第 29 卷 第 9 期
2006 年 9 月
计 算 机 学 报
CHINESE JOURNAL OF COMPUTERS
Vol. 29 No. 9
Sept. 2006

一个基于强 RSA 数字签名方案的改进

曹正军[1),2)] 刘木兰[2)]

[1)](上海大学数学系 上海 200444)

[2)](中国科学院数学与系统科学研究院数学机械化重点实验室 北京 100080)

摘 要 该文改进了 Zhu 等人的基于强 RSA 的数字签名方案. 原方案在系统建立阶段必须选取 QR_n 中的三个生成元,并且签名人在签名阶段还必须选取一个固定长度的素数. 改进方案只需选取两个生成元,而且只需选取一个固定长度的奇数. 新方案的计算量约是原方案的 1/2. 在强 RSA 假设下,文中分析了改进方案的安全性.

关键词 强 RSA 假设;生成元;自适应选择消息攻击;存在型伪造.

中图法分类号 TP309

Improvement of a Signature Scheme Based on Strong RSA

CAO Zheng-Jun[1),2)] LIU Mu-Lan[2)]

[1)](*Department of Mathematics, Shanghai University, Shanghai* 200444)

[2)](*Key Laboratory of Mathematics Mechanization, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing* 100080)

Abstract This paper improves the signature scheme based on strong RSA proposed by Zhu in 2001. The original scheme should select three generators in QR_n in the setup phase. In signing phase, the signer has to choose a prime number with prescribed length. The authors remove these restrictions. Only two generators and an odd should be selected in the improved scheme. The scheme saves about 1/2 computation cost of the original scheme. The authors also analyze its security under strong RSA.

Keywords strong RSA; generator; adaptive chosen-message attack; existential forgery

1 引 言

在文件上手写签名一直被作为一种证明签名者身份的标识,它表明签名人看过乃至同意文件的内容. 签名人作出签名后将无法否认,并要为自己的签名负责. 在法律上,签名是一种重要的诉讼证据. 生活中需要签名的事例举不胜举. 重要的如:给重病患者动手术,必须有亲属在手术协议书上签名;重要的商务合同必须有相关法人代表的签名,还需公证处公证;司法机关审讯犯罪嫌疑人的审讯记录也须有当事人的画押. 一般的如:写留言、借条、填登记表. 当然,随着高科技的发展,刑侦工作中采用的 DNA 检测,即利用个体的生理特征来鉴别有关主体,另当别论.

现实生活中,手写签名有很多缺陷. 高超的伪造者能够模仿签名人的笔迹伪造签名;采用高明的剥离技术,签名能够从一篇文章盗用移到另一篇文章;

收稿日期:2006-03-20;修改稿收到日期:2006-05-30. 本课题得到国家自然科学基金(90304012)、国家"九七三"重点基础研究发展规划项目基金(2004CB318000)资助. 曹正军,男,1971 年生,博士研究生,主要研究方向为信息安全与密码学. E-mail: zjcao@amss.ac.cn. 刘木兰,女,1941 年生,研究员,博士生导师,主要研究领域为信息安全、密码学、计算机代数.

文件在签名后能被替换;由于自然力的影响,笔迹会变得模糊,难以辨识.总之,依靠人体感官来辨识的手写签名是相当不安全的.为了克服这些缺陷,一门新技术即在数字世界中实现签名,在 20 世纪 70 年代末随着公钥密码学[2]的诞生发展起来了,这便是基于公钥基础设施(PKI)的数字签名(digital signature).

目前绝大部分数字签名方案都是基于离散对数问题和 RSA 问题的[3],典型的如 ElGamal 签名[4]、Schnorr 签名[5]以及美国的数字签名标准 DSA[6],都是基于离散对数问题.我们知道,利用 RSA 构造的签名方案模数长度不小于 1024bit(离散对数型的模数长度则是 512bit),因此效率较低.那么,能否利用 RSA 构造出效率较高的数字签名方案呢?为此,Cramer 和 Shoup[7]在 2000 年最早提出了一个基于强 RSA 假设的数字签名方案,但该方案不够简练.2003 年,Fischlin[8]在 Cramer-Shoup 方案的基础上进行了改进.事实上,该方案与国内学者朱华飞[1]在 2001 年提出的一个数字签名方案很类似.下面我们将对这三个方案加以叙述,然后再设计一个改进方案.新方案的优点在于,系统建立阶段只需选取两个生成元(比原方案少一个),签名人在签名阶段只需选取一个固定长度的奇数(原方案为素数).在同等规格的模数下,新方案的效率要明显优于原方案,计算量约是原方案的 1/2.并且在强 RSA 假设下,我们分析了改进方案的安全性.

2 三个基于强 RSA 假设的签名方案

2000 年,Cramer 和 Shoup[7]最早提出了一个基于强 RSA 假设的数字签名方案,他们证明了该方案在自适应选择消息攻击(adaptive chosen-message attack)下能够抵抗存在型伪造(existential forgery).为此,我们先介绍强 RSA 问题与强 RSA 假设,然后再叙述相关的三个方案.

定义 1(强 RSA 问题). 给定一个 RSA 模 $N=pq$ 和一个随机数 $c\in Z_N^*$,计算 $a,b\in Z_N^*$, $b\geq 2$,使得 $a^b=c \bmod N$.

强 RSA 假设.在不知道 N 因子分解情况下,计算强 RSA 问题是困难的.

2.1 CS-数字签名方案

建立.选取 $n=pq$,其中 $p=2p'+1$, $q=2q'+1$, 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 $h,x\in QR_n$ 和一个长为 $(l+1)$bit 的素数 e'. $H(\cdot):\{0,1\}^*\rightarrow\{0,1\}^l$ 为一安全无碰撞的 Hash 函数. $PK=(n,h,x,e',H)$, $SK=(p,q)$.

签名.设待签名的消息为 m,随机选取一个长为 $(l+1)$bits 的素数 $e\neq e'$ 以及 $y\in QR_n$;计算 x' 使得

$$(y')^{e'}=x'h^{H(m)} \bmod n,$$

计算 y 使得 $y^e=xh^{H(x')} \bmod n$,签名为 (e,y,y').

验证.首先检验 e 是否是长为 $(l+1)$bits 的奇数且 $e\neq e'$,然后计算

$$x'=(y')^{e'}h^{-H(m)} \bmod n$$

并验证

$$x=y^e h^{-H(x')} \bmod n.$$

2.2 Fischlin-数字签名方案

2003 年,Fischlin[8]指出 CS 方案中关于 x' 的计算过程是多余的.为此,他提出了一个改进方案:

建立.选取 $n=pq$,其中 $p=2p'+1$, $q=2q'+1$, 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 $h_1,h_2,x\in QR_n$. $H(\cdot):\{0,1\}^*\rightarrow\{0,1\}^l$ 为一安全无碰撞的 Hash 函数. $PK=(n,h_1,h_2,x,H)$, $SK=(p,q)$.

签名.设待签名的消息为 m,随机选取一个长为 $(l+1)$bit 的素数 e 以及长为 l bits 的串 α;计算 y 使得 $y^e=xh_1^{\alpha}h_2^{\alpha\oplus H(m)} \bmod n$,签名为 (e,α,y).

验证.首先检验 e 是否是长为 $(l+1)$bits 的奇数, α 长是否为 l bits,然后验证 $y^e=xh_1^{\alpha}h_2^{\alpha\oplus H(m)} \bmod n$.

Fischlin 的改进方案为了达到随机化目的,选取了一个长为 l bits 的随机串 α,这有利于抵抗选择消息攻击.而且改进方案明显地去除了原方案中的冗余成分,提高了系统的效率.

2.3 Zhu-数字签名方案

最近,我们从有关文献中发现,早在 2001 年国内学者朱华飞[1]就曾提出了一个与 Fischlin 的改进方案极其相似的协议:

建立.选取 $n=pq$,其中 $p=2p'+1$, $q=2q'+1$, p,p',q,q' 均为素数;记 QR_n 为 Z_n 中的二次剩余构成的群,随机选取三个生成元 $X,g,h\in QR_n$, $H(\cdot):\{0,1\}^*\rightarrow\{0,1\}^l$ 为一安全无碰撞的 Hash 函数. $PK=(n,g,h,X,H)$, $SK=(p,q)$.

签名.设待签名的消息为 m,随机选取一个长为 $(l+1)$bits 的素数 e 以及长为 l bits 的串 t;计算 y

使得 $y^e = Xg^t h^{H(m)} \bmod n$. 签名为$(e,t,y)$.

验证. 首先检验 e 是否是长为$(l+1)$bits 的奇数,然后验证

$$y^e = Xg^t h^{H(m)} \bmod n.$$

3　新改进方案

3.1　新改进方案的描述

Fischlin-方案和 Zhu-方案都引进了另一个公开参数(前者是 h_1,后者是 g),通过选取随机串 α(后者为 t),增强了系统抵抗选择消息攻击的能力. 事实上我们能够通过更简单的办法来实现这一目的,进一步去除冗余成分,提高系统的效率. 下面我们给出一个改进方案:

建立. 选取$n=pq$,其中 $p=2p'+1$,$q=2q'+1$,$|p|=|q|=512$ bits,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中的两个生成元 X,g. $H(\cdot):\{0,1\}^* \to \{0,1\}^{256}$ 为一安全无碰撞的 Hash 函数. $PK=(n,g,X,H)$,$SK=(p,q)$.

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

验证. 首先检验 e 是否是长为 257 bits 的奇数,然后验证

$$y^e = Xg^{H(m\|e\|X)} \bmod n.$$

定理 1.　上述协议中的每一步都能够实现,最后得到的签名能够通过验证.

证明.　由于签名人知道 n 的因子分解,可以求出 $\phi(n)$,从而计算出

$$d = e^{-1} \bmod \phi(n), \quad y = (Xg^{H(m\|e\|X)})^d \bmod n.$$

证毕.

3.2　效率分析

改进方案的效率要明显优于 Fischlin-签名方案和 Zhu-签名方案,具体情况如表 1 所示.

表 1　三种签名方案的比较

	Fischlin-签名方案	Zhu-签名方案	新改进方案
公钥	(n,x,h_1,h_2)	(n,X,g,h)	(n,X,g)
私钥	(p,q)	(p,q)	(p,q)
随机数	素数e,随机串α	素数e,随机串t	奇数e
签名	(e,α,y)	(e,t,y)	(e,y)
验证等式	$y^e = xh_1^{\alpha}h_2^{\alpha \oplus H(m)}$	$y^e = Xg^t h^{H(m)}$	$y^e = Xg^{H(m\|e\|X)}$

从表 1 中可以看出新改进方案少选了一个生成元,且签名时少选了一个随机串,验证方程中也少了一个幂运算. 因此,在同等规格的模数下,原方案与新方案的计算量之比约为 3∶2. 此外,原方案要求随机选取的 e 为素数,而新方案只要求 e 为奇数,无需进行素性检验. 故此,总的计算量约为原方案的1/2.

注记 1. 在原方案中,如果 e 为合数,不妨设 $e=ab$,则(a,t,y^b)和(b,t,y^a)都是关于同一消息的合法签名. 新方案则在验证等式中把 $H(m)$换成了 $H(m\|e\|X)$,利用 Hash 函数构造了一个新挑战,有效地抵制了上述攻击,去掉了素数要求.

注记 2. 在 Fischlin-方案和 Zhu-方案中分别记$\hat{X}=xh_1^{\alpha}h_2^{\alpha}$,$\overline{X}=Xg^t$,则相应的验证方程为

$$y^e = \hat{X}h_2^{H(m)}, \quad y^e = \overline{X}h^{H(m)} \pmod n.$$

由于$\hat{X}$,$\overline{X}$对攻击者而言都是已知的,所以这两个方案可以看成是改进方案的一种简单变型,但其安全性明显要弱于改进方案. 改进方案利用 Hash 函数的随机性,通过 $H(m\|e\|X)$把消息 m,签名数据 e 和公开参数 X 绑定在一起,有利于抵抗自适应选择消息攻击.

3.3　安全性分析

命题 1.　上述改进方案在自适应选择消息攻击(adaptive chosen-message attack)下能够抵抗存在型伪造(existential forgery).

证明.　我们首先解释在自适应选择消息攻击下攻击者 A 的攻击能力. 此时,攻击者 A 能够多次(在多项式时间内)访问签名预言机 SO(Signing Oracle),有一条记录带,把每次提交的询问 m_i和得到的回答(e_i,y_i)记录下来. 在每次提交新的询问时,A 能够根据先前的记录自主选择所提交的询问. 为了叙述方便,把 A 在攻击中的记录记为

$$\{(m_i,e_i,y_i):1 \le i \le t\},$$

可以假定 A 每次提交的询问是不相同的($i \ne j$,则 $m_i \ne m_j$). 现在需证:攻击者在经过多次询问后,得不到一合法的消息/签名(m,e,y)(m 不能作为 A 提交的询问),使得

$$y = (Xg^{H(m\|e\|X)})^d \bmod n.$$

为此,根据 A 找到的 e,y 分两种攻击类型加以讨论.

攻击 1. 根据攻击者得到的 e,只需考虑

(I) 存在某个 $i(\le t)$,使得 $e=e_i$. 此时又可分为两种情况:

(I_1) 如果 $H(m_i\|e_i\|X)=H(m\|e_i\|X)$,则

由于 $m \neq m_i$，$m_i \| e_i \| X \neq m \| e_i \| X$，从而 A 找到了 H 的一对碰撞. 由于在 ROM 模型下总是假设 H 是一理想的随机函数，故此，攻击者成功的概率 $Adv_{SO}(Q,R,t) \leq 1/2^{255}$，其中

$$Q=\{m_1,m_2,\cdots,m_t\},$$

$$R=\{(e_1,y_1),(e_2,y_2),\cdots,(e_t,y_t)\}.$$

(I_2) 如果 $H(m_i \| e_i \| X) \neq H(m \| e_i \| X)$，则显然有 $y_i \neq y \bmod n$. 不妨设 $H(m \| e_i \| X) > H(m_i \| e_i \| X)$，记 $H(m \| e_i \| X) - H(m_i \| e_i \| X) = \alpha$，由

$$y^{e_i} = Xg^{H(m \| e_i \| X)} \bmod n,$$

$$y_i^{e_i} = Xg^{H(m_i \| e_i \| X)} \bmod n,$$

可得 $(yy_i^{-1})^{e_i} = g^{H(m \| e_i \| X) - H(m_i \| e_i \| X)} = g^{\alpha} \bmod n$. 由于 $|e_i|=257$，$|\alpha| \leq 256$，所以 $e_i \neq \alpha$. 在已知 n, e_i, g^{α} 的情形下，攻击者找到合乎要求的 y 等同于解密利用 RSA 加密的 (yy_i^{-1})，加密指数为 e_i. 这与 RSA 的基本假设相矛盾.

(II) 对 $\forall i \leq t$，都有 $e \neq e_i$. 此时又可分为两种情况：

(II_1) 如果 $\exists i \leq t$，使得 $H(m_i \| e_i \| X) = H(m \| e \| X)$，则同 ($\mathrm{I}_1$) 一样，攻击者 A 能够找到 H 的一对碰撞，这与 ROM 模型下假设 H 是一理想的随机函数相矛盾.

(II_2) 如果 $\forall i, 1 \leq i \leq t$，都有 $H(m_i \| e_i \| X) \neq H(m \| e \| X)$，由于 $\{e_i\}_{1 \leq i \leq t}$ 是随机选取的，故 $\exists i$，$1 \leq i \leq t$，使得 $e_i > e$，从而根据

$$y^{e} = Xg^{H(m \| e \| X)} \bmod n,$$

$$y_i^{e_i} = Xg^{H(m_i \| e_i \| X)} \bmod n,$$

可得 $(yy_i^{-1})^{e} = g^{H(m \| e \| X) - H(m_i \| e_i \| X)} y_i^{e_i - e} \bmod n$. 在已知 $n, e, H(m \| e \| X), H(m_i \| e_i \| X), y_i^{e_i - e}$ 的情形下，攻击者 A 找到合乎要求的 y 就等同于解密利用 RSA 加密的 (yy_i^{-1})，加密指数为 e. 这与基本假设相矛盾.

也就是说，利用攻击者得到的 e，可以把攻击算法归约到 RSA 解密问题，然而在目前分解大数能力的条件下，RSA 解密问题是十分困难的.

攻击 2. 根据攻击者得到的 y，此时由于 X, g 均是 QR_n 中的生成元，且满足

$$y^{e} = Xg^{H(m \| e \| X)} \bmod n,$$

故此存在 α 使得 $y = g^{\alpha} \bmod n$，从而在已知 X, g 的情况下攻击者必能找到 X 关于 g 的一种表示，即

$$X = y^{e} g^{-H(m \| e \| X)} = g^{\alpha e - H(m \| e \| X)} \bmod n,$$

但这与强 RSA 假设矛盾.

事实上，如果攻击者能够从前 t 次询问与回答中，对某个 $i(\leq t)$ 得到 y_i 关于 g 的表示，即有 α_i 使得 $y_i = g^{\alpha_i} \bmod n$，那么，令 $\alpha_i e_i - H(m_i \| e_i \| X) = \alpha e - H(m \| e \| X)$ 求出一整数 α 即可. 但在已知 y_i 和 g 的情况下求 α_i 与强 RSA 假设矛盾.

总之，在给定 y 的情况下，可以利用攻击者求解 e 的算法来构造另一算法解决强 RSA 问题，从而与强 RSA 假设矛盾.

4 结束语

本文改进了一个基于强 RSA 的数字签名方案，新方案的计算量只是原方案的 1/2，并且在强 RSA 假设下分析了新方案的安全性. 改进方案利用 Hash 函数的单向性构造了一个复合挑战，因而能够进行灵活的变形. 利用这一特点可以设计盲签名、部分盲签名等一些重要的数字签名方案，我们将在今后的工作中进一步介绍这方面的结果.

参 考 文 献

1 Zhu Hua-Fei. New digital signature scheme attaining immunity to adaptive chosen-message attack. Chinese Journal of Electronics, 2001, 10(4): 484～486

2 Diffie W., Hellman M. E.. New directions in cryptography. IEEE Transactions on Information Theory, 1976, IT-22(6): 644～654

3 Rivest R. L., Shamir A., Adleman L. M.. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 1978, 21(2): 120～126

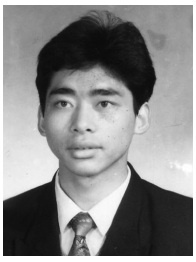
4 ElGamal T.. A public-key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 1985, 31(4): 469～472

5 Schnorr C. P.. Efficient identification and signatures for smart cards. In: Proceedings of Advances in Cryptology-Crypto'89, Berlin: Springer-Verlag, 1990, 239～251

6 Schneier B.. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2nd Edition. New York: Wiley, 1995, 521～522

7 Cramer R., Shoup V.. Signature schemes based on the strong RSA assumption. ACM Transactions on Information and System Security, 2000, 3(3): 161～185

8 Fischlin M.. The Cramer-Shoup Strong-RSA signature scheme revisited. In: Proceedings of the PKC 2003, Lecture Notes in Computer Science 2567, Berlin: Springer-Verlag, 2003, 116～129



CAO Zheng-Jun, born in 1971, Ph. D. candidate. His research interests include information security and cryptography.

LIU Mu-Lan, born in 1941, professor, Ph. D. supervisor. Her research interests include cryptography, information security and computer algebra.

Background

Digital signature is an important component of modern cryptography. It has greatly promoted the development of E-commerce. Lots of researchers have paid attention to the design and analysis of signature schemes. In this paper, the authors improve the signature scheme based on strong RSA proposed by Zhu. The original scheme should select three generators in QR_n in the setup phase. In signing phase, the signer must choose a prime number with prescribed length. The authors remove these restrictions. Only two generators and an odd should be selected in our scheme. The improvement scheme saves about 1/2 computation of the original scheme. The authors also prove its security under strong RSA assumption. The research is supported by the National Natural Science Foundation of China under grant No. 90304012 and National Basic Research Program (973 Program) of China under grant No. 2004CB318000. The research group is with Institute of Systems Sciences, Chinese Academy of Sciences. The group members have published a number of papers in international and internal journals and conferences about applied mathematics, cryptography and computer sciences, etc.