基于强 RSA 假设的签名方案*

汪保友[1,2], 胡运发[1]

[1](复旦大学 计算机科学与工程系,上海 200433);
[2](中国联通有限公司上海分公司,上海 200070)
E-mail: yfhu@fudan.edu.cn
http://www.fudan.edu.cn

摘要: 为了抵抗自适应选择信息攻击,提高签名生成效率,提出一种基于强 RSA 假设的签名方案.该方案与 RSA 算法的不同在于:它采用固定参数为指数底,明文信息的散列值为幂的指数函数;而 RSA 算法采用明文信息散列值为底,固定参数为幂的指数函数.在实现技巧上,可采用预先计算技术提高实现效率.此外,还选用陷门散列函数对基本签名方案进行改进,这个改进方案为签名算法提供散列陷门,其优点体现在,如果把签名过程分为"离线"和"在线"两部分,则签名者利用陷门,可显著提高"在线"的效率.可以证明,在强 RSA 假设下,此方案对自适应选择信息攻击是安全的.实验结果表明,该签名方案效率较高.

关 键 词: 数字签名;强 RSA 假设;散列函数;RSA;安全性
中图法分类号: TP309 **文献标识码**: A

本文介绍基于强 RSA 假设的数字签名方案.正如文献[1]中所定义的,安全即意味着能抵抗自适应选择信息攻击,这是数字签名方案中人们期望的最强的安全类型.能在这种情况下保证安全的数字签名方案,可以安全地部署于可能的最广泛的应用领域中.为证明本文方案的安全性,需要强 RSA 假设,此假设是由文献[2]最先提出的.此外还需要抗碰撞散列函数,实际上普通单向散列函数[3]已经足够.

本文方案的新颖性在于,它与文献[1,4]等一些可证明的安全方案不同,它是与状态无关的;而且比起这些方案,本文方案效率更高,所付出的代价是:要使用一个可能更强的假设.此外,在基本方案中选用陷门散列函数,得到的改进方案,用随机推测模型分析,在标准 RSA 假设下也是安全的.这意味着,我们的方案至少和标准 RSA 签名一样安全.本文第 1 节介绍一些相关概念.第 2 节介绍并分析基本的签名方案.第 3 节介绍并分析基于陷门散列函数的改进方案.第 4 节总结本文工作.

1 相关概念

1.1 RSA假设

RSA 问题如下:给定一个随机生成的 RSA 模数 n、指数 r 及随机数 $z\in Z_n^*$,找出 $y\in Z_n^*$,使得 $y^r=z$ 成立.指数 r 是从某个特定的概率分布中选择:特定的概率分布会产生特定形式的 RSA 问题.RSA 假设即假定 RSA 问题是难于求解的.

1.2 强RSA假设

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 $y^r=z$ 成立($r>1, y\in Z_n^*$).对指数

* 收稿日期: 2001-05-15; 修改日期: 2001-10-23
基金项目: 国家自然科学基金资助项目(69933010)
作者简介: 汪保友(1968-),男,安徽六安人,博士,工程师,主要研究领域为数字签名,电子商务,数字图书馆;胡运发(1940-),男,安徽合肥人,博士,教授,博士生导师,主要研究领域为数字图书馆,人工智能,数据与知识工程.

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 假设即是假定 flexible RSA 问题是难于求解的.它与普通的 RSA 假设的区别在于:RSA 假设,指数 r 的选择与 z 无关;而在强 RSA 假设中,指数 r 的选择可能与 z 有关.强 RSA 假设由文献[2]提出,随后被用在许多密码学方案的分析上.它可能是比 RSA 假设要求更强的假设,但迄今为止,要否定这两个假设,惟一的途径是找出求解整数因子分解问题的方法.

1.3 随机自缩减

RSA 问题有一个特性:随机自缩减(random self-reduction).即,已知 n 和 r,对任意的 $z\in Z_n^*$,计算 $y=z^{1/r}$ 的问题,可简化为:对任意的 $\tilde{z}\in Z_n^*$,计算 $\tilde{y}=\tilde{z}^{1/r}$.这意味着解决后一问题的有效算法,同样也可以有效地求解前一个问题.常见的缩减为:给定 z,随机选择 $s\in Z_n^*$,令 $\tilde{z}=s^r z$,则有 $y=\tilde{y}/s$.

随机自缩减特性的存在增强了 RSA 假设的可信度.这是因为如果存在一个算法,它对给定的 n 和 z 的部分取值,可求解 RSA 问题,则存在另一算法,针对同样的 n 和 z 的所有取值,可解 RSA 问题.Flexible RSA 问题也有随机自缩减特性,正如对 RSA 问题一样,这个随机自缩减特性,增强了强 RSA 假设的可信度.

1.4 自适应选择信息攻击

自适应选择信息攻击(adaptive chosen message attack)是一个“伪造算法”,其工作过程如下:当签名方案的密钥生成算法运行时,生成一个公钥,提供给伪造算法;生成一个私钥,提供给“指定签名者”.接着,伪造算法向指定签名者多次请求签名,每一次请求,伪造算法向指定签名者递交它所选择的信息;指定签名者对此信息签名,并向伪造算法传送这个签名.由于伪造算法在选择信息时是完全自由的;尤其是,伪造算法选择的信息可能与公钥有关,并可能与指定签名者以前的响应有关.最后,伪造算法产生伪造的签名,即信息没有提交给指定签名者,而能在此信息上附有有效的签名.当然,允许伪造算法失败,不能产生有效的伪造签名.

抗自适应选择信息攻击的安全性意味着:不存在“有效的”伪造算法,此算法生成有效伪造签名的成功概率“不可忽略”.

1.5 普通单向散列函数

普通单向散列函数簇(universal one-way family of Hash function,简称 UOWHFs)的概念是由文献[3]首先提出来的.具有如下性质的散列函数簇 H(按密钥 k 索引),称为普通单向散列函数簇.此性质为:如果攻击者选择信息 x,再随机选择密钥 k,则攻击者要找出一个 $y(y\neq x)$,而能使 $H_k(x)=H_k(y)$,将是非常困难的.

普通单向散列函数比起完全抗碰撞散列函数的属性要求要弱得多,从安全角度来看,基于这种弱要求的方案是令人满意的[5,6].注意,密钥 k 的长度可能随信息长度的增长而增长;对某些构造方式,增长率为对数级.

2 基本的签名方案

本节介绍基本的数字签名方案,再证明其安全性.

本方案可用两个安全参数 l 和 l' 表示,$l+1<l'$.比如选择 $l=160$,$l'=512$.方案中使用抗碰撞散列函数 H,H 的输出为小于 2^l 的正整数.推荐 H 选用安全散列算法 SHA-1.

对正整数 n,用 QR_n 表示模 n 的二次剩余.

密钥生成.选择两个 l' 位的随机素数 p 和 q,满足 $p=2p'+1$,$q=2q'+1$,p' 和 q' 都是素数.令 $n=pq$,再选择:

随机数 $h,x\in QR_n$;$l+1$ 位的随机素数 e'.

公钥是: (n,h,x,e').

私钥是: (p,q).

签名生成.为对信息 m 签名,选择一个 $l+1$ 位的随机素数 $e(e\neq e')$ 以及一个随机数 $y'(y'\in QR_n)$.

用方程式 $y^e=xh^{H(x')}$,求 y.其中 x' 满足方程式 $(y')^{e'}=x'h^{H(m)}$.

注意,可用私钥中 n 的分解因子计算 y.

签名是: (e,y,y').

签名验证.为验证信息 m 上签名 (e,y,y') 的真伪,步骤如下:

(1) 检查 e 是否是与 e'不同的 l+1 位奇数.

(2) 计算 $x'=(y')^{e'}h^{-H(m)}$.

(3) 检查 $x=y^e h^{-H(x')}$ 是否成立.

2.1 实现技巧

我们注意到,签名验证算法不需要证明 e 是素数.为提高签名验证和签名的速度,公钥中 h 可用 h^{-1}代替.

在生成签名过程中,计算 y 时的取幂运算可用如下方法大幅降低.首先选择随机数 a,令 $x=h^a \bmod p'q'$,把 a 存储在私钥中.这是可以接受的,因为 h 是 QR_n 的生成元的概率极大,由此产生的公钥概率分布并没有很大的改变.如果 $d=e^{-1} \bmod p'q'$,则 $y=h^b$,这里 $b=da+dH(x') \bmod p'q'$.因此,计算 y 的取幂运算是底数固定为 h 的 b 次幂.采用预先计算技术[7],使用预先计算的数值表,可充分降低模乘法的数量.

2.2 安全性证明

下面证明上述方案的安全性.

定理 1. 在强 RSA 假设及假定 H 是抗碰撞散列函数时,上述的签名方案对自适应选择信息攻击是安全的.

在证明定理 1 之前,为方便起见,先介绍下面的引理[8].

引理 1. 给定 $x,y\in Z_n^*$以及 $a,b\in Z$,满足 $x^a=y^b$,$\gcd(a,b)=1$,则可求解 $\tilde{x}\in Z_n^*$,使得 $\tilde{x}^a=y$.

为证明这个引理,可用扩展 Euclidean 算法,求解整数 b'和 k,使得 $bb'=1+ak$.简单的推算后表明 $\tilde{x}=x^{b'}y^{-k}$ 可满足此要求.引理 1 证毕. □

再回到定理 1 的证明.假定伪造算法做了 t 次签名请求后,能伪造签名.对 $1\le i\le t$,令 m_i 是第 i 次待签名的信息,(e_i,y_i,y_i')是第 i 次签名,$x_i'=(y_i')^{e'}h^{-H(m_i)}$.令$(e,y,y')$是信息 m 的伪造签名(此 m 是对所有的 $1\le i\le t$),$x'=(y')^{e'}h^{-H(m)}$.我们把伪造的类型分为 3 种:

类型Ⅰ. 对某些 $1\le j\le t, e=e_j, x'=x_j'$.

类型Ⅱ. 对某些 $1\le j\le t, e=e_j, x'\ne x_j'$.

类型Ⅲ. 对所有 $1\le i\le t, e\ne e_i$.

假定没有两个 e_i 相等,因此一个伪造签名只有一种类型.假定所有的 e_i 都不等于 e'.

如果有一个成功概率不可忽略的伪造者,则存在一个类型Ⅰ、类型Ⅱ或类型Ⅲ的伪造者,其获得成功的概率不可忽略.我们将证明任何一类伪造者都会成为否定强 RSA 假设的算法.事实上,类型Ⅰ、类型Ⅱ的伪造者能否定 RSA 假设,其证明和文献[4]中证明的非常相似.只有对类型Ⅲ的伪造者,才需要用到强 RSA 假设.

类型Ⅰ的伪造者

假定有类型Ⅰ的伪造者,其成功的概率不可忽略.我们要说明怎样利用这个伪造者,求解 RSA 问题.即,给定 n,一个随机数 $z\in Z_n^*$以及一个 l+1 位的随机素数 r,计算 $z^{1/r}$.

首先描述一个模仿伪造者的模拟器.选择 l+1 位的随机素数 $e_1,\ldots,e_t$,按如下方式创建公钥.令 $h=z^{2P_1e_1}$;再随机选择 $w\in Z_n^*$,令 $x=w^{2P_1e_1}$;最后,令 $e'=r$.

为给信息 m_i 签名,模拟器随机地选择 $y_i'\in QR_n$,计算 $x_i'=(y_i')^{e'}h^{-H(m_i)}$.接着,模拟器用方程式 $y_i^{e_i}=xh^{H(x_i')}$ 求解 y_i,此方程是易解的,原因在于 x 和 h 的 e_i 次方根是已知的.

容易看出,这个模拟器可以很好地模拟伪造者的行为.

假定伪造者在信息 m 上产生类型Ⅰ的伪造签名(e,y,y').即,对某些 $1\le j\le t, e=e_j$ 和 $x'=x_j'$,产生两个方程式:$(y')^{e'}=x'h^{H(m)}$ 和 $(y_j')^{e'}=x'h^{H(m_j)}$.

因为假定 H 是抗碰撞的,因此可假定 $H(m)\ne H(m_j)$.两个方程式相除,可求解 $v\in Z_n$ 及整数 $a\ \ 0 \pmod{e'}$,满足下式:$v^{e'}=h^a=z^{2aP_ie_i}$.

又因为 $\gcd(2a\tilde{O}_ie_i,e')=1$,$e'=r$.应用引理 1,容易计算 z 的 r 次方根.这违反了 RSA 假设.

类型Ⅱ的伪造者

与类型Ⅰ一样,类型Ⅱ的伪造者也可用来求解 RSA 问题:给定 $n,z\in Z_n^*$以及 r,计算 z 的 r 次方根.

可以假定:类型Ⅱ伪造者中定义的 j 值是固定的;如果不固定,我们可以猜测出.

我们再来描述一个模拟器,按如下方式创建公钥:

对 $1\le i\le t(i\ne j)$,选择 l+1 位的随机素数 e_i,令 $e_j=r$.再选择 l+1 位的随机素数 e',令 $h=z^{2e'\prod_{i\ne j}e_i}$.

随机选择 $w\in Z_n^*$,令 $y_j=w^{2\prod_{i\ne j}e_i}$.

随机选择 $u\in Z_n^*$,令 $x_j'=u^{2e'}$.

计算 $x=y_j^{e_j}h^{-H(x_j')}$.

接着,我们描述怎样给信息 m_i 签名.首先,假定 $i\ne j$.随机选择 $y_i'\in QR_n$,计算 $x_i'=(y_i')^{e'}h^{-H(m_i)}$.因为我们已知 x 和 h 的 e_i 次方根,所以容易计算对应的 y_i 值.其次,假定 $i=j$.因为我们已知 h 和 x_j' 的 e' 次方根,容易求解 y_j'.而 y_j 值已经确定.

至此,我们完成了对模拟器的描述.容易看出,此模拟器能很好地模拟伪造者的行为.

现在假定伪造者在信息 m 上做了类型 II 的伪造签名(e,y,y').这里 $e=e_j,x'\ne x_j'$,则有

$$y^e=xh^{H(x')},$$

$$y_j^{\ e}=xh^{H(x_j')}.$$

与类型 I 的讨论类似,我们可以把两个方程式相除,来计算 z 的 r 次方根.这违反了 RSA 假设.

类型III的伪造者

给定类型III的伪造者,我们要说明怎样利用它去求解 felxible RSA 问题.即已知 $n,z\in Z_n^*$,要计算 $r(r>1)$以及 z 的 r 次方根.

模拟器运行过程如下:随机选择 l+1 位素数 $e',e_1,\ldots,e_t$,令 $h=z^{2e'\prod_i e_i}$.

再选择一个随机数 $a\in\{1,\ldots,n^2\}$,令 $x=h^a$.

构造 QR_n 为 $p'q'$阶循环群.可以假定 h 是 QR_n 的生成元,因为其发生的概率相当大.

令 $a=bp'q'+c$,其中 $0\le c<p'q'$.因为 a 是在较大的区间里随机选择.从统计角度来看,c 的概率分布和 $\{0,\ldots,p'q'-1\}$区间上的均匀分布不可区分.而且,在 c 值给定的情况下,b 的条件概率分布和$\{0,\ldots,\lfloor n^2/p'q'\rfloor\}$区间上的均匀分布也是不可区分的.即 c 和 b 基本上是相互独立的.

因为 c 的概率分布基本上是均匀分布的,所以 x 基本上是 QR_n 中的随机元素.因为 x 和 h 所有相关的方根值已知,所以容易对所有的信息进行签名.

现在,假定伪造者产生一个类型III的伪造签名(e,y,y').则有

$$y^e=xh^{H(x')}=z^m.$$

这里,$m=2e'P_ie_i(a+H(x'))$.

令 $d=\gcd(e,m)$.因 $\gcd(d,2p'q')=1$ 意味着 $y^{e/d}=z^{m/d}$,假定 $e\nmid m$(即 e 不能整除 m),可用引理 1 中的算法计算 z 的 (e/d)次方根,因此 $e\nmid m$ 的概率不可忽略.令 r 是除 e 的素数,可构造 $r\mid 2e'P_ie_i$,则 $r\mid(a+H(x'))$的概率不可忽略.证明如下:令 $a=bp'q'+c$(同上).r 可能与 c 有关,而由前面结果可知,c 和 b 基本上是不相关的.可构造 $r\mid p'q'$,由此可得 $a+H(x')\equiv 0(\mathrm{mod}\ r)$的概率非常接近于 $1/r$.因此,$r\mid(a+H(x'))$的概率不可忽略.可用引理 1 中的算法计算 z 的 r 次方根,这违反了强 RSA 假设.

3 利用陷门散列函数的改进签名方案

回顾前面介绍的基本签名方案和信息 m 上的签名(e,y,y').令 $x'=(y')^{e'}h^{-H(m)}$,则有 $y^e=xh^{H(x')}$.可以把 $H(x')$看做为"陷门散列函数".陷门散列函数也可基于离散对数问题难解假设,按如下标准方式构造:令 g_1,g_2 是 s 阶 G 群的两个随机生成元(s 是 l+1 位的素数).为计算信息 m 的 hash 值,我们计算 $a,a=H(g_1^tg_2^{H(m)})$,这里 H 是普通的、抗碰撞的散列函数,t 的值等于随机选择的数 mod s.除了 hash 值 a,还输出附加信息 t.此方案的陷门是 g_2 为底 g_1 的对数.知道陷门的模拟器可以在不知道 m 的情况下求解 a;继而,给定 m,还可求解对应的附加信息 t.下面是基于陷门散列函数的签名方案.

密钥生成.选择两个 l'位的随机素数 p 和 q,满足 $p=2p'+1,q=2q'+1,p'$和 q'都是素数.令 $n=pq$,还需要选择:

随机数 $h,x\in QR_n$;

s 阶的 G 群,这里 s 是 l+1 位的随机素数,及 G 群的两个随机生成元 g_1 和 g_2.

公钥是: (n,h,x,g_1,g_2)连同 G 群(包括 s)的适当描述.

私钥是: (p,q).

签名生成.为在信息 m 上签名,要选择 l+1 位的随机素数 e 和随机数 $t\in Z_s$.

用方程式 $y^e = xh^{H(g_1^t g_2^{H(m)})}$,求 y.

签名是:(e,y,t).

签名验证.为验证信息 m 上签名(e,y,t)的真伪,首先检查 e 是否为 l+1 位奇数.其次,检查 $x = y^e h^{-H(g_1^t g_2^{H(m)})}$ 是否成立.

定理 2. 在强 RSA 假设、假定 H 是抗碰撞散列函数以及假设求 G 群的离散对数问题是困难的前提下,上述签名方案,对抵抗自适应选择信息攻击是安全的.

这个定理的证明和定理 1 的证明非常相似.详细证明略.

这个改进方案为签名算法提供了 hash 陷门.它的优点体现在,如果把签名代价分为"离线"和"在线"两部分,签名者用这个陷门,则"在线"的代价基本上是一次简单的模 s 乘法,生成签名的所有其他工作都可在实际接收到信息 m 以前完成.

4 结束语

本文介绍基于强 RSA 假设的签名方案.该方案与 RSA 算法的不同在于:它采用固定参数为指数底,明文信息的散列值为幂的指数函数;而 RSA 算法采用明文信息散列值为底,固定参数为幂的指数函数.在实现技巧上,可采用预先计算技术提高实现效率.此外,我们选用陷门散列函数对基本签名方案进行改进.这个改进方案为签名算法提供散列陷门,其优点体现在:如果把签名过程分为"离线"和"在线"两部分,则签名者利用陷门,可以显著提高"在线"的效率.可以证明,在强 RSA 假设下,此方案对自适应选择信息攻击是安全的.

文中描述的思想初步得以实现,其中普通单向散列函数是利用安全散列算法 SHA-1 构造的[6].签名算法分为两个阶段:密钥组织阶段和主要签名阶段.在密钥组织阶段,对给定的签名密钥,只需要运行 1 次.这一阶段生成一些数值表,可用在主要签名阶段,加速求幂运算.程序实现是采用 Visual C++ 6.0,实验环境为 Dell P II 工作站,型号 OptiPlex GX1,运行 Microsoft Windows 2000 操作系统.实验结果见表 1 和表 2.

Table 1 The times of basic arithmetic operations (as a baseline)

表 1 基本算术运算时间(作为比较基准)

Bits① \ Basic operations②	Modular multiplication③ (μs)	Squaring operation④ (μs)	Exponentiation⑤ (ms)
512	340	320	180
1 024	1 030	1 000	1 180

①位数,②基本运算,③模乘法运算,④平方运算,⑤求幂运算.

Table 2 The times of the algorithms

表 2 算法运行时间

Modulus① \ Phase②	Key set-up phase③ (ms)	Main signing phase④ (ms)	Signature verification⑤ (ms)
1 024	310	500	570

①模数,②阶段,③密钥组织阶段,④主要签名阶段,⑤验证签名.

致谢 感谢审稿人对本文非常中肯的评审意见.

References:

[1] Goldwasser, S., Micali, S., Rivest, R.L. A digital signature scheme secure against adaptive chosen-message attacks. SIAM Journal on Computing, 1988,17(2):281~308.

[2] Baric, N., Pfitzmann, B. Collision-Free accumulators and fail-stop signature schemes without trees. In: Fumy, W., ed. Proceedings of the Conference on Advances in Cryptology (EUROCRYPT' 97). Berlin, New York: Springer-Verlag, 1997. 480~494.

[3] Naor, M., Yung, M. Universal one-way hash functions and their cryptographic applications. In: Johnson, D.S., ed. Proceedings of the 21st Annual ACM Symposium on Theory of Computing (STOC' 89). Seattle, WA, New York: ACM Press, 1989. 33~43.

[4] Cramer, R., Amgaard, I. New generation of secure and practical RSA-based signatures. In: Koblitz, N., ed. Proceedings of the 16th Annual International Conference on Advances in Cryptology (CRYPTO' 96). Santa Barbara, CA, New York: Springer-Verlag, 1996. 173~185.

[5] Bellare, M., Rogaway, P. Collision-resistant hashing: towards making UOWHFs practical. In: Proceedings of the 17th Annual International Conference on Advances in Cryptology (CRYPTO' 97). Santa Barbara, CA, New York: Springer-Verlag, 1997.

[6] Shoup, V. A composition theorem for universal one-way hash functions. In: Proceedings of the Workshop on Advances in Cryptology (EUROCRYPT 2000). New York: Springer-Verlag, 2000.

[7] Lim, C.H., Lee, P.J. More flexible exponentiation with precomputation. In: Desmedt, Y.G., ed. Proceedings of the Conference on Advances in Cryptology (CRYPTO' 94). Santa Barbara, CA, New York: Springer-Verlag, 1994. 95~107.

[8] Guillou, L.C., Quisquater, J.J. A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory. In: Günther, C.G. ed. Proceedings of the Conference on Advances in Cryptology (EUROCRYPT' 88). Davos, Switzerland, New York: Springer-Verlag, 1988. 123~128.

A Signature Scheme Based on the Strong RSA Assumption*

WANG Bao-you[1,2], HU Yun-fa[1]

[1](*Department of Computer Science and Engineering, Fudan University, Shanghai* 200433, *China*);

[2](*China UniCmm Limited Shanghai Branch, Shanghai* 200070, *China*)

E-mail: yfhu@fudan.edu.cn

http://www.fudan.edu.cn

Abstract: For resisting the adaptive chosen message attack and improving the sign generation efficiency, a signature scheme based on the strong RSA assumption is described in this paper. The scheme uses a fixed base rather than by raising them to a fixed power, which is different from the RSA algorithm. Moreover, one can use pre-computation techniques in order to get a better efficiency. In addition, a hash function can be incorporated into the scheme in such a way that it offers a trapdoor to the sign algorithm. The merits of this amendatory scheme are that if one makes a distinction between the "off line" and the "on line" cost of signing, the signer can reduce "on line" cost significantly by using hash trapdoor. It is proved that the scheme is secure against the adaptive chosen message attack under the strong RSA assumption. The experimental results show that the scheme has high efficiency.

Key words: digital signature; strong RSA assumption (SRA); hash function; RSA; security

* Received May 15, 2001; accepted October 23, 2001

Supported by the National Natural Science Foundation of China under Grant No.69933010