜测素数p或q的能量分析攻击方法[12]. Witteman等分析者针对RSA-CRT带有能量消耗分支平衡算法防御措施的快速实现方式[13],提出了一种恢复密钥的能量分析攻击方法. Coppersmith提出了针对RSA的因子分解定理[14],如果能够获取p或q的低部分$\frac{1}{4}\times\log_2 n$位信息,那么可以直接恢复出$p$和$q$,但是目前并没有相关研究者在该条件下成功恢复出$p$和$q$值. 有许多研究者提出了已知$p$某些比特恢复$p$的实现方法[15~18],其中2021年Millera等研究者提出了一种减少格的维度和矩阵大小的方法[19],使得恢复RSA算法的密钥时间更少,速度更快.

目前,已发表的针对RSA-CRT模约减攻击都采用了相关能量分析与选择密文相结合的方式. 在一些场景中,通常可以获取模约减后的汉明重量值的一些信息,如何由汉明重量值恢复RSA-CRT算法的私钥是一个难题. 在本文中,我们提出了一种基于模板的模约减攻击方法,解决了如何由模约减后中间值的汉明重量恢复私钥的难题,并且提出了一种RSA-CRT私钥恢复算法.

2 相关工作

RSA-CRT运算包括模约减、模幂和重组三部分. 由于RSA-CRT公钥算法的特点,针对其进行模板攻击的研究较少. 许森等研究者针对RSA-CRT的重组部分提出了相似操作模板攻击方法[20],该方法主要是利用重组输出的已知数据和能量迹进行建模,然后对相同的能量迹中的相似操作部分进行匹配恢复未知数据. 此外,还有一些研究者针对RSA的密钥生成部分提出了不同的模板攻击方法[21,22].

由于模约减运算的复杂性,现有的攻击方法都采用了与选择密文相结合的方式,主要分为两类:第一种为等距离输入攻击[23,24]或单字节随机攻击;第二种则使用形如$n-k$的随机数据作为密文进行攻击[25,26],k为p的长度. 第一种方法通过选择随机密文c,将中间值$r=c \bmod p$作为相关能量分析攻击目标,采用从低到高逐字节攻击的方式,每次恢复中间值r的一个字节,直到逼近或恢复出完整的r,最后由r恢复出RSA-CRT的私钥p.

第二种方法为选择密文形如$c=n-x$的随机密文,其中随机密文x小于p,中间值$r=n-x(\mathrm{mod}\, p)=p-x$,因此该方法可以使用相关能量分析逐字节恢复私钥$p$. 与第一种方法相比,第二种方法直接恢复的是私钥$p$的某个字节,而且只需要采集一次能量迹即可,且恢复其他字节可以共用相同的能量迹,但每次使用能量迹不同位置的能量消耗.

3 RSA-CRT

RSA是一种被广泛应用的公钥密码算法,它的安全性依赖于大整数因子分解数学难题. RSA算法密钥可分为公钥(e, n)和私钥(p,q,d)两部分,且满足等式$n=p\times q$,$ed \equiv 1 \bmod (p-1)(q-1)$. 使用RSA算法对密文$c$进行解密运算对应于计算模幂$m=c^d \bmod n$.

RSA-CRT是一种利用中国剩余定理(Chinese Remainder Theorem, CRT)加速RSA运算的方法. RSA-CRT的实现可以分为模约减、模幂和重组三部分,如算法1所示. RSA-CRT模幂运算的操作数长度已降低为原来的一半,实现效率提升近4倍,因此在实际应用中,各设计工程师优先使用RSA-CRT算法,特别是在计算及存储资源有限的密码设备中.

4 一种基于模板的RSA-CRT模约减攻击方法

如算法1所示,其第2步计算$c_p=c \bmod p$和$c_q=$

$c \bmod q$ 即为模约减操作,其中 c 为密文,p、q 为RSA-CRT的私钥. 选择密文攻击是一种攻击模式,攻击者可按照其需要,对任意选择的输入执行密码运算,从中获取相关信息进行密码分析. 选择密文攻击可与其他密码分析技术相结合,以提升攻击效果. 本节介绍一种针对该操作的基于模板的攻击方法,通过选择密文,获取模约减后中间值 c_p 或 c_q 的汉明重量,最后由汉明重量变化值恢复出RSA-CRT的私钥.

算法1 RSA-CRT

输入:n, p, q, c

输出:$m = c^d \bmod n$

1. 预计算 $d_p = d \bmod (p-1)$ 和 $d_q = d \bmod (q-1)$;
2. 计算 $c_p = c \bmod p$ 和 $c_q = c \bmod q$;
3. 计算 $i_q = q^{-1} \bmod p$;
4. 计算 $m_p = c_p^{d_p} \bmod p$;
5. 计算 $m_q = c_q^{d_q} \bmod q$;
6. 计算 $m = m_q + q(q^{-1}(m_p - m_q) \bmod p)$;
7. 得出 m.

4.1 RSA-CRT密钥恢复方法

在RSA-CRT算法实现的第2步就是密文 c 模 p 的约减操作,之前的相关分析者针对该操作提出了一些分析方法,其中之一是通过能量分析与密文相结合恢复约减操作中间值 r,但在一些场景中,由侧信道的相关攻击方法并不能直接得到 r,而是得到 r 的一部分信息,比如 r 的汉明重量值. 本小节重点介绍如获取约减操作后中间值 r 的汉明重量,如何进行分析推理得到私钥 p,进而分解 n,得到 q.

通常在已知 r 情况下,可以直接求解其汉明重量值,但反过来则不能逆向求解出唯一的 r,这是由于汉明重量到 r 之间的映射关系不是单射. 在侧信道攻击中,由分而治之思想,通常可以获取 r 的逐比特、逐字节或更多位汉明重量值,获取多少位汉明重量值取决于CPU或专用IC计算时侧信道泄露信息的情况. 如果是逐比特汉明重量已知,那么相当于直接得到 r,但实际环境中通常不符合逐比特泄露的场景. 接下来本文介绍中间值 r 的逐字节汉明重量已知情况下如何恢复RSA-CRT私钥 p 的方法.

选取已知固定密文 c,由于 $r = c \bmod p$,如果得出 r,则通过计算 $p = \gcd(c - r, n)$ 可以恢复 p. 假设通过侧信道可以逐字节获取 r 的汉明重量,r 以字节为基表示为 $r = r_{k-1} | r_{k-2} | \cdots | r_1 | r_0$,如果 r 等于0,则 $p = \gcd(c, n)$,否则首先考虑恢复 r 的最低字节 r_0. 选择计算 $c - 1 (\bmod p) = r - 1$,通过穷举 r_0 从低到高第一个为1的各种情况,如表1所示,x 表示未知数0或1. 本文通过密文 c 采集的能量消耗进行模板匹配得到原 r_0 值的汉明重量,然后选择密文 $c-1$ 模板匹配得到现 r_0 值的汉明重量,进一步可以求出这两个汉明重量变化值,通过查表1可以得出第1个为1的置位. 如选择密文 $c-1$ 后汉明重量增加4,则可以确定原 r_0 值为 $xx10000$. 类似的方法,对 r_0 的其他比特值进行恢复,通过选择密文 $c - 1 \times 2^i$ 确定第2个为1的位置,直到得出 r_0 值,其中 $i-1$ 为最近恢复1的位置.

表1　中间值 r_0 汉明重量变化表

原 r_0 值	选择密文	现 r_0 值	汉明重量变化
$xxxxxxx1$	$c-1$	$xxxxxxx0$	–1
$xxxxxx10$	$c-1$	$xxxxxx01$	0
$xxxxx100$	$c-1$	$xxxxx011$	1
$xxxx1000$	$c-1$	$xxxx0111$	2
$xxx10000$	$c-1$	$xxx01111$	3
$xx100000$	$c-1$	$xx011111$	4
$x1000000$	$c-1$	$x0111111$	5
10000000	$c-1$	01111111	6
00000000	$c-1$	11111111	8

由表1分析可以得出,恢复一个字节,如每个字节的每个比特位都是1,最多需要匹配8次能量迹. 理想情况下,假设RSA-CRT私钥 p 的位数为512位,则恢复每个字节需要8次能量迹匹配,恢复 r 最多需要选择密文对应的512次能量迹匹配,加上固定密文 c 匹配对应的能量迹,最多需要匹配513次能量迹. 实际环境中每一次匹配可能需要多条能量迹,甚至上万条能量迹.

4.2 提升的RSA-CRT密钥恢复方法

由于每个选择密文对应的能量迹仅用于恢复 r 的某一个比特位为1的位置,且不能用于恢复 r 的其他字节或比特,使得能量迹的使用效率较低,这是由于能量分析攻击可以使用能量迹上的不同能量消耗值恢复密钥的不同比特. 本节将使用能量迹上的不同能量消耗值恢复中间值 r,减少RSA-CRT模约减模板攻击密钥恢复能量迹数量.

由于每次选择密文都是逐次减1,限制了选择中间值的变化,因此在选择密文时,使用 $c - 1 - \cdots - 1 \times 2^{63 \times 8} (\bmod p) = (r_{63} - 1) | (r_{62} - 1) | \cdots | (r_0 - 1)$ 代替原先 $c - 1 (\bmod p) = r - 1$. 显然当 $r_{i-1} - 1$ 不需要借位时,每个字节之间相互独立,可以通过汉明重量变化查找表1得出. 进一步分析可以得出,恢复 r 的最低字节没有变化,仍然可以按照原方法通过汉明重量变化查找表1得出. 当要恢复的字节 r_{i-1} 的 j 位数至最高位为0时,$r_{i-1,j} - 1 \times 2^j$ 需要从 r_i 字节借位,这时会影响 r_i 中的汉

明重量变化. 由于带有借位最小的选择密文等于r_i-2,并不改变r_i的最低位值,这种情况无法直接确定最低位值. 因此本方法首先分别使用原方法确定每个字节的最低位是否为1. 如某个字节最低位确定结果为1. 通过密文c采集的能量消耗进行模板匹配得到原r_i值的汉明重量,选择密文$c-2^{i\times 8+1}-2^{i\times 8}$模板匹配得到现$r_i$值(原$r_i$–3)的汉明重量,进一步可以求出这两个汉明重量变化值,通过查表2可以得出第2个为1的置位. 类似的方法,对r_i的其他比特值进行恢复,通过选择密文$c-2^{i\times 8+j}$确定第3个为1的位置,直到得出r_i值,其中$j-1$为最近恢复1的位置,直到该字节中间值确定.

表2 r_i最低位为1的带借位汉明重量变化表

原r_i值	选择密文	现r_i值(原r_i-3)	汉明重量变化
*xxxxxx*11	$c-2^{i\times 8+1}-2^{i\times 8}$	*xxxxxx*00	–2
*xxxxx*101	$c-2^{i\times 8+1}-2^{i\times 8}$	*xxxxx*010	–1
*xxxx*1001	$c-2^{i\times 8+1}-2^{i\times 8}$	*xxxx*0110	0
*xxx*10001	$c-2^{i\times 8+1}-2^{i\times 8}$	*xxx*01110	1
*xx*100001	$c-2^{i\times 8+1}-2^{i\times 8}$	*xx*011110	2
*x*1000001	$c-2^{i\times 8+1}-2^{i\times 8}$	*x*0111110	3
10000001	$c-2^{i\times 8+1}-2^{i\times 8}$	01111110	4
00000001	$c-2^{i\times 8+1}-2^{i\times 8}$	11111110	6

如某个字节最低位确定结果0,通过密文c采集的能量消耗进行模板匹配得到原r_i值的汉明重量,选择密文$c-2^{i\times 8+1}$模板匹配得到现值(原r_i-2)的汉明重量,进一步可以求出这两个汉明重量变化值,通过查表3可以得出第1个为1的位置. 类似的方法,对r_i的其他比特值进行恢复,通过选择密文$c-2^{i\times 8+j}$确定第2个为1的位置,直到得出r_i值,其中$j-1$为最近恢复1的位置,直到该字节中间值确定.

在以上分析基础上,假设RSA-CRT私钥p的位数为512位,加上固定密文c对应的能量迹匹配. 理想情况下,最多需要64+7+1=72次能量迹匹配. 与原方法一样,实际环境中每一次匹配可能需要多条能量迹,甚至上万条能量迹.

表3 r_i最低位为0的带借位汉明重量变化表

原r_i值	选择密文	现r_i值(原r_i-3)	汉明重量变化
*xxxxxx*10	$c-2^{i\times 8+1}$	*xxxxxx*00	–1
*xxxxx*100	$c-2^{i\times 8+1}$	*xxxxx*010	0
*xxxx*1000	$c-2^{i\times 8+1}$	*xxxx*0110	1
*xxx*10000	$c-2^{i\times 8+1}$	*xxx*01110	2
*xx*100000	$c-2^{i\times 8+1}$	*xx*011110	3
*x*1000000	$c-2^{i\times 8+1}$	*x*0111110	4
10000000	$c-2^{i\times 8+1}$	01111110	5
00000000	$c-2^{i\times 8+1}$	11111110	7

由上面介绍的已知中间值的每个字节汉明重量变化恢复中间值r的方法可知,如果可以得到中间值r每64位的汉明重量变化值,那么该方法仍然适合,而且理想情况下不超过72次能量迹匹配. 如果直接得到中间值r的汉明重量变化值,那么该方法仍然适合,而且理想情况下需要512+1=513次能量迹匹配. 该情况类似于逐比特恢复,但由于实际环境中r的每位不可能全是1,因此需要的能量迹匹配明显小于513.

综上,与原方法相比,提升的方法虽然减少了能量迹的采集次数,但是每次需要计算选择密文较复杂,容易出错,原方法相对更直接简单,但需要较多采集和匹配能量迹次数. 如上分析,该攻击方法可行的一个主要特点是选择密文攻击,因此设计者可以在工程实现中使用底数进行随机数乘法掩码进行防护. 当进行$c \bmod p$操作时,进行运算的密文c由c乘以随机数R替换,而不是最初选择的密文c,因此该防御措施使得攻击者无法选择密文进行攻击,以达到有效防护的效果. 但为了保证算法的结果正确性,需要在后面进行脱掩操作,这会增加性能方面的开销.

5 实验验证

在第4节基于模板的RSA-CRT模约减攻击方法基础上,本节进行基于模板攻击的RSA-CRT实现模约减攻击验证实验. 本实验对象是基于自制的ARM开发板,主芯片采用STM32F405RGT6芯片,该芯片基于ARM Cortex-M4内核,32位CPU,168 MHz主频. 本实验使用电磁探头采集芯片处理$c \bmod p$作的能量消耗,选用的探头是LANGER RF-B,选用的示波器是Lecroy 9104. 本实验选择最低字节的汉明重量建模,并且每个字节都复用该模板进行匹配. 结果表明,该方法成功恢复出了RSA-CRT私钥p,验证了该方法的可行性.

本实验第1步选取了60 000个随机明文,并使用示波器分别采集芯片处理$c \bmod p$操作的能量消耗,采样率设置为10 GS/s,每次采集10万个点,如图1所示. 第2步将采集的能量迹进行滤波、对齐预处理. 第3步本实验在泄露位置附近选择5个兴趣点. 第4步将$r=c \bmod p$中间值相同的汉明重量值对应的能量迹分为一组. 第5步计算每组能量迹的均值向量和协方差矩阵建模. 第6步通过第4节选择密文,每条密文重复1 000次并分别采集对应的能量迹,并进行模板匹配,匹配结果会得到64个比较高的概率值. 第7步由匹配出的汉

明重量值计算变化值,得出中间值r然后计算私钥p,并验证p的正确性.

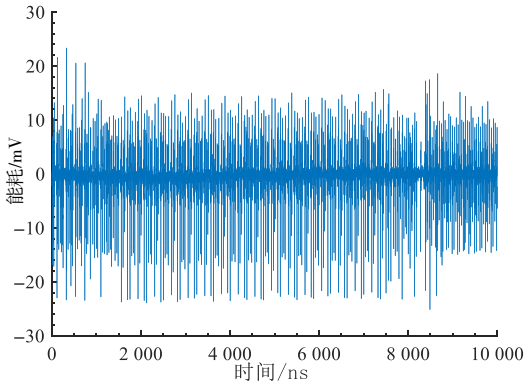


图1　RSA-CRT模约减操作能量迹

由于篇幅限制,本文仅介绍一个选择密文的实验模板匹配过程图. 中间值r大小为64字节,能量迹模板匹配结果的最高16字节汉明重量如图2所示,横轴表示采样时间,纵轴表示模板匹配的概率,并且图中使用不同的线型分别绘制了不同汉明重量模板对应的匹配概率. 通过分析可以得出,该能量迹中存在16个明显的尖峰,分别对应着16个字节的泄露时刻,而且每个尖峰处的最高概率值对应匹配9个模板的某一个汉明重量,即r在该字节处的汉明重量值.

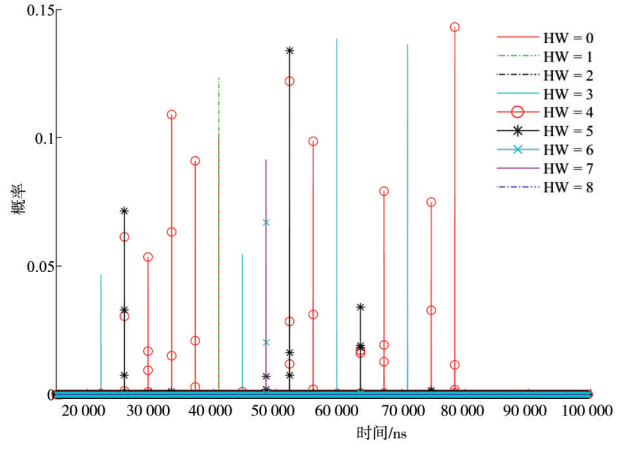


图2　能量迹模板匹配结果的高16字节汉明重量

进一步,由模板攻击相关理论得出,最高字节的汉明重量为模板匹配最高概率对应的汉明重量值,如图3所示. 其他字节分析类似不再赘述,能量迹模板匹配的32~48字节见图4,16~32字节见图5,最低16字节见图6.

由上面实验过程可以得出选择密文模约减后中间值的每个字节对应的汉明重量,将每个汉明重量与

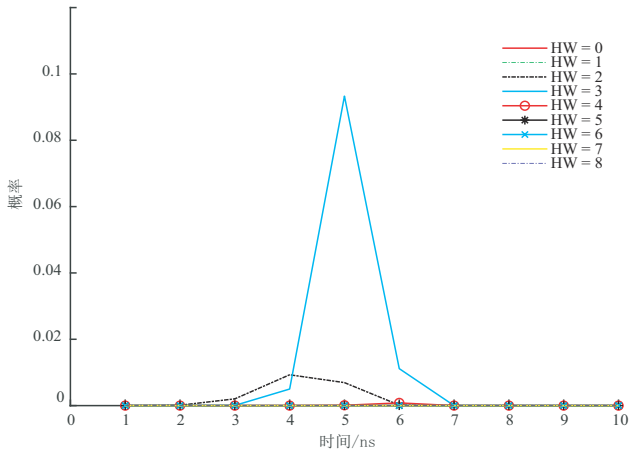


图3　能量迹模板匹配结果的最高字节汉明重量

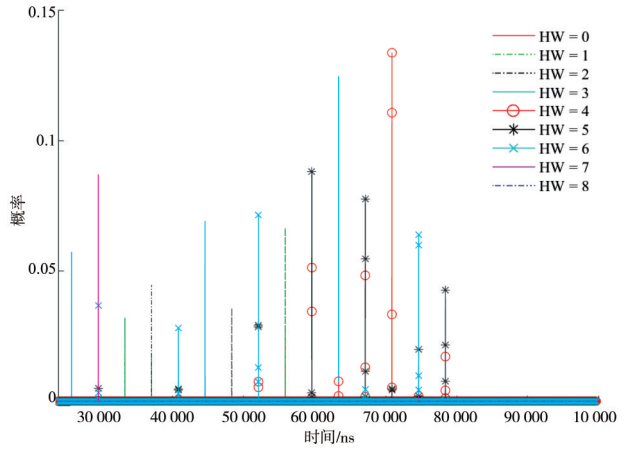


图4　能量迹模板匹配结果的32~48字节汉明重量

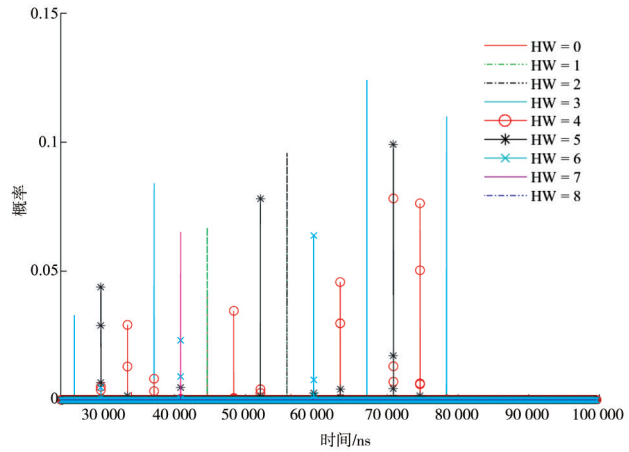


图5　能量迹模板匹配结果的16~32字节汉明重量

实际中间值的汉明重量相比,可以得出所有的汉明重量已全部正确恢复,因此可以进一步进行密钥恢复,验证了该方法的可行性. 实际中如果有两个字节匹配结果相近,那么需要增加条数,保证匹配结果的正确性.

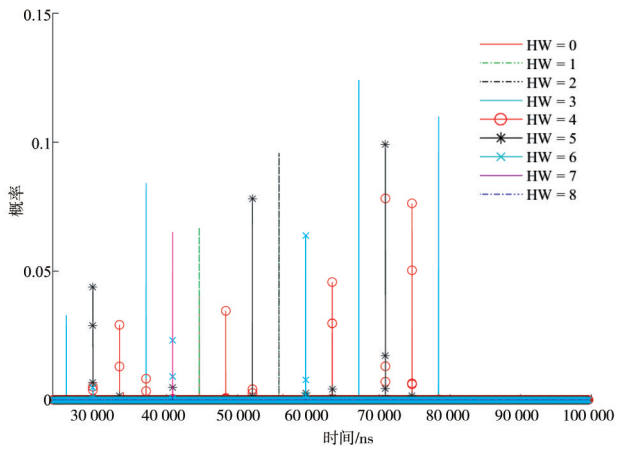


图6 能量迹模板匹配结果的低16字节汉明重量

6 结束语

RSA算法是一种基于大整数因子分解难题的公钥密码算法,该算法具有加解密和签名功能,在我国大量使用. 在实际环境中,RSA运算优先选择基于CRT模式实现,可以提高大约4倍计算速度. 能量分析攻击具有代价低、可行性强的特点,对密码算法实现的安全性构成极大威胁. 本文基于建模类场景,提出了一种基于模板的模约减攻击方法,解决了如何由模约减后中间值的汉明重量恢复私钥的难题. 建议设计者在工程实现中使用底数乘法掩码的防护方法,使得选择密文攻击不能有效进行,以达到有效防护的效果.

该方法基于模约减后中间值的汉明重量模型建模,通过采集选择密文模约减的能量迹进行模板匹配获取模约减后中间值的汉明重量,然后由本文提出的私钥恢复方法进行密钥恢复. 另外,该方法的优点在于理想情况下,基于中间值汉明重量模型建立的模板之间可以共用,且对中间值以多少位大小建模没有限制,可以选择字节大小,64位大小,甚至私钥p相同大小,实际环境中可根据泄露信息情况进行选取. 该方法可以为密码实现分析者和专业测评机构提供一种有效的攻击方法和评估手段.

致谢 本工作由中国互联网发展基金会资助.

参考文献

[1] KOCHER P, JAFFE J, JUN B. Differential power analysis [C]//Advances in Cryptology — CRYPTO' 99. Berlin: Springer Berlin Heidelberg, 1999: 388-397.

[2] MA X L, LI B, WANG H, et al. Non-profiled deep-learning-based power analysis of the SM4 and DES algorithms [J]. Chinese Journal of Electronics, 2021, 30(3): 500-507.

[3] CHARI S, RAO J R, ROHATGI P. Template attacks[C]// Cryptographic Hardware and Embedded Systems - CHES 2002. Berlin: Springer Berlin Heidelberg, 2003: 13-28.

[4] MANGARD S, OSWALD E, POPP T. Power Analysis Attacks: Revealing the Secrets of Smart Cards[M]. Berlin: Springer Science & Business Media, 2008.

[5] BRIER E, CLAVIER C, OLIVIER F. Correlation power analysis with a leakage model[M]//Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004: 16-29.

[6] 马向亮, 王宏, 李冰, 等. 基于能量分析技术的芯片后门指令分析方法[J]. 电子学报, 2019, 47(3): 686-691.
MA X L, WANG H, LI B, et al. A power analysis method against backdoor instruction in chips[J]. Acta Electronica Sinica, 2019, 47(3): 686-691. (in Chinese)

[7] LE T H, CLÉDIÈRE J, CANOVAS C, et al. A proposition for correlation power analysis enhancement[C]//Lecture Notes in Computer Science. Berlin: Springer Berlin Heidelberg, 2006: 174-186.

[8] RIVEST R L, SHAMIR A, ADLEMAN L. A method for obtaining digital signatures and public-key cryptosystems [J]. Communications of the ACM, 1978, 21(2): 120-126.

[9] MESSERGES T S, DABBISH E A, SLOAN R H. Power analysis attacks of modular exponentiation in smartcards [C]//Cryptographic Hardware and Embedded Systems. Berlin: Springer Berlin Heidelberg, 1999: 144-157.

[10] NOVAK R. SPA-based adaptive chosen-ciphertext attack on RSA implementation[C]//Public Key Cryptography. Berlin: Springer Berlin Heidelberg, 2002: 252-262.

[11] YEN S M, LIEN W C, MOON S, et al. Power analysis by exploiting chosen message and internal collisions - vulnerability of checking mechanism for RSA-decryption [C]//Progress in Cryptology - Mycrypt 2005. Berlin: Springer Berlin Heidelberg, 2005: 183-195.

[12] Witteman M. A DPA attack on RSA in CRT mode[EB/OL]. (2009-04-03) [2021-08-10]. https://www. riscure. com/archive.

[13] WITTEMAN M F, VAN WOUDENBERG J G J, MENARINI F. Defeating RSA multiply-always and message blinding countermeasures[C]//Topics in Cryptology - CT-RSA 2011. Berlin: Springer Berlin Heidelberg, 2011: 77-88.

[14] DON C. Small solutions to polynomial equations, and low exponent RSA vulnerabilities[J]. Journal of Cryptology, 1997, 10(4): 233-260.

[15] HOWGRAVE-GRAHAM N. Finding small roots of univariate modular equations revisited[C]//Crytography and

Coding. Berlin: Springer Berlin Heidelberg, 1997: 131-142.

[16] BONEH D, DURFEE G, FRANKEL Y. An attack on rsa given a small fraction of the private key bits[C]//Lecture Notes in Computer Science. Berlin: Springer Berlin Heidelberg, 1998: 25-34.

[17] MAY A. New RSA Vulnerabilities Using Lattice Reduction Methods[D]. Paderborn: University of Paderborn, 2003.

[18] CORON J S. Finding small roots of bivariate integer polynomial equations revisited[C]//Advances in Cryptology - EUROCRYPT 2004. Berlin: Springer Berlin Heidelberg, 2004: 492-505.

[19] MILLER S D, NARAYANAN B, VENKATESAN R. Coppersmith's lattices and "focus groups": An attack on small-exponent RSA[J]. Journal of Number Theory, 2021, 222: 376-392.

[20] XU S, LU X J, ZHANG K Y, et al. Similar operation template attack on RSA-CRT as a case study[J].Science China Information Sciences, 2018, 61(3): 1-17.

[21] VUILLAUME C, ENDO T, WOODERSON P. RSA key generation: New attacks[C]//Constructive Side-Channel Analysis and Secure Design. Berlin: Springer Berlin Heidelberg, 2012: 105-119.

[22] DE LA FE S, PARK H B, SIM B Y, et al. Profiling attack against RSA key generation based on a euclidean algorithm[J]. Information, 2021, 12(11): 462.

[23] DEN BOER B, LEMKE K, WICKE G. A DPA attack against the modular reduction within a CRT implementation of RSA[C]//Cryptographic Hardware and Embedded Systems - CHES 2002. Berlin: Springer Berlin Heidelberg, 2003: 228-243.

[24] KAEDI S, DOOSTARI M A, GHAZNAVI-GHOUSHCHI M B, et al. A new side-channel attack on reduction of RSA-CRT Montgomery method based[J]. Journal of Circuits, Systems and Computers, 2021, 30(3): 2150038.

[25] FEIX B, THIEBEAULD H, TORDELLA L. Recovering CRT-RSA secret keys from message reduced values with side-channel analysis[C]//Progress in Cryptology—INDOCRYPT 2014. Cham: Springer International Publishing, 2014: 53-67.

[26] KAEDI S, DOOSTARI M, GHAZNAVI-GHOUSHCHI M B. NEMR: A nonequidistant DPA attack-proof of modular reduction in a CRT implementation of RSA[J]. Journal of Circuits, Systems and Computers, 2018, 27(12): 1850191.

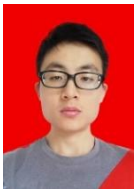
作者简介

马向亮　男，1986年3月生于山西省临汾市，博士，博士后，主要研究方向为信息安全、侧信道和故障攻击与防御.
E-mail: maxiangliang@tsinghua.edu.cn

乌力吉　男，1965年9月生于内蒙古呼和浩特市，工学博士，清华大学集成电路学院博士生导师，主要研究方向为信息安全芯片设计与安全性研究、汽车电子芯片设计与可靠性研究. 中国电子学会会员编号:E190035434M.
E-mail: lijiwu@tsinghua.edu.cn

王　宏　男，1972年9月生于江西省玉山县，博士，高级工程师，主要研究方向为密码学、信息安全、网络安全测评. 中国电子学会会员编号:E1900012458S.
E-mail: wh@nitsc.cn

张向民　男，1966年2月生于北京市，硕士，清华大学集成电路学院助理研究员，主要研究方向为信息安全、汽车电子.
E-mail: zhxm@tsinghua.edu.cn



黄克振　男，1988年9月生于山东省德州市，博士，正高级工程师，主要研究方向为信息安全、网络安全态势感知、网络安全威胁行为智能化认知.
E-mail: kezhen@iscas.ac.cn

刘玉岭　男，1982年1月生于山东省济南市，博士，正高级工程师，主要研究方向为网络安全测评技术.
E-mail: liuyuling@iie.ac.cn