

一个基于门限 ECC 的解密方案及其应用^{*})

张险峰 张 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)

摘 要 门限密码学提供了建立入侵容忍应用的新方法。在本文中,提出了一个基于 ECC 的门限解密方案,设计了一个基于 ECC 的零知识证明方法,研究了这些技术在入侵容忍 Web 安全中的应用。通过分析,本文提出的基于 ECC 的门限解密方法能比 Stanford 大学的 ITTC 项目所基于的门限 RSA 解密方案具有更高的安全性和执行效率。

关键词 入侵容忍,椭圆曲线密码体制(ECC),门限解密,Web 安全

A Threshold ECC Based Decryption Scheme and its Application

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

(IBM Technology Center, School of Computer Science and Engineering, UEST of China, Chengdu 610054)

Abstract The threshold cryptography provides a new approach to building intrusion tolerance applications. In this paper, a threshold decryption scheme based on elliptic curve cryptography is presented. A zero-knowledge test approach based on elliptic curve cryptography is designed. The application of these techniques in Web security is studied. Performance analysis shows that our scheme is characterized by excellent security as well as high efficiency.

Keywords Intrusion tolerance, Elliptic curve cryptography, Threshold decryption, Web security

1 引言

由于不可能预知所有未知形式的攻击,也不可能完全阻止新安全漏洞的引入,一些攻击仍不可避免地取得成功,因此,必须研究开发即使遭到攻击仍能运转的系统(入侵容忍系统)。门限密码学提供了新的建立安全有效的入侵容忍系统的方法,基于门限密码学的入侵容忍研究主要集中在门限加密、门限解密和门限签名方案的设计与实现上,目前这些方案的实现,特别是门限加密和门限解密的实现一般要求所使用的密码算法具有同态的属性,其原因在于:同态的密码算法可以很方便地将基于秘密共享的多个密文分片组合成整个消息的密文,而非同态密码算法则很难实现^[1],因此,在已有的研究成果中,几乎所有门限密码学的研究集中在基于同态密码算法(尤其是 RSA)的门限密码技术上。这其中,比较著名的研究项目是斯坦福大学的 ITTC (Intrusion Tolerance via Threshold Cryptography, 通过门限密码学实现入侵容忍)项目,该项目基于 RSA 来研究门限解密和门限签名方案,进而实现能够容忍入侵的应用^[2]。

目前, ECC (Elliptic Curve Cryptography, 椭圆曲线密码体制)被认为比 RSA 等其他公钥密码系统能够提供更好的加密强度、更快的执行速度和更小的密钥长度^[3,4],因而基于 ECC 的门限密码方案的设计是一个值得研究的问题,但由于 ECC 是一种非同态的密码算法,故设计基于 ECC 的门限密码方案具有理论上的创新性。在本文中,我们对基于 ECC 的门限解密方案和零知识证明方法进行了研究,并将研究结果应用于入侵容忍,在此基础上,研究了这些技术在入侵容忍 Web 安全中的应用。

本文首先对一些理论基础作了介绍和分析,然后分别提

出了基于 ECC 的门限解密方案和零知识证明方法,在第5节中研究了我们的方案和方法在 Web 安全中的应用,在第6节,我们对基于 ECC 的门限解密方案的性能进行了分析,最后是我们的结论。

2 理论准备

在本文中,设椭圆曲线 $E(F_p)$ (P 为大于 3 的素数) 包含一个循环子群 H , 其阶为 $|H|$, 在 H 中离散对数问题是难解的, g 为 H 的生成元。

2.1 Menezes-Vanstone 椭圆曲线密码系统^[5]

选择整数 d 且 $d \in [1, |H| - 1]$, 计算 $h = dg$, 将 g, h 公开, d 保密。设明文 $X = (x_1, x_2) \in Z_p^* \times Z_p^*$, 即 x_1, x_2 均属于 Z_p^* 。

加密操作:

1. 选择一随机数 $k, [0, |H| - 1], k$ 保密。

2. 计算

$$y = kg \quad (1)$$

3. 计算

$$(c_1, c_2) = kh \quad (2)$$

4. 计算 $s_1 = c_1 x_1 \bmod P$ 和 $s_2 = c_2 x_2 \bmod p$ 则由 X 加密后生成的密文是 (y, s_1, s_2)

解密操作:

1. 计算 $dy = dkg = k(dg) = kh = (c_1, c_2)$, 即:

$$dy = (c_1, c_2) \quad (3)$$

2. 计算

$$x_1 = s_1 c_1^{-1} \bmod p \quad (4)$$

$$x_2 = s_2 c_2^{-1} \bmod p \quad (5)$$

在本密码系统中,为了解密密文 (y, s_1, s_2) , 需要计算方程

^{*}) 国家836计划资助项目,项目编号:2002AA142040。张险峰 博士生,主要研究方向:信息和网络安全。张 峰 博士生,主要研究方向: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。

(3),(4)和(5),如果没有秘密值 d ,则要解出密文非常困难,因为这是一个 ECDLP(Elliptic Curve Discrete Logarithm Problem,椭圆曲线离散对数问题)难题。值得注意的是,用本系统对一明文加密时,系统首先应将明文编码成整数对 (x_1, x_2) 的形式。如果待加密的明文 F 需要编码成 f 个整数对 $(x_{11}, x_{12}), (x_{21}, x_{22}), \dots, (x_{f1}, x_{f2})$,在加密操作时,步骤2及3只需执行一次,生成 (c_1, c_2) 后,执行 f 次步骤4即可。由 F 生成的密文形式为: $(y, s_{11}, s_{12}), (y, s_{f1}, s_{f2}), \dots, (y, s_{f1}, s_{f2})$ 。对 F 解密时,解密操作的步骤1只需执行一次,计算出 (c_1, c_2) 后,执行 f 次步骤2即可。

2.2 (t, n) 秘密共享

将一秘密值 d 分割成 n 份影子,然后将此 n 份影子分别存储在 n 个不同的影子服务器上,只有通过所有的 n 份影子才能恢复秘密值 d ,此种秘密共享方法称为 (n, n) 秘密共享。把 d 分割成 n 份的方法很简单,根据 Frankel 的方法^[6],可选择 n 个属于 $[-P, P]$ (P 为域 F_p 的阶)的随机数 $d_1, d_2, \dots, d_n$,使得: $d = d_1 + d_2 + \dots + d_n$ 。

在 (n, n) 秘密共享中,即使攻击者成功入侵了 $n-1$ 个共享服务器,他也得不到秘密值 d ,但如果某台共享服务器崩溃或者它所存的影子丢失,则该秘密值将会丢失。为了保证可用性,文[2]提出的 (t, n) 门限共享方案值得借鉴。在该方案中,秘密值 d 按多种 (t, t) 共享方法来分割,每种分割称为一种联合(coalition),每种联合含有 t 份影子,这 t 份影子分别存储在 n 个服务器中的 t 个不同的服务器上。例如,当 $t=3, n=4$ 时,秘密值 d 的 (t, n) 秘密共享方法如图1所示。

服务器1	服务器2	服务器3	服务器4	
d_1	d_2	d_3	d_3	联合1: $d = d_1 + d_2 + d_3$
d_4	d_4	d_5	d_6	联合2: $d = d_4 + d_5 + d_6$

图1 d 的 $(3, 4)$ 秘密共享

图1中,每个 d_i 都是属于 $[-P, P]$ 的随机整数,且满足给定的方程。表的第 j 列表示共享服务器 j 可存储的多个不同的影子。在该例中,任何一台共享服务器出现故障或影子丢失都不会影响系统的工作,任何两台共享服务器被入侵后不会泄露 d 的任何信息,任何两台以上的共享服务器都能够应用所对应的秘密值 d 。因此,基于 (t, n) 共享,系统将具有容错和容忍入侵的能力,即能提供机密性,又能提供可用性。一般说来,当 n 固定时, t 越小,系统的容错能力越强,但系统越不安全; t 越大,系统容忍入侵的能力强,但容错能力差,因此,对 t 的选择要从可用性和安全性的角度折衷考虑。

本 (t, n) 秘密共享方案同 Shamir (n, t) 秘密共享方案相比,运算的开销大为减少,因为本方案只是执行若干模加和模减运算,而 Shamir (n, t) 秘密共享方案需要执行多项式乘法和插值法^[7]。

3 基于 ECC 的 (t, n) 门限解密方案

设 A 为发送者, B 为接收者, B 不保存私钥 d , d 以 (t, n) 共享的方式存储在 n 个影子服务器上。设 d 的一种联合(分割方法)为

$$d = d_1 + d_2 + \dots + d_t \quad (6)$$

该种联合所涉及的影子服务器为 $C_1, C_2, \dots, C_t$, B 保存有各影子 $d_i (1 \leq i \leq t)$ 所对的 d_{ig} (称为影子公钥)。

A 按照2.1节中加密操作对一明文 M_A 加密成密文 $(y, s_1,$

$s_2)$,并将密文传送给 B 。 B 按以下过程对密文进行解密。

门限解密操作:

1. 接收者 B 将密文三元式的第一项 $y (= kg)$ 广播给 $C_1, C_2, \dots, C_t$ 。

2. 各共享服务器 $C_i (i \in [1, t])$ 计算:

$$Q_i = d_i y \bmod P \quad (7)$$

并将 Q_i 发回给 B 。

3. B 得到所有的 $Q_i (i \in [1, t])$ 后,计算

$$Q = \sum_{j=1}^t Q_j = (q_1, q_2) \bmod p \quad (8)$$

4. B 计算:

$$b_1 = s_1 q_1^{-1} \bmod P \quad (9)$$

$$b_2 = s_2 q_2^{-1} \bmod P \quad (10)$$

解密的结果 (b, b) 即为密文所对应的明文。

证明:

$$Q = (q_1, q_2) \bmod P \quad (\text{由(8)式})$$

$$= \sum_{j=1}^t Q_j \bmod P$$

$$= \sum_{j=1}^t d_j y \bmod P \quad (\text{由(7)式})$$

$$= \sum_{j=1}^t d_j kg \bmod P \quad (\text{由(1)式})$$

$$= d kg \quad (\text{由(6)式})$$

$$= (c, c) \quad (\text{由(3)式})$$

因此有: $(b_1, b_2) = (x_1, x_2) \bmod p$ (由式(4)、(5)、(9)、(10))

4 基于 ECC 的零知识证明方法

在第3节中,假设某个共享服务器 $C_j (1 \leq j \leq t)$ 需要向实体 B 证明其拥有影子 d_i ,但又不能泄露 d_i 的任何信息,则可以通过基于 ECC 的零知识验证方法来实现,该方法设计如下:

1. B 选择两个属于 $[0, |H|-1]$ 的随机整数 a 和 b 。

2. B 分别计算 $(a_1, a_2) = a(d, g) \bmod P$ 和 $(b_1, b_2) = bg \bmod P$ 。

3. B 计算 $t_1 = a_1 b_2 \bmod P$ 和 $t_2 = a_2 b_2 \bmod P$,并将 (ag, t_1, t_2) 传给待验证的 C_j 。

4. C_j 收到消息 (ag, t_1, t_2) 后,首先计算 $d_i(ag) = (r_1, r_2) \bmod P$,然后计算: $z_1 = t_1 r_1^{-1} \bmod p$ 和 $z_2 = t_2 r_2^{-1} \bmod p$,并将计算结果 (z_1, z_2) 传回给 B 。

5. B 检查等式 $(b_1, b_2) = (z_1, z_2)$ 是否成立。如果成立,则该共享服务器拥有 d_i ,否则不能确定(因为正确的计算结果可能被更改)。

该方法的正确性可根据2.1节的 Menezes-Vanstone 椭圆曲线密码系统的原理很容易得到验证。

5 应用

5.1 Web 安全系统结构

为了提供 Web 服务的安全,Web 客户常通过 SSL(Security Socket Layer,安全套接层协议)和 Web 服务器进行安全连接,在 Web 客户和服务器进行 SSL 会话密钥协商的过程中,Web 客户需向 Web 服务器发送 Certificate Verity 消息来使服务器对客户端进行认证。该消息中含有经客户端私钥签名的预主密钥(premaster key),预主密钥是使用 Web 服务器

的公钥发送的,故 Web 服务器需使用相应的私钥进行解密。若一个攻击者能成功入侵到该 Web 服务器并取得其私钥,他就能伪装成该服务器或窃听从 Web 客户到该服务器之间的会话。因此,保证 Web 私钥至关重要。

下面,我们在文[2]的基础上提出了一个 Web 安全系统体系结构,该 Web 安全系统由图2中虚框里的组件组成,包括:Web 服务器、管理服务器、IDS(Intrusion Detection System,入侵检测系统)和 n 个共享服务器。

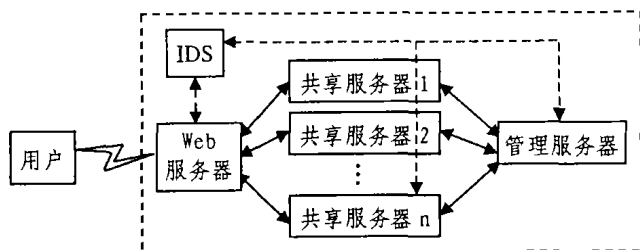


图2 Web 安全系统体系结构

在该系统中,Web 服务器通过通信链路(如 Internet)接收用户的访问请求。Web 服务器不保存自己的私钥 d_i ,该私钥通过 (t,n) 秘密共享存储在 n 个共享服务器上。Web 服务器上存储了每个影子 d_i 对应的影子公钥 $d_i g$ 和其他一些信息,包括公钥 $d g$ 、 g 、 P 和 $E(F_p)$ 等。IDS 检测、监控网络流及共享服务器、Web 服务器、管理服务器的状态。IDS 可执行在专用的硬件平台上,也可以作为一个软件模块运行在被监控的机器上。本文中,我们不详细探讨 IDS 的实现细节。管理服务器对存储在共享服务器上的影子的产生、更新进行管理,在某些情况下,它也可关闭或暂停共享服务器的执行。对秘密钥影子的更新并没有改变所对应的秘密钥本身。基于 (t,n) 秘密共享的情况下,即使一攻击者获得了存储在不同的共享服务器的 t 个以下的影子,一旦管理服务器对该私钥的影子进行了更新,则该攻击者所取得的影子变得毫无价值。当存储在共享服务器上的影子丢失或损坏的情况下,管理服务器也可对影子进行更新。因此,通过周期性的密钥更新,系统可以获得主动安全(proactive security)。

5.2 解密实现

当用户发送包含预主密钥的加密信息 (y, s_1, s_2) 给 Web 服务器后,Web 服务器将从 n 个服务器中指定使用的 t 个共享服务器, t 个共享服务器的选择可根据 n 个服务器的工作负荷情况来确定,以使各服务器工作负荷平衡。选定的 t 个共享服务器对应一种联合,基于该联合,每个共享服务器可确定在此联合中使用哪个影子 d_i ,然后系统可按照第3节提出的门限解密方案进行解密,只不过方案中的接收者 B 替换成了 Web 服务器。

5.3 影子拥有性检测

若攻击者成功入侵某台共享服务器,他可能会篡改该服务器所存储的影子 d_i ,共享服务器也可能会因为一些意外原因丢失 d_i ,在这些情况下,这些共享服务器将返回不正确的服务响应给 Web 服务器,为此,有必要对设计检测某台服务器是否拥有影子 d_i 的机制。由于 Web 服务器上存有和 d_i 相对应的 $d_i g$,因此,我们可基于第4节中设计的零知识证明方法来实现检验。通过该方法,既能够验证某台服务器影子的拥有情况,又不泄露该影子的任何信息。

6 性能分析

本文着重研究了基于门限 ECC 来建立 Web 安全的方案

和方法,而斯坦福大学的 ITTC 项目中研究了基于门限 RSA 建立入侵容忍的 Web 应用问题,两者有很大的相关性。因此,我们将对比 ITTC 项目中的相关方案(以下简称 ITTC 方案),从安全性、效率和可用性方面来对本文提出的 Web 安全方案进行分析。

ITTC 方案中,Web 服务器的私钥 k 以 (t,n) 共享方式处理,当 Web 服务器接收到待解密的消息 M 后,系统执行如下操作:(1)Web 服务器将 M 传给选定的 t 个共享服务器。(2)各共享服务器自行决定使用的影子 $k_i (1 \leq i \leq t)$,计算 $M^{k_i} \bmod N$ (N 为选定的 RSA 的公钥参数),并将结果传回给 Web 服务器。(3)Web 服务器将收到的 t 个计算结果 $M^{k_i} \bmod N$ 相乘,所得的结果即为 M 所对应的明文。

6.1 安全性

通过将 Web 服务器的私钥 d 以 (t,n) 共享方式分存在 t 个不同的共享服务器中,一个攻击者即使功入侵了 $t-1$ 个服务器也不能获得该私钥值。另外,在处理过程中,私钥 d 从没有单独节点上进行重建。因此,攻击者不能通过入侵系统的某个组件来获取私钥 d 。从这些方面,本方案与 ITTC 方案是等价的。

在本文提出的门限解密方案中,选定的 t 个服务器将计算结果 $(d_i y \bmod P)$ 传给 Web 服务器,攻击者即使得到 $(d_i y \bmod P)$,他也不能计算出影子 d_i 来,因为这一个 ECDLP 问题。在 ITTC 方案里,选定的 t 个服务器需将计算结果 $(M^{k_i} \bmod N)$ 传给 Web 服务器,攻击者要从计算结果 $M^{k_i} \bmod N$ 中解出 k_i 来,则他要解一个大整数因子分解的难题。从计算难度来讲,ECDLP 比大整数因子分解更难^[8],从这点上讲,本方案安全强度更高。

6.2 效率

在本文方案中,选定的 t 个共享服务器之间都不用通信,只有 Web 服务器和这 t 个共享服务器间有交互,这点与 ITTC 方案是相同的。下面,我们将从通信复杂性和计算复杂性的角度把本文的方案同 ITTC 方案进行比较,为了比较得合理,我们取本文方案中的 g (g 为 F_p 的生成元)的阶为 160 比特长,取 ITTC 方案中 RSA 的模长 N 为 1024 比特,因为密钥长为 160 比特 ECC 和 1024 比特的 RSA 提供了相同的安全级。同时根据文[8],有以下几个结论:(1)ECC 的 1 次标乘 $(d_i y)$ 要求 1200 次域乘法。(2)一次椭圆曲线点加或倍加操作要求 1 次域元求逆操作和 2 次域乘操作。(3)执行一次域元求逆操作相当于 3 次域乘操作。(4)1 次模 N 的模乘操作在时间上相当于 F_p 中执行 41 次域乘操作。(5)幂运算 $M^{k_i} \bmod N$ 平均要求 240 次 1024 比特的模乘操作。

在 ITTC 方案中,当系统要解密的密文 M 为 1024 比特时, M 相应的明文长度可达到 1024 比特,因此,我们假设 Web 客户加密的明文长度亦为 1024 比特,根据 2.1 节,该明文应编码成 4 个整数对(其长度实际上为 $16^2 \times 2 \times 4 = 2048$ 比特),Web 客户将明文加密传输给 Web 服务器后,后者将收到 4 个长度均为 640 比特的密文 $(y, s_{j1}, s_{j2}) (1 \leq j \leq 4)$ 。

为了解密,ITTC 方案需要广播 M 给选定的 t 个共享服务器, t 个服务器将各自返回长为 1024 比特的计算结果 $M^{k_i} \bmod N$,因此整个通信量是 $1024(t+1)$ 比特。而在本文案中,系统将长为 320 比特的 y 广播给选定的 t 个共享服务器,然后这 t 个服务器将分别传回长度为 320 比特的计算结果 $d_i y$ 给 Web 服务器,因此,整个通信量为 $320(t+1)$ 比特。显然,从通

信复杂性来讲,本文方案所需消耗的通信量是 ITTC 方案的

$$\frac{320(t+1)}{1024(t+1)} \approx 31.2\%.$$

另外,在 ITTC 方案中,系统对 M 解密的过程中,需要执行 t 次幂运算 $M^{t^i} \bmod N$ 和 $(t-1)$ 次模数为 N 的模乘操作,因此,所需的计算总量为:

$$\begin{aligned} 240 \times t + (t-1) &= 241t - 1 \text{ 次} && (\text{模数为 } N \text{ 的模乘操作}) \\ &= (241t - 1)41 && (F_p \text{ 中域乘操作}) \\ &= 9881t - 41 \text{ 次} \end{aligned}$$

而在本文方案中,通过 3.1 和 4.1 节可见,要解密 4 个长度分别为 640 比特的密文,系统需要在 F_p 中完成 t 次标乘 (d, y) , $(t-1)$ 次点加, 2 次域元求逆和 8 次域乘操作,因此,需要完成的计算总量为:

$$\begin{aligned} 1200 \times t + (t-1) \times (3+2) + 2 \times 3 + 8 \\ = 1205t + 9 \text{ 次} && (F_p \text{ 中域乘操作}) \end{aligned}$$

由于所选的门限 $t \geq 1$,显然有 $9881t - 41 > 1205t + 9$,因此,从计算复杂性来讲,ITTC 方案解密所花的时间约为本文方案的 $\frac{9881t-41}{1025t+9} \approx 9.64$ 倍。

因此,我们的方案从效率上比 ITTC 方案更优。

6.3 可用性

对于一个与 Web 服务器进行通信的用户而言,Web 服务器的私钥以共享的形式存储这一事实对他透明的。而且,基于 (t, n) 共享,即使 $(n-t)$ 个共享服务器所存的影子丢失或者服务器因故崩溃,我们的系统也能够提供正常的服务。

所以,本文方案提供了很高的可用性,在可用性方面,本文方案同 ITTC 方案等价。

7 相关工作

Malkin, Wu 和 Boneh 通过门限 RSA 方案建立了入侵容忍的 Web 和 CA 应用^[2]。Fray, Deswarte 和 Powell 在文^[9], 以及 Deswarte, Blain 和 Fabre 在文^[10]中描述了一个加密文件系统,在该系统中,密钥采用 Shamir 秘密共享方法分别存储在不同的密钥服务器中。当访问一文件时,该文件所对应的密钥需要重建。荆继武、冯登国基于 RSA 设计了一个入侵容忍 CA 方案^[11]。文^[12, 13]分别研究了基于 ECC 的 Nyberg-Ruepple 门限数字签名方案和 ElGamal 门限数字签名方案。然而,基于 ECC 的门限解密方案、基于 ECC 的入侵容忍应用

未见公开的研究发表。

结束语 在本文中,我们提出了一个基于 ECC 的门限解密方案,设计了一个基于 ECC 的零知识证明方法,基于提出的方案和方法,对具有入侵容忍功能的 Web 安全系统进行了研究,并且对我们的方案进行了详细的分析。本文中,我们没有对一些实现细节进行详细描述,下一步我们将完善这些工作。

参考文献

- 1 Benaloh J C. Secret sharing homomorphisms: keeping shares of a secret secret. In: Proc. Crypto'86. LNCS Vol. 263, Springer
- 2 Malkin M, Wu T, Boneh D. Building Intrusion Tolerance Applications. In: 8th USENIX Security Symposium
- 3 Xu Qiuliang, Li Daxing. Elliptic curve cryptosystems[J]. Journal of Computer Research and Development, 1999, 36(11): 1281 ~ 1288
- 4 张险峰, 秦志光, 刘锦德. 椭圆曲线加密体制的性能分析. 电子科技大学学报, 2001, 30(2): 144 ~ 147
- 5 朱文余, 孙琦. 计算机密码应用基础. 科学出版社, 2000. 174 ~ 175
- 6 Frankel Y. A practical protocol for large group oriented network. Eurocrypt 89, pp. 56 ~ 61
- 7 Shamir A. How to Share a Secret. In Communications of the ACM, 1979, 22(11): 612 ~ 613
- 8 Kobitz N, Menezes A, Vanstone S. The State of Elliptic Curve Cryptography. Designs, Codes and Cryptography, 2000, 19: 173 ~ 193
- 9 Fray J, Deswarte Y, Powell D. Intrusion tolerance using fine-grain fragmentation scattering. In: Proc. IEEE Symposium on Security and Privacy, Oakland, 1986. 194 ~ 201
- 10 Deswarte Y, Blain L, Fabre J. Intrusion tolerance in distributed computing systems. In: Proc. IEEE Symposium on Security and Privacy, Oakland, 1991, 110 ~ 121
- 11 荆继武, 冯登国. 一种入侵容忍的 CA 方案. 软件学报, 13(8)
- 12 Takaragi K, Miyazaki K, Takahashi M, et al. A threshold digital signature issuing scheme without secret communication. <http://grouper.ieee.org/groups/1363/StudyGroup/contributions/th-sche.pdf>
- 13 张险峰, 秦志光, 刘锦德. 一个基于椭圆曲线的 ElGamal 型 (t, n) 门限数字签名方案. 计算机科学, 2003, 30(5): 157 ~ 160

(上接第 31 页)

- 5 马小骏, 顾冠群. 基于测量的接纳控制研究. 计算机学报, 2001, 24(1)
- 6 Lee S, Song J. A Measurement-based Admission Control Algorithm using Variable-sized Window in ATM Networks. In: Intl. Conf. on Information, Communications and Signal Processing, IEEE 1997
- 7 Floyd S. Comments on Measurement-based Admissions Control for Controlled-Load Services. 1996, URL <ftp://ftp.ee.lbl.gov/papers/admit.ps.Z>
- 8 Gibbens R, Keely F. Measurement-Based Connection Admission Control. In: 15th Intl. Teletraffic Congress, Jun. 1997
- 9 Zukerman M, Tse P W. An adaptive connection admission control

scheme for ATM networks. In: Proc. ICC'97, IEEE Intl. Conf. on, Volume: 3, 1997

- 10 Rhee W, Lee J, et al. Admission control mechanism using measurement based dynamic provisioning in differentiated service networks. In: the 8th Intl. Conf. on Communication Systems, Volume: 1, 2002. 128 ~ 132
- 11 Guerin R, Ahmadi H, Naghshineh M. Equivalent Capacity and Its Application to Bandwidth Allocation in High-Speed Networks. IEEE Journal of Selected Areas in Communication, 1991, 9(7): 968 ~ 981
- 12 Beran J, Sherman R, Taqqu M S, Willinger W. Long-range dependence in variable-bit-rate video traffic. IEEE Transactions on Communications, 1995, 43(2)