第35卷 第14期 计 算 机 工 程 2009年7月
Vol.35 No.14 Computer Engineering July 2009
·安全技术· 文章编号：1000—3428(2009)14—0171—02 文献标识码：A 中图分类号：TP309.2

WLAN中基于ECDSA的三元鉴别方法

王国锋，龙昭华，蒋贵全
(重庆邮电大学计算机科学与技术学院，重庆 400065)

摘 要：以椭圆曲线密码学为基础，通过分析无线局域网的工程环境，选取合适的椭圆曲线参数，构造一种基于椭圆曲线数字签名、三元鉴别的双重签名方案。该方案可以强化对无线局域网中所有实体的鉴别，通信的任何一方都需要得到其他两方的身份验证，从而增强了无线网络环境下对访问控制的安全控制，可以抵制中间人攻击，支持无线网络中的宽带传输。

关键词：椭圆曲线数字签名算法；无线局域网；中间人攻击；三元鉴别

Tri-element Authentication Method Based on ECDSA in WLAN

WANG Guo-feng, LONG Zhao-hua, JIANG Gui-quan
(Dept. of Computer Science and Technology, Chongqing University of Posts & Telecommunications, Chongqing 400065)

【Abstract】 Based on ECC, by analyzing the engineering environment in WLAN and choosing appropriate ECC parameters, this paper describes a dual-signature scheme with tri-element authentication method. The scheme strengthens authentication for all the entities in WLAN. Any party's identity should be checked by others when associating, so that it can enhance the security of access control in wireless network, restrict man-in-the-middle attack, and support the bandwidth transport in wireless network.

【Key words】 Elliptic Curve Digital Signature Algorithm(ECDSA); WLAN; man-in-the-middle attack; tri-element authentication

1 概述

椭圆曲线离散对数问题(ECDLP)本身是一个纯粹的数学问题，椭圆曲线密码学(ECC)则是依据求解椭圆曲线离散对数问题而产生的，椭圆曲线在密码学中的使用是由 Neal Koblitz 和 Victor Miller 在 1985 年分别提出的。通过 20 多年的发展，ECC 已经在全球范围内引发了广泛的研究热潮，ECC 的主要优势是：(1)在某些情况下它能提供比其他公开密钥密码系统(如 RSA)更高等级的安全。(2)群之间的双线性映射，该理论基于 Weil 对或 Tate 对，双线性映射已广泛应用于密码学中，如基于身份的加密。不过其缺点是加密和解密操作的实现比其他机制花费的时间长，这对时间要求比较高的网络通信来说存在一些问题。

ECC 数学理论研究的一个分支是 ECC 的安全性[1]和计算速率[2]，而 ECC 在无线环境中的安全性和工作效率就是基于数学难题、密码机制以及工程应用。本文除了分析 ECDLP 的求解难度问题[3]，还通过结合无线局域网(WLAN)的应用环境，描述了一种三元实体鉴别的思想[4]。三元实体鉴别是在单向鉴别的基础上发展起来的，它基于无线网络的开放环境，鉴于网络实体在空中接口下的不确定性，为防范中间人攻击而形成一种“人人参与身份鉴别”的思想。本文通过融合 ECDLP、密码工作机制和 WLAN 的工程场景研究分析 ECC 在无线网络中的安全性和实现问题。

2 椭圆曲线加密技术

2.1 椭圆曲线的描述

从代数几何中得知，椭圆曲线是亏格为 1 的代数曲线，难以用初等函数表达，根据密码学的研究需要，引入了平面上的椭圆曲线函数，即 Weierstrass 方程式。为便于在网络环境下使用，本文关心的是一种受限形式的椭圆曲线。

本文定义了在二维平面有限域 F_p 上的椭圆曲线 $E(F_p)$：$E(F_p)=\{(x,y)\mid x,y\in F_p\}\cup O$，其中，$O$ 为无穷远点。$n=\#E(F_p)$ 是椭圆曲线 $E(F_p)$上的阶，p 是 n 的一个大素数因子，随机选取 E 上的某个生成元作为基点 G。$E(F_p)$, n, p, G 作为参数将影响 ECDSA 的工作性能。受限域上椭圆曲线 $E(F_p)$的方程式定义为 $y^2\equiv x^3+ax+b(\mathrm{mod}\ p)$。

2.2 椭圆曲线参数的选择

为应付各种可能的针对 ECC 的攻击，根据 2.1 节中的方程式，选择一条理想的椭圆曲线至关重要，寻找通过随机数算法生成的具有大素数阶的椭圆曲线是之后的工作。

考虑到 WLAN 的需要，所选择的椭圆曲线需要满足 2 个要求：安全性和快速性。因此，为加快椭圆曲线的实现速度，取 p 为广义 Mersenne 素数[5]，此类素数具有快速的模规约算法，满足 WLAN 对于时限的要求。

构造椭圆曲线参数的算法采用随机曲线算法，该算法产生曲线参数的过程如下：

(1)选择方程式参数 a,b。随机数生成算法在域 F_p 内生成 2 个随机数 a 和 b。

(2)选择椭圆曲线 $E(F_p)$阶 n。采用 SEA 算法计算 n，n 为某一大素数的幂运算的值，因此需要对 n 进行大 Mersenne 素数测试，如果测试没有通过，转向步骤(1)。

(3)计算出 Mersenne 素数 p 后，检测 a,b 需要是否满足不等式：$4a^3+27b^2\neq 0(\mathrm{mod}\ p)$，若满足，则确定椭圆曲线 $E(F_p)$，否则转向步骤(1)。

(4)选择基点 $G(x_G, y_G)$ 在 0~p 的范围内选择一随机数 x_G，

基金项目：国家质检总局公益性行业科研专项基金资助项目(10-226)；重庆市科技攻关计划基金资助项目(2007AC2053)

作者简介：王国锋(1984－)，男，硕士研究生，主研方向：无线网络，网络安全；龙昭华，教授、硕士；蒋贵全，副教授

收稿日期：2008-12-11 **E-mail：**wangguo84821@126.com

通过降幂求解算法计算得到 $y_{G'}$，选取随机数 u，计算 $y_G=(-1)^u y_G'(\mathrm{mod}\ p)$，若点$(x_G, y_G)$满足椭圆曲线方程，则确定该生成元为 G 点；否则，重新选取随机数 x_G；若长时间无法确定生成元 G，则转向步骤(1)。

所有参数选择完后即产生一条理想的安全椭圆曲线，由于这种参数的选择是一个复杂的过程而且生成时间相对比较长，因此在 WLAN 环境下，需要有一个安全椭圆曲线集，当工作环境改变时，选择备用的椭圆曲线。

3 三元实体鉴别方法的引入

WLAN 在接入访问控制方面涉及 3 个实体单元：用户工作站(STA)，无线网络接入点(AP)和鉴别服务器(AS)。基于 WLAN 工程环境对安全控制的严格要求，AP 作为无线信号的处理中心，为了防范伪装的 AP 破坏无线通信环境，需要加强对 AP 真伪的身份鉴别。因此，除了单向鉴别 STA 的身份外，AP 的身份也必须得到验证，而 AS 作为权威的鉴别中心受到 AP 与 STA 的信任，如何保障这种信任和权威性也需要进行研究。

3 类实体的工作环境为 STA 以无线的方式集中于 AP 通信，而 AP 与 AS 通过有线或无线的方式连接。

为保障 STA 不受到伪 AP 的干扰、非法的用户 STA 无法进入合法 AP 环境中以及 AS 能作为可信的第三方，本文描述了一种以三元对等鉴别为基础的鉴别机制，通过该机制，真正地实现对通信三方的身份鉴别。

AS 是证书管理中心，STA 与 AP 通过椭圆曲线密钥生成算法生成密钥对(*PubKey*,*SecKey*)，并将各自的 *PubKey* 通过安全通道送给 AS 保存，AS 通过这些实体的信息构造证书，颁发给 STA 和 AP，以标识 STA 与 AP 的身份。AS 颁发的证书都采用 ECDSA 进行了数字签名，在 STA 进入 AP 的覆盖范围内时就会进行关联操作，STA 与 AP 采用所选定的椭圆曲线 $E(F_p)$，以 AS 为中心互相进行身份的鉴别，任何一方验证失败都将不能工作，这就是三元鉴别的思想。三元鉴别不同于目前广泛采取的二元鉴别模式，有效阻止了中间人攻击。

4 三元实体鉴别方法的实现与技术分析

4.1 椭圆曲线数字签名算法的实现

根据第 2 节中椭圆曲线的定义和参数选择所得到的椭圆曲线方程式，本文给出一种椭圆曲线数字签名算法(Elliptic Curve Digital Signature Algorithm, ECDSA)的实现与验证过程。设待签名的消息为 P，公钥与私钥的关系为

$$PubKey=SecKey^{-1}\times G$$

三元实体相互鉴别中都使用了以下数字签名过程，这里假设是 AP 对来自 STA 签名的消息进行验证。

(1)签名过程

STA 对消息 P 的签名过程为：1)使用 SHA-256 散列函数计算 P 的哈希值得到 256 位的 $H(P)$。2)随机选取一个大整数 $k\in(0,\infty)$，计算 $Q=k\times G$。3)STA 对 P 的签名方程为 $S_{\mathrm{STA}}(P)=(H(P)\times k-Q)\times Sec_{\mathrm{STA}}$。4)STA 将组成的分组字段 $P\|Q\|S_{\mathrm{STA}}(P)$ 发送给 AP。

(2)验证过程

AP 收到来自 STA 的分组消息 $P\|Q\|S_{\mathrm{STA}}(P)$ 后，通过其之前获得的 STA 公钥验证发送该分组的身份，验证方法如下：1)使用 SHA-256 散列函数计算 P 的哈希值，得到 256 位的 $H(P)$。2)验证签名方程式为 $H(P)\times Q=Q\times G+S_{\mathrm{STA}}(P)\times Pub_{\mathrm{STA}}$。3)在验证方程式中代入 $H(P), S_{\mathrm{STA}}(P)$ 和 Pub_{STA}，若等式双方成立，则验证通过；否则，签名无效，丢弃分组。

4.2 三元鉴别分析

三元实体鉴别结构如图 1 所示。

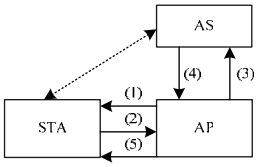

图 1 三元实体鉴别结构

WLAN 的三元实体鉴别由 AP 广播的关联帧发起，STA 响应关联，工作的过程如下：

(1)AP-> STA：$R1\|CertAP\|T$；

(2)STA->AP：$R1\|R2\|CertSTA\|Q1\|S_{\mathrm{STA}}(R1\|R2\|CertSTA)\|T$；

(3)AP-> AS：$R2\|R3\|CertSTA\|CertAP\|T$；

(4)AS->AP：$PubSTA\|PubAP\|Q2\|Q3\|S_{\mathrm{AS}}(R3\|ResSTA)\|S_{\mathrm{AS}}(R2\|ResAP)\|T$；

(5)AP->STA：$PubAP\|ResAP\|Q4\|S_{\mathrm{AP}}(R1\|R2\|CertSTA)\|S_{\mathrm{AS}}(R2\|ResAP)\|T$。

以上过程中的每一步为前者发往后者分组中的用于身份鉴别的消息字段。$R1$, $R3$ 为 AP 产生的随机数，$R2$ 为 STA 产生的随机数；T 为时间戳，标识鉴别分组的存活时间；*CertSTA*, *CertAP* 分别为 STA 和 AP 的证书；*PubSTA*, *PubAP* 分别为 STA 和 AP 的公开密钥；*ResSTA*, *ResAP* 分别为 AS 对 STA 和 AP 证书鉴别的结果；$Q1$, $Q2$, $Q3$, $Q4$ 分别为类似于 4.1 节中 ECDSA 签名过程中产生的一个生成元；$S_{\mathrm{AS}}()$表示 AS 对括号中内容进行的数字签名结果。

CertSTA, *CertAP*, $S_{\mathrm{AS}}()$, $S_{\mathrm{AP}}()$采用了之前选定的椭圆曲线的 ECDSA；而在 3 个实体之间传送的信息使用了 ECEH 进行加解密。

对基于 ECDSA 的三元鉴别过程的分析如下：

(1)AS 对 STA, AP 的验证

在步骤(3)、步骤(4)中，当 AS 收到来自 AP 的分组后，因为数字证书是 AS 颁发的，所以 AS 将采取 4.1 节中的验证过程对分组中的数字证书 *CertSTA* 和 *CertAP* 进行身份验证，并将验证结果签名后与 STA 和 AP 等信息组成分组传给 AP。

(2)AP 对 AS, STA 的验证

通过步骤(4)，AP 获得了 STA 的公开密钥 *PubSTA*，同时对步骤(2)中的 $S_{\mathrm{STA}}(R1\|R2\|CertSTA)$进行验证，通过验证随机数 $R1$ 的值判断步骤(2)的分组是否确实来自于步骤(1)中所关联的 STA，由此来定位 STA，防止鉴别过程中的伪 STA 攻击。下一步 AP 将对步骤(4)中的 $S_{\mathrm{AS}}(R3\|ResSTA)$进行验证，通过判断随机数 $R3$ 验证 AS 的签名。与此同时，AP 将获得 AS 发送过来的对 STA 的鉴别结果信息 *ResSTA*，其根据 *ResSTA* 验证了 STA 身份的真伪。倘若对 STA 的验证失败，AP 将丢弃分组，解除与该 STA 的关联。

(3)STA 对 AS, AP 的验证

通过步骤(5)，STA 获得了 AP 的公开密钥 *PubAP*，并对其中的签名字段 $S_{\mathrm{AP}}(R1\|R2\|CertSTA)$进行验证，通过随机数 $R1$, $R2$ 确定 STA 接收到的分组是否来自于步骤(1)中的 AP，完成 AP 的定位。下一步通过 AS 的公钥验证字段 $S_{\mathrm{AS}}(R2\|ResAP)$和 *ResAP* 的内容，根据 *ResAP*，STA 验证了 AP 身份的真伪。倘若对 AP 的验证失败，STA 将丢弃分组，解除与该 AP 的关联；若验证通过，三元鉴别过程结束，在 WLAN 环境中创建了一个安全的通道。 (下转第 208 页)