

云存储平台下基于混沌映射的数据加密算法设计

陈建辉¹, 赵 静²

(1 郑州航空工业管理学院 计算机学院, 河南 郑州 450015;

2 郑州航空工业管理学院 信息科学学院, 河南 郑州 450015)

摘 要: 提出一种基于混沌映射的云存储平台数据加密算法. 采用混沌敏感性特征表征方法进行云存储平台大数据的非结构化重组设计, 在非结构化特征分布空间中进行云数据的同态变换和关联映射对应, 构建云数据的混沌编码密钥, 采用码元自适应配对方法进行数据密钥的循环扩展, 根据明文攻击的强度, 在有限域中构建云存储平台加密的编码协议, 采用分段线性编码方法实现云平台下的存储数据算术编码和循环加密. 仿真结果表明, 采用该方法进行数据加密, 能提高云存储平台数据的抗攻击能力, 数据的隐写性能较好, 具有很好的加密存储性能.

关键词: 云存储平台; 混沌映射; 数据加密; 密钥; 明文攻击

中图分类号: TP309.7

文献标识码: A

文章编号: 1000-7180(2018)07-0127-06

Design of Data Encryption Algorithm Based on Chaotic Mapping in Cloud Storage Platform

CHEN Jian-hui¹, ZHAO Jing²

(1 School of Computer, Zhengzhou University of Aeronautics, Zhengzhou 450015, China;

2 School of Information Science, Zhengzhou University of Aeronautics, Zhengzhou 450015, China)

Abstract: A cloud storage platform data encryption algorithm based on chaotic mapping is proposed. The chaotic sensitivity feature representation method is used to design the unstructured reconfiguration of cloud storage platform big data. The homomorphism transformation and correlation mapping of cloud data are carried out in the unstructured feature distribution space, and the chaotic coding key of cloud data is constructed. The cyclic expansion of data key is carried out by means of symbol adaptive pairing method. According to the intensity of plaintext attack, the encoder protocol of cloud storage platform encryption is constructed in finite domain. The arithmetic coding and cyclic encryption of stored data on cloud platform are realized by piecewise linear coding method. The simulation results show that this method can improve the anti-attack ability of cloud storage platform data, the steganography performance of data is better, and the data encryption storage performance is good.

Key words: cloud storage platform; chaotic mapping; data encryption; key; plaintext attack

1 引言

在网络信息化时代, 云存储信息的安全关系到用户的隐私保护和整个网络信息系统的安全, 对云存储数据的安全管理的关键环节在于数据加密, 通过对云存储平台下的结构化数据加密设计, 确保信息安全^[1].

传统方法中, 对云存储数据的加密方法主要有椭圆加密方法、ECC 加密方法、分段 NTRUd 公钥加密方法等^[2,3], 通过加密密钥设计和码元组合设计, 采用编码和密钥转换方法, 实现数据的加密和解密. 根据上述原理, 相关文献进行数据加密算法研究, 其中, 文献[4]中提出一种基于椭圆曲线密码体制(Elliptic Curve Cryptography, ECC)的云存储平

台加密技术,在有限域中构建云存储平台加密的椭圆曲线方程,对加密数据线性分段编码,设计加密解密密钥进行云存储平台数据加密,提高加密数据的抗攻击能力,该方法在数据加密中存在计算开销过大和实时加密性能不好的问题,文献[5]中提出一种基于奇异值有限域填充加密的云存储平台数据量化编码算法,将公钥嵌入到主密钥分布的有限域中,填充密钥中心的敏感域参数,实现云存储平台的大数据加密,该方法需要大量的先验数据作为测试集,导致数据加密的抗攻击能力不好,文献[6]中提出基于多次重传机制的云存储平台的自适应线性加密方法,采用 MIMO 混合预编码方法构建混沌加密系统,实现数据分段加密,提高加密的实时性,该方法同样存在加密的抗干扰性不好和敏感性较大等问题。

针对上述问题,本文提出一种基于混沌映射的云存储平台数据加密算法。首先进行云存储平台下的数据结构分析,进行数据的混沌敏感性表征和混沌编码设计,构建数据加密密钥,结合明文攻击的信息熵特征进行加密算法优化,然后进行加密编码协议设计,最后进行数据加密算法设计,展示了本文方法在提高数据加密性能方面的优越性。

2 云存储平台大数据加密数学模型和特征分析

2.1 云存储平台大数据的非结构化重组

为了实现对云存储平台的数据加密设计,首先采用混沌敏感性特征表征方法进行云存储平台大数据的非结构化重组设计,在有限域中构建云存储平台加密的椭圆函数为 $Decrypt(sk, c^*)A^{-1} = T = (t_{i,j})_{i,j=1}^m$,采用循环密钥配对方法进行数据加密的结构化特征分解^[7],得到数据加密密钥的特征分解式为:

$$Decrypt(sk, c^*)A^{-1}A = \begin{bmatrix} t_{1,1} & \cdots & t_{1,m} \\ \vdots & \ddots & \vdots \\ t_{m,1} & \cdots & t_{m,m} \end{bmatrix} \begin{bmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,m} \end{bmatrix} \quad (1)$$

对云存储平台中的未加密数据采用随机性插值方法进行密钥扩展,将信息熵与方差作为加密的同态编码变量^[8],进行云存储平台大数据的非结构化重组,得到云存储大数据的扩展密钥:

$$Decrypt(sk, c^*)A^{-1}A = \begin{bmatrix} \alpha_1^{-1}t_{1,1} & \cdots & \alpha_1^{-1}t_{1,m} \\ \vdots & \ddots & \vdots \\ \alpha_m^{-1}t_{m,1} & \cdots & \alpha_m^{-1}t_{m,m} \end{bmatrix} \begin{bmatrix} \alpha_1 a_{1,1} & \cdots & \alpha_m a_{1,m} \\ \vdots & \ddots & \vdots \\ \alpha_1 a_{m,1} & \cdots & \alpha_m a_{m,m} \end{bmatrix} = E \quad (2)$$

定义待加密的云数据的长度为 n ,服从于标准正态分布函数,密钥扩展序列 $X = x_1, x_2, \dots, x_n$,并统计加密比特序列 X 的二项式和 $S_n = x_1 + x_2 + \dots + x_n$,采用椭圆曲线和混沌特征映射方法^[9],得到加密数据的特征重组输出为:

$$Decrypt(sk, c^*)AA^{-1} = \begin{bmatrix} t_{1,1} & \cdots & t_{1,m} \\ \vdots & \ddots & \vdots \\ t_{m,1} & \cdots & t_{m,m} \end{bmatrix} = E \quad (3)$$

采用码元频数检测方法,进行混沌加密数据的随机线性处理,构建 *Hash* 函数得到公钥加密明序列为:

$$Decrypt(sk, c^*)A^{(\alpha_1, \dots, \alpha_m)}Decrypt(sk, c^*)A^{-1}A = \begin{bmatrix} \alpha_1 a_{1,1} & \cdots & \alpha_m a_{1,m} \\ \vdots & \ddots & \vdots \\ \alpha_1 a_{m,1} & \cdots & \alpha_m a_{m,m} \end{bmatrix} \begin{bmatrix} \alpha_1^{-1}t_{1,1} & \cdots & \alpha_1^{-1}t_{1,m} \\ \vdots & \ddots & \vdots \\ \alpha_m^{-1}t_{m,1} & \cdots & \alpha_m^{-1}t_{m,m} \end{bmatrix} = E \quad (4)$$

计算码元频数的均匀分布值 $e = h(m)$,采用单比特检测方法得到云存储平台下大数据编码的二值化向量量化特征方程为:

$$Decrypt(sk, c^*)A^{(\alpha_1, \dots, \alpha_m)}A^{-1} = \begin{bmatrix} \alpha_1^{-1}t_{1,1} & \cdots & \alpha_1^{-1}t_{1,m} \\ \vdots & \ddots & \vdots \\ \alpha_m^{-1}t_{m,1} & \cdots & \alpha_m^{-1}t_{m,m} \end{bmatrix} = (A^{-1})A^{(\alpha_1^{-1}, \dots, \alpha_m^{-1})^T} \quad (5)$$

根据加密编码元素的比特长度,进行大数据加密的混沌映射对应^[10],得到云存储平台大数据的非结构化重组模型如图 1 所示。

2.2 加密数据的混沌敏感性表征

为了提高数据加密的抗攻击能力,需要采用混沌映射方法进行云存储大数据的敏感性表征,根据表征结果进行特征变换和编码设计,给出加密的比特序列 $s = \{s_i, i = 1 \cdots M \mid s_i \in S\}$,输入混沌初始敏感性参数 k ,采用对称 *Hash* 函数进行混沌加密的分段映射设计^[11],算法描述为:

$$C \rightarrow S; Certificate\{Cert_c\}$$

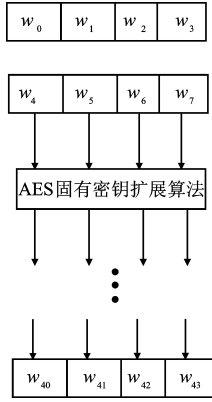


图 1 云存储平台大数据的非结构化重组

$C \rightarrow S: \text{ClientKeyExchange}\{K_c\}$

$C \rightarrow S: \text{CertificateVerify}\{\{\text{hash}(\text{messages})\}_{P_{c-1}}\}$

采用混沌映射密码体制构建云存储平台的结构化数据加密的分段线性混沌映射方程为:

$$f(x) = \begin{cases} x/p, & x \in [0, p) \\ (1-x)/p, & x \in [p, 1] \end{cases} \quad (6)$$

通过参数 p 来调整加密密钥对混沌初始值的敏感性,当 $p = 0.5$ 时,混沌映射为 Logistics 映射^[12],采用 Logistics 混沌映射进行云存储大数据的分段编码,输出码元个数为 n 的信源 $E = \epsilon_1, \epsilon_2, \dots, \epsilon_n$,根据混沌编码中每个符号出现的概率进行椭圆线性变换 $x_i = 2\epsilon_i - 1$,以 0 和 1 表示编码输出的码元频次,在混沌映射表征下,得到加密混沌比特序列 $X = x_1, x_2, \dots, x_n$ 的统计特征量 X 的二项式为 $S_n = x_1 + x_2 + \dots + x_n$,采用二值分离方法进行加密大数据的关联规则特征提取,得到关联规则特征量 S_n 的极值点 $\frac{S_n}{\sqrt{n}}$,取参数密钥 E 的一点 G ,混沌初始值 $\frac{S_n}{\sqrt{n}}$ 接近于标准的正态分布函数,结合混沌编码与加密之间的自相关性,进行编码映射图构建,当满足

$\lim_{n \rightarrow \infty} P\left(\frac{S_n}{\sqrt{n}} \leq z\right) = \varphi(z) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^z e^{-u^2/2} du$,得到输出混沌加密的自相关统计特征量为 $S_{obs} = \frac{|S_n|}{\sqrt{n}}$,根据 Logistic 映射的正态分布特性,得到加密输出的关联映射收敛于:

$$\begin{aligned} \lim_{n \rightarrow \infty} P\left(S_{obs} = \frac{|S_n|}{\sqrt{n}} \leq z\right) \\ = 1 - \frac{1}{\sqrt{2\pi}} \left(\int_{-\infty}^{-z} e^{-u^2/2} du + \int_z^{+\infty} e^{-u^2/2} du \right) \\ = 2\varphi(z) - 1 \end{aligned} \quad (7)$$

在非结构化特征分布空间中进行云数据的同态变换和关联映射对应,进行云存储平台的结构化数据加密,数据加密由 4 个算法组成: Setup, Extract, Encrypt 和 Decrypt,采用码元自适应配对方法进行数据密钥的循环扩展,进行数据加密和编码设计。

3 数据加密算法改进

3.1 混沌编码密钥设计

在采用混沌敏感性特征表征方法进行云存储平台大数据的非结构化重组设计的基础上,进行数据加密算法改进设计,本文提出基于混沌映射的云存储平台结构化数据加密算法。采用混沌映射结构重组移位密钥构建数据加密的统计量 P-value 为:

$$\begin{aligned} P\text{-value} &= 2[1 - \varphi(S_{obs})] \\ &= 2\left(1 - \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{S_{obs}} e^{-u^2/2} du\right) \\ &= \frac{2}{\sqrt{2\pi}} \int_{S_{obs}}^{+\infty} e^{-u^2/2} du \\ &= \frac{2}{\sqrt{\pi}} \int_{\frac{S_{obs}}{\sqrt{2}}}^{+\infty} e^{-t^2} dt \\ &= \text{erfc}\left(\frac{S_{obs}}{\sqrt{2}}\right) \end{aligned} \quad (8)$$

若统计量 $P\text{-value} \geq 0.01$,循环移位方向 $KS \in \{0, 1\}$ 为 1 位得到编码映射图^[13],密钥存储空间为 K 比特,在明文的累积概率区间内,得到线性编码的反函数:

$$f^{-1}(I) = \begin{cases} p * I, & s = "0" \\ 1 - (1 - p) * I, & s = "1" \end{cases} \quad (9)$$

式中, I 表示云存储平台的加密数据明文攻击的初始分布区间,设定初始值 $I = [0, 1]$,随着加密编码的明文数的增多,将明文分成 N 个块,采用分块加密方法^[14],得到输出加密编码的表达式为:

$$f(x) = \begin{cases} x/P_1, & x \in I_1 \\ (x - P_1)/P_2, & x \in I_2 \\ \dots\dots\dots & \dots\dots\dots \\ (x - \sum_{i=1}^{n-1} P_i)/P_n, & x \in I_n \end{cases} \quad (10)$$

式中, $P_i (i = 1, \dots, n)$ 表示混沌序列的区间分布概率,在区间 I_i 中进行混沌序列的随机化处理,在明文序列的循环窗口内,构建混沌编码密钥时隙满足:

$$\begin{cases} KC_1 = KC_1 \oplus \{t_j, t_{j+1}, t_{j+2}, \dots, t_{j+m-2}\} \\ KS_1 = KS_1 \oplus \{t_{j+m-2}\} \end{cases} \quad (11)$$

式中, $j = r \bmod 128$, 对 $f(x)$ 取反函数为:

$$f^{-1}(x) = \begin{cases} P_1 x \\ P_2 x + P_1 \\ \dots\dots \\ P_n x + \sum_{i=1}^{n-1} P_i \end{cases} \quad (12)$$

读取密文序列, 在密钥的特征分布空间, 采用码元自适应配对方法进行数据密钥的循环扩展, 实现混沌编码密钥设计, 这一实现的过程如图 2 所示.

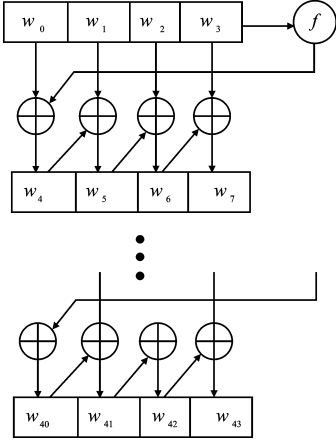


图 2 混沌密钥编码设计

3.2 云存储数据算术编码和循环加密

采用码元自适应配对方法进行数据密钥的循环扩展, 得到混沌映射加密的平均互信息函数为:

$$H = - \sum_{i=1}^n P_i \log_2(P_i) \quad (13)$$

在标准算术编码体系下, 云存储数据的编码序列 $s = \{s_i, i = 1, \dots, M \mid s_i \in S\}$ 的信息熵计算为:

$$P_n = \frac{1}{M} \text{card} \{s_i \mid s_i = S_n\} \quad (14)$$

式中, $S_n \in S, n = 1, \dots, N$, 结合分块密文编码方法, 得到数据加密的扩展密钥 $x = (x_1, \dots, x_m)^T \in \text{GF}(2^n)^m$, 通过密钥映射, 输出密钥的信息参量和长度分别为:

$$I^i = f^{-1}(x)(I^{i+1}) \quad (15)$$

$$\text{size}(I^i) = P_i \text{size}(I^{i+1}) \quad (16)$$

采用替代数据法进行循环加密^[15], 加密比特序列的长度:

$$\begin{aligned} \text{size}(I^1) &= \prod_{i=1}^M P(s_i \in S) \\ &= \prod_{n=1}^N (P_n)^{\text{card} \{s_i \mid s_i = S_n\}} \\ &= \prod_{n=1}^N (P_n)^{P_n M} \end{aligned} \quad (17)$$

对每个加密编码求逆:

$$-\log_2(\text{size}(I^1)) = - \sum_{n=1}^N P_n M \log_2(P_n) = \lceil K/m \rceil \quad (18)$$

在有限域中构建云存储平台加密的编码协议为^[16]:

• RkeyGen($param, rsk_{ID_i}, ID_i, ID_j$), 分组密码的组合序列 $x_1 x_2 x_3 \dots x_r$, 根据 SP800-22 rev1a 标准协议进行云存储编码, 得到第 N 个加密比特序列的公钥 $k_i, l_i \in Z_q^*$. 设置安全参数进行加密码元频次控制, 输出密钥 rk_{ij} , 令 $t_0 = H_1(g, g_1, g_2, g_3, h)$, 得到云存储平台数据加密的输出编码序列:

$$(rk_{1ij}, rk_{2ij}, rk_{3ij}, rk_{4ij}, rk_{5ij}, rk_{6ij}) = (g^{x_i k_i}, (g^{t_0} h)^{x_i k_i}, \frac{x_i}{x_i}, sr_{x_i}^{-1}(t_0 - t_i) sr_{x_i}^{-1}(t_i - t_0), k, g^{k_i}) \quad (19)$$

采用混沌敏感性表征和信息熵定位方法, 构建数据加密的隐写协议为:

C →

S: ClientHello{Ver_c, CipherSuite_c, R_c, SessionID}

S →

C: ServerHello{Ver_s, CipherSuite_s, R_s, SessionID}

解密算法为:

Decrypt(sk, c^*, z): 加密码文比特块 q_0 , 当满足 $q_0 \leftarrow Z \cap [0, 2^r/\pi)$, 密文空间输出的隐写密钥 $\vec{m} = (m_{i,j})$, 输出特征集: $param = \{G_1, G_2, e, g, g_2, g_3, h, H_1, H_2\}$,

综上算法设计, 实现云储存平台下的混沌映射数据加密, 加密算法的实现流程图如图 3 所示.

4 仿真实验与加密性能分析

为了测试本文方法在实现云存储平台数据加密中的性能, 进行仿真实验, 实验采用 Matlab 7 设计, 数据比特流的长度为 1024, 加密数据的规模集大小为 200Gbit, 测试数据集的规模为 200, 对待加密数据的采样频率为 12 KHz, 初始加密比特序列为:

```
100110101001010010010100101010010101001
010010101000010010100100101010010010100
101001010010100101010010001010010111011
110010010101001011101001010101010101010
101011001001010010
```

以上述采集的云数据加密比特序列为输入, 根

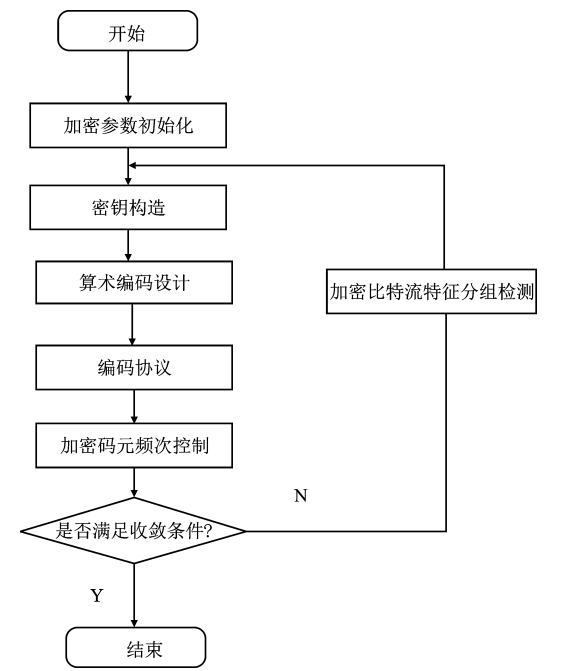


图 3 加密算法实现流程图

据表 1 的参数设定,进行数据加密仿真.

表 1 实验参数设置					
参数设置	$t_{\max}$	M	l	p_m	p_c
参数值	23	40	10	0.21	0.45

测试加密的训练集和测试样本集的握手时间,根据握手时间判断加密的深度和抗攻击能力,采用传统的 ECC 方法和本文的 RAS 方法,得到测试结果如图 4 所示.

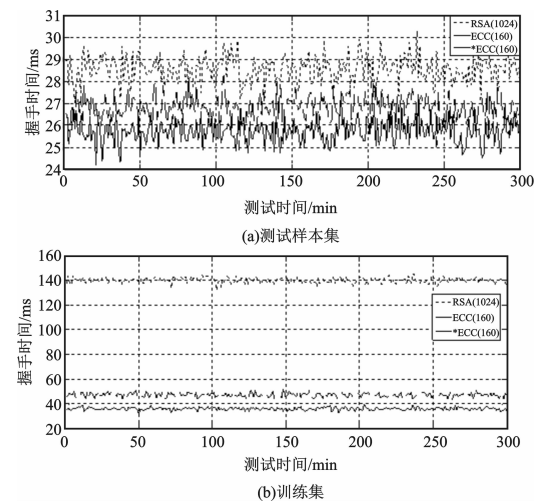


图 4 加密性能测试

分析图 4 得知,采用本文方法进行云存储平台数据加密的握手较短,说明数据加密的深度和实时性较好,加密的深度较高.进一步分析不同加密比特

序列率下的信息熵值,以此验证数据加密的强度,得到结果如图 5 所示.

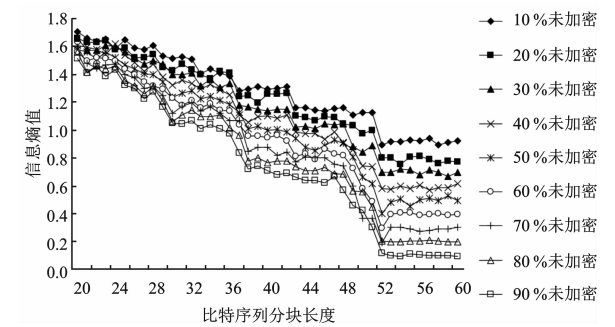


图 5 不同加密比特率下的信息熵测试

分析图 5 得知,采用本文方法进行数据加密,信息熵收敛性较好,相比传统方法,加密的抗攻击强度提高了 15.83%,被攻击者解密的数据降低了 6.98%,展示了本文方法在提高云存储数据保密性方面的优越性能.

4 结束语

云存储信息的安全关系到用户的隐私保护和整个网络信息系统的安全,云存储平台的结构化数据组合结构简单,导致云存储数据容易受到网络攻击,通过数据加密,提高数据的安全性.本文提出一种基于混沌映射的云存储平台数据加密算法.采用循环密钥配对方法进行数据加密的结构化特征分解,采用码元自适应配对方法进行数据密钥的循环扩展,结合混沌敏感性表征和信息熵定位方法,构建数据加密的隐写协议和编码协议,实现云平台下的存储数据算术编码和循环加密.研究得知,本文方法进行数据加密的性能较好,抗攻击能力较强,确保了云存储平台数据的安全性.

参考文献:

[1] 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.

[2] 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.

[3] 陶源,周喜,马玉鹏,等. 基于 Hash 函数的移动双向认证协议[J]. 计算机应用, 2016, 36(3): 657-660.

[4] Lee Y Y, Wang C H, Huang Y H. A hybrid RF/baseband precoding processor based on parallel-index

- selection matrix-inversion-bypass simultaneous orthogonal matching pursuit for millimeter wave MIMO systems[J]. IEEE Transactions on Signal Processing, 2015, 63(2): 305-317.
- [5] Vaseghi B, Pourmina M A, Mobayen S. Secure communication in wireless sensor networks based on chaos synchronization using adaptive sliding mode control [J]. Nonlinear Dynamics, 2017, 89(3):1689-1704.
- [6] Filali R L, Benrejeb M, Borne P. On observer-based secure communication design using discrete-time hyperchaotic systems[J]. Communications in Nonlinear Science and Numerical Simulation, 2014, 19(5): 1424-1432.
- [7] 黄天宇, 马林华, 胡星, 等. 一种实用的毫米波大规模 MIMO 混合预编码算法[J]. 电子与信息学报, 2017, 39(8): 1788-1795.
- [8] Rusu C, Mendez-Rial R, Gonzalez-Prelcic N, et al. Low complexity hybrid precoding strategies for millimeter wave communication systems[J]. IEEE Transactions on Wireless Communications, 2016, 15(12): 8380-8393.
- [9] 廖军, 蒋朝惠, 郭春, 等. 一种基于权重属性熵的分类匿名算法[J]. 计算机科学, 2017, 44(7): 42-46.
- [10] 徐志强, 袁德砮, 陈亮. 基于稀疏随机矩阵的再生码构造方法[J]. 计算机应用, 2017, 37(7): 1948-1952.
- [11] 孟博, 张金丽, 鲁金钊. 基于计算模型的 OpenID Connect 协议认证性的自动化分析[J]. 中南民族大学学报(自然科学版), 2016, 35(3): 123-129.
- [12] 来学嘉, 卢明欣, 秦磊, 等. 基于 DNA 技术的非对称加密与签名方法[J]. 中国科学: 信息科学, 2010, 40(2): 240-248.
- [13] 熊风光, 李希, 韩燮. 基于整体最小二乘的椭圆拟合方法[J]. 微电子学与计算机, 2017, 34(1): 102-105.
- [14] 周彦伟, 杨波, 张文政. 可证安全的移动互联网可信匿名漫游协议[J]. 计算机学报, 2015, 38(4): 733-748.
- [15] 冯超, 张权, 唐朝京. 计算可靠的 Diffie-Hellman 密钥交换协议自动证明[J]. 通信学报, 2011, 32(10): 118-126.
- [16] 郭良. 大数据环境下数据隐私加密算法的改进与仿真[J]. 计算机仿真, 2016, 33(8): 338-341.

作者简介:

陈建辉 男, (1978-), 硕士, 副教授. 研究方向为网络及信息安全. E-mail: 17153414@qq.com.

赵 静 女, (1978-), 博士研究生, 副教授. 研究方向为隐私管理.