

ECC 计时攻击研究与仿真

贾微微¹, 王潮², 顾健¹, 宋好好¹, 唐迪¹

(1. 公安部第三研究所, 上海 200031;
2. 上海大学特种光纤与光接入网省部共建重点实验室, 上海 200072)

摘要: 借助于隐马尔可夫模型思想, 提出了一种针对采用“倍点一点加”点乘算法的椭圆曲线数字签名体系的一种计时攻击方法, 并对美国国家标准与技术研究院 (NIST) 公布的二进制域上的 5 条 Koblitz 安全曲线进行了攻击仿真实验, 成功地攻击了除 K-571 以外的其他 4 条 Koblitz 安全曲线。对于每一条安全曲线仅采集一次时间数据、耗时几十分钟就能恢复出几乎全部的密钥比特, 实验结果表明, 该方法实施简单、成功率高, 是对当前安全曲线有较大威胁的一种侧信道攻击手段。

关键词: 侧信道攻击; 计时攻击; 隐马尔可夫模型; 椭圆曲线密码

中图分类号: TP309.7

文献标识码: A

doi:10.11959/j.issn.2909-109x.2016.00025

Research and simulation of timing attacks on ECC

JIA Hui-hui¹, WANG Chao², GU Jian¹, SONG Hao-hao¹, TANG Di¹

(1. The Third Research Institute of Ministry of Public Security, Shanghai 200031, China;
2. Shanghai University Key Lab of Specialty Fiber Optics and Optical Access Network, Shanghai 200072, China)

Abstract: Based on the hidden Markov model (HMM) idea, a timing attack on the elliptic curve digital signature system, which adopted the “double-and-add” scalar multiplication, was proposed. Simulation experiments on the secure Koblitz curve which released by the National Institute of Standards Technology (NIST) were implemented and four secure Koblitz curves except the K-571 were attacked successfully. The experiment results show that the attack can recover almost all the key bits in a few minutes by collecting only once time data, and is easy to implement at a high success rate.

Key words: side channel attack, timing attack, hidden Markov model, elliptic curve cryptography

1 引言

安全是计算机和通信系统长期以来一直关注的问题, 大量的研究工作也一直致力于解决这个问题。密码算法构成了可以作为构建模块来构造

针对特定目标的安全机制的原始材料, 这些算法包括对称密码、公钥密码以及散列函数等。椭圆曲线密码 (ECC, elliptic curve cryptography) 是 1985 年由 Koblitz 和 Miller 提出的一种公钥密码体制^[1], 有安全性高、占用带宽小、密钥长度短、

收稿日期: 2016-01-25; 修回日期: 2016-02-07。通信作者: 贾微微, jiahh@mctc.org.cn

基金项目: 国家自然科学基金资助重点项目 (No.61332019); 国家自然科学基金资助项目 (No.61572304, No.61272056); 上海科委科技创新行动计划技术标准基金资助项目 (No.13DZ0500501)

Foundation Items: Key Program of National Natural Science Foundation of China (No.61332019), The National Natural Science Foundation of China (No.61572304, No.61272056), The Technical Standard of Shanghai Science and Technology Innovation Action Plan (No.13DZ0500501)

计算速度快等特点,已被广泛应用于无线通信、密码芯片、电子商务等领域,也是卫星网络、物联网等新型网络的首选,因此,对其安全性的研究显得尤为重要。ECC 的安全性建立在椭圆曲线离散对数问题(ECDLP, elliptic curves discrete logarithm problem)的困难性之上,1999年9月28日,加拿大的 Certicom 公司宣布利用法国、澳大利亚、加拿大、美国、芬兰、奥地利等国家的 760 台计算机成功解决了 97 bit 的 ECDLP 问题。在解决问题过程中一共进行了 130 000 亿次椭圆曲线“点加”运算。2002 年 11 月 6 日,Chris Monico 博士带领 Notre Dame 大学数学研究中心的数学家利用 10 000 台计算机每天工作 24 h,历时 549 天才成功地完成了 Certicom 公司的 109 bit P 曲线的挑战,109 bit 也是目前传统攻击的最高挑战比特数。对于 NIST 公布的 ECC 安全曲线中最小的 163 bit 密钥长度来说,以目前计算机的计算速度进行穷举攻击大约需要 10^{12} 年,这证明 ECC 算法确实具有极高的安全性。

但事实上,密码算法不是决定整个密码安全性的唯一因素,密码算法的实现需要依附一个软件或者硬件设备平台,在这些设备运行过程中会与周围环境发生交互并受周围环境的影响。攻击者可以通过监测这些物理交互作用找出可以用于密码分析的有效信息,这种信息就被称为侧信道信息,而攻击利用侧信道信息进行攻击的方法就被称为侧信道攻击(SCA, side channel attack)。所谓侧信道攻击是指攻击者采集密码设备实现过程中内部状态无意泄漏的物理效应并进行分析,典型的侧信道攻击包括计时攻击^[2]、功耗攻击^[3]、电磁分析攻击^[4]、Cache 攻击^[5,6]、故障攻击^[7,8]、扫描式攻击^[9]等。

计时攻击是利用密码算法在执行过程中泄漏出来的时间信息来进行攻击的,由于要考虑性能优化问题,密码算法往往会使用一些分支语句、条件语句等来加快执行速度,但也同时给加解密时间带来了差异,这些差异可能会泄漏一些重要信息,计时攻击就是利用这种差异来推测密钥信息的。计时攻击不需要额外的硬件设备,既可在本地实现,也可以在远程网络中实现,并且由于计时攻击所需要的时间差异信息来源于密码算法

本身,因此,攻击威胁力比较大,是目前侧信道研究的热点之一。需要强调的是这种攻击方法主要适用于 RSA、ECC 等公钥密码。

1996 年, Kocher 首次提出了计时攻击的概念^[2],并成功地对 RSA 模指数运算实施了攻击;之后 Schindler 对基于 CRT 算法的 RSA 进行了攻击^[10],其主要思想是利用 Montgomery 算法运算时发生的额外约减所泄漏出来的时间差异来推测密钥。

OpenSSL 是一个开放源代码的 SSL 实现,主要用来实现通信的高强度网络加密,现在被广泛应用于各种网络应用程序中。斯坦福大学的 Brumley 等展示了怎样用计时攻击恢复出 OpenSSL 中 RSA 密码算法的私钥信息^[11],对 Kocher 提出的计时攻击方法进行了改进并对运行 OpenSSL 的服务器实施了远程攻击,通过 30 多万次的访问,2 h 左右恢复出了 1 024 bit 的 RSA 密钥。Canvel 设计出了一种针对 SSL 和 TLS 中的 CBC 加密体系的计时攻击方案^[12],可以解密一些简单的密文。

Cachalo 等提出了针对欧洲 NESSIE 项目中 GPS 识别体系的计时攻击^[13],仅用 800 次测量数据,耗时几秒钟就恢复出了其中的密钥,成功率高达 80%。Sakruai 通过观测解密谰言时丢弃信号的时间,提出了针对 EROC-2 公钥密码体制的一种计时攻击^[14],这种公钥密码体制被证明是非常安全的,并被写入了 IEEE P1363 标准中,目前很多国际密码标准组织将 EPOC 作为公钥密码的候选算法。Levine 等提出了针对低延时混合基系统的计时攻击^[15],这些系统是一些企图掩盖输入和输出信息之间对应关系的通信代理服务器,他们还提出了一种新的技术来抵御这种计时攻击。匈牙利人 Rudolf 等提出了一种重建密钥方法高级计时攻击^[16],利用统计学上方差分析和 t 检验方法对采集到的时间数据进行分析,成功地恢复出了 128 bit 的 RSA 密钥。

通过对计时攻击的研究发现,计时攻击主要应用在 RSA 公钥密码上,针对 ECC 的计时攻击目前还没有相关文献,本文基于隐马尔可夫模型(HMM, hidden Markov model)思想,以 HMM 为框架,提出了一种针对椭圆曲线数字签名算法(ECDSA, elliptic curve digital signature algo-

rithm) 的计时攻击方案, 对 NIST 公布的 5 条二进制域上的 Koblitz 安全曲线实施了攻击仿真实验, 解决了在实验过程中遇到的 3 个关键性技术问题, 成功地攻击了 5 条安全曲线中除 K-571 以外的其他 4 条曲线。针对这种攻击, 本文还提出了相应的防御措施, 并展望了针对 ECC 的计时攻击在今后的发展, 为以后实施物理攻击做好铺垫。

2 ECC 基本知识

ECC 的核心运算是椭圆曲线上的点乘运算 $Q = kP$, 这种令椭圆曲线上的一个非零点 P 重复相加 k 次的操作称为标量乘法, 它决定着椭圆曲线密码体制的运算速度。为了提高 ECC 的加解密速度, 密码学家们提出了许多计算点乘运算的算法, 基于二进制的“倍点一点加”(double-and-add) 算法就是被广泛应用的一种点乘算法, 算法描述如下。

算法 1 double-and-add 点乘算法

输入: 整数 $k > 0$ 和基点 P

输出: $Q = kP$

1) $k = (k_{l-1} \cdots k_1 k_0)$;

2) $Q \leftarrow 0$;

3) 对于 i 从 $l-1$ 到 0, 重复执行

$Q \leftarrow 2Q$

如果 $k_i = 1$, 则 $Q \leftarrow Q + P$;

4) 返回 Q 。

从算法 1 中可以看出, 当 k_i 为 0 或 1 时, 执行的运算量不同, 泄漏出来的信息就是运算的时间不同, 本文正是利用这个时间信息来进行计时攻击的。

由于 ECC 私钥的使用只发生在解密和数字签名过程中, 因此, 计时攻击也只能在这 2 个过程中使用, 本文选取在椭圆曲线数字签名 (ECDSA) 过程中使用计时攻击来获取私钥。数字签名的算法描述如下。

算法 2 ECDSA 签名的生成

输入: 参数组 $D = (q, FR, S, a, b, P, n, h)$, 私钥 d , 消息 m

输出: 签名 (r, s)

1) 选择 $k \in_R [1, n-1]$;

2) 计算 $kP = (x_1, y_1)$, 并将 x_1 转换为整数 $\bar{x}_1$;

3) 计算 $r = \bar{x}_1 \bmod n$, 若 $r=0$, 则跳转至步骤 1);

4) 计算 $e = H(m)$;

5) 计算 $s = k^{-1}(e + dr) \bmod n$, 若 $s=0$, 则跳转至步骤 1);

6) 返回 (r, s) 。

其中, P 为基点, m 为要签名的消息, H 表示一个密码杂凑函数, k 为产生的随机数, 称之为临时密钥, d 为私钥, (r, s) 表示签名。

3 隐马尔可夫模型

隐马尔可夫模型 (HMM) 是马尔可夫链的一种, 它的状态不能直接观察到, 但能通过观测向量序列观察到, 每个观测向量都是通过某些概率密度分布表现为各种状态, 每一个观测向量是由一个具有响应概率密度分布的状态序列产生。自 20 世纪 80 年代以来, HMM 被应用于语音识别, 取得了重大成功。到了 20 世纪 90 年代, HMM 还被引入计算机文字识别和移动通信核心技术“多用户的检测”。近年来, HMM 在生物信息科学、故障诊断、密码分析等领域也开始得到应用。HMM 和侧信道攻击的结合早有应用, 2003 年, Chris Karkof 等第一次将 HMM 用于密码分析上^[17], 并提出了一个用于恢复密钥的有效算法; 2005 年, Green 等^[18]对 HMM 在密码分析上的应用做了进一步研究, 提出了将 HMM 和启发式搜索相结合来进行密码分析的思想; 2009 年, 在亚密会上, Brumley 等^[19]提出了一种 Cache 计时模板攻击架构, 将 HMM 和向量量化理论运用到了 Cache 攻击中, 实现了针对 ECC 的攻击, 对于 160 bit 的密钥, 使其平均复杂度由 2^{160} 降低到 2^{48} 。本文提出的 HMM 与计时攻击的结合还是首次。HMM 涉及到的一些参数描述^[20]如表 1 所示。

表 1 HMM 的参数描述

参数	描述
状态数 N	状态有限集合 $S = \{S_1, S_2, \cdots, S_N\}$
观测数 M	观察值有限集合 $V = \{v_1, v_2, \cdots, v_M\}$
初始状态分布 $\pi_i = (\pi_i)$	$\pi_i = P(q_1 = S_i)$
状态转移概率 $A = \{a_{ij}\}$	$a_{ij} = P(q_{t+1} = S_j q_t = S_i)$
输出概率 $B = \{b_j(k)\}$	$b_j(k) = P(O_t = v_k q_t = S_j)$

在 HMM 的实际应用中有 3 个中心问题需要解决, 具体如下。

1) 评估问题: 对于给定模型 $\lambda = (A, B, \pi)$ 和观

察值序列 $O = \{o_1, o_2, \dots, o_T\}$, 求解产生给定观察值序列的概率 $P(O|\lambda)$, 用它可衡量给定模型与此观察值序列之间的匹配情况。

2) 解码问题: 对于给定模型和观察值序列, 求可能性最大的隐含状态序列。

3) 学习问题: 对于给定的一个观察值序列, 调整参数 λ , 使观察值的输出概率 $P(O|\lambda)$ 最大, 也就是用给定的观察值去训练 HMM 模型, 优化模型参数。

本文要解决的是 HMM 的 3 个中心问题中的解码问题。利用 HMM 进行侧信道攻击的基本思想是通过密码算法泄漏出来的侧信道信息对未知密钥比特序列进行猜测, 而 HMM 的解码问题是指通过对观察到的序列分析猜测未知状态序列, 两者有相似的地方, 可以建立这样一个 HMM 模型, 其中, 未知状态序列就是密钥 bit 序列, 而观测序列就是指通过侧信道获取的观测信息, 在本文中是指通过侧信道获取的计时信息。

4 基于 HMM 的计时攻击方案

计时攻击首先由 Kocher 于 1996 年提出, 并成功对 RSA 模指数运算进行了攻击, 其基本原理是利用密码算法在加解密过程中泄漏出来的时间信息来进行攻击的。密码系统加解密时间差异信息产生的来源为性能优化、分支运算、条件语句、RAM Cache 命中、运行时间不固定的处理器指令以及其他多变的原因。

在 double-and-add 算法中, 由于 if 语句的存在使密钥比特为 0 或 1 时执行的操作步骤不同, 比特为 1 时比比特为 0 时要多一步“点加”运算, 最终表现出来的是比特为 0 或 1 时的执行运算时间不同, 这就为实施计时攻击提供了可能性。

由算法 2 可知, 在步骤 2) 中有点乘运算, 所以可以利用计时攻击在计算 kP 点乘运算时求出临时密钥 k , 临时密钥在每次签名都不同, 因此, 一次签名只能采集一次计时数据, 这也是计时攻击难点所在。由于 $H(m)$ 、签名 s 已知, 就可以利用式(1)求出私钥 d 。

$$d = \frac{ks - h(m)}{r} \quad (1)$$

所以, 针对 ECDSA 攻击的关键就是利用获取的计时数据求解临时密钥 k 。基于 HMM 思想,

本文首先建立 double-and-add 标量乘法的 HMM, 如图 1 所示。

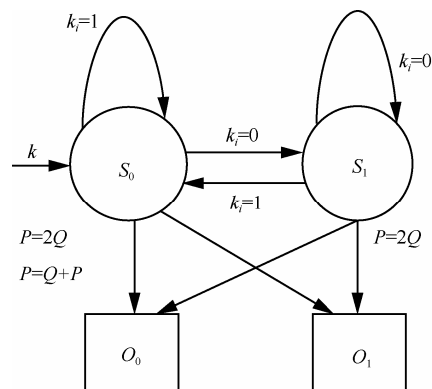


图1 double-and-add 标量乘法的 HMM

输入临时密钥 k 为一个二进制比特序列, 未知状态 S_0 和 S_1 取值为 0 或 1, 观察值 O_0 和 O_1 为所得到的时间数据, 最后由采集到的时间序列来猜测未知密钥比特序列。由于“倍点一点加”(DA)运算要比倍点(D)运算消耗的时间多, 因此, 可以通过对观察到的时间数据进行分析来确定算法体中执行的是 DA 运算还是 D 运算, 进而推测 S_0 和 S_1 的值, 假设观测到的时间数据确定算法执行过程是 (DA, D, D, DA, DA, D, DA, D, D, D, DA), 那么就可以确定临时密钥 k 的比特序列为 (10011010001)。此模型可以通过编写 C 程序来实现并采集有关计时信息, 具体过程如下。

假设临时密钥 $k=26$, 通过编写程序采集到的时间数据从最高位到最低位依次是 $t_1=0.000\ 189\ 668\ s$, $t_2=0.156\ 695\ s$, $t_3=0.070\ 859\ s$, $t_4=0.147\ 188\ s$, $t_5=0.056\ 313\ 2\ s$, 因为观察到 5 组数据, 那么可以推测密钥的长度 $l=5$, 分别对应 k_4 到 k_0 , 最高位 $k_4=1$ 是已知的, 那么第一个数据就舍弃不用, 通过余下的 4 个数据来推测剩余的密钥比特。比较数据发现: 第一个数据 t_1 明显比其他几个要小好几个数量级, 这是必然的, 因为执行第一次循环, Q 的初始值为 0, 它其实是执行的 $0+P$ 的运算, 没有用到大数运算中的“点加”运算, 所需时间较少。在后面 4 个数据中, t_2 和 t_4 大小相近并远大于 t_3 和 t_5 , 结合算法分析, $k_i=1$ 时要比 $k_i=0$ 时多执行一次“点加”运算, 不难推测出 t_2 和 t_4 是 $k_i=1$ 时算法的执行时间, t_3 和 t_5 是 $k_i=0$ 时算法的执行时间, 也就是 $k_3=1$, $k_2=0$, $k_1=1$, $k_0=0$, $k=(11010)_2=26$, 推测结果与原始密钥一致, 说明破解成功。

5 ECDSA 计时攻击的仿真实现

5.1 仿真实验过程中的关键技术

1) 精度问题

计时攻击主要通过对执行时间的监测来推算密钥, 由于差异值一般都很小, 因此需要高精度精确计时技术。本文采用的是 windows.h 库中获取机器内部时钟频率的 QueryPerformanceFrequency() 函数和 QueryPerformanceCounter() 函数。在定时前应该先调用 QueryPerformanceFrequency() 函数获得机器内部计时器的时钟频率, 接着在需要严格计时的事件发生前后分别调用 QueryPerformanceCounter() 函数, 利用 2 次获得的计数之差和时钟频率就可以计算出事件经历的精确时间, 利用这 2 个函数可以将计时时间精确到微秒级, 满足实验所需要的精度要求。

2) 阈值问题

由于受到噪声、Cache 命中失效、CPU 资源利用率等因素的影响, 每次执行得到的计时数据都不尽相同, 都有一个小范围的波动, 因此, 这里有一个阈值选择的问题, 阈值过大或过小都影响实验结果, 阈值一旦确定不准确就会对后面比特信息的判断产生直接影响。对于不同安全级别的曲线, 对应阈值就有很大的差异, 本文采用的是统计学方法, 通过上百次的计算得出 K-283 安全曲线, “倍点一点加”运算平均耗时为 0.205 537 s, “倍点”运算平均耗时为 0.101 148 s, 取阈值 $r = \frac{0.205\ 537 + 0.101\ 148}{2} = 0.153\ 323$ s, 然后从次高位

开始逐一判断 (最高位为 1 无需判断), 如果比特对应的计时时间大于 $r = 0.153\ 323$ s, 此比特就确定为 1; 反之, 如果比特对应的计时时间小于 $r = 0.153\ 323$ s, 就确定为 0。

3) 错误比特值确定

由于外界环境以及 CPU 本身的影响, 在判断密钥比特信息时会存在一定的误差, 并不能保证每次都能恢复出全部的密钥比特数, 而且对于 ECDSA 签名, 临时密钥都是随机选取, 也就是说每次的临时密钥都不相同, 因此, 只有一次采集时间数据的机会, 如果攻击失败, 怎样从已获取的临时密钥中快速找出错误的比特从而破解密码系统是一个非常关键的技术问题。

在实验过程中发现, 猜测出的临时密钥偶尔

会出现 1 个或 2 个错误比特的情况。虽然错误比特数较少, 但是对于传统的方法, 如果有 1 个错误比特, 最多需要进行 N (临时密钥长度) 次搜索, 复杂度为 $O(N)$, 如果有 2 个错误比特, 需要进行 $N(N-1)$ 次搜索, 复杂度为 $O(N^2)$ 。为了降低其搜索的复杂度, 本文提出使用 Grover 算法进行搜索以降低复杂度。Grover 算法是在第 28 届美国计算机学会举办的计算理论国际会议上提出的一种量子搜索算法^[21], 它将问题的搜索步数从经典算法的 N 缩小到 $\sqrt{N}$, 起到了对经典算法的二次加速作用, 从而显著地提高了搜索的效率。在猜测的临时密钥中, 如果只有一个错误比特, 那么只需要 $\sqrt{N}$ 次搜索就可以找出来, 如果有 M 个错误比特, 也仅需要 $\sqrt{\frac{N}{M}}$ 搜索即可, 搜索效率明显提高。

算法 3 Grover 搜索算法^[21]

Grover 搜索算法

1) 初始化 $(\frac{1}{\sqrt{N}}, \frac{1}{\sqrt{N}}, \frac{1}{\sqrt{N}} \dots \frac{1}{\sqrt{N}})$, 也就是说,

N 种状态的振幅是相同的。

2) 重复执行操作 $O(\sqrt{N})$

① 设 S 为输入中的一个基矢, 当 $C(S)=1$ 时, 把矢量 S 旋转 180° ; 当 $C(S)=0$ 时, 不变。

② 用变换 D 作用在个输入分量上。 D 定义为

$$D_{ij} = \begin{cases} \frac{2}{N}, & i \neq j \\ -1 + \frac{2}{N}, & i = j \end{cases}$$

3) 对输出进行测量, 观察结果为 S_v , 若 $C(S_v)=1$, 则得到结果, 否则, 重新开始算法。

对于长度为 256 bit 的临时密钥, 如果只有一个错误比特, 根据量子 Grover 搜索理论最多进行 16 次搜索就能找出, 而利用穷举搜索, 最多需要进行 256 次搜索, 搜索效率明显得到提高。

5.2 仿真实验及结果分析

实验环境为 Intel Core2 Duo CPU T6570 2.10 GHz, 内存 2 GB, 编程环境为 Microsoft Visual Studio C++ 2005。实验对象为 NIST 推荐的二进制域上的 5 条 Koblitz 安全曲线, 以 K-283 为例, 其安全曲线参数如表 2 所示。

表2 NIST 推荐的 K-283 安全曲线参数

K-283 曲线参数
$f(z) = z^{283} + z^{12} + z^7 + z^5 + 1, a=0, b=1, h=4$
$Gx=0x0503213F78CA44883F1A3B8162F188E553CD265F23C156$
$7A16876913B0C2AC2458492836$
$Gy=0x01CCDA380F1C9E318D90F95D07E5426FE87E45C0E8184$
$698E45962364E34116177DD2259$

其中, Gx 、 Gy 为基点的横纵坐标, 临时密钥 k 随机选取并取值为

$k=0xF74AC3B11234567855AC435962FE9AE$
 $2ED07577265DFF7F94451E061E163C613$

针对 ECDSA 的计时攻击流程如图 2 所示。

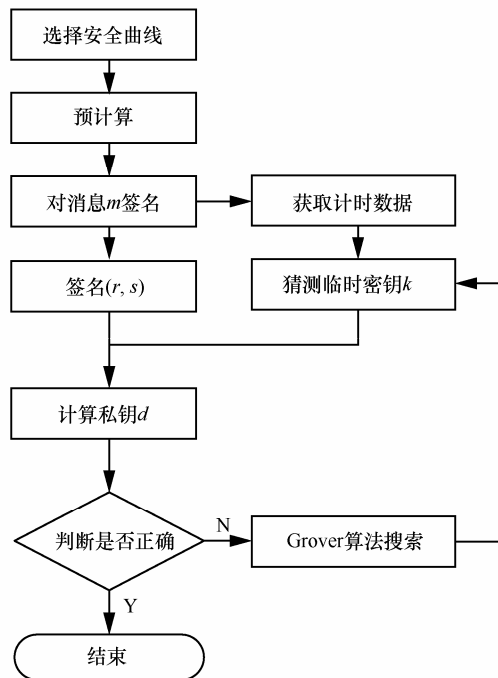


图2 计时攻击流程

根据流程图编写 C++ 程序, 当对消息 m 签名时, 在源程序中植入 `QueryPerformanceFrequency()` 和 `QueryPerformanceCounter()` 2 个函数, 在定时前应该先调用 `QueryPerformanceFrequency()` 函数获得机器内部计时器的时钟频率, 接着在密钥比特执行循环运算前后分别调用 `QueryPerformanceCounter()` 函数, 利用 2 次获得的计数之差和时钟频率就可以计算出事件经历的精确时间, 也就是执行一次密钥比特运算所消耗的时间。采集有关计时数据, 得到一组时间数据序列, 然后将得到的时间数据序列与先前确定出的阈值进行比较, 得到一个二

进制比特序列, 也就是猜测出的临时密钥, 实验仿真如图 3 所示。

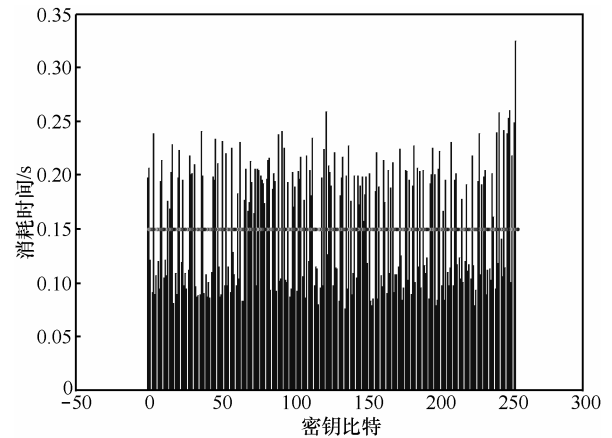


图3 double-and-add 算法计时攻击仿真 (256 bit 密钥)

通过对仿真图分析后得到的猜测密钥为

$k'=111101110100101011000011101100010001$
 $0010001101000101011001111000010101011011$
 $000100001101011001011000101111111010011010$
 $11100010111010100000111010101110110010011$
 $00101110111111110111111100101000100010100$
 $0111100000011000011110000101100011110001100$
 0010011

经比对, 猜测密钥 k' 与原始临时密钥 k 完全一致, 说明本次实验攻击成功。

本文提出的计时攻击是根据点乘算法中算法不同带来的时间差异信息进行的攻击, 并结合 HMM 模型进行了侧信道攻击的仿真, 对使用 double-and-add 算法的加密算法仅耗时几十分钟就可以恢复出全部的密钥, 可以看出计时攻击对密码安全性的强大威胁。预防此类攻击的方法就是消除点乘算法中表现出来的时间差异, 称之为“盲化技术”, 其中较流行的是 Montgomery 点乘算法, 具体如下。

算法4 Montgomery 点乘算法

输入: 整数 $k>0$ 和基点 P

输出: $Q = kP$

- 1) $k = (k_{l-1} \cdots k_1 k_0)$;
- 2) $P_1 \leftarrow P, P_2 \leftarrow 2P$;
- 3) 对于 i 从 $l-1$ 到 0 , 重复执行
 如果 $k_i = 1$, 则 $P_1 \leftarrow P_1 + P_2, P_2 \leftarrow 2P_2$
 否则, $P_2 \leftarrow P_1 + P_2, P_1 \leftarrow 2P_1$;
- 4) Return $Q = P_1$ 。

Montgomery 算法最大的特点就是密钥的比特无论是0还是1都执行相同的运算,也就是说 k_i 为0或1时的加密时间几乎是相同的,因此,可以有效地防御计时攻击。通过本文提出的计时攻击方法对采用 Montgomery 点乘算法的密码系统进行攻击得到的结果如图4所示。

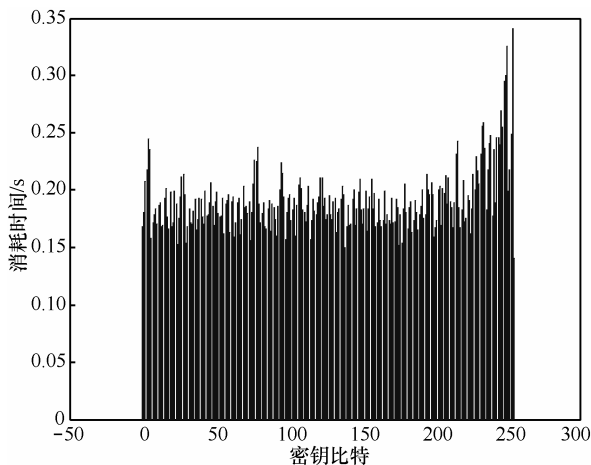


图4 Montgomery 算法计时攻击仿真(256 bit 密钥)

通过图4可以看出,计时攻击所得到的时间信息相差无几,很难通过时间差异来推测密钥,所以, Montgomery 点乘算法能够很好地防御本文提出的时间攻击。

6 结束语

计时攻击是最早被提出来的侧信道攻击方法,也是在侧信道攻击中少有的不用通过其他的辅助硬件就能实现的攻击方法,攻击成本较低,易于实现。但是国内对计时攻击的研究还处于初级阶段,而且大部分都是针对 RSA 公钥密码的攻击,针对 ECC 方面的研究分析几乎还没有涉及。本文基于 HMM 思想提出了一种针对 ECDSA 的计时攻击方法,并编程对 NIST 公布的安全曲线进行了仿真实验,解决了实验过程中存在的3个关键技术问题,仅耗时几分钟就能恢复出几乎全部的临时密钥比特值,对当前密码的安全性具有极大的威胁。消除点乘算法中的时间差异是抵御时间攻击最有效的方法,因此,研究构造能够抵御时间攻击并且加密速度又快的点乘算法具有重要现实意义。本文提供的仿真实验方法可以为以后研究有关计时物理实验攻击提供一些借鉴,实施计时物理

实验攻击也是下一步要研究的内容。侧信道攻击的提出为密码设计者提供了更高的要求,要求设计出来的密码系统除了能够抵御传统的数学攻击外还要抵御来自各个侧信道方向的攻击,只有这样的密码系统才称得上是一个安全的密码系统。

参考文献:

- [1] KOBLITZ N. Elliptic curve cryptosystems[J]. Mathematics of Computing American Mathematical Society, 1987, 48(48): 203-309.
- [2] KOCHER P C. Timing attacks on implementations of diffie-hellman, RSA, DSS and other systems[C]//International Cryptology Conference on Advances in Cryptology. c1996:104-113.
- [3] KOCHER P, JAFFE J, JUN B. Differential power analysis[C]//The 19th Annual International Cryptology Conference on Advances in Cryptology. c1999:388-397.
- [4] QUISQUATER J J, SAMYDE D. Electromagnetic analysis (EMA): measures and counter measures for smart cards[C]//The International Conference on Research in Smart Cards: Smart Card Programming and Security. c2001:200-210.
- [5] PADE D. Theoretical use of cache memory as a cryptanalytic side-channel[R]. Department of Computer Science, University of Bristol, 2002.
- [6] 赵新杰, 郭世泽, 王韬. 针对 AES 和 CLEFIA 的改进 Cache 踪迹驱动攻击[J]. 通信学报, 2011, 32(8): 101-110.
ZHAO X J, GUO S Z, WANG T, et al. Improved cache trace driven attack on AES and CLEFIA[J]. Journal on Communications, 2011, 32(8):101-110.
- [7] BONEH D, DEMILLO R A, LIPON R J. On the importance of checking cryptographic protocols for faults[J]. Journal of Cryptology, 2001, 14(2): 101-119.
- [8] 张金中, 寇应展, 王韬. 针对滑动窗口算法的椭圆曲线密码故障分析[J]. 通信学报, 2012, 33(1): 71-78.
ZHANG J Z, KOU Y Z, WANG T. Elliptic curve cryptosystem fault analysis on the sliding window algorithm[J]. Journal on Communications, 2012, 33(1):71-78.
- [9] YANF B, WU K J, KARRI R. Scan-based side-channel attack on dedicated hardware implementations of data encryption standard[C]//IEEE International Test Conference (ITC). c2004: 339-344.
- [10] SCHINDLER W. A timing attack RSA with the Chinese remainder theorem[C]//Lecture Notes in Computer Science (LNCS). c2000: 109-124.
- [11] BRUMLEY D, BONEH D. Remote timing attacks are practical[J]. Computer Networks, 2005, 48(5): 701-716.
- [12] CANVEL B, HILTGEN A, VAUDENAY S. Password interception in a SSL/TLS channel[J]. Information Technology Journal, 2003, 2729(3):583-599.
- [13] CATHALO J, KOEUNE F, QUISQUATER J J. A new type of

timing attack: application to GPS[M]//Berlin Heidelberg: Springer, 2003:291-303.

- [14] SAKURAI K, TAKAGI T. A reject timing attack on an IND-CCA2 public-key cryptosystem[C]//The 5th International Conference on Information Security and Cryptology. c2002:359-373.
- [15] LEVINE B N, REITER M K, WANG C, et al. Timing attacks in low-latency mix systems[M]//Berlin Heidelberg: Springer, 2004: 251-265.
- [16] TOTH R, FAIGL Z, SZALAY M. An advanced timing attack scheme on RSA[C]//The 13th International IEEE Telecommunications Network Strategy and Planning Symposium. c2008:1-24.
- [17] KARLOF C, WAGNER D. Hidden Markov model cryptanalysis[C]//Lecture Notes in Computer Science (LNCS).c2004:17-34.
- [18] GREEN P J, NOAD R, SMART N P. Further hidden Markov model cryptanalysis[M]//Berlin Heidelberg: Springer, 2005:61-74.
- [19] BRUMLEY B B, HAKALA R M. Cache-timing template attacks[C]//Lecture Notes in Computer Science (LNCS). c2009: 667-684.
- [20] RABINER L R. A tutorial on hidden Markov models and selected applications in speech recognition[J]. Proceedings of the IEEE, 1989, 77(2): 257-289.
- [21] GROVER L. A fast quantum mechanical algorithm for database search[C]//ACM Symposium on Theory of Computing. c1996: 212-219.

作者简介:



贾微微 (1986-), 男, 山东临沂人, 硕士, 公安部第三研究所工程师, 主要研究方向为信息安全、智能卡安全、云安全。



王潮 (1971-), 男, 江苏镇江人, 博士, 上海大学教授、博士生导师, 主要研究方向为网络信息安全与椭圆曲线密码学、量子计算密码、社会网络。



顾健 (1963-), 男, 江苏镇江人, 博士, 公安部第三研究所研究员、博士生导师, 主要研究方向为网络信息安全、智能卡安全、软件测试。



宋好好 (1979-), 女, 山东淄博人, 博士, 公安部第三研究所副研究员, 主要研究方向为网络信息安全、云安全。



唐迪 (1983-), 男, 陕西西安人, 博士, 公安部第三研究所助理研究员, 主要研究方向为隐私信息保护、车联网网络安全协议。