有序多重签名体制中阈下信道通信方法的研究

孟 涛,王建峰,孙圣和
(哈尔滨工业大学,黑龙江哈尔滨 150001)

摘 要: 本文分析了阈下信道技术在数字签名中的应用,并以一种有序多重数字签名方案为例,对其中存在的宽带和窄带阈下信道进行了具体分析.提出了一种有序多重签名体制下的窄带阈下信道通信方案,通过实时性测试确定阈下信息位数,从而满足了传输信息容量与实时性的要求.

关键词: 数字签名; 阈下信道; 多重签名
中图分类号: TN919.19 **文献标识码:** A **文章编号:** 0372-2112 (2007) 6A-112-03

Covert Communication Based on Subliminal Channel in Ordinal Digital Multi-signature

MENG Tao, WANG Jian-feng, SUN Sheng-he
(*Harbin Institute of Technology, Harbin, Heilongjiang* 150001, *China*)

Abstract: The subliminal channel is a covert communication channel constructed in public correspondence pattern. As a kind of the modern information hiding technology, it is used to transmit the secret information. The subliminal channel in general Elgamal signature is analyzed. And the wideband and narrowband subliminal channel in the ordinal digital multi-signature is discussed. A scheme of narrowband subliminal channel in the ordinal digital multi-signature is given and the bit rate of the sent message is confirmed by a real-time test so that the capacity and real-time request of the narrowband subliminal channel can be satisfied.

Key words: digital signature; subliminal channel; digital multi-signature

1 引言

阈下信道(Subliminal Channel)这一概念是 G.J.Simmons 于 1978 年在美国圣地亚国家实验室(Sandia National Labs)提出的[1].它是指在基于公钥密码技术的数字签名、认证等应用密码体制的输出密码数据中建立起来的一种隐蔽信道,除指定的接收者外,任何其他人均不知道密码数据中是否有隐藏信息存在[2,3].利用阈下信道传输的隐藏信息被称为阈下信息.

多重签名,是数字签名的一个重要应用,主要指多个用户需要同时对一份文件进行签名[4].多重签名主要分为广播多重数字签名和有序多重数字签名.有序多重数字签名指签名者对文件的签名必须遵照一定的顺序完成,通过签名验证者完成对有序多重签名的验证[5].

多重签名体制下的阈下信道问题在文献[6]中进行了一定的分析,但只对多重签名下的宽带信道进行了分析,而忽略了可以在签名中构造窄带阈下信道的问题.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.本文详细分析了在有序多重签名体制下的阈下信道问题,并针对窄带阈下信道进行了系统的签名实时性测试.

2 阈下信道的理论分析

2.1 阈下信道的条件分析

阈下信道形成的必要条件是密文的冗余性,即同一明文可以对应多种不同形式的密文[7].简单的说,如果存在一种具有特殊性质的密码算法,对每一明文可能存在两种密文,且均可使用同一密钥解密而恢复成同一明文,同时假设这些密文对可以由发送者和阈下接收者方便地分为两类:奇数类和偶数类,则能够建立一个无条件安全的 1 比特阈下信道.若能构造出一种密码体制,可使一种明文对应 k 种密文,则可以构造出 $\log_2 k$ 比特的阈下信道.

2.2 阈下信道的分类

按照阈下信息的容量,可以将阈下信道分为宽带信道和窄带信道.如果在一个签名方案中,a 比特用于传送签名,b 比特被用于提供签名的抗伪造,抗篡改和抗移植等安全的能力,其中 $b < a$,则剩余 a-b 比特可被用于阈下通信,而密文的冗余度同样也为 $a - b$ 比特.

收稿日期:2007-09-11;修回日期:2007-12-18

阈下信道受建立方法和宿主参数安全条件的限制往往不能达到最大容限.如果阈下信道用到所有或几乎所有 $a-b$ 比特的密码数据,则称之为宽带信道,否则称之为窄带信道.

按照阈下信道构造的机理,可根据接收方得到的发送方陷门信息的多少进行划分.根据共享信息的多少,Simmons 将阈下信道分为 I 型信道和 II 型信道.I 型阈下信道是指消息的发送者必须把秘密签名密钥交给阈下接收方,以便对方能恢复阈下信息;II 型阈下信道则不求消息的发送者将自己的签名私钥给接收方共享.显然,采用 I 型阈下信道时,消息的发送者必须承担签名被伪造的风险.

3　有序多重签名中的阈下信道分析

3.1　有序多重签名方案

下面介绍一种基于 Elgamal[8] 的有序多重签名方案,签名过程分为两部分:参数设置过程和签名过程.

参数设置过程在密钥生成中心(SKIA)进行.首先选取一个至少 512 位的大素数 p,设 g 是由 p 构成的有限域 GF(p)的本原元,再选取一个随机数 d 满足 $1<d<p-1$,计算 $q=g^d(\mathrm{mod}\ p)$,设置一个单向 hash 函数 h,其中四元组(h,p,g,q)是公开的,d 为 SKIA 的主私钥.

用户将自己的身份信息 ID 发送给 SKIA,SKIA 计算 $h(\mathrm{ID})$,再选择一个随机数 n,n 满足 $gcd(n,p-1)=1$,即 n 和 $p-1$ 互素.SKIA 计算 $y=g^n(\mathrm{mod}\ p)$,$x=(h(\mathrm{ID})-n*y)*(d^{-1})$.SKIA 将$(x,y)$发送给用户,用户的公钥为$(\mathrm{ID},y)$,私钥为 x.

签名过程开始时,消息的发送者 U_0 预先设计一种签名顺序,假设为$(U_1,U_2,\cdots,U_n)$.U_0 将这种签名顺序发送到每个签名者 $U_i(i=1,\cdots,n)$,按顺序进行签名后,由签名验证者 U_V 进行验证,完成签名过程.U_0 将消息 m 发送到第一位签名者 U_1,U_1 收到消息 m 后,进行如下操作:

第 1 步:签名者 U_1 生成随机数 k_1 作为会话密钥,满足 $gcd(k_1,p-1)=1$,即 k_1 和 $p-1$ 互素,计算 Elgamal 签名对 $r_1=q^{k_1}\ \mathrm{mod}\ p$,$s_1=(h(m,T_1)x_1-r_1*k_1)\ \mathrm{mod}\ (p-1)$,其中,$x_1$ 为用户 U_1 的私钥,T_1 为签名时间.

第 2 步:将签名消息$(m,(r_1,s_1),T_1)$发送到下一个签名者 U_2.

第 3 步:每一位签名者 $U_i(i\geqslant 2)$在收到 U_{i-1}发送的签名消息$(m,(s_{i-1},r_1,\cdots,r_{i-1}))$后进行如下操作:

(1)首先对该签名消息进行验证,验证公式如下:

$$q^{s_{i-1}}\prod_{j=1}^{i-1}r_j^{r_j}=\prod_{j=1}^{i-1}(g^{h(\mathrm{ID}_j)}*y_j^{(-y_j)})^{h(m,T_j)}\mathrm{mod}p \qquad (1)$$

其中,g 为由 p 构成的有限域 $GF(p)$的本原元.

如果式(1)成立,则继续进行下一步.否则拒绝签名.

(2)在验证正确后,U_i 随机选取 k_i 满足 $gcd(k_i,p-1)=1$,即 k_i 和 $p-1$ 互素,计算 $r_i=q^k\mathrm{mod}\ p$ 和 $s_i=s_{i-1}+(h(m,T_i)x_i-r_i*k_i)\mathrm{mod}(p-1)$.

(3)将签名消息

$(m,(s_i,r_1,\cdots,r_i),(T_1,\cdots,T_i))$发送给下一个签名者.

第 4 步:最后一个签名者 U_n 在验证完前面的签名后,先计算 s_n,r_n,然后计算 $R=\prod_{j=1}^{n}r_j^{r_j}\mathrm{mod}\ p$ 与 $S=R^*s_n\ \mathrm{mod}(p-1)$,则$(R,S)$即为签名者 $U_1,U_2,\cdots,U_n$ 对消息 m 产生的有序多重签名对.U_n 将签名消息$(m,(R,S),(T_1,\cdots,T_n))$发送给验证者 U_V.验证者 U_V 进行如下验证过程:

U_V 收到 U_n 送来的签名消息$(m,(R,S),(T_1,\cdots,T_i))$后,验证公式为,

$$R^Rq^S=\prod_{j=1}^{n}(g^{h(\mathrm{ID}_j)}*y_j^{(-y_j)})^{R*h(m,T_j)}\mathrm{mod}p \qquad (2)$$

如果式(2)成立,接受签名;如不成立,则拒绝签名.

3.2　基于该有序多重签名方案中的阈下信道分析

3.2.1　有序多重签名中的宽带阈下信道

在上述方案中,如果使用宽带阈下信道的话,则签名者 U_i 将待发送的阈下信息作为会话密钥 k 进行签名,然后将签名消息发送给下一个签名者 U_{i+1}.而作为阈下信息的接收方,如果要从中提取阈下信息的话,需要在接收端恢复出 k 的值,从而就需要计算出 $r_i\cdot k_i$ 的值,并计算出 ri 的乘法逆元.由上述签名方案可知,$r_i\cdot k_i$ 的值应满足 $r_i\cdot k_i=(s_{i-1}+h(m,T_i)x_i-s_i)\mathrm{mod}(p-1)$,但是由于在该签名方案中,签名者只把签名后的 si 发送给下一个签名者,因此若假设下一位签名者 U_{i+1} 为阈下接收方,则无法得到由签名者 U_{i-1}发出的 s_{i-1} 的值,也就无法计算出 $r_i\cdot k_i$,从而不能完成阈下信息的提取.因此,在这种有序的多重签名体制中无法构造宽带阈下信道.

3.2.2　有序多重签名中的窄带阈下信道

由于在该方案中签名者 U_{i+1}所接收到的签名消息为$(m,(s_i,r_1,\cdots,r_i),(T_1,\cdots,T_i))$,故可以选择 ri 作为阈下信息的载体,因此在该签名方案中可构造窄带信道.阈下信息的收发双方可以通过事先约定一个加密算法 E,将阈下信息用 E 加密后的值作为 ri 的最低有效位.若 r_i 的最低有效位为所需要传送的值,则发送签名,若不满足,则重复上述过程,每次选取成功的概率为 1/2.

同样,也可以在该签名方案中构造容量为 t 比特的阈下信道,可以规定 r_i 的某几位为采用 E 加密后的固定值,在这种情况下,需要多次选择 k 值以满足传送要求,通常,传递 t 位的阈下信息需要进行 2^t 次参数的选择.

4 基于 NTL 的窄带阈下信道测试

NTL(Number Theory Library)是涉及到任意精度大整数与实数的计算数论与计算代数(有限群、环、域、多项式)的算法库[9],由美国纽约大学的 Victor Shoup 开发并维护.由于 NTL 能提供任意长度的整数运算及大整数运算中所需要用到的一些必要函数,故成为 C 语言环境下实现密码算法的重要工具.前面提到,构造窄带阈下信道时可以规定 r_i 的某几位为采用 E 加密后的固定值,而参数选择的次数与所要传递信息的位数之间成指数级关系,从而进一步制约了签名所需时间.因此,在构造窄带阈下信道时,需要在签名时间和所传输信道容量中选择一个平衡点,即在满足签名的实时性的条件下,尽可能的提高传输信道的容量.以下是基于 *NTL* 的对于签名时间和所传输位数的测试.

4.1 测试环境

该测试是在个人 PC 机(CPU: P42.0GHz,内存:512MB)上进行,操作系统为 Windows XP,软件运行平台为 VC++6.0.

4.2 测试算法描述

测试算法基本如上所述,其中加密算法 E 采用 Vemam 加密体制.如果待传输的阈下信息为 t 位,则通常可任意选取一个小于 2^t 的数 m,并假设 m 为 Vemam 加密后的值,即 m 为待传输的阈下信息.采用随机数发生器生成随机数 k,计算 $r_i = q^k \bmod p$,然后判断 $m = r_i \bmod (2^t)$ 是否成立,若成立,则窄带阈下信道构造成功,输出运算时间.否则重新选择随机数 k,进行重复运算.

在测试过程中,可以不断增加 t 的值,计算签名所需要的时间,以便寻找传输信道容量和签名时间之间关系.为保证结果的准确性,可以通过改变 m 的值,进行多次测试,并输出其平均值.

4.3 测试结果

测试结果如下表所示:

位数 t(位)	时间(秒)	位数 t(位)	时间(秒)
0-10	0.1	18	113
11	1.0	19	246
12	2.5	20	1453
13	4.9	21	2231
14	12	22	4103
15	29	23	5796
16	47	24	13245
17	96	25	27862

从上表可以看出,当 $t < 10$ 时,即传输位数在 10 位以下,签名时间均在 1 秒以内.当 $t < 14$ 时,签名时间在 5 秒之内.当传输位数在 17 位以下时,所需时间均小于一分钟.在 20-21 位时,签名时间为几十分钟.而达到或超过 22 位时,所需时间已经超过一个小时.因此,当构造窄带阈下信道时,考虑到实时性要求,传输信道容量一般应选择在 15-19 位之间.

5 结论

本文分析了阈下信道技术在数字签名中的应用,并重点分析了基于 Elgamal 类算法的有序多重签名中阈下信道问题.作者指出在该签名中由于多重签名特性的宽带信道会被封闭,因而提出了利用窄带信道进行阈下信息传递的方案,并对签名的实时性进行了测试.对于多重签名的另外一种类型,即广播多重签名中的阈下信道问题分析,将有待于进一步研究.

参考文献:

[1] G J Simmons. The prisoners' problem and subliminal channel [C]. Proc of Cypto 83, 51-67, Santa Barbara, California, August 1983, Plenum Press NY, 1984.

[2] G J Simmons. Subliminal channels: past and present[J]. European Transactions on Telecommunicatoins, 1994, 4(4): 459-473.

[3] G J Simmons. Subliminal communication is easy using the DSA [J]. Proc of Eurocrypt 93, 1994, 218-232.

[4] 杜海涛,张青坡,钮心忻,杨义先.一个新的离散对数有序多重签名方案[J].计算机工程与应用,2007,43(2):148-150.
DU Haitao, ZHANG Qingpo, NIU Xinxi, YANG Yixian. New sequential multi-signature scheme based on discrete logarithm problem[J]. Computer Engineering and Applications, 2007, 43(2): 148-150. (in Chinese)

[5] 卢建朱,陈火炎,林飞. ElGamal 型多重数字签名算法及其安全性[J].计算机研究与发展,2000,37(11):1335-1339.
LU Jianzhu, CHEN Huoyan, LIN Fei. Elgamal type digital multisignature schemes and its security[J]. Journal of Computer Research and Development, 2000, 37(11): 1335-1339. (in Chinese)

[6] 祁明,隆益民,卓光辉.封闭阈下信道的若干新型签名方案[J].计算机工程与应用,2000,36(6):22-24.
Qi Ming, Long Yimin, Zhuo Guanghui. Some new signature schemes on sealing subliminal channals[J]. Computer Engineering and Applications, 2000, 36(6): 22-24. (in Chinese)

[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,2004,43(2)(增刊):34-37.
Li Shuhai, Wang Yumin. The models of closing the subliminal channels[J]. Acta Scientiarum Naturalium Universitatis Sunyatseni, 2004, 43(z2): 34-37. (in Chinese)

(下转第 6 页)

nonlinear/non-Gaussian Bayesian tracking[J]. IEEE Transactions on Signal Processing, 2002, 50(2): 174 - 188.
[25] Djuric P M, etc. Particle filtering[J]. IEEE Signal Processing Magazine, 2003, 20(5): 19 - 38.
[26] Bertozzi T, Ruyet D, etc. On particle filtering for digital communications[A]. IEEE Workshop on Signal Processing Advances in Wireless Communications Proceedings [C]. IEEE Press, 2003, 570 - 574.
[27] Scherb A, Zheng C. Comparison of methods for iterative joint data detection and channel estimation[A]. Proceedings of IEEE Vehicular Technology Conference[C]. VTC Spring, 2004, 98 - 102.
[28] Kotecha J H, Djuric P M. Sequential monte carlo sampling detector for rayleigh fast-fading channels[A]. Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)[C]. IEEE Press, 2000, 61 - 64.
[29] Andrieu C, Piechocki R J, Mcgeehan J P. Particle smoothing techniques with turbo principle for MIMO systems[A]. IEEE Workshop on Signal Processing Advances in Wireless Communications[C]. IEEE Press, 2003, 561 - 564.
[30] Yang J, Sun Y, etc. Channel estimation for wireless communications using space-time block coding techniques[A]. Proceeding of International Symposium on Circuits and Systems [C]. IEEE Press, 2003, 220 - 223.

作者简介:

张 玲 女,1978 年出生于山东省.2007 年 7 月毕业于清华大学自动化系并获得博士学位.现在中国海洋大学任教.研究方向为通信信号处理、智能信息处理.
E-mail: lingzhang03@mails.tsinghua.edu.cn

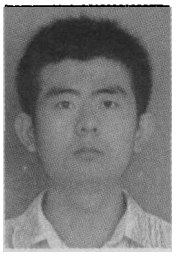
张贤达 男,1946 年出生于江西省.现任清华大学自动化系、清华信息科学与技术国家实验室教授、博士生导师.研究方向为信号处理、模式识别.IEEE 高级会员,在国际权威杂志 IEEE 汇刊和 Neural Computation 上发表论文近 40 篇.曾以第一获奖人获得国家自然科学奖和部级科技进步奖多项.出版学术著作 6 部.

(上接第 114 页)

[8] Mao Wenbo. Modern Cryptography: Theory and Practice[M]. Publishing House of Electronics Industry, 2004.
[9] V Shoup. A Computational Introduction to Number Theory and Algebra[M]. Cambridge University Press, 2005.

作者简介:

孟 涛 男,1961 年 5 月出生,1983 年于国防科技大学获学士学位,1988 年于哈尔滨工业大学获工学硕士学位,现为哈尔滨工业大学自动化测试与控制研究所博士研究生.主要研究方向为阈下信道、隐藏通信、信息安全.
E-mail: gorgan@126.com



王建峰 男,1984 年 6 月出生,2006 年于天津大学获得双学士学位,现为哈尔滨工业大学自动化测试与控制研究所硕士研究生.主要研究方向为数字签名中的阈下信道技术.
E-mail: flyy@tju.edu.cn

孙圣和 男,1937 年 10 月出生,1961 年毕业于哈尔滨工业大学电机系研究生班,现为哈工大教授、博导,自动化测试与控制研究所所长.研究方向为信号处理、数字水印、自动化测试.
E-mail: sunshenghe@hit.edu.cn