

一种前向安全数字签名方案的分析及改进

李顺波^{1,2}, 黄光球¹, 彭家龙²

(1. 西安建筑科技大学 管理学院, 陕西 西安 710055;
2. 西安建筑科技大学 理学院, 陕西 西安 710055)

摘要:前向安全在实际应用中能有效减少私钥泄露对过去时间段签名带来的损失,但会影响未来时段签名的安全性。针对未来时间段的私钥泄露问题,提出了一种强前向安全的数字签名方案。先是对刘亚丽(2010)等提出的基于模 m 的 n 方根难题的ElGamal前向安全数字签名方案进行了分析,发现该方案并不能保证未来时间段签名的安全性,即不具备后向安全。于是借助单向散列链技术对该方案的私钥更新和签名算法进行了有效改进,在刘亚丽所提方案的基础上构造了一种基于ElGamal体制的数字签名方案,并对该方案进行了分析。分析结果表明,新方案是正确有效的,同时具有前向安全性和后向安全性。

关键词:前向安全;后向安全;数字签名;ElGamal;单向散列链

中图分类号:TP309

文献标识码:A

文章编号:1673-629X(2016)11-0093-04

doi:10.3969/j.issn.1673-629X.2016.11.021

Analysis and Improvement for a Digital Signature Scheme of Forward Security

LI Shun-bo^{1,2}, HUANG Guang-qiu¹, PENG Jia-long²

(1. School of Management, Xi'an University of Architecture and Technology, Xi'an 710055, China;
2. School of Science, Xi'an University of Architecture and Technology, Xi'an 710055, China)

Abstract: Forward security can effectively reduce the damage caused by exposure of the secret key in the past time period, but may affect the signature in the future period. In order to solve this problem, a strong forward-secure signature is proposed. Firstly, Liu Yali's ElGamal forward-secure signature scheme in 2010 based on n root of module m is analyzed, and this scheme is not backward security, which means it can't guarantee the signature security in the future period. Then, by using a one-way hash chain, the key updating and signature algorithm is improved effectively. A new digital signature scheme based on ElGamal is presented on the basis of Liu's scheme and analyzed. The result shows that the new scheme is correct and feasible, with forward and backward security.

Key words: forward-secure; backward-secure; digital signature; ElGamal; one-way hash chain

0 引言

数字签名是公钥加密技术和数字摘要技术的应用,是保证数据机密性、完整性、真实性、不可否认性的有效手段,已广泛应用于电子商务、金融等领域。根据Kerckhof假设密码算法是公开的,其安全性完全依赖于私钥的安全性。一旦私钥被泄露,不仅当前的数字签名安全性受到威胁,而且过去时段签名的安全性也不能保证,势必导致原来签署的所有签名都作废。针对这个问题,Anderson^[1]于1997年首次提出前向安全

签名(Forward-secure signature)的思想,即当前私钥的暴露不会影响过去签名的安全性。1999年,Bellare和Miner^[2]具体给出了前向安全签名的正式定义,并构造了一种前向安全签名方案。2001年,Burmester等^[3]提出了强前向安全的概念,即同时保证前向安全和后向安全。随着电子商务和网络的发展,前向安全已成为信息安全领域的研究热点,提出了基于属性的前向安全^[4]、基于双线性对的前向安全^[5]、基于格的前向安全^[6]、强前向安全^[7-10]、前向安全代理^[11]等数字签名方案。

收稿日期:2015-09-11

修回日期:2015-12-24

网络出版时间:2016-10-24

基金项目:国家自然科学基金资助项目(11471255, 11526161);陕西省自然科学基金(2014JQ1027, 2015JQ1014);陕西省教育厅基金(2013JK0589);西安建筑科技大学基金(RC1338, RC1438, JC1321, JC1416)

作者简介:李顺波(1979-),男,副教授,博士,CCF会员,研究方向为密码学与信息安全。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20161024.1105.004.html>

2003 年,吴克力等^[12]给出了基于 ElGamal 体制的前向安全数字签名方案。接着夏峰等^[13]指出吴克力提出的方案并不具备前向安全性,并提出了一种新的基于 ElGamal 体制的前向安全签名方案,可以将当前私钥隐藏在签名中,确保签名具有前向安全性。2009 年,郭远等^[14]改进初始参数和私钥更新算法,设计了一种基于 ElGamal 体制的前向安全签名方案,但该方案无法保证其后向安全性。随后廖小平^[15]引入单向散列链对郭远的方案进行了改进,给出的方案既是前向安全又是后向安全的。2010 年,刘亚丽等^[16]构造了新的密钥生成算法,利用离散对数和合数模平方根困难问题,提出了一种基于 ElGamal 的前向安全签名方案,该方案具有前向安全性且优于夏峰的签名方案。

前向安全签名在当前私钥泄露时不会对过去时间段的签名造成危害,而后向安全能保证当前私钥的泄露不会对未来时段的私钥造成影响,即不必每次检测出私钥泄露就撤销当前的私钥系统而重建新的密钥系统。通过分析刘亚丽提出的方案,发现其无法保证后向安全性,文中借助单向散列链技术,改进方案的私钥进化和签名算法,给出了基于 ElGamal 体制的强前向安全数字签名方案。该方案可在满足前向安全性的基础上获得后向安全性。

1 前向安全数字签名

前向安全的基本思想是如果用户当前时间段的私钥泄露了,攻击者虽然可以伪造此时段后的签名,但无法伪造过去时间段的签名;其本质是将签名私钥泄露所带来的影响和损失尽可能减少到最小。前向安全数字签名方案主要由四部分组成:公钥和初始私钥生成、私钥更新、签名算法、验证算法。其关键是签名私钥的更新和签名算法。

用户先注册得到公钥 PK 和相应的初始私钥 SK_0 ,将私钥的有效期分成 T 个时段,分别记为 $1, 2, \dots, T$ 。在有效时段内,公钥 PK 是固定不变的,私钥随着时段的变化进行更新,记 i 时段的私钥为 SK_i ,更新公式为 $SK_i = h(SK_{i-1})$, h 是一个单向函数,求出 SK_i 后立即删除 SK_{i-1} 。这样当攻击者在 i 时段截获私钥 SK_i ,但无法获得前时段的私钥 $SK_{i-1}, SK_{i-2}, \dots, SK_0$,因此前向的私钥是安全的,称之为前向安全,其私钥更新过程如图 1 所示。

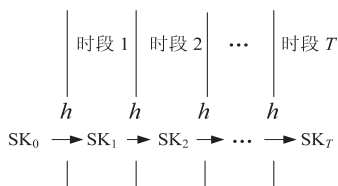


图 1 前向安全数字签名的私钥更新过程

2 刘亚丽方案及其安全性分析

2.1 刘亚丽的签名方案

(1) 初始参数。

选择一个大素数 p 和随机数 SK_0 (小于 p), g 是 $GF(p)$ 的生成元。计算 $PK = SK_0^{2^T} \bmod p$; 公开 p, g, T 和 PK 。

(2) 私钥更新算法。

若 $i = T + 1$, 则 SK_i 为空串。若 $1 \leq i \leq T$, 则 $SK_i = SK_{i-1}^2 \bmod (p-1) = SK_0^{2^i} \bmod (p-1)$ 。

(3) 签名算法。

① 选择随机数 $k \in Z_p$, 计算 $r = g^k \bmod p$;

② 选择随机数 $\mu \in Z_p$, 计算 $\omega = SK_i g^\mu \bmod p$;

③ 计算 $\delta = (H(m) + 2^{T-i} \mu r) k^{-1} \bmod (p-1)$, 其中 m 为签名消息;

④ 发送签名 (i, r, ω, δ) 给验证方。

(4) 验证算法。

如果 $(PK \omega^{-2^{T-i}})^r r^\delta = g^{H(m)} \bmod p$ 为真, 则认为签名有效; 否则, 认为无效。

2.2 刘亚丽方案的安全性分析

(1) 刘亚丽方案基于求合数模平方根和离散对数困难问题, 将当前时段签名密钥隐藏且仅使用密钥有关信息进行签名, 从而无法获得过去时段的私钥和签名, 具有前向安全性和抗伪造性。

(2) 方案不具备后向安全性。

若攻击者窃取了第 i ($1 \leq i \leq T$) 时段的私钥 SK_i , 私钥更新算法 $SK_{i+1} = SK_i^2 \bmod (p-1)$ 是公开的, 通过它可以求出 i 时段以后的所有私钥。假设攻击者求得 $i+3$ 时段的私钥 SK_{i+3} , 步骤如下:

① 签名方选择随机数 k' , 计算 $r' = g^{k'} \bmod p$;

② 签名方选择随机数 μ' , 计算 $\omega' = SK_{i+3} g^{\mu'} \bmod p$;

③ 计算 $\delta' = (H(m) + 2^{T-i-3} \mu' r') k'^{-1} \bmod (p-1)$, 则用户对消息 m 在 $i+3$ 时段的签名为 $(i+3, r', \omega', \delta')$, 并发给验证方;

④ 验证方利用签名方的公钥 PK, 验证下面等式是否成立:

$$(PK \omega'^{-2^{T-i-3}})^{r'} (r')^{\delta'} = g^{H(m)} \bmod p$$

因为:

$$(PK \omega'^{-2^{T-i-3}})^{r'} (r')^{\delta'} = [SK_0^{2^T} (SK_{i+3} g^{\mu'})^{-2^{T-i-3}}]^{r'}$$

$$(g^{k'})^{(H(m) + 2^{T-i-3} \mu' r') k'^{-1}} =$$

$$[SK_0^{2^T} (SK_{i+3} g^{\mu'})^{-2^{T-i-3}}]^{r'} g^{(H(m) + 2^{T-i-3} \mu' r')} =$$

$$(g^{-2^{T-i-3} \mu'})^{r'} g^{(H(m) + 2^{T-i-3} \mu' r')} = g^{H(m)} \bmod p$$

所以攻击成功, 即攻击者获得 i 时段的私钥 SK_i 后, 可以伪造出 i 时段以后的所有签名并通过验证算法, 即该方案不满足后向安全性。

3 基于 ElGamal 体制的强前向安全数字签名方案

新方案将借助单向散列链技术,改进初始参数、签名算法和验证算法。使得构造的方案既有前向安全性,又有后向安全性,即强前向安全的,从整体上有效地提高了数字签名的安全性。

3.1 单向散列链

单向散列函数 h (又称哈希函数、杂凑函数) 是将任意长度的消息 x 映射成一个固定长度的函数。满足 3 个性质:

- (1) 给定 x , 容易计算 $h(x)$ 。
 - (2) 给定 $h(x)$, 求出 x 在计算上是不可行的; 称为单向性。
 - (3) 找到两个值 x 和 y , 且 $x \neq y$, 使得 $h(x) = h(y)$ 在计算上是不可行的, 称为抗弱碰撞性。
- 对于随机选取的种子值 a (个人密码), 用单向散列函数 h 通过递归散列运算 $h^i(a) = h(h^{i-1}(a))$ ($i = 1, 2, \dots, T$ 且 $h^0(a) = a$) 构造长度为 T 的一串散列值 $a, h(a), h^2(a), \dots, h^i(a), \dots, h^{T-1}(a)$ 称为时段 T 的单向散列链。

令 $x_i = h^{T-i}(a)$, 也就是说 x_i 是散列链中的第 $T - i$ 个散列值, 如表 1 所示。当攻击者截获第 i 时段的 x_i , 可由公式 $x_{i-1} = h^{T-i+1}(a) = h(h^{T-i}(a)) = h(x_i)$ 容易得到前一时段 $i - 1$ 的 x_{i-1} 。但当攻击者窃取第 i 时段的 x_i 时, 由于 h 的单向性, 无法用公式 $x_i = h(x_{i+1})$ 获得后一时段的 x_{i+1} 。因此表 1 构造的散列链 $x_1, x_2, \dots, x_i, \dots, x_T$ 能保证其后向安全性, 为强前向安全的数字签名提供了设计理念。

表 1 时段 T 对应的散列链

时段	散列值	x 的值
1	$h^{T-1}(a)$	x_1
...
$i - 1$	$h^{T-i+1}(a)$	x_{i-1}
i	$h^{T-i}(a)$	x_i
...
T	$h^0(a)$	x_T

3.2 强前向安全签名方案

- (1) 初始参数。
 - ① 选择一个大素数 p 和随机数 SK_0 (小于 p) , g 是 $GF(p)$ 的生成元。计算 $PK = SK_0^{2^T} \bmod p$ 。
 - ② 选择随机数 a , 并计算 $x_0 = h^T(a)$ 。
 - ③ 公开 p, g, x_0, T 和 PK 。
- (2) 私钥更新算法。

若 $i = T + 1$, 则 SK_i 为空串。若 $1 \leq i \leq T$, 则 $SK_i = SK_{i-1}^{2^T} \bmod p$ 。

- (3) 签名算法。
 - ① 签名方生成第 i 时段和 $i + 1$ 时段的散列值 x_i 和 x_{i+1} , 其中 $x_i = h^{T-i}(a)$, $x_{i+1} = h^{T-i-1}(a)$ 。
 - ② 签名方选择随机数 $\mu \in Z_p$, 计算 $\omega = SK_i g^\mu \bmod p, r_i = g^{x_i} \bmod p$ 。
 - ③ 计算 $\delta = (H(m) + 2^{T-i} \mu r_i) x_i^{-1} \bmod (p - 1)$, 其中 m 为签名消息。
 - ④ 发送 (i, r_i, ω, δ) 给验证方。
- (4) 验证算法。

如果 $(PK \omega^{-2^{T-i}})^{r_i} r_i^\delta = g^{H(m)} \bmod p$ 为真, 则认为签名 (i, r_i, ω, δ) 有效; 否则, 认为 (i, r_i, ω, δ) 无效。
- (5) 安全性分析。
 - ① 有效性。

考察验证算法中的等式:

$$(PK \omega^{-2^{T-i}})^{r_i} r_i^\delta \bmod p = [SK_0^{2^T} (SK_i g^\mu)^{-2^{T-i}}]^{r_i} (g^{x_i})^{(H(m) + 2^{T-i} \mu r_i) x_i^{-1}} \bmod p = [SK_0^{2^T} (SK_0^{2^i} g^\mu)^{-2^{T-i}}]^{r_i} g^{H(m) + 2^{T-i} \mu r_i} \bmod p = [(g^\mu)^{-2^{T-i}}]^{r_i} g^{H(m) + 2^{T-i} \mu r_i} \bmod p = g^{H(m)} \bmod p$$
因此待验证的等式成立, 该签名方案正确, 且 (i, r_i, ω, δ) 为有效的数字签名方案。
 - ② 抗伪造性。

方案采用刘亚丽的方法。当攻击者截获了第 i 时段的签名 (i, r_i, ω, δ) , 由 $\omega = SK_i g^\mu \bmod p$, 若想通过 ω 得到隐藏的私钥 μ 是求解离散对数问题, 计算上是不可行的。

假若攻击者伪造了第 i 时段的私钥 SK'_i , 随机选取私钥 μ' 构造 $\omega' = SK'_i g^{\mu'} \bmod p$, 进而伪造第 i 时段的签名 $(i, r_i, \omega', \delta')$, 但在验证过程中由于 $SK'_i \neq SK_i$, 有 $(PK \omega'^{-2^{T-i}})^{r_i} r_i^{\delta'} \neq (PK \omega^{-2^{T-i}})^{r_i} r_i^\delta$, 因此验证算法无法通过, 该方案具有抗伪造性。

- ③ 前向安全性。

该方案的私钥更新算法 $SK_i = SK_{i-1}^{2^T} \bmod (p - 1)$ 基于 Rabin 模合数的平方根问题, 其等同于大数分解困难问题, 因此私钥的更新具有前向安全性。

由于签名算法 $\omega = SK_i g^\mu \bmod p$ 中有私钥 SK_i 的参与, 保证了其签名算法也具有前向安全性。

- ④ 后向安全性。

若攻击者截获了第 i 时段的签名 (i, r_i, ω, δ) , 尽管知道了 $r_i = g^{x_i} \bmod p$, 但 x_i, x_{i+1} 在单向散列链中且满足 $x_i = h(x_{i+1})$, 无法由 x_i 得到 x_{i+1} 。因此攻击者无法获得未来时段的签名, 也就是说即使第 i 时段的密钥泄露, 也不会影响此后时段签名的安全性。因此, 该方案具有后向安全性。
- 综上所述, 新方案具有不可伪造性、前向安全性和后向安全性; 借助单向散列链技术可以有效地提高签

名方案的安全性。

4 结束语

前向安全签名方案能有效降低因私钥泄露而造成的损失,但其普遍存在的缺陷就是无法保证私钥泄露后未来时段签名的安全性和及时发现机制。文中借助单向散列链技术,对刘亚丽的前向安全签名方案进行了改进,新方案弥补了其向后安全性,构造了基于 ElGamal 体制的强前向安全数字签名方案,该方案既具有前向安全性又有后向安全性。

参考文献:

- [1] Anderson R. Two remarks on public key cryptology [C]//The fourth annual conference on computer and communications security. New York: [s. n.], 1997:151-160.
 - [2] Bellare M, Miner S K. A forward-secure digital signature scheme [C]//Advances in Cryptology - Crypto '99. Berlin: Springer-Verlag, 1999:431-448.
 - [3] Burmester M, Chrissikopoulos V, Kotzanikolaou P, et al. Strong forward security [M]//Trusted information. US: Springer, 2001:109-121.
 - [4] 魏江宏,刘文芬,胡学先. 前向安全的密文策略基于属性加密方案[J]. 通信学报,2014,35(7):38-45.
 - [5] Yu Jia, Kong Fanyu, Cheng Xiangguo, et al. One forward-secure signature scheme using bilinear maps and its applications [J]. Information Sciences, 2014, 279:60-76.
 - [6] 李明祥,安 妮. 基于格的前向安全签名方案[J]. 密码学报,2016,3(3):249-257.
 - [7] 阿力木江·艾沙,库尔班·吾布力,艾斯卡尔·艾木都拉,等. 一种强前向安全数字签名方案[J]. 计算机工程与应用,2008,44(9):107-108.
 - [8] 徐光宝,姜东焕,梁向前. 一种强前向安全的数字签名方案[J]. 计算机工程,2013,39(9):167-169.
 - [9] 廖小平,蔡光兴. 一类具有强前向安全性的数字签名方案[J]. 湖北工业大学学报,2011,26(2):126-130.
 - [10] 王明伟,胡予濮. 一种前向-后向安全的数字签名方案[J]. 西安电子科技大学学报,2014,41(2):71-78.
 - [11] 曹 欣,魏仕民,卓泽朋. 三个前向安全代理签名方案的安全性分析[J]. 计算机工程与应用,2015,51(7):98-100.
 - [12] 吴克力,王庆梅,刘凤玉. 一种具有前向安全的数字签名方案[J]. 计算机工程,2003,29(8):122-123.
 - [13] 夏 峰,谢冬青,匡华清. 一类前向安全数字签名方案的分析与改进[J]. 计算机工程,2006,32(16):146-147.
 - [14] 郭 远,徐赐文. 基于 ElGamal 的前向安全签名方案的分析与改进[J]. 电脑知识与技术,2009,15(6):1459-1460.
 - [15] 廖小平. 前向安全数字签名方案的分析与改进[J]. 计算机与信息技术,2012,20(1):45-47.
 - [16] 刘亚丽,秦小麟,殷新春,等. 基于模 m 的 n 方根的前向安全数字签名方案的分析与改进[J]. 通信学报,2010,31(6):82-88.
-
- (上接第 92 页)
- and Applications, 2010, 362(2):415-426.
 - [4] Huang Y, Ng M, Wen Y. A new total variation method for multiplicative noise removal [J]. SIAM Journal on Imaging Sciences, 2009, 2(1):20-40.
 - [5] Donoho D L, Johnstone M. Adapting to unknown smoothness via wavelet shrinkage [J]. Journal of the American Statistical Association, 1995, 90(432):1200-1224.
 - [6] Geman D, Geman S. Stochastic relaxation, Gibbs distributions, and the Bayesian restoration of images [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1984(6):721-741.
 - [7] Rudin L, Osher S, Fatemi E. Nonlinear total variation based noise removal algorithms [J]. Physica D: Nonlinear Phenomena, 1992, 60(1):259-268.
 - [8] Strong D M, Chan T F. Spatially and scale adaptive total variation based regularization and anisotropic diffusion in image processing [C]//Diusion in image processing, UCLA math department cam report. [s. l.]: [s. n.], 1996.
 - [9] Dong G, Guo Z, Wu B. A convex adaptive total variation model based on the gray level indicator for multiplicative noise removal [C]//Abstract & applied analysis. [s. l.]: Hindawi Publishing Corporation, 2013.
 - [10] 胡学刚,张龙涛,蒋 伟. 基于偏微分方程的变分去噪模型 [J]. 计算机应用,2012,32(7):1879-1881.
 - [11] 胡学刚,楼越芳. 一种去除 Gamma 乘性噪声的全变分模型 [J]. 四川大学学报:工程科学版,2014,46(2):59-65.
 - [12] Wang Y, Yang J, Yin W, et al. A new alternating minimization algorithm for total variation image reconstruction [J]. SIAM Journal on Imaging Sciences, 2008, 1(3):248-272.
 - [13] 张红英,彭启琮. 变分图像复原中 PDE 的推导及其数值实验 [J]. 计算机工程与科学,2006,28(6):44-46.
 - [14] Shen J, Chan T F. Mathematical models for local nontexture inpaintings [J]. SIAM Journal on Applied Mathematics, 2002, 62(3):1019-1043.