对两类基于双线性对的签名方案的攻击 *

杜红珍
(宝鸡文理学院 数学系, 陕西 宝鸡 721013)

摘 要: Wen 和 Ma 提出了一个基于传统 PKI 体制上的聚合签名方案,并认为该方案在随机预言机模型下是可证明安全的。但本文指出 Wen-Ma 方案是可以普遍伪造的,敌手既可以伪造某一个签名人的(普通)数字签名又可以伪造多个签名人的聚合签名。另外,Dai 等人提出了一个适用于移动商务的基于身份的数字签名方案,但杜红珍发现该方案是不安全的,并给出了该方案的两种伪造攻击。

关键词: 聚合签名; 基于身份的数字签名; 随机预言机模型; 双线性映射
中图分类号: TN918 **文献标志码**: A **文章编号**: 1001-3695(2010)05-1879-03
doi:10.3969/j.issn.1001-3695.2010.05.078

Attacks on two signature schemes based on bilinear pairings

DU Hong-zhen
(*Dept. of Mathematics, Baoji University of Arts & Sciences, Baoji Shaanxi* 721013, *China*)

Abstract: Wen and Ma presented an aggregate signature scheme in the public key infrastructure setting and claimed their scheme is provably secure in the random oracle model. But this paper pointed out Wen-Ma scheme was universally forgeable, and an adversary could forge not only any signer's ordinary signatures but also aggregate signatures produced by many different signers. In addition, Dai et al. proposed an identity-based sinature scheme. DU Hong-zhen found out their scheme was insecure and gave two forgery attacks on the scheme.

Key words: aggregate signature; identity-based signature; random oracle model; bilinear maps

0 引言

在 2003 年欧密会上,Boneh 等人[1]提出了聚合签名(aggregate signature)的概念,聚合签名可以把 $k(>1)$ 个用户 P_i $(1\leqslant i\leqslant k)$ 对 k 个不同的消息 m_i 的普通数字签名 S_i 聚合成一个签名 σ, 而验证方只需检验合成后的签名 σ 便可以确认是否是用户 $P_i(1\leqslant i\leqslant k)$ 对 m_i 做的签名。聚合签名可以同时给多个消息、多个用户提供不可否认服务,可以把任意多个用户的签名压缩成一个签名,这大大减小了签名的存储空间,同时也降低了传输签名的网络带宽的要求。且把对任意多个签名的验证简化到一次验证,大大减少了签名验证的工作量,所以聚合签名在很大程度上提高了签名的验证与传输效率。在现实中,聚合签名技术可被用于分级 PKI 中的证书链,无线传感器网络的安全路由协议及数据库的外购等。对聚合签名的研究是目前的一个热点。现已有一些聚合签名方案[2~7]被提出。

为了简化电子邮件系统中的证书管理问题, Shamir[8] 于 1984 年提出了基于身份的密码学(ID-based public key cryptography, ID-PKC)的概念。在 ID-PKC 中,用户的公钥不是随机产生的,它由用户惟一的身份信息如电话号码、身份证号、IP 地址等推导出来,用户的私钥则是由一个称为私钥生成器(PKG) 的可信中心来产生的。显然, ID-PKC 消除了对用户证书的依赖,因此极大地简化了密钥管理问题。基于身份的数字签名是 ID-PKC 的一个重要的密码原型。第一个基于身份的数字签名方案是 Shamir[8] 提出的,但签名太长。如果用 1 024 bit 的 RSA 模数,签名的长度大约就是 2 048 bit。1988 年,Guillou 等人[9]改进了 Shamir 的方案,缩短签名的长度到 1 184 bit,然而该签名还是太长而不能被广泛应用。近年来,有许多利用双线性对构造的基于身份的签名方案被提出,如文献[10~13],这些方案的签名长度在与方案[8,9]达到的安全程度相当的情况下可以缩减到 320 bit。

2008 年,Wen 等人[14]提出了一个高效的基于传统 PKI 体制的聚合签名方案(简称 Wen-Ma 方案),并声称该方案在随机预言机模型下是抵抗存在性伪造攻击的。然而,笔者发现该聚合签名方案是不安全的,任意一个敌手(不知道签名人的私钥)既可以伪造签名人的普通数字签名又可以伪造多个签名人的聚合签名。Dai 等人[15]提出了一个适用于移动商务(mobile business)的基于身份的签名方案(简称 Dai-Wang-Hu-Yun 方案)。但是笔者指出该方案是可以普遍伪造的,并给出了该方案的两种伪造攻击。

1 预备知识

下面介绍双线性对的基础知识及相关困难问题。

令 k 是一个安全参数,q 是一个 k bit 的素数,G_1 是由 P 生成的阶为 q 的循环加法群,G_2 是有相同阶 q 的循环乘法群,设 G_1,G_2 群中的离散对数问题是困难问题。双线性映射 $e: G_1\times G_1\rightarrow G_2$ 满足下列性质:

a)双线性性。$\forall P,Q\in G_1, a,b\in Z_q^*$ 有 $e(aP,bQ)=e(P,Q)^{ab}$。

收稿日期: 2009-10-09; **修回日期**: 2009-11-24 **基金项目**: 国家自然科学基金资助项目(60873191); 宝鸡文理学院重点科研项目(ZK0952)

作者简介:杜红珍(1978-),女,陕西扶风人,讲师,博士,主要研究方向为密码学与信息安全(hongzhendu@163.com).

b)非退化性。$\exists P,Q\in G_1$,使得 $e(P,Q)\neq 1$。

c)易计算性。$\forall P,Q\in G_1$,存在有效算法计算 $e(P,Q)$。

双线性映射 e 可通过有限域上的超奇异椭圆曲线上的 Weil 对或 Tate 对来构造。

设 G_1 和 G_2 分别是两个阶都为素数 q 的加法群和乘法群,一个双线性映射 $e:G_1\times G_1\to G_2$,P 为 G_1 的一个生成元。

The Computational Diffie-Hellman Problem (CDHP)

$\forall a,b\in Z_q^*$,给定 $P,aP,bP\in G_1$,计算 $abP\in G_1$ 目前 CDH 问题仍是公认的数学难题。

2 *Wen-Ma* 方案介绍及安全性分析

2.1 *Wen-Ma* 方案介绍

Wen-Ma 的聚合签名方案[14]由五个算法〈KeyGen, Sign, Verify, Aggregate 和 Aggregate-Verify〉组成。

设$(G_1,+)$和$(G_2,\cdot)$是两个阶均为素数 q 的循环群,P,$P'(P\neq P')$为 G_1 的生成元,e 是一个双线性映射。两个全域 hash 函数 $H_1:\{0,1\}^*\to Z_q^*$,$H_2:\{0,1\}^*\to Z_q^*$。系统参数 params:$\{G_1,G_2,q,P,P',e,H_1,H_2\}$。

1)KeyGen 用户随机选取 $s\in Z_q*$ 作为自己的私钥,计算公钥 $Q=sP$。

2)Sign 给定消息 $M\in\{0,1\}*$,用户签名如下:

a)计算 $h_1=H_1(M,s)$ 和 $h_2=H_2(M)$;

b)计算 $R=h_1P$,$V=(h_1+h_2s)P'$。

则在消息 M 上的(普通)数字签名是(R,V)。

3)Verify 给定用户的公钥 Q,消息和签名对$(M,(R,V))$,验证者计算 $h_2=H_2(M)$,接受该签名当且仅当 $e(V,P)=e(P',R+h_2Q)$。

4)Aggregate $U=\{U_1,U_2,\cdots,U_k\}$ 表示要参与签名聚合的 k 个用户的集合(为了简便起见,假定是用户 U_i 对消息 M_i 签名),对于消息 $M_i\in\{0,1\}^*$,每个用户 $U_i\in U$ 利用上述 Sign 算法生成消息 M_i 的签名(R_i,V_i),聚合人计算如下:

$$R=\Sigma_{i=1}^{k}R_i,V=\Sigma_{i=1}^{k}V_i$$

则聚合签名为(R,V)。

5)Aggregate-Verify 给定 $U=\{U_1,U_2,\cdots,U_k\}$ 和用户 U_i 的公钥 Q_i,消息 $M_i\in\{0,1\}^*(1\leqslant i\leqslant k)$和聚合签名$(R,V)$,验证人计算 $h_{2i}=H_2(M_i)\ (1\leqslant i\leqslant k)$,接受该聚合签名当且仅当下式成立:

$$e(V,P)=e(P',R+\Sigma_{i=1}^{k}h_{2i}Q_i)$$

Wen-Ma 方案的安全性分析详见文献[14]。

2.2 Wen-Ma 方案的安全性分析

Wen 等人在随机预言机模型下给出了方案的安全性证明,指出他们的方案在 CDH 假设下可以抵抗敌手的存在性伪造攻击。然而,笔者发现 Wen 的签名方案是可以普遍伪造的。敌手 A 能够伪造任意一个签名人 U_i(公钥为 Q_i)的普通数字签名,也可以伪造 n 个签名人对 n 个不同消息 M_i 的聚合签名,现将敌手 A 的伪造描述如下:

a)Sign:给定某个消息 $M_i(1\leqslant i\leqslant k)$,$A$ 冒充用户 U_i 对消息 M_i 签名如下:

(a)随机选 $t_i\in Z_q^*$,计算 $V_i=t_ip'$;

(b)计算 $h_{2i}=H_2(M_i)$;

(c)令 $R_i=t_iP-h_{2i}Q_i$,则 $\sigma_i=(R_i,V_i)$就是 A 冒充 U_i 在消息 M_i 上的(普通)签名。

b)Verify。给定用户的公钥 Q_i,消息和签名对$(M_i,\sigma_i=R_i,V_i))$,验证者计算 $h_{2i}=H_2(M_i)$,接受该签名当且仅当 $e(V_i,P)=e(P',R_i+h_{2i}Q_i)$。显然伪造的签名 $\sigma_i=(R_i,V_i)$可以通过验证,因为:$e(V_i,P)=e(t_i,P',P)=e(P',t_iP)e(P',R_i+h_{2i}Q_i)$。

c)Aggregate-Sign。A 计算 $R=\Sigma_{i=1}^{k}R_i$,$V=\Sigma_{i=1}^{k}V_i$,则(R,V)就构成了 U_i 对 m_i 的聚合签名。

d)Aggregate-Verify。该伪造的聚合签名(R,V)也显然能通过验证等式

$$e(V,P)=e(P',R+\Sigma_{i=1}^{k}h_{2i}Q_i)$$

因为:$e(V,P)=e(\Sigma_{i=1}^{k}V_i,P)=e(\Sigma_{i=1}^{k}t_iP',P)=e(P',\Sigma_{i=1}^{k}t_iP)=e(P',\Sigma_{i=1}^{k}(R_i+h_{2i}Q_i))=e(P',R+\Sigma_{i=1}^{k}h_{2i}Q_i)$。所以,本文指出 Wen-Ma 的聚合签名方案是可以普遍伪造的。

3 Dai-Wang-Hu-Yun 方案介绍及安全性分析

3.1 Dai-Wang-Hu-Yun 方案介绍

基于 Hess 的签名方案[5],Dai 等人[6]提出了一个适用于移动商务的基于身份的数字签名方案,它由以下四个算法组成:

a)Setup。G_1 与 G_2 是两个阶为素数 q 的循环群,P 为 G_1 的生成元。$e:G_1\times G_1\to G_2$ 是一个 Tate 映射。PKG 随机选取 $s\in Z_q^*$作为系统主密钥,计算系统公钥 $P_{pub}=sP$。选取两个安全的 hash 函数 $H_1:\{0,1\}^*\to G_1^*$,$H_2:\{0,1\}^*\times G_1\to Z_q$。PKG 秘密保存 s。公开系统参数 params:$\{G_1,G_2,P,e,q,P_{pub},H_1,H_2\}$。

b)Extract Private Key。给定用户 U 的身份 ID,PKG 计算该用户的私钥 $d_{ID}=sQ_{ID}$,其中 $Q_{ID}=H_1(ID)$为用户的公钥。

c)Sign。当要对消息 m 签名时,用户 ID 计算如下:

(a)选随机数 $k\in Z_q*$,计算 $r=kP$;

(b)计算 $v=H_2(m,r)$;

(c)计算 $U=(v/k)d_{ID}$。

则在消息 m 上的签名为(U,r)。

d)Verify。给定消息 m,用户 ID 的公钥 Q_{ID},签名$(U,r))$,验证者计算 $v=H_2(m,r)$,接受签名当且仅当以下等式成立:

$$e(U,r)=e(Q_{ID},P_{pub})^v$$

Dai-Wang-Hu-Yun 方案的安全性分析见文献[6]。

3.2 Dai-Wang-Hu-Yun 方案的安全性分析

Dai-Wang-Hu-Yun 签名方案并不像作者们声称的那样可以为移动商务提供不可否认服务,实质上该签名方案是可以普遍伪造的,下面给出了该方案的两种伪造攻击:

a)第一种攻击方法。敌手 A(不知道用户 ID 的私钥)只要获得用户 ID(公钥 Q_{ID})的一个消息/签名就可以冒充该用户对任意消息签名(A 截获一个消息/签名是很容易的,因为发送消息/签名的信道是公开的)。

假设 A 截获了一个消息/签名对$(m,(U,r))$,A 首先计算 $v=H_2(m,r)$,再计算 $h=v^{-1}\bmod q$,接着可以计算 $T=hU=v^{-1}(v/k)d_{ID}=k^{-1}d_{ID}$。利用 T,A 可以冒充用户 ID 对任意消息 m'签名如下:

(a)选随机数 $k' \in Z_q^*$,计算 $r' = k'r$;

(b)计算 $v' = H_2(m', r')$;

(c)计算 $U' = (v'/k')T$。

则在消息 m' 上的签名为 (U', r')。

该签名 (U', r') 显然可以通过签名的验证等式 $e(U', r') = e(Q_{ID}, P_{pub})^{v'}$。因为:

$$e(U', r') = e((v'/k')T, k'r) = e((v'/k'k)d_{ID}, k'kP) = e(v'd_{ID}, P) = e(Q_{ID}, P_{pub})^{v'}$$

b)第二种攻击方法。Dai-Wang-Hu-Yun 的签名方案是可以普遍伪造的。敌手 A(不知道用户 ID 的私钥)可以冒充用户 ID(公钥 Q_{ID})对任意消息 m' 签名,其操作如下:

(a)选随机数 $k' \in Z_q^*$,计算 $r' = k'P_{pub}$;

(b)计算 $v' = H_2(m', r')$;

(c)计算 $U' = (v'/k')Q_{ID}$。

则在消息 m' 上的签名为 (U', r')。该签名 (U', r') 显然可以通过签名的验证等式

$$e(U', r') = e(Q_{ID}, P_{pub})^{v'}$$

因为: $e(U', r') = e((v'/k')Q_{ID}, k'P_{pub}) = e(Q_{ID}, P_{pub})^{v'}$

4　结束语

本文分析了 Wen 和 Ma 提出的聚合签名方案和 Dai 等人提出的基于身份的签名方案的安全性,指出这两种签名方案都是不安全的,并给出了方案的伪造攻击。

参考文献:

[1] BONEH D, GENTRY C, LYNN B, *et al*. Aggregate and verifiably encrypted signatures from bilinear maps[C]// Proc of Advances in Cryptology-Eurocrypt. Berlin: Springer-Verlag, 2003: 416-432.

[2] XU Jing, ZHANG Zhen-feng, FENG Deng-guo. ID-based aggregate signatures from bilinear pairings [C]// Proc of CANS. Berlin: Springer-Verlag, 2005: 110-119.

[3] GENTRY C, RAMZAN Z. Identity-based aggregate signatures[C]// Proc of PKC. Berlin: Springer, 2006: 257-273.

[4] SONG J, KIM H, LEE S, *et al*. Security enhancement in Ad hoc network with ID-based cryptosystem [C]// Proc of ICACT. Berlin: Springer-Verleg, 2005: 372-376.

[5] BELLARE M, NAMPREMPRE C, NEVEN G. Unrestricted aggregate signatures[C]// Proc of ICALP. Berlin: Springer-Verlag, 2007: 411-422.

[6] LI J, KIM K, ZHANG Fang-guo, *et al*. Aggregate proxy signature and verifiably encrypted proxy signature[C]// Proc of Prov Sec. Berlin: Springer-Verlag, 2007: 208-217.

[7] CHENG X, LIU J, WANG X. Identity-based aggregate and verifiably encrypted signatures from bilinear pairing[C]// Proc of ICCSA. Berlin: Springer-Verlag, 2005: 1046-1054.

[8] SHAMIR A. Identity-based cryptosystems and signature schemes [C]// Proc of Crypto'84. New York: Springer-Verlag, 1985: 47-53.

[9] GUILLOU L, QUISQUATER J. A paradoxical identity-based signature scheme resulting from zero-knowledge[C]// Proc of Advances in Cryptology-CRYPTO'88, LNCS 403. Berlin: Springer-Verlag, 1990: 216-231.

[10] CHA J, CHEON J. An identity-based signature from gap Diffie-Hellman groups[C]// Procof PKC. Berlin: Springer-Verlag, 2003: 18-30.

[11] SAKAI R, OHGISHI K, KASHHARA M. Cryptosystems based on pairing [C]// Proc of Symposium on Cryptography and Information Security. 2000: 26-28.

[12] HESS F. Efficient identity based signature schemes based on pairings [C]// Proc of SAC, LNCS 2595. Berlin: Springer-Verlag, 2003: 310-324.

[13] BARRETO P, LIBERT B, MCCULLAGH N, *et al*. Efficient and provably-secure identity-based signature and signcryption from bilinear maps [C]// Proc of Asiacrypt, LNCS 3788. 2005: 515-532.

[14] WEN Y, MA J. An aggregate signature scheme with constant pairing operations[C]// Proc of International Conference on Computer Science and Software Engineering. [S.l.]: IEEE, 2008: 830-833.

[15] HESS F. Exponent group signature schemes and efficient identity based signature schemes based on pairings[R]. [S.l.]: Cryptology ePrint Archive, 2002.

[16] DAI G, WANG M, HU H, *et al*. An effective signature scheme based on tate pairing for mobile business[C]// Proc of International Conference on Wireless Communications, Networking and Mobile Computing. 2008: 1-4.

(上接第 1855 页)

d)机制缺陷。虽然 Vista 试图在各个环节增加缓冲区溢出的难度,并不能从完全杜绝缓冲区溢出攻击。Vista 安全研究员 Skape 指出,由于 PE 文件映像基址的随机只针对前 16 位,后 16 位不会改变,可以通过覆盖返回地址的后 16 位数据来绕过 ASLR 技术。已经陆续有针对 Vista 的缓冲区溢出攻击问题报道。

4　结束语

正所谓道高一尺,魔高一丈,缓冲区溢出攻击和防御技术都在不断的发展。虽然 Vista 试图从各个方面增加缓冲区溢出攻击的难度,阻断缓冲区溢出对系统的攻击,但是要想完全杜绝缓冲区溢出攻击几乎是不可能的。因此,针对缓冲区溢出攻击,除了增加缓冲区溢出的难度外,还应该在缓冲区溢出攻击成功的情况下,研究如何将危害降低到最小。

参考文献:

[1] COWAN C, WAGLE P, PU C, *et al*. Buffer overflows: attacks and defenses for the vulnerability of the decade[C]// Proc of DARPA Information Survivability Conference and Expo. 2003: 227-237.

[2] ONE A. Smashing the stack for fun and profit[J]. Phrack Magazine, 1996,7(49):14-16.

[3] WHITEHOUSE O. An analysis of address space layout randomization on Windows Vista[EB/OL]. (2007-02-22). http://www.symantel.com/avcenter/reference/Address-space-layout-Randomization.pdf.

[4] SOTIROV A, DOWD M. Bypassing browser memory protections[C]. 2008.

[5] Data execution prevention[EB/OL]. (2003)[2009-04-01]. http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/BookofSP1/b0de1052-4101-44c3-a294-4da1bd1ef227.mspx.

[6] GS (buffer security check)[EB/OL]. [2009-03-15]. http://msdn.microsoft.com/en-us/library/8dbf701c(VS.80).aspx.