基于网络空间安全的 LBlock 密码技术的研究与实现

张爽 梁亚楠

（黑龙江大学数据科学与技术学院，黑龙江哈尔滨 150000）

摘要：网络空间是人们生活发展的信息环境，在大数据时代，网络空间的安全显得尤为重要，而密码技术又是保障网络空间安全的重要手段。本文对轻量级密码算法 LBlock 密码算法进行了研究与实现，结合当前网络安全时代的大环境，像 AES 诸如此类的算法已经不能满足任何场合的需求，而 LBlock 这样的轻量级算法可以在更小、更低端的嵌入式设备中应用，它对硬件和运算体量的要求更小，在 C/C++ 的环境下对其进行了实现，同时分析了其安全性，LBlock 密码技术作为一种高效率的轻量级密码算法具有很高的研究价值，但本文中如交互界面和算法进一步优化仍有待提升。

关键词：网络空间安全；安全性分析；分组密码；LBlock 算法

中图分类号：TN915.08 **文献标识码：**A **文章编号：**2096-4609（2019）37-0256-002

一、前言

在科学技术不断的发展中，人类社会已经步入到了信息数据化的时代，也称之为“大数据时代”。

在大数据的时代，信息产业成为了第一大产业，与所有的行业和所有的人都息息相关。在这个由信息作为基础资源所构建的生存网络中，安全也成了至关重要的话题。

LBlock 加密算法作为一种轻量级分组密码，于 2011 年 ANCS 会议上由吴文玲等人提出。[1]

本文正是基于网络空间安全的背景下对 LBlock 加密算法进行安全性分析，同时在 C++/C 环境下对其进行实现，该算法采用类 Feistel 算法结构，同时其密钥扩展算法是采用了 Feistel 结构和 SPN 结构，故 LBlock 加密算法具有很高的理论价值和实用价值。

二、网络空间安全

（一）网络空间概述

网络空间是所有信息的集合，是人们生存的信息环境，因此必须确保网络空间的安全。如今人们所处的这个环境之下，可以说是人工智能和“大数据”横行的一个环境，各类人群所使用的 App 为提供更高效的服务而收集用户信息，然而却有很多心思不正的人窃取用户数据，故网络空间安全成了一个热点话题。

（二）网络空间安全主要研究内容

网络空间安全作为一门学科是融合了计算机、电子、通信、物理、数学、生物甚至更多门学科的有关知识，它以这些为依托，但从本质上又有着极大的差别。它有着自己完整且独立的体系，以密码学、网络安全、信息内容安全和信息对抗作为主要的研究内容。

三、分组密码技术

（一）分组密码的基本原理

分组密码的工作模式第一步是将明文分为相同长度的块，一般常见的有 64 比特或者 128 比特为一组，设明文数据序列为p_1，p_2，……每 m 个组成一组明文 $P=(p_1, p_2, \cdots\cdots, p_m)$，用来进行加密的密钥为 $K=(k_1, k_2, \cdots\cdots, k_t)$，明文 P 在加密密钥的作用下转换成密文，记作$C=(c_1, c_2, \cdots\cdots, c_n)$，即$C=\sum_k(P)$。

从数学科学的层面分析的话，就是说分组密码的加密函数实际上是从长度为 n 的集合上映射到另一个长度为 n 的集合上，解密过程是加密过程的逆运算。

（二）分组密码的研究意义

分组密码有着体积小、运行快的特点，在如今要求时效性的社会大趋势是吻合的，同时轻量级的密码算法对于一些计算力低、处理信息弱的一些硬件设备也可以广泛应用。

并且分组密码综合性很高，除去自身的一些特点外，还易于标准化，便于推广和被大众接受。同样的，分组密码的研究意义还在于它有着很大的提升空间。

分组密码这一密码体系相较于公钥密码在可证明安全性上有着一定的差距，而且，机密性和完整性作为密码算法设计的两大目标，分组密码在完整性这一方面还有所欠缺，在机密性上较于其它已经比较成熟。

无论是对比而言还是从自身而言，分组密码都可以成为当今社会密码算法研究的热点，具有重大的现实意义和研究价值。

四、LBlock 加密算法分析与实现

（一）LBlock 加密算法的基本原理

LBlock 密码算法的基本思想也是采用了 Feistel 结构，它的明文分组长度为 64 位，密钥长度 80 位，由 32 轮迭代实现。在 LBlock 密码算法中有三部分：加密算法，解密算法和密钥调度（如图 1）。

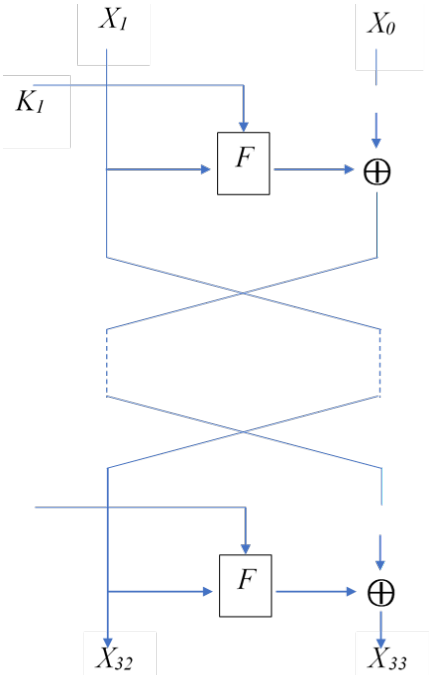

图1 LBlock的加密过程

在整个加密算法中，核心就体现在轮函数中，轮函数 F 定义为：

$$\{0, 1\}^{32} \times \{0, 1\}^{32} \rightarrow \{0, 1\}^{32} \quad (1)$$

$$(X, K_i) \quad \rightarrow U = P(S(X \oplus K_i))$$

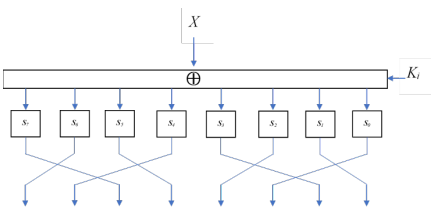

图2 LBlock加密算法轮函数F

其中 P 和 S 是在后文中出现的混淆和扩散函数，轮函数 F 的内涵就是将明文分组和

（下转第 258 页）

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

发展阶段，“互联网+”理念影响着我国高校思想政治教育工作。现阶段全国大部分高校已经开通了学校的官方网站、微博、微信公众号等新媒体平台，还有些有影响力的高校教师开通了个人微博等，有利于促进教育事业的发展。据《2018年中国高校园媒体发展报告》统计，全国高校超过96.8%已经开通了官方网站、90.5%的高校以及学院开通了微信公众号和微博平台，微信公众号平台成了现阶段校园媒体的主流形态。因此，高校要利用好新媒体平台来推动大学生文明素养的提升，发挥其主观能动性，潜移默化的影响大学生。例如，在微信公众号平台推送正确的道德话题，发起对校园不雅现象和不文明现象的讨论，正确引导大学生，树立正确的道德观和价值观，提升大学生的文明素养。

（二）加强大学生心理教育，提高个人文明觉悟

新时代背景下对当代大学生的思想观念提出了更高的要求，高校的大学生要从思想层面上认识到文明素养提升的重要性。一方面，高校思想政治教育工作者要加强对大学生思想道德修养，树立大学生正确的价值观，提升大学生的文明素养；另一方面，要重视大学生的心理教育，让大学生从心底发生改变，辨明是非，而不是用规章制度和行为规范等条条框框约束大学生，借助新媒体平台制作短视频，用事实引导大学生提高个人文明觉悟，提升大学生的文明素养促进大学生健康成长。

（三）搭建活动平台

设立专门文明素养提升平台，与学生社团、学生班级等进行“一对一”“一对多”文明规范与引导工作指导，发挥以点带面的榜样示范引导作用。注重以文化育人，开展文明校园创建和校园文化活动。强化基础文明教育的深度，挖掘一些纵横大一到大四的教育品牌活动，如“阅读经典，书香空港”等。

（四）点滴做起，文明自律

“不积跬步，无以至千里；不积小流，无以成江海”，这是我们每个人都知道的道理。高校学生提升文明素养要注重小事，自觉强化文明自律意识。大学生的文明素养提升不是一蹴而就的，要靠小事、点滴之事的积累，摒弃自身存在的文明行为陋习，自觉践行社会主义核心价值观。此外，学校要积极组织丰富多彩的提升文明素养的主题活动，如“光盘行动”“弯腰行动”，再邀请一些榜样到学生中间做讲座，做先进事迹报告，多树立学生身边的榜样，发挥榜样的主观能动性，让大学生从内心深处认可文明是一种美德。

综上所述，“勿以善小而不为，勿以恶小而为之，惟贤惟德，能服于人。”成功的人都有着高尚的道德情操和让人敬仰的文明素养。大学生进入更高一层学府，不仅是为了学好专业知识，更重要的是学会“做人”，养成良好的行为习惯，形成正确的人生观和价值观，从身边的点滴做起，从自己做起。高职院校也要注重对学生文明素养的教育，为学生搭建更广阔的平台，为学生树立更多的模范榜样，为学生提供更多走向社会的机会用案例潜移默化地影响学生。让文明素养成为大学生日常行为准则中的一种习惯，成为大学生思想中的一种理念，成功助推社会发展的隐形动力，使我国成为文明、自主、和谐、法制的友好型国家。

【作者简介】梁宇（1986-），女，研究生，讲师。

【课题项目】桂林理工大学2017年辅导员工作室“大学生基础文明素养提升工作室”专项课题，资助课题号：（GUT17GZS10）。

【参考文献】

[1] 李颖．论辅导员参与大学生心理健康教育的必然与应然[J]．天津农学院学报，2011(2)：58-61.

[2] 徐冠杰，吴健．大学生心理健康教育浅析[J]．成功（教育），2011(7)：3-4.

[3] 陈灿军．大学生心理健康问题分析及对策[J]．求索，2004(6)：189-191.

[4] 李福涛，张春伟．大学生文明素养提升的价值与路径[J]．沈阳师范大学学报（社会科学版），2016(4)：52-55.

（上接第256页）

密钥通过混淆和扩散的变化映射到另一个集合中。轮函数的结构如图2所示。

LBlock加密算法中混淆函数S是轮函数F的重要部分，它由8个4×4比特的S盒构成。S盒的设计原则也是遵照非线性的原则，所以S盒的强度很大程就决定了这整个算法的安全强度。混淆函数S可表示为一个集合的到另一个集合的映射，即：

$$\{0,\ 1\}^{32} \to \{0,\ 1\}^{32} \quad (2)$$

它将接收到的32位信息分成8个4位的分组，然后经过S盒代换重新连接为一段32位信息，映射以及代换关系如下表示：

$$Y = Y_7||Y_6||Y_5||Y_4||Y_3||Y_2||Y_1||Y_0 \to Z = Z_7||Z_6||Z_5||Z_4||Z_3||Z_2||Z_1||Z_0$$

（3-3）Z7=s7(Y7)，Z6=s6(Y6)，Z5=s5(Y5)，Z4=s4(Y4)，Z3=s3(Y3)，Z2=s2(Y2)，Z1=s1(Y1)，Z0=s0(Y0)。LBlock加密算法中S盒具体如表1所示。LBlock加密算法的密钥调度是采用了80位的密钥。设主密钥为K。存储在密钥寄存器中的K则表示为K=k79k78k77…k1k0。取在寄存器中存储的主密钥最左边32位作为第一轮轮函数的子密钥K1，然后进行如下操作来更新寄存器中的主密钥K：

For i=1,2,3,…,31

(i)K<<<29

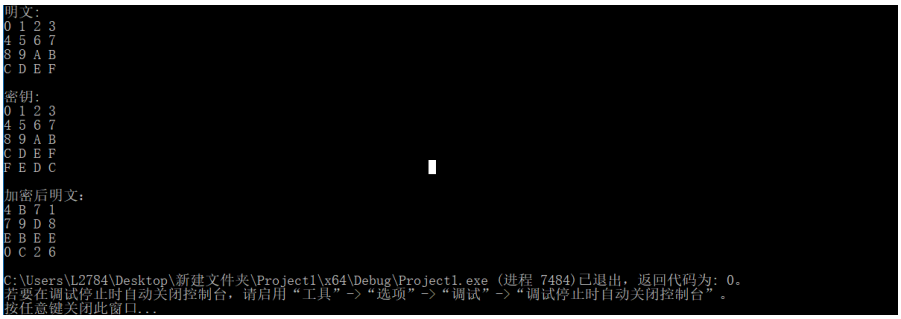

图3 LBlock加密算法运行结果

(ii)$[k_{79}k_{78}k_{77}k_{76}] = s_9[k_{79}k_{78}k_{77}k_{76}]$

$[k_{75}k_{74}k_{73}k_{72}] = s_8[k_{75}k_{74}k_{73}k_{72}]$

(iii) $[k_{50}k_{49}k_{48}k_{47}] \oplus [i]_2$

表1 LBlock加密算法中的S盒

	S盒
s_0	14, 9, 15, 0, 13, 4, 10, 11, 1, 2, 8, 3, 7, 6, 12, 5
s_1	4, 11, 14, 9, 15, 13, 0, 10, 7, 12, 5, 6, 2, 8, 1, 3
s_2	1, 14, 7, 12, 15, 13, 0, 6, 11, 5, 9, 3, 2, 4, 8, 10
s_3	7, 6, 8, 11, 0, 15, 3, 14, 9, 10, 12, 13, 5, 2, 4, 1
s_4	14, 5, 15, 0, 7, 2, 12, 13, 1, 8, 4, 9, 11, 10, 6, 3
s_5	2, 13, 11, 12, 15, 14, 0, 9, 7, 10, 6, 3, 1, 8, 4, 5
s_6	11, 9, 4, 14, 0, 15, 10, 13, 6, 12, 5, 7, 3, 8, 1, 2
s_7	13, 10, 15, 0, 14, 4, 9, 11, 2, 1, 8, 3, 7, 5, 12, 6
s_8	14, 9, 15, 0, 13, 4, 10, 11, 1, 2, 8, 3, 7, 6, 12, 5
s_9	4, 11, 14, 9, 15, 13, 0, 10, 7, 12, 5, 6, 2, 8, 1, 3

(iv) 将寄存器中当前内容的最左边的32位输出，作为轮密钥Ki+1。

其中s8和s9同样是两个4×4位的S盒。具体内容见表1。

（二）LBlock加密算法的C/C++实现

程序中主要设计函数有：加密过程的函数（Encryption），扩展密钥的函数（UpdateKeys），循环左移、异或、交换位置的函数（leftcyclicOR），核心的轮密钥函数（RoundF）以及输入输出函数。

测试结果符合设计目的中的功能，编译环境为Visual Studio 2017，采用的是Windows控制台程序的形式。运行结果以及每轮次结果截图如图3所示。

【作者简介】张爽（1981-），女，博士研究生，副教授，研究方向为数据库与知识库。

【参考文献】

[1] 王宁．几个轻量级分组密码算法的安全性分析[D]．济南：山东大学，2018.

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net