第 58 卷 第 1 期 2009 年 1 月
1000-3290/2009/58(01)/0113-07

物 理 学 报
ACTA PHYSICA SINICA

Vol.58,No.1,January,2009

基于现场可编程门阵列技术的混沌数字通信系统——设计与实现*

周武杰† 禹思敏

(广东工业大学自动化学院,广州 510006)

(2008 年 6 月 1 日收到;2008 年 7 月 13 日收到修改稿)

提出了基于 IEEE-754 标准和现场可编程门阵列(FPGA)技术的混沌数字通信系统的通用设计与硬件实现的一种新方法,实现了混沌加密体制与传统密码体制的结合.根据 Euler 算法,对连续混沌系统作离散化处理,通过 FPGA 硬件设计混沌离散系统,使其产生作为密钥的混沌数字序列,其中加密算法采用置乱扩展技术,并对算法进行了分析.设计驱动响应式同步保密通信系统,构建包含信号在内的闭环,实现发送端与接收端离散混沌系统的同步.以网格蔡氏混沌系统为例,对该保密通信系统进行了 FPGA 硬件实验,给出了技术实现过程、算法流程、硬件设计与实现结果.

关键词:网格多涡卷蔡氏电路,置乱扩展矩阵,现场可编程门阵列技术,混沌数字通信系统

PACC:0545

1. 引 言

四十多年来,混沌的发展经历了从认识了解、深化研究到工程应用等多个不同的阶段[1—53],特别是上世纪 90 代年以来,Pecora 和 Carroll 提出混沌同步的概念,在此基础上,利用混沌同步实现保密通信的方法受到了人们的关注[29—36],其中主要有混沌键控、混沌参数调制、混沌扩频、混沌码分多址等数字混沌通信技术[34—36,38—53].例如,文献[37]提出了混沌加密体制与传统密码体制相结合的算法,将传统密码算法的密钥空间拓展为混沌系统的参数和初值空间.如何把传统的数据加密算法与混沌加密算法相结合,应用于加密通信具有现实意义,是混沌加密通信发展的重要方向.

在技术实现方面,由于模拟电子电路的元器件参数离散性较大,存在发送系统与接收系统之间的电路参数失配问题,还原出信号的保真度得不到保证.解决方案之一是采用数字处理技术,对连续时间无量纲状态方程进行离散化处理和变量比例变换,用 FPGA 技术实现混沌数字调制保密通信系统,将网格状蔡氏离散混沌系统、混沌调制与明文置乱扩展技术相结合.我们给出了该方案的一般设计原理与硬件实现结果.

2. FPGA 混沌密码序列发生器

在文献[54]中,我们提出了基于 IEEE-754 标准的 FPGA 通用混沌信号产生器设计与硬件实现的一种新方法.根据 Euler 算法,对连续混沌系统作离散化处理,得到与之相应的归一化离散混沌迭代方程或差分方程,并利用模块化设计方法,将离散混沌系统划分为浮点数乘法器、浮点数加法器、浮点数符号函数运算器、浮点数正负绝对值运算器以及初始值与迭代值选择等五个基本模块的组合.其次,用硬件语言实现浮点数的乘法运算、加法运算、符号函数运算、正负绝对值运算,并以此为基础,最终能在 FPGA 硬件平台上产生多种不同类型的混沌序列.

混沌序列之所以适合于数字信息加密,是因为混沌运动具有既非周期又不收敛,运动轨迹上的点遍历整个区域、类似于随机噪声、对初始值极为敏感等特征.这些动力学特性使得混沌序列宽频带,类随机,有较好的保密性能,并且由确定性系统产生,使得混沌序列可控制可再生,为加密和解密提供了可

* 国家自然科学基金(批准号:60572073,60871025)和广东省自然科学基金(批准号:8151009001000060,8351009001000002)资助的课题.

† E-mail:wujiezhou@163.com

行性.

3. 基于混沌自同步的混沌数字保密通信系统

本文提出的混沌数字保密通信系统原理图如图1所示.图中主要包括信源编码模块、加密算法模块、驱动系统序列密码发生器模块、密码同步检测模块、解密算法模块、响应系统序列密码发生器模块、信源解码模块等部分,各个部分的作用如下.

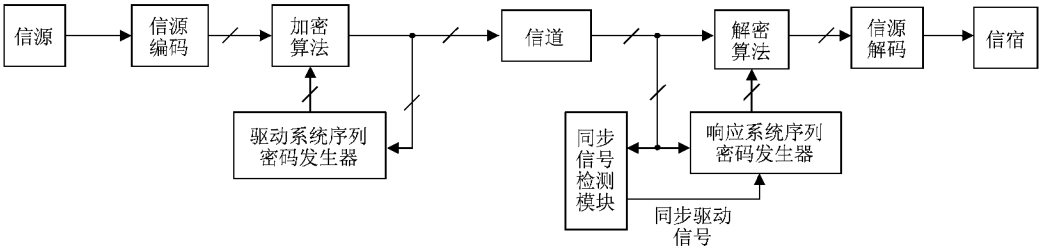

图1 数字保密通信系统原理图

信源编码模块在发送端将模拟信号进过取样、量化、编码变成二进制数字序列送加密算法模块.

加密算法模块一般采用异或运算,在发送端,它将来自信源编码的二进制数字序列与密码序列进行异或运算产生密文序列.加密完成后再通知驱动系统迭代一次,这样就可以保证数据的完整性.

驱动系统序列密码发生器模块的主要功能是产生用于加密的密码序列,它是数字加密通信系统中加密可靠性的核心部分,包括加密序列的产生(在发送端对明文的进行加密),因为是自同步系统,所以加密后的混沌序列还要作为驱动系统的迭代值.

解密算法模块也是采用异或运算,在接受端,则将密文序列与密码序列进行异或运算还原成二进制明文序列.

密码同步检测模块主要是产生密码同步信号来驱动响应系统密码发生器模块,用于对收方的密码序列产生器的状态进行更新.其工作原理是判断从经信道传输的密文是否改变,如果变化了,就产生一个驱动信号,一方面是驱动响应系统进行下一次迭代,另一方面是驱动解密算法模块进行解密.

响应系统序列密码发生器模块的主要功能是产生用于解密的密码序列,当它接收到密码同步检测模块生成的密码同步驱动信号,响应系统就迭代一次.

信源编码模块在接收端则把二进制数字还原为模拟信号,再经过直流分量滤波.为进一步提高其保密性能,还可将上述方案拓展到高阶级联混沌同步系统,限于篇幅,此处从略.

4. 基于网格状蔡氏混沌系统的实时语音保密通信系统的设计

本节将以网格状蔡混沌系统为例,对上述的保密通信系统进行 FPGA 实验,并通过语音保密通信来进行验证这个系统.需要说明的是,该方法对自同步的混沌系统具有普适性.

在多涡卷蔡氏电路的基础上[8,9,11—13],我们进一步提出了网格多涡卷蔡氏电路.无量纲状态方程为[23]

$$\begin{aligned}\frac{\mathrm{d}x}{\mathrm{d}t} &= \alpha[y - f_2(y) - f_1(x)],\\ \frac{\mathrm{d}y}{\mathrm{d}t} &= x - y + z,\\ \frac{\mathrm{d}z}{\mathrm{d}t} &= -\beta[y - f_2(y)],\end{aligned} \tag{1}$$

式中 $f_1(x) = m_1 x + m_0 m_1 \mathrm{sgn}(x)$, $f_2(y) = m_1 \mathrm{sgn}(y)$; α, β, m_0, m_1 为系统参数,典型值为 $\alpha = 8.5—10$, $\beta = 16$, $m_0 = 0.5$, $m_1 = 0.25$;网格蔡氏三维系统需要用数值积分来求得实数值混沌序列.典型的数值积分法有 Euler 算法、改进 Euler 算法和 Runge – Kutta 法.这三种离散化的方法各有优缺点.在这里我们用 Euler 算法来对(1)式作离散化处理.得归一化和离散化后的 2×2 网格状多涡卷蔡氏吸引子的无量纲状态方程为

$$\begin{aligned}x(n+1) &= ax(n) + by(n) + c\mathrm{sgn}(x(n))\\ &\quad + d\mathrm{sgn}(y(n)),\\ y(n+1) &= ex(n) + fy(n) + ez(n),\end{aligned}$$

$z(n+1) = gy(n) + k\mathrm{sgn}(y(n)) + hz(n)$，(2)

式中 a,b,c,d,e,f,g,h,k 为方程参数，采用 IEEE-754 标准的双精度格式表示.

实时语音混沌加密通信系统如图 2 所示. 音频输入/输出由 Wolfson 公司的低功耗立体声音频编/解码芯片 WM8731 完成. 在发送端，首先把模拟语音信号以 48 kHz 采样频率经过 A/D 转换成 16 位串行数据比特流，经串/并转换得到并行数据. 然后，在发送端，将语音信号数据流与混沌序列之和取模运算后得到密文序列再嵌入驱动系统混沌映射的输入端进行迭代运算以实现调制. 在接收端，把通过信道传输的密文序列一方面要作为响应系统混沌映射的输入值，一方面要响应系统产生的混沌序列进行异或运算解密，还原成二进制数据流，最后经 D/A 转换而恢复成模拟语音信号通过扬声器听到还原后的信号.

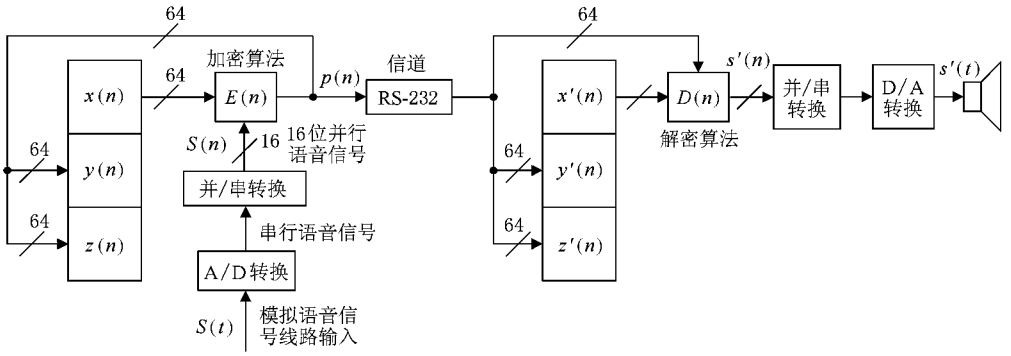

图 2　语音传输保密通信硬件实验系统

发端网格蔡系统的无量纲状态方程为

$$\begin{aligned} x(n+1) &= ax(n) + by(n) + c\mathrm{sgn}(x(n)) \\ &\quad + d\mathrm{sgn}(y(n)), \\ y(n+1) &= ep(n) + fy(n) + ez(n), \\ z(n+1) &= gy(n) + k\mathrm{sgn}(y(n)) + hz(n). \end{aligned} \quad (3)$$

接收端网格蔡系统的无量纲状态方程为

$$\begin{aligned} x'(n+1) &= ax'(n) + by'(n) + c\mathrm{sgn}(x'(n)) \\ &\quad + d\mathrm{sgn}(y'(n)), \\ y'(n+1) &= ep(n) + fy'(n) + ez'(n), \\ z'(n+1) &= gy'(n) + k\mathrm{sgn}(y'(n)) + hz'(n), \end{aligned} \quad (4)$$

式中 $p(n) = x(n) \wedge S(n)$，解密后的语音信号 $S'(n) = x'(n) \wedge x(n)$.

本实验是在同一型号的两块 FPGA 开发板中实现，其中信道传输中采用了 RS-232 串口(如图 3 所示)，其传输速率为 115200bit/s，注意要用交叉线传输. 即使在相同的开发板，在实际应用中，由于存在晶振误差，所以频率还是有所不同的，所以不能采用相同的时间间隔迭代驱动和响应系统的方程的方法进行同步，通过实验验证了此方法听到的语音还是有杂音，并且杂音成周期性. 通过以上的实验，我们在响应系统加上密码同步检测模块，这样就能很好的进行同步. 可见，实现保密通信的关键是实现驱动和响应系统混沌序列发生器的自同步，理论分析和 FPGA 硬件实验证明，如果发送器和接收器的初始状态不同，则经过短暂的瞬态过程，系统就能达到同步. 若信道传输有瞬间的误差，经过短暂的瞬态过程后，系统能恢复解密.

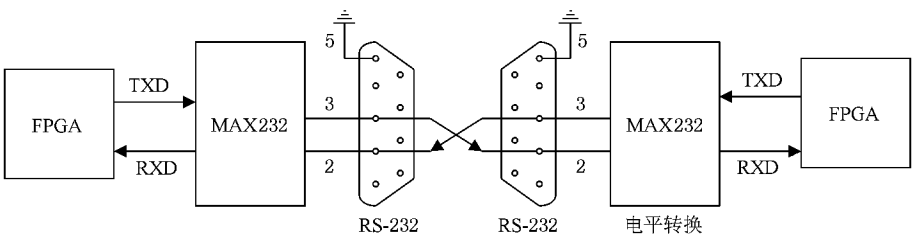

图 3　两块 FPGA 加密语音信号的串口传输原理图

5. 加密与解密算法分析

通过配置 WM8731 语音芯片,模拟语音信号经过取样、量化、编码变成 16 位串行二进制数据流,我们根据控制时钟把 16 位串行数据转换为 16 位的并行数据,这 16 位数字语音信号用行向量表示为 $S = [S_{15}\quad S_{14}\quad \cdots\quad S_1\quad S_0]$.基于数字语音信号置乱扩展机理.利用网格状蔡系统的混沌序列构造规则的矩阵 P,在此称为置乱扩展矩阵. P 是一个 $m \times n$ 矩阵,其数学表达式为

$$P = \begin{bmatrix} P_{11} & P_{12} & \cdots & P_{1n} \\ P_{21} & P_{22} & \cdots & P_{2n} \\ & & & \\ P_{m1} & P_{m2} & \cdots & P_{mn} \end{bmatrix}, \tag{5}$$

式中 m 的取值与并行语音信号位数相同,所以 $m = 16$.由于我们采用的是 IEEE-754 浮点数双精度标准,所以取 $n = 64$. 16 位语音信号行向量 $S = [S_{15}\quad S_{14}\quad \cdots\quad S_1\quad S_0]$ 与 P 矩阵进行相乘就可以把并行语音信号进行置乱扩展,得

$$M = S \times P = [S_{15}\quad S_{14}\quad \cdots\quad S_1\quad S_0] \times \begin{bmatrix} P_{11} & P_{12} & \cdots & P_{1,64} \\ P_{21} & P_{22} & \cdots & P_{2,64} \\ & & & \\ P_{16,1} & P_{16,2} & \cdots & P_{16,64} \end{bmatrix} = [M_{63}\quad M_{62}\quad \cdots\quad M_1\quad M_0], \tag{6}$$

M 就是经置乱扩展后的隐藏了语音的 64 位并行信号,采用混沌密钥 $X(n)$ 对此并行信号进行加密的过程为 $C = X(n) \oplus M$,得密文 $C = [C_{63}\quad C_{62}\quad \cdots\quad C_1\quad C_0]$,在加密的过程中我们根据密钥的指数不同选择置乱扩展矩阵 P(如图 4 所示).这样就可以使语音信号的置乱度进一步提高,抗破译性增强.具体方法是把 P 矩阵分为 P_1 和 P_2 两部分,即

$$P_1 = \begin{bmatrix} P_{1,1} & P_{1,2} & \cdots & P_{1,16} \\ P_{2,1} & P_{2,2} & \cdots & P_{2,16} \\ & & & \\ P_{16,1} & P_{16,2} & \cdots & P_{16,16} \end{bmatrix},$$

$$P_2 = \begin{bmatrix} P_{1,17} & P_{1,18} & \cdots & P_{1,64} \\ P_{2,17} & P_{2,18} & \cdots & P_{2,64} \\ & & & \\ P_{16,17} & P_{16,18} & \cdots & P_{16,64} \end{bmatrix}. \tag{7}$$

在(7)式中,S 和 P_1 相乘得到 $M_1 = [M_{63}, M_{62}, \cdots, M_{50}\quad M_{49}]$,这些位和混沌密钥的符号位、指数位、尾位的前四位要进行异或得到的部分密文 $C_1 = [C_{63}\quad C_{62}\quad \cdots\quad C_{50}\quad C_{49}]$,由于密文还要作为系统的迭代值,所以 $P_1 = 0$ 才能保证这些位是不被改变,否则混沌吸引子将会收敛或发散. P_2 矩阵是由单位矩阵经初等变换而来,故 P_2 每一行必定有一个单位 1,每一列最多只能有一个单位 1,数学表达式为

$$P_2 = \begin{bmatrix} 0 & P_{1,i_1} & \cdots & 0 & 0 & 0 \\ 0 & 0 & \cdots & 0 & P_{1,i_2} & 0 \\ & & & \ddots & & \\ 0 & 0 & P_{1,i_{48}} & \cdots & 0 & 0 \end{bmatrix}, \tag{8}$$

式中 $P_{1,i_1} = P_{1,i_2} = \cdots = P_{1,i_{48}} = 1$, $i_1, i_2, \cdots, i_{48} = 17-64$, $i_1 \neq i_2 \neq \cdots \neq i_{48}$.

满足这样条件的 P_2 矩阵总共有 P_{49}^{16}(约为 5×10^{25})种,在加密的时候根据指数的大小来选择不同的矩阵,这样语音信号就可以很好的隐藏.密码分析者就很难知道语音信号和混沌密钥异或的具体的位置,因为异或位置根据指数随时在变,只有系统设计者才知道指数和矩阵对应的函数关系.这样就使系统的安全性能进一步提高.

解密算法是上述加密算法的逆过程,解密过程为 $M = X'(n) \oplus C$,根据 $X'(n)$ 的指数 $e'(n)$ 来选择 P 矩阵,因为 P 是奇异矩阵,所以存在 P 的逆矩阵 P^{-1},那么解密后的语音 $S' = M \times P^{-1}$;具体的过程如图 5 所示.

加密算法和解密算法的从结构上来说,它是一种对称的算法.构造置乱扩展矩阵,混沌序列的产生采用了 IEEE-754 的浮点数算法标准,产生的 $x(n)$, $y(n)$, $z(n)$ 混沌序列具有更强的伪随机特性,根据混沌序列的指数选择置乱扩展矩阵,从而提高语音

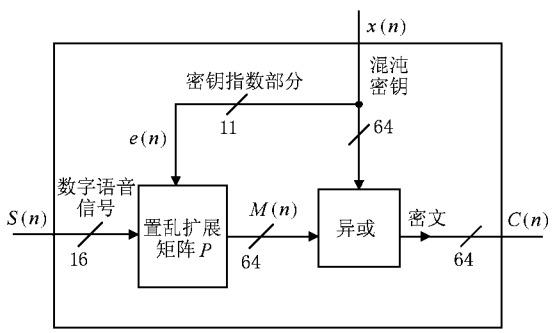

图 4 加密算法原理图

数据流置乱程度和算法的破译难度；网格蔡氏混沌系统对系统参数和初始值高度敏感性，使得算法的密钥空间非常大，在加密端可任意选择密钥.

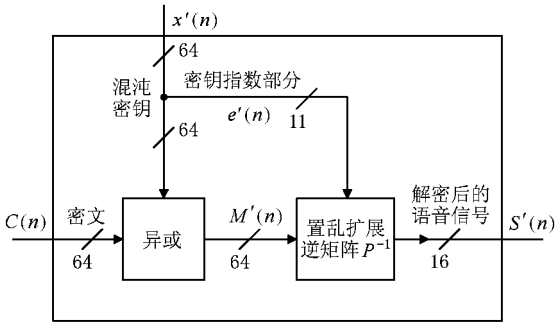

图 5　解密算法原理图

6. 硬件实现结果及其安全性能

根据图 2 至图 5 所示的方案进行实验，得如图 6 所示的硬件实验结果.其中图 6(a)为发送端电路经 $S(n)$ 调制后的 2×2 网格状多涡卷蔡氏吸引子，图 6(b)为 $x(n)-x'(n)$ 同步相图，图 6(c)为参数匹配情况下的实现结果，其中上图为输入的语音信号 $S(n)$，下图为解调后的 $S'(n)$，除有一定延时外，语音还原质量较好.在不正确解调的情况下所得的结果如图 6(d)所示.当发送端和接收端参数不严格匹配时，例如，发送端参数 $a=0.989$，接收端的参数 $a=0.989009$，其余参数相同，通过实验解调的信号产生严重失真，如图 6(e)所示.对于其他参数失配的情况，也有类似的结果.由此可见，本方案的混沌通信对参数匹配的要求很高，其安全性首先体现在对发送端与接收端的参数失配有较高的敏感性，因此，混沌方程的参数就相当于密钥，在窃听一方事先不知道发送端混沌方程参数的情况下，难以破译出有用信号.只有使收发两端参数达到严格的匹配，才能将有用信息解调出来.更为重要的是，由于本方案采用了传统加密与混沌加密相结合的算法，其中加密算法采用了置乱扩展矩阵技术，实现了混沌加密体制与传统密码体制的结合，密码分析者不仅需要破译系统的参数，还要破译其加密算法矩阵，进一步增加了破译的难度.

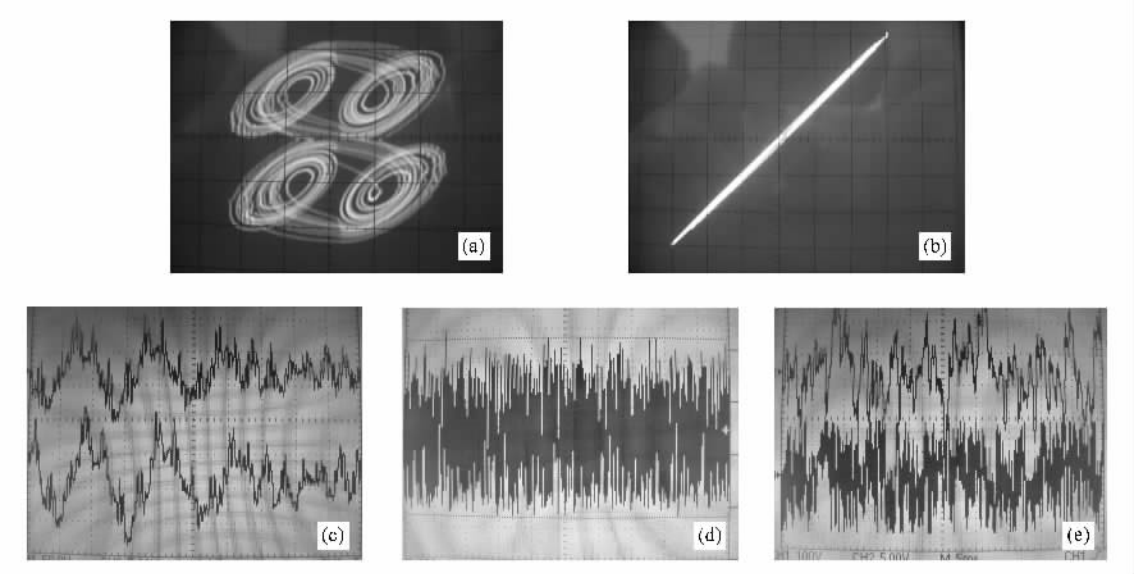

图 6　语音混沌保密通信的硬件实现结果　(a)经 $S(n)$ 调制后的 2×2 网格混沌吸引子；(b) $x(n)-x'(n)$ 同步相图；(c)正确解调的音乐信号；(d)不正确解调的信号；(e)参数失配情况下的信号解调

7. 结　论

提出并实现了一种具有应用价值的语音混沌保密通信系统方案，该方案的硬件与软件设计可行.在混沌数字通信系统设计中，数字混沌序列的产生是一个十分重要的问题，它直接影响到通信系统的硬件实现.在本方案中，采用了 IEEE-754 标准的浮点运算来产生数字混沌序列，进而提出了一种基于 IEEE-754 标准和 FPGA 技术的混沌数字保密通信系统的设计方案，实现了混沌加密体制与传统密码体制的相结合，给出了一种基于网格蔡氏混沌系统的

置乱扩展混沌加密算法,利用该方案进行了数字语音混沌保密通信的 FPGA 硬件实验研究.实验结果表明,该方案具有实时性较好,保密性较高的特点.需要说明的是,该方案不仅可用于语音保密通信,还可以用于传送机密二进制文件等.后续的工作需要解决的问题是如何通过以太网的传输实现,我们将做进一步的报道.

[1] Lorenz E N 1963 *J. Atmos. Sci.* **20** 130

[2] Chen G R, Lü J H 2003 *Dynamics of the Lorenz System Family: Analysis, Control, and Synchronization* (Beijing: Science Press) (in China) [陈关荣、吕金虎 2003 Lorenz 系统族的动力学分析、控制与同步 (北京 科学出版社)]

[3] Chua L O, Komuro M, Matsumoto T 1986 *IEEE Trans. Circuits Syst.* Ⅰ **33** 1072

[4] Elwakil A S, Kennedy M P 2001 *IEEE Trans. Circuits Syst.* Ⅰ **48** 289

[5] Elwakil A S, Özoguz S, Kennedy M P 2002 *IEEE Trans. Circuits Syst.* Ⅰ **49** 527

[6] Özoguz S, Elwakil A S, Kennedy M P 2002 *Int. J. Bifurc. Chaos* **12** 1627

[7] Chen A M, Lu J A, Lü J H, Yu S M 2006 *Physica* A **364** 103

[8] Suykens J A K, Vandewalle J 1993 *IEEE Trans. Circuits Syst.* Ⅰ **40** 861

[9] Yalcin M E, Suykens J A K, Vandewalle J 2000 *IEEE Trans. Circuits Syst.* Ⅰ **47** 425

[10] Yalcin M E, Suykens J A K, Vandewalle J 2002 *Int. J. Bifurc. Chaos* **12** 23

[11] Tang K S, Zhong G Q, Chen G R 2001 *IEEE Trans. Circuits Syst.* Ⅰ **48** 1369

[12] Zhong G Q, Man K F, Chen G R 2002 *Int. J. Bifurc. Chaos* **12** 2907

[13] Yu S M, Qiu S S, Lin Q H 2003 *Sci. Chin.* F **46** 104

[14] Yu S M, Ma Z G, Qiu S S, Lin Q H 2004 *Chin. Phys.* **13** 317

[15] Yu S M, Lin Q H, Qiu S S 2004 *Acta Phys. Sin.* **53** 2084 (in Chinese) [禹思敏、林清华、丘水生 2004 物理学报 **53** 2084]

[16] Yu S M 2004 *Acta Phys. Sin.* **53** 4111 (in Chinese) [禹思敏 2004 物理学报 **53** 4111]

[17] Yu S M 2005 *Acta Phys. Sin.* **54** 1500 (in Chinese) [禹思敏 2005 物理学报 **54** 1500]

[18] Yu S M, Lü J H, Leung H, Chen G R 2005 *IEEE Trans. Circuits Syst.* Ⅰ **52** 1459

[19] Lü J H, Yu S M, Leung H, Chen G R 2006 *IEEE Trans. Circuits Syst.* Ⅰ **53** 149

[20] Yu S M, Lü J H, Chen G R 2007 *IEEE Trans. Circuits Syst.* Ⅰ **54** 2087

[21] Yu S M, Lü J H, Tang K S, Chen G R 2006 *Chaos* **16** 033126

[22] Yu S M, Lü J H, Chen G R 2007 *Chaos* **17** 013118

[23] Yu S M, Tang K S, Chen G R 2007 *Int. J. Bifurc. Chaos* **17** 3951

[24] Lü J H, Chen G R 2006 *Int. J. Bifurc. Chaos* **16** 775

[25] Liu F, Liu S D, Liu G, Liu S K 2007 *Acta Phys. Sin.* **56** 5629 (in Chinese) [刘 峰、刘式达、刘 刚、刘式适 2007 物理学报 **56** 5629]

[26] Chen L, Wang D S 2007 *Acta Phys. Sin.* **56** 5661 (in Chinese) [谌 龙、王德石 2007 物理学报 **56** 5661]

[27] Peng F, Qiu S S, Long M 2005 *Acta Phys. Sin.* **54** 4562 (in Chinese) [彭 飞、丘水生、龙 敏 2005 物理学报 **54** 4562]

[28] Wang L, Wang F P, Wang Z J 2006 *Acta Phys. Sin.* **55** 3964 (in Chinese) [王 蕾、汪芙平、王赞基 2006 物理学报 **55** 3964]

[29] Li Y X 2008 *J. Commu.* **29** 46 (in Chinese) [李育贤 2008 通信学报 **29** 46]

[30] Yan S L 2005 *Acta Electro. Sin.* **33** 267 (in Chinese) [颜森林 2005 电子学报 **33** 267]

[31] Liu F C, Liang X M, Song J Q 2008 *Acta Phys. Sin.* **57** 1458 (in Chinese) [刘福才、梁晓明、宋佳秋 2008 物理学报 **57** 1458]

[32] Yu N, Ding Q, Chen H 2007 *J Commu.* **28** 73 (in Chinese) [于娜、丁 群、陈 红 2008 通信学报 **28** 73]

[33] Zhang Y, Chen T Q, chen B 2007 *Acta Phys. Sin.* **56** 56 (in Chinese) [张 勇、陈天麒、陈 滨 2006 物理学报 **56** 56]

[34] Yan S L, Wang S Q 2006 *Acta Phys. Sin.* **57** 1687 (in Chinese) [颜森林、汪胜前 2006 物理学报 **55** 1687]

[35] Sun L, Jiang D P 2006 *Acta Phys. Sin.* **55** 3283 (in Chinese) [孙 琳、姜德平 2006 物理学报 **55** 3283]

[36] Zhang P S, Zhu Y S 2007 *J. Electro. Infor. Techn.* **29** 2359 (in Chinese) [赵柏山、朱义胜 2007 电子与信息学报 **29** 699]

[37] Qiu S S, Cheng Y F, Wu M, Ma Z G, Yu S M, Liu X Y 2002 *J. South China Univ Techn.* **30** 76 (in Chinese) [丘水生、陈艳峰、吴 敏、马在光、禹思敏、刘雄英 2006 华南理工大学学报 **30** 76]

[38] Long M, Qiu S S, Peng F 2006 *Chin. J. Radio Scien.* **21** 74 (in Chinese) [龙 敏、丘水生、彭 飞 2006 电波科学学报 **21** 74]

[39] He H J, Zhang J S 2006 *J. Commu.* **27** 80 (in Chinese) [和红杰、张家树 2008 通信学报 **27** 80]

[40] Li J F, Li N, Li H 2004 *Acta Phys. Sin.* **53** 1694 (in Chinese) [李建芬、李 农、林 辉 2004 物理学报 **53** 1694]

[41] Xie K, Lei M, Feng Z J 2005 *Acta Phys. Sin.* **54** 1694 (in Chinese) [谢 鲲、雷 敏、冯正进 2005 物理学报 **54** 1694]

[42] Cai Y, Zhang J S 2003 *J. China Railw Socie.* **25** 61 (in Chinese) [蔡 颖、张家树 2006 铁道学报 **25** 61]

[43] Sun K H, Zhou J L, Mou J 2007 *J. Electro. Infor. Techn.* **29** 2436 (in Chinese) [孙克辉、周家令、牟 俊 2007 电子与信息学报 **29** 2436]

[44] Yu Z B, Feng J C 2008 *Acta Phys. Sin.* **57** 1409 (in Chinese) [余振标、冯久超 2008 物理学报 **57** 1409]

[45] Wang F P, Wang Z J, Guo J B 2003 *Acta Electro. Sin.* **31** 127 (in Chinese) [汪芙平、王赞基、郭静波 2003 电子学报 **31** 127]

[46] Li W, Hao J H, Qi B 2008 *Acta Phys. Sin.* **57** 1398 (in Chinese) [李　伟、郝建红、祁　兵 2008 物理学报 **57** 1398]

[47] Han J Q, Zhu Y S 2006 *J. Electro. Infor. Techn.* **28** 2359 (in Chinese) [韩建群、朱义胜 2006 电子与信息学报 **28** 2359]

[48] Yu S M, Lü J H 2007 *Proc. 26th Chinese Contr. Conf.* **6** 404 (in Chinese) [禹思敏、吕金虎 2007 第 26 届中国控制会议论文集 **6** 404(湖南，张家界，北京航空航天大学出版社)]

[49] Liao N H, Gao J F 2006 *J. Electro. Infor. Techn.* **28** 1255 (in Chinese) [廖旎焕、高金峰 2006 电子与信息学报 **28** 1255]

[50] Zhang Z M, Wang J 2006 *Chin. J. Radio Scien.* **21** 895 (in Chinese) [张正明、王　金 2006 电波科学学报 **21** 895]

[51] Zhang J S, Xiao X C 2001 *Acta Phys. Sin.* **50** 2121 (in Chinese) [张家树、肖先赐 2001 物理学报 **50** 2121]

[52] Wang Y F, Sheng H B, Yang X L 2006 *J. zhengjiang Univ.* **40** 1726 (in Chinese) [王云峰、沈海斌、严晓浪 2006 浙江大学学报 **40** 1726]

[53] Hu J F, Guo J B 2008 *Acta Phys. Sin.* **57** 1477 (in Chinese) [胡进峰、郭进波 2008 物理学报 **57** 1477]

[54] Zhou W J, Yu S M 2008 *Acta Phys. Sin.* **57** 4738 (in Chinese) [周武杰、禹思敏 2008 物理学报 **57** 4738]

Chaotic digital communication system based on field programmable gate array technology—Design and implementation*

Zhou Wu-Jie†　Yu Si-Min

(*College of Automation, Guangdong University of Technology, Guangzhou* 510006, *China*)

(Received 1 June 2008; revised manuscript received 13 July 2008)

Abstract

A novel universal approach for design and implementation of chaotic digital communication system based on IEEE-754 standard and field programmable gate array technology (FPGA) is proposed, combing chaos encryption with traditional cipher realization. By using the Euler algorithm and appropriate discrete processing, the continuous chaotic system is converted to a discrete chaotic system. Using FPGA hardware design system, digital chaotic sequence is generated as the key. Scrambling and expansion encryption algorithm is realized and analyzed. Driven and response of secure communication system is designed by constructing a loop including the signal and achieving chaotic synchronization between sender and receiver. Taking grid Chua chaotic system as an example, the secure communication system using FPGA hardware platform is implemented. The technical development process, algorithm flow chart, hardware design and realization result are also given.

Keywords: grid multi-scroll Chua's circuit, scrambling and expanding matrix, field programmable gate array technology, chaotic digital communication system

PACC: 0545

* Project supported by the National Natural Science Foundation of China (Grant Nos. 60572073, 60871025), the Natural Science Foundation of Guangdong Province (Grant Nos. 8151009001000060, 8351009001000002).

† E-mail: wujiezhou@163.com