第33卷 第18期 计 算 机 工 程 2007年9月
Vol.33 No.18 Computer Engineering September 2007
·安全技术· 文章编号：1000—3428(2007)18—0154—02 文献标识码：A 中图分类号：TP393.08

一类基于(*t*,*n*)门限密码的匿名潜信道方案

周宣武[1,2]，杨晓元[1,2]，魏 萍[1]，胡予濮[2]
(1. 武警工程学院网络与信息安全武警部队重点实验室，西安 710086；
2. 西安电子科技大学网络信息安全教育部重点实验室，西安 710071)

摘 要：分析了现有潜信道方案秘密信息泄漏、签名伪造、匿名身份不可追踪等安全漏洞以及潜信息滥用、协议过程复杂、签名认证运算开销大等不足之处。将门限密码与潜信道相结合，提出了一类基于(*t*, *n*)门限密码的匿名潜信道方案，实现了潜消息的门限可验证性与发送者的不可区分性，有效地保护了签名者的隐私信息，必要时又可对匿名身份实施追踪，避免了潜消息恢复权力与发送者匿名性滥用的缺陷，防止了对签名进行联合攻击和广义伪造攻击的安全隐患。方案中协议与算法安全、简洁、高效，降低了软硬件实现的系统开销，可广泛应用于计算机与无线通信等网络环境。

关键词：门限潜信道；有条件匿名性；(*t*, *n*)门限密码；多重秘密共享；身份盲化

Anonymous Subliminal Channel Scheme Based on (*t*, *n*) Threshold Cryptosystem

ZHOU Xuan-wu[1,2], YANG Xiao-yuan[1,2], WEI Ping[1], HU Yu-pu[2]
(1. Key Lab of Network and Information Security of Armed Police Force, Engineering College of Armed Police Force, Xi'an 710086;
2. Key Lab of Network and Information Security of the Education Ministry, Xidian University, Xi'an 710071)

【Abstract】 Security threats and system weakness of present subliminal channel schemes are analyzed. Combining Shamir Lagrange interpolation formula based secret-sharing scheme and subliminal channel, a threshold subliminal channel scheme with conditional anonymity based on (*t*, *n*) threshold cryptosystem is presented. The threshold secret-sharing of the scheme enables the subliminal message to be recoverable only by no less than *t* members of the *n* receivers, and the secret piece of each member can remain valid and secure after subliminal message recovering, so the scheme achieves multi-secret sharing. The probabilistic encryption algorithm and identity blinding make the subliminal message sender indistinguishable with other ordinary signers for secrecy protection, and the anonymity can also be conveniently revoked if necessary. The scheme prevents coalition attack and generalized signature forgery, avoids the misuse of subliminal message producing and recovering. Further detailed analyses also justify its brevity, security, high efficiency, and thus considerable improvement on system overheads regarding software and hardware application.

【Key words】 threshold subliminal channel; conditional anonymity; (*t*, *n*)threshold cryptosystem; multi-secret sharing; identity blinding

1983年Simmons G首次提出了潜信道(subliminal channel)的概念。潜信道是一种隐蔽信道，可用来向授权的接收人发送秘密信息，但任何未经授权的接收人无法发现该消息。潜信道有许多应用，潜信道的研究已受到越来越多的关注[1~4]。

(*t*,*n*)门限密码(threshold cryptosystem)最早是由Shamir和Blakley于1979年独立提出的，同时，他们分别基于Lagrange插值算法和多维空间点的性质提出了第1个(*t*,*n*)门限秘密共享方案。(*t*,*n*)门限秘密共享方案能够将一个秘密分给*n*个成员，使得至少*t*个成员合作才能恢复该秘密。秘密共享是信息安全和数据保密中的一项重要技术，它在重要信息和秘密数据的安全保存、传输及合法利用中起着非常关键的作用[5]。

本文将门限密码与潜信道相结合，基于椭圆曲线密码(elliptic curve cryptosystem, ECC)提出了一类匿名门限潜信道方案。利用椭圆曲线离散对数问题(elliptic curves discrete logarithm problem, ECDLP)设计单向陷门函数，发挥了椭圆曲线密码系统密钥量小、效率高的优势。在同等安全强度下，算法可用较小的开销(计算量、存储量、带宽、软件和硬件实现的规模等)和时延(加密和签名速度快)实现较高的安全性。

1 基于ECC的匿名门限潜信道方案

1.1 参数设定

鉴于安全性和执行效率的考虑，系统参数设定如下：

E为特征值 $Char(F_q)>3$ 的有限域，定义该域上的椭圆曲线E。$E: y^2 = x^3 + ax + b$ ($a,b \in F_q$, $4a^3+27b^2 (\mathrm{mod}\, q) \neq 0$。$q$为$n$-bits的素数 $n \geq 190$)，$P \in E(F_q)$是一个公开基点，P的阶为L ($L \geq 120$ bits)，$\#E(F_q)$为椭圆曲线的阶，至少有50位以上的大素因子。Ψ表示一个从$P=(x,y)$到x的单射函数，将其记为$(P)_x$。$\{V_1, V_2, \ldots, V_n\}$是由$n$个成员组成的潜信息接收组，$k_i \in Z_q^*$ ($i=0,1,2,\ldots,n$)分别为潜消息发送者S与V_i ($i=1,2,\ldots,n$)的私钥。h为安全无碰撞散列函数。$m_s \in Z_q^*$为

基金项目：国家自然科学基金资助项目(60473029)；教育部计算机网络与信息安全重点实验室开放课题基金资助项目(200409)
作者简介：周宣武(1980－)，男，硕士，主研方向：网络通信与信息安全；杨晓元，教授；魏 萍，副教授；胡予濮，教授、博士生导师
收稿日期：2006-10-13 **E-mail：**schwoodchow@163.com

待发送的潜消息。

1.2 协议初始化

step1 每个成员$V_i(i=1,2,\ldots,n)$秘密地将其公私钥对$(K_i=k_i,P,k_i)$发送到潜消息发送者S。

step2 对潜消息m_s，S构造Z_q上的t-1 次多项式

$$f(x)=a_0+a_1x+a_2x^2+\ldots+a_{t-1}x^{t-1}(a_0=m_s)$$

设 a 是 $GF(q)$ 的本原元素(显然 a 满足 $\delta_q(a)=\phi(q)>n$), 计算

$$m_i=f(a^i)\quad (i=0,1,2,\ldots,n) \tag{1}$$

其中，$m_i(i=1,2,\ldots,n)$作为成员V_i的消息分片。

step3 S 计算

$$u=f(a^{n+1})(\mathrm{mod}\ q) \tag{2}$$

$$v=h(m_s\|u) \tag{3}$$

1.3 签名生成协议

step1 对于消息 m，S 计算

$$C_i=m_iP\quad (i=0,1,2,\ldots,n) \tag{4}$$

$$h=h(m\|v\|(C_0)_x\|(C_1)_x\|\cdots\|(C_n)_x) \tag{5}$$

$$s_i=m_i-hvk_i(\mathrm{mod}\,q)\quad (i=0,1,2,\ldots,n) \tag{6}$$

step2 S发布$\sigma=(m,v,h,s_0,s_1,\ldots,s_n)$作为对消息$m$的签名。

1.4 签名验证协议

step1 任何合法的验证者都可以通过下式验证签名。

验证者首先检验

$$C_i?=s_iP+hvK_i\quad (i=0,1,2,\ldots,n) \tag{7}$$

step2 验证者验证

$$h?=h(m\|v\|(C_0)_x\|(C_1)_x\|\cdots\|(C_n)_x) \tag{8}$$

如果式(7) 、式(8)成立，则验证者接受$\sigma=(m,v,h,s_0,s_1,\ldots,s_n)$为一个有效的签名，否则为非法签名。

1.5 潜消息恢复协议

step1 每个成员V_i恢复出相对应的子消息

$$m_i=s_i+hvk_i(\mathrm{mod}\,q)\quad (i=1,2,\ldots,n) \tag{9}$$

step2 t个成员联合计算(假设为$V_1,V_2,\ldots,V_t$)

$$f(x)=\sum_{i=1}^{t}m_i\prod_{j=1,j\neq i}^{m}[(x-a^j)(a^i-a^j)^{-1}] \tag{10}$$

$$f(0)=a_0=m_s \tag{11}$$

1.6 潜消息验证协议

step1 成员计算

$$u=f(a^{n+1})(\mathrm{mod}\ q) \tag{12}$$

step2 验证

$$v?=h(m_s\|u) \tag{13}$$

若验证通过，则说明潜消息被正确恢复。

在群签名验证式(7)中

$$s_iP+hvK_i=(s_i+hvk_i)P$$

由式(6) $s_i=m_i-hvk_i(\mathrm{mod}\,q)$

$$\Rightarrow s_i+hvk_i=m_i(\mathrm{mod}\,q)\quad (i=0,1,2,\ldots,n)$$

$$\Rightarrow s_iP+hvK_i=m_iP=C_i\quad (i=0,1,2,\ldots,n)$$

$$\Rightarrow h=h(m\|v\|(C_0)_x\|(C_1)_x\|\cdots\|(C_n)_x)$$

这就证明了签名的正确性。

根据 Lagrange 插值公式，过$(a^i,\ m_i)(i=1,2,\ldots,t)$有一个 t -1 次多项式：

$$p(x)=m_1\frac{(x-\alpha^2)(x-\alpha^3)\cdots(x-\alpha^t)}{(\alpha-\alpha^2)(\alpha-\alpha^3)\cdots(\alpha-\alpha^t)}+m_2\frac{(x-\alpha)(x-\alpha^3)\cdots(x-\alpha^t)}{(\alpha^2-\alpha)(\alpha^2-\alpha^3)\cdots(\alpha^2-\alpha^t)}+\ldots+m_t\frac{(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{t-1})}{(\alpha^t-\alpha)(\alpha^t-\alpha^2)\cdots(\alpha^t-\alpha^{t-1})}$$

$$=\sum_{i=1}^{t}m_i\prod_{j=1,i\neq j}^{t}\frac{(x-\alpha^j)}{(\alpha^i-\alpha^j)}$$ ，易证

$p(x)=f(x)=a_0+a_1x+a_2x^2+\ldots+a_{t-1}x^{t-1}$，则

$$p(0)=\sum_{i=1}^{t}m_i\prod_{j=1,i\neq j}^{t}\frac{(-\alpha^j)}{(\alpha^i-\alpha^j)}$$

$$=\sum_{i=1}^{t}m_i\prod_{j=1,j\neq i}^{t}[-a^j(a^i-a^j)^{-1}]$$

$$=f(0)=a_0=m_s$$

同时潜消息验证协议式(12)、式(13)与协议初始化协议式(2)、式(3)相同。这就证明了潜消息恢复及验证协议的正确性。

2 方案分析

该方案除体现了现有潜信道方案的优点外，还具有以下特点：

(1)潜消息的门限可验证性。据 Lagrange 插值公式，t 个以上的用户联合他们的消息分片(a^i,m_i)通过式(10)及式(11)就可以恢复出潜消息 m_s，且联合恢复在计算上也是可行的。基于 Lagrange 插值公式的门限方案是已经证明的完备的(t,n)门限秘密共享方案，少于 t 个的用户联合无法恢复潜消息。方案实现了潜消息的门限可验证性，有效地防止了潜消息恢复权力的滥用，符合电子商务、电子政务等网络业务中联合监督、追踪的要求。

(2)潜消息的安全性。潜消息m_s经过了哈希函数处理，攻击者从 $v=h(m_s\|u)$ 恢复出m_s就必须攻击哈希函数的单向性以及中间参数u，由于h为安全无碰撞散列函数，因此在计算上是不可行的。若攻击者通过重新构造$f(x)$攻击m_s，但是在掌握至少t个成员的消息分片m_i之前，攻击也是不成立的。若多个内部成员联合攻击潜消息，由以上分析可知，也必须得到至少t个成员的消息分片，由于这些分片信息针对具体潜消息都是独立随机产生的，其他成员除了自己的消息分片外，并未得到任何其他成员的分片信息，因此内部成员联合攻击的攻击能力并不比单个攻击者及外部攻击者更具优势。

(3)签名的不可伪造性。生成合法签名σ的前提是掌握潜信息m_s、中间参数u以及n+1 个消息分片m_i，攻击由$C_i=m_iP$攻击消息分片m_i是求解多重的椭圆曲线离散对数问题，这在计算上是不可行的。若潜信息接收成员联合伪造发送者S的签名，即使所有成员联合得到了m_s、u以及n个消息分片$m_i$$(i=1,2,\ldots,n)$，联合攻击者仍然不能通过$C_0=m_0P$得到发送者$S$的分片消息$m_0$，因为这同样是求解ECDLP问题。所以所有潜信息接收成员的联合伪造攻击并不比单个攻击者及外部攻击者更具优势。

(4)潜信息使用的责任性。在签名信息σ中通过式(6)嵌入了潜信息发送者S及所有接收成员的私钥信息k_i，并且在验证式(7)中出现了所有成员及S的公钥k_i，产生、接收潜信息必须掌握相应的私钥，因此，潜信息发送者及所有接收者都对潜信息的使用负有责任，方案有效地防止了潜消息使用权力的滥用。

(5)潜信息发送者的不可区分性。潜信道的内部成员$V_i$$(i=1,2,\ldots,n)$知道带有潜信息的签名是由发送者$S$产生，但是对其他人来说，签名只是一个由$n$+1 个成员共同生成的多重签名。同时，在生成潜信息的多重签名中，所有成员及发送者S的签名私钥并无任何区别，除了成员$V_1,V_2,\ldots,V_n$以外，没有人可以确定发送者S的身份，方案实现了发送者身份的

(下转第 158 页)