对一种改进的 ElGamal 数字签名方案的攻击与改进

周 克 元
(宿迁学院文理学院 江苏 宿迁 223800)

摘 要 针对无 Hash 函数的 ElGamal 离散对数数字签名问题,对其各类改进方案进行分析研究,对最新的改进方案进行伪造签名攻击。给出 4 种伪造签名方法,证明其不具有安全性。针对其方案的缺点提出一个新的改进方案。证明了其正确性和安全性,可防止各种伪造攻击和同态攻击。

关键词 离散对数 数字签名 Hash 函数 伪造攻击 改进

中图分类号 TP309.7 **文献标识码** A DOI:10.3969/j.issn.1000-386x.2019.04.051

ATTACK AND IMPROVEMENT ON AN IMPROVED ELGAMAL DIGITAL SIGNATURE SCHEME

Zhou Keyuan
(*School of Liberal Arts and Science, Suqian College, Suqian 223800, Jiangsu, China*)

Abstract Aiming at the problem of ElGamal discrete logarithmic digital signature without Hash function, we analyzed and studied various improved schemes. In this paper, an improved ElGamal digital signature scheme was analytical attacked. We gave four forgery signature schemes and proved to be insecure. In view of the shortcomings of improved ElGamal digital signature scheme, we proposed a new improved scheme we proved its correctness and security, and it could prevent various forgery attacks and homomorphism attacks.

Keywords Discrete logarithm Digital signature Hash function Forgery attack Improvement

0 引 言

1976 年,Diffie 和 Hellman 提出数字签名概念[1],到目前,数字签名技术得到了长足的发展和极大的应用。数字签名是现代密码学中重要的分支,数字签名技术可广泛应用于数字文档的认证性、完整性和不可否认性,是网络环境下实现数据安全传输的重要手段。

数字签名技术一般依赖的数学难题有离散对数数学难题、因子分解数学难题和椭圆曲线数学难题。ElGamal 数字签名[2]是离散对数数字签名中的一种主要方案,方案有使用 Hash 函数和不使用 Hash 函数两个研究方向。

Hash 函数主要算法有 MD5 和 SHA-1 系列,王小云等[3-5]提出了 MD5 和 SHA-1 算法的杂凑碰撞,使得使用了 MD5 和 SHA-1 的 Hash 函数的相关密码算法不再安全,故设计不使用 Hash 函数的 ElGamal 离散对数数字签名方案成为研究的热点。相关学者对不使用 Hash 函数的 ElGamal 数字签名方案的复杂度和安全性(模指数模逆运算、签名验证方程)进行了各种分析和改进,提出了一系列改进方案。但由于构造者在构造签名方案时考虑得不够周全或者是一味追求签名协议的高效,使得有些签名协议并不安全。曲娜等[6]对原始的 ElGamal 数字签名方案进行了改进,减少了模逆运算的次数,张会影等[7]对 ElGamal 数字签名方案中的随机数进行了改进,增加了一个随机数,提出了一种改进方案,由于该两种方案中各参数之间的联系不够紧密,可被周克元[8]提出的一种伪造攻击方案攻击。白荷芳[9]、芦殿军[10]、李晓峰[11]亦对 ElGamal 数字签名方案进行了研究,提出了相关的改进方案,相关改进方案亦可被文献[8]中方法伪造签名攻击。李丽娟[12]

收稿日期:2017-08-31。宿迁市科研项目(Z201450)。**周克元**,讲师,主研领域:信息安全。

提出了一种新的 ElGamal 数字签名改进方案,声称文献[8]中的攻击方案无法攻击成功,经过分析,李丽娟方案安全性不够,可被包括文献[8]中攻击方法在内的多种方法伪造签名攻击,本文给出了 4 种伪造签名攻击方法。即到目前为止,已有的相关方案均不安全。本文进一步给出了一个新的改进方案,证明了其正确性和安全性。

1 原始无 Hash 函数 ElGamal 数字签名方案[2]

1.1 参数初始化

取大素数 p,取 $p-1$ 阶生成元 $g \in Z_p^*$,任取随机数 $x \in_R Z_{p-1}^*$且满足 $\gcd(x,p-1)=1$,计算 $y=g^x \bmod p$。公钥为(y,g,p),私钥为 x,待签名消息明文为 $m(m<p-1)$。

1.2 签名过程

(1) 随机选择 $k \in_R Z_{p-1}^*$,计算 $r=g^k \bmod p$;

(2) 计算 $s=(m-rx)k^{-1} \bmod (p-1)$;则$(r,s)$为 m 的签名。

1.3 验证过程

验证 $g^m=r^s y^r \bmod p$,正确则接受签名,否则拒绝签名。

2 对 ElGamal 方案的伪造签名攻击

文献[6-7]对 ElGamal 方案进行了改进,分别给出了改进方案。ElGamal 方案、曲娜方案、张会影方案中验证方程可统一为 $g^m=(y^u r^v)^w \bmod p$,该结构可被周克元伪造签名攻击[8],伪造签名攻击思路如下:

选取适当的 r、u、v、w 的值,将$(y^u r^v)^w \bmod p$ 变为 $g^Z \bmod p$ 形式,此时只需设 $m=Z \bmod (p-1)$,代入验证方程,则验证方程一定满足,从而可以伪造签名。下面以无 Hash 函数的 ElGamal 签名方案为例给出伪造签名攻击方法:

任取整数 $u,v<p-1$,设 $r=g^u y^v \bmod p$,$s=-v^{-1} r \bmod (p-1)$,$m=us \bmod (p-1)$,则(r,s)是 m 的有效签名。其中 v^{-1} 可由欧几里德扩展算法从 $vv^{-1} \bmod (p-1)=1$ 中计算出。

证明:验证方程右 $=g^{us}y^{vs}g^{xr} \bmod p=g^{us+xvs+xr} \bmod p=$

$$g^{us-xvv^{-1}r+xr} \bmod p=g^{us} \bmod p=$$

$$g^m \bmod p=\text{左}$$

验证方程成立,所以(r,s)是 m 的有效签名。

其他相似的研究中,白荷芳方案[9]验证方程为 $y^s r^r \bmod p=g^m \bmod p$,芦殿军方案[10]中验证方程为 $g^{ms^{-1}} r^{rs^{-1}} \bmod p \bmod q=y \bmod p \bmod q$(等价于 $g^m \bmod p \bmod q=y^s r^{-r} \bmod p \bmod q$),李晓峰方案[11]的验证方程为 $y^r r^n n^s \bmod p=g^m \bmod p$,显然均可被文献[5]中伪造签名攻击方法攻击,具体过程略。

3 李丽娟方案[12]

李丽娟亦对该类方案进行了分析,针对上述 m 放在指数中可被攻击的情况,提出一个改进方案,将消息 m 放在验证方程的底数中,宣称可以避免文献[8]中的攻击方法,李丽娟方案如下。

3.1 参数初始化

取大素数 p,取 $p-1$ 阶生成元 $g \in Z_p^*$,取随机数 $x \in_R Z_{p-1}^*$且满足 $\gcd(x,p-1)=1$,计算 $y=g^x \bmod p$。公钥为(y,g,p),私钥为 x,待签消息为 $m(m<p-1)$。

3.2 签名过程

(1) 随机选择两个不同整数 $k,t \in Z_{p-1}^*$,计算 $r=mg^k \bmod p$,$n=mg^t \bmod p$。随机整数 k、t 为临时密钥,不能泄露;

(2) 计算 $s=(1-tr-kn)s=(1-tr-kn)x^{-1} \bmod p-1$,则$(r,s,n)$为消息 m 的有效签名。

3.3 验证过程

验证方程为 $y^s r^n n^r=gm^{r+n} \bmod p$,正确则接受签名,否则拒绝签名。

4 对李丽娟方案的伪造签名攻击

李丽娟为防止文献[8]中的方法攻击,将验证方程中含有 m 项中的 m 放在底数中,改为 m^{r+u}形式。但实际情况却是可对验证方程两边求$(r+u)^{-1} \bmod p-1$ 指数运算,从而求出 m,此时将求出的 m 代入验证方程,则验证方程一定满足,从而伪造签名成功。文献[8]中攻击方法对李丽娟方案的伪造签名攻击过程见 4.1 节。

4.1 伪造签名攻击 1

任取整数 $u,v<p-1$,设 $r=g^u y^v \bmod p$,$n=1$,$s=-v \bmod p-1$,$m=g^{(u-1)(r+1)^{-1}} \bmod p$,则$(r,s,1)$是 m 的有效签名。其中$(r+1)^{-1} \bmod p-1$ 可由欧几里德扩展算法从$(r+1)(r+1)^{-1} \bmod p-1=1$ 中计算出。

证明:验证方程左 $=y^s r \bmod p = y^s g^u y^v \bmod p = g^u \bmod p$

右 $= gm^{r+n} \bmod p = gg^{(u-1)(r+1)^{-1}(r+1)} \bmod p =$

$gg^{u-1} \bmod p = g^u \bmod p =$ 左

验证方程成立,所以$(r,s,1)$是 m 的有效签名。

除此之外,李丽娟方案还有其他三种伪造签名攻击方法,具体过程如下。

4.2　伪造签名攻击 2

任取整数 $a,b<p-1$,取 $r=1$,$n=g^a y^b \bmod p$,$s=-b \bmod p-1$,$m=g^{(a-1)(1+n)^{-1}} \bmod p$,则$(r,s,1)$是 m 的有效签名。其中$(1+n)^{-1} \bmod p-1$ 可由欧几里德扩展算法从$(1+n)(1+n)^{-1} \bmod p-1=1$ 中计算出。

证明:验证方程左 $=y^s g^a y^b \bmod p = g^a \bmod p$

右 $= gg^{(a-1)(1+n)^{-1}(1+n)} \bmod p = g^a \bmod p =$ 左

验证方程成立,所以$(1,s,n)$是 m 的有效签名。

4.3　伪造签名攻击 3

任取整数 $u,v,a,b<p-1$,取:

$$r=g^u y^v \bmod p, n=g^a y^b \bmod p$$

$$s=(vn+br) \bmod p-1$$

$$m=g^{(un+ar-1)(r+n)^{-1}} \bmod p$$

则(r,s,n)是 m 的有效签名。其中$(r+n)^{-1} \bmod p-1$ 可由欧几里德扩展算法从$(r+n)(r+n)^{-1} \bmod p-1=1$ 中计算出。

证明:验证方程左 $=y^s g^{un} y^{vn} g^{ar} y^{br} \bmod p =$

$y^{s+vn+br} g^{un+ar} \bmod p =$

$g^{un+ar} \bmod p$

右 $= gg^{(un+ar-1)(r+n)^{-1}(r+n)} \bmod p = g^{un+ar} \bmod p =$ 左

验证方程成立,所以(r,s,n)是 m 的有效签名。

4.4　伪造签名攻击 4

任取整数 $r,s,n<p-1$,要求 $gcd(r+n,p-1)=1$,则逆元$(r+n)^{-1} \bmod p-1$ 存在,可由欧几里德扩展算法从$(r+n)(r+n)^{-1} \bmod p-1=1$ 中计算出。取 $m=(y^s r^n n^r g^{-1})^{(r+n)^{-1}} \bmod p$,则$(r,s,n)$是 m 的有效签名。

证明:验证方程右 $= gm^{r+n} \bmod p = gy^s r^n n^r g^{-1} \bmod p =$

$y^s r^n n^r \bmod p =$ 左

验证方程成立,所以(r,s,n)是 m 的有效签名。

4.5　攻击方法分析

上述给出的 4 种攻击方法中的消息 m,只是一些特殊的消息,甚至是一些无意义的消息,还不能对任意有意义的消息 m 进行伪造攻击,但足可以对李丽娟方案形成威胁。

上述各类攻击方案攻击成功的主要原因为在验证方程中,消息明文 m 单独出现,或者仅出现在指数中,或者仅在底数中。若在验证方程中将 m 设计为在指数和底数中都出现,则上述攻击方法将无法求出 m 的值,从而可以有效避免上述伪造签名攻击。下面给出李丽娟方案的改进方案。

5　改进方案设计

5.1　方案具体过程

(1) 参数初始化:取大素数 p,取 $p-1$ 阶生成元 $g \in Z_p^*$,随机选取$x \in_R Z_{p-1}^*$且满足 $\gcd(x,p-1)=1$,计算 $y=g^x \bmod p$。公钥为(y,g,p),私钥为 x,待签名明文消息为 $m(m<p-1)$。

(2) 签名过程:

① 随机任取两个不同整数 $k,t<p-1$,计算 $r=mg^k \bmod p$,$n=mg^t \bmod p$。随机整数 k、t 为临时密钥,不能泄露。

② 计算 $s=(m-tr-kn)x^{-1} \bmod p-1$,则$(r,s,n)$为消息 m 的有效签名,其中 x^{-1}可预求逆以减少运算时间。

(3) 验证过程:验证方程为 $y^s n^r r^n \bmod p = g^m m^{r+n} \bmod p$,正确则接受签名,否则拒绝签名。

(4) 正确性证明:验证方程左 $= g^{xs} m^r g^{tr} m^n g^{kn} \bmod p = g^{xs+tr+kn} m^{r+n} \bmod p = g^m m^{r+n} \bmod p =$ 右。

5.2　安全性分析

(1) 对抗从公钥中揭露私钥的攻击:攻击者若想从 $y=g^x \bmod p$ 求出 x,该问题为求解离散对数数学难题。

(2) 对抗从签名中求出私钥的攻击:验证者 B 接收到 A 发送的签名(r,s,n)后,若想利用签名值从签名方程 $s=(m-tr-kn)x^{-1} \bmod p-1$ 中求出发送者 A 的私钥 x,但签名方程含有三个未知参数 t、k、x,故无法求出发送者 A 的私钥 x。

(3) 抗替换消息伪造签名攻击:验证者 B 接收到签名消息$(m;r,s,n)$后,用另一消息 m'替换原有消息 m,进行伪造签名攻击,由签名过程,可计算出 $r'=rm' m^{-1} \bmod p$,$n'=nm' m^{-1} \bmod p$,但 s 值的计算需要 t、k、x 的值,故无法求出 s 值,替换消息伪造签名无法成功。

(4) 防止第 4 节中的 4 种方法的伪造签名攻击:第 4 节中的四种伪造攻击方法的本质是设计一些签名值 r、s、n,将其代入验证方程,由验证方程求出 m 的值,再将 r、s、n、m 代入验证方程,则验证方程显然成立,伪造签名攻击成功。

(下转第 333 页)

sorship in the network infrastructure[C]//Proceedings of the 20th USENIX conference on Security. USENIX Association Berkeley, 2011.

[15] Morrell C, Ransbottom J S, Marchany R, et al. Scaling IPv6 address bindings in support of a moving target defense [C]//The 9th International Conference for Internet Technology and Secured Transactions(ICITST-2014). IEEE, 2015: 440 - 445.

[16] 郭志强, 王振兴, 张连成,等. 基于 Hash 生成地址的移动 IPv6 高效安全路由优化方案[J]. 计算机应用与软件, 2016,33(6):105 - 109.

[17] Heydari V, Kim S I, Yoo S M. Anti-Censorship Framework using Mobile IPv6 based Moving Target Defense[C]//Proceedings of the 11th Annual Cyber and Information Security Research Conference. ACM, 2016.

[18] Arkko J, Vogt C, Haddad W. Enhanced Route Optimization for Mobile IPv6[EB/OL]. RFC 4866, Internet Requests for Comments,May 2007.

[19] Perkins C. Securing Mobile IPv6 Route Optimization Using a Static Shared Key[EB/OL]. RFC 4449, Internet Requests for Comments,Jun. 2006.

[20] Nikander P, Arkko J, Aura T, et al. Mobile IP Version 6 Route Optimization Security Design Background[EB/OL]. RFC 4225, Internet Requests for Comments, Dec. 2005.

[21] Kang D, Jung J, Lee D, et al. Security analysis and enhanced user authentication in proxy mobile IPv6 networks [J]. Plos One, 2017, 12(7):e0181031.

[22] Wakikawa R, Devarapalli V, Tsirtsis G, et al. Multiple Care-Of Addresses Registration[EB/OL]. RFC 5648, Internet Requests for Comments, Oct. 2009.

[23] Guo N, Peng F, Gao T. Secure Mobility Management for MIPv6 with Identity-Based Cryptography[M]//Information and Communication Technology. Springer International Publishing, 2015.

(上接第 325 页)

本文改进方案的验证方程为 $y^s n^r r^n \bmod p = g^m m^{r+n} \bmod p$,由于 m 同时出现在指数和底数中,即使验证方程中的其他参数均已知,也无法求出 m 的值,故第 4 节中的四种攻击方法均无法攻击成功,改进方案安全。

(5) 防止参数 k 同态攻击:假设签名者使用相同的参数 t 和不同的 k_1、k_2、k_3 对消息 m_1、m_2、m_3 签名,满足 $k_3 = k_1 + k_2 \bmod p - 1$,签名分别为:$(m_1; r_1, s_1, n_1)$、$(m_2; r_2, s_2, n_2)$、$(m_3; r_3, s_3, n_3)$,则有:

$$s_1 = (m_1 - tr_1 - k_1 n_1) x^{-1} \bmod p - 1$$

$$s_2 = (m_2 - tr_2 - k_2 n_2) x^{-1} \bmod p - 1$$

$$s_3 = (m_3 - tr_3 - k_3 n_3) x^{-1} \bmod p - 1 = (m_3 - tr_3 - (k_1 + k_2) n_3) x^{-1} \bmod p - 1$$

其中:x、t、k_1、k_2 未知,3 个方程 4 个未知量,无法求解,故同态攻击无法成功。

6 结　语

本文对各类改进的 ElGamal 离散对数数字签名方案进行了分析,对改进方案李丽娟方案进行了攻击分析,给出了 4 种攻击方法,证明了其存在安全缺陷。给出了一个新的改进方案,证明了其正确性和安全性,证明了其可防止伪造签名攻击和同态攻击。很好地解决了无 Hash 函数的 ElGamal 数字签名的改进问题。

参 考 文 献

[1] Diffie W, Hellman M. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644 - 654.

[2] El-Gamal T. A public-key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Trans. Inf. Theory, 1985, 31(4):469 - 472.

[3] Wang X, Lai X, Feng D, et al. Cryptanalysis of the hash functions MD4 and RIPEMD[C]//Proceedings of the 24th annual international conference on Theory and Applications of Cryptographic Techniques. Berlin:Springer-Verlag,2005.

[4] Wang X Y, Yu H B. How to Break MD5 and other Hash Functions [C]//Eurocrypt 2005. Berlin: Springer-Verlag, 2005: 1 - 8.

[5] Wang X Y, Yin Y L, Yu H B. Finding Collisions in the Full SHA-1[C]//Proceedings of the 25th annual international conference on Advances in Cryptology. Berlin:Springer-Verlag,2005: 17 - 36.

[6] 曲娜, 杜洪军, 颜达, 等. ELGamal 数字签名算法的一种变形[J]. 吉林大学学报(信息科学版), 2009, 27(6): 590 - 594.

[7] 张会影, 张军. 一种改进的 ElGamal 数字签名方案的研究与设计[J]. 计算机工程与科学, 2009, 31(12):35 - 37.

[8] 周克元. 对两个离散对数数字签名算法的攻击与改进[J]. 科学技术与工程, 2013, 13(32):9725 - 9729.

[9] 白荷芳, 王彩芬. 对一种变形 ELGamal 签名体制的分析[J]. 西北师范大学学报(自然科学版), 2006, 42(3): 109 - 110.

[10] 芦殿军,张秉儒. EIGamal 签名方案的安全性分析与改进[J]. 长江大学学报(自然科学版),2008,5(1):193 - 194.

[11] 李晓峰, 赵海, 王家亮, 等. 基于增加一个随机数的 ElGamal 数字签名算法的改进[J]. 东北大学学报(自然科学版), 2010, 31(8):1102 - 1105.

[12] 李丽娟,郭亚杰. 一种改进的 ElGamal 数字签名方案[J]. 计算机工程与科学,2016,38(6):1097 - 1102.