一个新的强 RSA 假设下的数字签名方案

李用江[1,2]，李 蔚[3]，朱晓妍[1]，葛建华[1]

(1. 西安电子科技大学 综合业务网理论及关键技术国家重点实验室，陕西 西安 710071；2. 广东海洋大学 信息学院，广东 湛江 524088；3. 郑州轻工业学院 信息与计算机系，河南 郑州 450002)

摘要：为提高强 RSA 困难假设条件下随机签名的生成和验证运算速度，提出一个新的签名方案. 通过随机选取模 n 下的幂指数 e，并采用 RSA 算法直接对与 e 绑定的消息签名，简化并去掉了曹等人方案中的冗余参数，在随机预言机模型下可证明该方案是安全的. 通过比较分析发现新方案的运算速度比类似的方案至少提高一倍.

关键词：数字签名；强 RSA 假设；自适应性选择消息攻击

中图分类号：TP309 **文献标识码**：A **文章编号**：1001-2400(2007)04-0634-04

New signature scheme based on the strong RSA assumption

LI Yong-jiang[1,2], *LI Wei*[3], *ZHU Xiao-yan*[1], *GE Jian-hua*[1]

(1. State Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071, China; 2. School of Information, Guangdong Ocean Univ., Zhanjiang 524088, China; 3. Dept. of Information & Computing Science, Zhengzhou Univ. of Light Ind., Zhengzhou 450002, China)

Abstract: To promote the speed of the random signature generation and verification algorithms under the strong RSA hardness assumption, a new signature scheme is proposed. In this scheme, by randomly selecting the exponent e under modular n and using the RSA algorithm to sign the message bound with e, the redundant parameters in Cao et al.'s signature scheme are simplified or deleted. The new scheme is proved to be secure in the Random Oracle Model. Detailed comparisons show that the speed of the new scheme is at least two times faster than that of the other schemes of such a kind.

Key Words: digital signature; strong RSA assumption; adaptive chosen-message attack

数字签名的概念首先由 Diffie 和 Hellman 引入[1]. 由于数字签名具有公开验证性、不可伪造性以及完整性等特点，因此它在信息安全业务、电子商务和电子政务中有着广泛的应用[2,3]. 第一个提出的数字签名方案为 RSA 签名方案[4]，RSA 签名方案形式简易、便于理解，并在实践中有着许多重要的应用. 近几年来，人们相继给出一些基础的随机 RSA 签名方案[5~8]，这些方案的安全性皆依赖于强 RSA 假设. 最近，曹等人给出一种改进的基于强 RSA 假设的签名方案[9]，并将文[9]的方案与文[6,7]的方案进行了比较，发现文[9]的方案效率明显优于文[6,7]中的方案. 然而，曹等人并未给出他们的方案与文[8]方案的比较. 事实上，文[9]中方案的效率高于文[8]中的方案.

笔者基于强 RSA 困难假设，利用模 n 下的随机幂指数，给出一个新的数字签名方案. 由效率分析可知，笔者提出的方案效率优于其他类似方案. 并且由方案的安全性分析可知，笔者提出的方案在随机预言机模型下可证明是安全的.

由于曹等人已在文[9]中给出了其方案与文[6,7]方案的效率比较(比较表明，文[9]方案的效率优于文[6,7]方案)，因此，为说明笔者提出方案的效率优于其他类似方案，只需表明笔者提出方案的效率优于文[8,9]方案. 为此，首先简要回顾文[9]的签名方案.

收稿日期：2007-01-10

基金项目：国家自然科学基金资助(60332030)；国家自然科学基金重大项目资助(60496316)；郑州轻工业学院校基金资助(2006XJJ17)

作者简介：李用江(1967-)，男，副教授，西安电子科技大学博士研究生.

1　强 RSA 问题和曹等方案的简要回顾

1.1　Flexible RSA 问题和强 RSA 问题

Flexible RSA 问题如下:给定一个 RSA 模数 n 及随机数 $z \in Z_n^*$,找出 r 和 y,使得 $y^r = z \bmod n$ 成立 $(r>1, y \in Z_n^*)$. 对指数 r 的选择可能有某种限制:特定的限制会产生特定形式的 Flexible RSA 问题. 强 RSA 假设[10]即是假定 Flexible RSA 问题是难于求解的.

1.2　曹等方案的简要回顾

建立. 选取 $n=pq$,其中 $p=2p'+1, q=2q'+1, |p|=|q|=512$ bit,其中 p, p', q, q' 均为素数. 记 QR_n 为 Z_n 中的二次剩余构成的群. 随机选取 QR_n 中两个生成元 X, g. $H(\cdot)$: $\{0,1\}^* \to \{0,1\}^{256}$ 为一个安全无碰撞的 Hash 函数. 公钥为 $K_P=(n, g, X)$, 私钥为 $K_S=(p, q)$.

签名. 设待签名的消息为 m, 随机选取一个长为 257 bit 的奇数 e,且 $(e, \varphi(n))=1$. 计算 y 使得 $y^e = Xg^{H(m\|e\|X)} \bmod n$. 签名为 (e, y).

验证. 首先验证 e 是否为长为 257 bit 的奇数. 然后验证 $y^e = Xg^{H(m\|e\|X)} \bmod n$.

笔者将在第 2 节中给出一个新的基于强 RSA 假设的签名方案,并在第 3 节中给出曹等人方案及文[8]方案与新方案的比较,最后在第 4 节中给出方案的安全性证明.

2　新的基于强 RSA 假设的方案

建立. 选取 $n=pq$,其中 $p=2p'+1, q=2q'+1, |p|=|q|=512$ bit,其中 p, p', q, q' 均为素数. $H(\cdot)$: $\{0,1\}^* \to Z_n$ 为公开的一个安全无碰撞的 Hash 函数. $K_P=(n)$, $K_S=(p, q)$.

签名. 设待签名的消息为 m, 随机选取一个长为 257 bit 的奇数 e,且 $(e, \varphi(n))=1$. 计算 y 使得 $y^e = H(m\|e) \bmod n$. 签名为 (e, y).

验证. 首先验证 e 是否为长为 257 bit 的奇数. 然后验证 $y^e = H(m\|e) \bmod n$.

曹等人在文[9]中证明了以上方案在强 RSA 假设下可抵抗适应性选择消息存在性伪造攻击.

3　效率比较

文[6]为文[5]的改进方案,并且文[6]的效率优于文[5]的效率. 由文[9]的效率分析可知,曹等人的方案效率优于文[6,7]方案(文[9]中给出了文[6,7]方案效率的一个详细比较列表,由该列表可知文[9]方案的效率优于文[6,7]的方案). 然而,文[9]并未同文[8]进行效率比较. 事实上,由表 1 可知文[9]方案的效率仍然高于文[8]. 限于篇幅,笔者仅在下面的比较中给出文[8,9]的一些主要细节. 由表 1 可知,新方案的效率优于其他类似的方案. 新方案的计算量仅为文[9]方案计算量的1/2. 新方案的签名生成速度和签名验证速度都比文[9]方案提高一倍.

表 1　文[8,9]与新方案的比较

	文[8]方案	文[9]方案	新方案
公钥	(n, h, x, e')	(n, g, X)	n
私钥	(p, q)	(p, q)	(p, q)
随机数	素数 e 及 $y' \in QR_n$	奇数 e	奇数 e
产生签名所需的模指数运算次数	2 次	2 次	1 次
验证签名所需的模指数运算次数	4 次	2 次	1 次
方案所需的模指数运算次数	6 次	4 次	2 次
签名	(e, y, y')	(e, y)	(e, y)

4 安全性分析

4.1 安全模型

在下面的 4.2 节中,笔者证明新方案可抵抗适应性选择消息攻击下的存在性伪造[11]. 给定一个签名方案(KeyGen, Sign, Ver),通过利用如下的挑战者和敌手 A 定义适应性选择消息攻击模型[11].

建立. 挑战者运行密钥生成算法 KeyGen 得到一个公钥 K_P 和相应的私钥 K_S. 敌手 A 仅获得 K_P.

询问. 这是一个自适应性选择过程. 在此期间,敌手 A 向挑战者询问至多 q_S 个自己选择消息 M_1, M_2, …, $M_{q_S} \in \{0, 1\}^*$ 的、关于公钥 K_P 的签名. 对于每个询问,挑战者回答一个签名 $S_i = \mathrm{Sign}(K_S, M_i)$.

输出. 最后,A 输出一个消息签名对 (M, S),若其满足:(1)M 不等于消息集合 $\{M_1, M_2, \cdots, M_{q_S}\}$ 中任何一个;(2)$\mathrm{Verify}(K_P, M, S)$ 是有效的,则称敌手获胜.

4.2 安全证明

利用 4.1 节的安全模型,在强 RSA 假设下,借助随机预言机模型证明方案的安全性.

定理 1 假定强 RSA 问题是困难的,则在随机预言机模型下,新方案可抵抗适应性选择消息攻击下的存在性伪造攻击.

证明 在签名方案中,在签名之前需要提问 Hash 函数的值 $H(m \| e)$. 下面的证明利用了随机预言机模型(Hash 函数可视为一个随机预言机,并认为 Hash 函数的输出是一致分布的).

假定存在一个多项式时间伪造者 F,他通过分别向随机预言机 H 和签名预言机询问 q_H 和 q_S 次,能够在时间多项式时间 t 内以不可忽略的概率 ε 伪造一个签名. 下面证明存在一个新的多项式时间概率算法 Challenger(以下称 Challenger 为挑战者),Challenger 能够在多项式时间内以一个不可忽略的概率求解任给的一个强 RSA 问题实例.

假定签名者 Signer 的系统参数、公钥 $K_P = (n)$ 和私钥 $K_S = (p, q)$ 如同第 2 节所述. F 具有上述的伪造 Signer 签名的能力. 为模拟 Signer,挑战者 Challenger 使用 Signer 的系统参数以及公钥. 然而,Challenger 并不知 Signer 的私钥道 $K_S = (p, q)$,但 Challenger 控制着随机预言机并能够模拟其输出. 现在,Challenger 收到一个随机选取的 $c \in Z_n^*$,尽管不知道私钥 K_S,Challenger 的目标是计算 a, b ($a \in Z_n^*$, $b \geqslant 2$),使得 $a^b = c \bmod n$. 在下面的游戏中,Challenger 模拟签名者回答随机预言机提问和签名预言机的提问. 在此之前,Challenger 自己建立一个列表 L,并将其初始化为空.

Hash-询问. 当 F 询问 $m_i \| e_i$ 的 Hash 值时(为简化证明,假定 e_i 符合签名方案中要求,即 e_i 是长为 257 bit的奇数),Challenger 首先检查列表 L 中是否存在一个向量 $(m_i \| e_i, c_i)$ 包含 $m_i \| e_i$. 若有,则 Challenger 将 c_i 返回给 F;否则,Challenger 随机选取 $u_i \in Z_n$ 并计算 $c_i = cu_i^{e_i} \bmod n$,然后,Challenger 置 $H(m_i \| e_i) := c_i$,将 $(m_i \| e_i, c_i)$ 添加至列表 L 中,并将 c_i 返回给 F. F 至多可进行 q_H 次 Hash 询问.

签名询问. 这是一个适应性选择过程. 在此期间,F 可根据自己的需要选择消息并提问相应的签名. 对于 $1 \leqslant j \leqslant q_S$,当 F 询问消息 M_j 的签名时,Challenger 随机选取 k_j(为简化证明,假定 k_j 符合签名方案中要求,即 k_j 是长为 257 bit的奇数)和 $y_j \in Z_n$,计算 $v_j = y_j^{k_j} \bmod n$,并置 $H(M_j \| k_j) := v_j$. 可能会有这样的情形发生:存在某个 t ($1 \leqslant t \leqslant q_H$),使得恰好成立 $M_j \| k_j = m_t \| e_t$;然而,这种情形发生的概率可以忽略,或者 Challenger 选取适当的 k_j 可避免这种情形的发生. 因此,为简化证明,忽略这种情形的发生. 然后,Challenger 将 $(M_j \| k_j, v_j)$ 添加至列表 L 中,并将 (k_j, y_j) 返回给 F 作为对消息 M_j 的签名. 事实上,由 (k_j, y_j) 产生的过程易知 $y_j^{k_j} = v_j = H(M_j \| k_j) \bmod n$,对 F 而言,(k_j, y_j) 为消息 M_j 的一个“合法”的签名. F 至多可进行 q_S 次签名询问.

输出. 最后,F 停止并对消息 m 输出一个自己认为有效的签名 (e, y)(即 F 发现 $y^e = H(m \| e) \bmod n$ 成立. 注意到 H 可视为一个随机预言机,从而 F 未经询问随机预言机 H 而正确猜测 $H(m \| e)$ 的值的概率可以忽略. 因此,可知经过询问 $H(m \| e)$ 后,存在一个 $1 \leqslant r \leqslant q_H$,使得 $m \| e = m_r \| e_r$,使得 m 不为消息集合 $\{M_1, M_2, \cdots, M_{q_S}\}$ 中任何一个. 由此及 Hash 询问的过程可知:$y^{e_r} = H(m_r \| e_r) = cu_r^{e_r} \bmod n$. 从而,Challenger 可计算 $c = (yu_r^{-1})^{e_r} \bmod n$(注意 $u_r^{-1} \bmod n$ 存在这一情形以一个几乎为 1 的概率发生,故以下假

定 $u_r^{-1} \bmod n$ 存在,同时,由于 $c \in Z_n^*$,这也意味着 $y \in Z_n^*$,故以下总是假定 $a = yu_r^{-1} \bmod n \in Z_n^*$). 这样,利用算法 F, Challenger 可以求解一个强 RSA 问题实例:即给定一个 RSA 模 $n = pq$ 和一个随机数 $c \in Z_n^*$, Challenger 可计算 a, b ($a \in Z_n^*$, $b \geqslant 2$),使得 $a^b = c \bmod n$,其中 $a = yu_r^{-1} \bmod n, b = e_r$.

由以上分析可知,Challenger 求解任给一个强 RSA 问题实例成功的概率直接依赖于 F 成功伪造签名的概率. 因此,若多项式时间伪造者 F 通过分别向随机预言机 H 和签名预言机询问 q_H 和 q_S 次,能够在时间 t 内以不可忽略的概率 ε 伪造一个签名,则存在多项式时间算法 Challenger,使得其通过运行算法 F 能够在多项式时间以不可忽略的概率求解任给的一个强 RSA 问题实例,而这与强 RSA 假设相矛盾. 因此,在强 RSA 问题困难假设下,笔者提出的方案可抵抗适应性选择消息攻击下的存在性伪造攻击.

5　结 束 语

笔者给出一个新的基于强 RSA 困难假设的数字签名方案. 由效率分析可知,文[9]方案的效率优于文献[5～8]的类似方案. 因此,只需给出新方案与文[9]的效率比较. 从第 3 节的效率比较可以看出,笔者提出的方案更为有效,即新方案计算量仅为文[9]方案计算量的1/2. 新方案的签名生成速度和签名验证速度都比文[9]方案提高一倍. 而且新方案是可证明安全的.

参考文献:

[1] Diffie W, Hellmann M. New Direction in Cryptography [J]. IEEE Trans on Information Theory, 1976, 22(6): 644-654.

[2] Xin Xiangjun, Li Fagen, Xiao Guozhen. A Fair Exchange Protocol Based on Short Signature with the Off-line Semi-trusted Third Party[J]. Journal of Xidian University, 2007, 34(1):92-95.

[3] Wu Qianhong, Zhu Xiaoyan, Wang Yumin. A Practical Electronic Auction Scheme Based on the RSA Function[J]. Journal of Xidian University, 2003, 30(6):788-791.

[4] Rivest R L, Shamir A, Adelman L. A Method for Obtain Digital Signatures and Public-key Cryptosystem [J]. Commun ACM, 1978, 21(2): 120-126.

[5] Cramer R, Shoup V. Signature Schemes Based on the Strong RSA Assumption [J]. ACM Trans on Infromation and System Security, 2003, 3(3): 161-185.

[6] Fischlin M. The Cramer-Shoup Strong-RSA Signature Scheme Revisited[C]//Proceedings of the PKC 2003. Berlin: Springer-Verlag, 2003: 116-129.

[7] Zhu H F. New Digital Signature Scheme Attaining Immunity to Adaptive Chosen-message Attack [J]. Chinese Journal of Electronics, 2001, 10(4): 484-486.

[8] 汪保友, 胡运发. 基于强 RSA 假设的签名方案[J]. 软件学报,2002,13(8): 1729-1734.

[9] 曹正军, 刘木兰. 一个基于强 RSA 数字签名方案的改进[J]. 计算机学报, 2006, 29(9): 1617-1621.

[10] Baric N, Pfitzmann B. Collision-free Accumulators and Fail-stop Signature Schemes Without Trees[C]//EUROCRYPT'97. Berlin: Springer-Verlag, 1997: 480-494.

[11] Goldwasser S, Micali S, Rivest R. A Digital Signature Scheme Secure Against Adaptive Chosen Message Attacks [J]. SIAM J Comput, 1998, 17(2): 281-308.

(编辑: 郭　华)