密码学报　ISSN 2095-7025　CN 10-1195/TN
Journal of Cryptologic Research, 2019, 6(6): 687–689
©《密码学报》编辑部版权所有.

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-82789618

分组密码专刊序言 (中英文)

吴文玲[1,2]

1. 中国科学院 软件研究所 可信计算与信息保障实验室, 北京 100190
2. 中国科学院大学, 北京 100049

通信作者: 吴文玲, E-mail: wwl@tca.iscas.ac.cn

中图分类号: TP309.7　　**文献标识码:** A　　DOI: 10.13868/j.cnki.jcr.000333

中文引用格式: 吴文玲. 分组密码专刊序言 (中英文)[J]. 密码学报, 2019, 6(6): 687–689.

英文引用格式: WU W L. Preface of special issue on block cipher[J]. Journal of Cryptologic Research, 2019, 6(6): 687–689.

Preface of Special Issue on Block Cipher

WU Wen-Ling[1,2]

1. Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China
2. University of Chinese Academy of Sciences, Beijing 100049, China

Corresponding author: WU Wen-Ling, E-mail: wwl@tca.iscas.ac.cn

为繁荣我国密码理论和应用研究, 推动密码算法设计和实现技术进步, 促进密码人才成长, 中国密码学会举办了全国密码算法设计竞赛. 22 个分组密码算法通过形式审查进入第一轮评估.

2019 年 9 月 27 日, 中国密码学会公布了进入第二轮评估的 10 个分组密码算法: uBlock、Ballet、FESH、TANGRAM、ANT、NBC、FBC、SMBA、Raindrop 和 SPRING.

为促进公众对分组密码算法的安全性评估和优化实现, 本刊组织了本期“分组密码”专刊, 刊登上述算法, 共包括 10 篇论文.

uBlock 的整体结构是 SP 结构, 非线性层采用 4 比特 S 盒, 利用 Feistel 结构设计了最优二元扩散层. uBlock 算法适应各种软硬件实现平台, 充分考虑了微处理器的计算资源, 可以利用 SSE、AVX2 和 NEON 等指令集高效实现, 硬件实现简单而有效. Ballet 的整体结构是变体的四分支 Lai-Massey 结构, 轮变换采用模加、循环移位和异或三种基本运算. Ballet 继承了 ARX 类算法的优点, 适宜软件实现. FESH 和 TANGRAM 的整体结构都是 SP 结构, 且轮变换均采用比特切片技术, 非线性层均采用 4 比特 S 盒. FESH 的线性层采用 4 轮迭代的 4 分支广义 Feistel 结构, 组合循环移位和异或运算达到较优的扩散性且同时兼顾实现性能. TANGRAM 的线性层采用精心选择的比特循环移位, 具有在资源受限环境下的实现优势. ANT 的整体结构是 Feistel 结构, 轮函数的基本运算仅包含比特与、循环移位和异或三种操作, 适宜轻量化实现. NBC 和 FBC 的整体结构都是扩展广义 Feistel 结构, NBC 的轮函数规模为 16 比

收稿日期: 2019-11-15　　定稿日期: 2019-12-10

特, 采用 16 级非线性反馈移位寄存器构造. FBC 轮函数的非线性层采用 4 比特 S 盒, 线性层采用循环移位异或型线性变换. SMBA 的整体结构为 Feistel-SP 结构, 非线性层采用两个 8 比特 S 盒, 线性层基于 Lai-Massey 结构设计. Raindrop 的轮函数包含 S 盒、行混合和比特级循环移位三种操作, 采用 3、5、7、9 比特规模的 S 盒, 设计方法类似 SHA3 的非线性层, 具有低延迟的优点. SPRING 的整体结构是 SP 结构, 非线性层采用 32 比特 S 盒, 基于环状串联结构的非线性反馈移位寄存器设计, 扩散层采用对合的字节变换.

进入第二轮评估的 10 个分组密码算法, 从整体结构分类, SP 结构的算法有 4 个: uBlock、FESH、TANGRAM 和 SPRING; Feistel 结构的算法有 3 个: ANT、SMBA 和 Raindrop; 扩展广义 Feistel 结构的算法有 2 个: NBC 和 FBC; Ballet 采用了变体 Lai-Massey 结构. 8 个算法使用了 S 盒: uBlock、FESH、TANGRAM 和 FBC 使用了 4 比特 S 盒, SMBA 使用了 8 比特 S 盒, NBC 和 SPRING 分别使用了 16 和 32 比特的大规模 S 盒, Raindrop 使用了奇数规模的 S 盒. 设计特点方面, uBlock 和 ANT 基于指令集设计, FESH 和 TANGRAM 采用了比特切片技术, Ballet 是典型的 ARX 类算法, SPRING 和 NBC 基于 NFSR 设计非线性部件, uBlock、TANGRAM 和 SMBA 等考虑了侧信道防护的代价.

目前的分析评估结果显示, 进入第二轮评估的 10 个算法对典型分组密码分析方法都是安全的. 由于时间有限, 对于相关密钥类分析方法的安全性、ARX 类算法的安全性、算法实现安全性、大规模 S 盒等分析评估不够深入. 10 个算法在各种平台的实现都有待进一步优化. 希望本专刊能起到抛砖引玉的作用, 吸引国内更多专家学者参与分组密码算法的安全性分析和优化实现, 推动我们国家密码算法研究、标准研制和应用推广.

To prosper the research of cryptology theory and application, promote the design and implementation of cryptographic algorithms, and encourage the growth of cryptographic talents, the Chinese Association for Cryptologic Research (CACR) held the National Cryptographic Algorithm Design Competition. Through formality review, 22 block ciphers are qualified to enter the first round evaluation. On September 27, 2019, the CACR published 10 ciphers, namely, uBlock, Ballet, FESH, TANGRAM, ANT, NBC, FBC, SMBA, Raindrop, and SPRING, for second round evaluation.

To promote the security evaluations and optimized implementations of block ciphers, this special issue of “Block Cipher” is organized and these 10 ciphers are included.

The framework of uBlock is SP structure. The nonlinear layer is constitute of 4-bit S-boxes. Feistel structure is used in the construction of optimal binary diffusion layer. uBlock adapts to various software and hardware implementations. It can be efficiently implemented by using SSE, AVX2, and NEON instruction sets, and the hardware implementation is simple and effective. The structure of Ballet is a variant of 4-branch Lai-Massey structure. Three basic operations, namely, Addition, Rotation, and XOR, are used in the round transformation. Ballet inherits the advantages of ARX ciphers and is suitable for software implementation. FESH and TANGRAM adopt SP structure. Both round transformations take advantage of bit-slice technique, and both nonlinear layers use 4-bit S-boxes. The linear layer of FESH is 4-round iterations of 4-branch generalized Feistel structure, which combines cyclic shift, and exclusive or operations to achieve both better diffusion and implementation performance. The linear layer of TANGRAM uses selective bit-wise cyclic shift, and has advantages in implementation in resource constrained environment. Framework of ANT is Feistel structure. The round function has only three basic operations: bit and, cyclic shift and exclusive or. The ANT round function is similar to round function of SIMON, but with more operands. Framework of NBC and FBC are extended generalized Feistel structure. NBC adopts 16-bit round function, which is constructed by 16-series nonlinear feedback shift register. Round function of FBC uses 4-bit S-boxes as the nonlinear layer, and the linear layer is composed of cyclic shift and exclusive or operations. SMBA is of Feistel-SP structure. The nonlinear layer makes use of two 8-bit S-boxes, and the linear layer is designed based on Lai-Massey structure. Three operations, S-box, MixRow, and bit-wise cyclic shift, are used in the round function of Raindrop. Raindrop shares similarity with nonlinear layer of SHA3 by using 3, 5, 7, 9-bit S-boxes. Raindrop has the advantage of low latency. SPRING is a cipher of SP structure. 32-bit S-boxes, which are designed based on nonlinear feedback shift register of ring series structure, act as the nonlinear layer. The diffusion layer adopts byte-wise involutional transformation.

Classify the 10 block ciphers entered the second round evaluation from structure, uBlock, FESH, TANGRAM, and SPRING are four ciphers of SP structure; ANT, SMBA, and Raindrop are three ciphers of Feistel structure; NBC and FBC are two ciphers of extended generalized Feistel structure; Ballet adopts a variant of Lai-Massey structure. Eight ciphers make use of S-boxes. uBlock, FESH, TANGRAM, and FBC choose 4-bit S-boxes. SMBA chooses 8-bit S-box. NBC and SPRING choose 16-bit and 32-bit large S-boxes respectively. Raindrop chooses S-box of odd size. In terms of design features, uBlock and ANT are designed based on instruction set; FESH and TANGRAM take advantage of bit-slice technique; Ballet is a classical ARX cipher; SPRING and NBC build the nonlinear layer based on nonlinear feedback shift register; uBlock, TANGRAM, and SMBA have considered the cost of side channel protection.

Current evaluation results have shown the security of these 10 ciphers against classical cryptanalysis methods of block cipher. Due to the limited time, evaluation of security against related-key cryptanalysis, security of ARX ciphers, implementation security, and some other problems are not thorough enough. In addition, further optimization of the implementation performances of these 10 ciphers in various platforms are expected. This special issue is expected to play an important role in attracting more domestic experts and scholars to participate in the security analysis and implementation performance optimization of candidate block ciphers of the competition, and to promote the development, standardization, and application of cryptographic algorithms in China.

作者信息

吴文玲 (1966–), 博士, 研究员.
主要研究领域为密码学.
wwl@tca.iscas.ac.cn

WU Wen-Ling (1966–), Ph.D., Professor, Doctoral Tutor. Her main research covers cryptology.
wwl@tca.iscas.ac.cn