基于椭圆曲线加密算法技术优势的探讨

夏先智[1] 赵 毅[2]

(重庆市信用合作社计算机中心 重庆400023)[1] (重庆交通学院计算机信息中心 重庆400074)[2]

The Research on Technical Advantages of ECC

XIA Xian-Zhi[1] ZHAO Yi[2]

(Computer Center of Chongqing Credit Union, Chongqing 400023)[1]

(Computer Information Center, Chongqing Jiaotong University, Chongqing 400074)[2]

Abstract ECC is a safer and more practical public key system than the other cryptography algorithm since public key cryptogram debited. Advantages of ECC on technology are exploited in this paper, which ensures itself a popular cryptography algorithm for public key system.

Keywords ECC, Encryption

1 引言

信息安全技术是一门综合性学科，其主要任务是研究计算机系统和通信网络内信息的保护方法以实现系统内信息的安全、保密、真实和完整。其中，信息安全的核心是密码技术。随着计算机网络不断渗透到各个领域，密码学的应用也随之扩大。

根据密钥类型不同将现代密码技术分为两类：一类是对称加密(秘密钥匙加密)系统，另一类是公开密钥加密(非对称加密)系统。

2 现代密码技术

2.1 对称加密系统

对称密码体制是一种传统密码体制，代表性的有：DES、AES、IDEA、RC5等，其安全性是基于密码体制设计者的水平、偏爱以及复杂的数学运算。

对称钥匙加密系统是加密和解密均采用同一把秘密钥匙，而且通信双方都必须获得这把钥匙，并保持钥匙的秘密[1]。因为加解密密钥相同，需要通信的双方必须选择和保存其共同的密钥，各方必须信任对方不会将密钥泄密出去。对于具有n个用户的网络，需要n(n-1)/2个密钥，在用户群不是很大的情况下，对称加密系统是有效的[2]。但是对于大型网络，当用户群很大、分布很广时，密钥的分配和保存就成了问题。另外，对称加密系统仅能用于对数据进行加解密处理，提供数据的机密性，不能用于数字签名，因而人们迫切需要寻找新的密码体制。

2.2 公开密钥加密系统

1976年 Whitfield Diffie 和 Martin Hellman 提出了公钥密码体制的概念。公钥加密系统中，加密和解密是相对独立的，加密过程使用公钥E，而解密使用一个不同的(但数学上相关的)私钥D。知道公钥可以对明文进行加密，但不能对密文进行解密。如果接收者选择并公布了他的公钥，其它任何人都可以用这一公钥来加密传送给接收者的消息。私钥是秘密保存的，只有私钥的所有者才能利用私钥对密文进行解密。由于公钥加密系统不存在对称加密系统中密钥的分配和保存问题，对于具有n个用户的网络，仅需要2n个密钥。除加密功能外，公钥系统还可以提供数字签名。

3 椭圆曲线密码算法出现的必要性

自公钥密码问世以来，学者们提出了许多种公钥加密方法，它们的安全性都是基于复杂的数学难题[3]。根据所基于的数学难题来分类，有以下三类系统目前被认为是安全和有效的：1)大整数因子分解系统(代表性的有RSA)；2)有限域(数学中的一种代数结构)离散对数系统(代表性的有DSA)；3)有限域椭园曲线离散对数系统(ECC)。当前最著名、应用最广泛的公钥系统是RSA系统，RSA系统是公钥系统的最具有典型意义的方法，大多数使用公钥密码进行加密和数字签名的产品和标准使用的都是RSA算法。RSA方法的优点主要在于原理简单，易于使用。但是，随着分解大整数方法的进步及完善、计算机速度的提高以及计算机网络的发展，作为RSA加解密安全保障的大整数要求越来越大。为了保证RSA使用的安全性，其密钥的位数一直在增加，比如，目前一般认为RSA需要1024位以上的字长才有安全保障。但是，密钥长度的增加导致了其加解密的速度大为降低，硬件实现也变得越来越难以忍受，这对使用RSA的应用带来了很重的负担，对进行大量安全交易的电子商务更是如此，从而使得其应用范围越来越受到制约[3,4]。DSA(Data Signature Algorithm)是基于有限域离散对数问题的数字签名标准，它仅提供数字签名，不提供数据加密功能[4]。安全性更高、算法实现性能更好的公钥系统椭圆曲线加密算法ECC(Elliptic Curve Cryptography)基于有限域上椭圆曲线的离散对数计算困难性，是Koblitz和Miller两人1985年提出的。定义在有限域(Fp或F(2m))的椭圆曲线($y^2=x^3+ax+b$)上的点(x,y)，再加上无穷点O，如按一定的规则运算将组成一个群。有限域上椭圆曲线乘法群也有相对应的离散对数计算困难性问题。因此，许多公开密码系统都是基于此问题发展出来的，如类似ELGamal，DSA等密码系统的ECES，ECDSA[5]。

下面探讨一下椭圆曲线和椭圆曲线上的密码算法。

夏先智 工程师。

有限域上的椭圆曲线：

在ECC中，我们关心的是某种特殊形式的椭圆曲线，即定义在有限域上的椭圆曲线。其方程如下：

$$Y^2=X^3+aX+b(\mathrm{mod}\ p) \quad (1)$$

其中p是素数，a和b为两个小于p的非负整数，它们满足：$4a^3+27b^2(\mathrm{mod}\ p)\neq 0$。

满足方程(1)的椭圆曲线如图1所示。

我们用Ep(a,b)表示模p椭圆群，其元素是满足上面方程的小于p的非负整数对(x,y)以及无穷远点O。在E上定义“+”运算，P+Q=R，R是过P、Q点的直线与曲线的另一点关于X轴的对称点(如图1)，当P=Q时R是P点的切线与曲线的另一交点的对称点(如图2)。

可以证明，椭圆曲线上的点关于“+”运算构成Abel群。

椭圆曲线离散对数问题(ECDLP)定义如下：给定素数p和椭圆曲线E，对Q=kP，在已知P，Q的情况下求出小于p的正整数k。

可以证明由k和P计算Q比较容易，而由Q和P计算k则比较困难。ECDLP是比整数因子分解问题(IFP)和离散对数问题(DLP)难得多的数学难题。

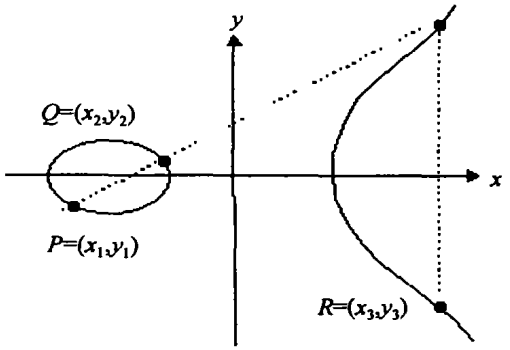

图1 椭圆曲线上的加法 P+Q=R

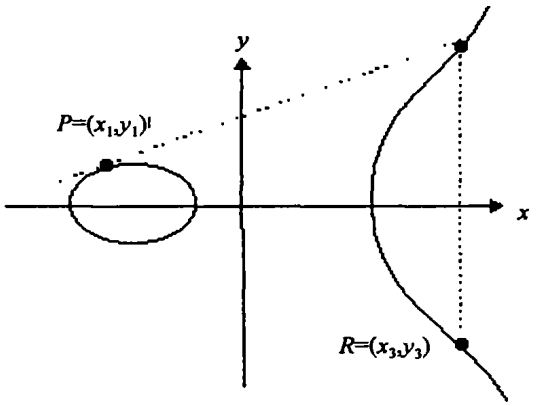

图2 椭圆曲线上的加法 P+P=2P=R

将椭圆曲线中的加法运算与离散对数中的模乘运算相对应，将椭圆曲线中的乘法运算与离散对数中的模幂运算相对应，我们就可以建立基于椭圆曲线的对应的密码体制。例如，对应D-H公钥系统，我们可以通过如下方式在椭圆曲线上予以实现：

在E上选取生成元P，要求由P产生的群元素足够多，通信双方A和B分别选取a和b，a和b予以保密，但将aP和bP公开，A和B间通信用的密钥为abP，这是第三者无法得知的。

对应ElGamal密码系统可以采用如下的方式在椭圆曲线上予以实现。

将明文m嵌入到E点上，选一点B∈E，每一用户都选一整数a，0<a<N，N为阶数已知，a保密，aB公开。欲向A送m，可送去下面一对数偶：$(kB, P_m+k(a_AB))$，k是随机产生的整数。A可以从kB求得$k(a_AB)$。通过：$P_m+k(a_AB)-k(a_AB)=P_m$，恢复P_m。

同样，对应DSA我们可以在椭圆曲线上构造ECDSA。

4 椭圆曲线加密算法(ECC)技术的优势

椭圆曲线密码体制自被引入以来逐步成为一个令人感兴趣的密码学分支。这种密码体制的诱人之处在于安全性相当的前提下，可使用较短的密钥，而且它是建立在一个不同于大整数分解及素域乘法群而广泛为人们所接受的离散数学问题的数学难题之上。同时，椭圆曲线资源丰富，同一个有限域上存在着大量不同的椭圆曲线，这为安全性增加了额外的保证，也为软、硬件实施带来了方便。

椭圆曲线加密方法与其它加密方法相比，有以下的优点：

1)安全性能更高。加密算法的安全性能一般通过该算法的抗攻击强度来反映。ECC和其他几种公钥系统相比，其抗攻击性具有绝对的优势。如160位ECC与1024位RSA、DSA有相同的安全强度。而210位ECC则与2048bitRSA、DSA具有相同的安全强度。

表1 ECC与RSA在安全性上的对照

ECC密钥长度	RSA密钥长	计算机解密代价(年)按每秒100万条指令计
160	1024	1E+12
320	5120	1E+36
600	21000	1E+78
1200	120000	1E+168

2)计算量小，处理速度快。虽然在RSA中可以通过选取较小的公钥(可以小到3)的方法提高公钥处理速度，即提高加密和签名验证的速度，使其在加密和签名验证速度上与ECC有可比性，但在私钥的处理速度上(解密和签名)，ECC远比RSA、DSA快得多。因此ECC总的速度比RSA、DSA要快得多。在相同的安全强度下，我们用160bit ECC进行加解密或数字签名要比用1024bit RSA、DSA快大约10倍。同时ECC系统的密钥生成速度比RSA快百倍以上。因此在相同条件下，ECC则有更高的加密性能。

3)存储空间占用小。ECC的密钥尺寸和系统参数与RSA、DSA相比要小得多。160位ECC与1024位RSA、DSA具有相同的安全强度，210位ECC则与2048位RSA、DSA具有相同的安全强度。意味着它所占的存贮空间要小得多。这对于加密算法在资源受限环境上(如智能卡等)的应用具有特别重要的意义。

4)带宽要求低。当对长消息进行加解密时，三类密码系统

有相同的带宽要求，但应用于短消息时ECC带宽要求却低得多。而公钥加密系统多用于短消息，例如用于数字签名和用于对称系统的会话密钥传递。带宽要求低使ECC在无线网络领域具有广泛的应用前景。

结论 目前，D－H密钥交换算法的专利已过期，RSA算法的专利期限也将面临结束，取而代之的是基于椭圆曲线的密码方案。ECC的这些特点使它必将取代RSA、D－H，成为通用的公钥加密算法。比如SET（Secure Electronic Transactions）协议的制定者已把它作为下一代SET协议中缺省的公钥密码算法。

参考文献

1 高品均，陈荣良. 加密算法与密钥管理[J]. 机界计算，2000，12：7～9

2 张克友，聂规划. NOVELL网的安全策略研究[J]. 电脑开发与应用，2001，14(10)：36～34

3 曾学蕾. 密码学的新方向[J]. 计算机应用，2002(12)：23～27

4 吴文玲，贺也平. 欧洲21世纪数据加密标准候选算法简评[J]. 软件学报，2001，12(1)：49～55

5 朱幼莲. 逻辑函数的计算机化简[J]. 计算机应用与软件，2003(2)：52～54

（上接第132页）

间的通信开销；第三，系统保证只有一个副本返回客户结果，减小了系统同外部应用间信道载荷。因此，同主动复制技术相比，SAR技术减小了整个系统的通信和处理开销，可以提高GCS性能，它特别适用于处理量大、消息交互频繁、对副本一致性要求不太严格的分布式应用。

4 SAR的一个分布式应用

现存的分布式应用大都采用了副本技术实现系统的容错。例如，CORBA定制了容错规范，CORBA2.2以上版本专门提出了容错CORBA[4]的概念，基于容错CORBA的GCS采用主动复制来提高分布式系统的可用性。而另外一种比较流行的中间件规范是Sun MicroSystem公司的EJB规范，在最新的EJB 2.0[5]版本中还没有正式的EJB容错规范，因此对EJB系统容错的探讨是一个新领域。而EJB是基于Server端构件的规范，因此提高基于EJB分布式系统的容错能力显得尤为重要，否则系统将出现由于Server崩溃而不可用的情况。一个直观的想法是采用CORBA规范中定制的组通信系统，但基于主动复制的组通信规范只适合于客户同处理机是多点通信的情形，而在EJB规范中，客户同处理机的交互是基于RMI-IIOP的点-点通信[5]，如果采用主从复制技术将不可能实现基于EJB规范的分布式应用容错，而我们认为本文提出的半主动副本技术是上述问题的一个解决方案。

客户同EJB服务器交互的基本过程为：客户stub通过JNDI找到Server（称为主服务器）后，客户向服务器发送RMI，服务器通过skeleton向EJB容器寻求方法调用，EJB容器将方法返回Server，Server在处理客户请求后，将结果返回客户。当主Server崩溃时，若系统是采用半主动复制技术进行错误屏蔽，有以下两种情形发生：

（1）当Server的崩溃发生在客户请求被备份之前，客户只有重新寻找Server。

（2）当客户请求已经被备份之后发生Server崩溃。如图3，类似于SAR应用于客户同处理机多点通信的情形（图2），但主副本向从副本发送的事件日志中，除了在主副本上所发生的事件外，还包含应用请求的信息，标记灰色者为当前主副本所在服务器。系统容错过程同3.3节所述相似，不再赘述。

由上可知，在这种客户同处理机点-点通信的分布式系统中，主动复制技术不再适用，而主/从复制技术的应用是一个可行方案，但对于有高可用性要求的系统而言，如上文提到的基于EJB规范的分布式应用，半主动复制技术是当然的首选。

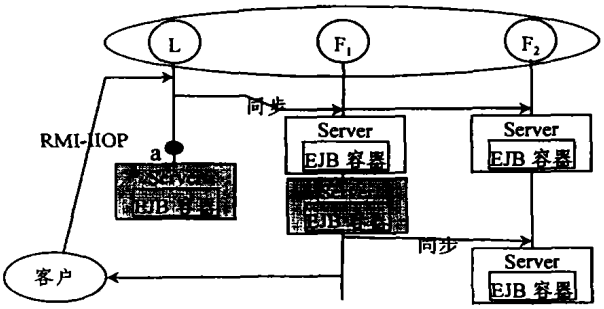

图3 SAR应用到基于EJB分布式系统容错

结束语 主动复制技术和被动复制技术在实现分布式系统容错时都有其不足之处，文中给出了一种兼具二者优点的半同步复制技术。此技术以消息为副本同步对象，在采用可靠的组播通信的前提下，应用被动复制的副本更替方案，很好地迎合了大型分布式应用对容错的需求。另外，我们将半主动复制技术应用于基于EJB规范中间件技术的容错问题，结果表明，此技术向此类分布式系统容错提供了一种很好的解决方案。因此，我们认为它是一种极具前景的分布式容错技术，对其的研究将成为分布式容错技术研究领域的热点。

文中并没有讨论对副本崩溃进行恢复的问题，这是我们下一阶段的研究工作。此外，在往后的研究工作中，我们还将致力于对SAR的副本同步做出更精确的描述、视图变化触发器等容错器件的设计等问题的研究，为此技术的实际应用奠定良好基础。

参考文献

1 Babaoglu O, et al. Group Communication in Partitionable Systems: Specification and Algorithms[J]. IEEE Transactions on Software Engineering, 2001, 27(4): 308～331

1 史殿习，等. 组通信中虚拟同步协议的研究与设计. 计算机研究与发展，2000，37(10)：1192～1196

3 Pedone F, et al. Exploiting Atomic Broadcast in Replicated Database. Processings of EuroPar. Southampton, England, Sep. 1998

4 CORBA 2.0 specification. http://www.omg.org

5 EJB 2.0 specification. http://java.sun.com/