第 25 卷第 2 期　　四川理工学院学报(自然科学版)　　Vol. 25　No. 2
2012 年 4 月　　Journal of Sichuan University of Science & Engineering(Natural Science Edition)　　Apr. 2012
文章编号:1673-1549(2012)02-0019-03

一种分割法阈下信道构造方案

吕晓庆, 郑　毅, 魏　航

(成都理工大学管理科学学院, 成都　610059)

摘　要:提出一种利用求解线性方程组分割法阈下信道构造方案。方案将阈下信息分割转化为几个独立的无害的子消息。通过传输这些子消息的签名的方式将阈下信息的各个子消息传给阈下信息的接收方, 阈下信息接收方可根据与签名者共享的秘密信息利用 Cramer 法则提取出阈下信息。

关键词:阈下信道;分割法;Cramer 法则

中图分类号:TB115　　**文献标识码**:A

阈下信道(也称秘密信道或暗道),阈下信道的概念最早是由美国圣地亚国家实验室的 Simmons G J 于 1978 年提出的[1],并于 1985 年和 1994 年,分别描述了如何利用 ElGamal 签名方案和 DSS 建立阈下信道,并指出了阈下信道的若干应用[2-4]。随后许多学者进行了大量的研究[5-13]。由于设计出的一些针对随机数会话密钥的封闭协议[14-17]的提出, 使得在某些特殊情况下无法通过这类信道来传输一些特定的秘密信息。Wu Chuan-kun[11] 提出了 Hash 信道的概念, 指出在没有使用随机数的数字签名中都存在阈下信道, 并给出了宽带与窄带两种阈下信道方案, 但该方案存在一定的缺陷, 阈下信息的二进制长度 k 在实际情况下不能超过 30, 当 k 比较大时, 寻找一个合适的签名消息比较困难, 一般需要经过 2k 尝试才有可能得到合适的签名消息, 有时候并不一定能找到相应的签名消息。张扬松、范安东等[12-13]通过引入矢量空间秘密共享技术和指定接受者签名加密技术,提出一种新的阈下信道方案,并根据被签名的无害消息的随机性, 利用中国剩余定理,提出了一种新的阈下信道方案。文中利用求解线性方程组来对阈下信息进行分割转化与提出,提出一种分割法阈下信道构造方案。

1　基于线性方程组的阈下信道构造方案

1.1　新的阈下信道方案

由于阈下信道的研究具有两面性,它既可用来帮助用户传递秘密信息,又可使得犯罪分子利用阈下信道传递信息而不被发现。根据被签名的无害消息的随机性, 基于分割选择法提出一种新的阈下信道方案[14]。方案中主要利用线性方程组的性质来对阈下信息进行分割。对于方案中用的签名算法,可利用 DSA 算法或 ELGmal 类签名算法,详细内可参见文献[18]。阈下信道的构造方案主要包括两部分:阈下信息的嵌入和阈下信息的提取。

1.2　阈下信息的嵌入

阈下信息的嵌入是指通过某种嵌入算法将阈下信息嵌入到表面看起来无害的宿主系统中的输入或输出参数中的一个过程。文中的宿主系统是数字签名算法系统。

在阈下通信以前, 阈下信息的收发双方共享

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & & \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

且 $|A|\neq 0$, $a_{ij}(1\leqslant i,j\leqslant n)\in Z^{*}$。设阈下信息为 x_i, 阈下信息发送者利用

$$\begin{cases} a_{11}x_1+a_{12}x_2+\cdots+a_{1n}x_n=b_1 \\ a_{21}x_1+a_{22}x_2+\cdots+a_{2n}x_n=b_2 \\ \vdots \\ a_{n1}x_1+a_{n2}x_2+\cdots+a_{nn}x_n=b_n \end{cases} \tag{1}$$

可以得到 n 个阈下信息的分割子信息 $b_1, b_2, \cdots, b_n$, 可

收稿日期:2012-03-07

作者简介:吕晓庆(1987-),女,黑龙江湃泉人,硕士生,主要从事计算数论与密码学方向的研究,(E-mail)dobegond@126.com

以看到在不知道 a_{ij} $(1 \leqslant i,j \leqslant n)$ 的情况下，这 n 个数跟 x_i 之间是独立的。发送者可以利用 DSA 算法或 ELGmal 类签名算法分别对 $b_i(1 \leqslant i \leqslant n)$ 进行签名，记对应的签名结果为 (b_i,s_i)，然后可以将这 n 个签名 $(b_i,s_i)(1 \leqslant i \leqslant n)$ 按顺序发送给阈下信道的收方。

1.3 阈下信息的提取

阈下信息的提取过程是指合法的阈下信息接受者在完成宿主验证过程后，根据阈下信息的提取算法以及于阈下信息的发方所共享的秘密信息提取阈下信息的过程。

在基于数字签名方案的阈下信道方案中，任何人都可以根据签名验证算法验证 (x_i,s_i) 签名的有效性。而对于合法的阈下信息的接受者可以利用他与签名发送者预先秘密共享的 A，得到线性方程组：

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n = b_n \end{cases} \tag{2}$$

根据该线性方程组(2)，阈下信息收方可以通过计算得到阈下信息，即该线性方程组的唯一一组解：

$$x_1 = \frac{|A_1|}{|A|}, x_2 = \frac{|A_2|}{|A|}, \cdots, x_n = \frac{|A_n|}{|A|}$$

其中 $|A_j|$ 是一个 j 阶行列式，它由 $|A|$ 去掉第 j 列换成由方程组常数项 b_1，b_2，…，b_n 组成的列而得到[19]。

一般来说，用 Cramer 法则来求方程组的解时，计算量较大，所以 n 的选取不宜过大，否则就会增加计算量与信息量。只有正确的共享秘密素数才能提取出正确的阈下信息。

安全性分析：由于 $a_{ij}(1 \leqslant i,j \leqslant n)$ 的随机性，因此所得到的 $b_i(1 \leqslant i \leqslant n)$ 仍是随机的，而且 a_{ij} 的选取数量较大且排列顺序复杂，这就更增加了中间人得到阈下信息的难度。

2 方案的数值模拟

取 $n = 3$ 进行数值模拟。设共享的矩阵为

$$A = \begin{pmatrix} 2 & -11 & 5 \\ 8 & -9 & 2 \\ 3 & 1 & 1 \end{pmatrix}$$

发送者根据要发送的信息 x_i，计算出 b_i，签名分别为 $(b_i,s_i)(1 \leqslant i \leqslant 3)$，并将它们发送给阈下信息收方。信息接收方收到签名后，根据克莱姆法则解线性方程组，可得阈下信息

$$x_1 = \frac{|A_1|}{|A|} = 11\ x_2 = \frac{|A_2|}{|A|} = 29\ x_3 = \frac{|A_3|}{|A|} = 87$$

由此可以看出，如果在未知共享矩阵的情况下，很难得到正确的阈下信息。

3 结束语

在阈下信道中，阈下信息发送方所发送的信息对于看守而言是随机的，文中正式利用这一条件以及线性方程组的性质，给出了一种分割法阈下信道构造方案，并进行了安全性分析。可以看到，由于线性方程组的系数较多且排列是随机的，只有得到正确的共享秘密才能提取出正确的阈下信息。

参 考 文 献：

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

[2] Simmons G J. The subliminal channel and digital signature[J]. Advances in Crypto-logy, Proc. Eurocrypt 84, Spring-Verlag,1985:364-378。

[3] Simmons G J. Subliminal communication is easy using the DSA[J]. Advances in Cryptology,Proc. Eurocrypt 93, Spring-Verlag,1994:218-232.

[4] Simmons G J. The subliminal channels in the U.S. digital signature algorithm[J]. SPRC 93,Rome,1994:35-54.

[5] Simmons G J. Subliminal communication is easy using the DSA[C]. in Eurocrypt 93,1994,218-232.

[6] Harn L,Gong G. Digital signature with a subliminal channel[J]. IEE Proc. Comput. Digit. Tech. 1997,144(6):387-389.

[7] Jan J K,Tseng Y M. New digital signature with subliminal channels based on the discrete logarithm problem[J]. in:Proceedings of the 1999 International Workshops on Parallel Processing,1999,198-203.

[8] Anderson R. The New ton channel[A]. Lecture Notes in Computer Science 1174[C]. Springer-Verlag,1996:151-156.

[9] Zhang Fangguo, Lee B, K in K. Exploring Signature Schemes with Subliminal Channel[A]. SC IS 2003,The 2003 Symposium on Cryptography and Information Security vol 1/2[C]. Itaya,Japan,2003.245-250.

[10] Lee Narn-Yih, Yang Shu-Ya. The design of integrating subliminal channel with access control[J]. Applied Mathematics and Computation,2005,171(1):573-580.

[11] Wu Chuankun.Hash channels[J].Computers & Security,2005,24(1):653-661.

[12] 张杨松,范安东,魏 霞.基于矢量空间秘密共享的阈下信道[J].陕西理工学院学报:自然科学版,2008,24(4):34-37.

[13] 范安东,张杨松.基于中国剩余定理的阈下信道构造方案[J].陕西理工学院学报:自然科学版,2009,25(1):27-30.

[14] 张 彤,杨 波,王育民,等.封闭阈下信道的若干方法[J].通信学报,2002,23(4):17-21.

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

[16] 董庆宽,张串绒,肖国镇.数字签名中阈下信道封闭协议研究[J].西安电子科技大学,2004,31(1):87-90.

[17] Simmons G J.An Introduction to the Mathematics of Trust in Security Prococols [A]. In Proceesings: Computer Security Foundations Workshop V I.Franconia[C].New Hampshire:IEEE Computer Society Press,1993,121-127.

[18] 杨 波.现代密码学[M].北京:清华大学出版社,2004.

[19] 姚慕生.高等代数学[M].上海:复旦大学出版社,2005.

A New Scheme of Subliminal Channel Based on Partition Method

LV Xiao-qing, *ZHENG Yi*, *WEI Hang*

(School Management Sciences, Chengdu University of Technology, Chengdu 610059, China)

Abstract: A new scheme of subliminal channel is put forward based on solving the linear equations. In this scheme, the sublimimal message is divided into several irrelevant parts, and they are sent to the receiver with digital signature scheme. The receiver can use the shares with the signer and Cramer's law to recover the subliminal message.

Key words: subliminal channel; partition method; Cramer's law