·安全技术· 文章编号：1000—3428(2013)09—0167—03 文献标识码：A 中图分类号：TP309

一种强前向安全的数字签名方案

徐光宝，姜东焕，梁向前

(山东科技大学信息科学与工程学院，山东 青岛 266590)

摘 要： 针对传统数字签名方案中的密钥泄露问题，在 Guillou-Quisquater 签名体制和 Rabin 密码体制的基础上，提出一个强前向安全的数字签名方案。通过引入双密钥，使攻击者即使得到签名者当前时段的 2 个签名密钥，也无法伪造其以前和此后时段的有效签名。分析结果表明，该方案是正确和安全的，同时具有前向安全和后向安全性，耗费时间较少。

关键词： 数字签名；前向安全；后向安全；强前向安全；Guillou-Quisquater 签名体制；Rabin 密码体制

A Strong Forward-secure Digital Signature Scheme

XU Guang-bao, JIANG Dong-huan, LIANG Xiang-qian

(*College of Information Science and Engineering, Shandong University of Science and Technology, Qingdao 266590, China*)

【Abstract】 Aiming at the problem of key disclose in existed digital signature schemes, a strong forward secure signature scheme, which is based on Guillou-Quisquater signature and Rabin cryptosystem is proposed. In this new scheme, the signer can produce one signature key by the traditional forward technology, and then generate another key with reverse thinking. The use of the two keys makes attackers can not forge the signer's previous and subsequent periods of valid signatures even if they get the signer's keys of the current period. Analysis result shows that it is correct and secure, moreover, it has the property of strong forward security. It is also less time-consuming than existing shcemes.

【Key words】 digital signature; forward-secure; backward-secure; strong forward-secure; Guillou-Quisquater signature system; Rabin cryptosystem

DOI: 10.3969/j.issn.1000-3428.2013.09.036

1 概述

前向安全的概念由文献[1]首次提出，此后，Bellare M 和 Miner S K 给出前向安全签名的正式定义，并基于文献[2]签名方案分别给出 2 个前向安全签名方案[3-4]。随着研究的深入，一些具有前向安全性的签名方案相继被提出，如前向安全的盲代理重签名方案[5]、前向安全的混合代理多重签名方案[6]、基于多项式秘密共享的前向安全门限签名方案[7]和基于双线性映射的前向安全门限签名方案[8]等，其中有些签名方案确实具备前向安全性，即签名者当前时段的签名私钥泄露后，并不会影响此前签署的消息有效性和合法性。然而，密钥泄露造成的另一个严重的后果是：签名者如果以后再行使签名权利，必须更换自己的公私钥，这样势必给签名者和验证者带来很多不便，甚至提高签名经济成本。

基于上述状况，文献[9]给出强前向安全的思想，同时提出一个基于 ElGamal 算法的强前向安全签名。强前向安全签名是指签名者的某时段的密钥泄露后，不会影响此前和以后时段签名的安全性。但该文献提出的签名需要借助于第三方才能实现，实用性不强。由于算法设计与实现的困难性，强前向安全签名提出后研究进展缓慢。文献[10]也提出了一种强前向安全数字签名方案，它利用单项散列链保证算法后向安全性。文献[11]提出一种具有强前向安全性的代理签名方案，该方案中为保证签名的后向安全，代理签名实施时需要原始签名人的参与，使得代理签名失去了意义。文献[12]提出一个基于身份的前向安全代理签名方案，文献[13]提出一个强前向安全的提名多代理签名方案，这 2 个方案的后向安全性仍然是采用与文献[10]中相同的单项散列链的思想来保障，在算法的实现过程中需要计算很多散列值，计算量较大。

根据上述实际需求，本文设计一个基于 Guillou-Quisquater 签名体制的强前向安全的数字签名方案，并分析该方案的安全性。

基金项目： 国家自然科学基金资助项目(61201431)；山东省优秀中青年科学家科研奖励基金资助项目(BS2010DX026)；青岛市科技发展计划基金资助项目(11-2-4-6-(1)-jch)；山东科技大学“春蕾计划”基金资助项目(2010AZZ183)

作者简介： 徐光宝(1980－)，男，讲师、硕士、CCF 会员，主研方向：信息安全，密码学；姜东焕，副教授、博士；梁向前，副教授

收稿日期： 2012-08-22 **修回日期：** 2012-10-14 **E-mail：** xu_guangbao@163.com

2 具有强前向安全性的数字签名方案

假定 A 为签名者，签名有效时间分为 T 个时段。他在每个签名时段都有2个签名私钥。

2.1 初始化

本文方案的初始化过程如下：

(1) A 随机选取2个大素数 p 和 q，满足 $p\equiv q\equiv 3 \bmod 4$，计算 $n=pq$，随机选取2个整数 v 和 w，使它们分别满足下面条件：

$\gcd(v,(p-1)(q-1))=1$，$\gcd(w,(p-1)(q-1))=1$

(2) A 随机选择2个私钥 $x,z\in {}_RZ_n^*$，计算公开密钥：

$y_1=(x^v)^{-1} \bmod n$，$y_2=(z^w)^{-1} \bmod n$

(3) A 计算：

$z_T=z^2 \bmod n$

$z_{T-1}=z_T^2=z^{2^2} \bmod n,\cdots$

$z_i=z_{i+1}^2=z^{2^{T+1-i}} \bmod n,\cdots$

$z_1=z_2{}^2=z^{2^T} \bmod n$

并将它们分别加密保存。

(4) A 公开 $\{n,y_1,y_2,v,w\}$。

2.2 签名密钥的更新

第 $i(1\leqslant i\leqslant T)$ 签名时段，A 一方面根据等式 $x_i=x_{i-1}^2 \bmod n$（$x_0=x \bmod n$）计算第 i 时段的第一私钥 x_i，同时永久删除 x_{i-1}；另一方面解密出 z_i 作为 i 时段的第二私钥。

2.3 签名的生成

假设 m 为待签名的消息。以第 $i(1\leqslant i\leqslant T)$ 签名时段为例，A 按如下步骤生成签名：

(1)随机选择2个整数 $k,r\in {}_RZ_n^*$，计算：

$Q=k^v r^w \bmod n$

(2)计算杂凑值：$e=H(m\|Q\|i)$，使之满足 $1\leqslant e<v$ 和 $1\leqslant e<w$；否则，返回步骤(1)。

(3)计算 $s_1=kx_i^e \bmod n$，$s_2=rz_i^e \bmod n$。

A 将 (m,s_1,s_2,e,i) 作为签名数据发送给验证者 B。

2.4 签名的验证

验证者 B 收到 A 发送的签名数据后，通过以下步骤来进行验证：

(1)计算 $Q'=s_1{}^v s_2{}^w y_1{}^{2^i e} y_2{}^{2^{T+i-1}e} \bmod n$。

(2)计算出 $e'=H(m\|Q'\|i)$。

(3)验证等式 $e=e'$ 是否成立，成立签名有效，否则签名无效。

3 方案的正确性和安全性分析

3.1 正确性分析

定理1 如果签名者执行2.3节的签名步骤，签名数据能通过2.4节的验证步骤的验证。

证明：因为

$$x_i=x_{i-1}^2 \bmod n=\left(x_{i-2}^2\right)^2 \bmod n=$$
$$x_{i-2}^{2^2} \bmod n=\cdots=x^{2^i} \bmod n$$
$$Q'=s_1{}^v s_2{}^w y_1{}^{2^i e} y_2{}^{2^{T+i-1}e} \bmod n=$$
$$(k x_i^e)^v (r z_i^e)^w y_1{}^{2^i e} y_2{}^{2^{T+i-1}e} \bmod n=$$
$$k^v r^w (x^{2^i})^{ve} (z^{2^{T+i-1}})^{we} y_1{}^{2^i e} y_2{}^{2^{T+i-1}e} \bmod n=$$
$$k^v r^w (x^v)^{2^i e} (z^w)^{2^{T+i-1}e} y_1{}^{2^i e} y_2{}^{2^{T+i-1}e} \bmod n=$$
$$k^v r^w (x^v y_1)^{2^i e} (z^w y_2)^{2^{T+i-1}e} \bmod n=$$
$$k^v r^w \bmod n=Q$$

所以有：

$$e'=H(m\|Q'\|i)=H(m\|Q\|i)=e$$

3.2 安全性分析

3.2.1 方案的安全性

本文的数字签名方案是基于 Guillou-Quisquater 签名体制和 Rabin 密码体制设计的。众所周知 Guillou-Quisquater 签名体制是安全的，Rabin 密码体制也已被证明破解难度等同于分解大整数[14]，而现在大整数分解是一个困难问题。

攻击者如果在仅知道签名者的公开参数和第 i 时段的签名 (m,s_1,s_2,e,i) 的情况下，伪造该时段 A 对其他消息 m' 的签名，他必须根据等式 $s_1=kx_i^e \bmod n$ 和 $s_2=rz_i^e \bmod n$ 求出 x_i 和 z_i，这等同于2次破译 Guillou- Quisquater 签名体制，在计算上是不可行的。当然如果攻击者随机选取2个数 $k',r'\in Z_n^*$，然后再通过计算 $\overline{Q}=(k')^v (r')^w \bmod n$，$\overline{e}=H(m'\|\overline{Q}\|i)$ 试图伪造签名 $(m',s_1',s_2',\overline{e},i)$，他必须通过 $s_1'=k'x_i^{\overline{e}} \bmod n$ 和 $s_2'=r'z_i^{\overline{e}} \bmod n$ 求出 s_1' 和 s_2'，这同样要求他知道 x_i 和 z_i 才能做到。因此，任何试图通过公开参数和当前时段签名伪造签名者当前时段对其他消息签名的做法都是不可行的。

在本文方案签名的验证过程中，需要计算：

$$Q'=s_1{}^v s_2{}^w y_1{}^{2^i e} y_2{}^{2^{T+i-1}e} \bmod n$$

其中，y_1 和 y_2 虽然恒不变，但对它们应用时却应用 $y_1{}^{2^i}$ 和 $y_2{}^{2^{T+i-1}}$，这样能有效避免文献[15]中提出的因实际签名私钥变成和具体时段无关的常数而引起的伪造攻击。

3.2.2 方案的前向安全性

定理2 签名者 A 的第 $i(1<i\leqslant T)$ 时段的密钥泄露，攻击者不能伪造此前时段的签名，因此，此前时段签名是安全的，即方案具有前向安全性。

证明：因为第 $i(1<i\leqslant T)$ 时段签名者 A 的签名私钥由两部分组成，即 (x_i,z_i)。一旦它们被泄露，攻击者如果想计算 A 的第 $i-1$ 时段的签名私钥 x_{i-1} 和 z_{i-1}，只能根据公式 $x_i=x_{i-1}^2 \bmod n$ 和 $z_{i-1}=z_i^2 \bmod n$。显然由 $z_{i-1}=z_i^2 \bmod n$ 求出 z_{i-1} 是很容易的，但由 $x_i=x_{i-1}^2 \bmod n$ 求出 x_{i-1} 等同于破解 Rabin 密码体制，所以，攻击者不能得到第 $i-1$ 时段的完整签名密钥 (x_{i-1},z_{i-1})，也就无法伪造该时段的合法签名。

3.2.3 方案的后向安全性

定理3 签名者 A 的第 $i(1\leqslant i<T)$ 时段的密钥泄露，攻击者不能伪造此后时段的签名，因此签名者在以后时段可以不必更换公钥继续进行签名，即方案具有后向安全性。

证明：因为第 $i(1<i\leqslant T)$ 时段签名者 A 的签名私钥由两部分组成，即 (x_i, z_i)。一旦它们被泄露，攻击者如果想计算 A 的第 $i+1$ 时段的签名私钥 x_{i+1} 和 z_{i+1}，只能根据公式 $x_{i+1}=x_i^2 \bmod n$ 和 $z_i=z_{i+1}^2 \bmod n$。显然，由 $x_{i+1}=x_i^2 \bmod n$ 求出 x_{i+1} 是很容易的，但是由 $z_i=z_{i+1}^2 \bmod n$ 求出 z_{i+1} 等同于破解 Rabin 密码体制，所以攻击者不能得到第 $i+1$ 时段的完整签名密钥 (x_{i+1}, z_{i+1})，当然也就无法得到 $i+1$ 时段以后时段的密钥。这样即使第 i 时段的密钥泄露，也不会影响此后时段的签名的安全性，签名者无需更换新的公钥。因此，本文方案具有后向安全性。

4 方案的运算量分析

鉴于文献[12-13]方案是和文献[10]方案一样通过单项散列链来保证签名是后向安全，是具有特殊功能的签名，一个是代理签名，另一个是提名多代理签名，与本文所提出的普通的数字签名方案不具有可比性，因此，仅将本文方案和文献[10]方案进行运算量比较。

为便于比较，下面仅就第 i 次签名及验证过程对 2 个签名方案的运算量进行比较，结果如表 1 所示。可以看出，在幂运算和模乘运算方面，本文方案处于劣势，但是因为幂运算仅多出 2 次，模乘运算也仅多出 5 次，所以多耗费时间可以忽略；本文方案求散列值运算次数是 2 次，但文献[10]运算次数却需要 T+4 次，其中，T 是方案中签名的阶段数，通常至少大于 10^2。这样每次签名时，文献[10]方案都比本文方案多 T+2 次散列值运算，造成了大量时间的耗费，实现难度远大于本文方案。

表1 2种方案的运算量比较 次

方案	幂运算	模乘运算	求散列值运算
本文方案	8	8	2
文献[10]方案	6	3	T+4

5 结束语

在当前以及今后一个相当长的时期，设计具有前向和后向安全性质的强前向安全签名方案是一个重要的研究任务。为此，本文提出了一个强前向安全的数字签名方案，方案中签名者拥有 2 个私钥，其中一个保证签名的前向安全性，另一个保证签名的后向安全性。分析结果表明，该方案在当前时段密钥泄露后，签名者此前和以后时段的签名仍然是安全的。本文方案可以有效解决困扰签名用户的密钥泄露问题，也为同行设计新的强前向安全签名方案提供了有益借鉴。

参考文献

[1] Anderson R. Two Remarks on Public Key Cryptology[C]// Proceedings of the 4th ACM Conference on Computer and Communication Security. Zurich, Switzerland: ACM Press, 1997: 16-30.

[2] Fiat A, Shamir A. How to Prove Yourself: Practical Solutions to Identification and Signature Problems[C]//Proceedings of Crytology-Crypto'86. Santa Barbara, USA: Springer-Verlag, 1987: 186-194.

[3] Bellare M, Miner S K. A Forward-secure Digital Signature Scheme[C]//Proceedings of CRYPTO'99. Berlin, Germany: Springer-Verlag, 1999: 431-448.

[4] Michel A, Leonid R. A New Forward-secure Digital Signature Scheme[C]//Proceedings of Cryptology-Asiacrypt'00. Kyoto, Japan: Springer-Verlag, 2000: 116-129.

[5] 邓宇乔. 前向安全的盲代理重签名方案[J]. 计算机工程与应用, 2011, 47(16): 97-100.

[6] 万世昌, 程丽红, 张 珍. 前向安全的混合代理多重签名方案[J]. 计算机工程与应用, 2011, 47(12): 80-83.

[7] 芦殿军, 张秉儒, 赵海兴. 基于多项式秘密共享的前向安全门限签名方案[J]. 通信学报, 2009, 30(1): 45-49.

[8] 于 嘉, 孔凡玉, 郝 蓉, 等. 一个基于双线性映射的前向安全门限签名方案的标注[J]. 计算机研究与发展, 2010, 47(4): 605-612.

[9] Burmester M, Chrissikopoulos V, Kotzanikolaou P, et al. Strong Forward Security[C]//Proceedings of the 16th International Conference on Information Security. Paris, France: Kluwer Academics Publishers, 2001: 109-119.

[10] 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.

[11] 杨 洁, 钱海峰, 李志斌. 一种具有强前向安全性的代理签名方案[J]. 计算机工程, 2008, 34(17): 162-163.

[12] 王勇兵, 王小杰. 基于身份前向安全的代理签名方案的安全性分析[J]. 西北师范大学学报, 2012, 48(1): 44-47.

[13] 李志敏, 王勇兵, 张建中. 强前向安全的提名多代理签名方案[J]. 济南大学学报: 自然科学版, 2012, 26(1): 37-40.

[14] 杨 波. 现代密码学[M]. 北京: 清华大学出版社, 2007.

[15] 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): 82-87.

编辑 金胡考