一个高效的基于身份和 RSA 的紧致多重数字签名方案

张亚玲　　张　璟　　王晓峰
(西安理工大学计算机科学与工程学院　西安　710048)

摘　要：紧致多重数字签名是指多个用户对同一个消息进行多重签名，所得多重签名的长度和单个用户签名的长度相当。该文提出一个高效的基于身份和 RSA 的紧致多重签名方案。签名和验证的效率比 Bellare 和 Neven 的多重签名方案提高了接近 50%，多重签名的长度和单个 RSA 签名长度相当，因为使用了基于身份的公钥密码，新方案很好地实现了多重签名的紧致性目标。在随机预言模型和 RSA 假设下证明了方案的安全性。

关键词：数字签名；紧致多重数字签名；公钥密码；RSA 密码体制
中图分类号：TP309　　**文献标识码**：A　　**文章编号**：1009-5896(2008)09-2246-04

An Efficient Identity Based Compact Multi-signature From RSA

Zhang Ya-ling　　Zhang Jing　　Wang Xiao-feng
(*the School of Computer Science and Engineering, Xi'an Univ. of Tech., Xi'an* 710048, *China*)

Abstract: A compact multi-signature is a special digital signature that allows multiple signers to generate a signature on the same message with the property that the length of the signature is almost same as that of an individual signature. An efficient identity based compact multi-signature scheme from RSA is proposed in this paper. The efficiency of the new scheme is improved by 50% than that of Bellare and Neven's scheme. The signature length of the new scheme is almost same as that of a single RSA signature, as the identity based public key is used, the goal to design a compact multi-signature is nearly achieved. The security of the new scheme is proved under the assumption of RSA in the random oracle model.

Key words: Digital signature; Compact multi-signature; Public key; RSA cryptography

1　引言

随着能量受限的小型信息设备，如PDA(Personal Digital Assistant)，RFID(Radio Frequency IDentification)，智能卡等的广泛应用，如何减少数据的传输量是一个至关重要的问题。密码技术通常用来保护这些设备的信息传输安全，对称密码用于保护通信信息的机密性，公钥密码特别是数字签名用作信息的安全认证技术。签名认证信息的长度在确保安全的情况下越短越好。

多重数字签名是指多个用户对同一个消息进行紧致签名(compact signature)，这里紧致是指多重签名的长度和单个用户签名的长度相当。多重签名可以广泛地应用于协同设计、计算网格及自动化办公系统等应用领域。文献[1]提出了首个多重数字签名方案后，不同的多重数字签名方案相继被提出[2−4]。与多重签名概念密切相关的是聚合签名(aggregate signatures)[5,6]，聚合签名是指n个用户对n个不同的消息进行签名，最后把这些签名聚合，得到一个长度和单个签名长度相当的签名。多重签名和聚合签名都有两个工作模式，一个是无序数字签名或者称为并行数字签名，一个是有序数字签名。

对多重数字签名的攻击分为两类：外部攻击和内部攻击。文献[2]提出了一个有序多重签名方案，文献[7]中给出了对文献[2]中方案的两个攻击方案。文献[8]给出了对3个不同的有序多重签名的次序伪造攻击，使得有序多重签名中的次序成为一个敏感的问题。Shao在文献[8]中甚至猜测设计一个安全的有序多重签名是不可能的，尤其是如何阻止对于内部人员的次序攻击是困难的，所以构造紧致的有序多重签名是一个棘手的问题。本文所讲的多重签名都是指无序的并行签名结构。

多重签名方案中签名结果大多是紧致的，但是验证过程则未必是紧致的，一般都是需要将所有签名者的公钥和多重签名一起发送给验证者，这在很大程度上抵消了紧致多重签名的优点。由于身份信息一般都比随机产生的公钥信息的长度要短的多，因此，基于身份的多重签名尤其具有吸引力。

目前，关于基于身份的多重签名(Identity-Based Multi-Signatures, IBMS)方案的研究结果可以参见文献[10,11]。文献[10]给出了一个基于身份的多重签名方案，方案使用了椭圆或超椭圆曲线上的双线性映射，然而双线性映射的实现尚

2007-12-28 收到，2008-06-10 改回
教育部科学技术研究重点项目(208139)，国家 863 计划重点课题(2007AA010305)和陕西省自然科学基础研究计划项目(2006F37)资助课题

不普遍，计算也比较复杂。考虑到RSA的广泛实现和应用，文献[11]提出了一个基于身份的多重RSA数字签名方案，该方案的核心思想是设计一个签名和验证的过程都紧致的多重签名方案。

本文提出了一个高效的基于身份和RSA的紧致多重签名方案。新方案是文献[11]中方案的一个改进。该方案的签名和验证过程的效率比原来的方案提高50%以上。

2　相关知识

RSA假设等相关知识参见文献[11]，下面给出方案安全性证明中需要的引理。

引理1　设 kg_{RSA} 是一个RSA密钥生成算法，输入安全参数 l，生成RSA三元组 (n,e,d)。假如已知 $y,u\in z_n^*$, $y\neq u$，$a,e\in z$ 满足 $y^a\equiv u^e \bmod n$，且 $\gcd(a,e)=1$，则可以求出 $x\in z_n^*$ 满足 $y\equiv x^e \bmod n$。

证明　根据 $\gcd(a,e)=1$，利用Euclidean算法，计算整数 s,t 满足 $sa+te=1$，

则 $y=y^{as+te}\equiv(u^s y^t)^e \bmod n$，所以 $x=u^s y^t \bmod n$ 满足 $y\equiv x^e \bmod n$。

3　基于身份和 RSA 的多重数字签名方案

下面给出文献[11]方案的一个改进方案，主要是为了提高签名和验证效率。新方案在签名者中设立了一个签名的发起者兼收集者。新方案具体如下所示：

(1)系统建立算法(Setup)　PKG生成系统RSA密钥 (n,e,d)，公布系统公钥 $\mathrm{mpk}=\{n,e\}$，保密私钥 $\mathrm{msk}=\{d\}$。公开密码学hash函数 $H:\{0,1\}^*\to z_n^*$，$h:\{0,1\}^*\to\{0,1\}^l$，$l\le\log_2 n$。

(2)私钥提取算法(Extract)　设签名者 U_i 的身份为 ID_i，PKG利用私钥 msk 计算 $Q_i=H(\mathrm{ID}_i)$，$x_i=Q_i^d \bmod n$，把 (ID_i,x_i) 作为 U_i 的身份证书，并通过秘密信道发送给 U_i；

U_i 接收到 (ID_i,x_i) 后，验证 $x_i^e\equiv Q_i \bmod n$。若验证式成立，则确信 x_i 是正确的。

(3)签名算法(Sign)　设有一个签名发起兼签名收集人 U_1，身份为 ID_1。设签名消息是 m，多重签名的签名者身份集合是 $L=\{\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_k\}$。

步骤1(签名发起)　U_1 随机选择一个 $r\in z_n^*$，计算 $R=r^e \bmod n$，广播发送 $(m,L,h(R))$ 给所有的签名者；

步骤2(单个用户签名算法)　每个签名者 U_i 在收到 $(m,L,h(R))$ 后，计算 $c=h(m\,||\,L\,||\,h(R))$，利用私钥 x_i 计算签名 $s_i=x_i^c \bmod n$，将 (ID_i,c,s_i) 发送给签名发起人 U_1；

步骤3(签名聚合算法)　U_1 接收到 (ID_i,c,s_i) $(i=1,2,\cdots,k)$ 后，进行签名聚合，计算 $S=r\prod_{i=1}^{k}s_i \bmod n$。$U_1$ 使用下面的多重签名验证算法确认多重数字签名 (c,S) 的正确性。若通过，得到消息 m 的签名者身份集合为 L 的多重签名 $(c,S)\in\{0,1\}^l\times z_n$，记为 (m,L,c,S)；若失败，签名发起人宣布签名失败；更进一步，针对每个 (ID_i,c,s_i)，可以通过测试等式 $s_i^e(H(\mathrm{ID}_i))^{-c}\equiv 1 \bmod n$ 是否成立判断部分签名的正确性。若成立，则签名 (ID_i,c,s_i) 有效；若不成立，则签名发起人可以追踪出 ID_i 的部分签名不能通过验证。

(4)多重签名的验证(Verify)　任何一个验证者得到多重数字签名 (m,L,c,S) 后，根据 $L=\{\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_k\}$ 首先计算签名者的公钥 $Q_i=H(\mathrm{ID}_i)$，$i=1,2,\cdots,k$，计算 $R=S^e\left(\prod_{i=1}^{k}Q_i\right)^{-c} \bmod n$，验证等式 $c=h(m\,||\,L\,||\,h(R))$ 是否成立。若等式成立，验证通过；否则，验证失败。

4　安全性分析

定理 1　新方案中基于身份的多重 RSA 签名算法是正确的。

证明　假如多重数字签名 (m,L,c,S) 是按照签名算法计算，则

$$S^e\left(\prod_{i=1}^{k}Q_i\right)^{-c} \bmod n\equiv\left(r^e\prod_{i=1}^{k}s_i^e\right)\left(\prod_{i=1}^{k}Q_i\right)^{-c} \bmod n$$
$$\equiv R\prod_{i=1}^{k}(x_i^e)^e\left(\prod_{i=1}^{k}Q_i\right)^{-c} \bmod n=R$$

因此　$c=h(m\,||\,L\,||\,h(R))$ 成立。　证毕

定理2　假如存在一个攻击者 A 可以 $(t,q_H+q_h,q_k,q_S,\varepsilon)$ 攻破本文的多重签名方案，则存在一个算法 B，在时间 $t_1\approx 2t+(q_H+q_k+q_S+1)O(\log^3 n)$ 以内，以概率 $\varepsilon_1\ge(1-\delta)^{q_k}(\delta/e)\varepsilon^2$ 成功地解决RSA单向性问题，其中 δ $(0<\delta<1/2)$ 是任意一个固定的小数。

证明　设算法 B 的RSA单向性问题是：任意给定 $y\xleftarrow{R}z_n^*$，求 x 满足 $y=x^e \bmod n$，其中 $(n,e,d)\xleftarrow{R}kg_{\mathrm{RSA}}$。假设有一个攻击者 A 可以 $(t,q_H+q_h,q_k,q_S,\varepsilon)$ 攻破本文的新方案。通过算法 B 与攻击者 A 的交互，算法 B 企图计算 $x\leftarrow B(n,e,y)$ 满足 $y=x^e \bmod n$。算法 B 模拟PKG与攻击者 A 的交互，使攻击者 A 产生一个存在伪造签名攻击。

(1)PKG密钥生成算法　算法 B 公布PKG的公开密钥 $\mathrm{mpk}=\{n,e\}$ 和密码学安全的hash函数 $H:\{0,1\}^*\to z_n^*$，$h:\{0,1\}^*\to\{0,1\}^l$，$l\le\log_2 n$。

(2)身份hash函数 H 询问：攻击者 A 询问算法 B 身份为 ID_i 的公钥 Q_i。算法 B 随机选择 $x_i\xleftarrow{R}z_n^*$，并随机以概率 $1-\delta$ 选择 $b_i=0$，计算 $Q_i\equiv x_i^e \bmod n$；以概率 δ($0<\delta<1/2$) 选择 $b_i=1$，计算 $Q_i\equiv yx_i^e \bmod n$。在hash询问 H 列表中添加记录 $(\mathrm{ID}_i,x_i,b_i,Q_i)$，将 $Q_i=H(\mathrm{ID}_i)$ 作为公钥，发送给攻击者 A；假如有 q_H 个hash函数 H 询问，计算量大约为 $q_H\cdot O(\log^3 n)$。

随机数hash函数 h 询问：假如攻击者 A 询问 (m_i,L_i,R_i) 的hash值 $h(m_i\,||\,L_i\,||\,h(R_i))$，算法 B 在hash询问 h 列表中查找是否有记录 (m_i,L_i,R_i,c_i)。若有返回 c_i；若没有，任选 $c_i\xleftarrow{R}\{0,1\}^l$，返回 $c_i=h(m_i\,||\,L_i\,||\,h(R_i))$，并在 h 列表中添加

记录 (m_i, L_i, R_i, c_i)。

(3)私钥提取询问　若攻击者A询问算法B身份为 ID_i 的私钥，算法B查找hash询问列表 H，检查记录项 $(\mathrm{ID}_i, x_i, b_i, Q_i)$，当 $b_i = 0$，则把 x_i 作为身份为 ID_i 的用户私钥，并通过秘密信道发送给攻击者A；当 $b_i = 1$，算法B令 $\mathrm{bad}_1 \leftarrow \mathrm{true}$，退出协议，宣布失败。假如询问了 q_k 个私钥提取询问，且算法B没有失败，该事件的概率为 $(1-\delta)^{q_k}$。

(4)签名询问　假设攻击者A询问关于 (m_i, L_i) 的多重签名 s_i。为了回答关于 (m_i, L_i) 的多重签名询问，算法B任意选择 $c_i \overset{R}{\leftarrow} \{0,1\}^l$，$S_i \overset{R}{\leftarrow} z_n^*$，计算 $R_i = S_i^e \left(\prod_{\mathrm{ID}_j \in L_i} Q_j \right)^{-c_i} \bmod n$。

查询hash询问 h 列表，假如表中有记录 $(m_i, L_i, *, c_i)$ 或者有记录 $(m_i, L_i, R_i, *)$，重新选择 $c_i \overset{R}{\leftarrow} \{0,1\}^l$，$S_i \overset{R}{\leftarrow} z_n^*$，重新计算 R_i。直到 R_i, c_i 是第一次出现。并令 $c_i = h(m_i \,||\, L_i \,||\, R_i)$，在 h 列表中添加记录 (m_i, L_i, R_i, c_i)；将多重签名 (m_i, L_i, c_i, S_i) 返回给攻击者A。

攻击者A验证多重签名 (m_i, L_i, c_i, S_i) 的正确性：显然有 $R_i = S_i^e \left(\prod_{\mathrm{ID}_j \in L_i} Q_j \right)^{-c_i} \bmod n$，$c_i = h(m_i \,||\, L_i \,||\, R_i)$ 成立。因此，这个模拟是完美的。假如询问了 q_s 个签名询问，计算量约为 $2\,q_s O(\log^3 n)$。

(5)攻击者A伪造　攻击者A可以 $(t, q_H + q_h, q_k, q_S, \varepsilon)$ 攻破本文的方案，则攻击者最终以概率 ε 成功伪造了一个有效的多重签名 $(\widetilde{m}, \widetilde{L}, \tilde{c}, \tilde{s})$，并且伪造是非平凡的，即攻击者$A$没有询问过关于 $(\widetilde{m}, \widetilde{L})$ 的多重签名，且身份集合 $\widetilde{L}$ 中至少有一个身份的私钥没有询问过。

得到A伪造的多重签名 $(\widetilde{m}, \widetilde{L}, \tilde{c}, \tilde{s})$ 后，算法B检查函数 H 询问列表。若 $\forall \mathrm{ID}_i \in \widetilde{L}$ 所有记录 $(\mathrm{ID}_i, x_i, b_i, Q_i)$ 中均有 $b_i = 0$，则算法B令 $\mathrm{bad}_2 \leftarrow \mathrm{true}$。否则，将 $b_i = 0$ 的身份集合记为 $\widetilde{L}_0$，将 $b_i = 1$ 的身份集合记为 $\widetilde{L}_1$，则 $\widetilde{L} = \widetilde{L}_0 \cup \widetilde{L}_1$，$\widetilde{L}_0 \cap \widetilde{L}_1 = \Phi$，且 $\widetilde{L}_1 \neq \Phi$。

B退出协议的概率 $P(\mathrm{bad}_2 \leftarrow \mathrm{true}) = (1-\delta)^{|\widetilde{L}|}$，因为算法$A$没有关于 b_i 的信息，所以集合 $\widetilde{L}$ 对应的 b_i 完全符合二项分布。B没有退出的概率为 $1-(1-\delta)^{|\widetilde{L}|}$，因为 $(1-\delta)^{|\widetilde{L}|} \leq 1-\delta$，所以还有 $1-(1-\delta)^{|\widetilde{L}|} \geq \delta$。

根据文献[12]中的分叉引理，最终攻击者A可以成功伪造另外一个有效的多重签名 $(\widetilde{m}, \widetilde{L}, \tilde{c}', \tilde{s}')$，$\tilde{c} \neq \tilde{c}'$。这样得到两个验证式子成立：

$$\widetilde{R} = \widetilde{S}^e \left(\prod_{\mathrm{ID}_j \in \widetilde{L}} Q_j \right)^{-\tilde{c}} \bmod n,\quad \widetilde{R} = \widetilde{S}'^e \left(\prod_{\mathrm{ID}_j \in \widetilde{L}} Q_j \right)^{-\tilde{c}'} \bmod n$$

(6)求解RSA问题：根据上面两个验证式

$$\widetilde{R} = \widetilde{S}^e \leq \left(\prod_{\mathrm{ID}_j \in \widetilde{L}} Q_j \right)^{-\tilde{c}} \bmod n$$

$$= \widetilde{S}^e \left(\prod_{\mathrm{ID}_j \in \widetilde{L}_0} x_j \right)^{-\tilde{c}e} \left(\prod_{\mathrm{ID}_j \in \widetilde{L}_1} x_j \right)^{-\tilde{c}e} y^{-|\widetilde{L}_1|\tilde{c}} \bmod n$$

$$\widetilde{R} = \widetilde{S}'^e \left(\prod_{\mathrm{ID}_j \in \widetilde{L}} Q_j \right)^{-\tilde{c}'} \bmod n$$

$$= \widetilde{S}'^e \left(\prod_{\mathrm{ID}_j \in \widetilde{L}_0} x_j \right)^{-\tilde{c}'e} \left(\prod_{\mathrm{ID}_j \in \widetilde{L}_1} x_j \right)^{-\tilde{c}'e} y^{-|\widetilde{L}_1|\tilde{c}'} \bmod n$$

算法B推得：

$$\left[\frac{\widetilde{S}}{\widetilde{S}'} \left(\prod_{\mathrm{ID}_j \in \widetilde{L}_0} x_j \right)^{\tilde{c}'-\tilde{c}} \left(\prod_{\mathrm{ID}_j \in \widetilde{L}_1} x_j \right)^{\tilde{c}'-\tilde{c}} \right]^e \equiv y^{|\widetilde{L}_1|(\tilde{c}-\tilde{c}')} \bmod n$$

若 $\gcd(|\widetilde{L}_1|(\tilde{c}-\tilde{c}'), e) \neq 1$，算法$B$令 $\mathrm{bad}_3 \leftarrow \mathrm{true}$，退出协议。否则根据 $\gcd(|\widetilde{L}_1|(\tilde{c}-\tilde{c}'), e) = 1$，利用引理1，令 $a = |\widetilde{L}_1|(\tilde{c}-\tilde{c}')$，$u = \frac{\widetilde{S}}{\widetilde{S}'} \left(\prod_{\mathrm{ID}_j \in \widetilde{L}_0} x_j \right)^{\tilde{c}'-\tilde{c}} \left(\prod_{\mathrm{ID}_j \in \widetilde{L}_1} x_j \right)^{\tilde{c}'-\tilde{c}}$，现在成立 $y^a \equiv u^e \bmod n$，可以求得 x 满足 $y \equiv x^e \bmod n$。至此算法B输出 x，成功地求解了与 kg_{RSA} 相关的RSA单向性问题。算法B成功求解RSA单向性问题的概率 $\varepsilon_1 \geq (1-\delta)^{q_k}(1-(1-\delta)^{|L|})(1/e)\varepsilon^2 \geq (1-\delta)^{q_k}(\delta/e)\varepsilon^2$。　证毕

由定理 2 知道，在 RSA 假设和随机预言模型下，所提出的多重签名是安全的。

5　效率分析

新方案是紧致的，因为多重签名 $(c, S) \in \{0,1\}^l \times z_n$ 的长度为 $l + \log n$，目前可以取 $160 + 1024 = 1184$ bit，单个 RSA 签名的长度是 1024 bit，因此新方案中多重签名长度非常逼近单个签名。在多重签名 (m, L, c, S) 的验证阶段，比验证单个 RSA 签名多计算了 $|L| + 1$ 个乘法和一个指数运算，公钥的计算多了 $|L|$ 个 hash 计算。与文献[11]方案的计算量比较见表 1，其中 k 是签名者个数。

表 1 文献[11] 的方案与本文方案计算一次签名和验证的计算量比较

	广播次数	指数计算次数	乘法次数	Hash计算次数	签名长度
文献[11]中方案	$2k$	$2k+1$	$2k-2$	$3k$	$l+\log n$
本文方案	1	$k+3$	$2k-1$	$2k+2$	$l+\log n$

从表 1 可以看出，本文方案中指数的运算次数为 $k+3$，文献[11]中的方案需要的指数运算需要 $2k+1$，本文方案中的指数运算量大约是文献[11]中方案的 50%，指数运算是 RSA 型数字签名中最为耗时的运算。综合评判，本文方案可以提高效率接近 50%。

6　结束语

本文给出了一个高效的基于身份和 RSA 的多重签名方案，方案设计的主要目标是实现多重签名的紧致性。本文方

案和文献[11]的方案相比，签名和验证的效率提高了接近一半，这个效率的改进是显著的。当然，本文方案还是一个无序的多重签名方案，能否设计出抗内部次序攻击的有序紧致多重数字签名方案是一个值得进一步关注的研究课题。

参 考 文 献

[1] Ohta K and Okamoto T. Multisignature schemes secure against active insider attacks [J]. *IEICE Trans. on Fundamentals*, 1999, E82-A(1): 21–31.

[2] 张健红, 韦永壮, 王育民. 基于RSA的多重数字签名[J]. 通信学报, 2003, 24(8): 150–154.
Zhang Jian-hong, Wei Yong-zhuang, and Wang Yu-min. Digital multisignatures scheme based on RSA [J]. *Journal of China Institute of Communications*, 2003, 24(8): 150–154.

[3] Lin C Y, Wu T C, and Zhang F. A structured multisignature scheme from the gap Diffie-Hellman group. Cryptology ePrint Archive Listing for 2003, Report no 90. http:// eprint. iacr.org/2003/090.pdf, 2003.

[4] Lysyanskaya A, Micali S, and Reyzin L. Sequential aggregate signatures from trapdoor permutations. Proceedings of Eurocrypt 2004, Springer-Verlag, 2004, LNCS 3027: 74–90.

[5] Boneh D, Gentry C, and Lynn B. Aggregate and verifiably encrypted signatures from bilinear maps. EUROCRYPT 2003, Springer-Verlag, 2003, LNCS 2656: 416–432.

[6] Cheng X, Liu J, and Wang X. Identity-based aggregate and verifiably encrypted signatures from bilinear pairing. Computational Science and Its Applications ICCSA 2005, Springer-Verlag, 2005, LNCS 3483: 1046–1054.

[7] 王天银, 张建中. 一种按序多重数字签名方案的安全性分析及改进[J]. 河南科技大学学报(自然科学版), 2005, 26(01): 31–34.
Wang Tian-yin and Zhang Jian-zhong. Cryptanalysis and improvement of sequential multi-signature scheme [J]. *Journal of Luoyang Institute of Technology*(*Natural Science*), 2005, 26(1): 31–34.

[8] Shao Zuhua. On the sequentiality of three optimal structured multisignature schemes [J]. ISPEC 2007, Springer-Verlag, 2007, LNCS 4464: 105–115.

[9] Shamir A. Identity-based cryptosystems and signature schemes. CRYPTO' 84, Springer-Verlag, 1985, LNCS 196: 47–53.

[10] Wang Lihua, Okamoto Eiji, and Miao Ying, *et al*.. ID-based series-parallel multisignature schemes for multi-messages from bilinear maps. WCC 2005, Springer-Verlag, 2006, LNCS 3969: 291–303.

[11] Bellare M and Neven G. Identity-based multi-signatures from RSA. CT-RSA 2007, Springer-Verlag, 2007, LNCS 4377: 145–162.

[12] Pointcheval D and Stern J. Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, 2000, 13(3): 361–396.

张亚玲：　女，1966年生，博士生，副教授，主要研究方向为网络信息安全.

张　璟：　男，1952 年生，教授，博士生导师，主要研究方向为网格计算.

王晓峰：　女，1966 年生，博士，副教授，主要研究方向为密码理论与网络安全.