文章编号:1001 - 9081(2010)01 - 0196 - 02

椭圆曲线数字签名中阈下信道通信研究

张秋余,孙战辉
(兰州理工大学 计算机与通信学院,兰州 730050)
(dsfyj@ lut. cn)

摘　要:针对阈下信道技术在椭圆曲线数字签名中的应用可能以及存在的安全隐患问题,通过对其中存在的窄带阈下信道进行实时性测试,在平衡传输信息容量与签名时间的条件下,确定了合理的阈下信息传输位数。实验结果表明,窄带阈下信道在椭圆曲线数字签名中可以被有效利用。

关键词:椭圆曲线密码体制;数字签名;窄带阈下信道;信息隐藏;Miracl 大数库
中图分类号: TP309　　**文献标志码**:A

Covert communication based on subliminal channel in elliptic curve digital signature algorithm

ZHANG Qiu-yu, SUN Zhan-hui
(*College of Computer and Communication, Lanzhou University of Technology, Lanzhou Gansu* 730050, *China*)

Abstract: There are narrowband and broadband subliminal channels in the Elliptic Curve Digital Signature Algorithm (ECDSA), but broadband subliminal channel cannot be safely used. Therefore, the real-time test of narrowband subliminal channel was done. The reasonable bit rate of the sent message was confirmed when the capacity and real-time requests of narrowband subliminal channel were satisfied. The result shows narrowband subliminal channel can be effectively used in ECDSA.

Key words: Elliptic Curve Cryptography (ECC); digital signature; narrowband subliminal channel; information hiding; Miracl large number library

0　引言

自 Simmons[1] 于 1978 年提出阈下信道概念以来,阈下信道已经发展成为一种典型的信息隐藏手段。研究表明,绝大多数数字签名方案中都可包含阈下信道的通信,其最大的特点是阈下信息包含于数字签名之中,但对数字签名和验证过程无任何影响。目前,关于阈下信道的研究主要分为两个方面:一是研究如何建立阈下信道;二是研究如何封闭阈下信道。虽然已经提出许多构造阈下信道[2-4]和封闭阈下信道[5-8]的方案,但多存在于理论研究阶段,真正得到的应用很少。

椭圆曲线密码体制(Elliptic Curve Cryptography, ECC)[9]的安全性是基于椭圆曲线上离散对数问题(Elliptic Curve Discrete Logarithm Problem, ECDLP)的。和其他公钥密码相比较,椭圆曲线具有每比特数据最高的安全强度,这样的好处是计算参数更小,密钥更短,运算速度更快,签名也更加短小,更适用于处理器速度、带宽及功耗受限的场合,因此应用前景十分广阔。

文献[10]证明了椭圆曲线数字签名中不仅存在窄带阈下信道,也存在宽带阈下信道。因此,阈下信道技术在椭圆曲线数字签名中应用已变成可能。但在利用宽带信道时,由于消息发送者需和接收者共享其私钥,这样发送者必须承担签名被伪造的风险,因此目前宽带信道不能被安全使用。而窄带阈下信道和宽带信道相比,尽管信道容量较小,但具有安全、不易被发现和封闭等优点,因此在实际应用中也存在很大价值[11]。基于此,本文通过搜索椭圆数字签名中适合的 r 使之最后 u 比特等于待传的 u 比特阈下消息来构造窄带信道,并基于 Miracl 大数库[12]对其进行了模拟测试。

1　椭圆曲线数字签名算法签名方案概述

设系统参数 $D = (F_q, E, P, n, FR, h')$。其中 F_q 为有限域;q 为有限域元素的个数;E 为定义在 F_q 一条椭圆曲线;$\#E(F_q)$ 为椭圆曲线的阶;公开基点 $P \in E(F_q)$,P 的阶为 n。FR 为有限域中元素的表示方法(用多项式表示或正规基表示),辅因子 $h' = \#E(F_q)/n$,满足 $h' \leqslant 4$。$h()$ 是一种安全散列函数。d_A 是签名者的私钥,对应的公钥为 Q_A。椭圆曲线数字签名算法(Elliptic Curve Digital Signature Algorithm, ECDSA)方案如下:

签名生成　签名者 Alice 利用上面的参数及自己的私钥按下述步骤对消息 m 进行签名。

1)随机地选择一个整数 $k, k \in [1, n-1]$,计算 $kP = (x, y)$,$r = x \bmod n$;

2)计算 $e = h(m)$;

3)计算 $s = k^{-1}(e + rd_A) \bmod n$,则 m 的签名为 (r, s)。

签名验证　当 Bob 收到 Alice 关于 m 的签名 (r, s) 后。

1)验证 r, s 是不是 $[1, n-1]$ 中的整数;

2)计算 $e = h(m)$;然后计算 $u = s^{-1}e, v = s^{-1}r$;

3)计算 $R = (x_1, y_1) = uP + vQ_A$,$r_1 = x_1 \bmod n$,如果 $r_1 = r$,则接受此签名。

收稿日期:2009 - 07 - 08;**修回日期**:2009 - 09 - 04。

作者简介:张秋余(1966 -),男,河北辛集人,副研究员,主要研究方向:信息安全、图像理解与识别、多媒体通信;　孙战辉(1983 -),男,河北赵县人,硕士研究生,主要研究方向:信息隐藏、数字签名。

2　基于 Miracl 大数库的窄带阈下信道测试

2.1　构造窄带阈下阈下信道

椭圆曲线数字签名中窄带阈下信道的构造可有两种方法:1)通过控制签名中 r 对 u 个大秘密数(收发双方事先秘密约定好)的二次剩余特性,使之与 u 阈下比特相适应来构造信道;2)通过搜索适合的 r 使之最后 u 比特等于待传的 u 比特阈下消息所构造的信道。因为后者效率较高且易于编程实现,所以本文采用第 2)种方法构造窄带阈下信道。

2.2　Miracl 大数库

Miracl 库是 Shamus Software Ltd 开发的一个大数库。在功能上它不但提供了高精度的大整数和分数的各种数学运算操作,而且提供了很多密码学算法中的功能模块,如 SHA、AES、DSA 等中的一些底层操作。最重要的是它还提供了很多椭圆曲线密码体制中的底层功能模块,所以成为实现密码算法的重要工具。另外,Miracl 库的内部实现采用了很多的汇编层的代码,故运行速度非常快,这样也可以提高签名的效率。

2.3　测试环境

本测试在VC++2008 中实现了算法的模拟仿真。执行系统的硬件配置为 Core2 duo1.6 GHz CPU,512 MB 内存;操作系统为 Windows XP SP3。

2.4　测试算法描述

前文提到构造窄带阈下信道时可以规定 r 的最后几位为要传递的阈下信息。而发送者计算量随所用阈下通信的比特数的增长成指数级增长关系,这也是该信道为窄带信道的原因。这就需要在签名时间和信道容量中找到一个平衡点,即在满足签名时间的情况下,传递尽可能多的阈下信息。

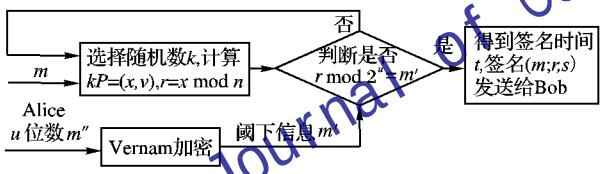

图 1　带阈下信息的签名流程

以下是基于 Miracl 大数库的测试步骤:

1) 椭圆曲线签名参数的选择 $D=(q,FR,a,b,n,h')$。利用文献[13]的方法在素数域 $F(p)$ 选择安全椭圆曲线及基点。考虑安全性和实现效率,p 为 192 位的大素数,且为伪梅森素数或类梅森素数;n 也为 192 位大素数;辅因子 $h'=\#E(F_q)/n=1$。

2) 假设签名者 Alice 要传 u 位的阈下信息,则 Alice 把要传递的信息经 Vernam 加密算法得到 u 位的数 m',即 m' 为传递的阈下信息。

3) Alice 利用 Miracl 大数库函数 bigrand( )生成一个大随机数 k 进行签名,利用库函数 ecurve_mult( )和 epoint_get( )计算 $kP=(x,y)$,$r=x \bmod n$,然后验证 $r \bmod 2^u=m'$ 是否成立。如果不成立,则重复执行 3),直到找到一个合适的 k 为止。

4) 利用 Miracl 库函数 mad( )计算 $s=k^{-1}(e+rd_A) \bmod n$,然后计算完成签名所需时间。

在测试过程中,Alice 首先要输入被签名的信息 m。测试过程中,不断增加 u 的值,计算签名所需的时间,以便在签名所传输信道容量和所需时间之间找到一种平衡。为了保证结果更准确有效,不断改变 m 和 m' 的值,并进行多次实验,最后输出其平均时间 t。

2.5　测试结果及分析

测试结果如表 1 所示,可以看出,在椭圆曲线数字签名中窄带阈下信道能被有效地利用。当 $u<8$ 时,签名所需时间 $t<1$ s;当 $u \leqslant 10$ 时,签名所需时间小于 10 s;当 $u \leqslant 14$ 时,$t<240$ s;当 $u \geqslant 15$ 时,随着时间不断增加,所需时间达到十几分钟,甚至超过一个小时。考虑实时性和传输较多信息的要求,当传输信道容量 $u=11 \sim 14$ 时是比较好的选择。

表 1　测试结果

位数 u/bit	时间 t/s	位数 u/bit	时间 t/s
0~5	<0.1	14	219
6	0.26	15	816
7	0.59	16	1726
8	1.2	17	3345
9	3.5	18	5589
10	9.0	19	6445
11	18.8	20	11120
12	42.8	21	19852
13	100	22	28768

3　结语

由于在椭圆曲线数字签名中构造宽带阈下信道存在安全隐患,所以本文对其存在的窄带信道进行了实时性测试,并确定了合理的阈下信息传输位数,为阈下信道在椭圆曲线数字签名的应用提供了一定的依据。在椭圆曲线数字签名中,对于在发送者不与接收者共享私钥情况下实现宽带阈下信道通信,将有待于进一步研究。

参考文献:

[1] SIMMONS G J. The Prisoner's Channel and the Subliminal Channel [C]// Proceedings of CRYPYO'83. New York: Plenum Press, 1984: 51-67.

[2] 刘欣, 李大兴. 基于 Schnorr 数字签名的阈下信道方案及分析[J]. 计算机工程与设计, 2007, 28(5): 1029-1031.

[3] 刘晓川, 侯整风. 一种安全构造 ElGamal 签名中阈下信道的算法[J]. 安徽师范大学学报: 自然科学版, 2007, 30(6): 647-650.

[4] XIE YUHUA, SUN XINGMING, XIANG LINGYUN, *et al*. A security threshold subliminal channel based on elliptic curve cryptosystem [C]// International Conference on Intelligent Information Hiding and Multimedia Signal Processing. Washington, DC: IEEE Computer Society, 2008: 294-297.

[5] 董庆宽, 牛志华, 肖国镇. ELGamal 类签名中的阈下信道封闭问题研究[J]. 计算机学报, 2004, 27(6): 845-848.

[6] 张彤, 杨波, 王育民, 等. 封闭阈下信道的若干方法研究[J]. 通信学报, 2002, 23(4): 17-21.

[7] 李恕海, 王育民. 封闭阈下信道的理论模型[J]. 中山大学学报: 自然科学版, 2004, 43(z2): 34-37.

[8] 朱有根. 抗阈下信道的盲签名方案[J]. 宁波大学学报: 理工版, 2002, 15(2): 62-63.

[9] 张方国, 王常杰, 王育民. 基于椭圆曲线的数字签名与盲签名[J]. 通信学报, 2001, 18(2): 186-192.

[10] 赵元志, 廖晓峰. 椭圆曲线数字签名算法的阈下信道[J]. 计算机工程与应用, 2005, 41(21): 92-93.

[11] 孟涛, 王建峰, 孙圣和. 有序多重签名体制中阈下信道通信方法的研究[J], 电子学报, 2007, 35(6A): 112-114.

[12] Multiprecision integer and rational arithmetic C/C++ library[EB/OL]. [2009-04-25]. http://www.shamus.ie/.

[13] 张方国, 王常杰, 王育民. GF(p)上安全椭圆曲线及其基点的选取[J]. 电子与信息学报, 2002, 24(3): 377-381.