第32卷 第14期 计 算 机 工 程 2006年7月
Vol.32 № 14 Computer Engineering July 2006
·安全技术· 文章编号：1000—3428(2006)14—0109—02 文献标识码：A 中图分类号：TP309

基于ECC的前向安全数字签名的研究与改进

符茂胜[1]，任 哲[2]，侯整风[3]
(1. 皖西学院计算机科学与技术系，六安 237012；2. 皖西学院数理系，六安 237012；3. 合肥工业大学计算机学院，合肥 230009)

摘 要：基于 ECC 的前向安全数字签名方案，签名中使用了不变量 $SK_i^{n^{T-i}}$，尽管签名私钥是前向安全性的，但实际上签名不具有前向安全性。该文提出了关联因子的概念，利用关联因子构造了一种新的基于 ECC 的前向安全数字签名方案，该方案不仅具有前向安全性，还具有较强的抗伪造性，有一定的理论和实用价值。

关键词：椭圆曲线；前向安全；数字签名；密钥进化

Study and Improvement of Forward-secure Digital Signature Based on ECC

FU Maosheng[1], REN Zhe[2], HOU Zhengfeng[3]
(1. Department of Computer Science & Technology, West Anhui University, Liuan 237012; 2. Department of Mathematic & Physics, West Anhui University, Liuan 237012; 3. Faculty of Computer, Hefei University of Technology, Hefei 230009)

【Abstract】 The paper points out that scheme in reference is not forward-secure because it uses constant $SK_i^{n^{T-i}}$ to sign a message. Although the secret key is forward-secure, the signature isn't forward-secure. This paper presents a new concept of connected-factor, and by which a new forward-secure signature based on ECC is designed, it is not only forward-secure, but also resistant to forging attack, it is suitable in theory and for some practice.

【Key words】 Elliptic curve cryptosystem (ECC); Forward-secure; Digital signature; Private key evolution

1 概述

在传统的数字签名系统中，其系统的安全性都是建立在密钥不被泄漏的基础上，一旦密钥暴露，攻击者可以伪造从过去到现在任意时间的签名，这个缺点严重影响数字签名的不可否认性。

为此，Rose Anderson[2]在1997年ACM CCS会议首次提出了前向安全数字签名的概念，即当前私钥的暴露不会影响到过去的大量数字签名的安全性。Bellare和 Miner在文献[3]中给出了前向安全签名一个正式而详细的定义：公钥的有效使用时间被划为T个时间段，记为1，2，…，T，见图1。

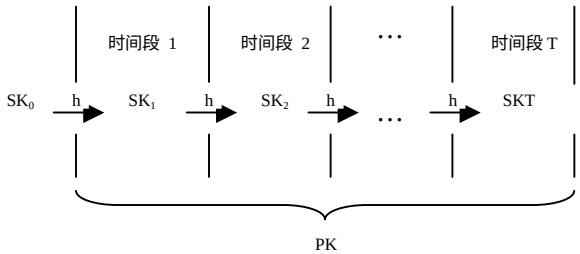

图1 前向安全数字签名特征

每个时间段i对应一个私钥 SK_i，在时间段i期间使用SK_i进行签名，当时间段i结束进入时间段i+1 时，由私钥进化函数(通常是一个单向函数h)计算出私钥 SK_{i+1} 后就可以删除 SK_i，然后用 SK_{i+1} 进行签名，直到下个时间段开始，在公钥的使用期内虽然私钥每隔一段时间就要变化一次，但对应的公钥PK保持不变。

此后，大量的前向安全数字签名算法[4~8]被提出来。这方面的研究基本上可以分两类：(1)是基于黑盒子方式的任意签名方案；(2)是基于Fait-Shamir方案或其变体的前向安全数字签名方案。

文献[1]提出了一种基于椭圆曲线密码体制(ECC)的前向安全数字签名方案。该方案的密钥更新具有前向安全性，但由于签名(r,s)中使用了不变量 $SK_i^{n^{T-i}}$，即在 i 时段的签名与该时间段的私钥 SK_i 没有建立关联，实际上签名不具有前向安全性。

本文分析了原方案的缺陷及其受到的攻击，提出了关联因子的概念，利用关联因子构造了一种新的基于 ECC 的前向安全数字签名方案，新方案建立了 i 时间段签名(i,(r,s))与该时段密钥 SK_i 的关联性，从而保证了签名的前向安全性。

2 原方案描述及其攻击

文献[1]的方案分为4部分：初始参数，私钥更新算法，签名和验证。具体如下：

选择一个安全的椭圆曲线，基点为P，其阶为n，n为满足nP=O的素数，选择一个单向安全的Hash函数h(x)。

2.1 签名者初始密钥对的生成

(1)将签名密钥的有效期分为T个时间段，选择一个大素数p和随机数 SK_0,$1<SK_0<p$；

(2)计算 $P_K=SK_0^{n^T}P$；

(3)系统公钥为 $\{p,T,P_K\}$，公开，初始密钥 SK_0 应保密。

基金项目：安徽省教育厅自然科学基金资助项目(2006KJ046B)；皖西学院青年基金资助项目(WXZQ0505)
作者简介：符茂胜(1972—)，男，硕士、讲师，主研方向：计算机网络与信息安全；任 哲、侯整风，教授
收稿日期：2006-03-06 **E-mail：**fums@wxc.edu.cn

2.2 私钥进化

当系统进入 i 时间段时，$1\le t\le T$，签名者使用拥有的 i-1 时间段的密钥 SK_{i-1}，计算 $SK_i=SK_{i-1}^n \bmod p$，删除系统中 i-1 时间段的密钥 SK_{i-1}，保密新生成的 i 时段的密钥 SK_i。

2.3 签名过程

(1)签名者任意选择随机数 k，0<k<n，计算 kP=(x，y)，r=xmodn，若 r=0，则返回(1)；

(2)计算 e=h(m)，$s=(ke+rSK_i^{n^{T-i}})P$；(3)以(r,s)作为消息 m 的签名发给验证方。

2.4 验证过程

(1)验证者计算 e=h(m)；

(2)计算 $X=e^{-1}(s-rP_K)=(x_1,y_1)$；

(3)如果X=0，则拒绝签名；否则计算 $r_1=x_1 \bmod n$，若 $r_1=r$，则接受这个签名。

前向安全数字签名要求当前密钥的暴露不会影响过去签名的安全性。也就是说，即使当前的私钥被盗，过去的签名还是很难伪造的，攻击者无法用现在的私钥伪造过去的签名。但是原方案在签名时使用了 $SK_i^{n^{T-i}}$ 进行签名运算，而

$$SK_i^{n^{T-i}}=(SK_{i-1}^n)^{n^{T-i}}=SK_{i-1}^{n^{T-i+1}}=\cdots=SK_0^{n^{T-i+i}}=SK_0^{n^T}$$

即 $SK_i^{n^{T-i}}$ 实际上是个与时间段 i 和私钥 SK_i 无关的不变量，这导致签名结果不具有前向安全性。假设攻击者获得第 i 时间段的私钥 SK_i，他就可以伪造过去任一时间段的签名。因为得到 SK_i 之后，就可以计算出 $SK_i^{n^{T-i}}=SK_0^{n^T}$，假设伪造过去时间段 j(j<i)的签名为 (r',s')。k' 为攻击者选择的一随机数，0< k' <n， k' P=(x，y)， r' =xmodn。

计算 e=h(m)， $s'=(k'e+r'SK_0^{n^T})P$。

验证：计算

e=h(m)，$X=e^{-1}(s'-r'P_K)=e^{-1}((k'e+r'SK_0^{n^T})P-r'P_K)=k'P=(x_1,y_1)$，显然 $r_1=r$，验证者接受伪造签名。

由上可见此方案实际上不具有前向安全性，其问题就在于每次用不变的 $SK_i^{n^{T-i}}=SK_0^{n^T} \bmod p$ 进行签名，没有将 i 时间段的签名(r,s)和该时间段的私钥 SK_i 建立关联，因而签名不具有前向安全性。

3 改进方案描述

为了避免原方案的缺陷，必须将 i 时间段的签名和该时间段的私钥 SK_i 之间建立关联，为此引入一个新的变量 R_i 用来建立关联。具体改进方案如下：

选择一个安全的椭圆曲线，基点为 P，其阶为 n，n 为满足 nP=O 的素数，选择一个单向安全的 Hash 函数 h(x)。

签名者初始密钥对的生成、私钥的进化的相关内容在 2.1 节、2.3 节中均有叙述。计算 $R_i=SK_iP$ 并公开，引入 R_i 是为了将时间段 i 的签名和该时间段的私钥 SK_i 建立关联，并称 R_i 为 i 时间段的关联因子。

3.1 签名过程

(1)签名者计算 e=h(m)，然后选择一个随机数 k，计算 $r=k-eSK_i \bmod n$；

(2)计算 $s=(k+rSK_i^{n^{T-i}})P$；

(3)以(i,(r,s))作为消息 m 的签名发给验证方。

3.2 验证过程

(1)验证者计算 e=h(m)， $X_1=rP+eR_i=(x_1,y_1)$；(2)计算 $X_2=(s-rP_K)=(x_2,y_2)$；(3)如果 X_1=0或X_2=0，则拒绝签名；否则比较 $x_2=x_1 \bmod n$，若相等则接受签名，否则拒绝签名。

3.3 新方案性能分析

(1)有效性。因为： $SK_i^{n^{T-i}}=SK_0^{n^T}$，所以 $X_2=(s-rP_K)=((k+rSK_i^{n^{T-i}})P-rP_k)=kP$，而 $X_1=rP+eR_i=kP$，故方案是正确的。

(2)关联因子 R_i 的关联性。由 $R_i=SK_iP$ 可知， R_i 是和i时间段私钥 SK_i 紧密相关的；由于 R_i 在i时间段公开，攻击者若通过伪造私钥 SK_j' (j<i)而伪造签名(j,(r',s'))，则验证无法通过。事实上，验证者是利用j时间段公开的关联因子 R_j 来验证签名的，即计算 e=h(m)， $X_1=r'P+eR_j=r'P+eSK_jP=(r'+eSK_j)P\ne(r'+eSK_j')P$，所以验证失败。

(3)前向安全性。由 SK_i 的计算公式 $SK_i=SK_{i-1}^n \bmod p$ 知，私钥 SK_i 的进化具有前向安全性。

假设 i 时间段的私钥 SK_i 泄露，攻击者伪造 j(j<i)时间段的签名为 $(j,(r',s'))$，其中 $r'=k'-eSK_j' \bmod n$ (SK_j' 是攻击者伪造的 j 时间段的密钥)， $s'=(k'+r'SK_j^{n^{T-j}})P$，验证时， $X_1=r'P+eSK_j'P\ne r'P+eR_i=k'P$，而 $X_2=(s'-r'P_K)=k'P$，验证过程无法通过。

因此，本方案私钥 SK_i 的进化和 i 时段的签名(i,(r,s))都具有前向安全性。

(4)抗伪造性。关联因子 R_i 是公开的，由 $R_i=SK_iP$ 可知，从 R_i 中求出私钥 SK_i 是椭圆曲线离散对数困难问题(ECDLP)；签名结果为 $(i,(r,s))$，由 r，s 的公式可知，如果无法知道私钥 SK_i，则显然也无法构造 i 时段的正确签名 $(i,(r,s))$；由验证公式可知，在不知道私钥 SK_i 的情况下，要想用一个假的私钥 SK_i' 进行签名运算，伪造有效的签名 $(i,(r',s'))$，也是椭圆曲线离散对数困难问题(ECDLP)，验证不能通过。

4 结束语

在前向安全数字签名中，密钥的进化既要保证密钥进化的单向性，另一方面又要受控于公钥便于验证，一般的单向函数(如 Hash 函数)是无法满足要求的。目前使用最多的是基于模 n 平方根的难题作为单向函数。利用椭圆曲线离散对数困难问题(ECDLP)，本文提出了关联因子的概念，用以辅助私钥进化，解决了上述难题，本文构造的新方案是前向安全数字签名在 ECC 上的一个有益尝试，具有一定的理论意义和实用价值。

参考文献

1 詹雄泉, 洪景新. 基于椭圆曲线密码体制的一种具有前向安全的数字签名方案[J]. 厦门大学学报, 2005, 44(2): 189-192.

2 Anderson R. Two Remarks on Public Key Cryptology[C]. Proc. of the 4th Annual Conference on Computer and Communications Security, ACM, 1997.

（下转第 113 页）