

文章编号:1001-9081(2014)08-2342-03

doi:10.11772/j.issn.1001-9081.2014.08.2342

无证书签名方案的安全性分析与改进

樊爱宛*, 申远, 赵伟艇

(平顶山学院 软件学院, 河南 平顶山 467002)

(*通信作者电子邮箱 faw_1978@163.com)

摘要:针对王怡等(王怡, 杜伟章. 无双线性对的无证书签名方案的分析及改进. 计算机应用, 2013, 33(8): 2250–2252)提出的无双线性对运算的无证书签名方案, 指出该方案无法抵抗伪造性攻击, 并提出改进方案。改进方案加强了签名算法中参数的关联程度, 以抵抗伪造性攻击。安全性分析结果表明, 在随机预言机模型下, 新方案对于自适应选择消息和身份攻击是存在性不可伪造的。改进方案避开双线性对和逆运算, 效率优于已有方案。

关键词:无证书签名; 双线性对; 离散对数问题; 随机预言机模型

中图分类号: TP309.7 文献标志码:A

Security analysis and improvement of certificateless signature scheme

FAN Aiwan*, SHEN Yuan, ZHAO Weiting

(Software School, Pingdingshan University, Pingdingshan Henan 467002, China)

Abstract: By analyzing the security of a certificateless signature scheme without bilinear pairing proposed by Wang Y, et al. (WANG Y, DU W. Security analysis and improvement of certificateless signature scheme without bilinear pairing. Journal of Computer Applications, 2013, 33(8): 2250–2252), the result that the scheme can not resist forgery attack was pointed out and an improved scheme was proposed. The improved scheme enhanced the relationship of parameters in signature algorithm to resist forgery attack. The results of security analysis show that the improved scheme is proved to be existentially unforgeable against adaptive chosen message and identity attacks in random oracle model. The improved scheme is more efficient than the existing schemes for avoiding bilinear pairings and inverse operation.

Key words: certificateless signature; bilinear pairing; discrete logarithm problem; Random Oracle Model (ROM)

0 引言

为解决公钥的证书管理和密钥托管问题, Al-Riyami 等^[1]于 2003 年提出了无证书的密码系统。该系统利用密钥生成中心(Key Generation Center, KGC)产生用户的部分私钥与用户随机选择的秘密值, 共同组成用户公钥对与私钥对。由于无证书签名系统的强应用性, 大量无证书签名方案被相继提出^[2–5]。但是, 大部分方案都存在两个缺陷: 1) 以 KGC 信任诚实为前提, 不能抵抗公钥替换攻击; 2) 以双线性对为计算方式, 签名计算效率偏低。

在保证签名安全强度的基础上, 提高签名计算效率, 是目前无证书签名方案研究的重点。2004 年, Huang 等^[6]第一次提出无双线性对的无证书签名方案。然而, Hu 等^[7]指出该方案是无法抵抗公钥替换攻击。2011 年, 张燕燕等^[8]给出了一个无双线性对计算的无证书签名方案。然而, 杨波等^[9]证明了该方案无法抵抗公钥替换攻击。2012 年, 王圣宝等^[10]提出了一个不使用双线性对的无证书签名方案, 虽然运算效率得到了很大的提高, 但是王怡等^[11]在 2013 年指出该方案的安全性是以 KGC 完全可信为基础的, 具有一定的安全局限性, 并设计了改进方案, 以下简称 WD(Wang-Du) 方案。

本文对 WD 方案进行了安全性分析, 发现该方案虽然提高了计算效率, 但是无法抵抗伪造攻击。本文在此基础上给

出了一个改进方案, 安全性分析结果表明在随机预言机模型(Random Oracle Model, ROM)下, 改进方案对自适应选择消息和身份攻击是存在性不可伪造的。

1 预备知识

假设 G 是一个阶为素数 q 的循环群, P 是它的一个生成元。本文所提出的签名方案基于以下数学难解问题。

定义 1 椭圆曲线离散对数问题(Elliptic Curve Discrete Logarithm Problem, ECDLP)。任取 $Q \in G$, 求 $n \in \mathbb{Z}_q^*$, 使其能够满足 $Q = nP$ 。

定义 2 椭圆曲线 Diffie-Hellman 问题(Curve Discrete Logarithm Problem, CDHP)。已知 $aP \in G, bP \in G$, 其中 $a \in \mathbb{Z}_q^*, b \in \mathbb{Z}_q^*$ 且 a 和 b 未知, 求 $abP \in G$ 。

2 WD 无证书签名方案

1) 系统参数生成。输入一个安全参数 k , KGC 选定系统参数 $params = \{q, FR, a, b, P, H_1, H_2, H_3, P_{pub}\}$ 。其中: F_q 为有限域; 整数 $q (0 < q < 2^k)$ 为大素数, 是所选有限域的阶; FR 是有限域 F_q 中元素的表示; 椭圆曲线的两个系数 $a, b \in F_q$, 构建椭圆曲线 $E: y^2 = x^3 + ax + b$; G 是一个阶为素数 q 的循环群, 该群的元素是由 E 坐标点和无穷远点构成; P 是 G 的一个生成元; H_1, H_2 和 H_3 是三个单向哈希函数, 能够保证信息的

收稿日期:2014-02-18;修回日期:2014-03-26。基金项目:河南省高校青年骨干教师资助计划项目(2013190);河南省教育厅科学技术研究重点项目(14B520039);2014 年河南省科技计划项目(142102210224)。

作者简介:樊爱宛(1978-),男,河南内乡人,副教授,硕士,主要研究方向:信息安全、智能算法; 申远(1983-),男,河南平顶山人,讲师,硕士,主要研究方向:信息安全; 赵伟艇(1966-),男,河南宝丰人,教授,主要研究方向:信息安全、计算机网络。

完整性,其中 $H_1: \{0,1\}^* \times G^2 \rightarrow \mathbf{Z}_q^*$, $H_2: \{0,1\}^* \rightarrow \mathbf{Z}_q^*$, $H_3: G \rightarrow \mathbf{Z}_q^*$ 。在 \mathbf{Z}_q^* 中随机选取系统主密钥 s , 记 $P_{\text{pub}} = sP$ 。选取系统主私钥 $s \in \mathbf{Z}_q^*$, 系统公钥 $P_{\text{pub}} = sP$ 。

2) 设置秘密值。输入系统参数 $params$ 和用户的身份标识 ID 。用户随机选取 $z_{ID} \in \mathbf{Z}_q^*$, 计算 $Z_{ID} = z_{ID}P$; 将 Z_{ID} 和 ID 发送给 KGC。

3) 部分私钥生成。KGC 利用用户的身份标识 ID 、系统参数 $params$ 和主密钥 s 生成用户部分私钥。输入用户的身份标识 ID 、系统参数 $params$ 和主密钥 s , KGC 为用户生成部分私钥。KGC 收到 Z_{ID} 和 ID 后, 随机选取 $r_{ID} \in \mathbf{Z}_q^*$; KGC 计算 $R_{ID} = r_{ID}P$; 计算 $D_{ID} = r_{ID} + H_1(ID, R_{ID}, Z_{ID})s + H_3(z_{ID})$; KGC 将 (R_{ID}, D_{ID}) 通过公开信道发送给用户。

4) 部分私钥验证。用户利用自己输入用户的身份标识 ID 、系统参数 $params$ 、 R_{ID} 和 D_{ID} , 验证部分私钥是否是 KGC 生成。用户计算等式 $D_{ID}P = R_{ID} + H_1(ID, R_{ID}, Z_{ID})P_{\text{pub}} + H_3(z_{ID}P_{\text{pub}})$ 是否成立。若成立, 则计算 $d_{ID} = D_{ID} - H_3(z_{ID}P_{\text{pub}})$ 。

设置公钥 用户设置其公钥为 $PK_{ID} = (Z_{ID}, R_{ID})$ 。

设置私钥 用户设置其私钥为 $SK_{ID} = (z_{ID}, d_{ID})$ 。

签名 当输入一个消息 $M \in \mathbf{Z}_q^*$, 用户按以下方式对消息 M 进行签名:

- 1) 选取 $k(k \in \mathbf{Z}_q^*)$, 计算 $K = kP$;
- 2) 计算 $h = H_2(ID, M, Z_{ID}, R_{ID}, K)$;
- 3) 计算 $v = (kh + z_{ID})/(z_{ID}h + d_{ID})$;
- 4) 发送消息和签名结果 (K, h, v) 。

验证 验证者按如下方式验证身份为 ID 的用户对消息 M 的签名有效性:

- 1) 计算 $h_1 = H_1(ID, R_{ID}, Z_{ID})$ 。
- 2) 判断 $v(hZ_{ID} + R_{ID} + h_1P_{\text{pub}}) = hK + Z_{ID}$ 等式是否成立。

若成立则输出 1; 否则输出 0。

3 WD 无证书签名方案的安全性分析

文献[11]指出, WD 方案可以抵抗积极不诚实的 KGC 攻击, 即攻击敌手无法伪造出有效密钥冒充用户签名。但实际上, WD 方案并没有满足不可伪造性。敌手 A 只需伪造 (K, h, v) , 使得验证者通过 $v(hZ_{ID} + R_{ID} + h_1P_{\text{pub}}) = hK + Z_{ID}$ 等式的判断即可。具体攻击如下:

- 1) 敌手 A 首先伪造 $v' \in \mathbf{Z}_q^*, h' \in \mathbf{Z}_q^*$, 计算 $h_1 = H_1(ID, R_{ID}, Z_{ID})$ 。
- 2) 然后根据 $v'(h'Z_{ID} + R_{ID} + h_1P_{\text{pub}}) = h'K' + Z_{ID}$ 等式, 计算 $K' = h'^{-1}v'(h'Z_{ID} + R_{ID} + h_1P_{\text{pub}}) - h'^{-1}Z_{ID}$ 。
- 3) 输出伪造签名 (K', h', v') 。

以上敌手 A 伪造的签名能够通过 $v(hZ_{ID} + R_{ID} + h_1P_{\text{pub}}) = hK + Z_{ID}$ 等式的判断, 具体证明如下:

$$\begin{aligned} h'K' + Z_{ID} &= h'(h'^{-1}v'(h'Z_{ID} + R_{ID} + h_1P_{\text{pub}}) - h'^{-1}Z_{ID}) + \\ Z_{ID} &= v'h'Z_{ID} + v'R_{ID} + v'h_1P_{\text{pub}} - Z_{ID} + Z_{ID} = \\ h'v'Z_{ID} + v'R_{ID} + v'h_1P_{\text{pub}} &= v'(h'Z_{ID} + R_{ID} + h_1P_{\text{pub}}) \end{aligned}$$

由上面证明可知, 伪造的签名可以满足签名验证式, 即伪造的签名是有效的。

在无证书数字签名伪造性攻击中, 敌手 A 攻击成功的原因是: 伪造签名者可以根据验证算法构建虚假签名算法, 替代原有签名算法。验证者利用签名者传送过来的签名结果 (K, h, v) 和公钥 P_{pub} 进行签名验证。在验证等式 $v(hZ_{ID} + R_{ID} + h_1P_{\text{pub}}) = hK + Z_{ID}$ 中, Z_{ID} 、 R_{ID} 和 P_{pub} 是公开的参数, 无法伪造。

造, 仅有 K 、 h 、 v 三个可伪造的参数。由于 h 并非验证者通过公开的参数产生的, 导致 h 和 K 没有任何关联, 敌手 A 可先伪造整数 h 、 v , 最后根据等式伪造 K 。

即使 h 是经验者通过公开的参数 $(ID, M, Z_{ID}, R_{ID}, K)$ 产生的, 从而构建了 h 和 K 之间的关联, 但是 WD 方案仍不能抵挡伪造性攻击。具体攻击如下:

- 1) 敌手 A 首先计算 $h_1 = H_1(ID, R_{ID}, Z_{ID})$;
- 2) 然后计算 $K' = -R_{ID} - h_1P_{\text{pub}}$, $h' = H_2(ID, M, Z_{ID}, R_{ID}, K')$;
- 3) 根据 $v'(h'Z_{ID} + R_{ID} + h_1P_{\text{pub}}) = h'K' + Z_{ID}$ 等式, 计算 $v' = -h'$;
- 4) 输出伪造签名 (K', h', v') 。

以上敌手 A 伪造的签名仍然能够通过 $v(hZ_{ID} + R_{ID} + h_1P_{\text{pub}}) = hK + Z_{ID}$ 等式的判断, 具体证明如下:

$$\begin{aligned} v'(h'Z_{ID} + R_{ID} + h_1P_{\text{pub}}) &= -h'(h'Z_{ID} + R_{ID} + h_1P_{\text{pub}}) = \\ Z_{ID} + h'(-R_{ID} - h_1P_{\text{pub}}) &= Z_{ID} + h'K' \end{aligned}$$

由以上两种攻击可知, WD 方案虽然改进了用户密钥的生成方式, 使得 KGC 生成部分私钥受到用户的约束, 积极不诚实的 KGC 无法伪造出有效的用户密钥, 但是方案设计的签名与验证算法是无法抵挡伪造性攻击。

4 改进方案及其安全性分析

4.1 改进方案

系统参数生成、设置秘密值、部分私钥生成、部分私钥验证、设置公钥和设置私钥过程与 WD 方案相同。

签名 当输入一个消息 $M \in \mathbf{Z}_q^*$, 用户按以下方式对消息 M 进行签名:

- 1) 选取 $k(k \in \mathbf{Z}_q^*)$, 计算 $K = kP$;
- 2) 计算 $h = H_2(ID, M, Z_{ID}, R_{ID}, K)$;
- 3) 计算 $v = (k + d_{ID} + hz_{ID}) \bmod q$;
- 4) 发送消息和签名结果 (M, K, v) 。

验证 验证者按如下方式验证身份为 ID 的用户对消息 M 的签名有效性:

- 1) 计算 $h_1 = H_1(ID, R_{ID}, Z_{ID})$;
- 2) 计算 $U = vP; U' = R_{ID} + h_1P_{\text{pub}} + hZ_{ID}$ 。
- 3) 判断 $U = K + U'$ 等式是否成立。若成立则输出 1; 否则输出 0。

4.2 改进方案的安全性分析

4.2.1 正确性

改进方案的签名及验证算法是正确的。根据改进方案中的签名验证等式进行算法正确性验证, 证明如下:

$$U = vP = ((k + d_{ID} + hz_{ID}) \bmod q)P = K + R_{ID} + h_1P_{\text{pub}} + hZ_{ID} = K + U' \quad (1)$$

4.2.2 不可伪造性

改进方案在自适应选择消息攻击下是存在性不可伪造的。下面在随机预言机模型下进行抗伪造性的证明。

定理1 在随机预言机模型下, 假设 A 为恶意的 KGC, 在多项式时间内, 至多做了 q_{H_1} 次 H_1 询问, q_{H_2} 次 H_2 询问, q_z 次秘密值询问和 q_v 次签名询问后, 以不可忽略的概率 ϵ 攻破本文改进方案, 那么存在一个算法 X , 在多项式时间内以 $\epsilon/(q_{H_1}q_{H_2})$ 的优势成功解决 ECDLP。

证明 令 X 是加法循环群 G 上的 ECDLP 解决算法, 给定一个 ECDLP 的随机实例 $(P, Y = aP)$, X 的目标是利用 A 的攻

击程序计算出 a 。

1) 系统参数生成。 X 选定系统参数 $D = \{q, FR, a, b, P, H_1, H_2, P_{pub}\}$ 及公钥 (Z_{ID}, R_{ID}) 发送给 A 。

2) A 的攻击。 X 将哈希函数 H_1, H_2 作为随机预言机, A 可以作 H_1 查询、 H_2 查询、秘密值查询、公钥查询和签名查询。由于 A 是恶意 KGC, 可以计算用户部分私钥, 故用户公钥和用户部分私钥都不需再查询。设 ID_i 是 A 对身份 ID 第 i 次查询, ID^* 为 A 攻击的对象, 所有查询的列表初始为空。

3) H_1 查询。格式为 $(ID_i, R_{ID_i}, Z_{ID_i}, h_{1ID_i})$ 的列表 $L1$ 保存在 X 中。当 X 收到攻击者 A 发送的针对 $(ID^*, R_{ID^*}, Z_{ID^*})$ 的查询时, 若 ID_i 在 $L1$ 列表中, 则 X 返回对应的 h_{1ID_i} 值; 否则 X 选择 $h_{1ID^*} \in \mathbf{Z}_q^*$, 且 h_{1ID^*} 不在 $(h_{1ID1}, h_{1ID2}, \dots, h_{1ID}q_{H_1})$, 将 h_{1ID^*} 返回给 A , 并将 (ID^*, h_{1ID^*}) 添加到表 $L1$ 中。

4) H_2 查询。格式为 $(ID_i, M_i, Z_{ID_i}, R_{ID_i}, K, h_{2ID_i})$ 的列表 $L2$ 保存在 X 中。当 X 收到攻击者 A 发送的针对 $(ID^*, M_i, Z_{ID^*}, R_{ID^*}, K)$ 的查询时, 若询问项存在于表 $L2$ 中, 则 X 返回对应的 h_{2ID_i} 值给 A , 否则 X 随机选择 $h_{2ID^*} \in \mathbf{Z}_q^*$ 返回给 A , 并将 $(ID^*, M_i, Z_{ID^*}, R_{ID^*}, K, h_{2ID^*})$ 添加到表 $L2$ 中。

5) 秘密值查询。格式为 (ID_i, z_{ID_i}) 的列表 $L3$ 保存在 X 中。当 X 收到攻击者 A 发送的针对 (ID_i, z_{ID_i}) 的查询时, 若询问项存在于表 $L3$ 中, 则 X 返回对应的 z_{ID_i} 值给 A 。否则判断 $ID_i = ID^*$ 是否成立, 若成立, 则 X 终止; 若不成立, 则 X 随机选择 $z_{ID^*} \in \mathbf{Z}_q^*$ 给 A , 并将 $\{ID_i, z_{ID_i}\}$ 添加到表 $L3$ 中。

6) 签名查询。 A 作签名询问, 判断 $ID_i = ID^*$ 是否成立, 若成立, 则 X 终止; 若不成立, X 根据签名算法计算出签名 (K, v) , 并将 (K, v) 发送给 A 。

A 输出身份为 ID^* , 关于消息 M 的有效伪造签名 (K, v) , 由分叉引理可知, A 能够生成消息 M 的另一个有效伪造签名 (K, v') , 设 $z_{ID^*} = a$, 则有:

$$vP = (k + d_{ID} + hz_{ID})P = K + R_{ID} + h_1P_{pub} + haP \quad (2)$$

$$v'P = (k + d_{ID} + h'z_{ID})P = K + R_{ID} + h_1P_{pub} + h'aP \quad (3)$$

$$(v - v')P = (h - h')aP; \quad a = (v - v')/(h - h') \quad (4)$$

如果 A 伪造签名成功, 那么 X 就能利用 A 求出了 ECDLP 的一个解。避免这种情况的发生为敌手 A 在秘密值查询和 H_2 查询时是以失败而告终的, 其概率至少为 $\varepsilon/(q_{H_1}q_{H_2})$ 。所以在多项式时间内 X 只能以至少 $\varepsilon/(q_{H_1}q_{H_2})$ 的优势成功解决 ECDLP。由此可见, 改进方案能抵抗敌手 A 在随机预言机模型下的选择适应性消息攻击。

5 改进方案效率分析

各种运算的时间符号定义和时间复杂度换算关系可按文献[12-13]估算, 其中: 相对乘法运算、加法运算、模运算、点加运算和散列运算都可以忽略不计。标记 E、M、A、P、I 分别代表方案中的双线性运算、指数运算、乘法运算、点乘运算和逆运算。1E≈1480A; 1M≈240A; 1P≈29A; 1I≈11A。

由表 1 可以看出: 文献[2]方案使用了复杂的双线性运算和指数运算, 文献[10]和文献[11]虽然在计算过程中也采用了无双线性和无指数运算, 但是这两种方案还使用了逆运算, 增加了计算量。因此本文改进方案, 在保证能抵抗自适应选择消息和身份攻击的同时提高了签名效率。改进方案有效解决了传统的基于证书密码系统中的证书管理问题, 因此减少了系统的开销, 更加适合当前使用广泛的低带宽、低计算的

无线网络安全应用。

表 1 本文方案与其他方案在运算量比较

签名方案	签名阶段	验证阶段	总运算量
文献[2]方案	2P	E + M + P	E + M + 3P
文献[10]方案	1P + 2I	3P	4P + 2I
文献[11]方案	1P + I	4P	5P + I
本文改进方案	1P	3P	4P

6 改进方案应用

无线传感器网络是由大量密集布置在物理区域内或者附近的传感器节点组成新型测控网络, 被广泛应用在军事、环境监测、医疗应用和智能家居等领域。无线传感器网络在提供便利的同时, 其本身出现的问题也越来越多, 信息传输的安全性和无线节点的生命周期已成为制约无线传感器网络发展的主要因素。

本文改进方案应用过程如下: 在无线传感器网络的初始化阶段, 由 KGC 生成系统参数 $params$, 并且为每个传感器节点生成部分私钥, 将其结果写入传感器节点的 ROM 中, 再由传感器节点自行生成相应的公私钥对; 在无线网络工作阶段, 传感器节点将检测到的数据进行签名, 经无线网络发送至服务器, 服务器对签名信息进行有效性验证, 若通过, 则证明信息有效, 否则信息无效。

本文改进方案的应用优势在于在保证签名方案能够抵抗自适应选择消息和身份攻击的同时, 有效降低了签名和验证的计算量和计算难度, 降低了无线传感器节点在签名计算过程中的能量消耗, 能够有效缓解当前制约无线传感器网络发展的问题。

7 结语

本文分析了王怡等^[11]提出的无双线性对无证书签名方案, 指出此方案不能抵抗伪造攻击。本文指出 WD 方案的安全性缺陷, 并提出了一个改进的方案。通过对改进方案的安全性分析, 证明了新方案对自适应选择消息和身份攻击是存在性不可伪造的。该方案的签名阶段只需要 1 个点乘运算, 验证阶段只需要 3 个点乘运算, 并且避开了逆运算。方案在保证能抵抗公钥替换攻击的同时提高了签名效率。

参考文献:

- [1] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography [C]// ASIACRYPT 2003: Proceedings of the 9th International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2003: 452–473.
- [2] ZHANG L, ZHANG F. A method to construct a class of certificateless signature schemes [J]. Chinese Journal of Computers, 2009, 32(5): 940–945. (张磊, 张福泰. 一类无证书签名方案的构造方法[J]. 计算机学报, 2009, 32(5): 940–945.)
- [3] WEI C, CAI X. New certificateless proxy blind signature scheme [J]. Journal of Computer Applications, 2010, 30(12): 3343–3345. (魏春艳, 蔡晓秋. 新的无证书代理盲签名方案[J]. 计算机应用, 2010, 30(12): 3343–3345.)
- [4] HONG D, XIE Q. Efficient certificateless signature scheme [J]. Journal of Computer Applications, 2010, 30(7): 1809–1811. (洪东招, 谢琪. 有效的无证书签名方案[J]. 计算机应用, 2010, 30(7): 1809–1811.)

(下转第 2349 页)

活约束判断问题,并给出了角色集 SoD 约束和激活约束判断过程的实现算法。针对虚拟岗位的生成和撤销过程,本文定义了完成上述过程所需要的生成和撤销的相关管理函数。本文的工作是 OB4LAC 模型实现跨域访问操作的基础性工作,未来的工作重点将集中在如何基于该模型实现业务层面的动态集成和优化问题。

参考文献:

- [1] PENG Y. Research of the organization-based access control method and model for e-government [D]. Dalian: Dalian University of Technology, 2012. (彭友.电子政务中基于组织的访问控制方法及模型研究[D].大连:大连理工大学,2012.)
- [2] LI H. Research of organization based access control model for electronic government system [D]. Dalian: Dalian University of Technology, 2009. (李怀明.电子政务系统中基于组织的访问控制模型研究[D].大连:大连理工大学,2009.)
- [3] DING F. Research on model of government organization authorization system based on OB4LAC [D]. Dalian: Dalian University of Technology, 2009. (丁锋.基于 OB4LAC 的政府组织授权系统模型研究[D].大连:大连理工大学,2009.)
- [4] SHAFIQ B, JOSHI J B D, BERTINO E, et al. Secure interoperation in a multi-domain environment employing RBAC policies [J]. IEEE Transactions on Knowledge and Data Engineering, 2005, 17(11): 1557 – 1577.
- [5] ZHONG L. Research on role-based inter-domain access control model [D]. Hangzhou: Zhejiang Normal University, 2011. (钟丽丽.基于角色的跨域访问控制模型研究[D].杭州:浙江师范大学,2011.)
- [6] LIU M, WANG X, HUANG H, et al. A detection model based on Petri nets of SMER constrains violation in dynamic role translation [J]. Journal of Computer Research and Development, 2012, 49(9): 1991 – 1998. (刘猛,王轩,黄荷娇,等.基于 Petri 网的 IRBAC 2000 域间动态转换 SMER 约束违反检测[J].计算机研究与发展,2012,49(9):1991 – 1998.)
- [7] LIAO J, HONG F, ZHU X, et al. Separation of duty in dynamic role translations between administrative domains [J]. Journal of Computer Research and Development, 2012, 49(9): 1991 – 1998.
- [8] LIU S, HUANG H. Role-based access control for distributed cooperation environment [C]// Proceedings of 2009 International Conference on Computational Intelligence and Security. Washington, DC: IEEE Computer Society, 2009: 455 – 459.
- [9] MA M, WOODHEAD S. Constraint enabled distributed RBAC for subscription-based remote network services [C]// Proceedings of the Sixth IEEE International Conference on Computer and Information Technology. Washington, DC: IEEE Computer Society, 2006: 1 – 6.
- [10] PENG Y, JU H, SONG Y, et al. OB4LAC: an organization-based access control model for e-government system [J]. Applied Mathematics and Information Science, 2014, 8(3): 1467 – 1474.
- [11] LI F, SU M, SHI G, et al. Research status and development trends of access control model [J]. Acta Electronica Sinica, 2012, 40(4): 805 – 813. (李凤华,苏铭,史国振,等.访问控制模型研究进展及发展趋势[J].电子学报,2012,40(4):805 – 813.)
- [12] RUSSELLO G, DULAY N. xDUCON: coordinating usage control policies in distributed domains [C]// Proceedings of the Third International Conference on Network and System Security. Washington, DC: IEEE Computer Society, 2009: 246 – 253.
- [13] ZHANG G, CONG W, TIAN J. The research of cross-domain usage control model in Web services [C]// Proceedings of the Second International Conference on e-Business and Information System Security. Piscataway: IEEE Press, 2010: 1 – 5.
- [14] DAI X, CHEN X, WANG Y, et al. An improved state transition-based security policy conflict detection algorithm [C]// Proceedings of the 2010 International Conference on Computational and Information Sciences. Chengdu: [s. n.], 2010: 609 – 612.
- [15] WANG X, FU H, ZHANG L. Research progress on attribute-based access control [J]. Acta Electronica Sinica, 2010, 38(7): 1660 – 1667. (王小明,付红,张立臣.基于属性的访问控制研究进展[J].电子学报,2010,38(7):1660 – 1667.)

(上接第 2344 页)

- [5] TSO R, KIM C, YI X. Certificateless message recovery signatures providing Girault's level-3 security [J]. Journal of Shanghai Jiaotong University: Science, 2011, 16(5): 577 – 583.
- [6] HUANG X, MU Y, SUSILO W, et al. Certificateless signatures: new schemes and security models [J]. The Computer Journal, 2004, 55(4): 457 – 474.
- [7] HU B C, WONG D S, ZHANG Z, et al. Key replacement attack against a generic construction of certificateless signature [C]// ACISP 2006: Proceedings of the 11th Australasian Conference on Information Security and Privacy, LNCS 4058. Berlin: Springer, 2006: 235 – 246.
- [8] ZHANG Y, WANG L. New DLP-based certificateless signature scheme [J]. Computer Engineering and Applications, 2011, 47(12): 62 – 64. (张燕燕,王亮亮.新型的基于 DLP 的无证书签名方案[J].计算机工程与应用,2011,47(12):62 – 64.)
- [9] YANG B, XIAO Z, LI S, et al. Analysis and improvement of certificateless signature scheme [J]. Computer Engineering, 2012, 38(9): 15 – 18. (杨波,肖自碧,李寿贵,等.一种无证书签名方案的分析与改进[J].计算机工程,2012,38(9):15 – 18.)
- [10] 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.)
- [11] 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及改进[J].计算机应用,2013,33(8):2250 – 2252.)
- [12] KIPNIS A, SHAMIA A. Cryptanalysis of the HFE public key cryptosystem by relinearization [C]// CRYPTO'99: Proceedings of the 19th Annual International Cryptology Conference Advances in Cryptology, LNCS 1666. Berlin: Springer, 1999: 19 – 30.
- [13] COURTOI N, KLIMOV A, PATARIN J. Efficient algorithms for solving overdefined systems of multivariate polynomial equations [C]// EUROCRYPT 2000: Proceedings of the 2000 International Conference on the Theory and Application of Cryptographic Techniques, LNCS 1807. Berlin: Springer, 2000: 392 – 407.