改进的ECC算法在网络信息安全中的研究

魏先民
(潍坊学院计算机工程学院 潍坊 261061)

摘 要 目前网络信息安全遭受许多网络威胁,现有的加密算法已经无法满足网络信息安全的需求。提出了一种基于网络信息安全的改进ECC算法,该算法基于原有的ECC算法,对其进行点积运算的优化和平方剩余判定的优化,并对私钥更新变换进行了优化,以提高原有ECC算法的运算效率和安全性能。实验表明,基于网络信息安全的改进ECC算法在安全性能上比常用的RSA算法以及原有的ECC算法都有显著提高,该方案切实有效。

关键词 改进ECC算法,网络信息安全,点积运算优化,私钥更新变换

中图法分类号 TP309.7 **文献标识码** A

Research on Improved ECC Algorithm in Network and Information Security

WEI Xian-min
(School of Computer Engineering, Weifang University, Weifang 261061, China)

Abstract Network information security suffers many network threats, the existing encryption algorithm has been unable to meet the needs of network and information security problems. This paper proposed an improved ECC algorithm based on network information security, and the algorithm is based on the original ECC algorithm and makes its dot product operation optimization and square residual determination, optimization and transformation of the private key update to improve the original operational efficiency and safety performance of the ECC algorithm. The experiments show that the ECC algorithm based on network information security has significant improvements in safety performance than the RSA algorithm as well as the original ECC algorithms, and the program is effective.

Keywords Improved ECC algorithm, Network and information security, Dot product operation optimization, Private key update transform

随着互联网进入高速发展的阶段,把互联网作为工具进行信息的交流变得越来越常见,从而导致传统事务的运作方式面临巨大的挑战[1]。伴随着这场浩大的网络革命,不管是政府还是企业单位等都期望将自己原有的经营理念和模式向互联网方向转变[2]。所以,通过网络处理政务、购物、洽谈业务等将成为一种必然的趋势[3]。随之产生的信息安全问题,也越来越受到人们关注[4]。

为了确保信息安全,就必须在一定程度上克服威胁网络信息安全的种种威胁[5]。在各种网络安全技术中,加密技术是最核心的一种技术,也是解决网络信息安全最直接、最有效和最重要的途径[6]。

本文基于原有的ECC算法提出了一种基于网络信息安全的改进ECC算法,对原有算法进行了点积运算的优化和平方剩余判定的优化,并且对私钥更新变换进行了优化,提高了安全性能。

1 RSA算法简介

RSA算法是目前人们使用最多的加密算法,该算法起源于20世纪70年代末,其创造者是美国斯坦福大学的几位科研人员[7]。它的防篡改机制与传统电子商务中使用的DES、MAC算法不同,特点是对已有的信息的抗抵赖性,且用途十分广泛[8]。

RSA算法由一个公开密钥和一个私人密钥组成,其公开密钥可以公布给任何人,但是私人密钥则是个人所有[9]。当发送方发送消息时,使用接收方的公钥对信息进行加密,在接收后用接收方的私钥对其进行解密;或者发送方用自有的私钥对信息进行加密,接收方用发送方的公钥对信息进行解密[10]。

若 p 和 q 是两个素数,且 $n=p*q$,设 $t=(p-1)*(q-1)$,再取一个随机数 e,满足 $e<t$ 且 e 与 t 互质,并满足 $d*e\%t==1$,最终得到3个数:n,d,e。假设明文为 $M(M<n)$,对其进行加密 $c=(M^{\wedge}d)\%n$,则得到密文 c,对其进行解密操作 $m=(c^{\wedge}e)\%n$,便可完成 c 的解密。

在其加密、解密的进程中,公钥由 n 和 d 两个数构成;私钥由 n 和 e 两个数构成。

因为无法将 n 分解成 p 和 q,所以RSA算法的安全性得到了保障。

2 传统ECC算法概述

2.1 ECC算法原理

ECC算法是公钥密码学算法的一种。其椭圆曲线密码

到稿日期:2012-03-21 返修日期:2012-09-19 本文受2012年山东省高等学校优秀中青年骨干教师国际合作培养项目基金资助。

魏先民(1969—),男,博士,副教授,主要研究方向为分布式计算、智能传感网络,E-mail:wfxyweixm@126.com。

学的名字是由其曲线形式类似于计算椭圆周长的方程而得名。在实际使用过程中，一般使用有限域上的椭圆曲线。

设 F_p 为素数域，其椭圆方程可以表示为：

$$y^2=x^3+ax+b \bmod p \tag{1}$$

式中，a,b 满足：

$$4a^3+27b^2\neq 0, a,b\in F_p \tag{2}$$

式(1)、式(2)可以表示成 $E_p(a,b)$。

点加和点乘是椭圆曲线上的基本运算。素数域 F_p 上的基本运算法则为：对于曲线上的任意点 $P=(x_1,y_1)$，$Q=(x_2,y_2)$，令 $P+Q=(x_3,y_3)$，则逆元公式为：

$$-P=(x,-y) \tag{3}$$

加法运算为：

$$\begin{cases} x_3=(\lambda^2-x_1-x_2) \bmod p \\ y_3=[\lambda(x_1-x_3)-y_1] \bmod p \end{cases} \tag{4}$$

而点乘运算实际上是点的累加过程，是倍点运算和点加运算的结合。

2.2 ECC 算法密码机制

对于 $E_p(a,b)$ 上的点构成的阿贝尔群，考虑公式 $Q=kp$，$k\in F_p$。基于 $E_p(a,b)$ 上的离散对数问题，设用户的私钥为 k，则用户的公钥可以表示为 $Q=kp$。基于此，通过 ECC 算法，加密和解密便可以顺利实现。

具体过程为：当用户 A 发送消息 M 给用户 B(其公钥为 PKB)时，立刻产生一个随机数 $n\in(0,p)$，并进行 $K_1=nG$ (G 为椭圆基点)和 $K_2=n\cdot PKB$ 的计算；然后用 K_2 的 X 坐标对 M 采用 ECC 算法进行加密，如 $ECC_{X(K_2)}(M)\parallel K_1$。最后，用户 A 将 $ECC_{X(K_2)}(M)\parallel K_1$ 发送给用户 B。

B 接收到 $ECC_{X(K_2)}(M)\parallel K_1$ 后，首先计算 $K=K_1\cdot SKB=n\cdot G\cdot SKB=n\cdot PKB=K_2$，然后用 K 的 X 坐标对 $ECC_{X(K_2)}(M)$进行解密，得到 M。到此，解密过程完成。

3 改进 ECC 算法

3.1 点积运算的优化

在使用 ECC 算法进行加密、解密的时候，会有大量的点积运算，如：

$$nP=P_1+\cdots+P_n \tag{5}$$

本文对其点积运算进行了优化，过程如下：

(1)将 n 用二进制数的形式表示，即 $n=(n_kn_{k-1}\cdots n_i\cdots n_1)$。式中，$n_i=0$ 或 1，$k=[\log_2 n]+1$。

(2)除去 $(n_kn_{k-1}\cdots n_i\cdots n_1)$ 的最高位 n_k，便可得 $(n_{k-1}\cdots n_i\cdots n_1)$。

(3)依照 $(n_{k-1}\cdots n_i\cdots n_1)$ 从高到低的顺序，当 $n_i=0$ 时，计算 $2P$；当 $n_i=1$ 时，计算 $2P+P$，并将计算结果作为下次运算的初始值，即 $2P\Rightarrow P$ 或 $2P+P\Rightarrow P$。

如果使用传统 ECC 算法，则需要进行 n 次运算；经过本文提出的优化策略，则平均只需要进行 $3/2[\log_2 n]$次运算，最多也只需要 $2[\log_2 n]$次运算，从而减少了运算时间，提高了运算速度。

3.2 平方剩余判定优化

平方剩余判定就是在明文映射到 ECC 曲线上的时候，对 P 的平方剩余的判定。现有的判定方法涉及大量的平方和取模运算，本文在提高其运算效率的基础上加以改进，提出一种判定快速算法。

假设曲线 $P_m(x,y)$上有明文 m 的映射，且存在下列关系：

$$\begin{cases} 256m\leqslant x\leqslant 256(m+1) \\ P_m(x,y)\in F_p \end{cases} \tag{6}$$

平方剩余判定就是计算模 P 下的平方剩余是否存在$A=x^3+ax+b$，即 A/q 的值是不是等于 1。本文提出的改进算法如下所示：

(1)把平方剩余判定变量表示为 J，且满足条件 $J=1$。

(2)假设 A 为偶数，那么便可以将其进行分解，得到：

$$(A/P)=(2/P)((A/2)/P) \tag{7}$$

对$(2/P)$进行求解后，再将其代入式(8)：

$$J(2/P)\Rightarrow J, A/2\Rightarrow A \tag{8}$$

假设 A 为奇数，那么便可以将其进行分解，得到下式：

$$(A/P)(P/A)=(A/P)((P \bmod A)/P)$$
$$=(-1)^{((A-1)/2)((P-1)/2)} \tag{9}$$

$$(A/P)=(-1)^{((A-1)/2)((P-1)/2)}((P \bmod A)/A) \tag{10}$$

综上，对(A/P)进行判定就是对$((P \bmod A)/A)$进行判定，可以进行以下计算：

$$J(-1)^{((A-1)/2)((P-1)/2)}\Rightarrow J \tag{11}$$

$$A\Rightarrow q \tag{12}$$

$$P \bmod A\Rightarrow A \tag{13}$$

$$q\Rightarrow P \tag{14}$$

假设 A 在奇数的基础上不是素数，那么便可将其分解成 $\prod A_i$；假设 A 在奇数的基础上又为素数，那么定义 A_i 为奇素数，可得：

$$(A/P)=(A_1/P)(A_2/P)\cdots(A_i/P) \tag{15}$$

然后对每一个(A_i/P)进行求解。

(3)如果计算得到 A 不为 1，那么返回步骤(2)，反之跳出算法。这个时候就可以根据 J 判断模 P 下的平方剩余是否存在 $A=x^3+ax+b$，如果 $J=1$，则存在 x^3+ax+b；如果$J=-1$，则不存在 x^3+ax+b，也不是平方剩余。

3.3 私钥更新变换优化

本文在传统 ECC 算法的基础上提出一种私钥更新变换机制，将用户的私钥进行不断的变换，以保证私钥的安全性。一般来说，用户先注册得到 PK 并保存对应的用户私钥 SK。把公钥的有效时间分为 T 个时间段，分别记为 $1,2,\cdots,T$。在公钥的时间段为 1 时，用户私钥为 SK_1；在公钥的时间段为 2 的时候，用户私钥为 SK_2，以此类推。利用单向 Hash 函数对 SK_{i-1}到 SK_i 进行变换操作，当 SK_i 变换成功后，立刻删除 SK_{i-1}。其更新变换过程如下所示：

$$\begin{array}{cccccc} T_1 & T_2 & T_3 & \cdots & T \\ SK_0 & SK_1 & SK_2 & \cdots & SK_T \end{array} \tag{16}$$

因为整个优化过程是利用单向 Hash 函数对其进行变换操作，所以大大增加了从后一个私钥推算前一个私钥的难度，增加了信息的安全性。

具体过程如下所示：

任意在有限域上选取两个大素数 p,q。假设用户 A 的私钥为 SK_0，设定其私钥的更新次数为 T，则其公钥的计算公式为：

$$PK=q^{SK_0 2T+1} \bmod p \tag{17}$$

公开大素数 p,q 和计算得到的用户 A 的公钥 PK 和 T。

用户根据所设定的时间段不断对私钥进行变换,得到新的私钥,再将旧的私钥进行删除。

设 j 为时间段,则私钥的更新方法如下所示:

如果 $j=T+1$,则 SK_j 为空,即用户私钥的有效期已到。

如果 $1\leqslant j<T+1$,则用式(18)计算下个时间段的用户私钥:

$$SK_{j+1}=SK_j^2 \bmod p-1 \tag{18}$$

4 算法仿真

在相同的安全强度下,算法采用密钥长度越小,其安全性能越高。本文在同样的网络中对 RSA 算法、原有 ECC 算法和改进 ECC 算法进行安全性能测试,其实验结果如图 1 所示。

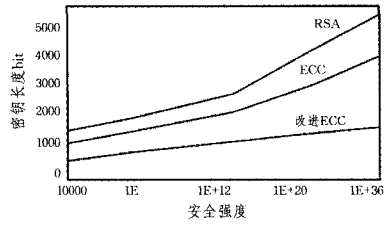

图 1 安全性能比较统计

从图 1 可以看出,经过本文改进后的 ECC 算法的抗网络攻击性能比其他算法更为优秀,且为了提高其安全性能而增加密钥长度的增长幅度比 RSA 算法和 DSA 算法小很多,具体比较如表 1 所列。

表 1 相同安全强度下模长比较

攻破时间	RSA 密钥长度	ECC 密钥长度	改进 ECC 密钥长度
104	512	106	96
108	768	132	118
1011	1024	160	124
1020	2048	210	156
1078	21000	600	418

从表 1 可以看出,在相同安全强度下改进 ECC 算法的密钥尺寸相对较小,说明其占用空间也小,这就意味着其防网络攻击能力更强。所有这些优势,使得改进 ECC 算法的安全性能比之以前的 RSA 算法和一般 ECC 算法来得更强。

从图 2 可以看出,在相同的网络中,分别采用 RSA 算法、ECC 算法和改进 ECC 算法进行加密,并使用穷举密码破解法对其进行解密操作,对改进 ECC 算法加密的信息进行解密的时间远大于 RSA 算法和 ECC 算法。综上所述,本文提出的改进 ECC 算法大大提高了网络信息的安全性能,达到了安全高效的目的。

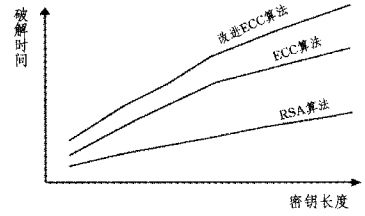

图 2 3 种算法破解时间比较

结束语 本文针对目前网络信息安全现状,提出了一种基于网络信息安全的改进 ECC 算法。该算法基于原有的 ECC 算法,对其进行点积运算的优化和平方剩余判定的优化,以提高原有 ECC 算法的安全性能。实验证明,改进 ECC 算法比普遍使用的 RSA 算法和原有的 ECC 算法安全性能更高。

参 考 文 献

[1] 赵龙,韩文报,杨宏志. 基于 SIMD 指令的 ECC 攻击算法研究[J]. 计算机研究与发展,2012,49(7):1553-1559

[2] 徐劲松,王志新,严迎建. ECC 专用指令处理器软硬件协同设计[J]. 计算机工程与设计,2012,33(3):916-920

[3] 尤马彦,凌捷,郝彦军. 基于 Elman 神经网络的网络安全态势预测方法[J]. 计算机科学,2012,39(6):61-63

[4] 罗利民,周震. 基于 IPV6 的网络安全入侵检测技术研究[J]. 科技通报,2012,28(4):114-115

[5] 陈亮,潘惠勇. 网络安全风险评估的云决策[J]. 计算机应用,2012,32(2):472-474

[6] 贺志强,楼芳,李亮. 基于攻击距离的攻击图优化方法[J]. 计算机工程与科学,2012,34(2):9-12

[7] 王庚,张景辉,吴娜. 网络安全态势预测方法的应用研究[J]. 计算机仿真,2012,29(2):98-101

[8] 查东辉. 网络蠕虫传播模型的分析与仿真研究[J]. 计算机仿真,2012,29(2):124-127

[9] 张栋毅. 校园网络安全分析与安全体系方案设计[J]. 计算机应用,2011,31(2):116-118

[10] 李志刚. 网络通信中加密算法优化仿真研究[J]. 计算机仿真,2011,28(12):130-133

[11] 熊万安,许春香. 一种新的基于 ECC 的 Ad hoc 组密钥协商协议[J]. 重庆邮电大学学报:自然科学版,2011,23(1):101-106

(上接第 135 页)

[4] Tian Li-qin, Lin Chuang, Sun Jin-xia. A kind of prediction method of user behavior for future trustworthy network [C]// Proc. of ICCT 06. Beijing: IEEE Press, 2006: 199-202

[5] Guo Shu-kai, Tian Li-qin, Shen Xue-li. Research on FAHP method in user behaviour trust computation[J]. Computer Engineering and Applications, 2011, 47(12): 59-61

[6] Tian Li-qin, Lin Chuang. A Kind of Game-Theoretic Control Mechanism of User Behavior Trust Based on Prediction in Trustworthy Network [J]. Chinese Journal of Computers, 2007, 30(11): 1930-1938

[7] Chen Ya-rui, Tian Li-qin, Yang Yang. Model and Analysis of User Behavior Based on Dynamic Game Theory in Cloud Computing[J]. Acta Electronica Sinica, 2011, 39(8): 1818-1822

[8] Saaty T L. Decisions with the Analytic Network Process(ANP) [C]// ISAHP'96 CANADA. University of Pittsburgh., USA, 1996

[9] Van Laarhoven P J M, Pedrycz W A. fuzzy extension of Statty's Priority theory[J]. Fuzzy Sets and Systems, 1983, 11: 229-241