一个基于ECC的ElGamal型(t,n)门限数字签名方案*)

张险峰　秦志光　刘锦德

(电子科技大学计算机学院IBM技术中心　成都610054)

An ElGamal_type(t,n)Threshold Digital Signature Scheme Based on ECC

ZHANG Xian-Feng　QIN Zhi-Guang　LIU Jin-De

(IBM Technology Center, College of Computer Science and Engineering ,UEST of China Chendu 610054)

Abstract This paper comprehensively introduces and analyzes Shamir Secret Sharing, Pedersen's Verifiable Secret Sharing based on ECC, verifiable secret sharing without a trusted center based on ECC and an ElGamal digital signature scheme based on ECC. Based on the theoretical introduction, an ElGamal_type(t, n) threshold digital signature scheme Based on ECC is designed. The performance of the scheme is analyzed. And an application based on the scheme is described. In the scheme, a trusted center to deal with the sharing secret is eliminated. No secret communication is required in the signature issuing phase. The scheme is characterized by excellent security as well as high efficiency.

Keywords Network security, Elliptic curve cryptography(ECC), ElGamal, Threshold digital signature, Secret Sharing

1 引言

门限数字签名是门限密码学的一个重要分支.将公司或团体的数字签名密钥以(t,n)门限方案分散给多人管理有多种好处.例如,(1)攻击者要想得到签名密钥必须得到t个"部分密钥"(亦称共享),这通常比较困难.(2)即使某个或某些部分密钥丢失,比如,存放某部分密钥的地点发生火灾,整个密钥也不会丢失.(3)实现权力分配,避免滥用职权:某些重大决定可能需要决策者的某些特定组合集体签署才能生效,签名密钥的共享使此变为可能[1].

1989年,Desmedt和Frankel提出了一个有效的ElGamal型(t,n)门限公钥密码系统[2],其特点:(1)(t,n)成员必须合作来对一密文进行解密.(2)任何≤t-1个不诚实的成员不能解密任何密文.该方案要求一个可信中心来生成和分配共享秘密.接着,Hwang和Pedersen证明可以不用可信中心[3,5].Pedersen的系统利用了非交互的可验证秘密共享(Verifiable Secret Sharing,VSS)方案[6].

1991年,Park和Kurosawa提出了一个不需要可信中心的ElGamal型(t,n)门限数字签名方案[7].适用于本方案的ElGamal型数字签名只是共享秘密的线性组合.然而,此方案要求签名者在通过网络交换信息时需秘密通信.

鉴于椭圆曲线密码体制(Elliptic Curve Cryptography, ECC)在加密强度、执行速度和密钥长度等方面所具有的独特优势,本文在基于ECC的基础上,提出了一个有效的、不需要可信中心的和在签名发布阶段不需秘密通信的ElGamal型(t,n)门限数字签名方案,该ElGamal型数字签名仅是一些共享秘密的线性组合.

2 理论基础

本文中,设p和q是大素数,E为椭圆曲线,基点P为椭圆曲线E上的一点,其阶为q,p,q,E和P公开,Z_q为有限域,其元素数(阶)为q.在我们提出的方案中,我们采用以下的几个基本方法来实现秘密共享.

2.1 Shamir秘密共享

Shamir秘密共享是一个(t,n)门限秘密共享方案,1个秘密处理者将秘密分成n份共享,并将此n份共享秘密分配给n个参与者,并须满足:(1)任何≤t-1个参与者不能获得关于共享秘密的任何信息;(2)任何≥t个参与者能够在多项式时间内计算该秘密.该秘密共享方案按以下步骤实现:

1)秘密处理者在Z_q上随机选择一个次数为(t-1)的多项式$f(x)=f_0+f_1x+\cdots+f_{t-1}x^{t-1}\pmod q$,满足$f(0)=f_0=d$.$f_1,f_2,\cdots,f_{t-1}$为$Z_q$上的随机数,这些都需要保密,在生成n个秘密共享之后即可销毁.q要大于最大可能的秘密数d和参与者总数n,并且公开.

2)秘密处理者通过计算多项式f(x)对n个不同i值,得出每个人的秘密共享:$t_i=f(i)\pmod q$,其中$i=1,\cdots,n$.并将t_i秘密传送给P_i.

任何t个参与者$P_{i_1},\cdots,P_{i_t}$可通过Lagrange内插法重构多项式:

$$f(x)=\sum_{l=1}^{t}\Big(\prod_{k\neq l,k=1}^{t}\frac{x-i_k}{i_l-i_k}\Big)f(i_l)\pmod q$$

$$=\sum_{l=1}^{t}\Big(\prod_{k\neq l,k=1}^{t}\frac{x-i_k}{i_l-i_k}\Big)t_{i_l}\pmod q$$

因此,秘密d可由d=f(0)来恢复.即:

$$d=\sum_{j=1}^{t}a_jt_{i_j}$$

其中,$a_1,\cdots,a_t$由式子$a_j=\prod_{k\neq j,k=1}^{t}\frac{i_k}{i_k-i_j}$确定.

另外,任何小于t个参与者的群体不能恢复秘密d.因为对于任意的$d'\in Z_q$,在Z_q上存在次数为t-1的多项式f'(x),

*)本课题得到国家计算机网络与信息安全管理中心项目(2002-研3-022)资助.张险峰　博士生,主要研究方向:信息和网络安全.秦志光　教授,博导,主要研究方向:网络安全,电子商务.刘锦德　教授,博导,主要研究方向:开放系统及其安全、中间件技术.

满足：$f'(i_j)=t_j$和$f'(0)=d'$。

2.2 基于ECC的可验证秘密共享

Pedersen提出了一种非交互可验证秘密共享方法[4]。“可验证”意味着每个参与者能验证他自己的共享。假设秘密处理者产生一个Z_q上的秘密d，并以公钥$Q=dP$来提交，Q为椭圆曲线上一点。秘密处理者可执行以下协议将秘密d分配给n个参与者$P_1,\cdots,P_n$。

分配协议

1)根据Shamir秘密共享方案，在Z_q上选择次数为$(t-1)$的多项式$f(x)=f_0+f_1x+\cdots+f_{t-1}x^{t-1}$，这里$f(0)=d=f_0$。根据该多项式计算共享$t_i$，$t_i=f(i)$，其中$1\leqslant i\leqslant n$。

2)将t_i秘密传送给P_i，并把$f_iP(i=1,\cdots,t-1)$广播给n个参与者。即秘密处理者秘密传送了Z_q上n个元素，同时公开了椭圆曲线E上$(t-1)$个点。

所有参与者P_i接收到秘密共享t_i和$f_iP(i=1,\cdots,t-1)$后，可执行以下协议来验证t_i的有效性。

验证共享协议

1)验证$t_iP=\sum_{j=0}^{i-1}i^j(f_jP)$是否为椭圆曲线E上一点，如果不是，则广播$t_i$并拒绝处理者；如果是，则转2)。

2)对于其他每个t_l，验证$t_lP=\sum_{j=0}^{t-1}l^j(f_jP)$是否为椭圆曲线E上一点。

3)如果处理者没被拒绝，则接受秘密处理者产生的秘密共享$t_i(i=1,\cdots,n)$，否则参与者不接收所产生的共享。

如果参与者小于t个，即使它们遵从共享验证协议并得到正确的秘密共享，也不能获得秘密[4]。

2.3 不需可信中心的可验证秘密共享

Pedersen的可验证秘密共享方法需要一个可信中心来作为秘密处理者，这是一个安全瓶颈，因为该秘密处理者知道该秘密。Pedersen随后提出了不需可信中心的可验证秘密共享方法[5]。该方法包括2.2节中提到的分配协议、验证共享协议和下面描述的随机数协议，通过执行随机数协议，每一个参与者P_i都扮演了秘密处理者的角色。

随机数协议

1)每一个参与者P_i随机选择$d_i(d_i\in Z_q)$，并广播d_iP给其他的参与者。

2)每个P_i通过运用2.2节中的分配协议来分配d_i。即P_i在Z_q上选择一次数为$(t-1)$的随机多项式$f_i(x)=f_{i,0}+f_{i,1}x+\cdots+f_{i,t-1}x^{t-1}$，$f_i(0)=d_i$。然后把$f_i(j)$秘密地传送给$P_j(\forall j\neq i)$，并广播$f_{i,j}P(j=1,\cdots,t-1)$给所有的参与者。

3)每个P_i执行2.2节中的验证共享协议。若P_i没被拒绝，则转步骤4)；否则停止。

4)每个P_i计算$t_i=\sum_{j=1}^{n}f_j(i)$，并保密。

5)每个P_i计算$Q=\sum_{i=1}^{n}d_iP$，$Q_i=t_iP$，并广播Q和Q_i。

由上可见，通过运用随机数协议，秘密$\sum_{i=1}^{n}d_i$能够被分配给$P_1,\cdots,P_n$，但秘密$\sum_{i=1}^{n}d_i$本身不需要一个可信中心来产生和分配，增加了安全性。

3 基于ECC的ElGamal数字签名方案[11]

ElGamal签名体制由T. ElGamal在1985年给出，其修正形式已被美国NIST作为数字签名标准(Digital Signature Standard，DSS)，方案的安全性基于求离散对数的困难性，方案的具体描述可参考文[8]。基于ECC的ElGamal数字签名方案是对ElGamal签名体制的一种变形，其安全性基于椭圆曲线离散对数问题的难解性。设h()为单向hash函数，其结果为$\{1,\cdots,q-1\}$。消息为m，该方案具体过程描述如下：

基于ECC的ElGamal数字签名方案过程描述如下。

密钥产生 用户A执行以下步骤：

1)随机选取密钥$d,d\in Z_q$。

2)计算点$Q=d\times P$。

3)A的公钥是(E,P,q,Q)，A的私钥是d。

签名的产生 用户A按如下步骤对信息m进行签名：

1)随机选取整数$k,k\in[1,q-1]$。

2)计算$k\times P=(x,y)$，令$r=x(\mathrm{mod}\ q)$。若$r=0$，则转步骤1)。

3)计算$s=dr+kh(m)(\mathrm{mod}\ q)$，若$s=0$，则转步骤1)。

4)用户A对消息m的数字签名为整数对(r,s)。

签名的验证 用户B采用以下步骤来验证A的签名(r,s)：

1)获得A的公钥(E,P,q,Q)，验证r和s都是区间$[1,q-1]$上的整数。

2)计算$(x',y')=sh(m)^{-1}P-rh(m)^{-1}Q$。

3)若$x'=r(\mathrm{mod}\ q)$，则接受签名；反之拒绝。

方案中，由于$(x',y')=sh(m)^{-1}P-rh(m)^{-1}Q=sh(m)^{-1}P-rh(m)^{-1}dP=h(m)^{-1}P(s-rd)=h(m)^{-1}P(kh(m))=kP=(x,y)$

而$r=x(\mathrm{mod}\ q)$，因此如果签名和验签过程正确，应有$x'=r(\mathrm{mod}\ q)$。

4 基于ECC的ElGamal型(t,n)门限数字签名方案

设$G=\{P_1,\cdots,P_n\}$表示签名者群体，在前面所介绍和分析的理论基础上，我们提出了基于ECC的ElGamal型(t,n)门限数字签名方案。该方案由密钥产生协议和签名发布协议组成。密钥产生协议要求所有签名者协作产生G的公开密钥Q；在签名发布协议里，若签名者子集$B\subseteq G$，并且B中包含t或t个以上诚实的签名者，则能够发布一签名(r,s)。任何小于等于$(t-1)$个不诚实的签名者不能伪造一签名。

密钥产生协议

G中每个签名者均执行2.3节的随机数协议。设P_i的秘密输出为t_i，公钥输出为：$Q=dP=\sum_{i=1}^{n}d_iP$，$Q_i=t_iP$，其中$1\leqslant i\leqslant n$，Q是G的公钥。

签名发布协议

1)从G中选择t个签名者$P_{i_1},\cdots,P_{i_t}$，设$S=\{i_1,\cdots,i_t\}$，设签名者子集$B=\{P_j|j\in S\}$。

2)每个签名者$P_i(i\in S)$计算$e_{i,S}=a_{i,S}t_i$，其中$a_{i,S}=\prod_{h\neq i,h\in S}\frac{h}{h-i}$。

3)每个签名者$P_i(i\in S)$产生一随机数$k_i(1\leqslant k_i\leqslant q-1)$。

4)每个签名者$P_i(i\in S)$计算$R_i=k_iP$，并将之广播给B的每个成员。

5)每个签名者$P_i(i\in S)$计算$(x,y)=\sum_{j\in S}R_j$(可以看出，每

个 P_i 算出来的(x,y)值都相同)。

6)每个签名者 $P_i(i\in S)$计算 $r=x(\mathrm{mod}\ q)$,$s_i=e_{i,s}r+k_ih(m)(\mathrm{mod}\ q)$,并把 s_i 广播给 B 的每个成员。

7)对于 $j(\neq i)\in S$,每个签名者 $P_i(i\in S)$验证 $R_i=s_ih(m)^{-1}P-rh(m)^{-1}a_{i,s}Q_i$ 是否成立。如果不成立,则拒绝 P_i 并停止。

8)每个签名者 $P_i(i\in S)$计算 $s=\sum_{j\in S}S_j$,然后输出(r,s)作为签名者群体的数字签名。

在以上协议中,对发布的数字签名(r,s)可作如下分析:

(a)由签名发放协议第6)步可得:$r=x(\mathrm{mod}\ q)$;由签名发放协议的第4)、5)步可得$(x,y)=\sum_{j\in S}R_j=\sum_{j\in S}k_jP=kP$,这里 $k=\sum_{j\in S}k_i$。所以 x 是点 kP 的 x 坐标。

(b)由于:$s=\sum_{j\in S}S_j$ (由签名发放协议第8步)

$=\sum_{j\in S}(e_{j,s}r+k_jh(m))$ (由签名发放协议第6步)

$=(\sum_{j\in S}e_{j,s})r+kh(m)$

$=(\sum_{j\in S}(\prod_{h\neq j,h\in S}\frac{h}{h-j}t_j))r+kh(m)$ (由签名发放协议第2步)

$=dr+kh(m)$ (由2.1节 Lagrange 内插法)

所以,$s=dr+kh(m)(\mathrm{mod}\ q)$,其中 d 是群 $P_1,\cdots,P_n$ 共享的秘密,其中 $Q=dP$,$k=\sum_{j\in S}k_i$。

由以上两点可以看出,本方案产生的签名(r,s)同3节中生成的基于 ECC 的 ElGamal 数字签名完全相同,签名(r,s)的验证也同3节的相同。

5 效率和安全性分析

本文提出的方案是一种基于 ECC 的(t,n)门限签名方案,因此具有引言中提到的门限方案和 ECC 的诸多优点。此外,还可从以下两方面对本方案的性能进行分析。

5.1 效率

在密钥产生协议中,$P_1,\cdots,P_n$ 均执行2.3节中的随机数协议,每个参与者 P_i 需要广播(t+2)个椭圆曲线上的点和(n-1)个有限域 Z_q 中的元素。在签名发布协议中,每个签名者首先广播1个椭圆曲线上的点,然后广播1个有限域 Z_q 中的元素,最后广播2个 Z_q 中的元素(即(r,s)签名)。当发送签名时,不需要在网络传输中进行秘密通信。

为分析的方便,假设椭圆曲线上点以比特串表示时长度均为2|P|(这里参数2意味着椭圆曲线 E 上点的 x 和 y 坐标),设每个有限域 Z_q 中的元素以比特串表示时长度均为|q|。则本方案各个阶段所需的通信量通过与 Park-Kurosawa 方案[7](其安全性同样基于椭圆曲线离散对数问题)在各阶段所需的通信量对比,可以看出,我们的方案在通信时所需的带宽更少,性能更优。对比结果见下表:

表1 通信复杂性比较

	密钥产生		签名发布	
	广播(bits)	秘密发送(bits)	广播(bits)	秘密发送(bits)
Park-Kurosawa 方案	2(t+2)|p|	(n-1)|q|	2t|P|+2|q|	(t-1)|q|
本文方案	2(t+2)|p|	(n-1)|q|	2|P|+2|q|	0

5.2 安全性

在本方案中,如果欺骗者在执行密钥产生协议时进行欺骗,则他将会在随机数协议中的第3)步被检测出来;如果欺骗者在签名发布协议的第6)步进行欺骗,则他将在第7)步被检测出来。

同时,本方案只在秘密产生阶段要求秘密通信。而在 Park-Kurosawa 方案中,每一次签名者群体发布签名时都要通过安全通信路径进行传送。这样,当高密级信息不允许在网络环境中传送时,本方案就体现出了更大的安全性和适应性。

6 应用

基于本文提出的(t,n)门限数字签名方案,下面描述了一个具体应用。在该应用中,签名者群体首先生成给定消息的数字签名,同时加密该消息,然后将签名及密文传送给验签者群体;验签者群体接收到数字签名和密文后,验证数字签名并解密密文。该应用具体实施步骤如下:

1)签名者群体 $P_1,\cdots,P_n$ 和验签者群体 $P'_1,\cdots,P'_n$ 分别执行2.3节的随机数协议。设签名者 P_i 的秘密输出是 t_i,公开输出是 $Q(=dP)$,$Q_i(=t_iP)(1\leqslant i\leqslant n)$,Q 是 $P_1,\cdots,P_n$ 的公钥;设验签者 P'_i 的秘密输出是 t'_i,公开输出是 $Q'(=d'P)$,$Q'_i(=t'_iP)(1\leqslant i\leqslant n)$,$Q'$ 是 $P'_1,\cdots,P'_n$ 的公钥。

2)签名者群体 $P_1,\cdots,P_n$ 选择 t 个签名者 $P_{i_1},\cdots,P_{i_t}$,设 $S=\{i_1,\cdots,i_t\}$,签名者子集 $B=\{P_j|j\in S\}$。每一个签名者 $P_i(i\in S)$产生一个随机数 $k_i(1\leqslant k_i\leqslant q-1)$,并执行以下操作:

(a)计算 $e_{i,s}'=a_{i,s}t_i$,其中 $a_{i,s}=\prod_{h\neq i,h\in S}\frac{h}{h-i}$。

(b)计算 $R_i=k_iP$ 和 $T_i=k_iQ'$,并将其广播。

(c)计算$(x,y)=\sum_{j\in S}R_j$。

(d)计算 $r=x(\mathrm{mod}\ q)$和 $s_i=e_{i,s}r+k_ih(m)(\mathrm{mod}\ q)$,并将其广播。

(e)对于所有的 $j(\neq i)\in S$,验证 $R_j=s_jh(m)^{-1}P-rh(m)^{-1}Q_j$ 是否成立,如果不成立,则拒绝 P_j 并停止。

(f)计算:$s=\sum_{j\in S}S_j$ 和$(x',y')=\sum_{j\in S}T_j$,然后把 x'作为密钥加密消息 m,并广播加密后的消息 m'和数字签名(r,s)。

3)验签者群体 $P'_1,\cdots,P'_n$ 选择 t 个验签者 $P'_{i_1},\cdots,P'_{i_t}$,设 $S'=\{i_1,\cdots,i_t\}$,验签者子集 $B'=\{P'_j|j\in S'\}$。每一个签名者 $P'_i(i\in S')$执行以下操作:

(a)计算:$e_{i,s'}'=a_{i,s'}S'_i$,这里 $a_{i,s'}=\prod_{h\neq i,h\in S'}\frac{h}{h-i}$。

(b)计算:$(x',y')=sh(m)^{-1}P-r\,h(m)^{-1}Q$。

(c)计算并广播:$R_i=e'_{i,s'}(x',y')$。

(d)计算并广播:$(x_d,y_d)=\sum_{i\in S'}R_i$。

(e)验证 $x'=r(\mathrm{mod}\ q)$是否成立。如果成立,则接受签名,并把 x_d 作为密钥解密 m'得到 m;否则不接受签名,停止。

结论 本文描述了一个基于 ECC 的 ElGamal 型(t,n)门限数字签名方案,具有很好的安全性和执行效率。在共享秘密的产生上,该方案不需要一个可信中心;在数字签名的发布上,该方案具有较低的通信复杂度,且不需安全的通信路径。通过比较,它比 Park-Kurosawa 方案更有效。目前,我们正在从事基于 ECC 的门限密码技术研究,由于 ECC 不是一种同态密码体制,研究开发基于 ECC 的门限密码技术比较困难,所以在这方面,我们还有很多工作要做。

PKI技术在IPSec系列协议中的应用*)

谭兴烈[1] 王天忠[2] 唐国栋[3] 周明天[4] 沈昌祥[5]

(四川大学数学学院 成都卫士通信息产业股份有限公司 成都610041)[1]

(成都卫士通信息产业股份有限公司 成都610041)[2] (信息产业部电子第三十研究所 成都610041)[3]

(电子科大卫士通信息安全实验室 成都610054)[4] (海军计算技术研究所 北京100841)[5]

Using PKI in IPSec Protocol Suite

TAN Xing-Lie[1] WANG Tian-Zhong[2] TANG Guo-Dong[3] ZHOU Ming-Tina[4] SHEN Chang-Xiang[5]

(Mathematics College of Sichuan University, Chengdu Westone Info Co,Ltd, Chengdu 610041)[1]

(Westone Information Industry INC,Chengdu 610041)[2] (No30 Electronic Institute,Ministry of Information Industry,Chengdu 610041)[3]

(Westone Information Secutity Lab,UESTC,Chengdu 610054)[4] (Navy Institute of Computing Technology,Beijing 100841)[5]

Abstract PKI and IPSec are the widely used technologies in today's information security area. In this paper,PKI and IPSec are discussed briefly at first. Then two methods of combining PKI with IPSec are proposed with details,and how to use PKI in IPSec configuration management is also discussed. Finally,it points out that identity of IPSec communication entity may be the special user but not limited to IP address with PKI. It also points out that PKI makes athentication of IPSec entity more secure and reliable,and makes IPSec configurations more flexible.

Keywords Public key infrastructure, IPSec protocol, Security association ,Internet key exchange protocol

1 引言

PKI(Public Key Infrastructure)即"公共密钥基础设施",是一个用公钥的概念和技术实施和提供安全服务的具有普遍适应性的安全基础设施,也是一个利用现代密码学中的公钥密码技术在开放的Internet网络环境中提供数据加密以及数字签名服务的统一的技术框架。IPSec是网络层安全的事实上的标准,尽管IPSec协议在处理多播协议以及在B2B环境中使用保留地址组建VPN等方面还存在这样那样的问题,但它目前还是得到了广泛的应用,是IP层安全公认的标准,同时它也是目前广泛利用的VPN技术。

本文首先简要介绍了PKI技术、IPSec技术,之后具体讨论了PKI技术与IPSec系列协议结合的方式,并分析了结合后带来的好处。

2 PKI技术及IPSec技术简介

2.1 PKI技术

2.1.1 *公开密码算法和证书体系* 区别于对称密码算法使用同一个密钥来加密/解密,公开密钥使用一个密钥对(公钥私钥对)来进行加密/解密,其中一个密钥加密的数据,只有使用另一个密钥来进行解密。用公钥加密,只能用对应私钥解密,这样就可以用来实现数据加密传送,也可以用来实现密钥的交换;用私钥来加密整个文档或文档的一个摘要,任何人都可以用公钥来解密检验其完整性。

公钥/私钥对的产生可以在可信的机构如CA中产生,此时私钥的分发通过安全的方式进行,公钥以证书的方式存放。公钥/私钥对也可以在CPU卡或USB令牌中产生,私钥产生后从不导出到CPU卡或USB令牌外,私钥运算只在设备内进行。

*)本文受国家863宽带VPN项目863-104-03-01课题资助。谭兴烈 博士,高工,主要研究方向为宽带VPN安全、应用系统安全及信息安全系统设计。

参考文献

1 徐秋亮.改进门限RSA数字签名体制.计算机学报,2000,23(5)

2 Desmedt Y, Frankel Y. Threshold Cryptosystem. In: Proc. of Crypto'89, Lecture Notes in Computer Science, LNCS 435, Springer Verlag,1990. 307～315

3 Hwang T. Cryptosystem for group oriented cryptography. In: Proc. of Eurocrypt'90, Lecture Notes in Computer Science, LNCS 473, Springer Verlag,1991. 352～360

4 Pedersen T P. Distributed Provers with Applications to Undeniable Signatures. In:Proc. of Eurocrypt'91, Lecture Note in Computer Science, LNCS 547, Springer Verlag,1991. 221～238

5 Pedersen T P. A Threshold Cryptosystem without a Trusted Party. In:Proc. of Eurocrypt'91,Lecture Notes in Computer Science, LNCS 547, Springer Verlag,1991. 522～526

6 Feldman. A Practical Scheme for Non-Interactive Verifiable Secret Sharing. In: Proc. of 28th IEEE symposium on Foundations of Computer Science,1987. 427～437

7 Park C,Kurosawa K. New ElGamal Type Threshold Digital Signature Scheme. IEICE Trans. Fundamentals, 1996,E79-A(1):86～93

8 王育民,刘建伟.通信网的安全-理论与技术.西安电子科技大学,1999

9 Shamir A. How to Share a Secret. Communications of the ACM, 1979,22(11):612～613

10 刘木兰,周展飞,陈小明.密钥共享体制.科学通报,2000.45(9)

11 http://grouper.ieee.org/groups/1363/StudyGroup/contributions/th-sche.pdf