一种面向群组通信的通用门限签密方案

彭长根,李 祥,罗文俊
(贵州大学计算机软件与理论研究所,贵州贵阳 550025)

摘 要: 基于椭圆曲线密码体制和 Schnorr 数字签名体制,建立了一个同时具有 (t, n) 门限签密和 (k, l) 共享验证功能的通用门限方案. 该方案克服了 Wang 等人方案的安全缺陷和 Hsu 等人方案的弱点;以较小的通信代价和高效的运算在群组通信中实现了保密性和认证性;在不暴露接收组的私钥和消息 m 的情况下,利用公开验证功能实现了发送方的不可抵赖性;另外,该方案还可以防止消息的猜测攻击,从而实现了语义安全性.

关键词: 门限签密; 共享验证; 群组通信; 椭圆曲线密码体制
中图分类号: TP309, TN918 **文献标识码**: A **文章编号**: 0372-2112 (2007) 01-0064-04

A Generalized Group-Oriented Threshold Signcryption Schemes

PENG Chang-gen, LI Xiang, LUO Wen-jun
(Institute of Computer Science, Guizhou University, Guiyang, Guizhou 550025, China)

Abstract: A generalized group-oriented threshold signcryption scheme based on elliptic curve cryptosystem and Schnorr's signature schemes is proposed in this paper. This scheme simultaneously fulfills the (t, n) threshold signcryption and the (k, l) threshold shared verification, and it has improved the drawbacks of Wang et al.'s scheme and Hsu et al.'s scheme. Our scheme provides both confidentiality and authenticity for group communication with lower communication cost and more efficient computation. Without divulging recipient's private key and the message m, non-repudiation of sender is provided by means of public verifiability in our scheme. In addition, our scheme can achieve semantic security by preventing the message guess attack.

Key words: threshold signcryption; shared verification; group communication; elliptic curve cryptosystem

1 引言

签密 (signcryption) 是 Zheng[1] 在 1997 年提出的一个新的认证加密 (authenticated encryption) 方案,它是指在一个单一的逻辑步骤中,能同时实现数字签名和公钥加密两项功能,并且它的计算代价远比传统的"先签名后加密"方法低得多. 自 Desmedt 提出群组密码学的概念以来,其研究越来越受到重视,应用也越来越广泛,同时也出现了不少面向群组通信的门限认证加密 (签密) 方案[2~5]. 为了使面向群组的门限认证加密方案更具有一般性和通用性,2000 年 Wang 等[6] 首次提出了一个面向群组通信的门限认证加密方案 (简称 WCL 方案),该方案同时实现了 (t, n) 门限签名加密功能和 (k, l) 共享验证功能. 但在此之后,相继有文献指出 WCL 方案存在一些安全缺陷[3,7~9],其中文献[3]指出 WCL 方案不是真正意义下的门限方案,文献[9]指出 Tseng 等[7] 对 WCL 方案的攻击和改进方案都是无效的,并从另一角度指出 WCL 方案存在的安全缺陷,但在文中未提出改进方案;而 Hsu 等[8] 的改进方案 (简称 HWW 方案) 需要密钥分配中心 KDC 始终参与签名加密阶段,且计算效率低. 所以建立一个安全有效的面向群组通信的通用门限签密方案,应该是一件有意义的工作.

本文基于椭圆曲线离散对数困难问题 (ECDLP) 和 Schnorr 数字签名体制,结合 Zheng 的签密思想,建立了一个新的面向群组通信的通用门限签密方案,该方案同时具有 (t, n) 门限签密功能和 (k, l) 共享验证功能,并克服了 WCL 方案的安全缺陷和 HWW 方案的弱点;方案在不暴露接收组的私钥和消息 m 的情况下,可以通过将签密转换成普通签名实现公开验证功能,以揭露发送方的抵赖;另外,该方案还克服了目前一些认证加密方案在抵抗已知明文攻击和消息猜测攻击方面的漏洞. 因此,本文所提出的方案实现了认证性、保密性、数据完整性和发送方的不可抵赖性. 由于方案是基于椭圆曲线密码体制建立,因而运算效率比 HWW 方案高得多,通信代价也较小.

2 一种新的面向群组通信的通用门限签密方案

本文提出的面向群组通信的门限签密方案共分为四个阶段:参数选择及密钥分配阶段、(t, n) 门限签密阶段、(k, l) 共享验证及消息恢复阶段和公开验证阶段.

2.1 参数选择及密钥分配阶段

这一阶段将利用 Shamir 秘密共享方案实现密钥分配,并用 Pedersen-VSS[10] 可验证方法实现对密钥分配中心 KDC 的欺

收稿日期:2005-05-24;修回日期:2006-09-26
基金项目:贵州省自然科学基金 (No. 2005-2107);贵州省省长基金 (No. 2005-368)

诈行为检测. 在本方案中,签密组记为 $G_S=(S_1,S_2,\cdots,S_n)$,验证接收组记为 $G_V=(V_1,V_2,\cdots,V_l)$,设 $(E_K(\cdot),D_K(\cdot))$ 是一对关于密钥 K 的对称加密/解密算法. 首先 KDC 选择一个单向无碰撞 hash 函数 $H(\cdot)$,并在有限域 F_p 上选择一条安全的椭圆曲线 $E(F_p)$ 和一个阶为 q 的基点 P,q 是一个大于 160bit 的大素数;然后随机选择 $x_s,x_v\in Z_q^*$ 分别作为组 G_S 和组 G_V 的私钥,则相应的公钥为 $Q_s=x_s\cdot P$ 和 $Q_v=x_v\cdot P$;最后 KDC 用下述方法为组 G_S 和组 G_V 的每个成员分配密钥:

(1) 由 Shamir 秘密共享方案,KDC 首先在 Z_q 上分别随机选择次数为 $t-1$ 和 $k-1$ 的多项式:

$$f_s(x)=a_0+a_1x+\cdots+a_{t-1}x^{t-1}\bmod q$$

$$f_v(x)=c_0+c_1x+\cdots+c_{t-1}x^{k-1}\bmod q$$

其中 $a_0=f_s(0)=x_s$,$c_0=f_v(0)=x_v$,$a_i,c_j\in Z_q^*$ $(i=1,2,\cdots,t-1,j=1,2,\cdots,k-1)$. 然后计算 $x_{si}=f_s(i)$ 和 $Q_{si}=x_{si}\cdot P$ 分别作为 S_i 的私钥和公钥 $(i=1,2,\cdots,n)$,$x_{vj}=f_v(j)$ 和 $Q_{vj}=x_{vj}\cdot P$ 分别作为 V_j 的私钥和公钥 $(j=1,2,\cdots,l)$.

(2) KDC 分别将子钥 x_{si} 和 x_{vj} 通过安全信道传送给 S_i $(i=1,2,\cdots,n)$ 和 V_j $(j=1,2,\cdots,l)$,并把 $a_i\cdot P$ $(i=1,2,\cdots,t-1)$ 和 $c_j\cdot P$ $(j=1,2,\cdots,k-1)$ 分别广播给组 G_S 的 n 个成员和组 G_V 的 l 个成员.

最后,KDC 公开参数:$E(F_p)$,P,p,q,$H(\cdot)$,Q_s,Q_v,Q_{si} $(i=1,2,\cdots,n)$,$(j=1,2,\cdots,l)$.

根据 Pedersen-VSS 验证方法,G_S 的每个成员 S_i $(i=1,2,\cdots,n)$ 可通过等式(1)验证 KDC 分配给自己的私钥 x_{si} 的有效性:

$$x_{si}\cdot P=\sum_{j=0}^{t-1}i^j\cdot(a_j\cdot P)\qquad(1)$$

若等式成立,则 S_i 收到的子密钥 x_{si} 正确,否则出现 KDC 欺诈. 同理,G_V 的每个成员 V_j $(j=1,2,\cdots,l)$ 也可通过类似的方法验证自己私钥 x_{vj} 的正确性.

2.2 (t,n)门限签密阶段

本阶段将实现由签密组 G_S 的 t 个成员对消息 $m\in Z_p^*$ 进行门限签密(少于 t 个成员无法完成签密). 假设这 t 个签密成员记为 $S=\{S_i\}_{i\in A}$,这里 $A\subseteq\{1,2,\cdots,n\}$ 且 $|A|=t$,并从 S 中随机选择一名成员作为签密合成员. 假设消息 m 包含足够的冗余信息,以便接收组在恢复该消息后能进一步判断其有效性. 签密操作利用 Schnorr 数字签名方案并结合 Zheng 的签密思想实现,具体操作步骤如下:

Step 1:每个签密成员 S_i $(i\in A)$ 随机选取一个整数 $k_i\in Z_p^*$,计算 $Y_{i1}=k_i\cdot P=(x_{i1},y_{i1})$,$y_{i2}=k_i\cdot Q_v=(x_{i2},y_{i2})$. 如果 $x_{i1}=0$ 或 $x_{i2}=0$,重新选择 k_i. 然后将 Y_{i1},Y_{i2} 通过安全信道发送给其它签密成员.

Step 2:每个签密成员 S_i $(i\in A)$ 首先计算:$Y_1=\sum_{i\in A}Y_{i1}=(x_1,y_1)$,$Y_2=\sum_{i\in A}y_{i2}=(x_2,y_2)$ 然后计算部分签名:

$$r=H(H(m),Q_v,x_1,x_2),\ s_i=k_i-x_{si}\cdot l_i\cdot r\bmod q$$

其中 $l_i=\prod_{j\in A,j\neq i}\frac{-j}{i-j}\bmod q$. 最后将部分签名 s_i 交给签密合成员.

Step 3:签密合成员收到部分签名 s_i 后,利用 S_i $(i\in A)$ 的公钥 Q_{si} 验证部分签名 s_i 的有效性,其验证等式为:

$$Y_{i1}=(r\cdot l_i\bmod q)\cdot Q_{si}+s_i\cdot P\qquad(2)$$

若等式成立,则部分签名 s_i 有效. 如果所有的 s_i 都有效,则计算合成签名 $s=\sum_{i\in A}s_i$,并用 $K=H(x_2)$ 作为对称钥加密消息 m,密文为 $c=E_k(m)$.

Step 4:签密合成员将签密 (c,r,s) 通过公开信道发送给接收组 G_V.

2.3 (k,l)共享验证及消息恢复阶段

接收组 G_V 收到签密 (c,r,s) 后,由 l 个成员中的 k 个来完成签密的验证和消息的恢复,假设这 k 个验证成员记为 $V=\{V_j\}_{j\in B}$,这里 $B\subseteq\{1,2,\cdots,L\}$ 且 $|B|=k$,并从这 k 个验证成员中随机选择一名作为验证执行员. 具体操作步骤如下:

Step 1:每个成员 V_j $(j\in B)$ 计算 $Y_1=r\cdot Q_s+s\cdot P=(x_1,y_1)$,$Y_{j2}=(x_{vj}\cdot l_j\bmod q)\cdot Y_1$,其中 $l_j=\prod_{i\in B,i\neq j}\frac{-i}{j-i}$. 然后将 Y_{j2} 交给验证执行员.

Step 2:验证执行员首先计算 $Y_2=\sum_{j\in B}Y_{j2}=(x_2,y_2)$,然后用密钥 $K=H(x_2)$ 恢复消息 $m=D_K(c)$,最后验证等式 $r=H(H(m),Q_v,x_1,x_2)$ 是否成立,. 如果等式成立,则签密通过验证,并进一步从 m 的冗余信息验证消息的有效性.

2.4 公开验证阶段

如果后来签密组 G_S 否认其对消息 m 的签密,则可通过以下操作进行公开验证,以证明 G_S 的欺骗:

Step 1:接收组 G_V 首先将签密 (c,r,s) 转换成普通签名 (m,r,s),然后将 $(H(m),r,s)$ 和 x_2 交给第三方验证.

Step 2:第三方先求出 $r\cdot Q_s+s\cdot P=(x_1,y_1)$,然后验证等式 $r=H(H(m),Q_v,x_1,x_2)$ 是否成立. 如果等式成立,则确信签密是发送给 G_V 的,因为 r 中包含接收组 G_V 的公钥 Q_v.

2.5 方案的正确性证明

定理 1 在 (t,n) 门限签密阶段,部分签名 s_i 的有效性可通过式(2)得以验证.

证明:若签密成员 S_i $(i\in A)$ 没有欺诈行为,则有

$$(r\cdot l_i\bmod q)\cdot Q_{si}+s_i\cdot P=(r\cdot l_i\bmod q)\cdot Q_{si}+((k_i-x_{si}\cdot l_i\cdot r)\bmod q)=(r\cdot l_i\bmod q)\cdot Q_{si}+k_i\cdot P-(r\cdot l_i\bmod q)\cdot(x_{si}\cdot P)=k_i\cdot P=Y_{i1}$$

即式(2)成立,证毕.

定理 2 若签密组 G_S 能严格遵循签密步骤,则指定接收组 G_V 的 k 个诚实成员就能正确恢复消息 m 并进行有效性验证;第三方也能够正确对签密进行公开验证.

证明:若签密组 G_S 能严格遵循签密步骤,就有

$$\begin{aligned}r\cdot Q_s+s\cdot P&=r\cdot(x_s\cdot P)+\sum_{i\in A}S_i\cdot P\\&=r\cdot x_s\cdot P+\left(\sum_{i\in A}(k_i-x_{si}\cdot l_i\cdot r)\bmod q\right)\cdot P\\&=r\cdot x_s\cdot P+\sum_{i\in A}k_i\cdot P-\left(\sum_{i\in A}x_{si}\cdot l_i\bmod q\right)\cdot r\cdot P,\end{aligned}$$

由 Lagrange 插值多项式性质有:

$$\sum_{i\in A}x_{si}\cdot l_i\bmod q=\sum_{i\in A}f_s(i)\cdot\prod_{j\in A,j\neq i}\frac{-j}{j-i}\bmod q$$

$= f_s(0) = x_s$,

所以有 $r \cdot Q_s + s \cdot P = \sum_{i \in A} k_i \cdot P = \sum_{i \in A} Y_{i1}$.

又因为 $\sum_{j \in B} Y_{j2} = \left(\sum_{j \in B} x_{vj} \cdot l_j \bmod q \right) \cdot Y_1$,由 Lagrange 插值多项式有:

$$\sum_{j \in B} x_{vj} \cdot l_j \bmod q = \sum_{j \in B} f_v(j) \cdot \prod_{i \in B, i \neq j} \frac{-i}{j-i} \bmod q = f_v(0) = x_v$$

则 $\sum_{j \in B} Y_{j2} = x_v \cdot Y_1 = x_v \cdot \sum_{i \in A} k_i \cdot P = \sum_{i \in A} k_i \cdot Q_v = \sum_{i \in A} Y_{i2}$.

这样指定接收组 G_V 的 k 个诚实成员就能正确求出 x_1 和 x_2,从而可以用密钥 $K = H(x_2)$ 正确恢复消息 $m = D_K(c)$,并能正确通过等式 $r = H(H(m), Q_v, x_1, x_2)$ 进行有效性验证,第三方也能正确通过该等式进行公开验证,证毕.

2.6 安全性分析

(1) 克服了 WCL 方案的安全缺陷

文献[7]指出在 WCL 方案中,存在攻击者能够求出签名组的私钥和会话钥的安全缺陷,而文献[9]指出了 WCL 方案存在当攻击者知道一组有效签密后就能够恢复其它消息的缺陷(已知明文攻击). 我们的方案克服了这些缺陷,首先若攻击者要从公开的信息求出签密方或接收方的私钥,它必须面对 ECDLP;其次我们方案采用的对称加密方法可以防止已知明文攻击,而攻击者要求出对称钥 $K = H(x_2)$,他必须要知道 k_i $(i \in A)$ 或验证参与者的私钥 x_{vj} $(j \in B)$.

(2) 具有不可伪造性

攻击者要伪造签名 (r, s) 是不可能的,首先他若要从等式 $s = k - x_s \cdot r \bmod q$(其中 $k = \sum_{i \in A} k_i$) 伪造 (r, s),他必须要知道签密组的私钥 x_s 和 k_i $(i \in A)$;其次,若要从等式 $r \cdot Q_s + s \cdot P = k \cdot P$ 伪造 (r, s),他只能先伪造 (k, r) 或 (k, s),然后求出 s 或 r,这都需要面对 ECDLP. 同样接收组要伪造签名 $(H(m), r, s)$ 欺骗第三方的公开验证也是不可能的,他需先伪造 (x_1, y_1),然后求出 $(x_2, y_2) = x_v \cdot (x_1, y_1)$,再从验证等式中求出 $r = H(H(m), Q_v, x_1, x_2)$,最后从等式 $r \cdot Q_s + s \cdot P = (x_1, y_1)$ 求出 s,这时他就必须求解 ECDLP.

(3) 具有签密组的不可抵赖性

如果签密组否认其签密,接收方可以将签密 (c, r, s) 转换成普通签名 $(H(m), r, s)$ 交给第三方验证. 由于验证等式 $r = H(H(m), Q_v, x_1, x_2)$ 包含指定接收方的公钥 Q_v,所以任何其他第三人都不能宣称自己是合法的接收者. 同样,由于签名 (r, s) 包含签密组的私钥 x_s,签密组也不能否认她对 m 的签密. 这种公开验证方法不会暴露接收组的私钥和消息 m,也不需要发送方的合作.

(4) 具有防止消息猜测攻击的能力(语义安全性)

语义安全(semantic security)是指攻击者不能确定它所猜测的消息是否为原始签名者所签的实际消息,即具有消息的不可分辨性(indistinguishability),这种猜测即使在攻击者知道了签名的情况下也不能成功. 但是目前的一些认证加密方案普遍存在不能抵抗这种猜测攻击的弱点:如果攻击者截获了一组有效签名 (r, s),他就可以利用验证等式猜测所发送的消息,对于明文空间较小的情况,这种攻击是有效的. 我们的方案可以防止这种消息猜测的攻击,攻击者要从验证等式 $r = H(H(m), Q_v, x_1, x_2)$ 猜测所发送的消息 m 是否为签名者所签的实际消息是不可能的,因为他不知道 x_2,而要求出 x_2,必须要知道 $k = \sum_{i \in A} k_i$ 或接收方的私钥 x_v.

(5) 具有密钥分配的可验证性

在子密钥分配阶段,签密组成员可以通过式(1)验证 KDC 分配给自己密钥的正确性,接收组成员也可用类似的方法验证所得到密钥的正确性.

(6) 具有部分签密的有效性验证

在签密阶段,签密合成员可以通过式(2)验证部分签名的有效性,以检测签密成员的恶意欺诈.

(7) 具有门限方案的安全性

由于方案是基于 Shamir 秘密共享方案建立,因此在签密阶段和验证阶段都具有门限方案的安全性:任意少于 t 个合法签密者无法得到有效的签密,任意少于 k 个合法的验证者无法合谋进行签密验证和恢复消息.

另外,为了避免消息重放,可在消息 m 中增加足够的冗余信息,用于进一步检验消息的有效性.

2.7 方案的效率分析

由于 WCL 方案和 Tseng 等[7]的方案存在安全漏洞,因此这里只将本文方案与 HWW 方案的效率进行比较. HWW 方案是基于 DLP 建立,其最为耗时的运算是幂模运算,用 T_e 表示,我们的方案是基于 ECDLP 建立,其最耗时的运算是点乘运算,用 T_p 表示. 假设取 $|p| = 1024$bit, $|q| = 160$bit,文献[11]指出 T_p 的速度大约比 T_e 快 8 倍. 表 1 给出了本文方案与 HHW 方案的通信代价和计算代价的比较分析.

表 1 通信代价及计算代价比较

	HWW 方案	本文方案
签密长度	$\|p\| + \|q\|$	$\|p\| + 2\|q\|$
总通信代价	$2t(t-1)\|p\| + (t+k)\|q\|$	$2t(t-1)\|q\| + (t+k)\|q\|$
签密计算量	$9tT_e$	$4tT_p$
验证及消息恢复计算量	$3tT_e$	$4tT_p$

从表 1 可以看出,HWW 方案的签密长度比本文方案短些,但从签密成员之间、签密成员与签密合成员之间和验证成员与验证执行员之间的总通信代价来看,本文方案的通信代价更小,而且还可以通过对椭圆曲线点进行压缩以进一步降低通信量. 对于运算复杂度,本文方案的运算效率比 HWW 方案高得多.

HWW 方案除了计算代价太大的缺点之外,还有一个弱点:每次签密的产生都需要 KDC 参加,在每次签密时,KDC 都需要重新选择会话多项式,并将会话私钥通过安全通道发送给签密参与者,同时向接收组广播会话公钥. 而本文的方案在系统参数产生后,就不再需要 KDC 的参与.

3 结束语

目前大多数面向群组的签密方案都是 (t, n) 门限签密功能和 (k, l) 门限共享验证功能分开的,因此同时具有门限签密

功能和门限共享验证功能的群组签密方案,在当前更具有通用性和应用价值,但目前已有的几个方案都存在安全缺陷或弱点.在这种情况下,本文基于椭圆曲线密码体制和 Schnorr 数字签名体制,结合 Zheng 的签密思想,设计了一个同时具有门限签密功能和门限共享验证功能的通用门限方案,该方案不但克服了目前一些方案的缺陷和弱点,而且具有更高的实现效率.方案除了实现保密性、认证性和数据完整性外,还可以利用公开验证功能防止发送方的抵赖,并可抵抗消息的猜测攻击以实现语义安全性.相对于目前的一些认证加密方案,我们的方案除了具有通用性外,其安全性考虑更全面.

参考文献:

[1] Yuliang Zheng. Signcryption and its application in efficient public key solutions [A]. LNCS1396, Information Security Workshop (ISW '97) [C]. Berlin: Springer-Verlag, 1997. 291 - 312.

[2] Chien-Lung Hsu, Tzong-Chen Wu. Authenticated encryption scheme with shared verification [J]. IEE-Computer Digital Technology, 1998, 145(2): 117 - 120.

[3] 曹珍富,李继国,李建中. 一个新的具有指定接收组(t, n)门限签名加密方案[J]. 通信学报. 2003, 24(5): 8 - 13.
Cao Zhen-fu, Li Ji-guo, Li Jian-zhong. A new (t, n) threshold signature encryption scheme with the specified receiver [J]. Journal of China Institute of Communications, 2003, 24(5): 8 - 13. (in Chinese)

[4] 李继国,曹珍富,李建中. 具有指定接收组(t, n)门限共享验证签名加密方案[J]. 电子学报, 2003, 31(7): 1086 - 1088.
Li Ji-guo, Cao Zhen-fu, Li Jian-zhong. (t, n) threshold shared verification signature encryption scheme with specified receiving groups [J]. Acta Electronica Sinica, 2003, 31(7): 1086 - 1088. (in Chinese)

[5] 张彰,蔡勉,肖国镇. 一个高效的门限共享验证签名方案及其应用[J]. 通信学报, 2003, 24(5): 134 - 139.
Zhang Zhang, Cai Mian, Xiao Guo-zhen. An efficient threshold shared verification signature scheme and its application [J]. Journal of China Institute of Communications, 2003, 24(5): 134 - 139. (in Chinese)

[6] Ching-Te Wang, Chin-Chen Chang, Chu-Hsing Lin. Generalization of threshold signature and authenticated encryption for group communication [J]. IEICE Transactions on Fundamentals, 2000, E83-A(6): 1228 - 1237.

[7] Yuh-Min Tseng, Jinn-Ke Jan, Hung-Yu Chien. On the security of generalization of threshold signature and authenticated encryption for group communication [J]. IEICE Transactions on Fundamentals, 2001, E84-A(10): 2606 - 2609.

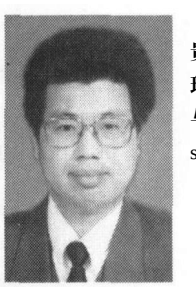
[8] Chien-Lung Hsu, Tzong-Sun Wu, Tzong-Chen Wu. Improvements of generalization of threshold signature and authenticated encryption for group communication [J]. Information Processing Letter, 2002, 81(1): 41 - 45.

[9] Shuhong Wang, Guilin Wang, Feng Bao, Jie Wang. Security notes on generalization of threshold signature and authenticated encryption for group communication [J]. IEICE Transactions on Fundamentals, 2004, E87-A(12): 3443 - 3446.

[10] T P Pedersen. Distributed provers with applications to undeniable signatures [A]. LNCS 547, Proc. of Eurocrypt '91 [C]. Berlin: Springer-Verlag, 1991. 221 - 242.

[11] N Koblitz, A Menezes, S Vanstone. The state of elliptic curve cryptography [J]. Designs, Codes, and Cryptography, 2000, 19(2-3): 173 - 193.

作者简介:



彭长根　男,1963 年出生于贵州锦屏县,贵州大学副教授,现为贵州大学计算机软件与理论研究所博士研究生,主要研方向为密码学与信息安全. E-mail: cgpeng63@sohu.com 或 sci.cgpeng@gzu.edu.cn

李　祥　男,1942 年出生于贵州安顺市,贵州大学教授,博士生导师,主要研究方向为计算复杂性,可计算性理论,计算机密码与信息安全.

罗文俊　男,1966 年出生于贵州绥阳县,贵州大学教授,博士,主要研方向为计算机密码与信息安全.