基于 RSA、ECC 以及组合公钥 ECC 数字签名体制的比较研究①

The Comparison Research of Digital Signature System

蒋泰　潘晓君　（桂林电子科技大学计算机与控制学院　桂林 541004）

摘　要：本文详细介绍了 RSA、ECC、及改进的组合公钥 ECC 签名体制的原理，并通过试验对这些算法的数字签名进行了分析和比较，得出了改进的组合公钥 ECC 算法具有系统参数小、处理速度快、密钥尺寸小等优点，它必将成为未来公钥签名体制的一个研究方向。

关键词：RSA　数字签名　椭圆曲线　组合公钥

1　引言

随着先今网络技术的飞速发展，网上信息传输等活动也日益频繁，如何保证及加强网络数据的安全性已经成为迫切需要解决的热点问题。数字签名是维护网络信息安全核心技术之一，在身份认证、数据完整性、抗抵赖性以及匿名性等方面有重要的应用已成为实现身份识别和信息安全认证的关键技术。曲线的数字签名系统是目前主流的数字签名系统之一，并且被认为是 RSA 公钥系统的最佳替代者。常用的数字签名体制：RSA，ECC。其中基于 RSA 的数字签名算法应用的非常广泛，而基于 ECC 的数字签名算法 ECDSA 则是现今签名算法的热点热点，本文在 ECDSA 签名体制的基础之上，提出了一种结合组合公钥的 ECC 签名算法，通过试验详细的分析和比较，得出了改进的结合组合公钥的 ECC 签名体制相对于 RSA、ECDSA 在性能上都有教大的改善，该签名体制具有较强的研究价值及应用前景。

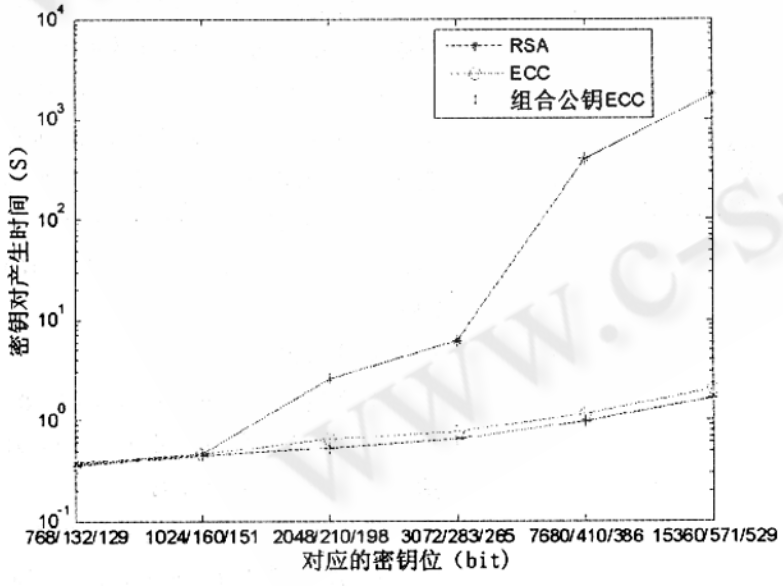

图 1　密钥对产生时间比较图

2　基于 RSA 的数字签名流程

2.1　RSA 密钥对生成步骤

① 选择 2 个足够大的素数 p、q。

② 计算 p 与 q 的乘积为 n = pxq。并由欧拉函数性质，计 φ(n) = (p −1) * (q −1)。

① 项目支持：国家电子信息产业发展基金项目

③ 取一个与 n 互素的奇数 e，满足 $1<e<\varphi(n)$，$\gcd(e,\varphi(n))=1$，那么(e,n) 就是公钥。

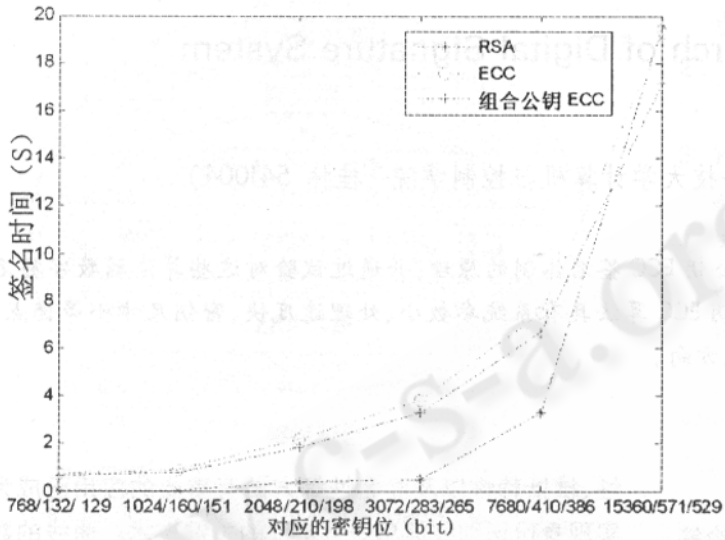

图 2　签名时间比较图

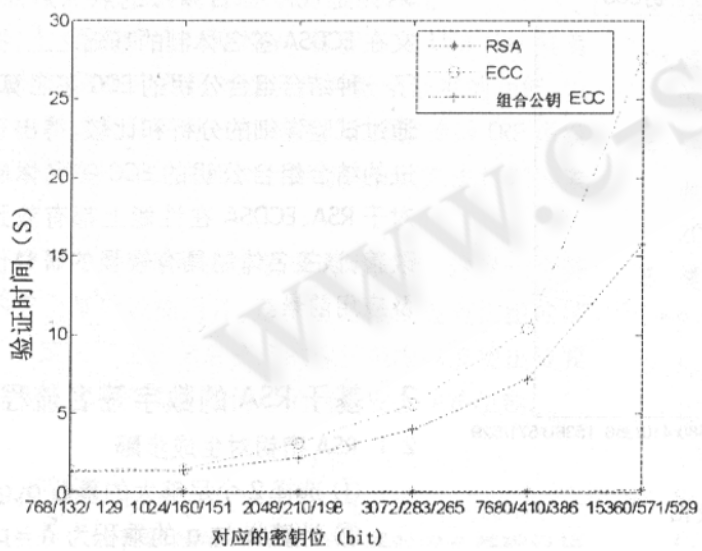

图 3　验证时间比较图

④ 通过 e，计算 d，要求满足 $e\times d=1 \bmod \varphi(n)$，那么(d,n)就是要求的私钥。

2.2 RSA 数字签名算法的签名步骤

我们假定待签名的消息明文为 P：

① 利用消息摘要算法(如 MD5 或 SHA－1)计算消息的散列值 h1＝H(P)。

② 用得到的私钥(d,n)加密散列值 $s=h1^d \bmod n$。s 就是签名的结果。

③ 为确保签名过程中的尽可能安全，可将消息和签名(M,s)加密后发送。

2.3 RSA 数字签名算法的验证步骤

① 取得发送方的公钥(e,n)。

② 解密签名 s，$h=s^e \bmod n$。

③ 通过相同的摘要算法计算消息的散列值 H(P)。

④ 比较，如果 h＝h1，表示签名有效；否则签名无效。

3 结合组合公钥椭圆曲线(ECC)签名体制

3.1 密钥生成步骤

在椭圆曲线参数确定的情况下，选择椭圆曲线上的 G1，G2 作为基点(这两个点的阶都是 n)，各自生成他们对应的密钥种子矩阵。用户 A 通过向密钥管理中心(KMC)提出申请，得到整数 l1 与 l2 ($1<l1,l2<n-1$) 作为自己的私钥，并且可以得到 A 的公钥 PA ＝l1G1＋l2G2。

3.2 签名步骤

① A 随机选择一个整数 p($1<p<n-1$)，利用基点 G1 和 G2 计算 R(xR，yR)＝p×G1＋p×G2；

② 对需要签名的消息 O 通过一个散列函数计算其散列值，h ＝ Hash(O)；

③ 计算 $x\equiv xR \pmod n$，其中 xR 为 R 的横坐标；

④ A 得到其签名：v1 ＝ pH ＋ xk1 (mod n)，v2 ＝ pH ＋ xk2 (mod n)；

⑤ A 用全局公钥 KU 对 x，v1，v2 进行加密，并将

EKU (x , v1 , v2) 加密的结果和 M 一并发给验证者 B 。

3.3 签名验证步骤

① B 用全局公钥 KU 对收到的 EKU (x,v1,v2) 进行解密,DKU(EKU(x,v1,v2)) = x , v1 , v2 ;

② B 采用与 A 相同的散列算法, 计算 h = Hash (O) ;

③ 计算 Q(xQ , yQ) = h-1(s1 ×G1 + s2 × G2 -x ×PA) ;

④ v ≡ xQ (mod n) , xQ 是点 Q 的 x 轴坐标值;

⑤ 若 v = x ,则验证成功,否则拒绝。

4 三种签名体制安全性及有效性分析

4.1 分析比较的编译环境

本文运行平台为 Windows XP、Pentium (R) 4 2.67G、512M 内存。采用的是 java 编程语言,并在 Matlab 的环境下仿真这三种签名体制。

4.2 三种算法相同安全性的密钥长度对应表

表 1　同等安全性下三种公钥签名体制对应的密钥位(单位:bit)

RSA、ECC、及组合公钥 ECC 算法的安全性比较						
RSA	768	1024	2048	3072	7680	15360
ECC	132	160	210	283	410	571
组合公钥 ECC	129	151	198	265	386	529

4.3 数字签名时间对照表

表 2　数字签名时间对照表(单位:秒)

RSA/ ECC/ 组合公钥 ECC	768/132/ 129	1024/160/ 151	2048/210/ 198	3072/283/ 265	7680/410/ 386	15360/571/ 529
密钥对产生	0.375	0.468	2.563	6.140	407.652	1746.322
	0.369	0.466	0.642	0.765	1.165	2.062
	0.358	0.453	0.529	0.653	0.977	1.651
签名	0.024	0.028	0.352	0.475	3.320	19.537
	0.740	0.920	2.183	3.824	7.542	19.262
	0.66	0.790	1.854	3.289	6.673	17.183
验证	0.028	0.030	0.034	0.038	0.056	0.122
	1.317	1.426	3.108	5.562	10.409	27.593
	1.304	1.347	2.179	3.954	7.106	15.741
总体签名效率比较	0.427	0.526	2.949	6.653	411.028	1765.981
	2.426	2.812	5.933	10.151	19.116	48.917
	2.322	2.590	4.562	7.896	14.756	34.575
破解时间 (MIPS YEARS)	10^8	10^{12}	10^{20}	10^{31}	10^{52}	10^{67}

4.4 试验结果比较图(以下各 MATLAB 仿真图横坐标均表示同等安全性下的密钥位数)

4.4.1 密钥对产生时间比较

图 1 的纵坐标采用了对数值形式。随着密钥对位数的不断增加,组合公钥 ECC 算法产生密钥对的速度略高于 ECC,但明显快于 RSA 算法。

4.4.2 签名时间比较

从图 2 可以看出,RSA 的签名速度优于 ECC 和组合公钥 ECC(在 15360/571/529 位以前),但是当密钥位进一步加大时,ECC 和组合公钥 ECC 签名速度快于 RSA,且组合公钥 ECC 签名速度更快。

4.4.3 验证时间比较

图 3 显示的验证时间比较图。如图所示:RSA 的验证速度非常快,当密钥位逐步加大时,验证速度似乎没有受到多大的影响。相反,ECC、组合公钥 ECC 的验证速度和 RSA 相比,有着非常大的差距,ECC 验证时间曲线增长的比较快,但组合公钥 ECC 没有 ECC 增长的那么快,特别是当密钥位达到比较大的数值时,组合公钥 ECC 算法的优势似乎越明显,验证速度也快了不少。

4.4.4 整个签名性能比较

图 4 显示的是整个数字签名体系的全部耗时比较,从试验仿真的图中可以看出, ECC、组合公钥 ECC 和 RSA 算法大概在 283 位时他们的总体消耗的时间差不多,但在 283 位以前 RSA 优于其他两中算法,在 283 位以后 ECC、组合公钥 ECC 优于 RSA,且随着密钥位的逐步加大,组合公钥 ECC 整体签名效率相对 ECC 也越明显。

4.4.5 安全抗攻击性比较

图 5 显示了三种签名算法抗攻击性的时间比较。从图中可以看出,要达到同等安全性,RSA 所要求增加的密钥位非常大,而 ECC、组合公钥 ECC 的密钥位增幅相对 RSA 来说就非常小,组合公钥 ECC 的密钥位增加的更少,正是此原因使得他们带宽占用、处理速度都优于 RSA。

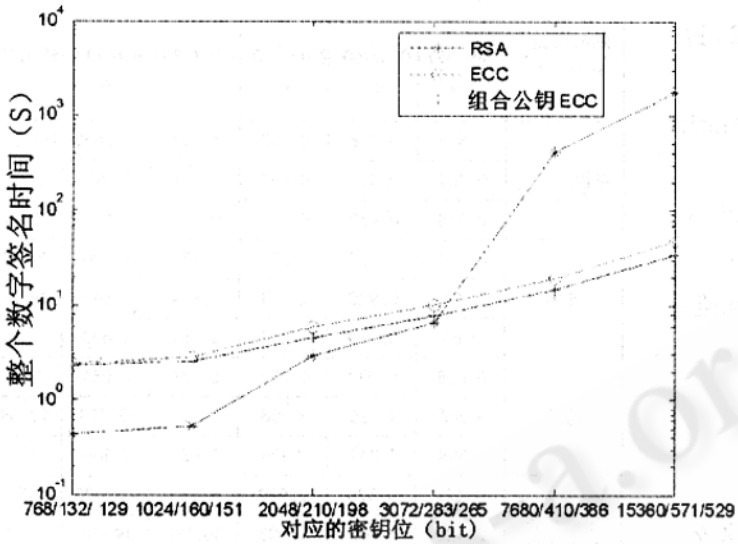

图 4　整个签名性能比较图

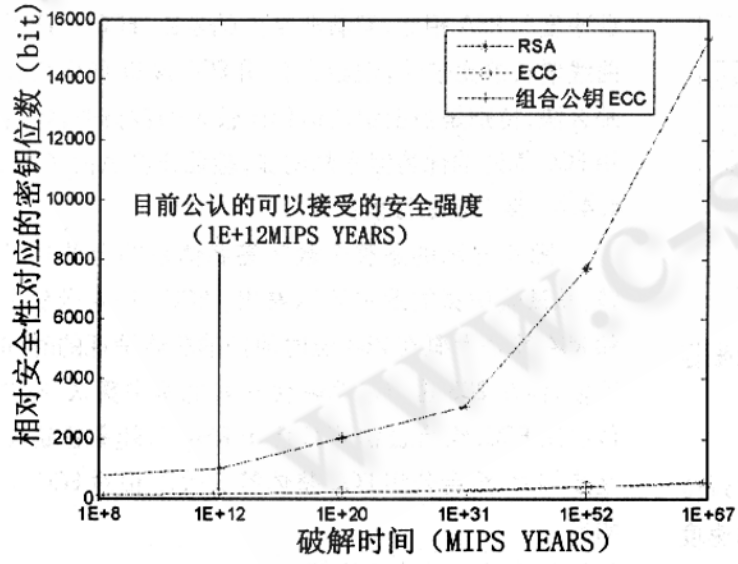

图 5　安全抗攻击性比较图

5　结束语

本文在椭圆曲线 ECDSA 签名体制分析的基础上，将其与组合公钥技术相互结合提出了一种改进的组合公钥 ECC 签名体制。通过试验分析比较，得出了该签名体制在带宽占用、密钥长度、处理速度、单位密钥位安全性等方面要优于通常使用的 RSA、ECC 等签名体制，具有很好的研究价值，是未来签名体制发展的一个方向。

参考文献

1　ANSI X9. 63. Elliptic Curve Digital Signature Algorithm (ECDSA). American Bankers Association, 1999.

2　M. Hasan, A. Wassal, VLSI Algorithms, Architectures, and Implementation of a Versatile GF(2m) Processor, IEEE Transactions on Computers, vol. 49 , no. 10 , Oct. 2000, pp. 1064 – 1073.

3　Lu Jian – zhu, Chen Huo – yan. New message recovery signature schemes and its security[J]. Mini – Micro Systems,2003,24(4):695 – 697.

4　杨君辉、戴宗铎、杨栋毅等一，种椭圆曲线签名方案与基于身份的签名协议[J]，软件学报，2000，11(10)：1303 – 1306.

5　赵小明、章美仁，RSA 数字签名技术在电子公文流传中的应用[J]，计算机工程与设计，2005，(5)：1214.

6　蔡庆华，公钥密码体制 RSA 算法[J]，安庆师范学院学报，2003 第 4 期.