对一种基于身份环签名方案的安全性分析

吴 淮[1]，孙 颖[2]，许春香[1]，伍 玮[3]

(1.电子科技大学计算机科学与工程学院 成都 611731; 2. 四川电力科学研究院 成都 610072;
3. 福建师范大学数学与计算机科学学院 福州 350007)

【摘要】分析了文献[18]中提出的基于身份环签名方案的安全性，发现其不具备存在不可伪造性这一数字签名最重要的性质，指出该方案是不安全的，并给出一种新的伪造攻击方法：身份组合伪造攻击。利用该攻击，一个恶意的环成员能够根据自己的身份伪造任意消息的有效环签名，且在伪造的环签名中，攻击者的身份甚至可以是不包含在此环签名的身份环中。

关 键 词 密码学; 数字签名; 伪造攻击; 环签名
中图分类号 TP309 文献标志码 A doi:10.3969/j.issn.1001-0548.2013.06.022

On the Security of an Identity-Based Ring Signature Scheme

WU Huai[1], SUN Ying[2], XU Chun-xiang[1], and WU Wei[3]

(1. School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 611731;
2. Sichuan electric power research institute Chengdu 610072;
3. School of Mathematics and Computer Science, Fujian Normal University Fuzhou 350007)

Abstract The security of the identity-based ring signature scheme of [18] is analyzed in this paper. It is found that this scheme did not possess the unforgeability property. It is also shown that the proposed scheme is insecure against a new kind of forgery attack, i.e. the identity assembly forgery attack. With such an attack, an adversary is able to forge valid ring signatures on any message based on the features of its identity, and the identity of the adversary can be even not included in the ring of the forged signature.

Key words cryptography; digital signature; forgery attack; ring signature

文献[1]提出了基于身份的密码体制，有效地消除了公钥基础设施(PKI)中对用户证书的验证和证书列表维护等一系列操作。在这种密码体制中，很容易从用户的电话号码、Email地址等唯一公开信息通过计算得出该用户公钥。对应的私钥则通过一个称之为密钥生成中心(PKG)的可信第三方计算得到，由于其简化了公钥管理过程，相较于传统的公钥密码体制而言，基于身份的密码体制能提供更大的便利。

环签名[2]是一种基于匿名性需求、面向群体的签名体制，一个用户可以根据需要选择群体成员并以匿名的方式签名，而被签名者选中的环成员甚至没有察觉。任何验证者通过验证环签名的有效性可以确定该签名来自环中某个成员，但无法确认签名者的真实身份。除了传统的环签名方案，多位学者还提出了门限环签名方案[3-4]，具有可追踪真实签名者的条件匿名环签名方案[5]等。

将基于身份密码学和环签名相结合，文献[6]首次提出基于身份的环签名方案，随后，基于身份的环签名方案得到进一步的研究[7-11]，这些方案均是基于双线对，其签名长度与环成员的人数成线性关系。一种非基于对运算构造环签名的方法在文献[12]中给出。文献[13-14]分别提出了固定签名长度的环签名方案，即签名长度独立于环成员人数。上述提到的所有环签名方案均是在随机预言机模型(random oracle model)下证明其安全性的，随机预言机模型将Hash函数看成是随机函数，其输出是随机值，因此，随机预言机模型下证明安全的方案在实际应用中并不一定安全[15]。因此，设计无随机预言机模型(standand model)下可证明安全的基于身份的环签名

收稿日期：2012－04－06；修回日期：2013－07－16
基金项目：国家自然科学基金(61003232，61173164)；国家自然科学基金国外青年基金(61150110483)；教育部博士点基金(20100185120012)；中央高校基本科研业务费(ZYGX2011J141)
作者简介：吴淮(1982－)，女，博士生，主要从事数字签名方面的研究.

是非常值得研究的。文献[16]提出了一个在标准模型下可证安全的签名方案，这是首次直接构造基于身份的环签名，签名的长度和环内成员个数成线性关系。随后文献[17]对该方案进行改进，使得签名长度和签名效率都有进一步的提高。文献[18]发现该方案不满足存在不可伪造性，在此方案的基础上给出了一个改进的基于身份环签名方案。该方案保留了文献[16-17]中方案的优点，即直接构造的基于身份的环签名，具有更短的签名长度和更少的双线性对运算。同时文献[18]声称新的环签名方案满足无条件匿名性和存在性不可伪造。

通过对文献[18]中的方案进行密码学分析发现，尽管该方案具有很多优点，却存在一种新的伪造攻击——身份组合伪造攻击。在该攻击下，一个敌手可以根据自身的身份特征及对应的私钥信息，计算任意消息的环签名，其中环成员身份由该敌手选择，因此，文献[18]中的方案不具备存在不可伪造性这一数字签名最重要的性质。

1 预备知识

本节回顾文中用到的环签名算法组成和安全模型、双线性对与困难问题假设等知识。

1.1 算法组成及安全模型

基于身份的环签名方案由以下算法构成。

系统建立(setup)：输入安全参数 k，算法输出系统主密钥 s 和公开参数 Params 。其中，Params 包括安全参数，消息空间，密钥空间和签名空间的描述，主密钥 s 由PKG保存。

密钥提取(key extract)：给定用户的身份 $\mathrm{ID}\in\{0,1\}^*$，输入公开参数 Params，主密钥 s，PKG 计算出该用户的私钥 d_{ID}，并通过秘密信道返还给用户。

签名(sign)：输入公开参数 Params，环的用户身份集合 R，签名用户 ID_π 的私钥 d_π 和待签名消息 M，算法输出 M 在身份集合 R 下的 $(1,n)$ 环签名 σ。

验证(verify)：输入公开参数 Params，构成环的用户身份集合 R，签名消息 M 及其环签名 σ，输出 Valid或者Invalid。

基于身份的环签名应满足两个安全性质：一是不可伪造性，即只有知道环中公钥所对应的私钥时才能伪造环签名；二是匿名性，即无法确定签名到底来自于环中哪个成员。具体定义如下：

定义 1 (不可伪造性)签名安全性的标准定义为选择明文攻击下的存在不可伪造性，这可以用一个攻击者 A 和一个挑战者 C 来定义：

挑战者 C 选择安全参数 k，运行系统建立算法 Setup，得到主密钥 s 和系统公开参数 Params 。C 保存主密钥 s，将公开参数 Params 发送给攻击者 A。

攻击者 A 可以有选择地进行多次密钥提取询问和签名询问。

密钥提取询问：A 适应性地选择身份 ID，询问 C 关于 ID 的私钥，C 运行密钥提取算法得到身份 ID 对应的私钥 d_{ID}，将 d_{ID} 返回给 A；

签名询问：A 适应性地选择消息 M 和包含 n 个用户身份的集合 $R=\{\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_n\}$ 进行环签名询问，C 运行签名算法，得到对应的环签名 σ，并将该签名返回给 A。

最后，攻击者输出一个环签名 (M^*,R^*,σ^*)，当 1) (M^*,R^*) 不曾出现在签名询问过程中；2) R^* 中的任何身份不曾出现在密钥提取询问过程中；3) 攻击者 A 伪造的环签名 (M^*,R^*,σ^*) 能够通过验证，即 $\mathrm{Verify}(M^*,R^*,\sigma^*)=\mathrm{Valid}$。则称攻击者 A 赢得了游戏，本文定义 $\mathrm{Adv}_A^{\mathrm{EU-CMA}}{}^{\mathrm{EU-CIA}}=\Pr[\mathrm{Awin}]$ 为攻击者 A 赢得游戏的概率。

定义 2 (无条件匿名性)给定一个基于 n 个身份构成的身份集合 R 的 $(1,n)$ 环签名 σ，任何敌手都不能以大于 $1/n$ 的概率猜对该签名的真正签名者究竟是 R 中的哪个用户，则称此基于身份的环签名方案满足无条件匿名性。

1.2 双线性对

设 G 和 G_T 是乘法循环群，G 的阶为素数 p，g 是群 G 的一个生成元。映射 $e:G\times G\to G_T$ 是一个双线性对，并满足以下性质：

1) 双线性：对任意 $a,b\in Z_p$，$e(g^a,g^b)=e(g,g)^{ab}$；

2) 非退化性：$e(g,g)\neq 1_{G_T}$；

3) 可计算性：对任意 $g^a,g^b\in G$，$a,b\in Z_p$，存在高效的算法计算 $e(g^a,g^b)$。

1.3 困难问题假设

计算性 Diffie-Hellman(CDH) 问题：给定 $(g,g^a,g^b)\in G$，其中 $a,b\in Z_p^*$，计算 g^{ab}。

计算性Diffie-Hellman(CDH)困难假设：如果不存在一个有效的算法 C，可以在多项式时间 t 内以优势 ε 解决群 G 中的CDH问题，则称 $(t,\varepsilon)-\mathrm{CDH}$ 假设成立。

2 环签名方案及安全性分析

本节首先回顾在文献[18]中，提出的标准模型下基于身份的环签名方案，接着对该方案进行安全性分析，并给出一种新的身份组合伪造攻击方法。

2.1 环签名方案回顾

文献[18]提出的标准模型下安全的基于身份环签名方案描述如下：

参数建立(setup)：乘法循环群 G,G_T 满足 $|G|=|G_T|=p$，p 是大素数，g 是群 G 的生成元。双线性对 $e:G\times G\to G_T$，随机选取密码学Hash函数 $H_m:\{0,1\}^*\to Z_p^*$。选择一个秘密值 α，计算 $g_1=g^\alpha$。随机选择 $g_2,u'\in G$，以及长度为 n_u 的向量 $\boldsymbol{U}=(u_i)$，其中 $u_i\in G$。系统的主密钥为 g_2^α，公共参数 $\text{Params}=(G,G_T,e,g,g_1,g_2,H_m,u',U)$。

密钥提取(key extract)：ID 是长度为 n_u 的比特串，表示用户的身份。给定身份 $\text{ID}=(I_1,I_2,\cdots,I_{n_u})$，密钥生成中心(PKG)计算身份 ID 对应的私钥 d_{ID}；随机选择 $r_{\text{ID}}\in Z_p^*$，计算 $d_{\text{ID1}}=g_2^\alpha(u'\prod_{i\in V}u_i)^{r_{\text{ID}}}$，$d_{\text{ID}_2}=g^{r_{\text{ID}}}$，其中 V 表示身份 ID 比特串中比特为1的索引集合，即 $V\subseteq\{1,2,\cdots,n_u\}$。记身份 ID 的私钥 $d_{\text{ID}}=(d_{\text{ID}_1},d_{\text{ID}_2})$。

签名生成(Sign)：签名人选定环身份集合 $R=\{\text{ID}_1,\text{ID}_2,\cdots,\text{ID}_n\}$，签名人的实际身份为 $\text{ID}_\pi\in R,(\pi\in\{1,2,\cdots,n\})$。对待签名消息 M，计算 $H_m(R,M)=m$。相应的环签名算法如下：随机选取 $r_1,r_2,\cdots r_n\in Z_p$，计算 $R_0=d_{\text{ID}_\pi,1}^m\prod_{j=1}^n(U_j)^{rj}$，$R_1=g^{r_1}$，$R_2=g^{r_2},\cdots,R_n=g^{r_n}$，这里 $U_j=u'\prod_{i\in V_j}u_i$。环签名 $\sigma=(R_0,R_1,R_2,\cdots,R_n)$。

签名验证(verify)：给定消息 M 的环签名 $\sigma=(R_0,R_1,\cdots,R_n)$，验证者首先计算 $H_m(R,M)=m$，以及 $U_j=u'\prod_{i\in V_j}u_i$。检验等式 $e(R_0,g)=e(g_1,g_2)^m\times\prod_{j=1}^n e(U_j,R_j)$ 是否成立，若成立则输出valid，否则invalid。

2.2 对环签名方案的安全性分析

文献[18]提出的标准模型下基于身份的环签名方案是基于Waters基于身份加密方案[19]构造的。在计算性Diffie-Hellman困难假设下，文献[18]在标准模型下给出了方案的存在性不可伪造证明，但是方案的安全模型并没有考虑在环签名这种多用户的方案中和各个用户身份之间的关联性，这直接导致了该方案在安全性证明过程中仅考虑了环签名中的单个用户身份私钥提取情况，没有考虑到环签名中多个用户身份之间可以进行组合抵消的情况。因此，尽管文献[18]声称方案的不可伪造性可以归约到计算性Diffie-Hellman假设，但实际上该方案存在一种身份组合伪造攻击，即敌手A能够利用一个已知的身份和对应的私钥，按照一定规律选择环成员身份，可以伪造该组成员对任意消息的环签名，这里环成员身份与已知身份 ID_A 满足特定关系，下面详细描述本文的攻击算法。

攻击者A首先对身份 $\text{ID}_A=(\text{ID}_{A1},\text{ID}_{A2},\cdots,\text{ID}_{An})$ 进行密钥提取询问，获得对应的私钥 $(D_{A1},D_{A2})=(g_2^\alpha(u'\prod_{i\in v}u_i)^{r_A},g^{r_A})$。利用该私钥，攻击者$A$可以伪造环签名，环成员身份由$A$选定，设环成员的身份集合为 $R=\{\text{ID}_1,\text{ID}_2,\cdots,\text{ID}_l\}$，其中 $l\bmod 2=1$ 且 $\text{ID}_A\notin R$。

再给出攻击者A在已知身份 $\text{ID}_A=(\text{ID}_{A1},\text{ID}_{A2},\cdots,\text{ID}_{An})$ 和对应的私钥 $(D_{A1},D_{A2})=(g_2^\alpha(u'\prod_{i\in v}u_i)^{r_A},g^{r_A})$ 情况下，对方案的一般性攻击，随后给出具体实例来说明文献[18]中的方案存在安全隐患。

1) 取 $k_j=1$ 或 $k_j=-1$，满足 $\sum_{i=1}^l k_j=1$，即存在 $\left\lfloor\frac{l}{2}\right\rfloor+1$ 个 $k_j=1(j\in z_l^*)$，$\left\lfloor\frac{l}{2}\right\rfloor$ 个 $k_j=-1(j\in z_l^*)$。A 选择环成员的身份 $R=\{\text{ID}_1,\text{ID}_2,\cdots,\text{ID}_l\}$ 使得下面方程成立。

$$K\times(\text{ID}_1,\text{ID}_2,\cdots,\text{ID}_l)^{\text{T}}=$$

$$(k_1,k_2,\cdots,k_l)\begin{bmatrix}\text{ID}_{11}&\text{ID}_{12}&\cdots&\text{ID}_{1n}\\ \text{ID}_{21}&\text{ID}_{22}&\cdots&\text{ID}_{2n}\\ \vdots&\vdots&\text{O}&\vdots\\ \text{ID}_{l1}&\text{ID}_{l2}&\cdots&\text{ID}_{\text{ln}}\end{bmatrix}=$$

$$(\text{ID}_{A1},\text{ID}_{A2},\cdots,\text{ID}_{An})$$

即 $\sum_j^l k_j I_{ji}=\text{ID}_{Ai}$，$i\in\{1,2,\cdots,n\}$。

2) A随机选择待签名的消息 M，计算 $m=H(R,M)$，然后计算环签名 $\sigma'=(s',R_1',R_2',\cdots,R_l')$，其中 $s'=D_{A1}^m$，$R_1'=D_{A2}^{mk_1},R_2'=D_{A2}^{mk_2},\cdots,R_l'=D_{A2}^{mk_l}$。容易验证，伪造的环签名满足验证式：

$$e(g_2,g_1)^m\prod_{j=1}^{l}e(U_j,R_j)=$$

$$e(g_2,g_1)^m\prod_{j=1}^{l}e(u'\prod_{i\in V_j}u_i,D_{A2}^{mk_j})=$$

$$e(g_2,g_1)^m\prod_{j=1}^{l}e(u'\prod_{i\in V_j}u_i,g^{r_Amk_j})=$$

$$e(g_2,g_1)^m\prod_{j=1}^{l}e((u'\prod_{i\in V_j}u_i)^{r_Amk_j},g)=$$

$$e(g_2,g_1)^m e(\prod_{j=1}^{l}((u'\prod_{i\in V_j}u_i)^{r_Amk_j}),g)=$$

$$e(g_2,g_1)^m e((u')^{r_Am\sum_{j=1}^{l}k_j}\prod_{i\in(V_1\cup V_2\cup\cdots V_l)}((u_i)^{\sum_{j=1}^{j=l}k_j\mathrm{ID}_{ji}})^{r_Am},g),$$

$$(\text{由于}\sum_{j=1}^{l}k_j=1,\ \sum_{j=1}^{j=l}k_j\mathrm{ID}_{ji}=\mathrm{ID}_{Ai})=$$

$$e(g_2,g_1)^m e((u'\prod_{i\in V_A}u_i)^{r_Am},g)=$$

$$e(g_2^{\alpha m},g)e((u'\prod_{i\in V_A}u_i)^{r_Am},g)=$$

$$e(g_2^{\alpha m}(u'\prod_{i\in V_A}u_i)^{r_Am},g)=e(D_{A1}^m,g)=e(s,g)$$

因此，$\sigma'=(s',R_1',R_2',\cdots,R_l')$是一个有效的环签名，即$A$利用一个已知身份对应的私钥可以伪造任意消息$M$的有效环签名，且该环可以是由$A$设 定的除自身以外的其他用户组成。为了使签名随机化，可以选择$r_j\in Z_p$，使得$\sum_{j=1}^{j=l}k_j\mathrm{ID}_{ji}r_j=\mathrm{ID}_{Ai}$成立，然后计算$R_j=D_{A2}^{mk_jr_j}$，$j\in\{1,2,\cdots,l\}$。

举例说明身份组合伪造攻击。假定攻击者A选择身份$\mathrm{ID}_A=1101$，密钥提取得到的私钥为$(D_{A1},D_{A2})=(g_2^{\alpha}(u'\prod u_i)^{r_A},g^{r_A})$。

1) A选取$K=(1,1,1,-1,-1)$，$R=\{\mathrm{ID}_1,\mathrm{ID}_2,\mathrm{ID}_3,\mathrm{ID}_4,\mathrm{ID}_5\}$使得$K\times(\mathrm{ID}_1,\mathrm{ID}_2,\mathrm{ID}_3,\mathrm{ID}_4,\mathrm{ID}_5)^{\mathrm{T}}=1101$，即：

$$K\times(\mathrm{ID}_1,\mathrm{ID}_2,\mathrm{ID}_3,\mathrm{ID}_4,\mathrm{ID}_5)^{\mathrm{T}}=$$

$$(1,1,1,-1,-1)\begin{bmatrix}0&1&1&0\\1&1&1&1\\1&0&0&1\\1&1&1&0\\0&0&1&1\end{bmatrix}=(1,1,0,1)$$

环成员分别为$\mathrm{ID}_1=0110$，$\mathrm{ID}_2=1111$，$\mathrm{ID}_3=1001$，$\mathrm{ID}_4=1110$，$\mathrm{ID}_5=0011$。

2) 选择待签名的消息M，计算$m=H(R,M)$，由验证式得出$\sum_{j=1}^{j=l}k_j\mathrm{ID}_{ji}r_j=\mathrm{ID}_{Ai}$，选取$r_j\in Z_P,j\in\{1,2,\cdots,l\}$，使得下面方程组成立：

$$\begin{cases}0\cdot r_1+r_2+r_3-r_4-0\cdot r_5=1\\r_1+r_2+0\cdot r_3-r_4-0\cdot r_5=1\\r_1+r_2+0\cdot r_3-r_4-r_5=0\\0\cdot r_1+r_2+r_3-0\cdot r_4-r_5=1\end{cases}$$

任意选取$r_2\in Z_p$，得出$r_1=r_3$，$r_4=r_5=1$，$r_2=(2-r_1)\mathrm{modp}$，然后计算$s'=D_{A1}^m$，$R_1'=D_{A2}^{mk_1r_1}$，$R_2'=D_{A2}^{mk_2r_2},\cdots$，$R_5'=D_{A2}^{mk_5r_5}$，伪造的环签名为$\sigma'=(s,R_1',R_2',\cdots,R_5')$。显然，该签名$\sigma'$满足环签名验证式。

3 结束语

本文对文献[18]中提出的基于身份环签名方案进行安全分析，给出了一种新的伪造攻击方法——身份组合伪造攻击。在该攻击下，敌手可以根据已掌握的身份对应的私钥，通过选择环成员的身份来伪造任意消息的环签名。

参考文献

[1] SHAMIR A. Identity-based cryptosystems and signature schemes[C]//Proceeding of CRYPTO 1984. Berlin: Springer, 1984.

[2] RIVEST R, SHAMIR A, TAUMAN Y. How to leak a secret [C]//Advances in ASIACRYPT 2001. Berlin: Springer-Verlag, 2001.

[3] BRESSON E, STERN J. SZYDLO M. Threshold ring signatures and applications to Ad-hoc groups[C]// CRYPTO'02. Berlin: Springer, 2002: 465-480.

[4] MELCHOR C A, CAYREL P L, GABORIT P, et al. A new efficient threshold ring signature scheme based on coding theory[C]//PQCrypto 2008: Proceedings of the 2nd International Workshop on post Quantum Crytography, LNCS 5299. Berlin: Springer, 2008.

[5] ZENG S, JIANG S, QIN Z. A new conditionally anonymous ring signature [C]//COCOON 2011, LNCS. Berlin: Springer, 2011.

[6] ZHANG F, KIM K. ID-based blind signature and ring signature from pairings[C]//Advances in ASIACRYPT 2002. Berlin: Springer-verlay, 2002.

[7] AWASTHI A, LAL S. ID-based ring signature and proxy ring signature schemes from bilinear pairings. Cryptology ePrint Archive[EB/OL]. [2012-02-23]. http://eprint.iacr.org/2004/184.pdf.

[8] CHOW S, YIU S, HUI L. Efficient identity based ring signature[C]//ACNS 2005. Berlin: Springer, 2005.

[9] HERRANZ J, SÁEZ G. A provably secure ID-based ring signature scheme[EB/OL]. [2012-02-23]. http://eprint.iacr.org/.

(下转第943页)

guided by proportional navigation[J]. IEEE Trans on Control Systems Technology, 2002, 10(4): 556-567.
[2] RUE A K. Precision stabilization systems[J]. IEEE Trans on Aerospace and Electronics Systems, 1974, AES-10(1): 34-43.
[3] KENNEDY P J. KENNEDY R L. Direct versus Indirect line of sight (LOS) stabilization[J]. IEEE Trans on Control Systems Technology, 2003, 11(1): 3-15.
[4] YU S, ZHAO Y Z. A new measurement method for unbalanced moments in a two-axis gimbaled seeks[J]. Chinese Journal of Aeronautics, 2010, 23(1): 117-122.
[5] YU S, ZHAO Y Z. Simulation study on friction compensation method for inertial platform based on disturbance observer[J]. Journal of Aerospace Engineering, 2008, 222(3): 341-346.
[6] ADEGBEGE A A, HEATH W P. Internal model control design for input-constrained multivariable processes[J]. American Institute of Chemical Engineers, 2011, 57(12): 3459-3472.
[7] WANG L K, LIU X D. Gain scheduled state feedback control for discrete-time-varying poly-topic systems subject to input saturation[J]. Circuit Syst Signal Process, 2011, 30(6): 1165-1182.
[8] ADEGBEGE A A, HEATH W P. Two-stage multivariable anti-windup design for internal model control constraints [C]//Proceedings of 9th International Symposium on Dynamics and Control of Process Systems, International Federation of Automatic Control. Leuven, Belgium: [s.n.], 2010: 276-281.
[9] 姜长生, 吴庆宪, 陈文华, 等. 现代鲁棒控制基础[M]. 哈尔滨: 哈尔滨工业大学出版社, 2005.
JIANG Chang-shen, WU Qing-xian, CHEN Wen-hua,et al. Essentials of modern robust control[M]. Harbin: Press of Harbin Institute of Technology, 2005.
[10] HU T S, LIN Z L, CHEN B M. An analysis and design method for linear systems subject to actuator saturation and disturbance [J]. Automatica, 2002, 38(2): 351-359.
[11] HU T S, LIN Z L. Practical stabilization of exponentially unstable linear systems subject to actuator saturation nonlinearities and disturbance[J]. International Journal of Robust and Nonlinear Control, 2001, 11(6): 555-588.
[12] GAHINET, P, APKARIAN P. A linear matrix inequality approach to H∞ control[J]. Robust and Nonlinear Control, 1994, 4(4): 421-448.
[13] ZHANG J H, XIA Y Q. New LMI approach to fuzzy H∞ filter designs[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2009, 56(9): 739-743.
[14] CHOI H C, CHWA D Y, HONG S K. An LMI approach to robust reduced-order H∞ filter design for polytopic uncertain systems[J]. International Journal of Control, Automation and Systems, 2009, 7(3): 487-494.

编 辑 黄 莘

(上接第929页)

[10] LIN C Y, WU T C. An identity-based ring signature scheme from bilinear pairings[EB/OL]. [2012-02-23]. http://eprint.iacr.org/.
[11] ZHANG F, KIM K. Efficient ID-based blind signature and proxy signature from bilinear pairings[C]//Information Security and Privacy, 8th Australasian Conference, ACISP 2003. Wollongong, Australia: [s.n.], 2003.
[12] AU M, LIU J, TSANG P, et al. A suite of ID-based threshold ring signature schemes with different levels of anonymity[EB/OL]. [2012-02-23]. http://eprint.iacr.org/.
[13] DODIS Y, KIAYIAS A, NICOLOSI A, et al. Anonymous identification in Ad hoc groups[C]//EUROCRYPT 2004. Berlin: Springer-Verlag, 2004.
[14] NGUYEN L. Accumulators from bilinear pairings and applications[C]//CT-RSA 2005. [S.l.]: [s.n.], 2005.
[15] CANETTI R, GOLDREICH O, HALEVI S. The random oracle methodology, revisited[J]. Journal of the ACM, 2004, 51(4): 557-594.
[16] AU M, LIU J, YUEN T, et al. ID-based ring signature scheme secure in the standard model[C]//IWSEC. [S.l.]: [s.n.], 2006.
[17] 张跃宇, 李晖, 王育民. 标准模型下基于身份的环签名方案[J]. 通信学报, 2008, 29(4): 40-44.
ZHANG Yue-yu, LI Hui, WANG Yu-min. Identity-based ring signature scheme under standard model[J]. Journal of Communications, 2008, 29(4): 40-44.
[18] 刘振华, 胡予濮, 牟宁波, 等. 新的标准模型下基于身份的环签名方案[J]. 电子与信息学报, 2009, 31(7): 1727-1731.
LIU Zhen-hua, HU Yu-pu, MOU Ning-bo, et al. New identity-based ring signature in the standard model[J]. Journal of Electronics & Information Technology, 2009, 31(7): 1727-1731.
[19] WATERS B. Efficient identity-based encryption without random oracle[C]//Proc EUROCRYPT 2005. Berlin: Springer-Verlag, 2005.

编 辑 税 红