



一种基于椭圆曲线的前向安全数字签名

陈辉焱¹, 袁 勇², 万宗杰¹, 刘 乐², 杨 毅¹

(1. 北京电子科技学院 北京 100070; 2. 西安电子科技大学 西安 710071)

摘 要: 具有前向安全的数字签名是一种重要的数字签名方案, 其要求攻击者即使在 t 时段入侵系统获得签名密钥, 也无法伪造 t 时段之前的签名。换句话说, 前向安全数字签名确保了密钥泄露时段以前所有签名的有效性。基于椭圆曲线离散对数问题和因数分解问题, 构造了一种基于椭圆曲线的前向安全数字签名方案, 并且对方案的安全性和效率进行了系统的分析和证明。

关键词: 前向安全; 椭圆曲线; 离散对数; 签名; 大数分解

doi: 10.11959/j.issn.1000-0801.2015202

A Forward-Secure Digital Signature Based on Elliptic Curve

Chen Huiyan¹, Yuan Yong², Wan Zongjie¹, Liu Le², Yang Yi¹

(1. Beijing Electronic Science and Technology Institute, Beijing 100070, China;

2. Xidian University, Xi'an 710071, China)

Abstract: The forward-secure digital signature is an important digital signature scheme. It requires that even if the attackers have already been given a signature key by invading a system in t time, it still can't forge signatures before time t . In other words, the forward-secure digital signature provides an assurance that any signatures in the previous periods are still valid before the key compromises. Based on the elliptic curve discrete logarithm problem and the factoring problem, a forward-secure digital signature scheme was put forward, and the safety and efficiency of the program was analyzed and proved systematically.

Key words: forward-secure, elliptic curve, discrete logarithm, signature, factoring

1 引言

在一般的数字签名中, 签名密钥一旦泄露, 不但后面签名的安全性无法保证, 先前签名的安全性也无法保证。为了解决这个问题, 几种不同的方式被提出。很多人尝试通过几个系统的密钥分配来降低密钥泄露的可能性。就像

在参考文献[1]中提到的, 这种方法十分昂贵, 以至于对于个体用户来说并不实用。既然每一个系统仍然可能遭受相同的攻击, 因此实际的风险也并没有减少。

另一种降低由于密钥泄露所引起安全性的方法被称为前向安全。主要思想是确保密钥仅在很短的时间段内使用, 当前的密钥泄露并不会影响前面时间段的安全性。设

收稿日期: 2015-05-15; 修回日期: 2015-08-01

基金项目: 中央高校基本科研业务费专项资金资助项目(No.328201521), 北京电子科技学院重点实验室开放基金课题(No.2014kf-chy)

Foundation Items: The Fundamental Research Funds for the Central Universities(No. 328201521), Open Fund of Key Laboratory of Beijing Electronic Science and Technology Institute(No.2014kf-chy)

论文引用格式: 陈辉焱, 袁勇, 万宗杰等. 一种基于椭圆曲线的前向安全数字签名. 电信科学, 2015202

Chen H Y, Yuan Y, Wan Z J, et al. A forward-secure digital signature based on elliptic curve. Telecommunications Science, 2015202

计一个如此系统的挑战在于,在不改变公共信息的前提下改变秘密信息。这种方式在参考文献[2,3]中在密钥交换背景下被看作前向安全。在数字签名中,前向安全与一些简单的方案首先被 Anderson^[4]提出。Bellare 和 Miner^[5]首次给出了前向安全数字签名的正式定义,并基于 Fiat A 和 Shamir A^[6]签名方案给出了两个前向安全数字签名方案。

前向安全数字签名的主要思想是在传统的数字签名方案中添加了“密钥进化算法”。在密钥进化算法中,密钥被拆分为很多时间段,在每一个时间段中有不同的密钥。每一个密钥被用于签名特定时间段的签名信息,并且在每一个时间段结束时产生新的密钥。前一时间段的密钥被抹去。就像一般的签名方案一样,在所有的时间段内只存在唯一的公钥。验证算法不仅要检测签名是否有效,而且还要检测它是否是在特定的时间段内产生的。因此在一个具有前向安全的方案中,自适应选择信息的攻击者即使获得了当前时间段的密钥想要伪造前面时间段的签名是困难的。特别是过去的密钥并不能通过当前的密钥获得。在一个前向安全数字签名方案中,即使当前的密钥泄露了,过去时间段的签名仍然是可信的。

目前,多数前向签名方案的安全性都是建立在大素数因子分解和有限域离散对数问题之上的。随着用户对安全性要求的提高,密钥长度势必增加,造成了基于乘法群上的数字签名方案运行速度大大降低,使得现有的前向签名方案无法再适应拥挤的网络、智能卡和无线终端等资源有限的设备和环境,使得前向签名的实用性大大减弱。随着设备的要求越来越苛刻,椭圆曲线密码体制的优越性进一步体现出来。对于具有同样规模的密码参数,椭圆曲线加密(elliptic curve cryptography, ECC)算法每一字节密钥的强度要比 RSA 和 ElGamal 密码系统大得多。而要达到相同的加密强度, ECC 参数的规模要比上述两者小得多。这使得 ECC 和椭圆曲线数字签名算法(elliptic curve digital signature algorithm, ECDSA)在实现和实际应用中具有更快的速度和更大的安全优势^[7]。

随着近两年计算机网络以及移动通信终端技术的快速发展,椭圆曲线密码体制^[8]越来越受到人们的重视,正逐步成为当前主流的公钥密码体制。参考文献[9]提出了一种基于椭圆曲线的前向数字签名方案,但是该方案并不具备真正的前向安全性。因为攻击者一旦知道了签名人任意时段的签名私钥就可以伪造签名者任意时段的签名。因此本文在研究 A-R 算法^[10]的基础上,根据椭圆曲线的相关知识构

建了一种全新的基于椭圆曲线的前向安全数字签名方案。该方案具有真正的前向安全性,在下文将会进行详细的论述。

2 基本概念

本文用到的符号说明如下。

- F_p : 表示有 p 个元素的有限域,其特征为大素数 p 。
- Z_n^* : 表示有 n 个元素的整数环 Z_n 除了 0 元素以外的其他所有元素。
- $h(m)$: 表示信息 m 用散列函数进行处理后的输出值。

2.1 前向安全签名方案的定义及性质

前向安全签名的定义如下。

定义 1 (前向安全数字签名方案) 前向安全数字签名方案一般包括密钥生成算法、密钥进化算法、签名算法和验证算法。可以形式化地表示为 $FS=(KG, evolving, sign, verify)$ 。下面分别介绍这 4 个算法。

- 密钥生成(key generator, KG)算法: 在该算法中,选择 $k \in N, T$ 表示方案运行的总周期数,把作为秘密参数的 k, T 和其他参数输入系统,输出公钥 PK 和初始私钥 SK_0 。用 $(PK, SK_0) \leftarrow KG(1_k, T)$ 表示。
- 密钥进化(evolver)算法: 在该算法中,用户在本周期 $(j-1)$ 结束时输入当前周期的私钥 SK_{j-1} , 输出下一周期私钥 SK_j , 然后删除上一周期的私钥 SK_{j-1} 。用 $SK_j \leftarrow Evo(SK_{j-1})$ 表示。
- 签名(sign)算法: 在该算法中,输入已知的当前周期 j 、私钥 SK_j 和要签名的签名消息 M ; 输出该周期对消息 M 的签名 (j, ξ) 。用 $(j, \xi) \leftarrow Sgn_{SK_j}(M)$ 表示。
- 验证(verify)算法: 在该算法中,输入已知的当前周期 j 、公钥 PK 、签名消息 M 、待验证签名 (j, ξ) ; 输出值为 0 表示拒绝该签名, 输出值为 1 表示接受该签名。用 $b \leftarrow V_{f_{PK}}(M, (j, \xi))$ 表示。

在上面 4 个算法中,密钥产生算法和签名算法为概率性算法;而密钥进化算法和验证算法为确定性算法。约定如果总周期数为 T , 则 SK_{T+1} 为空字符串。

定义 2 (不可伪造性) 不可伪造性(unforgeability)是指在不知道前向安全签名私钥的条件下,任何攻击者都不可能成功伪造任何一个有效的前向安全签名。

定义 3 (前向安全性) 前向安全性(forward-secure)是指在前向签名方案中,即使入侵者获得了在 t 时刻的密钥,也无法还原 t 时刻之前的密钥,从而无法伪造 t 时刻之前的签名。



2.2 基于的困难问题

定义 4 (椭圆曲线离散对数问题) 给定一个椭圆曲线 E , P 为椭圆曲线上的一点, 且阶为大素数 n 。选取一随机数 $k \in Z_n^*$, 可以很容易计算出 $Q=kP$ 。但是如果知道 P 和 Q , 求解 k 却是十分困难的。

定义 5 (大数分解问题) p 和 q 为两个大素数, $N=p \cdot q$ 。知道 p 和 q 求解 N 是容易的, 但是如果知道 N 要求出 p 和 q 却变得十分困难。

3 基于椭圆曲线的前向安全签名设计

(1) 密钥生成算法

- 选取一条在域 F_p 上的安全椭圆曲线 E , 取属于 E 上的一点 P , 其阶为大素数 n 。
- 设方案的总周期为 T 。随机选取两个不同的大素数 p_1 和 p_2 , 计算 $N=p_1 p_2$ 且 $N > n$ 。
- 取整数 $d_0 \in Z_n^*$, 输出私钥 $SK_0=d_0$ 。
- 计算 $Q=SK_0^{-2^{T-1}} P$, 输出公钥 $PK=(P, E, n, Q)$ 。

(2) 密钥进化算法

当系统进入 j 时段时, $1 \leq j \leq T$, 签名者使用拥有 $j-1$ 时段的密钥 SK_{j-1} 计算 $SK_j=SK_{j-1}^2 \pmod N$, 删除系统中 $j-1$ 时段的密钥 SK_{j-1} , 并保密新生成的 j 时段的密钥 SK_j 。

(3) 签名算法

- 取整数 k , 使 $k \in Z_n^*$ 。
- 计算 $k^{2^{T-1-j}} P=(x, y)$, $r=x \bmod n$ 。若 $r=0$, 则转到步骤①。
- 计算消息的散列值 $e=h(m||r||j)$, $s=SK_j e k \bmod n$ 。若 $s=0$, 则转到步骤①。

- 发送签名 (j, ξ) 和信息 m 给验证者, 其中 $\xi=(r, s)$ 。

(4) 验证算法

- 取得公钥 $PK=(P, E, n, Q)$, 签名 (j, ξ) 和信息 m , 验证 $r, s \in Z_n^*$ 。
- 计算 $e=h(m||r||j)$ 。
- 计算 $(se^{-1})^{2^{T-1-j}} Q=(x_1, y_1)$ 。
- 计算 $v=x_1 \bmod n$ 。
- 计算 $v=r$, 若成立, 签名有效; 否则签名无效。

4 安全性分析

4.1 正确性

由密钥进化算法中的密钥进化公式 $SK_j=SK_{j-1}^2 \pmod N$, 能够得到 $Q=SK_0^{-2^{T-1}} P=SK_j^{-2^{T-1-j}} P$, 如式(1):

$$\begin{aligned} (se^{-1})^{2^{T-1-j}} Q &= (SK_j k)^{2^{T-1-j}} Q \\ &= SK_j^{2^{T-1-j}} k^{2^{T-1-j}} SK_j^{-2^{T-1-j}} P \\ &= k^{2^{T-1-j}} P \\ &= (x, y) \end{aligned} \quad (1)$$

所以本方案显然是正确的。

4.2 前向安全性

(1) 密钥进化算法的前向安全性

本方案中的签名私钥 SK_j 在签名过程中根据时段 $j(1 \leq j \leq T)$ 不同而不断进行更新, 而签名公钥 PK 在这个签名过程中始终保持不变。因为采用的密钥进化算法 $SK_j=SK_{j-1}^2 \pmod N$ 是有名的数学难题, 因此如果攻击者想通过私钥 SK_j 求出 j 时段之前的私钥, 就必须求解模大数 N 的 2 次同余方程, 而要求解此二同余方程就必须对大数 N 进行分解, 这就面临大数分解的难题, 所以私钥 SK_j 具有前向安全性。

(2) 签名算法的前向安全性

假如攻击者已经获得了第 j 时段的私钥, 它如果想要第 j 时段的私钥来伪造第 $j-1$ 时段的签名, 如式(2):

$$\begin{aligned} (se^{-1})^{2^{T-2j}} Q &= (SK_j k)^{2^{T-2j}} Q \\ &= SK_j^{2^{T-2j}} k^{2^{T-2j}} SK_j^{-2^{T-1-j}} P \\ &= SK_j^{2^{T-1-j}} k^{2^{T-2j}} P \\ &\neq k^{2^{T-2j}} P \end{aligned} \quad (2)$$

通过上面的分析, 本方案解决了攻击者一旦知道了签名人任意时段的签名私钥, 在不知道前面时刻私钥的情况下就可以伪造签名者任意时段签名的问题。

因此, 通过以上两部分的系统分析可以得出: 当攻击者知道第 j 时段的签名以及私钥时, 攻击者无法伪造 j 时段之前的签名。所以本签名方案具有真正意义上的前向安全性。

4.3 抗伪造性

PK 作为签名算法的公钥, 如果攻击者想通过公钥 PK 中的参数 Q 来获取私钥 SK_j , 那么他将面临椭圆曲线的离散对数问题。因此攻击者是无法通过公钥来获取签名者的私钥 SK_j 。签名 s 作为签名在 j 时段的签名重要组成部分, 由 $s=SK_j e k \bmod n$ 可知, 如果攻击者想通过 s 得到实际签名私钥 SK_j 就必须知道 k 的值。而如果要求解 k 就要面临椭圆曲线离散对数的求解问题, 因此攻击者无法通过 s 获得签名私钥 SK_j 。由前面的验证算法可知, 如果攻击者在不知道私钥 SK_j 和 k 的情况下, 想用一伪造的私钥 SK_j' 进行签名, 则验证无法通过, 具体证明过程如下。

假设攻击者伪造 j 时段的私钥 SK_j' , 随机选取随机数

$k' \in Z_n^*$ 计算 $s' = SK_j' ek' \bmod n$, $k'^{2^{r+1-j}} P = (x', y')$ 和 $r' = x' \bmod n$, 进而伪造 j 时段的签名记为 (j, ξ') , 其中 $\xi' = (r', s')$, 但是在验证过程中, 由于:

$$\begin{aligned} (s'e^{-1})^{2^{r+1-j}} Q &= SK_j'^{2^{r+1-j}} k'^{2^{r+1-j}} Q \\ &= SK_j'^{2^{r+1-j}} k'^{2^{r+1-j}} SK_j'^{-2^{r+1-j}} P \\ &\neq k'^{2^{r+1-j}} P \\ &= (x', y') \end{aligned} \quad (3)$$

因此, 验证无法通过, 本方案具有较强的抗伪造性。

5 方案性能

通过对基于椭圆曲线的前向安全数字签名方案的4个算法的描述能够发现: 在密钥进化算法中采用的是二次剩余运算; 在签名算法中只进行了一次点乘运算和零次模逆运算; 在验证算法中只进行了一次点乘运算和一次模逆运算。在基于椭圆曲线的数字签名算法中最耗费时间的就是点乘运算和模逆运算, 因此, 本方案的签名与验证速度是非常快速的, 计算效率也是相当可观的。

6 结束语

椭圆曲线密码已成为当前的主流密码算法, 在人们的日常生活中发挥着越来越大的作用。本文基于椭圆曲线的离散对数问题构造了一种基于椭圆曲线的高效前向安全数字签名方案, 并有力地保证了新签名方案的正确性和安全性, 在电子商务或电子政务等领域中, 具有广泛的应用前景。

参考文献

- 1 Bellare M, Rogaway P. The exact security of digital signatures: how to sign with RSA and Rabin. *Proceedings of Cryptology-Eurocrypt 1996 Lecture Notes in Computer Science (LNCS)*, Cambridge, UK, 1996: 399~416
- 2 Guillou L, Quisquater J. A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory. *Proceedings of Cryptology-Eurocrypt 1988 Lecture Notes in Computer Science (LNCS)*, Davos, Switzerland, 1988
- 3 Micali S. A secure and Efficient Digital Signature Algorithm. Technical Report, MIT/LCS/TM-501, 1994
- 4 Anderson R. Two remarks on public-key cryptography. *Proceedings of the 4th Annual Computer and Communications Security (ACM)*, Zurich, Switzerland, 1997
- 5 Bellare M, Miner S K. A forward-secure digital signature scheme. *Proceedings of the 19th Annual International Cryptology Conference*, Santa Barbara, CAL, USA, 1999: 431~448
- 6 Fiat A, Shamir A. How to prove yourself: practical solutions to

identification and signature problems. *Proceedings of Cryptology-Crypto'86*, Santa Barbara, CAL, USA, 1986: 186~194

- 7 隋爱芬, 杨义先, 钮心忻等. 基于椭圆曲线密码的可认证密钥协商协议的研究. *北京邮电大学学报*, 2004, 27(3): 28~32
- Sui A F, Yang Y X, Niu X X, *et al.* Research on the authenticated key agreement protocol based on elliptic curve cryptography. *Journal of Beijing University of Posts and Telecommunications*, 2004, 27(3): 28~32
- 8 蔡满春, 杨义先, 胡正明. 基于椭圆曲线密码机制的一种电子现金方案. *北京邮电大学学报*, 2004, 27(2): 44~47
- Cai M C, Yang Y X, Hu Z M. Electronic cash scheme based on elliptic curve cryptosystem. *Journal of Beijing University of Posts and Telecommunications*, 2004, 27(2): 44~47
- 9 王尚平, 候红霞, 李敏. 基于椭圆曲线的前向安全数字签名方案. *计算机工程与应用*, 2006(18): 150~151
- Wang S P, Hou H X, Li M. A forward-secure digital signature scheme based on elliptic curves. *Computer Engineering and Applications*, 2006(18): 150~151
- 10 Michel A, Leonid R. A new forward-secure digital signature scheme. *Proceedings of Advances in Cryptology - Asiacrypt 2000*, Kyoto, Japan, 2000: 116~129

[作者简介]



陈辉焱, 男, 博士, 北京电子科技学院硕士生导师, 西安电子科技大学与北京电子科技学院密码学联合培养硕士生导师, 主要研究方向为格密码、椭圆曲线及其密码方案。



袁勇, 男, 西安电子科技大学硕士生, 主要研究方向为信息安全、椭圆曲线及其密码方案。

万宗杰, 男, 北京电子科技学院讲师, 主要研究方向为网络安全、椭圆曲线及其密码方案。

刘乐, 男, 西安电子科技大学硕士生, 主要研究方向为信息安全、椭圆曲线及其密码方案。

杨毅, 男, 北京电子科技学院硕士生, 主要研究方向为信息安全、椭圆曲线及其密码方案。