多用户环境中签名方案的安全性研究

王平水[1]，赵俊杰[2]
（1. 安徽财经大学 信息工程学院，安徽 蚌埠 233041；
2. 安徽财经大学 成人教育学院，安徽 蚌埠 233061）

摘 要：数字签名已经成为网络信息时代身份认证的重要手段之一。为了使数字签名技术得到更广泛应用，研究了数字签名方案在多用户环境中的安全性。众所周知，一个安全的数字签名方案即使在自适应选择明文攻击下存在性伪造在计算上也是不可行的，认为这在多用户环境中是不充分的，为此，将该安全性概念扩充到多用户环境，并通过实例证明了在单用户环境中安全的签名方案施加适当的限制后在多用户环境中同样也是安全的。

关键词：数字签名；存在性伪造；密钥置换；随机 oracle
中图分类号：TP309.7 **文献标识码**：A **文章编号**：1673-629X(2009)01-0157-04

Research on Security of Multi-User Setting Signature Schemes

WANG Ping-shui[1], ZHAO Jun-jie[2]
(1. College of Information Engineering, Anhui University of Finance & Economics, Bengbu 233041, China;
2. College of Adult Education, Anhui University of Finance & Economics, Bengbu 233061, China)

Abstract: Digital signature has been a primary means of identity authentication in era of network information. To make the technology of digital signature be more widely applied, researched the security of the digital signature schemes in the multi-user setting. It was well known that a secure signature scheme must be computationally infeasible even existential forgery against adaptive chosen-message attacks. Argued that it is not adequate for the multi-user setting. For that extended this security notion to the multi-user setting and showed that signature schemes proven secure in the single-user setting can, under reasonable constraints, also be proven secure in the multi-user setting.

Key words: digital signature; existential forgery; key substitution; random oracle

0 引 言

数字签名方案的安全性均依赖于所基于的加密体制。传统加密算法的安全性，诸如公钥密码算法、签名算法、消息认证算法等，在单用户环境下被广泛研究。也就是说，合法的实体可以进行解密数据、签名数据以及认证数据等，然而对手的目标是想方设法危及这些任务的安全性。简单说，密码协议的安全性在两个用户的环境中已被研究，其中对手试图获得通信双方建立的密钥信息。

近年来，研究主要集中于在多用户环境中定义和证明加密算法的安全性。如 Bellare 和 Rogaway 最先给出了在多用户环境中对称实体认证方案和密钥传输方案的安全性定义，并证明了相应协议是安全的[1]。之后，Bellare、Boldyreva 和 Micali 又给出了在多用户环境下公钥密码系统的安全性定义[2]。上述突出成果是解释了攻击，如 Hastad 攻击，如果同一消息 m（或与 m 线性相关）被三个实体基于 RSA 加密方案取 $e=3$ 进行加密时，对手能够很容易获取消息明文 m。然而并不能以此认为 Hastad 攻击攻破了单用户环境下公钥密码系统的安全目标，原因很简单，在这个环境中只有一个合法的实体。已经证明有些公钥密码系统在单用户环境下是安全的，在多用户环境下也是安全的。

笔者认为，在多用户环境中数字签名方案的安全性需要附加适当的限制条件[3]。通过考查一些常用的数字签名方案中存在有所谓的“密钥置换”攻击，认为由 Goldwasser、Micali 和 Rivest 提出的数字签名方案安全性定义在多用户环境下是不充分的，然而，该定义可以很容易扩充到多用户环境中。而且可以证明在单用户环境下安全的签名方案，通过合理的参数限制，在多用户环境下同样也是安全的。

收稿日期：2008-04-29
基金项目：教育部社科规划办青年基金项目(07JC870006)；安徽省自然科学基金项目(2006KJ017C)
作者简介：王平水(1972-)，男，安徽萧县人，硕士，副教授，研究方向为数据库与信息安全。

1 安全性隐患

1984 年，Goldwasser、Micali 和 Rivest 介绍了在单用户环境中签名方案的安全性概念(以下简称 GMR 安全性)，即：一个安全的数字签名方案即使在自适应选择明文攻击下存在性伪造在计算上也是不可行的[4,5]。这里，对手给出了一个合法用户的公钥和一个相应的签名 oracle，其目标是对任一 oracle 中未曾询问过的消息产生一个有效的签名，这样的消息和签名对被称为“存在性伪造”。这个安全性概念是可以接受的。

以下进一步阐明在多用户环境中可能危及到签名方案安全性的另一类攻击——置换密钥攻击(简称 KS 攻击)。

对手 E 提供了用户 A 的公钥和 A 对某消息 m 的签名 S_A，其目标是产生一个合法的公钥 / 私钥对以表明 S_A 也是它对消息 m 的签名，称此密钥对为置换密钥。E 必须知道与它公钥相应的私钥，否则 E 通过宣称它的公钥是和 A 完全相同的很容易实施 KS 攻击。

KS 攻击能在多种签名方案中被成功使用，以下证明在 Gennario - Halevi - Rabin 签名方案(GHR 签名方案)中存在这种攻击。在 GHR 方案中，A 的公钥包括一个模数 n(两个相同长度的安全素数 pq 之积)和一个 $t \in_R Z_n^*$，私钥为 (p,q)。为了对消息 m 签名，A 计算 $e = H(m)$，其中 H 为 Hash 函数，并求出 $s^e \equiv t(\mathrm{mod}n)$，$s \in \{1,2,\cdots,n-1\}$，假定 $\gcd(e,(p-1)(q-1)) = 1$，则仅存在唯一的解 s，即 A 对消息 m 的签名。为了验证签名，需要计算 $e = H(m)$ 并检验 $s^e \equiv t(\mathrm{mod}n)$ 是否成立。在给定 n,t,m,s 的情况下，对手 E 可通过如下方式实施 KS 攻击：选择等长的安全素数 $\bar{p}$ 和 $\bar{q}$ 使得 $\bar{n} = \overline{pq} > s$，并计算 $\bar{t} = s^e \mathrm{mod}\bar{n}$，其中 $e = H(m)$。于是，$(\bar{n},\bar{t})$ 和 $(\bar{p},\bar{q})$ 是一对合法的公钥 / 私钥对，s 将是 E 对消息 m 的签名。

问题是 KS 攻击是否对该签名方案真正构造了一个攻击。既然在单用户环境中只有一个公钥，一个成功的 KS 攻击不能与 GMR 安全性定义相矛盾。

笔者认为，在多用户环境中一个签名方案的攻击者能够获得成功，当且仅当它能产生一个存在性伪造或者能产生一个置换密钥。

2 安全性定义

以下用形式化的方式描述一个签名方案的概念及其安全性。

定义 1 一个签名方案 S 是由基于安全参数 k 的三组算法对 (D,D_V)、(G,G_V) 和 (E,E_V) 构成。其中：

D 为域参数产生算法，它是一个随机算法，以 1^k 作为其输入，输出一个能够被一个或多个用户共享的域参数集合 D，和一些可能的状态消息 I(用来证明这些域参数确实满足安全性要求)。作为特例，算法 D 可能直接返回其输入值，即 1^k。

D_V 为域参数有效性算法，它是一个确定性的算法，输入域参数集合 D，和一些可能的状态信息 I，输出单独的一位用以标识域参数是否符合特定的安全要求。

G 为密钥对产生算法，它是一个随机算法，输入域参数集合 D，输出公钥 / 私钥对 (y,x)。

G_V 为公钥有效性算法，它是一个双方的零知识协议。双方都以 (D,y) 作为输入，其中，D 是有效的域参数集合，y 是一个公钥。一方(证明者)还有一个作为输入的私有密钥 x。协议 G_V 允许一方(证明者)向另一方(验证者)证实：y 是与其私有密钥 x 相应的有效的公开密钥。

E 是签名产生算法，它是一个随机算法，输入消息 m 和与域参数 D 相联系的私有密钥 x，输出数字签名 s。

E_V 是签名验证算法，它是一个确定性的算法，输入消息 m、数字签名 s、一个有效的域参数集合 D 和有效的公开密钥 y，输出 True 或 False。

要求 $E_V = (m,s,D,y) = \mathrm{True}$，$D$ 是一个通过算法 D 产生的有效的域参数集合，y 是基于域参数集合 D 通过算法 G 产生的有效的公开密钥(与私有密钥 x 相应)，并且 $E(m,D,x) = s$。

例如，在 DSA 签名方案中，域参数为素数 p 和 q，且 $q \mid (p-1)$，和一个阶为 q 的元素 $g \in Z_p^*$。域参数有效性算法 D_V 检验 p 和 q 都为素数，且 $q \mid (p-1)$，$2 \leqslant g \leqslant p-1$ 且 $g^q \equiv 1(\mathrm{mod}p)$。DSA 的公开密钥 $y = g^x \mathrm{mod}p$，其中 $x \in_R [1,q-1]$ 是私有密钥。密钥有效性算法 G_V 可以检验 $2 \leqslant y \leqslant p-1$ 和 $y^q \equiv 1(\mathrm{mod}p)$，为了证实私有密钥知识，要求用 DSA 签名一个消息。

在第 1 部分中，提出了一个对手在多用户环境签名方案中攻击是成功的，如果它能够产生一个存在性伪造或者一个置换密钥。事实上，在任何情况下，对手实施攻击都是针对于一个特殊的公开密钥。因此，最初仅有一个公开密钥，满足多用户环境下签名的要求，通常对手是通过出示其他实体的公开密钥来进行冒充以示它知道相应的私有密钥。

定义 2 对手 E 的签名方案 $S = [(D,D_V),(G,G_V),(E,E_V)]$ 是一个随机算法，其输入为通过算法 D 产生的有效的域参数集合 D、一个通过算法 G 产生

的基于域参数集合 D 的公开密钥 y 和一个基于 y 的 oracle 签名 Q。D 的输出是一个公开密钥 $\bar{y}$,一个位串 $\bar{x}$,消息 m 和签名 $\bar{s}$。对手被认为是成功的,如果它的输出 $(\bar{y},\bar{x},m,\bar{s})$ 满足如下条件:

1) 如果消息 m 没有被 Q 询问,则 $\bar{y}=y$ 且 $E_V(m,\bar{s},D,\bar{y})$ = True。

2) 如果消息 m 被 Q 询问并返回签名 s,则 $\bar{s}=s$,$G_V((D,\bar{y}),(D,\bar{y},\bar{x}))$ = True 且 $E_V(m,\bar{s},D,\bar{y})$ = True。

说明:

(1) 如果多项式时间的对手不存在成功的可能性,则这种签名方案 S 是安全的。

(2)上述定义中条件 1 对应于一个存在性伪造,条件 2 对应于密钥置换攻击。

3　一些安全的签名方案

注意到在单用户环境下安全的签名方案能够稍加修改使其在多用户环境下同样也是安全的。

定理 1　任何在单用户环境下安全的(具有 GMR 安全性)签名方案能够转换成在多用户环境下也是安全的(定义 2 安全性)。

证明:令签名方案 S 在单用户环境下是 GMR 安全的,定义一个签名方案 S',S' 除了在签名之前需预先通过公开密钥以特定方式格式化消息外,其他均与签名方案 S 相同。既然对手 E 需要知道与公开密钥相应的私有密钥,E 的公开密钥必须不同于合法实体 A 的公开密钥,否则对手 E 要想产生一个存在性伪造就必须研究 A 的私有密钥,这与签名方案 S 在单用户环境下是安全的假设相矛盾。由于经过 E 格式化的消息没有与之相应的 A 格式化的消息,因此,签名方案 S' 上的密钥置换攻击也注定要失败。

事实上,按照签名方案标准不需要在签名之前利用公开密钥对消息进行格式化处理,因此,实际应用中,签名方案在多用户环境下也是真正安全的就显得至关重要了。

以下通过对常见的几种签名方案研究,来阐明笔者的观点。

3.1　Schnorr 签名方案

Schnorr 签名方案[6]的参数为素数 p 和 q,且 $q\mid(p-1)$,和一个阶为 q 的元素 $g\in Z_p^*$。实体 A 的公开密钥为 $y=g^x \bmod p$,其中 $x\in_R[1,q-1]$ 是相应的私有密钥。为了签名消息 m,A 计算 $r=g^k \bmod p$,$e=H(m,r)$ 和 $s=ex+k \bmod q$,其中 $k\in_R[1,q-1]$,(s,e) 为 A 对消息 m 的签名。为了验证签名,需要计算 $r'=g^s y^{-e} \bmod p$,并检验 $e=H(m,r')$ 是否成立。

定理 2　令 p,q 和 g 是域参数,假定离散对数问题 $<g>$ 是不可解的,那么,在随机 oracle 模型下,Schnorr 签名方案在多用户环境下是安全的。

证明:Pointcheval 和 Stern 已经证明了 Schnorr 签名方案在离散对数问题 $<g>$ 是不可解的前提下是 GMR 安全的,因此,只需证明该签名方案能够抵抗密钥置换攻击即可。

假定对手 E 成功地产生了不同于 A 的公开密钥/私有密钥对 $(\bar{y},\bar{x})$,使得 (s,e) 既是 A 又是 E 在消息 m 上的签名。既然两个签名都是有效的,于是就会有 $e=H(m,r)$,其中 $r=g^s y^{-e} \bmod p$;$e=H(m,\bar{r})$,其中 $\bar{r}=g^s \bar{y}^{-e} \bmod p$。由于 H 是一个随机函数,产生一个碰撞的可能性就是可以忽略的。因此,能够令 $\bar{r}=r$,如果 $y^e \equiv \bar{y}^e \pmod p$ 且 $y=\bar{y}$,这将会产生矛盾。

3.2　DSA 签名方案

DSA 签名方案[7]的参数为素数 p 和 q,且 $q\mid(p-1)$,和一个阶为 q 的元素 $g\in Z_p^*$。实体 A 的公开密钥为 $y=g^x \bmod p$,其中 $x\in_R[1,q-1]$ 是相应的私有密钥。为了签名消息 m,A 计算 $r=f(g^k \bmod p)$ 和 $s=k^{-1}(H(m)+xr) \bmod q$,其中 $k\in_R[1,q-1]$ 且 $f:<g>\to Z_q$,转换函数 f 定义为 $f(h)=h \bmod q$,(s,e) 为 A 对消息 m 的签名。为了验证签名,需要计算 $r'=f(g^{s^{-1}H(m)} y^{s^{-1}r} \bmod p)$,并检验 $r=r'$ 是否成立。

目前,还没有关于 DSA 签名方案能够抵抗存在性伪造的安全性证明,以下对 DSA 在多用户环境下的安全性加以证明。

定理 3　令 p、q 和 g 是域参数,假定 DSA 是 GMR 安全的,f 具有抗碰撞性,则 DSA 在多用户环境下是安全的。

证明:假定对手 E 成功地产生了一对置换密钥,也就是说,输入 p,q,g,y,输出 $(m,r,s,\bar{x},\bar{y})$,使得 $\bar{y}=g^{\bar{x}} \bmod p$,$\bar{y}!\equiv y \pmod p$,$r=f(g^{s^{-1}H(m)} y^{s^{-1}r} \bmod p)$ 且 $r=f(g^{s^{-1}H(m)} \bar{y}^{s^{-1}r} \bmod p)$。由于 $\bar{y}!\equiv y \pmod p$,则有 $g^{s^{-1}H(m)} y^{s^{-1}r}! \equiv g^{s^{-1}H(m)} \bar{y}^{s^{-1}r} \pmod p$。因此对手 E 在 f 上就产生一个碰撞,这与 f 具有抗碰撞性相矛盾。

3.3　ECDSA 签名方案

ECDSA 签名方案的参数为有限域 F_q,F_q 上的椭圆曲线 E,$\#E(F_q)=nh$,其中 n 是素数,阶为 n 的点 $G\in E(F_q)$。实体 A 的公钥是 $Q=dG$,其中 $d\in_R[1,n-1]$ 为相应的私有密钥。为了签名消息 m,A 计算 $r=x(kG) \bmod n$ 和 $s=k^{-1}(H(m)+dr) \bmod n$,其中 $k\in_R[1,n-1]$,(r,s) 为 A 对消息 m 的签名。为了验证签名,需要计算 $r'=s(s^{-1}H(m)G+s^{-1}rQ) \bmod n$,并

检验 $r = r'$ 是否成立。

以下证明 ECDSA 签名方案通过对域参数适当加以限制后在多用户环境下是安全的。

定理 4 令 E 为 F_q 上的椭圆曲线，且 $n = \#E(F_q)$ 为素数，$n > q$，G 为 $E(F_q)$ 上阶为 n 的点。假定 F_q、E、G 和 n 是域参数，Hash 函数 H 是抗碰撞的，那么在普通群模型中，ECDSA 在多用户环境下是安全的。

证明：在普通群模型中，Hash 函数 H 是抗碰撞的，ECDSA 具有 GMR 安全性已有证明。在此，只需证明该签名方案能够抵抗密钥置换攻击即可。

假定对手 E 成功地产生了不同于 A 的公开密钥/私有密钥对 $(\overline{Q}, \overline{d})$，使得 (r, s) 既是 A 又是 E 在消息 m 上的签名。既然两个签名都是有效的，于是有 $x(s^{-1}H(m)G + s^{-1}rQ) \equiv x(s^{-1}H(m)G + s^{-1}r\overline{Q}) \pmod{n}$。由于 $n > q$，则 F_q 中任一元素的二进制表示都小于 n，因此，$x(s^{-1}H(m)G + s^{-1}rQ) = x(s^{-1}H(m)G + s^{-1}r\overline{Q})$，于是有 $s^{-1}H(m)G + s^{-1}rQ = \pm(s^{-1}H(m)G + s^{-1}r\overline{Q})$。基于上述等式并结合私有密钥 $\overline{d}$，E 能够很容易确定 d。由于求解离散对数问题尚没有有效的算法，因此，对手 E 就不可能产生一个置换密钥。

4 结束语

研究了签名方案的安全性现状，分析了其中存在的安全性隐患，给出了签名方案在多用户环境下的安全性定义。在单用户环境下安全的签名方案能够很容易通过对公开密钥及消息摘要进行 Hash 以转换成在多用户环境下也是安全的。证明了 Schnorr、DSA、ECDSA 等签名方案通过对域参数做合理限制后在多用户环境下是安全的。

参考文献：

[1] Bellare M, Rogaway P. Entity authentication and key distribution[C]// In Advances in Cryptology - Euro - Crypt'93, LNCS773. Berlin: Springer - Verlag, 1993: 232 - 249.

[2] Bellare M, Boldyreva A, Micali S. Public - key encryption in a multi - user setting: security proofs and improvements[C]// In Advances in Cryptology - Euro - Cryption' 2000, LNCS1807. Berlin: Springer - Verlag, 2000: 259 - 274.

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

[4] 王 纯. 数字签名安全性研究[J]. 电脑与电信, 2006(11): 43 - 45.

[5] 王龙斌, 廉玉忠. 数字签名的安全性分析[J]. 信息工程大学学报, 2003(3): 90 - 92.

[6] 卿斯汉. 安全协议[M]. 北京: 清华大学出版社, 2005: 215 - 220.

[7] 杨 波. 现代密码学[M]. 北京: 清华大学出版社, 2003: 139 - 191.

(上接第 156 页)

大的电流冲击对单片机造成干扰，导致程序指针赋值错误，程序跑飞。针对这些情况，在返程程序中嵌入了上述的软件看门狗程序，使系统运行正常，小车可以成功地行走到目标位置，从而解决了由于电机电流冲击引起的单片机程序跑飞现象。

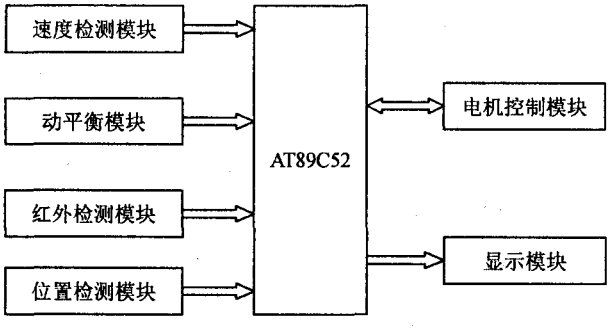

图 5 智能小车系统组成

文中介绍的方法既保证了局部程序的可靠运行，又不必在此过程中复位单片机，也就不必再次重复运行前面的程序段。在保证了 C 语言快速开发性的同时，提高了程序段的可靠性。

参考文献：

[1] 李烈彪, 李 仙. 计算机系统的可靠性技术[J]. 计算机技术与发展, 2007, 17(11): 142 - 145.

[2] 范立南. 单片机原理及应用教程[M]. 北京: 北京大学出版社, 2006.

[3] 卢大伟, 刘炳云. 用定时器实现软件看门狗应注意的问题[J]. 中国仪器仪表, 1998(4): 36 - 37.

[4] Thomas F, Nayak M. A hardware/software codesign for improved data acquisition in a processor based embedded system [J]. Microprocessors and Microsystems, 2000, 24(3): 129 - 134.

[5] 吴允平, 蔡声镇, 乐仁昌. 单片机任务型软件"看门狗"原理及应用[J]. 计算机工程与应用, 2004, 40(34): 122 - 123.

[6] 刘芳芳, 黄会雄. 单片机测控系统抗干扰方法的研究和改进[J]. 电子质量, 2006(1): 62 - 63.

[7] Zhou Y Q. Design and development of portable data acquisition system for vehicle roadway test[J]. Automation Insteumentation, 2006, 27(8): 61 - 63.