

# 具有强盲性的高效无证书盲签名方案

龚国昌\*, 石志寒

(空军工程大学 防空反导学院, 西安 710051)

(\*通信作者电子邮箱 ggc619@163.com)

**摘要:**针对无证书盲签名方案存在的效率低、不具备强盲性的缺点,提出了一种具有强盲性的高效无证书盲签名方案。该方案严格按照无证书盲签名的定义,将签名过程分成了系统建立、密钥生成、盲签名及签名验证四个阶段。同时,该方案基于椭圆曲线离散对数问题(ECDLP),引入三个随机盲化参数。性能分析结果表明,所提方案在随机预言模型下是安全的,具有高效性和强盲性。

**关键词:**无证书签名;盲签名;椭圆曲线离散对数问题;随机预言模型

**中图分类号:**TP309.7 **文献标志码:**A

## Strongly blind and efficient certificateless blind signature scheme

GONG Guochang\*, SHI Zhihan

(College of Air and Missile Defense, Air Force Engineering University, Xi'an Shaanxi 710051, China)

**Abstract:** Concerning that the existing schemes of certificateless signature are neither strongly blind nor efficient, a strongly blind and efficient scheme was proposed. The scheme was divided into four stages: setup, extract, sign and verify, in strict accordance with the definition of certificateless blind signature. Meanwhile, the scheme was based on Elliptic Curve Discrete Logarithm Problem (ECDLP), and introduced three random blind parameters. The results of performance analysis show that the proposed scheme is safe under the random oracle model, and they also show that the scheme is efficient and strongly blind.

**Key words:** certificateless signature; blind signature; Elliptic Curve Discrete Logarithm Problem (ECDLP); random oracle model

## 0 引言

无证书盲签名是通过无证书签名和盲签名结合而实现的,因此无证书盲签名方案不仅具有无需证书和密钥托管的特性,而且具有盲性。无证书盲签名的良好特性使其成为数字签名领域的研究热点。

对无证书盲签名的研究和改进,离不开对无证书签名和盲签名的深入研究。2003年,Al-Riyami等<sup>[1]</sup>提出了第一个无证书盲签名方案。随着研究的深入,一些无证书签名方案<sup>[2-5]</sup>相继被提出,但由于这些方案都是采用双线性对来进行构造,存在着效率不高的问题。文献[6]提出了一种无需双线性对的无证书签名方案,大大提高了运算效率,然而王怡等<sup>[7]</sup>指出其存在无法抵抗积极不诚实的恶意密钥生成中心(Key Generation Center, KGC)攻击问题,并给出了改进方案。盲签名由Chaum<sup>[8]</sup>首次提出,文献[9]指出,构造盲签名方案时,若采用三个随机盲化参数,则能得到强盲签名。文献[10]基于双线性对,采用两个随机盲化因子,提出了一种无证书盲签名方案,但方案的效率较低,且无法达到强盲性的要求。文献[11]提出了一种只需要一个双线性对的无证书盲签名方案,但方案也只采用了两个随机盲化因子。

本文首先给出了无证书盲签名的定义和安全模型,并在此基础上提出了一种不含双线性对的无证书盲签名方案。该方案避免了双线性对的使用,并且引入了三个随机盲化参数,具有高效性和强盲性。

## 1 预备知识

### 1.1 困难问题

椭圆曲线离散对数问题(Elliptic Curve Discrete Logarithm Problem, ECDLP):假设 $E(F_q)$ 为有限域 $F_q$ 上的一条椭圆曲线,对于任意两点 $P, Q \in E(F_q)$ ,如果存在正整数 $m$ ,使得 $Q = mP$ ,那么由 $P, Q$ 求 $m$ 的值即为椭圆曲线离散对数问题。

### 1.2 无证书盲签名的定义

一个无证书盲签名方案由以下四个算法组成。

1) 系统建立(Setup):是一个概率多项式时间算法,由KGC完成。输入参数 $k$ , KGC输出系统的主密钥 $s$ 和系统参数 $params$ 。

2) 密钥生成(Extract):是一个概率多项式时间算法,由签名者和KGC交互来完成。首先, KGC根据签名者身份ID,系统参数 $params$ 以及主密钥 $s$ ,生成签名者的部分私钥 $d_m$ ,并将 $d_m$ 秘密发送给签名者。签名者选取一个随机数 $s_m$ 作为自己

**收稿日期:**2014-01-02; **修回日期:**2014-02-21。 **基金项目:**国家自然科学基金资助项目(61272486); 中国博士后基金资助项目(2013M542331); 陕西省自然科学基金资助项目(2013JQ8035)。

**作者简介:**龚国昌(1991-),男,山东菏泽人,硕士研究生,主要研究方向:网络与信息安全; 石志寒(1965-),男,湖南张家界人,副教授,硕士,主要研究方向:智能信息处理。

的秘密值。最后,签名者根据  $d_{ID}, s_{ID}$  和  $params$ , 求出私钥  $sk_{ID}$  和公钥  $PK_{ID}$ 。

3) 盲签名 (Sign): 是一个概率多项式时间算法, 由签名者和用户交互来完成。算法可描述为  $v = \text{Sign}(ID, m, params, sk_{ID})$ , 具体包括承诺、消息盲化、签名和去盲化四个步骤。

4) 签名验证 (Verify): 是一个确定多项式时间算法, 由验证者完成。输入  $(v, ID, m, params, PK_{ID})$ , 输出对签名的验证结果 (正确或错误)。

### 1.3 无证书盲签名安全模型

如果一个无证书盲签名方案能够抵抗适应性选择消息攻击下的存在性伪造, 就称这个无证书盲签名是安全的。根据攻击者的能力不同, 本文将攻击者分为两类  $A_1, A_2$ , 其攻击能力描述如下:

1) 攻击者  $A_1$  无法获得主密钥, 无法得到目标实体的部分私钥, 但可以替换任何实体的公钥。

2) 攻击者  $A_2$  可以获取主密钥, 能够得到任何实体的部分私钥, 并且无法替换公钥。

## 2 无证书盲签名方案

1) 系统建立: 设  $E$  为安全的椭圆曲线,  $H: \{0, 1\}^* \times E \rightarrow \mathbf{Z}_n^*$  为一种哈希函数。KGC 选择随机数  $s \in \mathbf{Z}_n^*$ , 计算  $P_{\text{pub}} = sG$ , KGC 保存主密钥  $s$ , 公开系统参数  $params = \{E, n, G, P_{\text{pub}}\}$ 。

2) 密钥生成: KGC 随机选择  $r_{ID} \in \mathbf{Z}_n^*$ , 计算  $R_{ID} = r_{ID}G$ ,  $h_1 = H(ID \| R_{ID})$ ,  $d_{ID} = r_{ID} + h_1s$ , 将  $\{d_{ID}, R_{ID}\}$  秘密发送给签名者。签名者检验  $d_{ID}G = R_{ID} + H(ID \| R_{ID})P_{\text{pub}}$  是否成立, 成立则接受  $d_{ID}$  作为部分私钥。签名者随机选择  $s_{ID} \in \mathbf{Z}_n^*$  作为其秘密值。计算私钥  $sk_{ID} = d_{ID} + s_{ID}$ , 公钥  $PK_{ID} = s_{ID}G$ 。

3) 盲签名: 签名包括承诺、消息盲化、签名和去盲化四个步骤。

#### ①承诺。

签名者随机选择  $k_{ID} \in \mathbf{Z}_n^*$ , 计算  $U_{ID} = k_{ID}G$ , 将  $U_{ID}$  和  $R_{ID}$  发送给用户。

#### ②消息盲化。

用户随机选择  $a, b, c \in \mathbf{Z}_n^*$ ,  $U = aU_{ID} + bP_{ID} + cG$ , 其中  $P_{ID} = PK_{ID} + R_{ID} + H(ID \| R_{ID})P_{\text{pub}}$ 。计算  $h_2 = h(m \| U)$ ,  $h'_2 = b^{-1}(c - h_2)$ , 将  $h'_2$  发送给签名者。

#### ③签名。

签名者计算  $v' = k_{ID}^{-1}(h'_2 + sk_{ID})$ , 并将  $v'$  发送给用户。

#### ④去盲化。

$v = bv' + a$ , 请求者便得到签名者对  $m$  的盲签名  $(h_2, v)$ 。

#### 4) 签名验证。

验证者验证  $U$  与  $U'$  是否相等, 其中  $U' = vU_{ID} + h_2G$ 。若相等则签名合法。

## 3 方案的性能分析

### 3.1 正确性分析

方案具有正确性。

证明 由签名算法可知:

$$U' = vU_{ID} + h_2G = (bv' + a)U_{ID} + h_2G =$$

$$\begin{aligned} & aU_{ID} + bk_{ID}^{-1}(h'_2 + sk_{ID})U_{ID} + h_2G = \\ & aU_{ID} + b(h'_2 + sk_{ID})G + h_2G = \\ & aU_{ID} + b(d_{ID} + s_{ID})G + (bh'_2 + h_2)G = \\ & aU_{ID} + b(PK_{ID} + R_{ID} + H(ID \| R_{ID})P_{\text{pub}}) + \\ & (c - h_2 + h_2)G = aU_{ID} + bP_{ID} + cG \end{aligned}$$

所以,  $U = U'$ , 新方案具有正确性。

### 3.2 强盲性分析

方案具有强盲性。

证明 假设签名者保留了签名的中间变量  $\{k_{ID}, U_{ID}, h'_2, v'\}$ 。如果签名者无法从中获取待签消息, 并且无法从  $\{h'_2, v'\}$  追踪到  $\{h_2, v\}$ , 则称签名具有强盲性。

在本方案中, 具有以下等式:

$$h'_2 = b^{-1}(c - h_2) \quad (1)$$

$$v' = k_{ID}^{-1}(h'_2 + sk_{ID}) \quad (2)$$

$$v = bv' + a \quad (3)$$

1) 盲性。  $h_2$  经过式 (1) 的盲化后得到  $h'_2$ , 保证了消息的盲性。

2) 不可链接性。签名者若要追踪签名, 则需要求出三个随机数  $a, b, c$  的值。签名者无法根据式 (1) ~ (3) 求出  $a, b, c$  的值, 因此签名者无法追踪签名, 方案具有不可链接性。

方案满足盲性和不可链接性, 因此具有强盲性。

### 3.3 安全性分析

定理 1 在 ECDLP 和随机预言模型下, 方案能抵抗攻击者  $A_1$  适应性选择消息攻击下的存在性伪造。

证明  $A_1$  与挑战者  $C$  进行一个交互的攻击游戏 Game 1, 如果  $A_1$  能够在多项式时间内成功伪造出签名者  $T$  对消息  $m_T$  的签名, 则  $A_1$  赢得游戏。

Game 1 描述如下:

初始化:  $C$  运行系统建立算法, 将系统参数发送给  $A_1$ , 模拟随机预言机回答  $A_1$  的如下提问。

$h_1$  查询:  $C$  管理列表  $l_{h_1} = \{ID_i, R_i, h_{1i}\}$ , 当  $h_1$  查询的  $\{ID_i, R_i\}$  在  $l_{h_1}$  中, 则返回  $\{ID_i, R_i, h_{1i}\}$ ; 如果  $l_{h_1}$  中不存在  $\{ID_i, R_i\}$ , 则  $C$  随机选择  $h_{1i} \in \mathbf{Z}_n^*$ , 将  $\{ID_i, R_i, h_{1i}\}$  添加到  $l_{h_1}$  中并返回给  $A_1$ 。

部分私钥查询:  $C$  管理列表  $l_p = \{ID_i, d_i, PK_i\}$ , 当部分私钥查询的  $ID_i = ID_T$ , 则  $C$  中止模拟 (事件  $E1$ )。当  $ID_i \neq ID_T$ , 如果  $ID_i$  在  $l_p$  中, 则返回  $\{ID_i, d_i\}$ ; 如果  $l_p$  中不存在  $ID_i$ , 则模拟部分私钥生成算法, 生成  $d_i$ , 求出  $PK_i = d_iG$ , 将  $\{ID_i, d_i, PK_i\}$  添加到  $l_p$  中, 并将  $\{ID_i, d_i\}$  返回给  $A_1$ 。

公钥查询: 如果公钥查询的  $ID_i$  在  $l_p$  中时, 则返回  $\{ID_i, PK_i\}$ ; 如果  $l_p$  中不存在  $ID_i$ , 则模拟部分私钥生成算法生成  $d_i$ , 计算  $PK_i = d_iG$ , 将  $\{ID_i, d_i, PK_i\}$  添加到  $l_p$  中, 并将  $\{ID_i, PK_i\}$  返回给  $A_1$ 。

公钥替换查询:  $C$  在  $l_p$  中查找需要替换的  $ID_i$ , 将  $PK'_i$  替换原来的  $PK_i$ 。

$h_2$  查询:  $C$  管理列表  $l_{h_2} = \{m_i, U, h_{2i}\}$ ,  $A_1$  将  $\{m_i, U\}$  发送给  $C$ , 如果  $\{m_i, U\}$  已经在  $l_{h_2}$  中, 则返回  $\{m_i, U, h_{2i}\}$ ; 否则将  $C$  随机生成  $h_{2i} \in \mathbf{Z}_n^*$ , 将  $\{m_i, U, h_{2i}\}$  添加到  $l_{h_2}$  中并返回给  $A_1$ 。

签名查询:  $C$  管理列表  $l_s = \{ID_i, m_i, v_i\}$ ,  $A_1$  将需要签名

的  $ID_i, m_i$  发送给  $C$ , 当  $ID_i = ID_T$  且  $m_i = m_T$  时 (事件  $E2$ ), 则  $C$  模拟中止。否则,  $C$  模拟签名算法生成  $S_i$ , 将  $\{ID_i, m_i, v_i\}$  添加到  $l_s$  并发送给  $A_1$ 。

伪造签名: 假设  $A_1$  经过  $q_{h_1}$  次  $h_1$  查询,  $q_p$  次部分私钥查询,  $q_s$  次签名查询, 及多项次其他查询, 以概率  $\varepsilon$  成功伪造  $ID_T$  对  $m_T$  的合法签名  $(h_{2T}, v_T)$ 。根据分叉引理<sup>[12]</sup>, 重复上述查询, 但采用不同的哈希值, 得到  $(h'_{2T}, v'_T)$ 。

由签名验证等式  $vU_{ID} + h_2G = aU_{ID} + bP_{ID} + cG$  得

$$vk_{ID} + h_2 = ak_{ID} + bsk_{ID} + c \quad (4)$$

将  $(h_{2T}, v_T), (h'_{2T}, v'_T)$  代入式(4)中, 得

$$v_T k_{ID} + h_{2T} = ak_{ID} + bsk_{ID} + c \quad (5)$$

$$v'_T k_{ID} + h'_{2T} = ak_{ID} + bsk_{ID} + c \quad (6)$$

求解式(5)、式(6)组成的二元一次方程组, 即可求出  $k_{ID}, sk_{ID}$ 。又因  $U_{ID} = k_{ID}G, P_{ID} = sk_{ID}G = PK_{ID} + R_{ID} + H(ID \parallel R_{ID})P_{Pub}$  均已知, 故挑战者  $C$  利用  $A_1$  的能力成功求解出 ECDLP 一个实例。

概率分析: 已知  $\Pr[\overline{E1}] \geq (1 - 1/q_{h_1})^{q_p}, \Pr[\overline{E2}] \geq (1 - 1/q_{h_1})^{q_s}, \Pr[A_1 | \overline{E1} \wedge \overline{E2}] = \varepsilon$ , 求出  $\varepsilon' = \Pr[A_1 \wedge \overline{E1} \wedge \overline{E2}] \geq (1 - 1/q_{h_1})^{q_p+q_s}\varepsilon$ 。所以挑战者  $C$  能够利用攻击者  $A_1$  在多项式时间内至少以概率  $(1 - 1/q_{h_1})^{q_p+q_s}\varepsilon$  解决了 ECDLP 的一个实例, 这与 ECDLP 的困难性相违背, 故新方案能抵抗攻击者  $A_1$  适应性选择消息攻击下的存在性伪造。

**定理 2** 在 ECDLP 和随机预言模型下, 方案能抵抗攻击者  $A_2$  适应性选择消息攻击下的存在性伪造。

证明  $A_2$  与挑战者  $C$  进行一个交互的攻击游戏 Game 2, 如果  $A_2$  能够在多项式时间内成功伪造出签名者  $T$  对消息  $m_T$  的签名, 则  $A_2$  赢得游戏。

Game 2 描述如下:

初始化:  $C$  将系统参数和系统主密钥  $s$  发送给  $A_2$ ,  $C$  模拟随机预言机回答  $A_2$  的如下提问。

$h_1$  查询、 $h_2$  查询仿照 Game 1。

部分私钥查询:  $C$  管理列表  $l_p = \{ID_i, d_i, PK_i\}$ , 当部分私钥查询  $ID_i$  在  $l_p$  中, 则返回  $\{ID_i, d_i\}$ ; 如果  $l_p$  中不存在  $ID_i$ , 则模拟部分私钥生成算法, 生成  $d_i$ , 求出  $PK_i = d_iG$ , 将  $\{ID_i, d_i, PK_i\}$  添加到  $l_p$  中, 并将  $\{ID_i, d_i\}$  返回给  $A_2$ 。

公钥查询: 如果公钥查询的  $ID_i$  在  $l_p$  中时, 则返回  $\{ID_i, PK_i\}$ ; 如果  $l_p$  中不存在  $ID_i$ , 则模拟部分私钥生成算法生成  $d_i$ , 计算  $PK_i = d_iG$ , 将  $\{ID_i, d_i, PK_i\}$  添加到  $l_p$  中, 并将  $\{ID_i, PK_i\}$  返回给  $A_2$ 。

签名查询:  $C$  管理列表  $l_s = \{ID_i, m_i, v_i\}$ ,  $A_2$  将需要签名的  $ID_i, m_i$  发送给  $C$ , 当  $ID_i = ID_T$  且  $m_i = m_T$  时 (事件  $E1$ ), 则  $C$  模拟中止。否则,  $C$  模拟签名算法生成  $S_i$ , 将  $\{ID_i, m_i, v_i\}$  添加到  $l_s$  并发送给  $A_2$ 。

伪造签名: 假设  $A_2$  经过  $q_{h_1}$  次  $h_1$  查询,  $q_s$  次签名查询, 及多项次其他查询, 以概率  $\varepsilon$  成功伪造  $ID_T$  对  $m_T$  的合法签名  $(h_{2T}, v_T)$ 。根据分叉引理<sup>[12]</sup>, 重复上述查询, 但采用不同的哈希值, 得到  $(h'_{2T}, v'_T)$ 。

将  $(h_{2T}, v_T), (h'_{2T}, v'_T)$  代入式(4)中, 得

$$v_T k_{ID} + h_{2T} = ak_{ID} + bsk_{ID} + c \quad (7)$$

$$v'_T k_{ID} + h'_{2T} = ak_{ID} + bsk_{ID} + c \quad (8)$$

求解式(7)、式(8)组成的二元一次方程组, 即可求出  $k_{ID}, sk_{ID}$ 。又因  $U_{ID} = k_{ID}G, P_{ID} = sk_{ID}G = PK_{ID} + R_{ID} + H(ID \parallel R_{ID})P_{Pub}$  均已知, 故挑战者  $C$  利用  $A_2$  的能力成功求解出 ECDLP 一个实例。

概率分析: 已知  $\Pr[\overline{E1}] \geq (1 - 1/q_{h_1})^{q_s}$ , 已知  $\Pr = [A_2 | \overline{E1}] = \varepsilon$ , 所以  $\varepsilon' = \Pr[A_2 \wedge \overline{E1}] \geq (1 - 1/q_{h_1})^{q_s}\varepsilon$ , 挑战者  $C$  能够利用攻击者  $A_2$  在多项式时间内至少以概率  $(1 - 1/q_{h_1})^{q_s}\varepsilon$  解决了 ECDLP 的一个实例, 这与 ECDLP 的困难性相违背, 故新方案能抵抗攻击者  $A_2$  适应性选择消息攻击下的存在性伪造。

### 3.4 效率分析

表 1 是本文方案与文献[10]、[11]中的方案计算量的对比, 其中  $P$  表示双线性对运算,  $M$  表示  $G_1$  中的点乘运算,  $E$  表示  $G_2$  中的幂运算。已知  $M$  的计算量比  $P$  小得多, 而与  $E$  相当, 故在签名阶段和验证阶段, 本文方案所需的计算量均小于文献[10]、文献[11]中的方案。

表 1 不同方案的计算量比较

方案	签名阶段	验证阶段
文献[10]方案	5M	2P+2M
文献[11]方案	2M+3E	P+M+E
本文方案	4M	2M

## 4 结语

针对现有的无证书盲签名方案在效率上和强盲性上存在的问题, 提出了一种具有强盲性的无需双线性对的无证书盲签名方案。同时, 给出了新方案在随机预言模型下的安全性证明, 指出新方案的安全性是基于椭圆曲线离散对数问题的困难性。与现有方案相比, 新方案不仅避免了双线性对运算, 大大提高了无证书盲签名的效率, 而且通过引入三个随机盲化参数, 达到了强盲性的要求。

### 参考文献:

- [1] AL-RIYAMI S, PATERSON K. Certificateless public key cryptography[C]// Cryptology - Asiacrypt 2003. Berlin: Springer-Verlag, 2003: 452-473.
- [2] HUANG X, MU Y, SUSILO W, et al. Certificateless signature revisited[C]// Proceedings of the 12nd Australian Conference on Information Security and Privacy, LNCS 4586. Berlin: Springer-Verlag, 2007: 308-322.
- [3] ZHANG L, ZHANG F T, ZHANG F G. New efficient certificateless signature scheme[C]// Proceedings of the EUC Workshops 2007. Berlin: Springer-Verlag, 2007: 692-703.
- [4] YUAN Y, LI D, TIAN L, et al. Certificateless signature scheme without random oracles[C]// Proceedings of the ISA 2009. Berlin: Springer-Verlag, 2009: 31-40.
- [5] YUAN H, ZHANG F, HUANG X, et al. Certificateless threshold signature scheme from bilinear maps[J]. Information Sciences, 2010, 180(23): 4714-4728.
- [6] WANG S, LIU W, XIE Q. Certificateless signature scheme without bilinear pairings[J]. Journal on Communications, 2012, 33(4): 93-98. (王圣宝, 刘文浩, 谢琪. 无双线性配对的无证书签名方案[J]. 通信学报, 2012, 33(4): 93-98.) (下转第 1901 页)

部分,第三方可以通过用户的手机信息确认用户的合法性,同时却不能够获取用户转发给移动云服务的私人信息。第三方协议与 Opaak 协议<sup>[3]</sup>相比较,虽然都把接入控制端作为半可信状态,但本文除了使第三方不参与用户登录使用云服务过程,在用户注册以及共享资源环节,也不让用户信息暴露给接入控制端。

在用户的个人证书验证方面,考虑到用户丢失证书的安全风险。在 Opaak 身份证书协议的基础上增加了身份证书绑定用户手机的功能。这里对身份密钥的顺序拆分既降低了用户身份证书被盗用的概率,又避免了因为使用复杂的加密方法增加客户端计算量的问题(具体如式(7)所示)。

## 5 结语

本文提出了一种移动云环境下的安全隐私保护机制,可以在保护用户隐私的前提下,保证用户合法地使用移动云存储与共享服务。协议中用半可信的第三方给用户身份提供证明,用户凭借身份证书在移动云服务端进行虚拟账户的注册。在三方协议中,用户只透露私人信息中的手机信息给接入控制端,第三方通过手机信息验证用户的合法身份。为了防止第三方获取用户隐私和移动云服务的商业机密,之后将不再参与用户与云服务间的密钥验证过程。用户身份证书注册和云服务账户的验证过程中本文均采用零知识验证算法,在保证用户密钥安全的同时节省计算开销和密钥传递时间。在密钥处理上,本文的身份密钥和共享密钥都是使用绑定用户身份信息的方法,防止攻击者盗用用户信息,同时也防止用户把权限外借给别人使用。同时验证了第三方的半可信状态以及身份密钥与共享密钥的安全性。

### 参考文献:

- [1] LING C, SU W, MENG K, *et al.* cloud computing security: Architecture, mechanism and modeling[J]. Chinese Journal of Computers, 2013, 36(9): 1765–1784. (林闯, 苏文博, 孟坤, 等. 云计算安全: 架构、机制与模型评价[J]. 计算机学报, 2013, 36(9): 1765–1784.)
- [2] OpenID[EB/OL].[2013-10-20]. <http://openid.net>.
- [3] MAGANIS G, SHI E, CHEN H, *et al.* Opaak: using mobile phones to limit anonymous identities online[C]// Proceedings of the 10th International Conference on Mobile Systems, Applications, and Services. New York: ACM, 2012: 295–308.
- [4] WANG Z, SHA K, LYU W. Slight homomorphic signature for access controlling in cloud computing[J]. Wireless Personal Communications, 2013, 73(1): 1–11.
- [5] CAMENISCH J, LYSYANSKAYA A. A signature scheme with efficient protocols[M]. Berlin: Springer, 2003: 268–289.
- [6] CAMENISCH J, STADLER M. Efficient group signature schemes for large groups[C]// Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology. London: Springer-Verlag, 1997: 410–424.
- [7] WANG C, CHOW S S M, WANG Q, *et al.* Privacy-preserving public auditing for secure cloud storage[J]. IEEE Transactions on Computers, 2013, 62(2): 362–375.
- [8] WANG C, CAO N, REN K, *et al.* Enabling secure and efficient ranked keyword search over outsourced cloud data[J]. IEEE Transactions on Parallel and Distributed Systems, 2012, 23(8): 1467–1479.
- [9] SUNDARESWARAN S, SQUICCIARINI A, LIN D. Ensuring distributed accountability for data sharing in the cloud[J]. IEEE Transactions on Dependable and Secure Computing, 2012, 9(4): 556–568.
- [10] LIU X, ZHANG Y, WANG B, *et al.* Mona: secure multi-owner data sharing for dynamic groups in the cloud[J]. IEEE Transactions on Parallel and Distributed Systems, 2013, 24(6): 1182–1191.
- [11] BOHLI J, GRUSCHKA N, JENSEN M, *et al.* Security and privacy enhancing multi-cloud architectures[J]. IEEE Transactions on Dependable and Secure Computing, 2013, 10(4): 212–224.
- [12] ZHU Y, XU R, TAKAGI T. Secure k-NN computation on encrypted cloud data without sharing key with query users[C]// Proceedings of the 2013 International Workshop on Security in Cloud Computing. New York: ACM, 2013: 55–60.
- [13] REN K, WANG C, WANG Q. Toward secure and effective data utilization in public cloud[J]. IEEE Networks, 2012, 26(6): 69–74.
- [14] WANG C, WANG Q, REN K, *et al.* Toward secure and dependable storage services in cloud computing[J]. IEEE Transactions on Services Computing, 2012, 5(2): 220–232.
- [7] WANG Y, DU W. Security analysis and improvement of certificateless signature scheme without bilinear pairing[J]. Journal of Computer Applications, 2013, 33(8): 2250–2252. (王怡, 杜伟章. 无双线性对的无证书签名方案的分析和改进[J]. 计算机应用, 2013, 33(8): 2250–2252.)
- [8] CHAUM D. Blind signatures for untraceable payments [C]// Proceedings of Crypto83. Heidelberg: Springer-Verlag, 1983: 199–203.
- [9] YAO Y, ZHU H, CHEN K. Generalized ElGamal type blind signature based on affine transform[J]. Acta Electronica Sinica, 2000, 28(7): 128–129. (姚亦峰, 朱华飞, 陈抗生. 基于二元仿射变换的广义 ElGamal 型盲签名方案[J]. 电子学报, 2000, 28(7): 128–129.)
- [10] SU W, ZHANG Y, ZHANG X, *et al.* Certificateless blind signature scheme[J]. Journal of University of Electronic Science and Technology of China, 2009, 38(4): 533–536. (苏万力, 张跃宇, 张晓红, 等. 无证书盲签名方案[J]. 电子科技大学学报, 2009, 38(4): 533–536.)
- [11] YANG X, LIANG Z, GUO Y, *et al.* An efficient certificateless blind signature scheme[J]. Journal of Nanjing University of Posts and Telecommunications: Natural Science Edition, 2009, 29(3): 37–42. (杨晓元, 梁中银, 郭耀, 等. 一个高效的无证书盲签名方案[J]. 南京邮电大学学报: 自然科学版, 2009, 29(3): 37–42.)
- [12] POINTCHEVAL D, STEM J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3): 361–396.

(上接第 1892 页)