文章编号:1671-4598(2017)08-0241-03 DOI:10.16526/j.cnki.11—4762/tp.2017.08.062 中图分类号:TP309.2 文献标识码:A

网络信息安全中 DES 数据加密技术研究

赵 彩,丁 凰
(西安交通大学 城市学院计算机科学与信息管理系,西安 710018)

摘要:网络信息安全关系到数据存储安全和数据通信安全,为了提高网络信息安全管理能力,需要进行数据优化加密设计,提出一种基于前向纠错编码的 DES 数据公钥加密技术,采用 Gram—Schmidt 正交化向量量化方法构建 DES 数据的 Turbo 码模型,通过三次重传机制产生密文序列,对密文序列进行前向纠错编码设计,结合差分演化方法进行频数检验,实现网络信息安全中 DES 数据加密密钥构造,选择二进制编码的公钥加密方案有效抵抗密文攻击;仿真结果表明,采用该加密技术进行 DES 数据加密的抗攻击能力较强,密钥置乱性较好,具有很高的安全性和可行性。

关键词:网络信息安全;数据加密;编码;密文

Research on DES Data Encryption Technology in Network Information Security

Zhao Cai, Ding Huang
(Department of Computer Science and Information Management, Xi′an JiaoTong University City College, Xi′an 710018, China)

Abstract: Network information security related to the data storage security and data communication security, in order to improve the network information security management capabilities, the need for data encryption optimization design, this paper puts forward a DES public key data encryption technology based on forward error correction encoding before the construction of DES data using Gram—Schmidt orthogonal vector quantization method of Turbo code model to produce ciphertext sequence by the three retransmission mechanism, the ciphertext sequence of FEC encoding design, combined with the differential evolution method of frequency test, the realization of DES data encryption key structure in network information security, public key encryption scheme to choose binary encoding resist ciphertext attack. The simulation results show that the encryption technology used in DES data encryption has strong anti attack ability, good scrambling key, high security and feasibility.

Keywords: network information security; data encryption; coding; ciphertext

0 引言

网络信息技术的发展使得大量的信息数据通过网络实现云存储和传输通信,通过网络实现信息传输相比传统的光纤传输和有线数据传输更具有方便、快捷和低成本的优点,但由于网络传输的开放性和网络自组织性,网络信息安全形势不容可观,攻击者通过植入病毒和通过窃密的方法截取传输数据,严重影响了用户的信息安全[1]。因此,需要一种有效的数据加密技术,通过 DES 数据加密,通过设计网络安全协议,通过算术编码构造数字证书,增强数据传输的保密性能,研究 DES 数据加密技术在网络信息安全构造中具有重要的现实意义[2]。

由于 DES 数据组合结构简单,通常采用的是整数线性组合方案构建成一个单向函数,传统的加密密钥是一组线性无关向量的整数线性组合,导致对 DES 数据加密的难度较大,抗攻击性能不强,传统方法中,对 DES 数据加密技术主要有最短向量加密方案、单比特加密方案、身份验证加密方案和混沌保密通信加密方案等[3-4],上述方法通过对 DES 数据进行线性编码设计,采用广义隐写算法进行 DES 数据码元频数检测和链路层密钥设计,通过双线性映射机制构建加密数据的 Hash 函数,实现加密解密算法设计,具有一定的抗攻击能力,取得了一定的研究成果,其中,文献[5]中提出一种基于 DCT 变换与 DNA 运算相结合的加密技术,采用线性循环多径信道编码方法进行数字加密设计,采用比特序列调制方法进行随机性码元频数检测,降低了数据被破译的概率,但是该算法计算开销较大,影响了数字通信传输的实时性;文献[6]设计了一种分簇安全路由协议保密通信方法,采用 NTRUd 公钥加密进行无无线传感器网络信息通信中的分簇路由设计;文献[7]采用一种 TinySBSec 的轻量级 WSN 链路层加密算法,对 DES 数据通信中的隐写数据通同态数据融合和链路层重构方法进行对称加密和椭圆加密,提高了抗攻击能力,但上述方法存在的问题是抗干扰能力不强,密钥占据了比较大的资源空间。针对上述问题,本文提出一种基于前向纠错编码的 DES 数据公钥加密技术,采用 Gram—Schmidt 正交化向量量化方法构建 DES 数据的 Turbo 码模型,通过三次重传机制产生密文序列,对密文序列进行前向纠错编码设计,结合差分演化方法进行频数检验,实现网络信息安全中 DES 数据加密密钥构造,选择二进制编码的公钥加密方案有效抵抗密文攻击,实现加密算法改进设计,最后进行仿真实验分析,展示了本文方法在提高加密性能和抗攻击能力方面的优越性。

收稿日期:2017-03-03; **修回日期**:2017-03-26。

作者简介:赵 彩(1982-),女,甘肃陇西人,硕士研究生,讲师,主要从事数据挖掘方向的研究。

1 DES 数据的 Turbo 码模型与密钥方案

1.1 Turbo 码模型

为了实现网络信息安全中 DES 数据加密改进,首先采用 Gram—Schmidt 正交化向量量化方法构建 DES 数据的 Turbo 码模型,通过三次重传机制产生密文序列,采用驱动—响应式混沌模型增强序列密码的安全性,进行 DES 数据通信传输的

数字证书设计，在密钥序列的生成中采用链路层密钥流的向量量化方法，构建了二进制伪随机序列表达 DES 数据的 Turbo 码，进行密钥方案设计[8]。假设序列 $a_0a_1a_2\cdots a_n$ 和 $b_0b_1b_2\cdots b_n$ 是 n 位的 DES 数据二进制串，设 $G_1,,G_2$ 是阶为 p 的有向图模型，DES 数据序列密码的线性映射表示为 $e:G_1\times G_1\to G_2$，产生的密文为 c 的比特序列后，流密码体制集合 $p_0,\ldots,p_{l-1}$，在一个周期内，选择整数 $\Pi_{i,b}=\chi^{\Pi}_{i,b}-\delta^{\Pi}_{i,b}(1\leqslant i\leqslant\mu)$ 作为公钥元素个数，计算各游程中的基向量 $g_1=g^a,h=g^\beta$，将一个流密码的安全强度转化为 DES 数据传输的链路层加密序列检验问题[9]，假设有二进制序列 $a_0,a_1,a_2,\cdots$，通过加密序列检验生成一个素数集合 $\{p_{i,j}\}_{1\leqslant i,j\leqslant\mu}$，其中 $p_{i,j}$ 的大小为 η 位，用 $\{a_i\}$ 表示生成的 Turbo 码序列之间的周期序列，给出两个假设为：$H_1:\{0,1\}^*\to Z_q^*$，$H_0:\{0,1\}^*\to Z_q^*$。对二进制序列的每一位，存在任意 t 个 μ^2 位的明文向量 $\vec{m}_1,\ldots,\vec{m}_t$，当显著性水平 α 为 5%时，在给定显著性水平下，系统的输出码元为：$param=\{G_1,G_2,e,g,g_2,g_3,h,H_1,H_2\}$，通过三次重传机制产生密文序列，如图 1 所示。

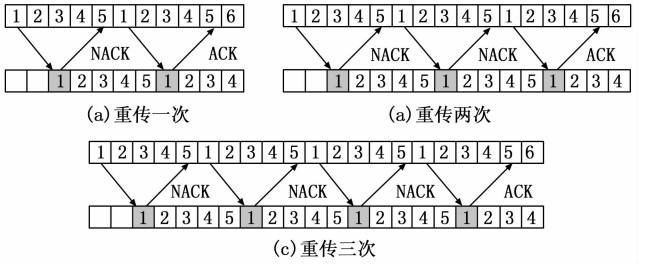

图 1 Turbo 编码三次重传机制

构建有向图 $G=(V,E)$ 进行链路重传设计，当存在一个标量 $k_{d,e}$，定义 $\Gamma_O(v)=\{e\in E\mid tail(e)=v\}$ 即节点 v 的输出编码特征矢量，$|\Gamma_I(v)|$ 为网络信息安全管理中心中协作传输节点 v 的入度。对 Turbo 码编码的向量量化函数 $C(x)=(c_{n-1}x^{n-1}+c_{n-2}x^{n-2}+\ldots+c_1x+c_0)$ 进行非线性时间序列重组，得到输出密钥 $mk=\{g_1,a,\beta\}$，计算 DES 数据加密链路层的有向统计量 rk_{ij}，令 $t_0=H_1(g,g_1,g_2,g_3,h)$，采用 Gram－Schmidt 正交化向量量化方法得到统计量 z 的计算公式为：

$$z=\frac{r-u_r}{\sigma_r}\sim N(0,1) \tag{1}$$

对序列随机性游程检验的公式：

$$y=z=\frac{r-u_r}{\sigma_r}=\frac{(lr-2n_0n_1-l)\sqrt{l-1}}{\sqrt{2n_0n_1(2n_0n_1-l)}} \tag{2}$$

通过 Turbo 码模型设计，在三次重传机制产生密文序列，构建驱动－响应模型，对密文序列进行前向纠错编码设计。

1.2 密钥方案构造

基于 Turbo 码模型结构进行 DES 数据加密密钥方案设计[10]，在密钥设计之前，给出如下定义：

1）$S^{n-1}=\{x\in R^n:\|x\|=1\}$ 定义为链路层块内 DES 数据单位范围（unit sphere）；

2）v 表示一个 n 维的向量；

3）$\|v\|=[v,v]^{1/2}$ 为链路层重加密钥的欧式距离；

4）$H_i(u)=\{x\in R^n:[x,u]=i\}$ 是游程总数，其中 $i\in Z^+,u\in S^{n-1}$；

5）A 是实数域 R^n 的一个子空间，且满足二维均匀分布：

$$A^{\perp}=\{x\in R^n:[x,v]=0,\forall v\in A\} \tag{3}$$

6）假设 $\{v_1,v_2,\cdots,v_m\}$ 是数据点的链距离分布的基向量，这组基向量的稀疏特征定义如下：

$$span(v_1,v_2,\cdots,v_m)=\{[v_1,v_2,\cdots,v_m]x:x\in R^n\} \tag{4}$$

根据上述定义，基于密度相似邻居检验方法得到相似 k 距离邻居序列，对于任意一组向量 $v_1,v_2,\cdots,v_m$，对象 p 的第 k 距离满足 $dist(p,o')\leqslant dist(p,o)$，正交化向量 $v_1{}^*,v_2{}^*,\cdots,v_m{}^*$ 定义如下：

$$\begin{aligned}v_i{}^*&=v_i-\sum_{j=1}^{i-1}\mu_{i,j}v_j{}^*\\ v_1{}^*&=v_1\end{aligned} \tag{5}$$

其中：$i=1,\cdots,m,\mu_{i,j}=\dfrac{<v_i,v_j^*>}{<v_j^*,v_j^*>}$

根据上述定义，密钥生成方案构造如下：

DES 数据加密的明文序列：$m=m_1m_2m_3\cdots$；

各游程中的密钥序列：$z=z_1z_2z_3\cdots$；

一个周期内 0 与 1 的数目各占 $N/2$，生产的密文序列：$c=c_1c_2c_3\cdots$；

对二进制序列的加密序列进行向量量化分解，得到加密变换：$c_i=E(z_i,m_i)(i=1,2,3,\cdots)$；

密钥构造的解密变换：$m_i=D(z_i,c_i)(i=1,2,3,\cdots)$；

计算 $C_1=MY^s$，输入用户私钥 SK_L，更新存储密文 ck，计算私钥 SK_L，初始化序列 ck，对应 ck_i 值不为 1 的属性集合 β，即通过解密运算可译得 DES 数据明文为：

$$m_i=D(z_i,E(z_i,m_i))=m_1m_2m_3\cdots(i=1,2,3,\cdots) \tag{6}$$

通过上述密钥构造，完成 DES 数据的一次密码通信。

2 加密算法优化设计

2.1 前向纠错编码设计

在上述进行了 DES 数据的 Turbo 码模型与密钥方案构造的基础上，进行 DES 数据加密算法优化设计，本文提出一种基于前向纠错编码的 DES 数据公钥加密技术，对密文序列进行前向纠错编码设计，利用加密数据在授权中心的密钥差异性保存信源参数（ser,MSK），利用隐私保护中的密钥生成的信道特征，计算得出密钥的各态历经荷载 $T_{i,j}=g^{t_{i,j}}(i\in[1,n],j\in[1,n_i])$ 和 $Y=e(g,h)^y$，在系统应用支撑层输出的加密数据的素数集合 $p_0,\ldots,p_{l-1}$，其中 p_i 为 DES 数据在序列位串上的位移，用 π 表示二进制序列 $a_0,a_1,a_2,\cdots$ 矢量乘积。定义频数检验的显著性水平为 $x_0=q_0*\pi$，其中 q_0 满足：$q_0\leftarrow\bigcap[0,2^\gamma/\pi)$，当二进制序列的每一位的频数小于 2^{λ^2}，用 0 和 1 分布进行前向纠错，在加密过程中通过连贯性检验或串检验，在分布区间 $\bigcap[0,q_0)$ 内，得到前向纠错三次重传的密钥为 $b=(b_{i,j})_{0\leqslant i,j\leqslant\beta}\in(-2^\alpha,2^\alpha)^{\beta\times\beta}$ 和 $b=(b'_{i,j})_{1\leqslant i,j\leqslant\mu}\in(-2^{\alpha'},2^{\alpha'})^{\mu\times\mu}$，加密数据独立分布在整数 x_i、x'_i 和 Π_i 中，当 $0\leqslant j\leqslant l-1$ 时，序列中出现 00、01、10 码元的频数满足：

当 $1\leqslant i\leqslant\tau$ 时，Cai－Cusick 公钥加密的比特率 $x_i\bmod p_j=2r_{i,j}$，其中 $r_{i,j}\leftarrow z\bigcap(-2^{\varphi'-1},2^{\varphi'-1})$；

当 $0\leqslant i\leqslant l-1$ 时，加密密钥随机选择一个向量 u 比特率 $x'_i\bmod p_j=2r'_{i,j}+\delta_{i,j}$，其中 $r'_{i,j}\leftarrow z\bigcap(-2^\varphi,2\varphi)$；

当 $0\leqslant i\leqslant l-1$ 时，明文块从单位范围 $S^{n-1}=\{x\in^n:\|x\|=1\}$ 中随机选择公钥 $\Pi_i\bmod p_j=2\bar{\omega}_{i,j}+\delta_{i,j}\cdot2^{\varphi'+1}$ 作为要加密的密文，其中第 $l+1$ 层的密文 $\bar{\omega}_{i,j}\leftarrow\bigcap(-2^\varphi,2^\varphi)$。解密公

钥 $pk=[x_0,(x_i)_{0\leqslant i\leqslant\tau},(x'_i)_{0\leqslant i\leqslant l-1},(\Pi_i)_{0\leqslant i\leqslant l-1}]$，解密私钥 $sk=(p_j)_{0\leqslant j\leqslant l-1}$。

综上分析，得到 DES 数据加密前向纠错编码过程为：Encrypt $(pk,m\in\{0,1\}^l)$，要想解密密文 C，需将公钥元素进行量化分解[11]，并从攻击者出获得唯密文攻击的密钥，在前向纠错编码向量 $b=(b_i)_{1\leqslant i\leqslant\tau}\in(-2^{\alpha},2^{\alpha})^{\tau}$ 和 $b=(b'_i)_{0\leqslant i\leqslant l-1}\in(-2^{\alpha'},2^{\alpha'})^{l}$ 中进行二次重传，采用 Pan－Deng 唯密文方案，计算密文 $c=\left[\sum_{i=0}^{l-1}m_i\cdot x'_i+\sum_{i=0}^{l-1}b'_i\cdot\Pi_i+\sum_{i=1}^{\tau}b_i\cdot x_i\right]_{x_0}$，以此为基础进行加密改进设计。

2.2　DES 数据公钥加密方案

结合差分演化方法进行频数检验，采用 Turbo 编码数据分组，假设 $(a_0,a_1,\cdots,a_m)$ 是密文 C 中需要恢复的消息，DES 数据的 Turbo 码分布的特征向量 $\chi'_{i,b}$ 和 $\chi^{\Pi}_{i,b}$，频数检验的过程描述为：

1）先在物理层输入 DES 数据标签索引位置，为 $x_{i,b}=\chi_{i,b}-\delta_{i,b}(1\leqslant i\leqslant\beta)$，设用户（或敌手）的密钥参数 $\delta_{i,b}=[\chi_{i,b}]_{\pi}+\xi_{i,b}\cdot\pi-CRT_{p_{m,n}}(2r_{i,b,m,n})_{1\leqslant m,n\leqslant\mu},r_{i,b,m,n}\leftarrow Z\cap(-2^{\varphi'-1},2^{\varphi'-1}),\xi_{i,b}\leftarrow Z\cap[0,2^{\lambda+\log_2(\mu^2)+\mu^2}\cdot\eta/\pi)$。

2）在前向纠错方案下，$x'_{i,b}=\chi'_{i,b}-\delta'_{i,b}(1\leqslant i\leqslant\mu)$，加密方案操作符 $\delta'_{i,b}=[\chi'_{i,b}]_{\pi}+\xi'_{i,b}\cdot\pi-CRT_{p_{m,n}}(2r'_{i,b,m,n})_{1\leqslant m,n\leqslant\mu},r'_{i,b,m,n}\leftarrow Z\cap(-2^{\omega},2^{\omega})$，运行 $Gen(1^k)$ 生成密钥 $K\,\xi'_{i,b}\leftarrow Z\cap[0,2^{\lambda+\log_2(\mu^2)+\mu^2}\cdot\eta/\pi)$。

3）当查询令牌满足 $\Pi_{i,b}=\chi^{\Pi}_{i,b}-\delta^{\Pi}_{i,b}\upsilon$，输出频数检测结果 $\delta^{\Pi}_{i,b}=[\chi^{\Pi}_{i,b}]_{\pi}+\xi^{\Pi}_{i,b}\cdot\pi-CRT_{p_{m,n}}(2\bar{\omega}_{i,b,m,n}+\delta_{i,b,m,n}\cdot 2^{\omega'+1})_{1\leqslant m,n\leqslant\mu},\bar{\omega}_{i,b,m,n}\leftarrow Z\cap(-2^{\varphi},2^{\varphi}),\xi^{\Pi}_{i,b,m,n}\leftarrow Z\cap[0,2^{\lambda+2\log_2(\mu)+\mu^2}\cdot\eta/\pi)$。

结合差分演化方法进行频数检验，采用二进制编码得到加密密钥构造目标函数为：

$$x=(x_1,x_2,\cdots,x_m)\in X \tag{7}$$

差分演化的变异操作抽象为：

$$y=f(x)=(f_1(x),f_2(x),\cdots,f_n(x))\in Y \tag{8}$$

其中：x 是标准的频数检验向量；X 是游程检验函数；y 是游程总数；Y 是目标空间。对于所有的 $1\leqslant i,j\leqslant\mu$，使用二进制编码的公钥加密方案，得到 DES 数据的加密可靠性判断方式如下：

$$X_{ij}(t+1)=\begin{cases}V_{ij}(t+1),f(V_{ij}(t+1))<f(X_{ij}(t))\\X_{ij}(t),otherwise\end{cases} \tag{9}$$

加密的可靠性问题演化为一个多目标优化问题中，选取序列密码有 $c\bmod p_{i,j}=C^{\gamma}(c_1,\ldots,c_t)\bmod p_{i,j}=C^{\gamma}(c_1\bmod p_{i,j},\ldots,c_t\bmod p_{i,j})\bmod p_{i,j}$，DES 数据加密的抗攻击度计算得到 $|C^{\gamma}(c_1\bmod p_{i,j},\ldots,c_t\bmod p_{i,j})|\leqslant 2^{\eta-4}\leqslant p_{i,j}/8$，输出密文的置乱度 $C^{\gamma}(c_1\bmod p_{i,j},\ldots,c_1\bmod p_{i,j})\bmod p_{i,j}=C^{\gamma}(c_1\bmod p_{i,j},\ldots,c_1\bmod p_{i,j})$，根据算法改进，得到加密算法的输入输出过程描述为：

Decrypt（sk，c）：输出信源编码 $m=(m_0,\ldots,m_{l-1})$ 其中 $m_j\leftarrow[c]_{p_j}\bmod 2$。

Add（pk,c_1,c_2）：公钥回传链路层，输出 $c_1+c_2\bmod x_0$。

Mult（pk,c_1,c_2）：数据传输的 Turbo 码采样输出 $c_1\cdot c_2\bmod x_0$，密文 $c^*=\left[\sum_{1\leqslant i,j\leqslant\mu}m_{i,j}\cdot x'_{i,0}\cdot x'_{j,1}+\sum_{1\leqslant i,j\leqslant\mu}b'_{i,j}\cdot\Pi_{i,0}\cdot\Pi_{j,1}+\sum_{1\leqslant i,j\leqslant\beta}b_{i,j}\cdot x_{i,0}\cdot x_{j,1}\right]_{x_0}$。

3　仿真实验分析

为了测试本文算法在实现 DES 数据加密中的性能，进行仿真实验，实验采用 Matlab 仿真软件编程设计，实验的硬件环境为：CPU Inter Pentium 4，内存 2.0 GHz 的 PC 机，数据的采样频率为 1.954 Hz，生成 Turbo 码间隔为 100 Hz，其它参数配置检表 1。

表 1　实验参数设置

参数设置	t_{max}	M	l	p_m	p_c
参数值	1024	80	220	0.025	0.15

根据上述数据加密仿真环境和参数设定，进行数据，首先给出原始的 DES 数据序列描述如下：

DES 数据序列 1：

10110100011001110011000110001110110000111111010000100111101101111111111111000111001100111000111000011100010001100111100010100111001011110101010010110111111001100000101011010101010110011

DES 数据序列 2：

10111001110101011011000110100011000100001010111000100010001000010011100010001110001001001000000110010000010001011101101001011001001011010111000101010011101001010100100000011001101

输出序列密码 1：

11010110101001101111010101010110001101100010001010101010101001010011010010101010100001000010101010101010100001000100100001010010010100101010101010010110010101010101010100011

输出序列密码 2：

01010101010011010101001001010101010101001001001001010001010010101010101010010101001001010010100101010101010101001010011100101101010101010010100010010100100001

分析上述输入数据和输出密码序列对比得知，采用本文方法进行数据加密，输出密码具有较好的置乱性，能有效提高明文攻击，表 2 给出了上述两组密码序列的统计分析结果。

表 2　密码序列结果统计分析

检测参数	序列 1	序列 2
0 的频数 n_0	134	112
1 的频数 n_1	132	132
00 的频数 n_{00}	68	68
01 的频数 n_{01}	65	43
10 的频数 n_{10}	42	58
11 的频数 n_{11}	64	72
游程总数 r	245	543
频数检验值 y_1	4.5648e－03	1.5443e－02
序列检验值 y_2	1.6432	2.0121
游程检验值 y_3	1.4223	1.2212

（下转第 247 页）

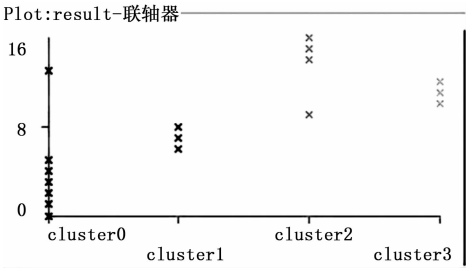

图 4　聚类结果

出，只要样本的属性间关系明确，便可以学习到准确率很高的聚类中心及结果。

4　结束语

在知识经济逐渐兴起，信息技术飞速发展，商业竞争日益加剧的背景下，知识管理得到越来越多企业的重视。为了解决知识管理中出现各种信息通信和知识共享问题，原本用于语义 Web 的本体论也被引入到知识管理中。

本文针对目前知识管理中本体特别是中文本体构建自动化程度低以及重用度低的问题，结合企业生产应用，提出了多分类支持向量机的本体设计方法和 K－均值聚类的本体设计方法流程，分析了支持向量机及统计学的基本原理与应用与 K－均值的基本原理与应用，实现了基于类间相对分类度的概念分类和基于类间相对分类度的概念聚类，并在此基础上，构建了本体关系框架，验证了方法的可行性。

参考文献：

[1] 李兴春. 计算机信息检索中的本体构建研究 [J]. 重庆文理学院学报，2013，3：87－91.

[2] 张　娟. 基于本体的可重构知识管理系统研究综述 [J]. 现代商贸工业，2009，21 (19)：59－60.

[3] 张　祥，李　星，温韵清，等. 语义网虚拟本体构建 [J]. 东南大学学报：自然科学版，2015，4：652－656.

[4] Dibike Y B，Solomatine D，Velickov S，et al. Model Induction with Support Vector Machines：Introduction and Applications [J]. Journal of Computing in Civil Engineering，2014，15 (3)：208－216.

[5] Ren H，Tian J，Wierzbicki A P，et al. Ontology Construction and Its Applications in Local Research Communities，Modeling for Decision Support in Network－Based Services [M]. Springer Berlin Heidelberg，2012：279－317.

[6] Xue S，Jing X，Sun S，et al. Binary－decision－tree－based multiclass Support Vector Machines [A]. 2014 14th International Symposium on Communications and Information Technologies (ISCIT) [C]. IEEE，2014：85－89.

[7] 任维武，胡　亮，赵　阔. 基于数据挖掘和本体的入侵警报关联模型 [J]. 吉林大学学报 (工学版)，2015 (3)：899－906.

[8] Balabantaray R C，Sarma C，Jha M. Document Clustering using K－Means and K－Medoids [J]. International Journal of Knowledge Based Computer System，2015，1 (1).

(上接第 243 页)

统计结果分析可以看出，采用本文方法进行数据加密设计，能更好地满足频数检验的要求，提高加密性能。图 2 给出了采用不同方法进行数据加密的抗攻击性效能对比，分析图 2 结果得知，采用本文方法进行 DES 数据加密，抗攻击能力较强，性能优于传统模型。

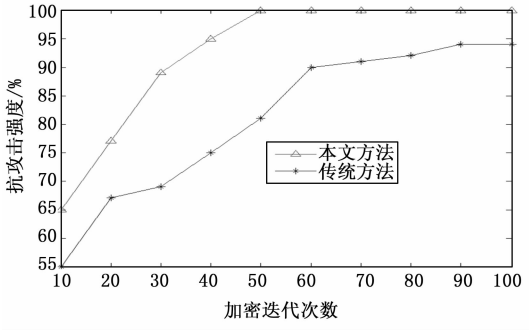

图 2　加密抗攻击性能对比

4　结束语

本文提出一种基于前向纠错编码的 DES 数据公钥加密技术，采用 Gram－Schmidt 正交化向量量化方法构建 DES 数据的 Turbo 码模型，通过三次重传机制产生密文序列，对密文序列进行前向纠错编码设计，结合差分演化方法进行频数检验，实现网络信息安全中 DES 数据加密密钥构造，选择二进制编码的公钥加密方案有效抵抗密文攻击。通过加密算法设计和实验分析表明，采用该加密技术进行 DES 数据加密的抗攻击能力较强，密钥置乱性较好，具有很高的安全性和实用价值。

参考文献：

[1] 林如磊，王　箭，杜　贺. 整数上的全同态加密方案的改进 [J]. 计算机应用研究，2013，30 (5)：1515－1519.

[2] 刘乐柱，张季谦，许贵霞，等. 一种基于混沌系统部分序列参数辨识的混沌保密通信方法 [J]. 物理学报，2014，13 (1)：010501.

[3] Lin Y P，Vaidyanathan P P. Theory and design of two－dimensional filter bank：A review [J]. Multidimensional System & Signal Processing，1996，7 (3)：263－330.

[4] Suzukit，Kudo H. Two－dimensional non－separable block－lifting structure and its application to M－channel perfect reconstruction filter banks for lossy－to－lossless image coding [J]. IEEE Transactions on Image Processing，2015，24 (12)：4943－4951.

[5] 徐光宪，徐山强，郭晓娟，等. DCT 变换与 DNA 运算相结合的图像压缩加密算法 [J]. 激光技术，2015，39 (6)：806－810.

[6] 龙昭华，龚　俊，王　波，等. 无线传感器网络中分簇安全路由协议保密通信方法的能效研究 [J]. 电子与信息学报，2015，37 (8)：2000－2006.

[7] 白恩健，朱俊杰. TinySBSec—新型轻量级 WSN 链路层加密算法 [J]. 哈尔滨工程大学学报，2014，35 (2)：1－6.

[8] 汤殿华，祝世雄，曹云飞. 一个较快速的整数上的全同态加密方案 [J]. 计算机工程与应用，2012，18 (28)：117－122

[9] 秦　怡，吕晓东，巩　琼，等. 利用附加密钥旋转在光学联合相关结构中实现多二值图像加密 [J]. 光学学报，2013，33 (3)：7－9.

[10] Shen L，Sun G，Huang Q，et al. Multi－level discriminative dictionary learning with application to large scale image classification [J]. IEEE Transactions on Image Processing，2015，24 (10)：3109－3123.

[11] Thiagarajan J J，Ramamurthy K N，Spanlas A. Learning stable multilevel dictionaries for space representations [J]. IEEE Transactions on Neural Networks & Learning Systems，2015，26 (9)：1913－1926.