椭圆曲线加密系统的性能分析*

张险峰** 秦志光 刘锦德

(电子科技大学微机所 成都 610054)

【摘要】对比其他公钥系统，分析了椭圆曲线加密系统(ECC)的安全性和有效性；说明了ECC与其他公钥加密系统相比，能提供更好的加密强度、更快的执行速度和更小的密钥长度，因此可用较小的开销和时延实现较高的安全性，能满足在带宽、计算能力或存储能力等受限的应用场合。

关 键 词 公钥体制； 椭圆曲线加密系统； 密码； 安全性

中图分类号 TP309

在密码学应用中有三类系统一般被认为是安全且有效的，即：整数的因式分解系统、离散对数系统、椭圆曲线离散对数系统，它们分别基于整数因式分解问题、离散对数问题和椭圆曲线离散对数问题(ECDLP)[1,2]。这些数学问题经过数学家和计算机科学家多年的深入研究还没能得出其有效算法。近年来椭圆曲线上的密码系统(ECC)越来越受到重视，其安全性就是基于椭圆曲线离散对数的难解性。

1 安全性分析

虽然椭圆曲线点运算的概念很容易理解，但产生合适的符合安全性条件的椭圆曲线和有效执行点乘运算的方法却是极端复杂。合适的椭圆曲线参数一旦产生即可形成一椭圆曲线群，并可为许多用户所公用，这些用户可基于此群生成其公/私密钥对。ECC安全性即是从公钥 kG 和基点 G 中很难计算出私钥 k 这一特性。

由Hasse定理： $p+1-2\sqrt{p}\leqslant \#E(F_p)\leqslant p+1+2\sqrt{p}$ ($\#E(F_p)$ 表示椭圆曲线群上点的总数)，可求出椭圆曲线上点的总数的范围[3]。虽然可由Schoof算法计算出 $\#E(F_p)$ 的精确值，但其过程非常复杂。椭圆曲线群上点的有限性和点数目的难确定性对加密而言是好的属性，因为这些曲线只是包含了一些离散的点，攻击者不知如何把这些点相连成曲线，也就不知如何应用几何关系。

椭圆曲线上的离散对数问题在 $\#E(F_p)$ 有大的素因子时是一个难题，只有指数复杂度解法比整数因式分解和模 p(p 为素数)的离散对数问题更难。然而对于超奇异椭圆曲线和不规则椭圆曲线，其ECDLP相对容易，易遭到特定算法的攻击。此时ECDLP可退化为有限域低次扩域上的离散对数问题，从而能在多项式时间内求解[4,5]。由于这些情况很容易被鉴别，从而可避免相应的攻击。

基于模运算的整数因式分解问题和离散对数问题都存在亚指数时间复杂度的通用算法。亚指数时间算法没有指数时间算法难。目前采用最快的算法来计算这两类问题所需要的时间复杂度为：$O\ (\exp\{1+O(1)\sqrt{\ln p\ln(\ln p)}\})$ (p 为模的大小)。而解ECDLP最有效的算法只有指数时间算法，其时间复杂度为：$O(\sqrt{p})$[2]。因此，ECDLP较另两类问题更为难解，表明ECC能以更小的密钥长度产生与其他公钥体制相同等级的安全性。

ECC、RSA和DSA的安全性分析如表1所示。在表中，MIPS-年指以每秒执行100万条指令的计算机运行一年。如果1万台运算速度达到1 000 MIPS的计算机并行处理，其模长为 $n\approx 2^{160}$，解ECDLP要96 000年。当前，一般认为破译时间为 10^{12} MIPS-年代表安全。为此，RSA和DSA要求

2000年10月13日收稿

* 国防科技预研基金资助项目，基金号：99J6.3.2.DZ02

** 男 28岁 博士生

模长为1 024 bit，而160 bit 对于 ECC 就已经足够；且当密钥长增加时，ECC 的安全性比 RSA/DSA 增加快得多。如240 bit 密钥长的 ECC 比2 048 bit 模长的 RSA/DSA 安全，虽然此时 RSA/DSA 从1 024 bit 增加到2 048 bit，而 ECC 只是从160 bit 增加到240 bit[6]。

表1　ECC、RSA 和 DSA 的安全性分析比较

破译所需时间/MIPS-年	RSA/DSA 密钥长度	ECC 密钥长度	RSA/ECC 密钥长度之长
10^4	512	106	5:1
10^8	768	132	6:1
10^{12}	1 024	160	7:1
10^{20}	2 048	210	10:1
10^{78}	21 000	600	35:1

2　有效性分析

一个公钥加密系统的有效性需考虑三个因素：计算开销、密钥长度和带宽。对不同系统的有效性进行比较时应基于相同的安全级。为了使比较尽量具体，本文选择密钥长为160 bit 的 ECC 和 1 024 bit 的 RSA 和 DSA。这些密钥长为各自系统提供了彼此相当的安全级[7]。

2.1　计算开销

计算开销决定了变换公钥和私钥所需的计算量。对于 DSA 和基于 ECC 的椭圆曲线数字签名算法(ECDSA)或椭圆曲线加密方案(ECES)，大部分数字签名和加密变换操作能进行预计算。RSA 一般选择 e=65 537=(2^{16}+1)，这样 e 的二进制表达式中只含两个“1”，可大大减少计算量。假设一次椭圆曲线加法大约需花10次模乘的开销，一次1 024 bit 模乘运算要求一个单元时间，所有应用于离散对数加密系统的预计算技巧同等地应用在基于椭圆曲线的系统中[3]。

各系统的计算开销如表2所示，q 为160 bit 长，表中数据表示完成给定操作所需的时间单元数。这些数据没有考虑到各自系统可能采取的一些优化措施，只是提供了大致的比较。

表2　各系统的计算开销分析比较表

	基于 GF(q)的 ECDSA 或 ECES	RSA(n=1 024 bit，e=2^{16}+1)	离散对数系统/1 024 bit
加密	120	17	480
解密	60	384	240
签名	60	384	240
验签	120	17	480

与 ECC 相比，其他公钥体制由于产生密钥所需的计算非常复杂，在计算能力受限的情况下很难产生合适的密钥。而 ECC 可在很短的时间里产生符合条件的密钥，因此，即使一个计算能力非常有限的灵巧卡也能产生满足要求的密钥对。

虽然基于域 F_p 和 F_2m 的 ECC 在安全性和标准化上没有区别，但在实际的应用上其性能和成本还是有区别的。另外，由于 ECC 的基域及其元素表示法能被选择，从而域运算(域加、域乘、域求逆)能被优化。对于基于离散对数和整数因式分解的公钥密码系统就不能做到这一点。

2.2　密钥长度

密钥长度决定存储密钥对和系统参数需要的比特数。ECC、RSA/DSA 的系统参数和密钥对长度比较如表3所示。

表3 ECC、RSA/DSA 的系统参数和密钥对长度比较

	系统参数/ bit	公钥/ bit	私钥/ bit
RSA	——	1 088	2 048
DSA	2 208	1 024	160
ECC	481	161	160

由此可见，ECC 所用的系统参数和密钥对比 RSA/DSA 要求的短。

2.3 带 宽

带宽是指传送一加密消息或一签名所需传输的比特数。当三类公钥系统用于加密或对长消息进行数字签名时，具有相似的带宽要求。但当传送短消息时带宽的要求就值得注意，因为公钥密码系统经常用于传送短消息，如为对称密码系统传送会话密钥。为了进行具体的比较，假设待签消息为2 000 bit 长，待加密消息为100 bit 长，几种情况下签名和加密消息的长度分析如表4所示。

表4 几种体制下的签名长度和加密消息的长度

	签名长度/bit	加密消息长度/bit
RSA	1 024	1 024
DSA	320	——
ElGamal	——	2 048
ECC	320	321

因此当转换短消息时，ECC 能比其他公钥系统提供更大的带宽节省。而且 ECC 的点压缩技术进一步节省了存储密钥、证书的空间和带宽。

通过以上分析可见，ECC 与其他公钥加密系统相比，能提供更好的加密强度、更快的执行速度和更小的密钥长度，因此 ECC 可用较小的开销(所需的计算量、存储量、带宽、软件和硬件实现的规模等)和时延(加密和签字速度高)实现较高的安全性。特别适用于计算能力和集成电路空间受限(如 IC 卡)、带宽受限(如无线通信和某些计算机网络)、要求高速实现的情况。

3 结 束 语

从加密观点看，开发 ECC 的主要动机是它们与已建立的系统相比基于不同的数论问题，具有合理的安全期望，没有很大的附加开销，在某些特定场合，ECC 能够提供其他系统不能提供的安全性。以前提出了许多新的公钥密码系统作为已建立系统的补充，其中多被攻破，其他的执行代价又太高，而 ECC 值得进行进一步分析。

在普通数群 Z_p 中的离散对数问题比 ECDLP 问题容易解决，得益于数域筛方法的提出和不断完善。而在过去20年里解 ECDLP 的技巧没有明显进步，这对于椭圆曲线方法较有利。

总之，ECC 和已建立的其他公钥系统相比所取得的研究成果相对少，这可能是因为该系统本身难以攻破，或者可能只是该系统没有被很好地理解，无论哪种情况，都值得作进一步研究。

参 考 文 献

1 Menezes A J. Elliptic curve public key cryptosystems. USA: Kluwer Academic Publishers,1993

2 Ceiticom Corporation Whitepaper. Canada: Ceiticom Corporation ,1997

3 Xiang Qian, Liu Zhao. Simplest accomplishment of arithmetric on Galios fields. Journal of University of Electronic Science and Technology of China, 2000, 29(1): 5~9[**向 茜, 刘 钊. 伽罗华域上代数运算的最简实现. 电子科技大学学报**, 2000, 29(1): 5~9]

4 **王育民, 刘建伟. 通信网的安全——理论与技术. 西安: 西安电子科技大学**, 1999

5 Man Young Rhce. Cryptography and secure communications. USA: McGraw-Hill Co,1994

6 Wayne Patterson. Mathematical cryptology for computer scientists and mathematicians. USA: Rowman & Dittlefield, 1987

7 Xiong Jintao, Liu Hongxiu, Pi Dezhong. Lucas public-key cryptosystem and its security. Journal of University of Electronic Science and Technology of China, 1999, 28(4): 397~401 [**熊金涛, 刘红秀, 皮德忠. 公钥密码体制及其安全性. 电子科技大学学报**, 1999, 28(4): 397～401]

Analysis of Security and Efficiency on Elliptic Curves Cryptosystems

Zhang Xianfeng　　Qin Zhiguang　　Liu Jinde

(College of Computer Science and Engineering, UEST of China　Chengdu　610054)

Abstract　The security and efficiency of ECC are analyzed comparing with other public-key cryptosystems. It is shown that ECC can provide greater strength, higher speed and smaller keys than other systems. Thus ECC can get relatively high security with less cost and time delay, and can meet security requirements in some applications with limited bandwidth, computational power or storage space.

Key words　public-key cryptosystems；elliptic curves cryptosystems；cryptography；security