可证明安全数字签名方案的密码学分析*

王永峰, 胡运红
(运城学院 应用数学系, 山西 运城 044000)

摘 要: 为了克服基于身份密码体制的密钥托管问题和基于无证书密码体制的公钥替换问题,研究者提出了基于证书密码体制的概念。针对李志敏等人提出的基于证书的签名方案提出分析,证明其不满足不可伪造性;针对黄茹芬等人提出的基于证书盲签名方案提出分析,结果表明它不能抵抗公钥替换攻击;对何俊杰提出的基于身份的部分盲签名方案提出分析,指出它不能抵抗窜改协商公共信息攻击。

关键词: 基于身份的签名方案; 基于证书的签名方案; 部分盲签名方案; 随机预言模型; 公钥替换攻击; 窜改协商公共信息攻击

中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2013)12-3749-04

doi:10.3969/j.issn.1001-3695.2013.12.060

Cryptanalysis of provably digital secure signature schemes

WANG Yong-feng, HU Yun-hong
(*Dept. of Applied Mathematics, Yuncheng University, Yuncheng Shanxi* 044000, *China*)

Abstract: In order to overcoming key-escrow problem of ID-based cryptosystem and public key replacing problem of certificateless cryptosystem, researcher proposed the definition of certificate-based cryptosystem. This paper analyzed the certificate-based signature scheme by Li Zhi-min et al. The result showed that it couldn't meet the safe requirement of unforgeability. It analyzed a certificate-based blind signature scheme by Huang Ru-fen et al. The result indicated that it was not security by replacing public key attack. It analyzed an ID-based partially blind signature scheme by He Jun-jie et al. The result indicated that it didn't resist the changing agreed information attack.

Key words: ID-based signature scheme; certificate-based signature scheme; partially blind signature; random oracle model; public key replacement attack; changing agreed public information attack

0 引言

为了解决传统公钥密码体制中证书管理带来的开销问题,文献[1]提出了基于身份的密码体制,它是利用用户的身份信息(如 IP 地址、电子邮箱等)作为用户公钥,而对应的私钥由可信 PKG 生成。由于不再需要证书,基于身份的密码体制不存在证书管理问题。因为 PKG 掌握每个用户的私钥,可以伪装成任意用户生成合法有效的签名信息或加密信息,所以基于身份的密码体制存在固有的密钥托管问题。为了解决这个问题, 2003 年,Gentry[2] 提出基于证书加密的概念,克服了传统公钥密码体制和基于身份公钥密码体制的安全缺陷。在基于证书密码体制中,用户自己生成公钥和私钥,CA 利用用户身份信息和公钥生成证书,利用用户私钥和证书生成有效的签名信息或加密信息。之后,基于证书的公钥密码体制得到国内外学者们的广泛关注[3~6]。Kang 等人[3] 提出了基于证书的签名方案和安全定义。Wu 等人[4] 进一步完善了基于证书签名体制的安全定义。2012 年,李继国等人[5] 提出基于证书强指定验证者签名的概念和安全模型,并在随机预言模型下证明了所提方案的安全性。同年,李志敏等人[6] 提出了一个基于证书数字签名方案,整个签名算法不需要双线性对运算,而在签名验证算法中需要一个双线性对运算,并在随机预言模型下证明了其安全性。但是本文分析发现文献[6]的方案不可以抵抗广义伪造攻击,也就是说任意第三方都可以成功伪造攻击。

盲签名的概念是由 Chaum[7] 提出的,它是指签名者所签消息的具体内容,同时,不可以将签名和最终得到的签名对应起来。盲签名可广泛应用在各种需要匿名性的场合,如电子选举、电子招标等。之后,人们对盲签名方案作了广泛研究[8~10]。2007 年,刘亚丽等人[8] 提出前向安全的盲签名方案,邱钢等人[9] 指出文献[8]的方案是不安全的。基于强 L-SDHP 难题,文献[10]设计了一个高效的无可信 PKG 的盲签名方案。2012 年,黄茹芬等人[11] 构造了一类可证安全的基于证书盲签名方案。本文分析发现文献[11]的方案不可以抵抗公钥替换攻击。

在盲签名中,由于签名者完全不知道所签消息的具体内容,可能造成签名被非法使用。为了解决这个问题,Abe 等人[12] 提出了部分盲签名的概念,它是指允许签名者在签名中嵌入与用户事先协商的公共信息,并且这些公共信息不可以被删除或窜改。之后,多种部分盲签名方案被提出或分析[13~18]。

收稿日期: 2013-03-25; **修回日期**: 2013-05-02 **基金项目**: 国家自然科学基金资助项目(11241005);运城学院研究生科研启动项目(YPU-2010033)

作者简介: 王永峰(1979-),男,山西运城人,讲师,硕士,主要研究方向为密码学、信息安全(d2000d@163.com);胡运红(1974-),女,山西运城人,副教授,博士,主要研究方向为最优化理论与方法、数据挖掘、机器学习、支持向量机理论与算法等.

文献[13]定义了基于身份的部分盲签名方案的安全模型,并证明了在随机预言模型下所提出的方案是安全的。李明祥等人[14]指出文献[13]提出的安全模型是不完善的;2008年,崔巍等人[15]设计了一个基于身份的高效部分盲签名方案;李明祥等人[16]分析文献[15]的方案不可以抵抗窜改协商信息攻击,并作了改进;2013年,何俊杰等人[17]指出文献[16]提出的改进方案仍然不可以抵抗抗窜改协商信息攻击,又作了改进。2012年,何俊杰等人[18]提出了一个高效的基于身份的部分盲签名方案,并在随机预言模型下证明了方案是不可伪造的。本文分析发现文献[18]的方案同样不可以抵抗窜改协商信息攻击。

1 预备知识

1.1 双线性映射

设 G_1 与 G_2 分别为阶为大素数 q 的加法群和乘法群,若映射 $e:G_1\times G_1\to G_2$ 满足下列性质,则称此映射为双线性映射。

性质1 双线性。对所有的 $U,V\in G_1$ 和 $a,b\in Z_q^*$,总有 $e(aU,bV)=e(U,V)^{ab}$。

性质2 非退化性。存在 $U,V\in G_1$,使得 $e(U,V)\neq 1_{G_2}$,其中 1_{G_2} 是 G_2 的单位元。

性质3 可计算性。对所有的 $U,V\in G_1$,存在高效的算法计算 $e(U,V)$。

1.2 困难性假设

1)离散对数问题(DLP) 设 G 是一个乘法群,并且 P、Q 均为 G 的元素,计算一个正整数 $n\in Z_q^*$,使之满足 $Q=aP$。

2)计算 Diffie-Hellman 问题(CDH) 设 P 是 q 阶循环群 G_1 的生成元,给定 $P,aP,bP\in G_1$。其中,$a,b\in \mathbf{Z}_q^*$,且未知,计算 abP。

假设 DLP 和 CDH 计算是困难的,即对于概率多项式时间的对手,可以成功解决上述问题的优势是可以忽略不计的。

2 李志敏等人的方案及其分析

2.1 李志敏等人的方案

基于 Diffie-Hellman 问题困难假设下,李志敏等人构造了一个基于证书签名方案[6],并在随机预言模型下证明了其安全性。

1)参数生成

CA 选取阶均为素数 q 的加法群 G_1 和乘法群 G_2,P 为 G_1 的一个生成元,构造一个双线性映射 $e:G_1\times G_1\to G_2$,随机选取秘密值 $s\in Z_q^*$ 作为系统主私钥,系统公钥为 $P_{\text{pub}}=sP$,三个安全的 hash 函数 $H_1,H_2,H_3:\{0,1\}^*\times G_1\to G_1$,系统公开参数 params 为 $\{G_1,G_2,q,p,P,P_{\text{pub}},e,H_1,H_2,H_3\}$。

2)密钥生成

用户 A 任意选择 $x\in Z_q^*$,计算公钥为 $PK_A=xP$,私钥为 $K_A=x$。

3)证书生成

给定用户 A 的身份 ID_A 和其公钥 PK_A,CA 计算证书 $\text{Cert}_A=sH_1(\text{ID}_A,PK_A)$。

4)签名生成

对消息 $m\in\{0,1\}^*$,用户 A 如下计算:

a)任意选择 $r\in Z_q^*$;

b)$W=r^{-1}(C_A+K_AH_2(m,\text{ID},PK_A))$;

c)计算 $V=rH_3(m,W)$;

d)签名 $\sigma=(W,V)$;

5)签名验证。

收到签名消息 σ 以后,验证者验证等式 $e(PW,V)=e(P_{\text{pub}}H_1(\text{ID}_A,PK_A),H_3(m,W))\cdot e(PK_AH_2(m,\text{ID}_A,PK_A),H_3(m,W))$ 是否成立。若成立,接受签名;否则,认为签名无效。

2.2 李志敏等人方案的安全分析

对任意消息 $m\in\{0,1\}^*$,伪造攻击如下:

a)任意选择 $r\in Z_q^*$;

b)$W^*=r^{-1}P_{\text{pub}}H_1(\text{ID}_A,PK_A)+r^{-1}PK_AH_2(m,\text{ID},PK_A)$;

c)计算 $V^*=rH_3(m,W)P^{-1}$;

d)签名 $\sigma^*=(W^*,V^*)$。

接下来证明 σ^* 是有效的。$e(PW^*,V^*)=e(Pr^{-1}P_{\text{pub}}H_1(\text{ID}_A,PK_A),rH_3(m,W)P^{-1})\cdot e(r^{-1}PPK_AH_2(m,\text{ID}_A,PK_A),rH_3(m,W)P^{-1})=e(P_{\text{pub}}H_1(\text{ID}_A,PK_A),H_3(m,W))\cdot e(PK_AH_2(m,\text{ID}_A,PK_A),H_3(m,W))$。等式成立,说明伪造成功。

3 黄茹芬等人的方案及其安全分析

3.1 黄茹芬等人的方案

黄茹芬等人[11]的方案包括系统建立、密钥生成、证书生成、签名产生和签名验证五种算法。

1)系统建立

给定安全参数 1^k,CA 选取阶均为素数 q 的加法群 G_1 和乘法群 G_2,P 为 G_1 的一个生成元,构造一个双线性映射 $e:G_1\times G_1\to G_2$,计算 $g=e(P,P)$,随机选取秘密值 $s_c\in Z_q^*$ 作为系统主私钥,记为 msk,系统公钥为 s_cP,记为 mpk,两个安全的 hash 函数 $H_1:\{0,1\}^*\to Z_p^*$,$H_2:\{0,1\}^*\times G_1\to Z_p^*$。系统公开参数为 $\{G_1,G_2,e,p,P,\text{mpk},g,H_1,H_2\}$。

2)密钥生成

给定系统参数和身份 ID_A,签名者随机选取 $s_A\in Z_p^*$ 作为用户私钥,用户公钥为 $PK_A=(X_A,Y_A)$,$X_A=\dfrac{1}{s_A}P$,$Y_A=\dfrac{\text{mpk}}{s_A}$。

3)证书生成

输入 params、msk、PK_A 以及 ID_A,CA 计算私钥 $Q_A=H_1(\text{ID}_A\|PK_A)$,输出证书为 $\text{Cert}_A=\dfrac{1}{Q_A+s_c}P$。

4)签名产生

输入 params、s_A、Cert_A 以及消息 m,算法运行如下:

a)承诺。签名者随机选择 $r\in Z_p^*$,计算 $R=g^r\in Z_q^*$,并把 R 发送给用户。

b)盲化。用户随机选择 $\alpha,\beta\in Z_q^*$ 作为盲化因子,计算 $U=R^\alpha g^\beta$,$h=H_2(m,U)$ 和 $h'=\alpha^{-1}(\beta+h)\bmod p$,将 h' 发给签名者。

c)签名。计算 $V'=(r+h')s_A\text{Cert}_A$,将 V' 发送给用户。

d)解盲。用户计算 $V=\alpha V'$,输出签名 $\sigma=(m,V,h)$。

5)签名验证

输入 params、PK_A 以及 σ,验证算法如下:

a)计算 $Q_A = H_1(\mathrm{ID}_A \| PK_A)$ 以及 $h = H_2(m, U)$;

b)验证下式是否成立:

$$h = H_2(m, e(V, X_A Q_A + Y_A) g^{-h})$$

若成立,输出"接收",否则,输出"拒绝"。

3.2　黄茹芬等人方案的安全分析

参考文献[4,11]的安全模型提出基于证书的数字签名方案存在两类攻击者:第一类攻击者 A_{I} 可以替换任何用户的公钥,但不能访问用户对应公钥的证书;第二类攻击者 A_{II} 知道系统主私钥,可以产生用户证书,但不能替换用户公钥。不可伪造性分析指出,在随机预言机模型和 q-SDH 困难假设以及 E-inv-CDH困难假设下,所构造的方案对攻击者 A_{I} 和 A_{II} 都是不可伪造的。但本文发现该方案对攻击者 A_{I} 是不安全的。

在密钥生成阶段,A_{I} 随机选取 $t_1, t_2 \in Z_p^*$,生成用户 A 的公钥 $PK_A = (X_A^*, Y_A^*)$,其中 $X_A^* = \frac{1}{t_1}P, Y_A^* = \frac{t_2}{t_1}P$。

在证书生成阶段,A_{I} 计算 $Q_A^* = H_1(\mathrm{ID}_A \| PK_A^*)$,输出证书为 $\mathrm{Cert}_A^* = \frac{1}{Q_A^* + t_2}P$。

在签名产生阶段,算法运行如下:

a)承诺。签名者随机选择 $r \in Z_p^*$,计算 $R = g^r \in Z_q^*$,并把 R 发送给用户。

b)盲化。对签名消息 m,A_{I} 随机选择 $\alpha, \beta \in Z_q^*$ 作为盲化因子,计算 $U = R^\alpha g^\beta$,$h = H_2(m, U)$ 和 $h' = \alpha^{-1}(\beta + h) \bmod p$,将 h'发送给签名者。

c)签名。签名者计算 $V'^* = (r + h') t_1 \mathrm{Cert}_A^*$,将 V'^* 发送给用户。

d)解盲。用户计算 $V^* = \alpha V'^*$,输出签名 $\sigma = (m, V^*, h)$。

下面证明 $\sigma = (m, V^*, h)$ 是有效的。

a)计算 $Q_A^* = H_1(\mathrm{ID}_A \| PK_A^*)$ 以及 $h = H_2(m, U)$;

b)验证:

$$H_2(m, e(V^*, X_A^* Q_A^* + Y_A^*) g^{-h}) =$$

$$H_2(m, e(\alpha V'^*, \frac{Q_A^* + t_2}{t_1}P) g^{-h}) =$$

$$H_2(m, e(\alpha(r + h') t_1 \frac{1}{Q_A^* + t_2}P, \frac{Q_A^* + t_2}{t_1}P) g^{-h}) =$$

$$H_2(m, e((\alpha r + \beta + h)P, P) g^{-h}) = H_2(m, e((\alpha r + \beta)P, P)) =$$

$$H_2(m, g^{\alpha r} g^\beta) = H_2(m, R^\alpha g^\beta) = H_2(m, U) = h$$

方案默认 $Y_A = s_c X_A$,利用 CA 掌握 s_c 的信息,输出证书 $\mathrm{Cert}_A = \frac{1}{Q_A + s_c}P$,使得签名有效。之所以可以成功攻击,是因为方案并没有验证 $Y_A = s_c X_A$ 是否成立。为此,可以在验证签名时,同时验证 $e(P, Y_A) = e(P_{\mathrm{pub}}, X_A)$ 是否成立。若该等式与 $h = H_2(m, e(V, X_A Q_A + Y_A) g^{-h})$ 同时成立,认为签名有效;否则,拒绝签名。

4　何俊杰等人的方案及其安全分析

4.1　何俊杰等人的方案

在 Shim[19] 所提方案基础上,文献[18]构造的基于身份部分盲签名方案参与实体由密钥生成中心 PKG、用户 A、签名者 B 组成,主要算法包括 PKG 设置、密钥提取、发布协议和验证四部分。

1)PKG 设置

PKG 选取阶为素数 q 的加法群 G_1 和乘法 G_2, P 为 G_1 的一个生成元,构造双线性对 $e: G_1 \times G_1 \to G_2$,选择抗碰撞的 hash 函数 $H_1: \{0,1\}^* \to G_1$, $H_2: \{0,1\}^* \times G_1 \to Z_q^*$, $H_3: \{0,1\}^* \to Z_q^*$。随机选择主密钥 $s \in Z_q^*$,系统公钥为 $P_{\mathrm{pub}} = sP$。系统公开参数为 $\{G_1, G_2, e, q, P, P_{\mathrm{pub}}, H_1, H_2, H_3\}$。

2)密钥提取

假设签名者 B 的身份为 $\mathrm{ID} \in \{0,1\}^*$,PKG 计算 B 的私钥为 $S_{\mathrm{ID}} = sQ(\mathrm{ID})$(其中 $Q(\mathrm{ID}) = H_1(\mathrm{ID})$),并将其通过安全信道发送给 B。B 通过验证等式 $e(Q_{\mathrm{ID}}, P_{\mathrm{pub}}) = e(S_{\mathrm{ID}}, P)$ 是否成立。如果成立,B 的公私钥为 $(Q_{\mathrm{ID}}, S_{\mathrm{ID}})$;否则,请求 PKG 重发。

3)发布协议

设需要签名信息为 m,用户和签名者协商的公共信息为 c。

a)承诺。签名者首先随机选取 $k' \in Z_q^*$,计算 $U' = k'P$,将 U'发送给用户 A。

b)盲化。用户 A 随机选择 $\alpha, \beta \in Z_q^*$,计算 $U = \alpha U' + \beta P$, $h = H(\mathrm{ID}, m, U)$, $h' = \alpha h \bmod q$,将 h'发送给签名者 B。

c)盲签名。签名者 B 收到 h'后,计算 $V' = h' k' P_{\mathrm{pub}} + H_3(c) S_{\mathrm{ID}}$,将 V'发给用户 A。

d)脱盲。用户 A 计算 $V = V' + \beta h P_{\mathrm{pub}}$,最终生成部分盲签名为 (U, V)。

4)验证

验证者收到消息 m 的签名 $(\mathrm{ID}, m, c, (U, V))$ 以后,计算 $Q_{\mathrm{ID}} = H_1(\mathrm{ID})$, $h = H_2(\mathrm{ID}, m, U)$, 验证等式 $e(V, P) = e(hU + H(c) Q_{\mathrm{ID}}, P_{\mathrm{pub}})$ 是否成立。若成立,接收签名;否则,拒绝。

4.2　何俊杰等人方案的安全分析

虽然文献[18]声称在随机预言模型下,证明提出的方案对自适应选择消息和身份攻击,是不可伪造的,将其安全性归约为计算 Diffie-Hellman 假设,但仍可以证明它是不安全的。

在部分盲签名方案中,允许签名人在签名中嵌入与用户协商好的公共信息 c。所谓窜改协商信息攻击是指签名请求者将原先协商好的信息 c 窜改为 $c_1 (c_1 \neq c)$,仍然可以使得签名通过验证。本文分析发现,该方案不可以抵抗窜改协商信息攻击。

下面假设在签名者不知情的情况下,用户 A 将信息 c 窜改为 $c_1 (c_1 \neq c)$,具体攻击步骤如下:

a)承诺。签名者首先随机选取 $k' \in Z_q^*$,计算 $U' = k'P$,将 U'发送给用户 A。

b)盲化。用户 A 随机选择 $\alpha, \beta \in Z_q^*$,计算 $U = \alpha U' + \beta P$, $h = H_2(\mathrm{ID}, m, U)$, $h^* = \frac{H_3(c)}{H_3(c_1)} h$, $h'^* = \alpha h^* \bmod q$,将 h'^* 发送给签名者 B。

c)盲签名。签名者 B 收到 h'^* 后,计算 $V'^* = h'^* k' P_{\mathrm{pub}} + H_3(c) S_{\mathrm{ID}}$,将 V'^* 发送给 A。

d)解盲。用户 A 计算 $V^* = \frac{H_3(c_1)}{H_3(c)}(V'^* + \beta h^* P_{\mathrm{pub}})$,得到

消息(m,c_1)的部分盲签名(U,V^*)。

下面证明$(\mathrm{ID},m,c_1,U,V^*)$是可以通过验证的:计算$Q_{\mathrm{ID}}=H_1(\mathrm{ID})$,$h=H_2(\mathrm{ID},m,U)$,验证等式:

$$e(V^*,P)=e(\frac{H_3(c_1)}{H_3(c)}(V'^*+\beta h^* P_{\mathrm{pub}}),P)=$$

$$e(\frac{H_3(c_1)}{H_3(c)}(\alpha h^* k' P_{\mathrm{pub}}+H_3(c)S_{\mathrm{ID}}+\beta h^* P_{\mathrm{pub}}),P)=$$

$$e(\frac{H_3(c_1)}{H_3(c)}(\alpha\frac{H_3(c)}{H_3(c_1)}hk' P_{\mathrm{pub}}+H_3(c)S_{\mathrm{ID}}+\beta\frac{H_3(c)}{H_3(c_1)}hP_{\mathrm{pub}}),P)=$$

$$e((\alpha hk' P_{\mathrm{pub}}+H_3(c_1)S_{\mathrm{ID}}+\beta hP_{\mathrm{pub}}),P)=$$

$$e((\alpha hk' P_{\mathrm{pub}}+\beta hP_{\mathrm{pub}}),P)e(H_3(c_1)S_{\mathrm{ID}},P)=$$

$$e((\alpha hk'+\beta h)P,P_{\mathrm{pub}})e(H_3(c_1)Q_{\mathrm{ID}},P_{\mathrm{pub}})=$$

$$e(hU+H_3(c_1)Q_{\mathrm{ID}},P_{\mathrm{pub}})$$

5 结束语

针对三个可证明安全的数字签名方案[6,11,18],本文指出李志敏等人提出的基于证书的数字方案不可以抵抗任意第三方的伪造攻击,黄茹芬等人提出的基于证书的盲签名方案不可以抵抗公钥替换攻击,何俊杰等人提出的部分盲签名方案不可以抵抗协商公共信息攻击。

由于随机预言模型下的安全性并不等同于标准模型下的安全性,研究者倾向认为标准模型更接近于现实模型,所以在标准模型下可证明安全同时尽可能少地运用双线性对的数字签名方案是下一步需要重点关注的一个研究课题。

参考文献:

[1] SHAMIR A. Identity-based cryptosystems and signature schemes [C] //Proc of CRYPTO'84. Berlin: Springer,1984:47-53.

[2] GENTRY C. Certificate-based encryption and the certificate revocation problem [C]//Lecture Notes in Computer Science, vol 2656. Berlin: Springer-Verlag, 2003:272-293.

[3] KANG B G, PARK J H, HAHN S G. A certificate-based signature scheme[C]//Lecture Notes in Computer Science, vol 2964. Berlin: Springer-Verlag,2004:99-111.

[4] WU Wei, MU Yi, SUSILO W, *et al*. Certificate-based signatures revisited [J]. Journal of Universal Computer Science, 2009, 15(8):1659-1684.

[5] 李继国,钱娜,黄欣沂,等. 基于证书强指定验证者签名方案[J].计算机学报,2012,35(8):1579-1587.

[6] 李志敏,徐馨,李存华. 高效的基于证书数字签名设计方案 [J]. 计算机应用研究,2012,29(4):1430-1433,1444.

[7] CHAUM D. Blind signature for untraceable payments [C] //Proc of Advances in Cryptology-CRYPTO. Berlin: Plenum Press, 1983: 199-233.

[8] 刘亚丽,殷新春,陈决伟. 基于 ELGAMAL 前向安全的盲签名方案 [J].通信学报,2007,28(8A):48-53.

[9] 邱钢,王宏,肖鸿 等. 两种前向安全盲签名体制的安全性分析 [J]. 西安电子科技大学学报,2010,37(1):107-111.

[10] 周萍,何大可. 高效无可信 PKG 的新型盲签名方案[J]. 计算机应用研究,2012,29(2):626-629.

[11] 黄如芬,农强,黄振杰. 一类可证安全的基于证书盲签名[J]. 计算机应用研究,2012,29(12):4622-4625,4630.

[12] ABE M, FUJISAKI E. How to date blind signatures [C] //Proc of International Conference on Theory and Applications of Cryptology and Information Security. Berlin: Springer-Verlag,1996:244-251.

[13] CHOW S S M, HUI L C K, YIU S M. Two improved partially blind signature schemes from bilinear pairings[C]//Proc of the 10th Australasian Conference on Information Security and Privacy. Berlin: Springer-Verlag,2005:316-328.

[14] 李明祥,李峰,王涛. 部分盲签名综述[J]. 计算机应用研究,2012,29(12):4437-4440.

[15] 崔巍,辛阳,胡程渝. 高效的基于身份的(受限)部分盲签名方案 [J]. 北京邮电大学学报,2008,31(4):53-57.

[16] 李明祥,赵秀明,王洪涛. 对一种部分盲签名方案的安全性分析与改进[J]. 计算机应用,2010,30(10):2687-2690.

[17] 何俊杰,孙芳,祁传达. 基于身份的部分盲签名方案的分析与改进[J]. 计算机应用,2013,33(3):762-765.

[18] 何俊杰,王娟,祁传达. 安全高效的基于身份的部分盲签名方案 [J]. 计算机应用,2012,32(5):1388-1391.

[19] SHIM K A. An ID-based aggregated signature scheme with constant pairing computation[J]. Journal of Systems and Software, 2010, 83(10):1873-1880.

(上接第 3748 页)

[5] Di RAIMONDO M, GENNARO R, KRAWCZYK H. Deniable authentication and key exchange[C]//Proc of the 13th ACM Conference on CCS. New York:ACM Press, 2006:400-409.

[6] Di RAIMONDO M, GENNARO R, NAOR M. New approaches for deniable authentication[J]. Journal of Cryptology, 2009, 22(4): 572-615.

[7] DODIS Y, KATZ J, SMITH A. Composability and on-line deniability of authentication[C]//Proc of the 6th Theory of Cryptography Conference. Berling: Springer-Verlag, 2009:146-162.

[8] NAOR M. Deniable ring authentication[C]//Proc of the 22nd Annual International Cryptology Conference on Advances in Cryptology. London: Springer-Verlag, 2002481-498.

[9] SUSILO W, MU Yi. Non-interactive deniable ring authentication [C]//Proc of ICISC[S.l.]:Springer, 2004:386-401.

[10] DOWSLEY R, HANAOKA G, IMAI H, *et al*. Round-optimal deniable ring authentication in the presence of big brother[C]//Proc of the 11th International Conference on Information Security Applications Berlin:Springer-Verlag, 2011:307-321.

[11] BONEH D, NAOR M. Timed commitment[C]//Proc of CRYPTO. [S.l.]: Springer, 2000:236-254.

[12] GARAY J A, POMERANCE C. Timed fair exchange of standard signatures[C]//Proc of FC[S.l.]: Springer, 2003:190-207.

[13] JIANG Shao-quan. Dwork-Naor ZAP and its application in deniable authentication, revisited[C]//Proc of the 6th International Conference on Information Security and Cryptology. Berlin: Springer-Verlag, 2011:443-454.

[14] JIANG Shaoquan. Timed encryption with application to deniable key exchange[C]//Proc of the 9th Annual International Conference on TAMC. Berlin:Spring-Verlag, 2012:248-259.