一些可证安全签名方案的密码学分析*)

明 洋 王育民

(西安电子科技大学综合业务网络国家重点实验室 西安 710071)

摘 要 最近,Okamoto提出一个在标准模型下可证安全的签名方案,Victor K. Wei等人提出两个在标准模型下可证安全的短签名方案。在本文中,我们指出这三个方案在多用户环境下是不安全的,不能抵抗强密钥替换攻击。在这种攻击中,一个敌手能够生成新的公钥满足合法签名者生成的合法签名。

关键词 密钥替换攻击,可证安全,双线性对

Cryptanalysis of Some Provably Secure Signature Schemes

MING Yang WANG Yu-Min

(State Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071)

Abstract Recently, Okamoto and Victor K. Wei et al. proposed provably signature scheme in the standard model and two provably short signature schemes in the standard model respectively. In this paper, we show that the three schemes are all insecure against strong-key substitution attacks under the multi-user setting. In this attack, an adversary can generate a new public key satisfying legitimate signatures created by the legitimate signer.

Keywords Key substitution attacks, Provably secure, Bilinear pairings

1 引言

在1988年,Goldwasser, Micali和Rivest[1]提出在单用户环境下签名方案的安全概念,即适应性选择消息攻击下的存在性不可伪造。这里敌手被提供一个合法用户的公钥以及关于这个公钥的签名预言机。敌手的目标是产生新消息的有效签名且这个消息以前没有询问过签名预言机;这样的消息签名对称为存在性伪造。当前,大部分可证安全签名方案都满足这个安全定义。最近,Wilson和Menezes[2]对一些签名方案提出了相同签名密钥选择攻击。后来,Menezes和Smart[3]在这个攻击下分析了一些签名方案的安全性,并称此攻击为密钥替换攻击,即给定合法用户U的公钥以及某个消息m的用户U的签名σ,一个敌手A试图生成不同于用户U的新的公钥并且满足消息m的签名σ也是敌手A的有效签名。在文[4,5]中,Tan进一步指出了一些签名方案不能抵抗密钥替换攻击,然而这些方案在适应性选择消息攻击下存在性不可伪造的这个安全定义[1]中,都是可证明安全的。

在密钥替换攻击中,如果敌手A知道新公钥所对应的私钥,那么我们称为弱密钥替换攻击。否则称为强密钥替换攻击。在强密钥替换攻击中,给定一个合法签名σ,敌手A生成的新公钥满足由合法签名者生成的所有合法签名,那么称这样的攻击为普遍(universal)强密钥替换攻击;如果敌手A生成的新公钥满足一个特殊的合法签名,而不是所有的合法签名,那么称这样的攻击为局部(local)强密钥替换攻击。在密钥替换攻击中,敌手可以声称他/她签署具有合法签名的消息,而事实上,他/她根本没有签署那个消息。在现实中,随着电子商务的日益发展,电子彩票将成为不可缺少的业务之一。当客户从彩票发行者那里购买彩票时,为了防止电子彩票的复制,客户首先对彩票进行签名以保证自己拥有这个彩票,然后彩票发行者对这个彩票以及客户的签名再进行签名,这样确保如果彩票重奖时,仅仅只有合法的客户能够从彩票发行者那里认领奖金,而阻止多次的认领。当攻击者知道某个客户从彩票发行者那里认领奖金,如果他能够生成一个不同的公钥,但是仍然满足客户对电子彩票的签名通过这个公钥的验证,那么攻击者也能够从彩票发行者那里认领奖金。因此,一个安全签名方案应该能够抵抗密钥替换攻击。

在这篇文章中,我们指出Okamoto的签名方案[6]以及Victor K. Wei等人提出的两个短签名方案[7]都不能抵抗强密钥替换攻击,事实上这些方案在标准模型下都是可证安全的能够抵抗适应性选择消息攻击下的存在性伪造。然而,在多用户环境[3]下,Goldwasser等人提出的安全定义[1]不能充分地保证签名方案的安全性。

2 双线性对

设G_1和G_2是两个乘法循环群,且阶数都为素数p,g_1是群G_1的生成元,g_2是群G_2的生成元。设G_T是阶数为素数p的加法群,$\Psi: C_2 \to C_1$是同态映射满足$g_1 = \Psi(g_2)$。一个双线性映射$e: G_1 \times G_2 \to G_T$满足下面的性质:

(1)双线性性:对于所有的$u \in G_1$,$v \in G_2$和$a,b \in Z$满足$e(u^a, v^b) = e(u,v)^{ab}$。

(2)非退化性:$e(g_1, g_2) \neq 1$。

(3)可计算性:存在有效的算法对于所有的$u \in G_1$,$v \in G_2$去计算$e(u,v)$。

那么e称为双线性对,它可以从基于有限域中椭圆曲线上的Weil对或Tate对得到。为了简便,我们可以设$G_1 = G_2$和$g_1 = g_2$。

3 Okamoto签名方案和密码学分析

Okamoto基于双线性对提出一个有效的签名方案[6],并且在标准模型下证明了方案的安全性,即能够抵抗适应性选

*)基金项目:国家自然科学基金资助项目(60473072)。明 洋 博士生,主要研究方向为密码学理论,电子商务。王育民 教授,博士生导师,主要研究方向为信息论,密码,编码。

择消息攻击下的存在性伪造，但我们指出该方案仍然是不安全的，不能抵抗强密钥替换攻击。

3.1 Okamoto 签名方案

密钥生成：随机选取生成元 $g_2,u_2,v_2\in_R G_2$，设 $g_1=\Psi(g_2)$，$u_1=\Psi(u_2)$ 以及 $v_1=\Psi(v_2)$。随机选取 $x\in_R Z_p^*$，计算 $w_2=g_2^x\in G_2$。则公钥为 (g_1,g_2,w_2,u_2,v_2)，私钥为 (x)。

签名生成：假设被签名的消息 $m\in Z_p^*$。签名者随机选取 $r,s\in_R Z_p^*$，计算 $\sigma=(g_1^m u_1 v_1^s)^{1/x+r}$。这里 $1/(x+r)$ 是在模 p 下计算。如果 $x+r=0 \bmod p$，那么选取不同随机值 r。则消息 m 的签名为 (σ,r,s)。

签名验证：给定公钥 (g_1,g_2,w_2,u_2,v_2)，消息 m 和签名 (σ,r,s)。验证者检验 $m,r,s\in Z_p^*$，$\sigma\in G_1$，$\sigma\neq 1$ 以及 $e(\sigma,w_2g_2^r)=e(g_1,g_2^m u_2 v_2^s)$。如果成立，则输出“接受”；否则输出“拒绝”。

3.2 Okamoto 签名方案的密码学分析

我们给出 Okamoto 签名方案的安全性分析，得出该方案不能抵抗普遍强密钥替换攻击，具体攻击如下：

首先一个敌手 A 随机选取 $\alpha\in_R Z_p^*$ 满足 α 和 $p-1$ 互素，计算 $\overline{g_2}=g_2^\alpha$，$\overline{w_2}=w_2^\alpha$。则公钥 $(g_1,\overline{g_2},\overline{w_2},u_2,v_2)$ 为不知道相应私钥的新公钥（注意，$\overline{g_2}$ 也是 G_2 中的生成元，同时存在一个同态映射 $\overline{\Psi}$ 满足 $g_1=\overline{\Psi}(\overline{g_2})$）。给定任何消息 m 的合法签名 (σ,r,s) 下，所有这些签名对于敌手 A 也是有效的签名。因为

$$e(\sigma,\overline{w_2}(\overline{g_2})^r)=e(\sigma,(w_2g_2^r)^\alpha)=e(\sigma,w_2g_2^r)^\alpha=e(g_1,g_2^m u_2 v_2^s)^\alpha$$
$$=e(g_1,g_2^{\alpha m}u_2v_2^{\alpha s})=e(g_1,(\overline{g_2})^m u_2 v_2^{\alpha s})$$

4 Victor K. Wei 等人的两个短签名方案和密码学分析

Victor K. Wei 等人提出了两个短签名方案[7]（我们定义为方案 1 和方案 2）并在标准模型性下证明了安全性，但是我们指出这两个方案仍然是不安全的，不能抵抗强密钥替换攻击。

4.1 方案 1

参数生成：设 $e:G_1\times G_1\to G_T$，G_1 的阶为素数 p 且 g 为群 G_1 的生成元。定义消息空间为 $\{0,1\}^{l_1}$ $H:\{0,1\}^{l_1}\to\{0,1\}^l/\{0^l\}(l<\log_2 p)$。

密钥生成：随机选取 $x,y\in_R Z_p^*$，计算 $X=g^x$，$Y=g^y$，$Z=g^{xy}$。公钥为 (g,X,Y,Z)，私钥为 (x,y)。

签名生成：给定消息 $m\in\{0,1\}^{l_1}$，随机选取非零元素 m_1，$m_2\in\{0,1\}^l$ 满足 $m_1\oplus m_2=H(m)$，计算 $\sigma=g^{1/((x+m_1)(y+m_2))}$，则消息 m 的签名为 (m_1,σ)。

签名验证：给定消息 m 的签名 (m_1,σ)，计算 $m_2=H(m)\oplus m_1$，验证 $m_1\neq 0$，$m_2\neq 0$ 以及 $e(\sigma,ZX^{m_2}Y^{m_1}g^{m_1m_2})=e(\sigma,g^{(x+m_1)(y+m_2)})=e(g,g)$。如果验证通过，则输出“接受”；否则输出“拒绝”。

4.2 方案 1 的密码学分析

我们给出 Victor K. Wei 等人方案 1 的安全性分析，指出该方案是不安全的，不能抵抗局部强密钥替换攻击。具体攻击如下：

给定消息 m 的有效签名 (m_1,σ)，敌手 A 随机选取的 $\overline{X}$，$\overline{Y}\in_R G_1$，计算 $m_2=H(m)\oplus m_1$ 和 $\overline{Z}=\frac{ZX^{m_2}Y^{m_1}}{\overline{X}^{m_2}\overline{Y}^{m_1}}$，则 $(g,\overline{X},\overline{Y},\overline{Z}$ 为敌手 A 生成的新公钥。给定消息 m 的有效签名 (m_1,σ) 下，那么这个签名对于敌手 A 也是有效的签名，因为

$$e(\sigma,\overline{Z}\overline{X}^{m_2}\overline{Y}^{m_1}g^{m_1m_2})=e(\sigma,ZX^{m_2}Y^{m_1}g^{m_1m_2})$$
$$=e(\sigma,g^{x+m_1)(y+m_2)})$$
$$=e(g,g)$$

4.3 方案 2

基于 CL 方案[8]，Victor K. Wei 等人给出一个新的短签名方案，具体描述如下：

密钥生成：随机选取 $x,y,z\in_R Z_p^*$，计算 $X=g^x$，$Y=g^y$，$Z=g^z$。则公钥为 (g,X,Y,Z)，私钥为 (x,y,z)。

签名生成：随机选取 $a\neq 1$，非零随机数 R，计算 $A=a^x$，$b=a^y$，$B=a^{yz}$，$c=a^{x+(m+zR)xy}$。则消息 m 的签名为 (R,a,A,b,B,c)。

签名验证：给定消息 m 的签名 (R,a,A,b,B,c)，验证

$e(A,g)=e(a,Z)$，$e(b,g)=e(a,Y)$，$e(B,g)=e(A,Y)$

$e(B,g)=e(b,Z)$，$e(c,g)=e(ab^mB^R,X)$，$a\neq 1$，$R\neq 0$

如果验证通过，则输出“接受”；否则输出“拒绝”。

4.4 方案 2 的密码学分析

我们给出 Victor K. Wei 等人方案 2 的安全性分析，指出该方案是不安全的，不能抵抗普遍强密钥替换攻击。具体攻击如下：

敌手 A 随机选取 $\alpha\in Z_p^*$，计算 $\overline{g}=g^\alpha$，$\overline{X}=X^\alpha$，$\overline{Y}=Y^\alpha$，$\overline{Z}=Z^\alpha$。则公钥 $(\overline{g},\overline{X},\overline{Y},\overline{Z})$ 为敌手 A 生成的新公钥。给定任何消息 m 的合法签名 (R,a,A,b,B,c) 下，所有这些签名对于敌手 A 也是有效的签名。因为

$$e(A,\overline{g})=e(A,g^\alpha)=e(A,g)^\alpha=e(a,Z)^\alpha$$
$$=e(a,Z^\alpha)=e(a,\overline{Z})$$
$$e(b,\overline{g})=e(b,g^\alpha)=e(b,g)^\alpha=e(a,Y)^\alpha$$
$$=e(a,Y^\alpha)=e(a,\overline{Y})$$
$$e(B,\overline{g})=e(B,g^\alpha)=e(B,g)^\alpha=e(A,Y)^\alpha$$
$$=e(a,Y^\alpha)=e(A,\overline{Y})$$
$$e(B,\overline{g})=e(B,g^\alpha)=e(B,g)^\alpha=e(b,Z)^\alpha$$
$$=e(b,Z^\alpha)=e(b,\overline{Z})$$
$$e(c,\overline{g})=e(c,g^\alpha)=e(c,g)^\alpha e(ab^mB^R,X)^\alpha$$
$$=e(ab^mB^R,X^\alpha)^\alpha=e(ab^mB^R,\overline{X})$$

结束语 在这篇文章中，我们指出 Okamoto 的签名方案和 Victor K. Wei 等人提出的两个短签名方案是不安全的，不能抵抗普遍或局部强密钥替换攻击。我们指出在单用户环境下，签名方案抵抗适应性选择消息攻击下的存在性不可伪造是不充分的。因此，一个安全签名方案的设计应能够抵抗在多用户环境下密钥替换攻击。

参 考 文 献

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

2 Blake Wilson S, Menezes A. Unknow key-share attacks on the station-to-station (STS) protocol. In: Proc. PKC'99, Lecture Notes in Computer Science 1560, Berlin: Springer-Verlag, 1999. 154～170

3 Menezes A, Smart N. Security of signature schemes in a multi-user setting. Des. Codes Cryptogr., 2004, 33(3): 261～274

4 Tan C H. Key substitution attacks on some provably secure signature schemes. IEICE Transactions on Fundamentals, 2004, E87-A (1): 226～227

5 Tan C H. Key substitution attacks on provably secure short signature schemes. IEICE Trans actions on Fundamentals, 2005, E88-A (2): 611～612

6 Okamoto T. Efficient blind and partially blind signatures without random oracle. In: Proc. TCC 2006, Lecture Notes in Computer Science 3876, Berlin: Springer-Verlag, 2006. 80～99

7 Victor K, Wei, Yuen T H. More short signatures without random oracles. Cryptology ePrint Archive: [Report 2005/463, 2005]. http://eprint.iacr.org/ 2005/ 463

8 Camenisch J, Lysyanskaya A. Signature schemes and anonymous credentials from bilinear maps. In: Proc. CRYPTO 2004, Lecture Notes in Computer Science 3152. Berlin: Springer-Verlag, 2004. 56～72