Computer Science and Application 计算机科学与应用, 2015, 5, 125-132
Published Online April 2015 in Hans. http://www.hanspub.org/journal/csa
http://dx.doi.org/10.12677/csa.2015.54016

Hans汉斯

Research on Mixed Encryption of DES and LFSR and FPGA Implementation

Yu Gang[1,2], Yongjun Wen[1,2*], Min Deng[1,2], Weixuan Xia[1,2], Feng Bin[1,2], Wenpin Liao[1,2], Lijun Tang[1,2*]

[1]Hunan Province Higher Education Key Laboratory of Modeling and Monitoring on the Near-Earth Electromagnetic Environments (Changsha University of Science & Technology), Changsha Hunan
[2]Department of Physics and Electronic Science, Changsha University of Science and Technology, Changsha Hunan
Email: *doudou.wen@163.com, *tanglj2000@263.net

Received: Apr. 28th, 2015; accepted: May 14th, 2015; published: May 20th, 2015

Abstract

With the growing of network information, the issue of information security has become the bottleneck of the development of network source application. This paper aimed at file's security in the computer and Internet, and researched on DES encryption algorithm and the algorithm of LFSR. Based on above algorithms, we designed a mixed encrypted method realized by FPGA; according to the password combination that is inputted by the user, a bunch of keys will be produced by LFSR and sent to computer by USB. The function of software on the computer is communicating with USB chip and encrypting files with DES algorithm. The results showed that this scheme has good effect and high processing speed on encrypting any certain files, and has a good effect for protecting files on network space.

Keywords

DES Encryption Algorithm, LFSR, FPGA, Encrypting Files

DES和LFSR混合加密的研究与FPGA实现

刚　煜[1,2]，文勇军[1,2*]，邓　敏[1,2]，夏伟轩[1,2]，宾　峰[1,2]，廖文平[1,2]，唐立军[1,2*]

[1]近地空间电磁环境监测与建模湖南省普通高校重点实验室(长沙理工大学)，湖南 长沙

*通讯作者。

[2]长沙理工大学物理与电子科学学院，湖南 长沙
Email: *doudou.wen@163.com, *tanglj2000@263.net

收稿日期：2015年4月28日；录用日期：2015年5月14日；发布日期：2015年5月20日

摘 要

随着网络信息交流量日益增长，信息安全问题成了网络资源应用的发展瓶颈。本文针对计算机与网络上文件的安全性问题，对DES算法以及LFSR密码生成算法进行研究，设计了基于DES和线性反馈移位寄存器(LFSR)的混合加密算法并通过FPGA实现，FPGA根据用户输入的密码组合，通过线性反馈移位寄存器产生一串密钥，然后通过USB将这串密钥发送至计算机中。上位机软件实现与下位机的USB通讯、用DES算法对任意文件进行加密和解密的功能。结果表明，该方案对任意文件加密效果好、速度较快，对于网络空间文件保护有较好的效果。

关键词

DES加密算法，LFSR，FPGA，文件加密

1. 引言

随着 21 世纪网络信息时代的到来，网络空间上的文件保护问题成为了人们应用网络空间的心病。如何保护文件里的信息不被泄漏、保证文件的保密性和安全性是各行各业都很重视的课题，无论是政府、企业还是个人都逐渐依赖计算机存储信息，并借助网络传递、交换重要资料和洽谈贸易。这些信息无论是私人信息还是部门信息，无论是军用信息还是商业信息，在进行处理和传递前要以电子文档的形式存储在单机、服务器或网络上任意一台客户机上，因此电子文档的安全存储成为实现信息安全的首要条件[1]。

针对网络信息安全性问题，CESVMC (Computable Encryption Scheme based on Vector and Matrix Calculations)加密方案，提升了数据存储、运算过程中的安全性，但运算时间比较长，存储和通信的负载较大[2]。通过软件运算进行加密与使用硬件进行加密相比，软件加密更容易破解。本文利用软件硬件各自的优势，取长补短，将 FPGA 用于加密算法设计，探索一个以 FPGA 为核心加密方案。

2. DES 和 LFSR 混合加密

2.1. DES 算法介绍

数据加密标准(Data Encryption Standard, DES)是由 IMB 公司研究发表，美国国家标准与技术研究院于 1977 年标准化的，目前最广泛应用的用于加密机密信息的加密方法[3]-[5]。

DES 算法的加密由四部分完成，分别为：初始置换函数 IP、子密钥 Ki、密码函数 F、末置换函数 IP-1 [6] [7]。DES 算法需要用户提供一共 64 位长度的密钥用于加密与解密。算法可以提供高质量的数据保护，具有相当高的复杂性，实行经济而且运行效率高[8]。

DES 算法只用到了 64 位密钥中的其中 56 位，还有 8 位并未参与 DES 运算，随着计算机的发展计算机运行速度越来越快，使得使用暴力破解法破解 DES 密钥的时间越来越短。为了保证使用 DES 算法的安全性，一般需要采用多重 DES 算法和 AES 加密算法，加长密钥的长度，增强 DES 安全性。

2.2. 线性反馈移位寄存器(LFSR)

一个 n 级反馈移位寄存器如图 1 所示，其中 $f(s_1,s_2,\cdots,s_n)$ 称为反馈函数，当 $f(s_1,s_2,\cdots,s_n)$ 为一线性函数时，则称上图的反馈移位寄存器为线性反馈移位寄存器(Linear Feedback Shift Register, LFSR) [9]。线性反馈移位寄存器具有非常适合硬件实现、能产生大的周期序列、能产生好的统计特性的序列、易于使用代数方法进行结构分析的特点[10]-[12]。

可设 n 级线性反馈移位寄存器的反馈函数：

$$f(s_1,s_2,\cdots,s_n)=c_n s_1 \oplus c_{n-1}s_2 \oplus \cdots \oplus c_1 s_n \tag{1}$$

其中 $C_i\ (i=1,2,\cdots,n-1)$ 为 0 或者 1，一般 C_n 都为 1。

由于反馈函数是作为最后一级的输入，又根据移位寄存器的特点，反馈的结果会在 n 个时刻之后输出，于是可以推导出输出序列$\{s_i\}$：

$$s_{n+k}=c_n s_{n+k-1} \oplus c_{n-1}s_{n+k-2} \oplus \cdots \oplus c_1 s_k \tag{2}$$

可以看出 S_{n+k} 与过去最近的 n 个时刻的输出 S_i 都有关系。

本设计的密钥生成模块采用带有适当的反馈函数的 LFSR 结构，使输出的 56 位密钥与 128 位的初始密钥都相关。当 LFSR 需要用作流密码器设计时，一般要求 LFSR 可以产生最大周期的密钥流，而当 n 级 LFSR 的反馈函数是本原多项式时，LFSR 输出的可以达到最大周期 $2n-1$。这里 LFSR 的作用是令 128 位长度的初始密钥的每一位都至少与输出的 56 位长度的密钥中的一位相关。因此，可以根据需求设计 LFSR 的结构，而不必将其反馈函数设计成本原多项式。

本设计用户输入的原始密钥长度是 128 位，因此，需采用 128 级的 LFSR 结构。为了简化设计，可以令输出的 56 位密钥是连续输出的。基于这几个条件要求，式(2)中，$n=128$，$k\in[a+1,a+56]$，$a\in[0,+\infty)$，则式(2)可以改写成：

$$s_{128+k}=c_{128}s_{128+k-1} \oplus c_{127}s_{128+k-2} \oplus \cdots \oplus c_1 s_k \tag{3}$$

如果每一个环节都接一个反馈的话，程序的工作量会比较大，因此可以进行以下简化，由于 k 是连续递增变化的，可令反馈函数 f 在每连续 56 个环节之内至少有一个反馈环节，取 c_1，c_{57}，c_{113}，c_{128} 的值为 1，其它 c_i 值为 0，因此，根据式(1)、式(2)以及式(3)，本设计的 LFSR 的输出可以表示为：

$$S_{128+k}=S_{112+k} \oplus S_{56+k} \oplus S_k \tag{4}$$

根据式(4)，可以得出 LFSR 结构如图 2 所示。若输出的 56 位密钥在 LFSR 输出第 128 位之后，就可保证初始密钥每一位都与输出密钥相关。该方法的优点是产生密钥速度快，但直接加密会带来传输速度慢等问题。

2.3. DES 算法与 LFSR 的混合加密方法

综合上述的方法，采取 LFSR 方法生成密钥，将 LFSR 与 DES 相结合进行加密的方案，即可提高速度，又可增加安全性。具体实现方法如下。

在硬件上，FPGA 根据键盘输入的密码通过 LFSR 产生密钥之后，通过 USB 芯片传送给加/解密程序。软件上，加/解密程序将接受的密钥全部接受后再次通过 DES 算法产生子密钥，读取计算机上的文件然后进行加/解密，操作全部完成后删除原文件，从而完成对计算机上文件的加/解密，达到对计算机上文件的保护目的。

该方法允许用户输入密码组合长度最高可以达到 16 位，可能的密码组合的个数超过 1016 个。但是如果输入的密码长度是 16 位，由上面的描述可知，每一位密码都代表一个 8 位的 KeyValue，16 位的密

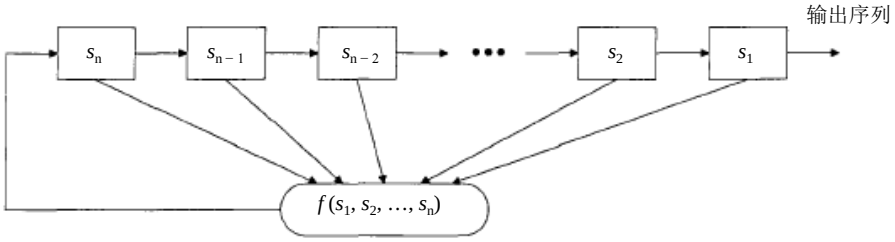

Figure 1. Linear feedback shift register
图 1. 线性反馈移位寄存器

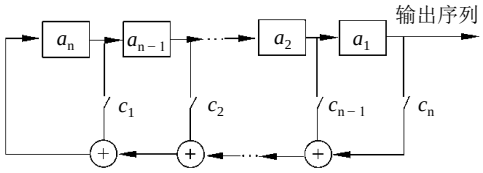

Figure 2. Framework of linear feedback shift register
图 2. 线性反馈移位寄存器的结构

码长度代表整个密钥长度为 128 位，当攻击者不知道每一个键值所代表的 KeyValue 时，可能的组合就有 $2^{128}-1$ 个，因此，可以保证足够的安全性。

但 128 位长度超出了 DES 所需要的密钥长度，即用户输入的密码会有一部分无效。因此必须设计一种密钥生成方案，使输入的 128 位密钥中每一位至少与输出的 56 位长的密钥每一位相关的，这种方案可通过 FPGA 实现，但必须考虑尽量低的硬件复杂度，图 3 为加密系统结构框图。

3. FPGA 实现方法

FPGA 加密器由上位机程序以及硬件装置构成，硬件装置由 FPGA 最小系统电路、USB 芯片工作电路、按键电路构成，相关电路设计方案如下。

3.1. USB 芯片 CY7C68013A 电路设计

USB 芯片 CY7C68013A 电路共由 CY7C68013A 芯片电路、24MHz 晶振电路、EEPROM 电路、Mini USB 接口与 CY7C68013A 连接电路构成，其电路原理图如图 4 所示。

时钟信号是芯片正常工作的必要条件，24 MHz 晶振电路为 CY7C68013A 芯片提供外部参考时钟信号。Mini USB 接口通过 D−和 D+两个网络与 CY7C68013A 芯片相连接。通过这个 Mini USB 接口，用户可以用数据线将硬件装置与计算机连接起来。USB 数据通过差分线路 D−和 D+在硬件装置和计算机之间传递。需要从计算机读取数据时，D−和 D+的数据进入 USB 芯片后芯片会自行对数据进行解码，将解码后的数据存进 FIFO 缓冲区，供 FPGA 读出。当 FPGA 需要向计算机发送数据时，通过 FD[0..7]向芯片发送数据，然后芯片会自动将接收到的数据编码，然后将编码后的数据通过 D−和 D+发送至计算机中。Mini USB 接口的作用还有通过 USB 上的 5 V 供电为整个硬件装置提供电能。EEPROM 电路用于储存每次复位或者上电后 USB 芯片读取的固件程序。

3.2. FPGA 电路设计

本文采用的 FPGA 芯片是 Altera 公司 Cyclone II 系列的 EP2C5T144C8N 芯片，其电路由 FPGA 供电电路、JTAG 电路、FPGA 配置电路、FPGA 外部时钟电路组成，其原理图如图 5 所示。

FPGA 供电电路使用 3.3 V 电源为各个电源引脚提供电压，1.2 V 电源为 FPGA 内部的逻辑元件提供

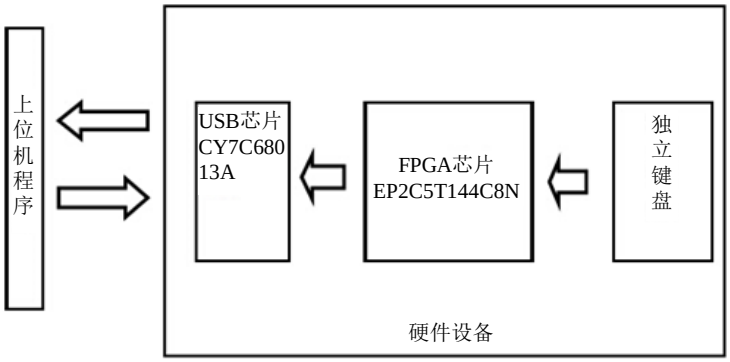

Figure 3. The overall design of encryption device
图 3. 加密器系统结构框图

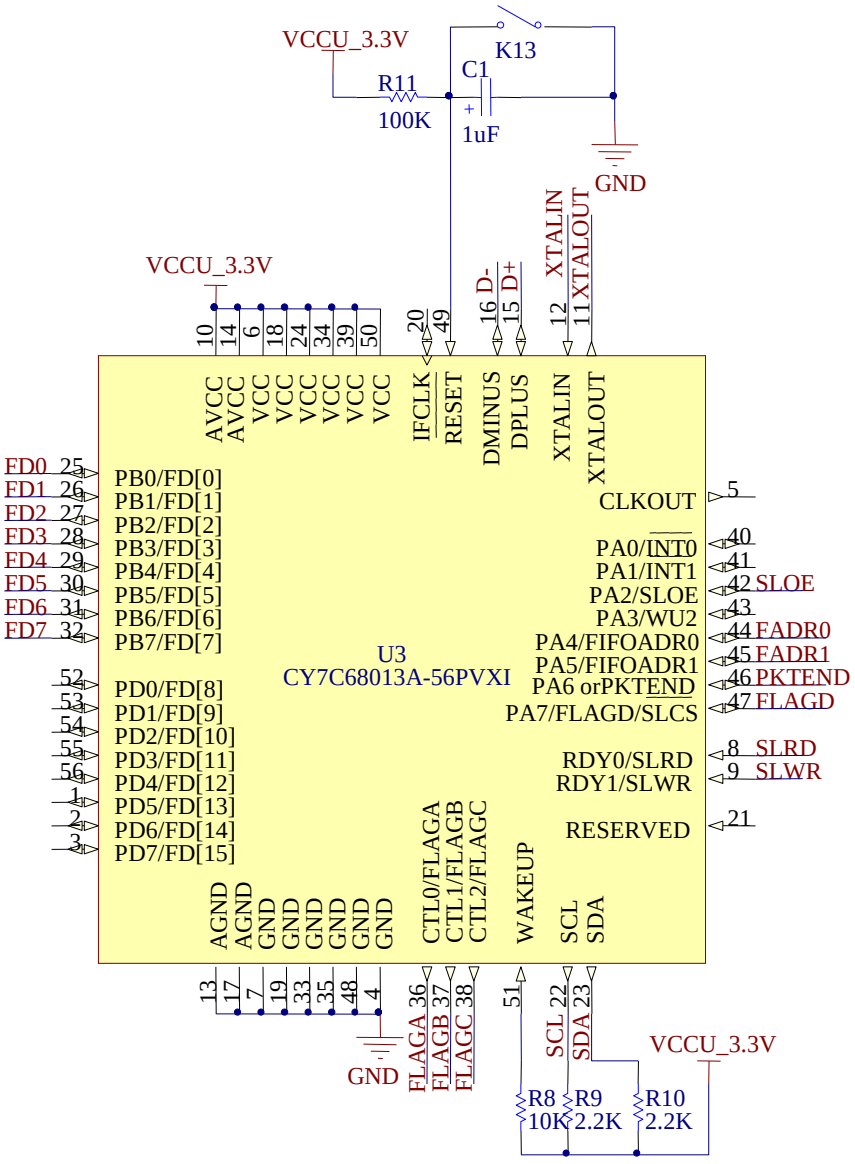

Figure 4. The schematic of CY7C68013 circuit
图 4. CY7C68013 电路原理图

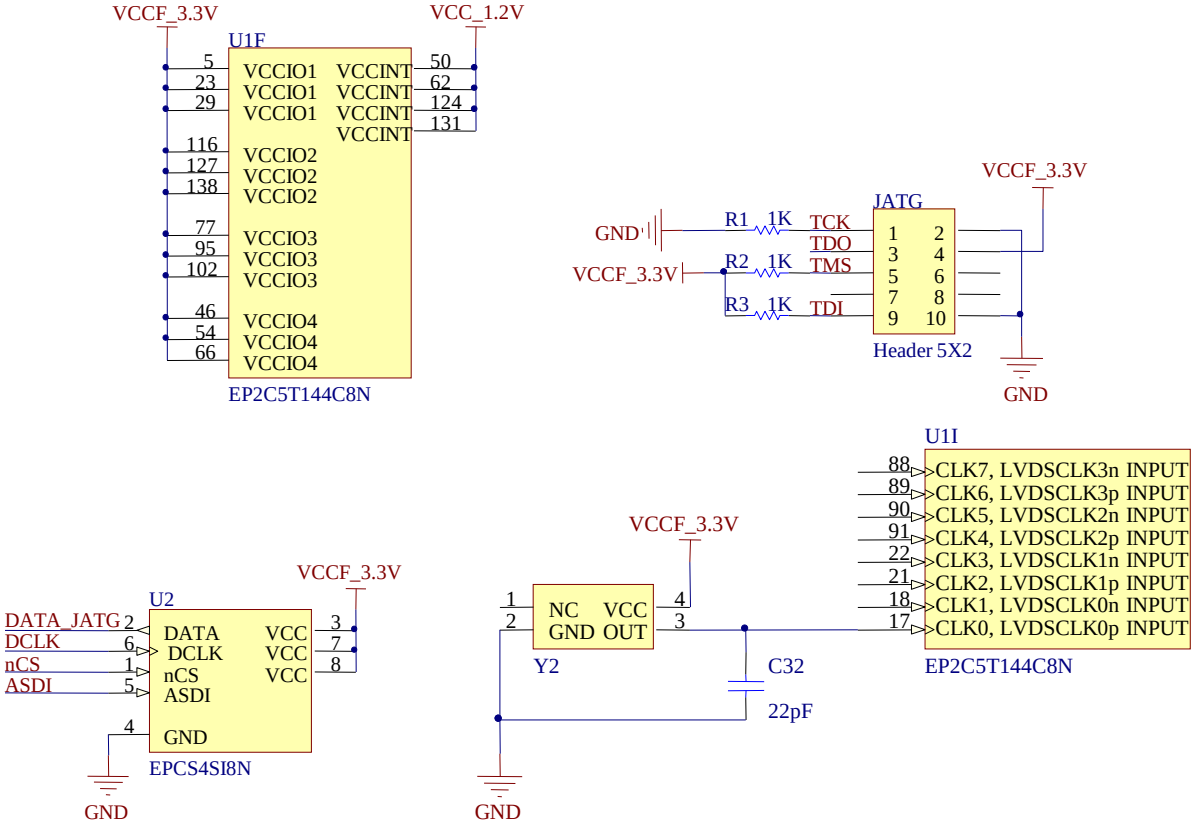

Figure 5. The schematic of FPGA circuit
图 5. FPGA 电路原理图

电能。本设计使用的 JTAG 接口为 10 针 JTAG 接口，JTAG 电路使已经被综合好的 FPGA 逻辑下载至 FPGA 上进行在线调试工作。在 FPGA 配置电路中，本文使用 EPCS4SI8N 作为 FPGA 的配置芯片，每次复位或者掉电之后，FPGA 内储存配置信息的 RAM 里的数据便会丢失，所以需要配置芯片电路用于储存配置 FPGA 的配置信息，通过 JTAG 接口将由 sof 文件转化而来的 JIC (JTAG Indirect Configuration)文件下载到配置芯片中，通过这种模式下载可以简化电路的整体设计。外部时钟源是一片 50 MHz 的有源晶振，FPGA 时钟电路为 FPGA 提供参考时钟信号，以确保状态机、密钥生成、按键输入去抖等功能顺利实现。

3.3. FPGA 逻辑设计

整个 FPGA 逻辑设计主要分 3 部分设计：控制模块设计、密码输入模块设计以及密钥生成模块设计。本文使用 Verilog HDL 作为硬件描述语言来进行 FPGA 编程。其工作流程图如图 6 所示。

控制模块用于执行上电后软件全局复位、接收从 PC 机上发来的指令(0x01)、根据指令做出相应的响应三个操作。软件全局复位是为了确保 FPGA 逻辑中所有模块都可以同时复位，不会产生不确定的结果。其操作是通过对 50 MHz 主时钟的脉冲进行计数，当计数值小于设定值时复位信号保持低电平，让全局保持复位状态；当计数值等于设定值时，复位信号拉高，所有模块进入工作状态。当 FPGA 收到的来自计算机的指令后，控制模块会先把密码输入模块打开，等待用户输入密码。当用户输入密码完毕后，控制模块会禁止密码输入功能，然后打开密钥生成模块。密钥发生模块会自动将生成的密钥发送到计算机中。

密码输入模块用于执行接收输入密码、将不同的键值编码成不同的编码值和按下确定键后将整个密

钥送到 PR (密钥生成模块)中三个操作。人按下按键的时候，按键可能会处在反复在按下和松开两个状态中来回切换的状态，密码输入模块先进行消抖操作，然后将接收到的按键进行编码操作，当密码全部输入完成后根据按下的是发送键还是清除键对密码进行发送或者清空处理。

密钥生成模块的作用是把按键输入模块输出的数据接收，根据此数据通过线性反馈移位寄存器产生伪随机数列，再将数据送往 USB 芯片的缓存区中。

4. 验证及测试

把 FPGA 加密设备连接至计算机之后，计算机的上位机能识别加密器的 USB 设备并读取相关的 VID，PID。等待计算机使用者选择需要加密的文件之后，由使用者在独立键盘上输入密码，按下确认键之后 FPGA 将会把密钥通过 USB 芯片发至计算机中，计算机则开始进行加密操作，加密完成后计算机自动删除源文件并显示整个加密所消耗的时间，保留加密之后的文件，对于不同大小的文件其验证结果如表 1 所示。从表 1 可以看出，本加密器能够稳定的加密并还原计算机文件，加密和解密速度近 1 M/s。

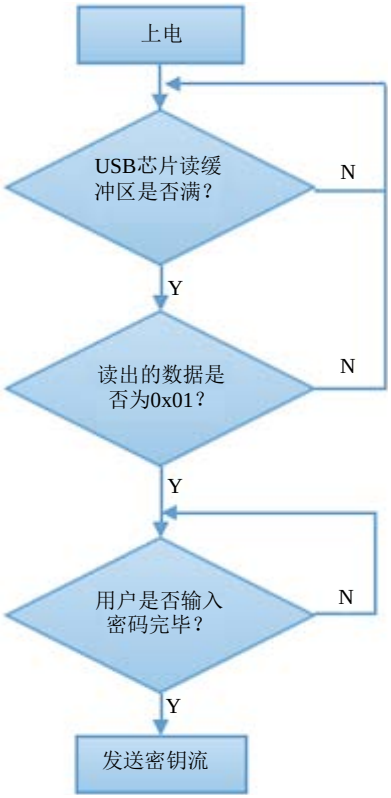

Figure 6. The working flow chart of FPGA
图 6. FPGA 的工作流程图

Table 1. The data of encryption rate
表 1. 加密速度测试数据

文件大小	加解密消耗时间
60 KB	62 ms
20 MB	20.79 s
50 MB	51.97 s

5. 结论

本文提出了一种基于线性反馈移位寄存器的加密计算机文件的方案，从理论上证明了这种方案的可行性并且通过 FPGA 实现。该方案结合了软件和硬件加密优势，具有很高的安全性，可应用于网络文件存储和传输，有一定的应用价值。

基金项目

国家科技支撑计划项目(2014BAH28F04)，湖南省重点学科，湖南省高校科技创新团队，湖南省教育厅科学研究项目(14C0031)，湖南省教学改革研究项目(湘教通[2013]223 号)。

参考文献 (References)

[1] 胡祥义, 徐冠宁, 杜丽萍 (2013) 基于云计算的文件加密传输方法. *网络安全技术与应用*, **5**, 18-22.

[2] 黄汝维, 桂小林, 余思, 庄威 (2011) 云环境中支持隐私保护的可计算加密方法. *计算机学报*, **12**, 2391-2402.

[3] 黄光明 (2013) 基于 DES_RSA 加密算法的改进与实现. 硕士论文, 东北师范大学, 沈阳.

[4] 邱世中 (2013) 基于 FPGA 的 DES 混沌加密算法实现与改进. 硕士论文, 广东工业大学, 广州.

[5] 吴明航 (2013) DES 和 RSA 混合加密算法的研究. 硕士论文, 哈尔滨工业大学, 哈尔滨.

[6] Hu, M.Y. (2014) Analysis and improvement of the security of DES algorithm. *WIT Transactions on Information and Communication Technologies*, **57**, 317-324.

[7] Alani, M.M. (2012) Neuro-cryptanalysis of des and triple-DES. *Lecture Notes in Computer Science*, **7667**, 637-646.

[8] 丁显信 (2013) DES 算法的硬件实现方法研究及 FPGA 实现. 硕士论文, 青岛科技大学, 青岛.

[9] 李鹏, 颜学龙, 孙元 (2014) 基于多配置 LFSR 的测试生成结构设计. *计算机工程与科学*, **5**, 814-820.

[10] 朱楠 (2010 基于 FPGA 的流密码机设计. 硕士论文, 西安电子科技大学, 西安.

[11] 肖旭韬, 张雪锋 (2013) 基于线性反馈移位寄存器和组合猫映射的伪随机序列生成方法. *计算机应用研究*, **1**, 161-164.

[12] 潘晓英 (2015) 基于线性反馈移位寄存器和分组密码的伪随机数生成方法. *通信技术*, **2**, 228-231.