

文章编号:1001-9081(2010)04-1042-03

数字签名方案的同底构造攻击

陈宁宇, 顾永跟, 苏晓萍

(湖州师范学院 信息与工程学院, 浙江 湖州 313000)

(nychen@hutc.zj.cn)

摘要:在数字签名中,由于签名因子或整个签名方案设计的不合理,使得攻击者很容易通过将签名验证等式进行变形,将其转换成一个同底的等式,并通过指数的相等伪造出签名数据。针对此问题,提出同底构造攻击的概念,并明确指出,在进行数字签名设计时,必须回避这种现象。通过实例说明了这些例子中签名协议设计的不安全性,并给出一些通用方法说明如何对这些签名方案进行改进。

关键词:同底构造;代理签名;群签名;盲签名;公钥

中图分类号: TP309 **文献标志码:** A

Identical base construction attack on digital signature scheme

CHEN Ning-yu, GU Yong-gen, SU Xiao-ping

(School of Information and Engineering, Huzhou Teachers College, Huzhou Zhejiang 313000, China)

Abstract: This paper studied many digital signature schemes and had found them insecure because of the irrationality of these signature factors or the whole signature scheme, which made the attackers be able to transform the signature verification equation into a equation with the same base number and easily forge signature datum through the equation of the two exponents. The paper proposed a new concept: the attack based on identical base construction, and explicitly indicated that defects could be avoided in designing digital signature. Meanwhile, four examples were given to illustrate the insecurity in signature designing. Finally, some general ways to improve these signature schemes were provided

Key words: identical base construction; proxy signature; group signature; blind signature; public key

0 引言

随着公钥密码学^[1]在20世纪70年代末的诞生,基于公钥基础设施(Public Key Infrastructure, PKI)的数字签名技术也应运而生。数字签名必须满足一些基本要求,即:签名是可信的,签名是不可伪造的,签名是不可重用的,签名的文件是不可改变的,签名是不可抵赖的。在数字签名的实现过程中,采用公开密码算法对长文件签名效率太低。为了提高效率,数字签名协议经常和Hash函数相结合,即用Hash函数先产生消息的摘要,或者称之为指纹,然后再对消息摘要进行签名,这样使得伪造者不能把消息和它的签名剥离开来。

除了普通数字签名之外,很多具有特殊用途的数字签名也被提了出来,如盲签名、代理签名和群签名等。当前,大部分签名方案都是基于离散对数和RSA的。这意味着,对一个安全的签名体制而言,攻击者如果要伪造签名,则必须解决大数离散对数问题或者是大数因子分解问题。但在实际构造签名协议时,由于构造者考虑的问题不够周全或者是一味追求签名协议的高效,使得签名协议并不安全。如文献[2]作者指出,如果签名协议中存在孤悬因子,那么别人就很轻易伪造出签名。

对于任何一个签名协议而言,签名验证的有效性是通过等式来实现的,在等式里面的所有数据中,有些是公钥数据,其余则是签名数据。而且,等式中往往存在 x^y 这样一些因

子。签名数据可能在底数 x 上,也可能在指数 y 上。如果一个签名协议设计得不合理,很容易构造出满足等式的签名数据而伪造签名。

定义 在数字签名验证等式中,如果可以将验证等式 $M = M'(\bmod n)$,或者从验证等式中抽取的某部分伪造成 $M = M'(\bmod n)$,经过一系列变换成为 $g^m = g^{m'}(\bmod n)$,而签名数据或者部分数据包含在 m 或 m' 中(m 和 m' 中不再含有高次剩余或离散对数求解问题),这样就能由 $m = m'$ 伪造出签名数据,本文称之为同底构造攻击。

例 在1.1节的签名方案中,验证等式实际上是 $e' = h(g^{S_p} g^{y_B e'}, m)(\bmod p)$,其中 g 和 y_B 是公钥数据,而 S_p 和 e' 是对消息 m 的签名。这样就可以随意构造 $g^\delta = g^{S_p} g^{y_B e'}$,得到 e' 的值为 $h(g^\delta, m)$,由同底关系得到 $\delta = S_p + y_B e'(\bmod q)$ 求得 S_p 的值,从而伪造签名。

因此,在签名协议设计时,对这些签名数据的设计是非常重要的。否则,攻击者将避开求解高次剩余或离散对数,利用同底构造攻击伪造出签名。本文结合四个有代表性的具体签名协议,围绕同底构造攻击,指出这些签名协议设计的不安全性。

1 Awasthi-Lal 签名方案与分析

文献[3]作者在1996年首次提出了代理签名的概念,即:在一个代理签名方案中,一个被指定的代理签名人 can 代表原

收稿日期:2009-08-18;修回日期:2009-11-12。

作者简介:陈宁宇(1974-),男,江西修水人,讲师,硕士研究生,主要研究方向:信息安全、密码学、并行计算;顾永跟(1967-),男,浙江湖州人,教授,博士研究生,主要研究方向:信息安全、形式化方法;苏晓萍(1971-),女,浙江青海人,副教授,硕士,主要研究方向:移动计算、网络QoS。

始签名人进行有效的代理签名。盲签名^[4]是一种特殊的数字签名技术,除了满足一般的数字签名技术的基本特征外,还必须满足:1)盲性,即签名者不知道所签文件或消息的具体内容;2)不可追踪性,在签名的文件或消息被拥有者公布后,签名者不能追踪签名。2002年,文献[5]作者引入了代理盲签名的概念,以便签名同时拥有代理签名和盲签名的特点。

1.1 Awasthi-Lal 签名方案

文献[6]的第二个签名方案是一个代理盲签名方案。签名系统由3部分组成,即原始签名者A、代理签名者B和签名接收者C。

初始化阶段 p, q 为两安全大素数且 $q \mid p-1, g \in \mathbf{Z}_p^*$ 且阶为 $q, x_A, x_B \in \mathbf{Z}_q^*$ 分别代表A和B的私钥, $y_A = g^{x_A} \bmod p, y_B = g^{x_B} \bmod p$ 分别代表A和B的公钥。 $h(\cdot)$ 为一安全的哈希函数。

代理阶段 A 随机选取 $k \in \mathbf{Z}_q^*$, 计算 $r = g^k \bmod p, \sigma = x_A + k \cdot r \bmod q$ 和 $y_p = g^{rB} \bmod p$, A 秘密发送 (σ, r) 给B。B 接收到 (σ, r) 后, 验证 (σ, r) 的有效性, 计算 $s = \sigma + x_B \bmod q$ 。

签名阶段 B 随机选择 $K \in \mathbf{Z}_q^*$, 计算 $R = g^K \bmod p$ 并发送 R 给C。C 随机选择 $\alpha, \beta \in \mathbf{Z}_q^*$, 计算 $r' = Rg^{-\alpha}y_p^{-\beta} \bmod p, e' = h(r', m) \bmod q, e = e' + \beta \bmod q$, 发送 e 给B。B 收到 e 后, 计算 $s' = K - s \cdot e \bmod q$, 并发送 s' 给C。现在C计算 $S_p = s' + \alpha \bmod q$, 则 (m, S_p, e') 就是代理盲签名。

验证阶段 任何人都可以计算 $e' = h(g^{S_p}y_p^{e'} \bmod p, m)$ 来验证签名的有效性。

1.2 分析

在此签名方案中,所有人都可计算 $y_p = g^{rB} \bmod p$, 所以实际的签名验证等式是: $e' = h(g^{S_p}g^{rB}, m) \bmod p$ 。显然,任何人都可以利用同底构造攻击伪造签名。对于消息 m , 随机选取 $\delta \in \mathbf{Z}_q^*$, 计算得到 e' 的值为, $e' = h(g^\delta, m) \bmod p$ 。利用 $g^{S_p} \cdot g^{rB} = g^\delta \bmod p$, 由同底关系得到 $S_p = \delta - y_B e' \bmod q$, 因此得到的 (m, S_p, e') 就是有效签名。

正确性 $h(g^{S_p}y_p^{e'}, m) = h(g^{S_p}g^{rB}, m) = h(g^\delta, m) = e' \bmod p$ 。

2 Duc-Cheon-Kim 签名方案与分析

2.1 Duc-Cheon-Kim 签名方案

为了减轻密钥泄密后带来的严重后果, Anderson 于1997年提出了前向安全签名的概念。文献[7]是一个前向安全的盲签名方案。

1) 系统建立。产生两个安全大素数 p 和 q , 计算 $N = pq, \varphi(N) = (p-1)(q-1)$ 。产生和 $\varphi(N)$ 互素的随机数 λ , 选取 $a \in \mathbf{Z}_N^*$ 且其阶大于 λ 。选取 $r_0 \in \mathbf{Z}_\lambda^*, s_0, e \in \mathbf{Z}_N^*$, 计算: $V = a^{-r_0} s_0^{-\lambda} \bmod N, f_1 = a^e \bmod N, v_1 = V^2 a^e \bmod N, l = (2r_0 - e) \div \lambda, r_1 = (2r_0 - e) \bmod \lambda, s_1 = a^l s_0^2 \bmod N$, 则私钥为: $SK_1 = (1, r_1, s_1, v_1, f_1)$, 公钥为: $PK = (N, a, V, \lambda)$ (记号 \div 表示: 如果 $a = qb + r$, 则 $a \div b = q$)。

密钥更新, 若在 i 时刻的私钥为 (i, r_i, s_i, v_i, f_i) , 选取 $e \in \mathbf{Z}_N^*$, 计算: $v_{i+1} = v_i^2 a^e \bmod N, f_{i+1} = f_i^2 a^e \bmod N, l = (2r_i - e) \div \lambda, r_{i+1} = (2r_i - e) \bmod \lambda, s_{i+1} = a^l s_i^2 \bmod N$, 则在 $i+1$ 时刻的私钥为 $(i+1, r_{i+1}, s_{i+1}, v_{i+1}, f_{i+1})$, 公钥则保持不变。

2) 签名过程

a) Signer 选取 $t \in \mathbf{Z}_\lambda^*, u \in \mathbf{Z}_N^*$, 计算 $x = a^u u^\lambda \bmod N$, 发送 x 给 User。

b) User 选取盲因子 $\alpha, \gamma \in \mathbf{Z}_\lambda^*$ 和 $\beta \in \mathbf{Z}_N^*$, 计算: $x' = xa^\alpha \beta^\lambda v_i^\gamma \bmod N, c' = H(i \| f_i \| m \| x'), c = c' - \gamma \bmod \lambda$, 发送 c 给 Signer (\parallel 表示比特的串)。

c) Signer 计算: $y = t + cr_i \bmod \lambda, \omega = (t + cr_i) \div \lambda, z = a^\omega u s_i^c \bmod N$, 发送 y, z 给 User。

d) User 计算: $y' = (y + \alpha) \bmod \lambda, \omega' = (y + \alpha) \div \lambda, \omega'' = (c' - c) \div \lambda, z' = a^{\omega'} v_i^{-\omega''} z \beta \bmod N$, 得到消息 m 的盲签名为: (f_i, c', y', z') 。

验证, 对于给定公钥 (N, a, V, λ) 和签名 (f_i, c', y', z') , 计算: $v_i = V^{2i} f_i \bmod N, x'' = a^{y'} z'^\lambda v_i^{c'} \bmod N$, 如果 $c' = H(i \| f_i \| m \| x'')$, 则接受签名。

2.2 分析

签名验证方程实际上是:

$$c' = H(i \| f_i \| m \| a^{y'} z'^\lambda (V^{2i} f_i)^{c'})$$

显然, 这个验证方程中的 $a^{y'} z'^\lambda (V^{2i} f_i)^{c'}$ 有3个因子 $a^{y'}, z'^\lambda$ 和 $(V^{2i} f_i)^{c'}$, 因为 z' 和 f_i 都是签名数据, 所以3个因子都可构造造成 a 为底数的指数形式。这样, 就可以进行签名伪造。

随机选择 d_1, d_2 和 d_3 , 令:

$$z' = a^{d_1} \bmod N, f_i = V^{-2i} a^{d_2} \bmod N$$

按下列方式计算 c' 为:

$$c' = H(i \| f_i \| m \| a^{d_3}) \bmod N$$

利用:

$$a^{y'} z'^\lambda (V^{2i} f_i)^{c'} = a^{y'} a^{d_1 \lambda} a^{d_2 c'} = a^{d_3}$$

由同底关系得到: $y' = d_3 - d_1 \lambda - d_2 c' \bmod \lambda$, 从而伪造了签名 (f_i, c', y', z') 。

正确性:

$$H(i \| f_i \| m \| a^{y'} z'^\lambda (V^{2i} f_i)^{c'}) = H(i \| f_i \| m \| a^{d_3}) = c' \bmod N$$

3 Tseng-Jan 签名方案与分析

在数字签名过程中, 有时多个用户都可对一个文件进行签名和认证, 这就是群签名^[8]。

通常群签名具有以下特性: 1) 只有群中的成员才能代表整个群体对消息进行签名; 2) 群的接收者能够验证签名是否为这个群的有效签名, 但不能看出产生签名的是哪个具体成员; 3) 一旦以后对签名产生争议, 群权威能够根据签名识别出签名者的身份。

3.1 Tseng-Jan 签名方案

文献[9]是一个群签名方案, 签名方案过程如下:

初始化: 系统公用参数: p, q 为两个安全大素数且 $q \mid p-1, g \in \mathbf{Z}_p^*$ 且阶为 q 。成员密钥: 群中每一个成员 P_i 随机选择 $x_i \in [1, q-1]$, 并计算 $y_i = g^{x_i} \bmod p$, 分别作为 P_i 的私钥和公钥。群权威 T 的密钥: T 随机选取 $x_T \in [1, q-1]$, 并计算 $y_T = g^{x_T} \bmod p$, 分别作为 T 的私钥和公钥。

群成员加入: 对于群中每一个成员 P_i, T 随机选择 $k_i \in \mathbf{Z}_q^*$, 计算 $r_i = g^{-k_i} y_i^{k_i} \bmod p, s_i = k_i - r_i x_T \bmod q$ 。T 秘密将 (r_i, s_i) 发送给 P_i, P_i 收到 (r_i, s_i) 后, 验证等式 $g^{s_i} \cdot y_T^{r_i} \cdot r_i = (g^{x_i} \cdot y_T^{r_i})^{x_i} \bmod p$, 如果等式成立, 则 (r_i, s_i) 是 T 给 P_i 的有效身份证书。

签名:群成员 P_i 对消息 m 进行签名,先随机选择三个数 $a, b, d \in [1, q-1]$, 计算 A, C, D, E, B 的值。 $A = r_i^a \bmod p, C = r_i \cdot a - d \bmod q, D = g^b \bmod p, E = y_T^d \bmod p, B = s_i \cdot a - b \cdot h(A, C, D, E) \bmod q$ 。再随机选择 $t \in [1, q-1]$, 计算 $r = (g^B \cdot y_T^C \cdot D^{h(A, C, D, E)} \cdot E)^t \bmod p, s = t^{-1} (h(m) - x_i \cdot r) \bmod q$ 。则签名为: (r, s, m, A, B, C, D, E) 。

验证及签名识别:任何验证方可验证下面等式来识别签名的有效性, $(g^B \cdot y_T^C \cdot D^{h(A, C, D, E)} \cdot E)^{h(m)} \equiv (g^B \cdot y_T^C \cdot D^{h(A, C, D, E)} \cdot E \cdot A)^r \cdot r^s \bmod p$ 。同时,一旦产生争议,群权威也可通过验证相关等式来识别签名者身份(详见文献[9])。

3.2 分析

此签名方案存在很大安全漏洞,首先它缺乏可证实性,即在出现异议时,群权威实际上还需要其他信息才能证实签名者的身份。更重要的是,任何人都可以通过签名验证等式以同底构造攻击进行广泛的签名伪造。伪造过程如下。

验证等式为:

$$(g^B \cdot y_T^C \cdot D^{h(A, C, D, E)} \cdot E)^{h(m)} \equiv (g^B \cdot y_T^C \cdot D^{h(A, C, D, E)} \cdot E \cdot A)^r \cdot r^s \bmod p \quad (1)$$

将其转化为两个等式:

$$(g^B \cdot D^{h(A, C, D, E)} \cdot E)^{h(m)} \equiv (g^B \cdot D^{h(A, C, D, E)} \cdot E)^r \cdot r^s \bmod p \quad (2)$$

$$(y_T^C)^{h(m)} \equiv (y_T^C \cdot A)^r \bmod p \quad (3)$$

显然,式(2)和式(3)两边分别相乘就等于式(1),因此,通过它们构造出来的数据就是伪造出来的签名。这里将式(2)伪造成 g 为底的指数形式,将式(3)伪造成 y_T 为底的指数形式。

对任意消息 m , 随机选择 $r', B', C', d', e' \in [1, q-1]$, 令 $r = g^{r'}, B = B', C = C', D = g^{d'}, E = g^{e'}$ 。构造 $A = y_T^{x'} \bmod p$, 现在,由式(3),得到 $(y_T^C)^{h(m)} \equiv (y_T^{C+x'})^r \bmod p$, 故:

$$C \cdot h(m) = (C + x')r \bmod q$$

$$x' = C \cdot h(m)r^{-1} - C \bmod q$$

所以得到 $A = y_T^{C \cdot h(m)r^{-1} - C} \bmod p$

同样,由式(2)得到 $(g^{B+d' \cdot h(A, C, D, E) + e'})^{h(m)} \equiv (g^{B+d' \cdot h(A, C, D, E) + e'})^r \cdot g^{r's} \bmod p$, 得到 $(B + d' \cdot h(A, C, D, E) + e')(h(m) - r) = r's$, 所以得到 $s = (B + d' \cdot h(A, C, D, E) + e')(h(m) - r)r^{-1} \bmod q$ 。这样就伪造了一个签名。

正确性:将伪造签名代入上述签名验证等式,得到等式的两边都等于 $(g^{B+d' \cdot h(A, C, D, E) + e'} \cdot y_T^C)^{h(m)} \bmod p$ 。

4 Xue-Cao 签名方案与分析

4.1 Xue-Cao 签名方案

Xue-Cao 签名方案也是一代理盲签名方案,方案如下。

签名系统由原始签名者 A 、代理签名者 B 和签名接收者 C 三部分组成。

初始化阶段: p, q 为两安全大素数且 $q \mid p-1, g \in \mathbf{Z}_p^*$ 且阶为 $q, x_A, x_B \in \mathbf{Z}_q^*$ 分别代表 A 和 B 的私钥, $y_A = g^{x_A} \bmod p, y_B = g^{x_B} \bmod p$ 分别代表 A 和 B 的公钥。 m_w 为 A 发给 B 的委托授权书。 \parallel 表示比特串的并, $h(\cdot)$ 为一安全的哈希函数。

代理过程: A 随机选择 $\bar{k} \in \mathbf{Z}_q^*$, 计算 $\bar{r} = g^{\bar{k}} \bmod p, \bar{s} = \bar{k} + x_A h(m_w, \bar{r}) \bmod q$, 将 (m_w, \bar{r}, \bar{s}) 发送给 B 。 B 验证等式 $\bar{r} y_A^{h(m_w, \bar{r})} \bmod p$, 如果成立则计算 $s' = (\bar{s} + x_B y_B) \bmod q$ 。计算 $y_P = g^{s'} \bmod p$ 作为代理签名公钥。

签名过程: B 随机选取 $k \in \mathbf{Z}_q^*$, 计算 $t = g^k \bmod p$, 发送 t 给 C 。 C 随机选择 $a, b \in \mathbf{Z}_q^*$, 计算 $r = t g^{-a} y_P^{-b} \bmod p, e' = h(r \parallel m) \bmod q, e = e' + b \bmod q$ 。 C 发送 e 给 B 。 B 计算 $s'' =$

$(k - s'e) \bmod q$, 发送 (m_w, \bar{r}, s'') 给 C 。 C 计算 $s = g^{s''-a} \bmod p$ 。则代理盲签名为: (m, m_w, \bar{r}, s, e') 。

签名验证等式为: $e' = h(s \cdot y_P^{e'} \bmod p \parallel m) \bmod q$ 。

4.2 分析

在此签名方案中,实际上 s 是一个孤悬因子^[2], 很容易从孤悬因子出发伪造签名。当然,我们也可进行同底构造攻击伪造签名。方法如下:不妨设 $s = y_P^s \bmod p$, 随机选择 $u \in \mathbf{Z}_q^*$, 计算 $e' = h(y_P^u \bmod p \parallel m) \bmod q$ 得到 e' 的值, 由 $y_P^s \cdot y_P^{e'} = y_P^u \bmod p$, 所以 $s = y_P^{u-e'} \bmod p$, 从而伪造签名。

正确性: $h(s \cdot y_P^{e'} \parallel m) = h(y_P^{u-e'} y_P^{e'} \parallel m) = h(y_P^u \parallel m) = e' \bmod q$

5 数字签名方案改进的分析

本文首次提出了同底构造攻击的概念,并通过实例,说明任何人都可以通过同底构造攻击,绕开求解离散对数问题,从而伪造签名。在这一类数字签名方案中,攻击者是通过一系列等式变换得到等式 $g^m = g^{m'}$, 从而得到等式 $m = m'$, 因为签名数据包含在 m 或 m' 当中,因此,就轻易能伪造签名了。所以,防伪造签名也应从防止构造 $g^m = g^{m'}$ 着手,将签名数据重新设计或增加公钥数据。例如,假如 $m = m'$ 最终可以转化为 $m_1 + m_2 = m_1' + m_2'$, 签名数据是 m_1, m_2, m_1', m_2' , 我们可以根据实际情况选择某个数据比如 m_1 , 将这个签名数据对应改为 g^{m_1} (签名过程要适当更改);或者将 m_1 设置为私钥,而 g^{m_1} 成为公钥数据。这样,攻击者显然就不能构造等式 $g^m = g^{m'}$ 了,因而也就无从伪造签名。

参考文献:

- [1] DIFFIE W, HELLMAN M E. New directions in cryptography[EB/OL]. [2009-06-20]. <http://www.cs.jhu.edu/~rubin/courses/sp03/papers/diffie.hellman.pdf>.
- [2] 曹正军, 刘木兰. 数字签名方案中的孤悬因子和冗余数据[J]. 计算机学报, 2006, 29(2): 249-255.
- [3] MAMBO M, USUDA K, OKAMOTO E. Proxy signature: Delegation of the power to sign messages[J]. IEICE Transactions of Fundamentals, 1996, E79-A(9): 1338-1354.
- [4] CHAUM D. Blind signature for untraceable payments[C]// Proceedings of Crypto' 82. New York: Springer-Verlag, 1983: 199-203.
- [5] TAN ZUOWEN, LIN ZHOJUN, TANG CHUNMING. Digital proxy blind signature schemes based on DLP and ECDLP[EB/OL]. [2009-06-20]. <http://www.mmrc.iss.ac.cn/pub/mm21.pdf/tan.pdf>.
- [6] AWASTHI A K, SUNDER L. Proxy blind signature scheme[J]. Transactions on Cryptology, 2005, 2(1): 5-11.
- [7] DUC N D, CHEON H I, KIM K. A forward-secure blind signature scheme based on the strong RSA assumption[C]// The 9th Annual International Workshop on Selected Areas in Cryptography. Berlin: Springer-Verlag, 2003: 11-21.
- [8] CHAUM D, HEYST E. Group signatures[C]// Advances in Cryptology-EuroCrypt' 91. Berlin: Springer-Verlag, 1992: 257-265.
- [9] TSENG Y M, JAN J K. Reply improved group signature scheme based on the discrete logarithm problem[J]. Electronics Letters, 1999, 35(16): 1324-1325.
- [10] XUE QING-SHUI, CAO ZHEN-FU. A new proxy blind signature scheme with warrant[C]// Proceedings of the 2004 IEEE Conference on Cybernetics and Intelligent Systems. New York: IEEE, 2004: 1386-1391.