计算机科学2002Vol. 29№. 6

椭圆曲线加密算法及其在 WTLS 中的应用*)

Elliptic Curve Algorithm and its Application of WTLS

余 堃[1] 周明天[1] 杨光志[2]

(电子科技大学计算机学院 成都610054)[1] (西南计算中心 绵阳621000)[2]

Abstract Elliptic curve algorithm is a kind of public key one that has been gradually mature, and a trend in a new public key standard algorithm. This paper depicts elliptic curve algorithm and generats a report about comparison with RSA, DH, etc. In the end, as a typical application of WTLS, the operation processes about primitive and schema are defined according to IEEE1363, and put in pratice.

Keywords Public key, Elliptic curve algorithm, RSA, DSA, DH, WTLS, IEEE P1363, Certificate, IFP, DLP

1 椭圆曲线算法

椭圆曲线指由 Weierstrass 方程:

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6 \quad (1)$$

所确定的平面曲线。若 F 是一个域,$a_i \in F, i=1,2,\cdots,6$满足式(1)的数偶(x, y)称为 F 域上的椭圆曲线 E 上的点。F 可以是有理数域,也可以是复数域,还可以是伽罗瓦域 GF(p')。除了曲线 E 上的点外,还需要加上一个无穷远点 O,可以理解为沿 y 轴趋向无穷远的点。

椭圆曲线的图像是关于 x 轴对称的,例如方程 $y^2=x^3-x$ 的图像如图1。

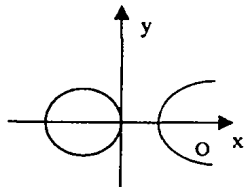

图1 方程 $y^2=x^3-x$ 的图像

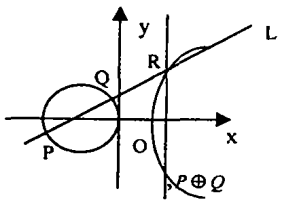

图2 椭圆曲线上的⊕运算

1.1 椭圆曲线上的⊕操作(图2)

设 $P=(x_1,y_1), Q=(x_2,y_2)$是 E 上任意两点,L 是 PQ 连线。若 P 和 Q 重合于一点,则 L 就退化为 P 点的切线。设 L 和曲线相交于另一点 R,L' 是 R 点和无穷远点 O 的连线,即 L' 是过 R 点引 y 轴平行线,L' 和曲线交于一点,用 P⊕Q 表示。实际上 P⊕Q 和点 R 是关于 x 轴对称的。若 P 和 Q 关于 x 轴对称或重合于 x 轴,则 PQ 垂直于 x 轴,这时 L 和椭圆曲线交于无穷远点 O。

1.2 ⊕运算的性质

定理1 若 P 和 Q 是曲线 E 上任意两点,PQ 连线 L 交 E 于另一点 R,则:①$(P\oplus Q)\oplus R=Q$;②$P\oplus O=P$;③ $P\oplus Q=Q\oplus P$;④E 上存在一点 Q,使 $P\oplus Q=O$;⑤对于 E 上的任意点 P,Q,R,$(P\oplus Q)\oplus R=P\oplus(Q\oplus R)$

O 点可以看作运算⊕的零元素。可以看出⊕运算满足交换律和结合律。所以可以证明椭圆曲线上的点关于⊕运算构成 Abel 群。

为方便起见,把 P⊕P 记为2P,P⊕P⊕…⊕P(m 次)记为 mP。

1.3 椭圆曲线的阶

定义1 P 是椭圆曲线 E 上的一点,若存在最小的正整数 n,使 nP=O,其中 O 是无穷远点,则称 n 是 P 的阶。

1.4 椭圆曲线密码系统

如前所述,椭圆曲线加密算法只是以伽罗瓦域的椭圆曲线运算实现传统公钥算法。具体实现方式是用由⊕运算迭代构成的"乘法"(*)运算代替整数域上的指数运算。

加密过程是这样的,把明文编码成 E 上的点,再通过椭圆曲线运算转换为另一个点,就成为密文。解密时把这个点用解密的椭圆曲线运算还原,从中可以得到明文信息。

在使用椭圆曲线算法时,必须制定椭圆曲线的参数。椭圆曲线包含以下参数。

·有限域 GF(q)。q 是素数或2^m。

·曲线方程。当 q 是素数时,方程为 $y^2=x^3+ax+b$;当 q 是2^m 时,方程为 $y^2+xy=x^3+ax^2+b$。a 和 b 是 GF(q)的元素。

·素数 r 和曲线上阶为 r 的点 G(G 称为阶 r 的子群的生成元)。

·可选的因子 $k=\#E/r$(#E 是 E 上点的个数)。

下面以椭圆曲线 Diffie - Hellman(ECDH)算法为例说明椭圆曲线算法的实现过程:

1)双方确定椭圆曲线参数,包括 q 和伽罗瓦域 GF(q)(q 可以是素数,也可以是2^m)、曲线方程、r 及生成元 G,作为公开信息。

2)A 产生一个 E 上的点 a,B 产生一个 E 上的点 b,分别作为自己的私钥。

3)A 计算 $PA=Ga$,B 计算 $PB=Gb$。

4)A 把 PA 传送给 B,同时 B 把 PB 传送给 A。

5)A 计算 $P=PB*a$,B 计算 $P'=PA*b$。

E 上的点 P=P' 就是协商出来的密钥。同样可以看出

*)本文的工作得到国家八六三项目(863-301-7-9)的支持。余 堃 副教授,研究方向:网络计算、安全计算、电子商务。周明天 博导,教授,研究方向:网络分布式计算、中间件计算。杨光志 高工,研究方向:网络计算、计算复杂性研究。

ECDH 算法的安全性依赖于 ECDLP 的困难性。

2 椭圆曲线算法的特点

2.1 安全性问题

对于一种加密算法来说，最重要的是提供较强的安全性。和传统的基于 IFP[1]（Integer Factorization Problem）和 DLP[1] 的（Discrete Logarithm Problem）算法比较，基于 ECDLP（Elliptic Curve Discrete Logarithm Problem）的椭圆曲线算法可以提供更高的安全性。虽然不能证明破解 RSA 算法必须通过解决 IFP，破解 DH 算法必须解决 DLP，破解椭圆曲线算法必须解决 ECDLP，但目前的研究都是通过这些途径进行的。经过多年的研究，对 DLP 和 IFP 的破解已经取得了重大的进展，出现了很多卓有成效的算法，如 NFS（Number Field Sieve）[4]技术，使这两个难题的难度大大降低了。而近20年来对 ECDLP 的分析研究基本上没有什么重大进展。这就使得椭圆曲线算法能以较小的密钥长度获得较高的安全性。

2.2 性能问题

在基于 DLP 和 IFP 的算法中，使用最频繁的是指数运算，而在基于 ECDLP 的椭圆曲线算法中，使用最频繁的是较为复杂的 GF(q) 上的椭圆曲线⊕运算。孤立地从这一点来看，椭圆曲线算法的速度远远低于传统算法的速度。但是从上节的讨论可以看出，椭圆曲线算法可以用较小的密钥长度获得较高的安全性，这一点对于其运算性能的提高是至关重要的。根据目前的研究，使用160位长度的椭圆曲线算法（$GF(2^{160})$）可以提供和使用1024位密钥，其安全性与 RSA 相同，而136位的椭圆曲线算法（$GF(2^{136})$）的安全性相当于768位的 RSA 算法。

由于可以使用较短的密钥，和传统的公钥加密算法相比，椭圆曲线算法在时间（处理速度）和空间（存储空间的需求）上都显示出了较强的优势。以下是来自 RSA 实验室的测试数据。

表1 椭圆曲线算法和 RSA 密钥存储空间的比较

单位为位（bit）

	基于 GF(q) 的 ECDS 或 ECES	RSA：n 为1024位，$e=2^{16}+1$
系统参数	(4 * 160)+1=641	0

表2 椭圆曲线算法和 RSA 算法的存储空间比较

公钥	160+1=161	1024+17=1041
私钥	160（加上系统参数，长度是801）	2048（如果使用 CRT 模式，长度为2056）

表2是椭圆曲线算法和 RSA 运行时间的比较，单位为进行一次1024位模乘（modular multiplication）的时间。

表3 椭圆曲线算法和 RSA、离散对数系统运行速度的比较

	基于 GF(q) 的 ECDS[2] 或 ECES[2]（q 为160bit）	RSA：n 为1024位，$e=2^{16}+1$，CRT 模式	基于1024位素数的离散对数系统
加密	120	17	480
解密	60	384	240
签名	60	384	240
校验	120	17	480

从以上数据可以看出，在提供相同安全性的前提下，椭圆曲线算法可以提供比传统算法更好的时间和空间性能。

3 椭圆曲线算法在 WTLS 协议中的应用

由于椭圆曲线算法的上述优势，它目前正逐渐进入信息安全应用领域，特别是对运行性能和存储空间要求较高的嵌入式系统和智能卡系统中。WAP 协议诞生于解决手机上网问题，其中的通信安全子协议 WTLS（Wireless Transport Layer Security）[5]建议采用椭圆曲线算法，以适应移动设备系统存储空间小、处理能力低、无线信道传输带宽狭窄的场合。

3.1 WTLS 协议

WTLS 是 WAP 协议栈的可选模块，用于提供移动设备到 WAP 网关的通信安全。WTLS 协议从 TLS 1.0[5]演化而来，针对无线信道和嵌入式系统的特殊要求作了一些修改，并引入了椭圆曲线算法作为推荐使用的算法。WTLS 的主要步骤如图3。在一个 WTLS 安全连接上，应用程序经过加密保护，并附上带密码的消息摘要，可以防止被窃听和篡改。

3.2 椭圆曲线算法在 WTLS 协议实现中的应用

在 WTLS 中定义了椭圆曲线算法 ECDH 和 ECDSA 作为可选的算法之一。ECDH 用于交换密钥协商信息，而 ECDSA 用于对密钥协商信息进行数字签名。

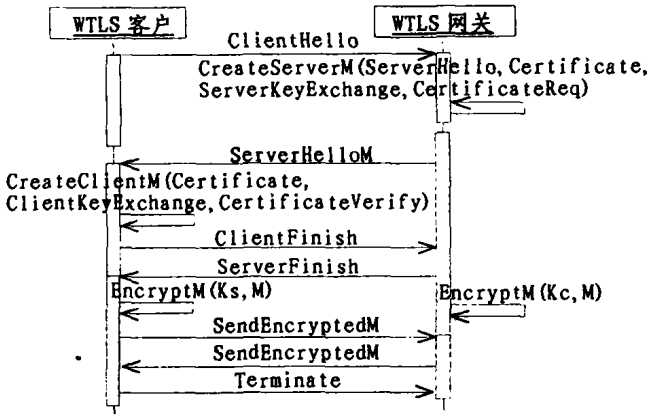

图3 WTLS 协议交互步骤

客户机在向服务器发送连接请求时，其中包含了可选的密钥协商算法。如果客户机提议使用 ECDH-ECDSA 算法进行密钥协商，ClientHello 中算法信息内容就会包括椭圆曲线参数，包括曲线方程系数、伽罗瓦域定义参数、生成元 G 和阶 r。如果服务器同意使用这种算法，ServerHelloM 就会向客户机发送自己的含有 ECDH 公钥和 ECDSA 公钥的证书，这些证书都是用 ECDSA 算法签名的。然后客户机在自己的 ECDH 证书或在密钥交换信息中向服务器发送自己的 DH 公钥，这些信息同样是用 ECDSA 算法签名的。这样双方通过 ECDH 算法可以安全地协商出一个秘密值，再通过一个伪随机数产生方法从这个秘密值中产生安全连接所需的全部参数。

3.3 WTLS 中椭圆曲线算法的软件实现

在 WTLS 中，椭圆曲线算法应遵照 IEEE P1363[1]实现，但协议问题没有给出具体的实现。本文使用原语（Primitive）和模式（Scheme）两个层次来定义椭圆曲线算法的操作过程。原语实现最基本的数学运算，而模式调用原语实现一定的安全功能。

3.3.1 原语 在 WTLS 的椭圆曲线算法实现中需要的原语如下：

（下转第101页）

策略中，惩罚技术最为通用和有效。惩罚技术本质是通过惩罚不可行解，把约束问题转化为无约束的优化问题。

然而，如何设计惩罚函数以有效地惩罚非可行解，对问题的解决至关重要，目前尚缺少普遍意义的指导原则。另外，对特定的约束优化问题，需要谨慎地选择合适的遗传运算。本文系统地阐述了遗传算法处理约束的策略和方法，特别是它的惩罚策略和遗传操作技术，希望能为实际工程应用中设计和开发具有更高性能、适用约束优化的进化算法提供和开拓一些新的思路。

参 考 文 献

1 Gen M, Cheng Runwei. Genetic algorithms and engineering design. New York: Wiley-Interscience, 2000

2 Gen M, Cheng Runwei. Genetic algorithms and engineering optimization. New York : Wiley-Interscience, 2000

3 Herrera F, Verdegay J L. Genetic algorithms and soft computing. Heidelberg Physica-Verlag, 1996

4 Man K F, Tang K S, Man S K. Genetic algorithms : concepts and designs London; New York : Springer, 1999

5 Michalewicz Z, Dasgupta D, et al. Evolutionary algorithms for industrial engineering problems. International Journal of Computers & Industrial Engineering, 1996, 30(4)

6 Glover F, Greenberg H. New approaches for heuristic search: A bilateral linkage with artificial intelligence. European Journal of Operational Research, 1989, 39: 119～130

7 Tanese R. distributed genetic algorithms for function optimization: [Ph. D. Thesis]. University of Michigan , Ann Arbor, MI, 1989

8 Michalewicz Z. Genetic Algorithm + Data Structure = Evolution Programs. Springer-Verlag, New York , 1994

9 Davis L. Handbook of genetic algorithms, New York, Van Nostrand Reinhold, 1991

10 Michalewicz Z, Attia N. Evolutionary algorithms for constrained engineering problems. In: Proc. of the third annual conf. on Evolutionary Programming, 1994. 98～108

11 Bean J C M, Hadj-Alouane A B. A dual genetic algorithm for bounded integer programs: [Technical Report TR 92-53]. Department of industrial and operations engineering , the University of Michigan, 1992

12 Hadj-Alouane A B, Bean J C. A Genetic algorithm for multichoice integer programs: [Technical Report TR 92-50]. Department of industrial and operations engineering , the University of Michigan, 1992

13 Powell D, Skolnick M M . Using Genetic algorithm in engineering design optimization with nonlinear constraints. In: Proc. of the 5th Intl. conf. on Genetic algorithm, 1993. 424～430

14 Schoenauer M, Xanthakis S. Constrained GA optimization. In: Proc. of the 5th Intl. conf. on Genetic algorithm, 1993. 573～580

15 Cheng R, Gen M. Genetic algrithms for multi-row machine layout problem. Engineering Design and Automation, 1996(to appear)

16 Wright A H. Genetic algorithm for real parameter optimization, (in): [21]205-218, 1991

17 Michalewicz Z, et al. Evolutionary operations for continuous convex parameter spaces. In: Proc. of the third annual conf. on Evolutionary Programming, 1994. 84～97

18 Janilow C, Michalewicz Z. An experimental comparison of binary and floating point representations in genetic alogrithms. In: Proc. of the 4th Intl. conf. on Genetic algorithm, 1991. 31～36

19 Gen M, Liu B, Ida K. Evolution program for deterministic and stochastic optimizations. European Journal of Operational Research, 1996(in press)

20 Tamaki H, et al. A Comparison study of genetic coding for the traveling salesman problem. In: Proc. of the 1th IEEE Intl. conf. on Evolutionary computation(ICEC'94)

21 Rawline G J E. Foundations of Genetic Algorithm. Morgen Kaufmann, San Mateo, CA, 1991

（上接第95页）

·ECSVDP-DH (Elliptic Curve Secret Value Derivation Primitive, Diffie-Hellman version)：椭圆曲线 Diffie-Hellman 秘密值生成原语，用于实现 ECDH 算法的数学运算，即用对方的 ECDH 公钥和自己的 ECDH 私钥计算双方协商的秘密值。

·ECSP-DSA (Elliptic Curve Signature Primitive, DSA version)：椭圆曲线 DSA 签名原语，用于实现 ECDSA 签名的数学运算，即用自己的私钥和数据产生签名数据。

· ECVP-DSA (Elliptic Curve Verification Primitive, DSA version)：椭圆曲线 DSA 校验原语，用于实现 ECDSA 校验的数学运算，即用对方的公钥和数据对签名进行校验。

3.3.2 *模式* 在 WTLS 的椭圆曲线算法实现中需要的模式如下：

·ECKAS-DH (Elliptic Curve Key Agreement Scheme, Diffie-Hellman version)：椭圆曲线 Diffie-Hellman 密钥协商模式，用于完成 ECDH 算法在应用程序中的全部过程。该过程在我们的实现中定义如下：

1)建立和双方密钥相关的有效的椭圆曲线域参数。

2)选择有效的私钥 s。

3)取得对方的公钥 w'。

4)通过调用 ECSVDP-DH 原语，用自己的私钥 s 和对方的公钥 w' 计算出秘密值 z。

5)把秘密值 z 转化为字节串 Z。

6)双方从字节串 Z 产生密钥。

·ECSSA (Elliptic Curve Signature Scheme with Appendix)：代附加数据的椭圆曲线签名模式，其中包含实现应用程序中使用的 ECDSA 签名数据(c,d)产生操作和签名数据校验操作。该签名过程在我们的实现中定义如下：

1)选择有效的私钥 s 和有效的域参数。

2)把消息 M 编码为整数表示形式 f。

3)通过调用 ECSP-DSA 原语，从整数 f 和私钥 s 产生出签名数据(c, d)。

4)输出签名。

而 ECSSA 的校验过程定义如下：

1)取得对方的公钥 w' 和相关的域参数。

2)把消息 M 编码为整数表示形式 f。

3)通过调用 ECVP-DSA 原语，对签名进行校验。如果校验成功，输出“校验成功”，否则输出“校验失败”。

小结 本文介绍了椭圆曲线密码体制及其应用，并以 WTLS 为例探讨了该密码体制实现的具体措施。该方法已由我们在国内首先用软件设计实现，已在康佳 WAP 手机上调试成功，并在该系统上可靠稳定地运行六个月以上。

参 考 文 献

1 Institute of Electrical and Electronics Engineers. Standard Specification for Public Key Cryptography. IEEE P1363 working draft D13, March 2001

2 Institute of Electrical and Electronics Engineers. Standard Specifications for Public Key Cryptography: Additional Techniques. IEEE P1363A, working draft D5, Aug. 2000

3 Robshaw M J B, Yin Y L. Elliptic Curve Cryptosystems. RSA Laboratory. http://www. rsasecurity. com/rsalabs/ecc/elliptic_curve. html, June 27, 1997

4 WAP Forum. Wireless Transport Layer Security. 06-Apr-2001, URL: http://www. wapforum. org/

5 Dierks T, Allen C. The TLS Protocol. Jan. 1999. rfc2246