第 41 卷第 5 期　　遥　测　遥　控　　Vol. 41, No. 5
2020 年 9 月　　Journal of Telemetry, Tracking and Command　　September 2020

Email:ycyk704@163.com　TEL:010-68382327　010-68382557

Simpira 置换的差分路线研究

李　铮[1,2]，张建标[1]，赵静远[3]，徐万山[1]，袁艺林[1]
（1 北京工业大学信息学部 可信计算北京市重点实验室　北京 100022
2 中国科学院信息工程研究所 信息安全国家重点实验室　北京 100093
3 北京遥测技术研究所　北京 100094）

摘要：对称密码算法设计由算法结构设计和内部置换函数设计组成，但又不是一种单纯的累加，算法结构与置换函数之间的配合与相互作用也是至关重要的，相应的分析工作可为密码算法的安全性评估和设计提供参考。Simpira 是一族密码置换，整体结构为广义 Feistel 结构，其 F 函数基于 AES，最终选取的 F 函数相当于 2 轮 AES 轮函数。研究的对象是 Simpira 设计文档中提到的一种结构，是 Simpira-2 的一种简化情形，算法的状态大小为 256 比特，整体结构为 Feistel 结构，其中 F 函数采用 1 轮 AES。在这种简化的情况中，研究给出了 4 轮 6 个活跃 S 盒和 5 轮 15 个活跃 S 盒的截断差分路线的可能模式，通过 S 盒、列混合操作中差分的计算和分析，对应上述 4 轮、5 轮截断差分，具体路线的概率分别可达到 2^{-36}、2^{-91}。

关键词：Simpira；Feistel 结构；AES；差分路线；活跃 S 盒
中图分类号：TP309　　**文献标识码：**A　　**文章编号：**CN11-1780(2020)05-0052-05

Study for differential trails of Simpira

LI Zheng,　ZHANG Jianbiao,　ZHAO Jingyuan,　XU Wanshan,　YUAN Yilin
（1. Beijing Key Laboratory of Trusted Computing, Faculty of Information Technology,
Beijing University of Technology, Beijing 100124, China;
2. State Key Laboratory of Information Security, Institute of Information Engineering,
Chinese Academy of Sciences, Beijing 100093, China;
3. Beijing Research Institute of Telemetry, Beijing 100094, China）

Abstract: The design of symmetric cryptographic algorithms is composed of structure and internal permutation, but it is not a simple accumulation, the coordination and interaction between the structure and the internal permutation is also crucial, the corresponding cryptanalysis can help to the security evaluation and the design of symmetric cryptographic algorithms. Simpira is a family of cryptographic permutation. The overall structure is a generalized Feistel structure, and its F function is based on AES. The object of this paper is a structure mentioned in the Simpira document, which is a simplified case of Simpira-2. The algorithm's state size is 256 bits, and the overall structure is Feistel structure, whose F function is 1-round AES. This paper focuses on the simplified case mentioned above, so the 4-round truncated differential trail with 6 active S-boxes and the 5-round truncated differential trail with 15 active S-boxes are presented. By the computation and analysis of differentials in S-box and MixColumns, corresponding to the 4-round and 5-round truncated differential trails, the probabilities of two differential trails can reach 2^{-36}, 2^{-91}, respectively.

Key words: Simpira; Feistel structure; AES; Differential trails; Active S-boxes

引　言

我们处在一个信息爆炸的时代，无论是人们日常生活中的社交网络、线上支付，还是航空航天、卫星探测等科工项目，都离不开密码算法的应用。由于加密速度快，对称密码算法在很多效率要求比较高的事务中得到了广泛的应用。

收稿日期：2020-07-15　收修改稿日期：2020-08-30

目前，对称密码算法设计进入一个相对成熟、较为稳定的发展阶段，算法结构的类型主要包括有 Feistel 结构、SPN（substitution permutation network）结构、ARX（modular addition，rotation and bitwisexor）结构等，而算法的置换函数是提供算法随机性的重要部件，它对于密码算法的安全性和效率等性能都十分重要。对称密码算法设计由算法结构设计和内部置换函数设计组成，但又不是一种单纯的累加，算法结构与置换函数之间的配合与相互作用也是至关重要的。对配套密码算法进行安全性分析研究，除了对于该算法本身具有评估价值之外，还可以对于算法结构和置换函数的设计与结合方式给出理论参考，对密码算法的设计也有一定的指导意义。

高级加密标准 AES（Advanced Encryption Standard）[1]于 2001 年由 NIST（National Institute of Standards and Technology）颁布，其安全性和效率经过了密码分析者和工程设计人员多年来的分析、应用和研究，实践出真知，AES 至今在安全性和效率两个方面的表现仍然十分突出，应用十分广泛，现今已成为许多算法设计的标杆算法，也是相似应用方向的模板算法。其设计过程遵循宽轨道设计原则，AES 经由嵌套，改造等多种方式，呈现在不同对称密码算法当中，提供着稳定可靠的性能。更因如此，AES 及其相关算法的安全性研究具有十分重要的价值和意义。Simpira 置换[2]是由 Gueron 和 Nicky Mouha 在 2016 年亚密会上提出的，是一族密码置换，其内核算法即为 AES，充分利用了 AES 高效成熟的指令集，实现了高吞吐量。SPHINCS[3]由 Bernstein 等在 2015 年欧密会上提出，是基于哈希函数算法、具有后量子安全性的数字签名算法。后来，其设计者又将其运用到了 SPHINCS 当中，提出了 SPHINCS-Simpira[4]，为原始的 SPHINCS-256 算法加快了实现速度。

1　Simpira 算法介绍

Simpira 置换支持 128×b 比特的输入，其中 b 是一个正整数，其设计目标是为了覆盖现有的 64 位存储器，实现高吞吐量，因为现有处理器已经具有 AES 的指令集。为了充分利用指令集，实现高吞吐量，Simpira 以 AES 的轮函数作为唯一的构建模块，对于 b=1 的情形，Simpira 相当于轮密钥具有固定取值的 12 轮 AES，对于 $b\geqslant 2$，Simpira 的 F 函数为 2 轮 AES，整体结构为广义 Feistel 结构。对于以上所有的情形，考虑进区分器的情况，设计者给出的安全界均为 2^{128}。$b\in\{1,2,3\}$时 Simpira 的框架图如图 1 所示。

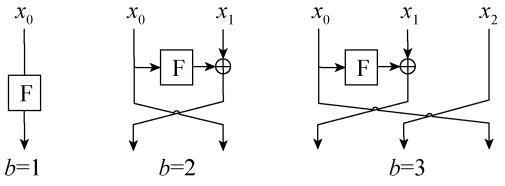

图 1　Simpira 的框架图（$b\in\{1,2,3\}$）[2]

Fig. 1　Structure of Simpira（$b\in\{1,2,3\}$）[2]

本文主要研究的情形为 F 函数为 1 轮 AES 的情形，因此，接下来再简单介绍一下 AES 的轮函数，包括密钥加、S 盒代换、行移位、列混合这四个步骤。这里考虑单密钥的情形，因此忽略密钥加。S 盒代换操作过程如图 2 所示，行移位操作过程如图 3 所示，列混合是对状态的每一列进行线性变换，变换公式如下：

$$\begin{pmatrix} b0\\ b1\\ b2\\ b3 \end{pmatrix}=\begin{pmatrix} 02 & 03 & 01 & 01\\ 01 & 02 & 03 & 01\\ 01 & 01 & 02 & 03\\ 03 & 01 & 01 & 02 \end{pmatrix}\begin{pmatrix} a0\\ a1\\ a2\\ a3 \end{pmatrix} \qquad (1)$$

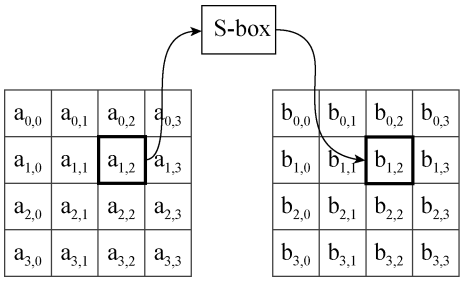

图 2　AES 中的 S 盒代换[1]

Fig. 2　S-box operation in AES[1]

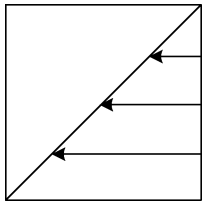

图 3　AES 中的行移位[1]

Fig. 3　ShiftRows operation in AES[1]

2　安全性分析相关研究

密码算法的设计离不开安全性分析评估。Simpira 置换支持可变的状态大小 128×b 比特，其中 b 为正整数，

即为 Simpira-*b*。鉴于差分分析和线性分析在安全性评估中的重要意义，其设计者在安全性评估中给出了最小活跃 S 盒个数的下界。此外，Simpira 置换适用于多种功能模式，设计者提出了许多应用场景，包括 Even-Mansour 分组密码结构，或用于限制输入长度的哈希函数的无密钥的 Davies-Meyer 结构。Mendel 等[5]对基于 Davies-Meyer 结构的哈希函数 Simpira-4 给出了全轮的碰撞攻击，主要基于 15 轮 40 个活跃 S 盒的碰撞路线。鉴于他们的研究工作，Simpira 也经历了从 v1 版本到 v2 版本的改变。Rønjom 等[6]发现了 Simpira-4 算法中的不变子空间，Zong 等[7]给出了 9 轮 Simpira-4 算法的不可能差分路线。Simpira 置换选取著名的 AES 算法作为内部函数，密码工作者在过去的二十年间持续、广泛地研究 AES 类算法的安全性，AES 类算法的安全性分析是密码学领域的焦点问题之一，陆续有一些缩减轮数 AES 的区分攻击出现。区分攻击的目的在于将密码算法与随机置换区分开来，也就是找到非随机特性，使得在相应的测试中，密码算法与随机置换的测试结果具有足够不同的概率。本文发现的差分路线即为密码算法区分器的一种形式，在算法安全性要求范围内，对缩减轮数简化版本密码算法进行了分析研究。

3 差分路线研究

差分分析是密码分析中最重要的分析方法之一，寻找概率大于随机情况的差分路线，以此作为非随机特性，是差分分析的关键，概率越高，区分效果越好。一般来说，差分路线中的活跃 S 盒越少，则差分路线的概率越高。事实上，Simpira 设计文档中也考虑了轮函数为 1 轮 AES 的情况，并给出在 b=2 的情况下，需要 25 轮来保证至少有 25 个线性活跃 S 盒。本文研究的对象就是 Simpira-2 的这种简化情形，算法的状态大小为 256 比特，整体结构为 Feistel 结构，其中 F 函数采用 1 轮 AES。

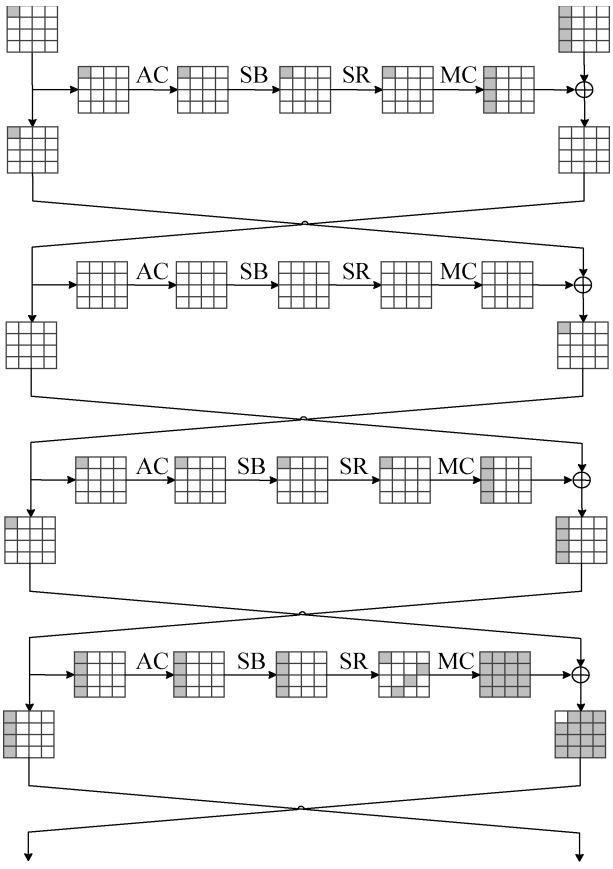

图 4 4 轮截断差分路线

Fig. 4 4-round truncated differential trail

对于这种情形，我们研究给出了 4 轮截断差分路线，共有 6 个活跃 S 盒，如图 4 所示，对应具体的 4 轮差分路线，概率为 2^{-36}；以及 5 轮截断差分路线，共有 15 个活跃 S 盒，如图 5 所示，对应具体的 5 轮差分路线，概率为 2^{-91}。在图 4 和图 5 中，灰色方块代表字节的差分非零，部分取值需满足一些约束条件；而白色方块表示该字节为全零差分。中间状态的符号表示说明，第 r 轮的输入状态记为 S^r，第 r 轮的输入差分记为 ΔS^r，S^r 中（i,j）位置的字节记为 $S^r[i][j]$，其中 $r\geqslant 1$，$0\leqslant i\leqslant 3$，$0\leqslant j\leqslant 3$。第 r 轮字节代换 S 盒的输出状态为 S^r_{SB}，类似地，第 r 轮过程中的状态依次为输入状态，常数加、字节代换、行移位、列混合和总的输出状态，即 $S^r, S^r_{\mathrm{AC}}, S^r_{\mathrm{SB}}, S^r_{\mathrm{SR}}, S^r_{\mathrm{MC}}, S^{r+1}$，第 r 轮的输出状态 S^{r+1}，即第 r+1 轮的输入状态，其中 $S^r_{\mathrm{MC}} \oplus S^{r-1} = S^{r+1}$。

根据 Feistel 结构的性质，在第 1 轮中，初始状态的左侧一半，共有 128 比特进入 AES 算法的 S 盒。为使得总体活跃 S 盒的个数更少，我们优先考虑了第 1 轮中有 1 个活跃 S 盒的情况，也就是第 1

轮 S 盒代换的输入状态中，只有 1 个非零 S 盒。首先经过第 1 轮的常数加和 S 盒代换操作，并不改变活跃 S 盒的个数。此外，我们选取（0, 0）位置的字节作为活跃 S 盒，因此在第 1 轮中行移位操作相当于一个恒等变换，并不改变活跃 S 盒的个数和位置。经过第 1 轮的列混合操作时，其输入差分具有 1 个活跃 S 盒，输出差分具有 4 个活跃 S 盒，这里的输出状态与初始状态当中的右侧一半比特异或。因为我们可以自由地选取初始状态，所以选取初始状态右侧一半与第 1 轮中列混合的输出状态完全相等，这样可以抵消掉第 1 轮中 F 函数的输出差分，由此，第 2 轮中 F 函数的输入差分为零，即活跃 S 盒的个数为零。

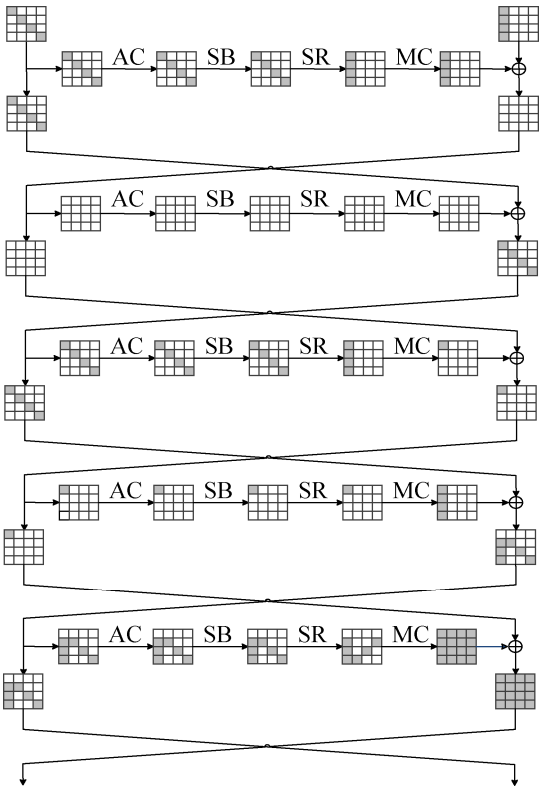

图 5　5 轮截断差分路线

Fig. 5　5-round truncated differential trail

第 2 轮中 F 函数的输出状态与初始状态的左侧一半比特异或，于是第 3 轮中 F 函数的输入状态与初始状态的左侧一半完全相等，可以选择第 3 轮中 F 函数的差分变换与第 1 轮中的情况相同，因此，第 3 轮中 F 函数的输入差分具有 1 个活跃 S 盒，输出差分具有 4 个活跃 S 盒。由于第 2 轮中 F 函数的输入差分为零，所以第 4 轮中 F 函数的输入差分与第 3 轮中 F 函数的输出差分一致。然后在第 4 轮中，常数加和 S 盒代换并不改变活跃 S 盒的位置和个数情况，在行移位操作之后，4 个活跃 S 盒分布到了互不相同的列。于是，在列混合之后，第 4 轮 F 函数输出的整个差分状态中的每个 S 盒都活跃，实现了首次差分扩满的现象。在第 4 轮末尾，第 4 轮 F 函数的输出状态与第 3 轮 F 函数的输入状态异或，这里限定两状态在（0, 0）位置的差分抵消。至此，给出了 4 轮 6 个活跃 S 盒的截断差分路线。

具体分析第 4 轮 F 函数后异或的情况，为了使得（0, 0）位置处的差分抵消，那么第 3 轮的输入差分与第 4 轮 F 函数的输出差分相等，即 $\Delta S^3[0][0]=\Delta S^4_{\mathrm{MC}}[0][0]$，例如，列出一组可能的相关差分取值：

$$\begin{cases}\Delta S^3[0][0]=\Delta S^3_{\mathrm{AC}}[0][0]=0x77\\ \Delta S^3_{\mathrm{SB}}[0][0]=\Delta S^3_{\mathrm{SR}}[0][0]=0x9b\\ \Delta S^3_{\mathrm{MC}}[0][0]=\Delta S^4[0][0]=\Delta S^3_{\mathrm{AC}}[0][0]=0x2d\\ \Delta S^4_{\mathrm{SB}}[0][0]=0xb6\\ \Delta S^4_{\mathrm{MC}}[0][0]=0x77\end{cases} \tag{2}$$

这里第 3 轮、第 4 轮中（0, 0）位置 S 盒的差分概率均为 2^{-6}，其他 S 盒的取值不受列混合操作的限制，因此，4 轮差分路线具有 1+0+1+4=6 个活跃 S 盒，概率可以达到 2^{-36}。如果由此路线出发，那么第 5 轮中有 15 个活跃 S 盒，由此得到的 5 轮截断差分路线将具有 21 个活跃 S 盒。

为寻找活跃 S 盒个数更少的差分路线模式，我们在截断差分路线中加入列混合中的线性约束，并选取 S 盒输入、输出的差分状态，进而给出具有 15 个活跃 S 盒的 5 轮截断差分路线，如图 5 所示。为使得 $\Delta S^3[i][j]=\Delta S^3_{\mathrm{AC}}[i][j]$，$\Delta S^3_{\mathrm{SB}}[i][j]$ 分别为（i, j）位置 S 盒的输入差分和输出差分，且 $0\leqslant i\leqslant 3$，$0\leqslant j\leqslant 3$。根据第 3 轮的行移位

$$\Delta S^3_{\mathrm{SR}}[0][0]=\Delta S^3_{\mathrm{SB}}[0][0],\ \Delta S^3_{\mathrm{SR}}[1][0]=\Delta S^3_{\mathrm{SB}}[1][1],\ \Delta S^3_{\mathrm{SR}}[2][0]=\Delta S^3_{\mathrm{SB}}[2][2],\ \Delta S^3_{\mathrm{SR}}[3][0]=\Delta S^3_{\mathrm{SB}}[3][3] \tag{3}$$

第 3 轮列混合输出状态差分 $\Delta S_{\mathrm{MC}}^{3}$ 的（0, 0）字节为非零，$\Delta S_{\mathrm{MC}}^{3}$ 的（1, 0）、（2, 0）和（3, 0）字节为零，分别有

$$\begin{cases} \Delta S_{\mathrm{MC}}^{3}[0][0] = 02\bullet \Delta S_{\mathrm{SR}}^{3}[0][0] \oplus 03\bullet \Delta S_{\mathrm{SR}}^{3}[1][0] \oplus \Delta S_{\mathrm{SR}}^{3}[2][0] \oplus \Delta S_{\mathrm{SR}}^{3}[3][0] \neq 0 \\ \Delta S_{\mathrm{MC}}^{3}[1][0] = \Delta S_{\mathrm{SR}}^{3}[0][0] \oplus 02\bullet \Delta S_{\mathrm{SR}}^{3}[1][0] \oplus 03\bullet \Delta S_{\mathrm{SR}}^{3}[2][0] \oplus \Delta S_{\mathrm{SR}}^{3}[3][0] = 0 \\ \Delta S_{\mathrm{MC}}^{3}[2][0] = \Delta S_{\mathrm{SR}}^{3}[0][0] \oplus \Delta S_{\mathrm{SR}}^{3}[1][0] \oplus 02\bullet \Delta S_{\mathrm{SR}}^{3}[2][0] \oplus 03\bullet \Delta S_{\mathrm{SR}}^{3}[3][0] = 0 \\ \Delta S_{\mathrm{MC}}^{3}[3][0] = 03\bullet \Delta S_{\mathrm{SR}}^{3}[0][0] \oplus \Delta S_{\mathrm{SR}}^{3}[1][0] \oplus \Delta S_{\mathrm{SR}}^{3}[2][0] \oplus 02\bullet \Delta S_{\mathrm{SR}}^{3}[3][0] = 0 \end{cases} \quad (4)$$

在第 4 轮的 F 函数之后，为抵消（0, 0）处的差分，需要满足 $\Delta S^{3}[0][0] = 02\bullet \Delta S_{\mathrm{SR}}^{4}[0][0] = 02\bullet \Delta S_{\mathrm{SB}}^{4}[0][0]$。在上述前提条件下，第 3 轮和第 4 轮位置 S 盒的输入输出情况需要特别研究，其他活跃 S 盒均可直接取到概率 2^{-6}。特别地，当第 3 轮（0, 0）位置 S 盒的输入输出差分取值为 $\Delta S^{3}[0][0] = 0xc8$, $\Delta S_{\mathrm{SB}}^{3}[0][0] = 0xe$，该 S 盒的概率为 2^{-6}，当第 4 轮（0, 0）位置 S 盒的输入输出差分取值为 $\Delta S^{4}[0][0] = 0x1$，$\Delta S_{\mathrm{SB}}^{4}[0][0] = 0x64$，该 S 盒的概率为 2^{-7}。综上，5 轮差分路线具有 4+0+4+1+6=15 个活跃 S 盒，概率可以达到 2^{-91}。

4　结束语

本文对于 Simpira 置换的差分路线进行了初步探索，对标准 Feistel 结构下简化版 F 函数为 1 轮 AES 的情况，给出了 4、5 轮截断差分路线，对应差分路线的概率分别达到 2^{-36}、2^{-91}。高级加密标准 AES 的安全性和效率等性能出众，经过了多年来的分析评估、应用和研究，现今应用十分广泛，对于分组密码算法的设计具有很强的参考价值和参照意义，它在不同密码结构中的混合应用，对于 AES 本身和相关密码算法，比如 Simpira 置换，其安全性、效率等性能的评估可以相互借鉴。此外，对于相关密码算法的分析工作在数学本质上是对有限域多项式系统的研究，也是一个数学困难问题。因此，这些安全性分析工作在理论和应用方面都具有很重要的意义。

参考文献

[1] DAEMEN J, RIJMEN V. The Design of Rijndael: AES - The Advanced Encryption Standard[M]. Information Security and Cryptography, Springer, 2002.

[2] GUERON S, MOUHA N. Simpira v2: a family of efficient permutations using the AES round function[C]. Advances in Cryptology – ASIACRYPT 2016: 95–125.

[3] BERNSTEIN D J, HOPWOOD D, et al. SPHINCS: practical stateless hash-based signatures[C]. EUROCRYPT 2015: 368–397.

[4] GUERON S, MOUHA N. SPHINCS-Simpira: fast stateless hash-based signatures with post-quantum security[EB]. IACR Cryptol. ePrint Arch,2017: 645.

[5] DOBRAUNIG C, EICHLSEDER M, MENDEL F. Cryptanalysis of Simpira v1[C]. SAC 2016: 284–298.

[6] RØNJOM S. Invariant subspaces in Simpira[EB]. IACR Cryptol. ePrint Arch, 2016: 248.

[7] ZONG Rui, DONG Xiaoyang, WANG Xiaoyun. Impossible differential attack on Simpira v2[J]. Sci. China Inf., 2018, 61(3): 16–22.

[作者简介]

李　铮　1992 年生，讲师，主要从事对称密码算法的分析与设计研究工作。

张建标　1969 年生，教授，主要从事信息安全可信计算方面的研究工作。

赵静远　1987 年生，博士，主要从事对称密码算法的分析与设计研究工作。

徐万山　1988 年生，博士研究生，主要从事信息安全可信计算方面的研究工作。

袁艺林　1992 年生，博士研究生，主要从事信息安全，云计算等的研究工作。