

DOI: 10.11830/ISSN.1000-5013.201611078



数字对讲机语音加密方法及实现

龚雪¹, 张育钊¹, 庄铭杰¹, 唐加能^{1,2,3}

(1. 华侨大学 工学院, 福建 泉州 362021;
2. 华侨大学 机电及自动化学院, 福建 厦门 361021;
3. 福建先创电子有限公司, 福建 泉州 362000)

摘要: 提出一种数字对讲机实时语音加密方案. 首先, 利用线性同余发生器和复合混沌系统设计加密系统. 利用 Chebyshev 映射和 Cubic 映射构造动态变参数复合混沌系统, 并用线性同余发生器为复合混沌系统提供初值. 然后, 基于 STM 32 硬件平台设计数字对讲机语音加密系统, 加密算法中所有步骤都在 STM 32 平台上实现. 经测试表明: 该加密系统具有较高的安全性和较好的实时性.

关键词: 数字对讲机; 语音加密; 混沌系统; STM 32 平台

中图分类号: TP 391 **文献标志码:** A **文章编号:** 1000-5013(2018)05-0756-06

Method and Implementation of Voice Encryption in Digital Interphone

GONG Xue¹, ZHANG Yuzhao¹,
ZHUANG Mingjie¹, TANG Jianeng^{1,2,3}

(1. College of Engineering, Huaqiao University, Quanzhou 362021, China;
2. College of Mechanical Engineering and Automation, Huaqiao University, Xiamen 361021, China;
3. Centron Communications Technologies Fujian Limited Liability Company, Quanzhou 362000, China)

Abstract: A digital interphone voice encryption scheme is proposed. Firstly, we designed a cryptosystem based on linear congruential generator and a hybrid chaotic system. The hybrid chaotic system with variable parameter is constructed based on Chebyshev map and Cubic map. And we utilize linear congruential generator to provide the initial value for hybrid chaotic system. Then, a digital interphone voice cryptosystem is realized in STM 32 hardware platform. And all the steps described in the algorithm is implemented in STM 32. Finally, the experimental results show that the cryptosystem has higher security and better real-time performance.

Keywords: digital interphone; voice encryption; chaotic system; STM 32 platform

数字对讲机具有抗干扰能力强、通话质量好、频谱利用率高的特点, 是专用无线通信的一种重要方式. 数字对讲机语音加密算法的研究有着极其重要的意义. 语音信号具有冗余性和数据量大的特点, 传统的加密算法, 如数据加密标准(DES)、高级加密标准(AES)、公钥加密算法(RSA)等通常需要大量的存储空间和计算资源, 而且随着信息技术的发展, 这些算法难以保证语音加密传输的实时性和安全性^[1-6]. 在有限计算精度下, 混沌系统的混沌特性会退化, 混沌序列会出现短周期现象. 与离散混沌系统相比, 连续混沌系统有更为复杂的混沌特性, 但是由于连续混沌系统多为高维系统, 在硬件平台上实现

收稿日期: 2016-11-22
通信作者: 张育钊(1963-), 男, 副教授, 博士, 主要从事无线通信的研究. E-mail: zyz@hqu.edu.cn.
基金项目: 国家自然科学基金资助项目(61573004); 福建省教育厅项目(JA15035); 福建省泉州市科技项目(2014Z103, 2015Z114)

时,多需要进行浮点数运算,运算量很大,难以保证语音的实时性.基于此,本文研究适合在硬件平台上实现的离散混沌系统,提出一种数字对讲机语音加密方案.

1 混沌语音加密算法

1.1 线性同余发生器

线性同余发生器(LCG)是目前主流的随机数发生器之一^[7],其递推公式为

$$\left. \begin{aligned} x_n &= (a \times x_{n-1} + c) \pmod{m}, & n &= 1, 2, 3, \dots, \\ r_n &= x_n / m, & n &= 1, 2, 3, \dots, \end{aligned} \right\} \quad (1)$$

式(1)中: a 为乘子; c 为增量; m 为模数,通常取2的指数幂,均为非负整数.显然, $x_n \in (0, m), r_n \in (0, m)$.利用式(1)产生随机数时,应选取合适的参数,才能得到周期长且随机性好的序列.

1.2 Cubic 映射

Cubic 是一个简单的一维离散混沌映射,其映射方程为

$$x_{n+1} = ax_n^3 - bx_n. \quad (2)$$

随着参数 a 的变化,混沌序列 x_n 的取值也在发生变化.当 $a=1$ 时, $x_n \in (-2, 2)$; 当 $a=4$ 时, $x_n \in (-1, 1)$. 随着参数 b 的变化,混沌映射会历经倍周期分岔达到混沌状态.当 $b>2.3$ 时, x_n 的取值是随机的,即出现混沌状态.

1.3 Chebyshev 映射

Chebyshev 映射方程为 $y_{n+1} = \cos(\mu \cos^{-1} y_n)$. 其中: μ 为 Chebyshev 映射的阶数,当 $\mu>2$ 时,混沌映射具有正的 Lyapunov 指数,系统处于混沌状态, $y_n \in (-1, 1)$.

1.4 加密系统设计

LCG 受计算精度约束,产生的随机数序列的周期与处理器的机器字长有关.为了产生随机性更好的随机数,把 LCG 产生的随机数存储在一个一维数组中,用作复合混沌系统的初值.

虽然 Chebyshev 映射和 Cubic 映射的非线性方程简单,易于在硬件平台上实现,但是它们的混沌运动却极其复杂.因此,基于 Chebyshev 映射和 Cubic 映射设计一个动态变参数复合混沌系统,利用一个子系统的输出状态影响另一个子系统的参数,从而使子系统间相互扰动.复合混沌系统的初值则由 LCG 定时产生.复合混沌系统原理框图,如图 1 所示.

对 Chebyshev 映射中的阶数 μ 和 Cubic 映射中的分岔参数 b 进行扰动,其扰动数学表达式为

$$\left. \begin{aligned} \mu_{n+1} &= \mu_n + w \mid x_i \mid / 2^n, \\ b_{n+1} &= b_n + w \mid y_i \mid / 2^n. \end{aligned} \right\} \quad (3)$$

由式(3)推导可得

$$\left. \begin{aligned} \mu_{n+1} &= \mu_1 + w \mid x_n \mid / 2 + w \mid x_n \mid / 2^2 + \dots + w \mid x_n \mid / 2^n, \\ b_{n+1} &= b_1 + w \mid y_n \mid / 2 + w \mid y_n \mid / 2^2 + \dots + w \mid y_n \mid / 2^n. \end{aligned} \right\} \quad (4)$$

式(4)中: x_n, y_n 为混沌系统迭代值; w 为加权系数.当分岔参数 $\mu>2, b>2.3$ 时,系统进入混沌状态.故取 μ_1, b_1 分别为 4.0, 2.5, w 为 0.5. 由于 $\mid x_n \mid, \mid y_n \mid$ 取值范围均在 $(0, 1)$ 之间,因此, $\mu_{n+1} \in (4.0, 4.5), b_{n+1} \in (2.5, 3.0)$, 保证了系统有好的混沌特性.同时,由于 b_{n+1} 为关于 x_n 的函数, μ_{n+1} 为关于 y_n 的函数,故 μ_{n+1} 和 b_{n+1} 具有良好的随机性.

在有限计算精度下,经过相当长的一段时间后,即使复合混沌系统产生的混沌序列演化为周期序列,由于 LCG 定时为混沌系统提供初值,使混沌系统能跳出周期态,重新回到混沌状态.因此,能有效地减弱在有限计算精度下混沌序列的短周期现象.

1.5 混沌序列二值化

数字对讲机内部模拟语音信号经过采样、量化和压缩编码后变成数字信号.复合混沌系统产生的是

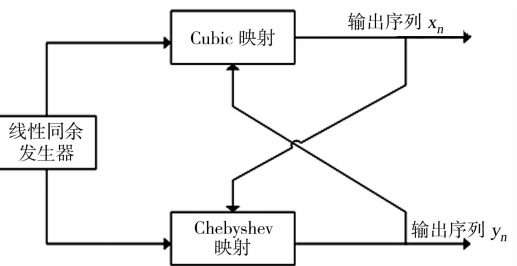


图 1 复合混沌系统原理框图
Fig. 1 Principle block diagram
of hybrid chaotic system

实数混沌序列,故必须对混沌序列进行二值化操作.对混沌系统每次迭代产生的实数值,作如下约定,即

$$k_i = \begin{cases} \text{round}(10^3 \times (10^2 x_i - \text{round}(10^2 x_i))) \bmod 2, & \text{round}(10^2 x_i) < 10^2 x_i, \\ \text{round}(10^3 \times (1 - (10^2 x_i - \text{round}(10^2 x_i)))) \bmod 2, & \text{round}(10^2 x_i) \geq 10^2 x_i. \end{cases} \quad (5)$$

式(5)中: $\{k_i\}$ 为混沌二值序列; $\text{round}(\cdot)$ 为四舍五入运算.文中加密算法最终产生了两列混沌二值序列 $\{K1_i\},\{K2_i\}$.

2 混沌序列性能测试

结合实际的加密和解密运算,当加密系统产生的混沌密钥序列较长时,需对序列的随机性进行分析.美国国家标准与技术研究院(NIST)发布的随机数和伪随机数发生器统计测试组件是当前测试伪随机序列系能工具中最权威的一种^[8-10].该软件测试包由15项核心测试组成,每项测试的结果均以P-value值表示.显著水平 α 可用于测试中,若 $P\text{-value} \geq \alpha$,则该项测试通过;若 $P\text{-value} < \alpha$,则该项测试未通过. α 的取值范围为 $[0.000\ 1, 0.010\ 0]$,通常取 $\alpha = 0.010\ 0$.按照NIST测试要求,为保证测试结果的可靠性与准确性,每个被测序列的长度应为 $10^3 \sim 10^7$,实验中,取被测序列长度为 10^6 bit.分别对复合混沌系统产生的两列密钥序列 $\{K1_i\}$ 和 $\{K2_i\}$,以及单独的Cubic和Chebyshev映射产生的混沌序列进行随机数测试.测试结果如表1所示.表1中:*表示该项测试未能通过.

由表1可知:复合混沌系统产生的混沌二值序列通过了NIST的15项随机数测试;而分别单独利用Cubic和Chebyshev映射产生的混沌序列,未能通过所有的测试项.由此可得,文中设计的复合混沌系统能够产生随机性好的混沌序列,可用于语音加密.

表1 NIST 随机数测试结果
Tab.1 Results of NIST statistical randomness tests

测试项目	$K1_i$	$K2_i$	Chebyshev	Cubic
近似熵测试	0.151 174	0.955 945	0.048 607	*
块内频率测试	0.989 085	0.576 670	0.103 177	*
累积和测试 1	0.943 118	0.848 737	*	*
累积和测试 2	0.975 783	0.483 106	*	*
傅里叶变换测试	0.073 544	0.693 142	0.652 959	0.588 217
频率测试	0.942 602	0.464 169	*	*
线性复杂度测试	0.476 157	0.604 003	0.625 460	0.428 728
随机偏离测试	0.843 414	0.906 234	*	*
随机偏离变量测试	0.980 223	0.983 363	*	*
最长游程测试	0.973 407	0.276 984	0.846 625	0.428 728
重叠模块匹配测试	0.928 315	0.399 082	0.113 472	0.600 336
非重叠模式匹配测试	0.847 938	0.934 219	0.230 662	0.296 988
二阶矩阵阶测试	0.647 301	0.689 402	0.648 821	0.348 845
游程测试	0.109 154	0.788 287	*	*
串行测试 1	0.103 048	0.570 724	0.419 788	0.126 726
串行测试 2	0.635 447	0.727 470	0.600 591	0.662 565
通用统计测试	0.119 937	0.544 292	0.340 496	0.911 993

3 数字对讲机语音加密系统设计

3.1 数字对讲机语音通信的基本特点

在数字对讲机内部,模拟语音信号经过A/D转换和压缩编码后变为数字信号.因此,加密过程是对数字信号进行加密.数字对讲机体积较小,只允许安装等运算能力的处理单元,算法和硬件系统设计需要考虑运算量大小.与此同时,数字对讲机语音通话实时性要求高,如果延时过大,会影响正常的通话.

数字对讲机系统是在窄带下进行语音的压缩传送,其信道宽度一般为12.5 kHz或6.25 kHz,传输速率在 $1.2 \sim 4.8\text{ kbit} \cdot \text{s}^{-1}$.因此,为了适应低速率语音通信的要求,必须采用合适的语音压缩编码算

法. 数字对讲机语音传输具有实时性, 在加密过程中, 加密单元要能及时产生密钥序列.

3.2 硬件系统设计

为了验证加密算法在数字对讲机语音加密中的可行性, 利用 AMBE 声码器、CSP 1027 音频编解码器和 STM 32 硬件平台进行数字对讲机语音加密系统的设计. 加密系统硬件框图, 如图 2 所示.

系统以 STM 32 控制器为核心, 完成语音的加密和解密运算. 采集的模拟语音信号经过 CSP 1027 音频编解码器 A/D 转换, 将得到的 PCM 数据送给 AMBE 声码器进行压缩编码. 声码器每 20 ms 输出一帧语音数据, 通过同步通信的方式发送给 STM 32. 同时, STM 32 产生相应长度的混沌密钥序列, 对明文语音数据进行加密, 组帧后发送回声码器. 密文语音数据经声码器解码后发送给 CSP 1027 音频编解码器, 通过 D/A 转换输出为密文语音信号.

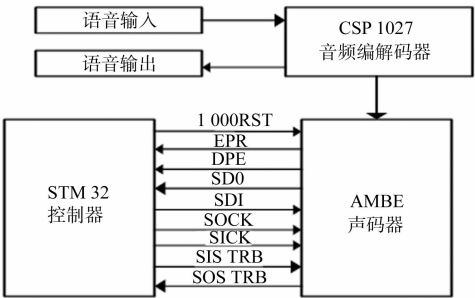


图 2 系统硬件框图
Fig. 2 Block diagram of system hardware

3.3 软件设计

AMBE 工作在串行被动有帧模式下, AMBE 对 CSP 1027 芯片 24 脚的 8 kHz 信号进行计数, 计满 160 个采样点 (20 ms) 后, 做编码运算. STM 32 采用查询方式判断 AMBE 声码器是否有数据输出.

系统首先通过 MIC-IN 输入语音信号到音频编解码 CSP 1027. CSP 1027 对输入的语音信号进行采样和量化后, 转换为 PCM 编码数据. AMBE 声码器接收 PCM 语音数据后, 进行压缩编码, 每 20 ms 输出一帧数据. STM 32 接收到一帧数据后, 首先, 提取出有效语音数据; 然后, 利用复合混沌系统产生等长度的混沌密钥序列对明文数据进行加密, 并将加密完的数据组帧后, 发送回声码器. 声码器收到一帧完整的数据后进行解码, 发送给 CSP 1027, 经过数模转换, 通过喇叭播放出加密后的语音. 其流程图如图 3 所示.

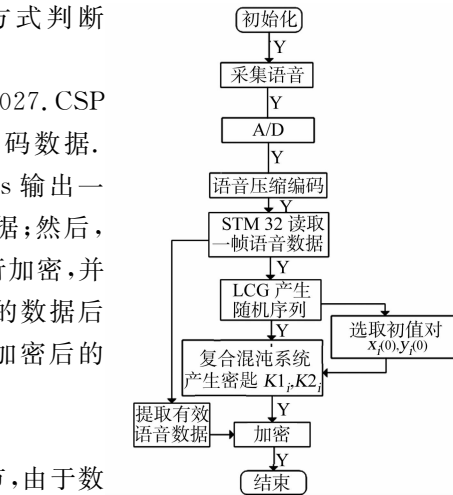


图 3 加密流程图
Fig. 3 Encryption diagram

加密具体有以下 7 个步骤.

- 1) STM 32 接收到一帧语音数据, 每帧数据包含 34 个字节, 由于数字对讲机低速率编码要求和 AMBE 声码器编码速率不同, 每帧数据中有效数据最多为 96 bit, 最少为 48 bit. 为了保证实时性, 只对有效数据进行加密. 因此, 首先提取帧数据中的有效数据部分.

- 2) 设置 LCG 的初值对 (x_0, a, c, m) 和迭代次数 n , 利用 LCG 生成的随机序列构成一个一维数组 R_n , 复合混沌系统的初值对 $x_i(0), y_i(0)$ 依次从数组 R_n 中选取, i 为 $(0, 1, 2, 3, \dots, n)$.

- 3) 设置复合混沌系统的初值对 $(\mu_i, y(0)), (a, b_1, x(0))$, 以及加权系数 w , 产生与有效语音数据相同长度的密钥序列 $\{K1_i\}, \{K2_i\}$.

- 4) 利用密钥流序列 $\{K1_i\}$ 与语音明文序列进行异或操作, 得到密文 $P_i = K1_i \oplus M_i$.

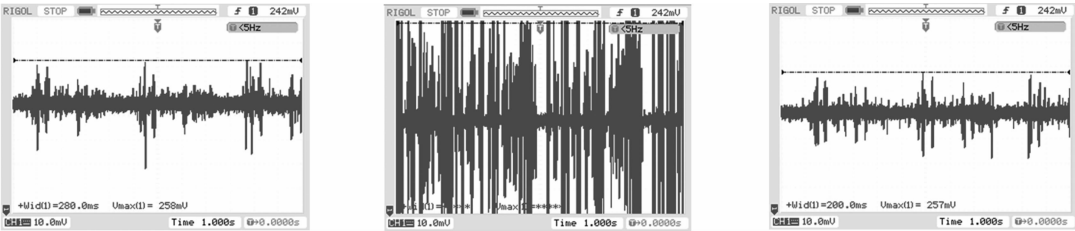
- 5) 利用密钥流序列 $\{K2_i\}$ 与密文 $\{P_i\}$ 进行异或操作, 得到密文 $C_i = K2_i \oplus P_i$, 即当前语音帧加密后的密文.

- 6) 一帧语音数据加密完, 密文经声码器解码后, 发送给 CSP 1027, 经 D/A 转换, 输出为模拟语音.

- 7) STM 32 再次接收到一帧语音数据, 操作步骤同上, 直到一段语音加密完则结束. 解密过程为加密过程的逆过程, 即明文 $M_i = C_i \oplus K2_i \oplus K1_i$.

3.4 加密效果

使用数字示波器实时捕捉原始语音信号和加解密后语音信号的波形, 结果如图 4 所示. 由图 4 可知: 加密后的语音信号波形图杂乱无章, 呈现出杂乱无章的状态; 将语音信号放大后, 输入扬声器, 人耳听到的是刺耳的噪声, 无法听清楚语音内容; 解密后的语音信号波形与原始语音信号波形图形状类似, 通过喇叭播放后, 虽然语音含有一些杂音, 但是并不影响听清楚语音内容.



(a) 原始语音 (b) 加密后语音 (c) 解密后语音

图 4 语音加解密效果图

Fig. 4 Effect diagram of voice encryption and decryption

4 加密系统性能分析

4.1 语音质量主观评价

为了进一步判断经过加解密处理后语音信号的保真度,进行主观语音质量测试.平均意见方法(MOS)是应用最为广泛的评估语音质量的一种指标.当 MOS 评分为 5 时,人耳能很清楚地听到语音信息,语音无失真和延迟;当 MOS 评分为 4 时,人耳能听清楚语音信息,语音信息中有少量杂音,延迟小;当 MOS 评分为 3 时,人耳听不太清除语音信息,语音有一定延迟和失真;当 MOS 评分小于 3 时,人耳已基本听不清语音信息,杂音较大.在工程应用中,通常认为评分在 3 分以上时,语音质量较好.

实验中,请来 10 个测试人,分别对 12 组不同的语音样本,进行 MOS 评分测试,利用 MOS 评分评价加解密后语音的质量.测得结果,如表 2 所示.由表 2 可知:加密后语音信号的 MOS 评分较低,可以判定加密后人耳难以听清语音信息;而解密后语音信号的 MOS 评分达到 3 以上,可以判断解密后的语音信息音质较好,人耳可以听清语音信息.

4.2 密钥敏感性测试

为了验证本算法对密钥的敏感程度,在硬件开发平台下微小改变 LCG 或者复合混沌系统中某一参数,使得误差 $\Delta=0.01$.利用数字示波器观测输出解密波形,结果如图 5 所示.由图 5 可知:与原始信号波形相比,解密后的波形显得杂乱无章,只有在密钥完全正确时,才能正确解密;当某个密钥有微小差别时,解密会出错;播放解密后的语音,人耳所听到的语音刺耳尖锐,无法辨别语音内容.

表 2 MOS 评分
Tab. 2 MOS score

语音样本编号	加密后 MOS 值	解密后 MOS 值
1	1.0	3.6
2	1.3	3.7
3	1.1	3.4
4	1.0	3.5
5	1.0	3.6
6	1.2	3.5
7	1.0	3.6
8	1.1	3.5
9	1.3	3.8
10	1.1	3.6
11	1.3	3.8
12	1.2	3.7

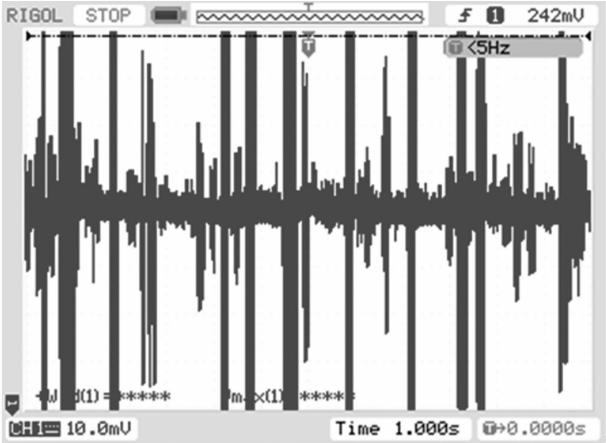


图 5 错误解密语音信号波形图

Fig. 5 Waveform diagram of error decrypted voice signals

在 Matlab 软件仿真环境下,其加密运算为浮点运算,且运算字节长度明显大于硬件平台.在硬件开发平台下,受微控制单元(MCU)计算字长的限制,密钥的精度远小于计算机软件仿真环境.因此,加密算法的敏感性低于计算机仿真环境中的敏感性.

4.3 密钥空间分析

使用线性同余发生器 LCG 和复合混沌系统构成的加密系统,其密钥 K 由 K_{LCG} , K_C (K_{LCG} 由线性同

余发生器产生, K_c 由复合混沌系统产生)两部分组成,二者相互独立.因此,其密钥空间可以表示为

$$K = K_{LCG} + K_c. \tag{7}$$

式(7)中: K_{LCG} 由初值 x_0 、乘子 a 、增量 c 和模数 m 组成; K_c 由参数 μ, b 和加权系数 w 组成.由节 4.1 分析可知,任一密钥微小的改变都导致解密失败,密钥的灵敏度为 10^{-2} .因此,加密算法密钥空间约 2^{50} .

由此可见,该加密算法可保证足够的密钥空间抵抗穷举攻击.同时,针对加密过程中的每一帧语音数据,采用 LCG 数组中不同值作为复合混沌系统迭代初值,其安全性可以得到有效保证.

4.4 延迟

对于数字对讲机语音实时通信而言,延迟非常重要.文中设计的数字对讲机语音加密系统延迟很小.加密系统延时时间主要包括语音压缩编码和密钥序列产生两部分.加密过程中,由于每帧语音数据包含的比特数较少,STM 32 时钟频率达 72 MHz,在接收到一帧数据后,可以快速产生密钥序列用于加密.AMBE 声码器有独立的语音编码和解码单元,可同时完成语音的编码和解码任务,并且所有的编码和解码都在芯片内部完成,不需要额外的存储器.

5 结束语

提出的加密系统由线性同余发生器 LCG 和复合混沌系统组成.通过 STM 32 硬件平台、AMBE 声码器和 CSP1027 音频编解码器构造了数字对讲机语音加密系统,在该平台上完成了加密系统的实验研究.经过多次加、解密测试证明,文中加密算法能够完成语音实时加密,虽然受硬件计算字长的影响导致密钥敏感性变弱,但是由于密钥参数多,所以有足够的密钥空间抵御穷举攻击.

参考文献:

[1] ALANAZI H O,ZAIDAN B B,ZAIDAN A A,*et al.* New comparative study between DES, 3DES and AES within nine factors[J]. Computer Science,2010,3(2):152-157.

[2] ANEES A,SIDDIQUI A M,AHMED F. Chaotic substitution for highly autocorrelated data in encryption algorithm [J]. Communications in Nonlinear Science and Numerical Simulation, 2014, 19(9): 3106-3118. DOI: 10. 1016/j. cnsns. 2014. 02. 011.

[3] BARENGHI A,BERTONI G M,BREVEGLIERI L,*et al.* A fault induction technique based on voltage underfeeding with application to attacks against AES and RSA[J]. Journal of Systems and Software, 2013, 86(7): 1864-1878. DOI:10. 1016/j. jss. 2013. 02. 021.

[4] HU Hanping,LIU Lingfeng,DING Naida. Pseudorandom sequence generator based on the Chen chaotic system[J]. Computer Physics Communications,2013,184(3):765-768. DOI:10. 1016/j. cpc. 2012. 11. 017.

[5] AHMAD M,ALAM B,FAROOQ O. Chaos based mixed keystream generation for voice data encryption[J]. International Journal on Cryptography and Information Security,2012,2(1):39-48.

[6] AZZAZ M S,TANOUGAST C,SADOUDI S,*et al.* Synchronized hybrid chaotic generators: Application to real-time wireless speech encryption[J]. Communications in Nonlinear Science and Numerical Simulation,2013,18(8):2035-2047. DOI:10. 1016/j. cnsns. 2012. 12. 018.

[7] LEHMER D H. Mathematical methods in large-scale computing units[C]//Proceedings of a Second Symposium on Large-Scale Digital Calculating Machinery. Cambridge:Harvard University Press,1951:141-146.

[8] VAJARGAH B F,ASGHARI R. A pseudo random number generator based on chaotic henon map (CHCG)[J]. IJMEC,2015,5(15):2120-2129. DOI:649123/10134.

[9] RUKHIN A,SOTO J,NECHVATAL J,*et al.* A statistical test suite for random and pseudorandom number generators for cryptographic applications[J]. Applied Physics Letters,2015,22(7):1645-1679. DOI:10. 1063/1. 4928732.

[10] 张伟伟. 通信系统中语音质量评价的研究[D]. 北京:北京邮电大学,2014.

(责任编辑:钱筠 英文审校:吴逢铁)