

文章编号:1001-9081(2011)07-1859-03

doi:10.3724/SP.J.1087.2011.01859

对两个基于离散对数的数字签名方案的攻击分析与改进

范函^{1,2},张少武¹

(1.信息工程大学电子技术学院,郑州450004; 2.许继昌南通信设备有限公司,河南许昌461000)

(han_21st@yahoo.com.cn)

摘要:利用陈宁宇等人(陈宁宇,顾永跟,苏晓萍.数字签名方案的同底构造攻击.计算机应用,2010,30(4):1042-1044)提出的同底构造攻击方法对两个基于离散对数的数字签名方案进行了攻击分析。对李方伟等人(李方伟,谭利平,邱成刚,基于离散对数的代理盲签名.电子科技大学学报,2008,37(2):172-174)提出的一种改进的代理盲签名方案进行了攻击分析,发现不诚实的代理签名人利用伪造攻击,可以假冒代理签名接收人生成有效的代理盲签名。对 LEIN HARN 等人(HARN L, REN JIAN, LIN CHANGLU. Design of DL-based certificateless digital signatures. Journal of Systems and Software, 2009, 82(5):789-793)提出的一种基于离散对数的无证书签名方案进行了攻击分析,发现不诚实的密钥生成中心(PKG)可以伪造用户的私钥。给出了攻击的方法,分析了造成攻击的原因并提出了相应的改进措施。

关键词:数字签名;离散对数;代理盲签名;无证书签名;同底构造攻击

中图分类号:TP309.7 文献标志码:A

Attack analysis and improvement on two DL-based digital signature schemes

FAN Han^{1,2}, ZHANG Shao-wu¹

(1. Institute of Electronic Technology, Information Engineering University, Zhengzhou Henan 450004, China;

2. XJ Changnan Communications Equipment Company Limited, Xuchang Henan 461000, China)

Abstract: The method of identical base construction attack on digital signature scheme proposed by CHEN NING-YU et al. (CHEN NING-YU, GU YONG-GEN, SU XIAO-PING. Identical base construction attack on digital signature scheme. Journal of Computer Applications, 2010, 30(4): 1042-1044) was used to carry out attack analysis on the two DL-based digital signature schemes. The improved proxy blind signature scheme proposed by LI FANG-WEI et al. (LI FANG-WEI, TAN LI-PING, QIU CHENG-GNAC. A proxy blind signature scheme based on DLP. Journal of Electronic Science and Technology, 2008, 37(2): 172-174.) was analytical attacked. It was found out that, using the forgery attack, a dishonest proxy signer could fake proxy signature receiver to generate valid proxy blind signature. A DL-based signature scheme without certificates proposed by Lein Harn et al. (HARN L, REN JIAN, LIN CHANGLU. Design of DL-based certificateless digital signatures. Journal of Systems and Software, 2009, 82(5): 789-793) was analyzed and it was found that the dishonest Private Key Generator (PKG) can forge the user's private key. The cause of the attack was analyzed and the attack methods and the improvement measures were presented.

Key words: digital signature; discrete logarithm; proxy blind signature; certificateless digital signature; identical base construction attack

0 引言

数字签名是现代信息安全系统的核心技术之一。1976年,Diffie 和 Hellman 在他们的著名文献《密码学的新方向》^[1]里首次提出了数字签名的概念。数字签名在身份认证、数字完整性、不可抵赖性等方面的功能实现,都有重要应用。对于基于离散对数的安全的数字签名方案,攻击者想要进行伪造攻击,就要面临解离散对数的难题。但实际构造的签名方案,由于签名因子或整个签名方案设计的不合理,使得攻击者很容易通过将签名验证等式进行变形,将其转换成一个同底的等式,并通过指数的相等伪造出签名数据,攻击者可以避开求解高次剩余或离散对数,这使得签名方案丧失了安全性。这就是陈宁宇等人在文献[2]中提出的同底构造攻击的概念。

本文用同底构造攻击的方法对两个基于离散对数的数字签名方案(李方伟等人^[3]提出的改进的代理盲签名方案(以下简称李方案)、Lein Harn 等人^[4]提出的基于离散对数的无证书签名方案(以下简称 HARN 方案))进行了攻击分析,并针对原方案的缺陷,根据代理盲签名的性质和无证书签名的定义及攻击模型,提出了改进方法。

1 李方案的攻击分析与改进

在 Mambo 等人提出的代理签名体制中^[5],称为代理签名人的一一个指定签名人,可以代表原始签名人签字。按照数字签名权力委托过程的方式,代理签名可分为完全代理、部分代理和具有授权证书的代理三种基本类型。代理签名在许多应用领域如电子交易、安全移动代理等方面发挥着重要的作用,在提出后即受到了广泛关注。之后,许多特殊类型的代理签

收稿日期:2010-12-27;修回日期:2011-01-28。

作者简介:范函(1963-),男,河南许昌人,工程师,硕士研究生,主要研究方向:密码学、数字签名; 张少武(1964-),男,河南洛阳人,教授,主要研究方向:密码学、信息安全。

名被提了出来,如多重代理签名、门限代理签名及代理盲签名等。2002 年,谭作文等人在文献[6]中引入了代理盲签名的概念,之后多个代理盲签名方案被相继提出^[7-8],代理盲签名方案同时具备了代理签名和盲签名的安全性优点。

1.1 李方案介绍

李方伟等人针对文献[9]中代理盲签名方案的缺陷,提出了一种改进的新方案^[3]。

首先介绍文献[9]中 WANG 的代理盲签名方案如下:

设待签名的消息为 m ,安全参数 p,q 为两个大素数,且 $q \mid (p-1)$; g 为 $GF(q)$ 的本原元; h 为一个安全的单向 Hash 函数; \parallel 表示比特串并; A 为原始签名人, B 为代理签名人, C 为代理签名接收人; $x_A, x_B, x_C \in [1, p-1]$ 分别为 A, B, C 的私钥; 相应的公钥分别为: $y_A = g^{x_A} \bmod p, y_B = g^{x_B} \bmod p$ 和 $y_C = g^{x_C} \bmod p$ 。

代理授权过程如下:

1) 原始签名人 A 随机选择 $k_A \in Z_q^*$, 计算 $r_A = g^{k_A} \bmod p, s_A = x_A + k_A y_B \bmod q$, 并将 (r_A, s_A) 发送给代理签名人 B 。

2) B 检验 $g^{s_A} = y_A r_A^{x_B} \bmod p$ 。如果等式成立, B 则接受 (r_A, s_A) , 并计算代理签名私钥 $x_p = s_A + x_B y_A \bmod q$, 相应的代理签名公钥为: $y_p = g^{x_p} = g^{s_A} y_B^{x_A} = y_A r_A^{x_B} y_B^{x_A} \bmod p$ 。接收者可以通过 A, B 的公钥 y_A, y_B 以及公开信息 r_A 计算 y_p 。

代理盲签名过程如下:

1) B 随机选取 $k \in Z_q^*$, 计算 $t = g^k \bmod p$, 并把 t 发送给代理签名接收人 C 。

2) C 选择随机数 $a, b \in Z_q^*$, 进行以下计算:

$$\begin{aligned} r &= t g^{a+x_c} y_p^{-b} \bmod p \\ e &= h(r \parallel m) \bmod q \\ e' &= e + b \bmod q \end{aligned}$$

把 e' 发给 B 。

3) B 接收到 e' , 计算 $s' = k - e' x_p \bmod q$, 并发送 s' 给 C 。

4) C 用接收到的 s' 计算 $s = s' + a \bmod q, (m, s, e)$ 就是一个有效的代理盲签名。

代理盲签名的验证过程为: 验证者收到 (m, s, e) 之后, 验证 $e = h(g^s y_p y_C \bmod p) \bmod q$, 如果等式成立则接受, 否则拒绝。

李方伟等人针对文献[9]中代理盲签名方案的缺陷, 提出了一种改进的新方案如下:

参数设置与原方案相同, 代理授权过程如下:

1) 原始签名人 A 随机选择 $k_A \in Z_q^*$, 计算 $r_A = g^{k_A} \bmod p, s_A = x_A r_A + k_A y_B \bmod q$, 并将 (r_A, s_A) 发送给代理签名人 B 。

2) B 检验 $g^{s_A} = y_A r_A^{x_B} \bmod p$ 。如果等式成立, B 则接受 (r_A, s_A) , 并计算代理签名私钥 $x_p = s_A + x_B r_A \bmod q$, 相应的代理签名公钥为 $y_p = g^{x_p} = g^{s_A} y_B^{x_A} = y_A r_A^{x_B} y_B^{x_A} \bmod p$ 。检验接受者可以通过 A, B 的公钥 y_A, y_B 以及公开信息 r_A 计算 y_p 。

代理盲签名过程如下:

1) B 随机选取 $k \in Z_q^*$, 计算 $t = g^k \bmod p$, 并把 t 发送给代理签名接收人 C 。

2) C 选择随机数 $a, b, u \in Z_q^*$, 进行以下计算:

$$\begin{aligned} r &= t^b g^a y_p^{bu} \bmod p \\ e &= h(r \parallel m) \bmod q \\ e' &= \frac{e}{b} - u \bmod q \end{aligned}$$

随即把 e' 发给 B 。

3) B 接收到 e' , 计算 $s' = k - e' x_p \bmod q$, 并发送 s' 给 C 。

4) C 用接收到的 s' 计算 $s = bs' + a \bmod q, (m, s, e)$ 就是一个有效的代理盲签名。

代理盲签名的验证过程为: 验证者收到 (m, s, e) 之后, 验证 $e = h(g^s y_p \bmod p \parallel m) \bmod q$, 如果等式成立则接受, 否则拒绝。

1.2 对李方案的攻击分析

经分析发现, 通过验证等式, 利用同底构造攻击^[2], 代理签名人 B 可以假冒代理签名接收人 C 并伪造消息 m' 即可得到有效的代理盲签名。因为 $y_p = g^{x_p} \bmod p$, 所以验证等式也为 $e = h(g^s g^{x_p} \bmod p \parallel m') \bmod q$ 。对于消息 m' , B 随机选取 $\sigma \in Z_q^*$ 计算得到 e 的值为 $e = h(\sigma \parallel m') \bmod q$ 。利用 $g^s g^{x_p} = g^\sigma \bmod p$, 由同底关系得到 $s + x_p e = \sigma \bmod q$, 且代理签名私钥 x_p 是由代理签名人 B 计算的, 所以代理签名人 B 即可计算出 $s = \sigma - x_p e \bmod q$, 因此得到的 (m', s, e) 就是一个有效的代理盲签名。代理签名人 B 假冒代理签名接收人 C 向验证者发送 (m', s, e) , 验证者收到后验证 $e = h(g^s y_p \bmod p \parallel m') \bmod q$, 如果等式成立则接受, 否则拒绝。

正确性:

$$\begin{aligned} h(g^s y_p \bmod p \parallel m') \bmod q &= \\ h(g^s g^{x_p} \bmod p \parallel m') \bmod q &= h(g^\sigma \parallel m') \bmod q = e \end{aligned}$$

1.3 对此盲代理签名方案的改进

为了抵抗这种伪造攻击, 可对李方案做进一步改进。在代理盲签名过程中, 改为 C 计算 $r = t^b g^{a+x_c} y_p^{bu} \bmod p$, 同时验证式变为 $e = h(g^s y_p y_C \bmod p \parallel m) \bmod q$, 其他部分均保持不变。

代理盲签名的验证过程为: 验证者收到 (m, s, e) 之后, 验证 $e = h(g^s y_p y_C \bmod p \parallel m) \bmod q$, 如果等式成立则接受, 否则拒绝。

证明

$$\begin{aligned} g^s y_p y_C \bmod p &= g^{bs' + a} y_p^e y_C \bmod p = \\ g^{b(k-e'x_p)+a} y_p^{(e'+u)b} y_C \bmod p &= g^{bk+a} y_p^{bu} y_C \bmod p = \\ t^b g^a y_p^{bu} g^{x_c} \bmod p &= t^b g^{a+x_c} y_p^{bu} \bmod p = r \end{aligned}$$

1.4 本文改进方案的安全性分析

因为经上述改进后, 验证式变为 $e = h(g^s y_p y_C \bmod p \parallel m) \bmod q$, 又因为 $y_C = g^{x_c} \bmod p$, 所以验证式也为 $e = h(g^s g^{x_c} \bmod p \parallel m) \bmod q$ 。如果仍采用上述攻击方法, 代理签名人 B 利用 $g^s g^{x_p} g^{x_c} = g^\sigma \bmod p$, 由同底关系得到 $s + x_p e + x_c = \sigma \bmod q$, 虽然代理签名人 B 可计算出代理签名私钥 x_p , 但是因为不知道代理签名接收人 C 的私钥 x_c 而无法计算出 s , 则代理签名人 B 不能由这种攻击方法伪造出一个有效的代理盲签名。改进方案在其他方面仍保持原方案的安全性。

2 HARN 方案的攻击分析与改进

2003 年, Al-Riyami 等人在文献[10]提出了无证书公钥密码体制的概念。在该体制中, 用户的密钥由两个部分生成: 一部分是由密钥生成中心使用主密钥为用户生成基于身份的部分私钥, 并通过安全信道发送给用户; 另一部分是用户自选的秘密值。用户将上述两个部分组合生成真正的私钥。可信中心生成的基于用户身份的部分私钥是将用户身份与用户公钥结合起来的关键, 因而, 无证书公钥密码系统不存在传统公钥体制中证书的管理问题。因为用户独自生成密钥, 密钥生成中心不知道用户的私钥, 所以解决了基于身份的公钥密码体制所固有的密钥托管问题。随后, 一些基于无证书公钥密码体制的数字签名方案陆续被提出^[11-12]。

2.1 HARN 方案介绍

HARN 方案是一种基于离散对数的无证书签名方案, 它

由改进的 ElGamal 签名方案转换而来,包括 4 个算法。

1) 私钥生成中心(Private Key Generator, PKG)密钥生成 $K_{\text{pk}}(1^n)$:这个算法输入安全参数 1^n ,输出公共参数 params 和 PKG 的主私钥。

(1) 产生一个大素数 p 和一个生成元 $g \in Z_p^*$ 。

(2) 随机选择 $x \in Z_p^*$ 作为私钥,计算公钥 $y = g^x \bmod p$ 。

(3) 把 $\text{params} = (p, g, y)$ 作为 PKG 的公共参数,同时保留 x 作为 PKG 的主密钥。

2) 用户密钥生成 $K_u(\text{params}, ID)$:这个算法输入公共参数 params 和用户的身份 ID ,与 PKG 互动后输出用户的私钥 s 和公钥 (r, R) 。

(1) 用户随机选择 $v \in Z_{p-1}^*$ 作为私钥,且 $\gcd(v, p - 1) = 1$,计算 $u = g^v \bmod p$ 。发送 $\{ID, u\}$ 给 PKG。

(2) PKG 产生参数对 (r, z) ,并满足条件 $g^{h(ID, r)} = y^r t^z \bmod p$,这里 h 是一个单向哈希函数。为此,PKG 首先选择一个 $k \in Z_{p-1}^*$ 且 $\gcd(k, p - 1) = 1$,然后计算 $t = g^k \bmod p$ 和 $r = u^k \bmod p$ 。PKG 解线性方程 $h(ID, r) = xr + kz \bmod (p - 1) \Rightarrow z = k^{-1}(h(ID, r) - xr) \bmod (p - 1)$ 。把求出的 (r, z) 发送给用户。

(3) 用户提取参数对 (r, s) ,并满足条件 $g^{h(ID, r)} = y^r r^s \bmod p$ 。为此,用户计算 $s = v^{-1}z \bmod (p - 1)$ 和 $R = r^s \bmod p$, s 即为用户的私钥, (r, R) 是用户的公钥。

3) 消息签名 $\text{Sign}(\text{params}, m, s)$:这个算法输入公共参数 params 、消息 m 和用户私钥 s ,输出对消息 m 的签名 σ 。

(1) 随机选取 $l \in Z_{p-1}^*$ 且 $\gcd(l, p - 1) = 1$,计算 $r_1 = l^s \bmod p$ 。

(2) 从 $h(m, r_1) = sr_1 + ls_1 \bmod (p - 1)$ 中解出 $s_1 = l^{-1}(h(m, r_1) - sr_1) \bmod (p - 1)$ 。

(3) $\sigma = (r, R, r_1, s_1)$ 即为对消息 m 完整的无证书数字签名。

4) 签名验证 $\text{Vf}(\text{params}, ID, m, \sigma)$:这个算法输入公共参数 params 、用户的身份 ID 和消息 m ,输出拒绝或接受。

由如下两个等式验证基于身份 ID 和公钥 (r, R) 对消息 m 的无证书数字签名 σ 的正确性:

$$g^{h(ID, r)} = y^r R \bmod p; r^{h(m, r_1)} = R^{r_1} r_1^s \bmod p$$

若两个等式同时成立,则接受签名 σ ,否则拒绝签名 σ 。

2.2 对 HARN 方案的攻击分析

经分析发现,由于用户的一个公钥 r 是由 PKG 计算的,不诚实的 PKG 利用同底构造攻击可以伪造出用户的私钥 s 。PKG 随机选取 $\alpha \in Z_{p-1}^*$ 且 $\gcd(\alpha, p - 1) = 1$,计算 $r = g^\alpha \bmod p$ 。因为有 $g^{h(ID, r)} = y^r r^s \bmod p$,所以有 $g^{h(ID, r)} = g^{xr} g^{\alpha s} \bmod p$ 。由同底关系可得 $h(ID, r) = xr + \alpha s \bmod (p - 1)$,且 x 为 PKG 的私钥,因而 PKG 从中即可解出 $s = \frac{h(ID, r) - xr}{\alpha}$ 。这样,

PKG 就伪造出了用户的私钥 s ,因此得到的签名 $\sigma = (r, R, r_1, s_1)$ 即为对消息 m 的有效签名。

攻击的正确性验证:

$$1) y^r R \bmod p = g^{xr} R \bmod p = g^{xr} r^s \bmod p = g^{xr} g^{\alpha s} \bmod p = g^{xr + \alpha s} \bmod p = g^{h(ID, r)}$$

$$2) R^{r_1} r_1^s \bmod p = R^{r_1} r_1^{-1} \bmod p = r^{sr_1} r_1^s \bmod p = r^{sr_1 + ls_1} \bmod p = r^{h(m, r_1)}$$

2.3 对 HARN 方案的改进

为了消除此方案这一缺陷,可对第二个算法用户密钥生

成 $K_u(\text{params}, ID)$ 改进如下:

用户密钥生成 $K_u(\text{params}, ID)$:这个算法输入公共参数 params 和用户的身份 ID ,与 PKG 互动后输出用户的私钥 s 和公钥 (r, R) 。

1) 用户发送自己的 ID 给 PKG。

2) PKG 收到用户的 ID 后,随机选择一个 $k \in Z_{p-1}^*$ 且 $\gcd(k, p - 1) = 1$,然后计算 $t = g^k \bmod p$,把 t 发送给该用户。

3) 用户随机选择 $v \in Z_{p-1}^*$ 作为私钥,且 $\gcd(v, p - 1) = 1$,计算 $r = t^v \bmod p$ 并公开 r 作为用户的公钥。

4) PKG 产生参数 z ,并满足条件 $g^{h(ID, r)} = y^r t^z \bmod p$,这里 h 是一个单向哈希函数。为此,PKG 解线性方程 $h(ID, r) = xr + kz \bmod (p - 1) \Rightarrow z = k^{-1}(h(ID, r) - xr) \bmod (p - 1)$ 。把求出的 z 发送给用户。

5) 用户提取参数对 (r, s) ,并满足条件 $g^{h(ID, r)} = y^r r^s \bmod p$ 。为此,用户计算 $s = v^{-1}z \bmod (p - 1)$ 和 $R = r^s \bmod p$, s 即为用户的私钥, (r, R) 是用户的公钥。

其他部分保持原方案不变。

2.4 对本文改进方案的安全性分析

在一般性定义的无证书签名方案中,私钥生成中心 PKG 只执行系统生成和部分私钥生成两个算法,私钥生成中心 PKG 只能产生用户的部分私钥,用户的公钥和私钥都是由用户自己生成的。在相应的无证书数字签名算法攻击模型中攻击者主要为两种类型。第一类攻击者 A_I:这类攻击者只可以替换任意用户的公钥,但不知道系统的主密钥,他抽取可信中心的部分私钥或者直接获得签名密钥,然后进行签名;第二类攻击者 A_{II}:能够拥有主密钥,可以自己产生部分私钥,但是却不能进行公钥替换。而此基于离散对数的无证书签名方案却由私钥生成中心(PKG)生成用户的公钥 r ,这样就使私钥生成中心 PKG 有机会进行公钥替换攻击,不符合无证书数字签名的一般性定义。此改进方案中用户的公钥 r 改为由用户自己生成,而不是由私钥生成中心 PKG 生成,这样就不给私钥生成中心 PKG 以可乘之机进行公钥替换攻击,使改进的方案对于上述攻击模型是安全的。改进方案在消除了缺陷的同时仍保持了原方案的特点及其他方面的安全性。

3 结语

本文利用陈宁宇等人提出的同底构造攻击方法对李方伟等人的基于离散对数的代理盲签名方案和 Lein Harn 等人的基于离散对数的无证书数字签名方案进行了攻击分析,给出了攻击方法,证明了两个方案都存在着安全缺陷。并根据代理盲签名的性质和无证书签名的定义及攻击模型,对造成攻击的原因进行了分析并提出了相应的改进措施。本文的分析表明,对攻击分析方法的研究与应用有助于设计出安全可靠的数字签名方案。

参考文献:

- [1] DIFFIE W, HELLMAN M E. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644–654.
- [2] 陈宁宇,顾永跟,苏晓萍.数字签名方案的同底构造攻击[J].计算机应用,2010,30(4):1042–1044.
- [3] 李方伟,谭利平,邱成刚.基于离散对数的代理盲签名[J].电子科技大学学报,2008,37(2):172–174.
- [4] HARN L, REN JIAN, LIN CHANLU. Design of DL-based certificateless digital signatures[J]. The Journal of Systems and Software, 2009, 82(5): 789–793.

- tion, 2005, 169(2): 982–994.
- [3] BELLOVIN S, MERRITT M. Encrypted key exchange: Password-based protocols secure against dictionary attacks[C]// Proceedings of the 1992 IEEE Symposium on Research in Security and Privacy. Washington, DC, IEEE Computer Society, 1992: 72–84.
- [4] BELLOVIN S, MERRITT M. Augmented encrypted key exchange: Password-based protocol secure against dictionary attacks and password file compromise[C]// Proceedings of the 1st ACM Conference on Computer and Communications Security. New York: ACM, 1993: 244–250.
- [5] BELLARE M, POINTCHEVAL D, ROGAWAY P. Authenticated key exchange secure against dictionary attacks[C]// International Conference on the Theory and Application of Cryptographic Techniques. Berlin: Springer-Verlag, 2000: 139–155.
- [6] BOYKO V, MACKENZIE P, PATEL S. Provably-secure password authentication and key exchange using Diffie-Hellman[C]// EUROCRYPT2000. Berlin: Springer-Verlag, 2000: 156–171.
- [7] KATZ J, OSTROVSKY R, YUNG M. Efficient password authenticated key exchange using human-memorable passwords[C]// EUROCRYPT 2001. Berlin: Springer-Verlag, 2001: 475–494.
- [8] ABDALLA M, FOUQUE P-A, POINTCHEVAL D. Password-based authenticated key exchange in the three-party setting[C]// Public Key Cryptography, LNCS 3386. Berlin: Springer-Verlag, 2005: 65–84.
- [9] JIANG S Q, GONG G. Password based key exchange with mutual authentication[C]// Proceedings of SAC 2004, LNCS 3357. Berlin: Springer-Verlag, 2004: 267–279.
- [10] SHAO JUN, CAO ZHENFU, WANG LICHENG. Efficient password-based authenticated key exchange without public information [C]// Proceedings of ESORICS 2007, LNCS 4734. Berlin: Springer-Verlag, 2007: 299–310.
- [11] FENG D G, CHEN W D. Modular approach to the design and analysis of password-based security protocols[J]. Science in China: Series F, 2007, 50(3): 381–398.
- [12] Trusted computing group. Trusted computing platform alliance (TCPA). Main specification version 1.1b[S], 2001.
- [13] VIET D Q, YAMAMURA A, TANAKA H. Anonymous password-based authenticated key exchange [C]// Proceedings of INDOCRYPT 2005, LNCS 3797. Berlin: Springer-Verlag, 2005: 244–257.
- [14] YANG J, ZHANG Z. A new anonymous password-based authenticated key exchange protocol [C]// Proceedings of INDOCRYPT 2008, LNCS 5365. Berlin: Springer-Verlag, 2008: 200–212.
- [15] SHIN S H, KOBARA K, IMAI H. A secure threshold anonymous password authenticated key exchange protocol[C]// Crypto 2009, LNCS 4752. Berlin: Springer-Verlag, 2009: 444–458.
- [16] SHERMAN S, M. CHOW, KIM-KWANG R C. Strongly-secure identity-based key agreement and anonymous extension[C]// Proceedings of ISC 2007, LNCS 4779. Berlin: Springer-Verlag, 2007: 203–220.
- [17] 关晨至, 石永革. 基于DAA的可信双向匿名认证密钥协商协议[J]. 计算机系统应用, 2009, 18(12): 59–61, 78.
- [18] BRESSON E, CHEVASSUT O, POINTCHEVAL D. New security results on encrypted key exchange[EB/OL].[2010-08-20]. <http://www.iacr.org/cryptodb/archive/2004/PKC/3376/3376.pdf>.
- [19] JUELS A, BRAINARD J. Client puzzles: A cryptographic defense against connection depletion attacks[C]// Proceedings of Networks and Distributed Systems Security. New York: ACM, 1999: 151–165.
- [20] BELLARE M, ROGAWAY P. Entity authentication and key distribution[C]// Advances in Cryptology—CRYPTO'93, LNCS 773. Berlin: Springer-Verlag, 1993: 232–249.
- [21] 林闯, 蒋屹新, 尹浩. 网络安全控制机制[M]. 北京: 清华大学出版社, 2008.
- [22] WILSON S B, JOHNSON D, MENEZES A. Key agreement protocols and their security analysis[C]// Proceedings of the 6th International Conference on Cryptography and Coding, LNCS 1355. Berlin: Springer-Verlag, 1997: 30–45.
- [23] 周永彬, 张振峰, 冯登国. 一种认证密钥协商协议的安全分析及改进[J]. 软件学报, 2006, 17(4): 868–875.
- [24] BELLARE M, ROGAWAY P. Provably secure session key distribution the three party case[C]// Proceedings of the 27th Annual ACM Symposium on the Theory of Computing. New York: ACM, 1995: 57–66.
- [25] DESMEDT Y, FRANKEL Y. Threshold cryptosystems[C]// Advances in Cryptology—CRYPTO'89, LNCS 435. Berlin: Springer-Verlag, 1990: 307–315.
- [26] PEDERSEN T P. A threshold cryptosystem without a trusted party [C]. Advances in Cryptology—EUROCRYPT'91. Berlin: Springer-Verlag, 1991: 522–526.
- [27] KOBLITZ N, MENEZES A, VANSTONE S. The state of elliptic curve cryptography[J]. Designs, Codes and Cryptography, 2000, 19(2/3): 173–193.
- [28] CHEN L, CHENG Z, SMART N P. Identity-based key agreement protocols from pairings[J]. International Journal of Information Security and Privacy, 2007, 6(4): 213–241.

(上接第1861页)

- [5] MAMBO M, USUDA K, OKAMOTO E. Proxy signatures: Delegation of the power to sign messages[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 1996, E79-A(9): 1338–1354.
- [6] TAN ZUOWEN, LIN ZHOUJUN, TANG CHUNMING. Digital proxy blind signature schemes based on DLP and ECDLP[J]. MM Research Preprints, 2002, 21(7): 212–217.
- [7] AWASTHI A K, SUNDER L. Proxy blind signature scheme[J]. Transactions on Cryptology, 2005, 2(1): 5–11.
- [8] SUN H M, HSIEH B T. On the security of some proxy blind signature schemes[EB/OL].[2010-08-20]. <http://eprint.iacr.org>.
- [9] WANG SHAOBIN, HONG FAN, CUI GUOHUA. Secure efficient proxy blind signature schemes based DLP[C]// Proceedings of the Seventh IEEE International Conference on E-Commerce Technology. New York: IEEE, 2005: 452–455.
- [10] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography [C]// Cryptology-Asiacrypt 2003, LNCS 2894. Berlin: Springer-Verlag, 2003: 452–473.
- [11] CASTRO R, DAHAB R. Two notes on the security of certificateless signatures[C]// Proceedings of the 1st International Conference on Provable Security, LNCS 4784. Berlin: Springer-Verlag, 2007: 85–102.
- [12] HUANG XINYI, MU YI, SUSILO W, et al. Certificateless signature revisited [C]// Proceedings of the 12th Australasian Conference on Information Security and Privacy, LNCS 4586. Berlin: Springer-Verlag, 2007: 308–32.