第 35 卷 第 4 期 计 算 机 工 程 2009 年 2 月
Vol.35 No.4 Computer Engineering February 2009
·安全技术· 文章编号：1000—3428(2009)04—0180—03 文献标识码：A 中图分类号：TP309

基于圆性质的加密算法

葛丽娜[1,2]，贺忠华[2]，江焯林[1]
(1. 华南理工大学计算机科学与工程学院，广州 510640；2. 广西民族大学数学与计算机科学学院，南宁 530006)

摘 要：原有对称加密算法采用置换与替换技术。该文提出一种基于圆性质的对称密钥加密算法，采用随机数技术与密码学杂凑函数，使加密后的密文随机分布于 n 维几何空间，实现了抗密码分析攻击，而穷举攻击在计算上是不可行的。该算法适用于带时间戳加密、短明文加密等应用环境，实验结果验证了其可行性。

关键词：对称密码；加/解密算法；圆性质

Encryption Algorithm Based on Circle Property

GE Li-na[1,2], HE Zhong-hua[2], JIANG Zhuo-lin[1]
(1. School of Computer Science and Engineering, South China Univ. of Tech., Guangzhou 510640;
2. School of Mathematics and Computer Science, Guangxi University of Nationalities, Nanning 530006)

【Abstract】 The former symmetric encryption algorithms use substitution and transposition techniques. This paper presents a symmetric encryption algorithm based on circle property. The techniques of random number and cryptographic hash function are used in this algorithm. So the cipher text randomly distributes in the n-dimensional space and led to cryptanalysis being difficult. From the security analysis the brute-force attacks are infeasible. It is applicable for encryptions with timestamp and short plain text encryptions. Experimental results verify that this algorithm is feasible.

【Key words】 symmetric cryptogram; encryption and decryption algorithm; circle property

1 概述

基于几何方法，文献[1]和文献[2]分别提出采用智能卡的有效远程登录认证方法和秘密共享方案，为信息安全研究开拓了新方向。其后，一些学者提出几何认证方法[3-7]。在此类系统中，每个用户与 CA 服务器共享一个秘密，当用户被系统认证为合法用户后，可以登录系统并与服务器共享秘密。文献[5-7]根据圆的几何特性构造认证协议，其中，用户与服务器共享的秘密构成一个圆。文献[8]指出文献[1]方案的安全缺陷，并修正文献[4]方案，使其能抵制用户口令猜测攻击。文献[9]针对文献[1]可能面临的安全隐患，即可能的 CA 背叛和 CA 服务器泄露，提出采用智能卡 CA 代替 CA，以避免不可信 CA 的违规操作带来的安全问题。

当用户登录系统后，利用用户与系统共享的秘密，使该用户在系统中以几何方法加密的方式与服务器、其他合法系统用户以及系统资源进行通信，可以进一步发展几何方法在信息安全中的应用。本文尝试以几何空间中的点作为通信双方的共享密钥，利用几何方法设计对称加/解密算法。

在本文中，p 表示一个大素数，且 $p\equiv3(\mathrm{mod}4)$，可以利用下式求得一个二次剩余元素方根[10]：

$$x=a^{(p+1)/4}(\mathrm{mod}p)$$

其中，$a\in QR_p$；x 是 a 的模 p 的一个平方根。算法中的运算定义于有限域 $GF(p)$上。

2 密码算法

现有密码学分为 2 种，即传统密码学和公钥密码学。传统密码加密又称对称加密或单钥加密，是公钥密码产生之前唯一的加密技术。对称加密系统最重要的特征是加密与解码的密钥相同。公钥密码学与其之前的密码学完全不同，它使用 2 个独立的密钥。对称密码体制与公钥密码体制各有优势，对称密码一般用于会话加密，公钥密码通常用于密钥分配与数字签名。

攻击对称加密密码体制主要包括如下 2 种方法：

(1)密码分析学。依赖算法性质和明文的一般特征或某些明密文对，此类形式的攻击企图利用算法特征推导特别的明文或使用的密钥。对称密码体制的所有分析方法都利用以下事实：明文的结构和模式在加密后仍然被保存，并能在密文中找到一些相关信息。

(2)穷举攻击。攻击者对一个密文尝试所有可能的密钥，直到把它转化为可读的有意义明文。平均而言，获得成功至少要尝试所有可能密钥中的一半。

3 算法描述

本文加密算法属于对称加密方法，双方共享密钥是空间中的一个秘密点，利用密钥、明文、随机数和杂凑函数建立一个圆，并利用圆上的任意一点表示密文。

定理 p 是一个奇素数，如果 2 是一个模 p 二次非剩余，则任意 $z\in[0,p)$ 能表示为 $k(k\geq2)$个整数模 p 的平方之和[11]。

定理是下文加密算法的理论基础，圆 $\sum_{i=1}^{n}(x_i-c_i')^2=R(\mathrm{mod}\ p)$ 的半径平方 R 可以分解为 n 个整数模 p 的平方之和，由此可以获得该圆上的一点。

3.1 加/解密算法

设 p 为一个形如 $p\equiv3(\mathrm{mod}4)$的大素数，用户 A 与用户 B

基金项目：国家自然科学基金资助项目(60572139)；教育部新世纪优秀人才支持计划基金资助项目(NCET-06-0744)；霍英东教育基金资助项目(101069)

作者简介：葛丽娜(1969－)，女，博士研究生，主研方向：网络与信息安全；贺忠华，讲师、硕士；江焯林，博士研究生

收稿日期：2008-08-21 **E-mail：**gelina100@gmail.com

共享一个秘密点$(c_1, c_2,\cdots,c_n)$，称为 A 与 B 之间的共享密钥；设明文 $m\in[0,p)$；假设几何空间的维数为 n；密文记为 C；密码学杂凑函数 $f=[0,p),[0,p),[0,p)\to[0,p)$。

3.1.1　加密算法

加密算法指 A 将明文 m 加密为密文 C，具体步骤如下：

(1)用户 A 任选一个随机数 $s\in[0,p)$，并计算 $c_1'=f(c_1, c_2,s)$, $c_2'=f(c_2,c_3,s)$, $\cdots$, $c_n'=f(c_n,c_1,s)$, $R=m+s(\mathrm{mod}\ p)$。

(2)由 $(c_1',c_2',\cdots,c_n')$ 与 R 建立圆Ω的方程，即

$$\sum_{i=1}^{n}(x_i-c_i')^2=R(\mathrm{mod}\ p)$$

称Ω为秘密圆。

(3)在Ω上任取一点 $Q(q_1,q_2,\cdots,q_n)$，根据定理，利用如下方法求 Q：

1)随机找到 n-2 个数对$(e_j,\ d_j)$满足 $e_j\equiv d_j^2\ (\mathrm{mod}p)$, j=1, 2,$\cdots$,n-2，令

$$\begin{cases}q_1=d_1+c_1'(\mathrm{mod}\ p)\\ q_2=d_2+c_2'(\mathrm{mod}\ p)\\ \cdots\\ q_{n-2}=d_{n-2}+c_{n-2}'(\mathrm{mod}\ p)\end{cases}$$

2)随机生成 $d_{n-1}\in(0,p)$，计算 $e_{n-1}=d_{n-1}^2(\mathrm{mod}\ p)$，$e_n'=R-\sum_{j=1}^{n-1}e_j(\mathrm{mod}\ p)$，则 $d_n=e_n'^{(p+1)/4}(\mathrm{mod}\ p)$；计算 $e_n=d_n^2(\mathrm{mod}\ p)$。

3)重复 2)，直到 $e_{n-1}+e_n=R-\sum_{j=1}^{n-2}e_j(\mathrm{mod}\ p)$，令 $q_{n-1}=d_{n-1}+c_{n-1}'(\mathrm{mod}\ p)$，$q_n=d_n+c_n'(\mathrm{mod}\ p)$。

4)令 $Q=(q_1,q_2,\cdots,q_n)$。

(4)将 (Q,s) 记为 m 的密文，即 $C=(Q,s)$。

步骤(3)中的 d_n即 e_n的模 p 的平方根。

3.1.2　解密算法

解密算法指用户 B 将密文 $C=(Q,s)$ 解密，获取明文 m，具体步骤如下：

(1)用户 B 根据 s 与密钥$(c_1,\ c_2,\cdots,c_n)$计算 $c_1'=f(c_1, c_2,s)$, $c_2'=f(c_2,c_3,s)$, $\cdots$, $c_n'=f(c_n,c_1,s)$，获得 $O'(c_1',c_2',\cdots,c_n')$。

(2)根据 $O'(c_1',c_2',\cdots,c_n')$与密文中的 $Q(q_1,q_2,\cdots,q_n)$ 计算 $R'=\sum_{i=1}^{n}(q_i-c'_i)^2(\mathrm{mod}\ p)$ $m'=R'-s(\mathrm{mod}\ p)$，m'是解密出来的明文，即 m=m'。

3.2　算法的正确性

加密时，由于 Q 是秘密圆上的一点，秘密圆圆心为$(c_1',c_2',\cdots,c_n')$、半径平方 R=s+m(mod$p$)，因此解密时 Q 与 $O'(c_1',c_2',\cdots,c_n')$之间的距离平方 R'等于秘密圆的半径平方 R。

因为 $R=m+s(\mathrm{mod}\ p)$，则 $R'=m+s(\mathrm{mod}\ p)$，所以

$$m=R'-s(\mathrm{mod}\ p)$$

4　算法分析

4.1　安全性分析

4.1.1　穷举攻击

假设攻击者窃听到密文 $c=(Q,s)$，并采用穷举攻击方法，企图获取密钥、明文。当空间维数为 n 时，密钥的取值数目可达 p^n，因为 $2^{|p|-1}<p<2^{|p|}-1$，所以密钥可取值的数目达$(2^{|p|-1})^n\sim(2^{|p|}-1)^n$。攻击者可以将每个可能的密钥都用于解密，比较解密的内容，从而获密钥。该过程所需时间为$(2^{|p|-1})^n\times t\sim(2^{|p|}-1)^n\times t$，其中，$t$ 为每次解密所需时间。攻击者的平均计算次数通常为总次数的一半，因此，所需平均时间为$(2^{|p|-1})^n\times t/2\sim(2^{|p|}-1)^n\times t/2$。例如，当 n=2, $|p|$=512 时，t=0.008 s，则平均攻击时间为 5.70×10^{297} 年~2.28×10^{298} 年，可见，穷举攻击在计算上是不可行的。

4.1.2　密码分析攻击

每次加密都在最初密钥$(c_1, c_2,\cdots,c_n)$的基础上导出本次加密的秘密圆的圆心 $(c_1',c_2',\cdots,c_n')$，即以密钥与一次性随机数 s 为参数求杂凑函数，将其结果作为秘密圆的圆心，半径平方是明文与 s 之和。因此，对相同明文每次加密后，得到的是不同秘密圆。在秘密圆上任取一点作为密文，即使秘密圆相同，每次取到的点是不同的。因此，本文加密算法将一个明文分组的密文均匀地分布在定义于 $GF(p)$上的 n 维空间中，增加了密码分析攻击的难度。

差分分析和线性分析是常用的密码分析方法，但不适用于本文加密算法。差分分析主要针对加密算法迭代中产生的差分。线性密码分析的基本原理通过分析多组明文-密文对，找一个有效的线性等式，以便从中解出密钥。在本文算法中，每次加密时，密钥的各个分量都与随机数进行杂凑函数运算，使运算结果完全随机化，因此，无法找到明文-密文对的线性关系。

假设攻击者得到了一个明文 m 的 k 次加密密文$(x_{1,1}, x_{1,2},\cdots,x_{1,n})$, $(x_{2,1}, x_{2,2},\cdots,x_{2,n})$,$\cdots$, $(x_{k,1}, x_{k,2},\ldots,x_{k,n})$，若他想从上述数据中破解密钥、明文，则需要建立式(1)。

$$\begin{cases}(x_{1,1}-f(c_1,c_2,s_1))^2+(x_{1,2}-f(c_2,c_3,s_1))^2+\ldots+(x_{1,n}-f(c_n,c_1,s_1))^2=\\ \qquad\qquad m+s_1(\mathrm{mod}\ p)\\ (x_{2,1}-f(c_1,c_2,s_2))^2+(x_{2,2}-f(c_2,c_3,s_2))^2+\ldots+(x_{2,n}-f(c_n,c_1,s_2))^2=\\ \qquad\qquad m+s_2(\mathrm{mod}\ p)\\ \ldots\\ (x_{k,1}-f(c_1,c_2,s_k))^2+(x_{k,2}-f(c_2,c_3,s_k))^2+\ldots+(x_{k,n}-f(c_n,c_1,s_k))^2=\\ \qquad\qquad m+s_k(\mathrm{mod}\ p)\end{cases}\tag{1}$$

其中，$(c_1, c_2,\cdots,c_n)$, m 是未知数，其他均为已知数，方程个数可以根据求解需要而定，即 k 可以是任意的。在式(1)中，未知量之间存在非线性指数关系，即对多个未知量构成杂凑函数(f 为一个杂凑函数)，因此，对算法的密码分析攻击可归约到非线性的有限域方程组求解上。要解式(1)只能采用穷举法，而穷举法对本方案是不可行的。同理，即使明文 m 已知，利用式(1)仍然不能求出密钥$(c_1, c_2,\cdots,c_n)$。

4.2　算法的计算方法分析

本文算法与其他对称加解密算法不同，其结构不是替换、置换的形式，而是采用函数与随机变换的形式。算法结构简单，实现方便。

加密算法涉及杂凑函数与在圆上任取一点的运算，杂凑函数的运算速度通常很快，在圆上任取一点需要 n 次的平方运算。密文规模需要一个空间点和一个随机数表示。

4.3　算法的应用

本文加密算法可实现带时间戳的加密。加密算法的输入参数除了明文 m 外，还有一个公开参数即随机数 s。如果 s 用时间戳 T 代替，则该算法成为带有时间戳的加密算法，在加密过程中调用了 $f(c_1,c_2,T)$, $f(c_2,c_3,T)$,$\cdots$, $f(c_n,c_1,T)$，由于 f 是带有 3 个参数的杂凑函数，因此即使已知 $f(c_1,c_2,T)$和 T，仍然无法求出 c_1 与 c_2。同理，无法找到 T'使 $f(c_1,c_2,T)$=$f(c_1,c_2,T')$，即攻击者无法篡改带有时间戳的密文。因此，本文算法适用于带时间戳的加密应用环境。

本文加密算法拥有密文不可区分的优势，且密文扩大了

明文带宽的不足，适用于用于一些短消息的加密，对短明文的加密具有强安全性。比如对只有“0”或“1”消息的加密，如果某加密算法对于某明文的密文固定，密钥拥有者若提供加密预言机服务，则明文信息很容易被确定。而本文算法每次加密均将某明文随机分布到密文空间中，则密钥拥有者即使提供了加/解密预言机服务，攻击者也很难获得到明文。

本文算法可以为“几何认证系统”提供后续安全服务，比如为合法用户与几何认证服务器之间协商会话密钥等。

5 实验与分析

笔者从 2 个方面分析算法性能：时间消耗和密文信息量消耗。通过 Java 编程语言实现本文算法，所有运算定义于有限域 $GF(p)$上，涉及的点与圆均位于 $n(n=2,10,20,30,40,50)$维几何空间中。硬件环境如下：CPU 频率为 2.5 GHz，内存为 512 MB，操作系统为 Window XP 单台机器，开发工具是 JDK，其版本为 1.5，采用 eclipes-SKD-3.0.1 的集成工具。

5.1 时间消耗

5.1.1 加密算法

加密算法的时间消耗如表 1 所示，其中，$|p|$表示 p 的二进制位数。由表 1 可以看到，当空间维数不变时，p 的大小对算法的影响较大。当 $n=2$ 时，若 p 取 512 位的大素数，则加密时间为 30 ms；若 p 取 768 位的大素数，则加密时间为 90 ms。当 p 取值不变时，空间维数 n 由 2 变为 50 时，加密时间消耗变化很小。例如，当 p 取 512 位的大素数时，若 $n=2$，则加密需要的时间为 30 ms；若 $n=50$，则时间消耗为 34 ms，变化很小。可见，当 n 变大时，密钥长度呈线性增长，而安全强度呈指数级增长。要获得强的密钥安全性并使时间消耗较少，应选择 p 的位数短而 n 值大的情形，但此时每个分组的信息量只有$|p|$。由于算法有选择 n 与$|p|$的灵活性，因此本文算法能适应不同应用与安全需求。

表 1 加密算法的时间消耗

$\|p\|$/bit	一个明文分组的加密时间/ms					
	n=2	n=10	n=20	n=30	n=40	n=50
768	90	93	94	96	97	99
512	30	31	31	33	33	34
32	0.7	1.3	1.8	2.3	2.8	3.5

5.1.2 解密算法

解密算法的时间消耗如表 2 所示。比较表 2 与表 1，可知解密时间消耗的变化趋势与加密算法相同。

表 2 解密算法的时间消耗

$\|p\|$/bit	一个明文分组的解密时间/ms					
	n=2	n=10	n=20	n=30	n=40	n=50
768	23	24	25	27	28	29
512	8	9	10	11	11	12
32	0.14	0.25	0.35	0.40	0.43	0.50

5.1.3 与 DES 时间消耗的比较

在相同实验环境下，DES 的加/解密时间消耗见表 3。

表 3 DES 加/解密时间消耗 ms

加密	解密
0.29	0.22

在穷举攻击下，本文加/解密算法在$|p|$=32 bit, n=2 时，密钥长度为 64，安全强度略优于 DES。由表 1 和表 2 可知，本文加密时间为 0.7 ms，解密时间为 0.14 ms。由表 3 知 DES 的加密时间为 0.29 ms，解密时间为 0.22 ms，且 DES 的明文分组是 64 位，而本文算法的明文分组是 32 位。本文算法的加密时间消耗多于 DES，而解密时间略小于 DES。

5.2 密文信息带宽消耗

密文具体表示为 $C=(Q,s)$，即 n 维空间的一点和一个随机数，一个点包含 n 维坐标，因此，所占空间为 n 个有限域 $GF(p)$中的数，则密文所占空间总数为$(n+1)$个。一个明文分组占的空间为 1 个。密文的带宽是明文带宽的$(n+1)$倍，即密文的带宽与空间的维数 n 成正比。因此，本文加密算法适用于小量信息的数据加密。密文长度消耗见表 4。

表 4 密文长度消耗

$\|p\|$/bit	密文信息带宽消耗/Byte					
	n=2	n=10	n=20	n=30	n=40	n=50
56	21	77	147	217	287	357
512	192	704	1 344	1 984	2 624	3 264
768	288	1 056	2 016	2 976	3 936	4 896

6 结束语

几何方法被逐步用于用户远程登录的身份认证和秘密共享，为适应几何认证系统的进一步应用，应扩展几何方法在信息安全领域的适用范围。本文基于 n 维几何空间中圆的性质，利用随机数、密码学杂凑函数等技术设计了一个对称的加/解密算法，它适用于有多种不同安全需求的环境。本文只是初步实现了上述算法，可以进一步对其进行优化，以得到更高的加/解密速度。

参考文献

[1] Wu Tzone-chen. Remote Login Authentication Scheme Based on a Geometric Approach[J]. Computer Communications, 1995, 18(12): 959-963.

[2] Wu Tzone-chen, He Weihua. A Geometric Approach for Sharing Secrets[J]. Computer & Security, 1995, 14(2): 135-145.

[3] Hwang Min-shiang. Cryptanalysis of a Remote Login Authentication Scheme[J]. Computer Communications, 1999, 22(8): 742-744.

[4] Chien Hung-yu, Jan Jinn-ke, Tseng Yuh-min. A Modified Remote Login Authentication Scheme Based on Geometric Approach[J]. Journal of Systems and Software, 2001, 55(3): 287-290.

[5] Wang Shiuh-jeng. Yet Another Login Authentication Using N-dimensional Construction Based on Circle Property[J]. IEEE Trans. on Consumer Electronics, 2003, 49(2): 337-341.

[6] Wang Shuhong, Bao Feng, Wang Jie. Comments on Yet Another Log-in Authentication Using N-dimensional Construction[J]. IEEE Transactions on Consumer Electronics, 2004, 50(2): 606-608.

[7] Yang Fuw-yi, Jan Jinn-ke. Cryptanalysis of Log-in Authentication Based on Circle Property[J]. IEEE Transactions on Consumer Electronics, 2004, 50(2): 625-628.

[8] 万 涛, 马建峰. 基于几何方法的远程登录认证方案的密码分析[J]. 西安电子科技大学学报, 2003, 30(3): 378-380, 402.

[9] 李 颖, 刘金刚, 李锦涛. 远程登录几何认证方案的安全漏洞分析和解决办法[J]. 微电子学与计算机, 2003, 20(6): 46-50.

[10] 毛文波. 现代密码学理论与实践[M]. 北京: 电子工业出版社, 2004.

[11] Chor Leong-peng, Jing Hsu-wen, Chong Tan-peng. A Geometric Approach for Shared Secrets, a Refinement[J]. Computers & Security, 1998, 17(10): 725-732.