密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research, 2022, 9(4): 698–708

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

Alzette 的安全性分析*

许 峥[1,2], 李永强[1,2], 王明生[1,2]

1. 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
2. 中国科学院大学 网络空间安全学院, 北京 100049

通信作者: 李永强, E-mail: yongq.lee@gmail.com

摘 要: 本文研究了 Alzette (2020 年美密会议上提出的 ARX 结构 S 盒) 抗差分类分析的安全性. 首先, 对于模加操作上的有效异或差分, 通过利用符号差分的概念, 本文给出了符号差分比特之间关系的比特向量表示. 其次, 通过将 Lipmaa-Moriai 限制条件以及符号差分比特约束条件转化为 SMT 问题, 本文提出了一种基于 SAT/SMT 求解器的 ARX 结构不可能差分区分器自动化搜索工具. 该自动化工具是首个利用 Lipmaa-Moriai 限制条件以及符号差分搜索 ARX 结构不可能差分区分器的自动化工具. 利用该工具可以发现被传统搜索方法忽略的有效的不可能差分区分器. 最后, 通过利用新的自动化工具以及传统方法搜索 Alzette 的不可能差分区分器, 在输入差分汉明重量为 2、输出差分汉明重量为 1 的条件下, 我们分别发现了 128 993 个和 128 767 个不可能差分区分器, 证明新的自动化工具能够更好地过滤无效差分路径; 此外, 将新的自动化搜索工具用于搜索 4 轮无密钥注入 SPECK64 不可能差分区分器, 在输入差分汉明重量为 2、输出差分汉明重量为 1 的条件下, 我们发现了 128 976 个不可能差分区分器, 说明 Alzette 设计团队的安全性评估是不够全面的. 据我们所知, 这是首次利用不可能差分性质评估 Alzette 的安全性.

关键词: Lipmaa-Moriai 限制条件; 符号差分; 不可能差分; Alzette; SAT/SMT 求解器

中图分类号: TP309.7 **文献标识码:** A DOI: 10.13868/j.cnki.jcr.000543

中文引用格式: 许峥, 李永强, 王明生. Alzette 的安全性分析[J]. 密码学报, 2022, 9(4): 698–708. [DOI: 10.13868/j.cnki.jcr.000543]

英文引用格式: XU Z, LI Y Q, WANG M S. Security analysis of Alzette[J]. Journal of Cryptologic Research, 2022, 9(4): 698–708. [DOI: 10.13868/j.cnki.jcr.000543]

Security Analysis of Alzette

XU Zheng[1,2], LI Yong-Qiang[1,2], WANG Ming-Sheng[1,2]

1. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
2. School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

Corresponding author: LI Yong-Qiang, E-mail: yongq.lee@gmail.com

Abstract: This paper studies the security of Alzette (a 64-bit ARX-based S-box proposed at CRYPTO 2020) against differential-like cryptanalysis. Firstly, for a valid XOR differential over a modulo addition, the bit-vector representation of the relations between signed differential bits is given by using the concept of signed differences. Secondly, by converting Lipmaa-Moriai constraints and the

* 基金项目: 国家自然科学基金 (61772516, 61772517)
Foundation: National Natural Science Foundation of China (61772516, 61772517)
收稿日期: 2021-08-27 定稿日期: 2022-01-11

constraints between signed differential bits into SMT problems, a SAT/SMT-based automatic search tool is proposed for impossible differential distinguishers in ARX structures. The automatic tool is the first tool to use Lipmaa-Moriai constraints and signed differences to automatically search for impossible differential distinguishers in ARX structures. This tool can find valid impossible differential distinguishers that are ignored by traditional search methods. Finally, impossible differential distinguishers for Alzette are searched by using the proposed automatic tool and traditional methods, and 128 993 and 128 767 impossible differential distinguishers with wt(InD) = 2 and wt(OutD) = 1 are found, which means that the new automatic tool can better filter invalid differential characteristics. Moreover, by searching impossible differential distinguishers for 4-round no-key SPECK64 using the proposed automatic tool, 128 976 impossible differential distinguishers with wt(InD) = 2 and wt(OutD) = 1 are found, which means that the security assessment of Alzette's design team is not comprehensive enough. To the best of our knowledge, this is the first time that the impossible differential property is used to evaluate the security of Alzette.

Key words: Lipmaa-Moriai constraints; signed differences; impossible differentials; Alzette; SAT/SMT solver

1 引言

认证加密算法 (authenticated-encryption, AE) 是指能同时实现数据加密和真实性认证功能的算法, 是密码学家在研究加密算法和认证算法的基础之上, 根据现实应用需求提出的对称密码算法. 随着物联网的发展, 密码算法越来越多地被应用在资源受限的环境中. 由于现有的认证加密算法以及 Hash 函数不适用于资源受限的环境中, 美国国家标准与技术研究所 (NIST) 启动了一项进程, 以征集、评估并标准化适用于资源受限环境中的带关联数据的认证加密 (AEAD) 算法以及 Hash 函数 [1]. 2019 年 4 月 18 日, NIST 共收到 57 个算法, 其中的 56 个被接收为第一轮候选算法. 经过公开反馈以及内部评定, NIST 于 2019 年 8 月 30 日公布了 32 个第二轮候选算法. 经过更加严格的安全性评估, 2021 年 3 月 29 日, NIST 公布了 10 个决赛候选算法: ASCON、Elephant、GIFT-COFB、Grain-128AEAD、ISAP、PHOTON-Beetle、Romulus、SPARKLE、TinyJambu 以及 Xoodyak. 在这 10 个决赛候选算法之中, SPARKLE 算法由于使用了新的 64 比特 S 盒 (Alzette) 而备受关注.

Alzette [2] 是由 Beierle 等人在 2020 年美密会上提出的一种 ARX (模加、循环移位、异或) 结构的 64 比特 S 盒. ARX 结构的安全性是通过分析其抗各种攻击的鲁棒性来评估的. 对于 ARX 结构最成功的攻击之一是差分类攻击 (差分攻击 [3] 和不可能差分攻击 [4,5]). 由于 Alzette 是 SPARKLE 算法唯一的非线性来源, 而模加又是 Alzette 唯一的非线性来源, 因此评估模加的差分性质对评估 Alzette 以及 SPARKLE 抗差分类分析的安全性是十分关键的.

模加的差分性质已经被研究了几十年. 在 2001 年的 FSE 会议上, Lipmaa 和 Moriai 提出了一种计算具有两个可变输入的模加的差分概率的对数时间算法 [6]. 在 2010 年的 SAC 会议上, Mouha 等人引入了 S 函数的概念并利用 S 函数来评估具有任意数量输入分支模加的差分概率 [7]. 在 2020 年的亚密会议上, Azimi 等人提出了一种针对具有一个常量输入的模加的比特向量差分模型 [8]. 为了更好地评估分组密码抗差分分析的安全性, Lai 等人在 1991 年的欧密会议上提出了 Markov 密码的概念 [9]. 在 Markov 假设下, 一条差分路径的概率可以通过将每一轮的差分传播的概率相乘得到. 事实上, Markov 假设被用于几乎所有对分组密码的差分攻击以及不可能差分攻击中. 在近二十年中, 利用自动化工具搜索差分路径以及不可能差分区分器成为了一种新的趋势. 这些自动化工具主要分为三类: 利用 Matsui 算法类的分支定界搜索算法 [10–13]、利用混合整数线性规划 (MILP) 模型 [14,15] 以及利用 SAT/SMT 求解器 [16–21]. 这些方法都是基于 Markov 假设的. 在 Markov 假设下, ARX 结构的差分路径的概率等于每一轮中的每个模加的差分概率的乘积. 然而, 由于 Alzette 中没有任何的密钥注入, 利用基于 Markov 假设的自动化搜索方法来搜索 Alzette 的差分路径以及不可能差分区分器, 可能会将无效的差分路径识别为有效并遗漏一些有效的不可能差分区分器, 从而导致对 Alzette 抗差分类分析的安全性评估不够准确. 因此, 提出一种能

够更好地过滤无效的差分路径的方法是十分重要的.

为了更好地过滤无效差分路径, 密码学家研究了差分比特之间的关系并部分解决了上述问题. 在 2005 年的欧密会议和美密会议上, Wang 等人利用符号差分发现了 MD4、MD5 和 SHA-1 的碰撞 [22–24]. 随后, Leurent 对于连续的异或差分比特提出了多比特限制的概念并提出了一种搜索有效差分路径的自动化工具: ARX Toolkit. 利用该工具, Leurent [25] 发现了 Yu 等人 [26] 只利用符号差分找到的一条 Skein 算法的差分路径是无效的. 在 2013 年, Mouha 等人 [20] 利用 Lipmaa-Moriai 限制条件以及符号差分搜索 3 轮 Salsa20 的最优差分路径. 他们发现了一条 ARX Toolkit 无法过滤的差分路径, 证明 Leurent 的自动化工具只能捕捉到连续比特之间的关系而无法捕捉非连续比特之间的关系, 因此该工具依然无法成功过滤部分无效的差分路径. 然而, Mouha 等人的方法是自动化与手动推导相结合的方法, 无法完全自动化地过滤无效的差分路径, 因此不适用于搜索不可能差分区分器.

本文研究了 Alzette 抗差分类分析的安全性. 对于模加操作上的有效异或差分, 通过利用符号差分的概念, 本文给出了符号差分比特之间关系的比特向量表示. 通过将 Lipmaa-Moriai 限制条件以及符号差分比特约束条件转化为可满足性模理论 (satisfiability modulo theories, SMT) 问题, 本文提出了一种基于 SAT/SMT 求解器的 ARX 结构不可能差分区分器自动化搜索工具. 该自动化工具是首个利用 Lipmaa-Moriai 限制条件以及符号差分搜索 ARX 结构不可能差分区分器的自动化工具. 通过利用符号差分, 该自动化工具可以捕捉连续比特以及非连续比特之间的关系; 通过利用 Lipmaa-Moriai 限制条件, 该自动化工具可以有效地过滤仅满足符号差分比特约束条件而不满足 Lipmaa-Moriai 限制条件的无效差分路径. 因此, 利用该自动化工具可以发现被传统搜索方法忽略的有效的不可能差分区分器. 将本文提出的自动化工具用于搜索具有常数 $c = \texttt{0xb7e15162}$ 的 Alzette (即 $A_{\texttt{0xb7e15162}}$) 的不可能差分区分器: 在输入差分汉明重量为 1、输出差分汉明重量为 1 的条件下, 我们发现了 4096 个不可能差分区分器; 在输入差分汉明重量为 2、输出差分汉明重量为 1 的条件下, 我们发现了 128 993 个不可能差分区分器. 然而, 在输入差分汉明重量为 2、输出差分汉明重量为 1 的条件下, 利用传统方法搜索 Alzette 的不可能差分区分器, 我们发现了 128 767 个不可能差分区分器, 证明本文提出的自动化工具能够更好地过滤无效差分路径. 因此, 利用本文提出的方法, 密码分析者可以更好地评估 ARX 结构抗不可能差分分析的安全性, 从而给出 ARX 结构更加精确的安全性评估结果. 同时, 由于 Alzette 是一个 SPECK 类结构, 我们分别利用本文提出的自动化搜索工具以及传统方法搜索 4 轮无密钥注入 SPECK64 [27] 的不可能差分区分器. 在输入差分汉明重量为 2、输出差分汉明重量为 1 的条件下, 我们分别发现了 128 976 个以及 128 018 个不可能差分区分器. $A_{\texttt{0xb7e15162}}$ 与 4 轮无密钥注入 SPECK64 的不可能差分区分器的数量如表 1 所示. 据我们所知, 这是首次利用不可能差分性质评估 Alzette 的安全性.

表 1 一步 $\boldsymbol{A}_{\texttt{0xb7e15162}}$ 与 4 轮无密钥注入 SPECK64 不可能差分区分器的数量

Table 1 Numbers of impossible differential characteristics for $\boldsymbol{A}_{\texttt{0xb7e15162}}$ and 4-round no-key SPECK64

Method	Cipher	$\mathbf{wt}(\texttt{InD}) = 1, \mathbf{wt}(\texttt{OutD}) = 1$	$\mathbf{wt}(\texttt{InD}) = 2, \mathbf{wt}(\texttt{OutD}) = 1$
本文提出的方法	$A_{\texttt{0xb7e15162}}$	4096	128 993
	No-key SPECK64	-	128 976
传统方法	$A_{\texttt{0xb7e15162}}$	-	128 767
	No-key SPECK64	-	128 018

本文结构安排如下: 第 2 节简要介绍本文中所用到的符号、Lipmaa-Moriai 限制条件、符号差分、Alzette 的结构以及 SPECK 算法等预备知识; 第 3 节介绍如何利用 Lipmaa-Moriai 限制条件以及符号差分比特约束条件, 构建基于 SAT/SMT 求解器的 ARX 结构不可能差分区分器自动化搜索工具; 第 4 节将新的自动化工具以及传统的搜索方法应用于搜索 Alzette 和 4 轮 SPECK64 的不可能差分区分器; 第 5 节总结本文工作.

2 符号、预备知识及算法简介

2.1 符号

本文中使用的符号如下所示:

$x\|y$: 比特串 x 与 y 的集联.
$x \wedge y$: x 与 y 的逐比特逻辑与.
$x \oplus y$: x 与 y 的逐比特异或.
$x \boxplus y$: x 加 y 模 2^n.
$\overline{x}$: x 的逐比特取反.
$\mathrm{wt}(x)$: x 的汉明重量.
$x[i]$: x 的第 i 比特, 其中 $i=0$ 为最低有效比特.
$x \ll r$: x 左移 r 个比特.
$x \gg r$: x 右移 r 个比特.
$x \lll r$: x 循环左移 r 个比特.
$x \ggg r$: x 循环右移 r 个比特.
Δx: x 与 x' 的异或差分: $\Delta x = x \oplus x'$.
$\Delta^+ x$: x 与 x' 的加法差分: $\Delta^+ x = x - x' \mod 2^n$.
$\Delta^\pm x$: x 与 x' 符号差分: $\Delta^\pm x[i] = x[i] - x'[i] \in \{-1, 0, 1\}$.
`InD`: 输入差分.
`OutD`: 输出差分.

2.2 预备知识

定义 1 (加法模 2^n [6]) 令 $x, y \in \mathbb{F}_2^n$, 则

$$x \boxplus y = x \oplus y \oplus \mathrm{carry}(x, y),$$

其中 $\mathrm{carry}(x,y) = (c[n-1], c[n-2], \cdots, c[0]) \in \mathbb{F}_2^n$ 是 $x \boxplus y$ 的进位比特向量, 递归定义为: $c[0] = 0$; $c[i+1] = (x[i] \wedge y[i]) \oplus (x[i] \wedge c[i]) \oplus (y[i] \wedge c[i])$, $0 \le i \le n-2$.

定义 2 (模加的异或差分概率 [6]) 加法模 2^n 的异或差分被定义为一个三元组 $(\alpha, \beta \mapsto \gamma)$, 其中 $\alpha, \beta \in \mathbb{F}_2^n$ 是两个输入差分、$\gamma \in \mathbb{F}_2^n$ 是输出差分. 则模加的异或差分概率被定义为

$$P(\alpha, \beta \mapsto \gamma) = \frac{\#\{(x,y) | (x \boxplus y) \oplus ((x \oplus \alpha) \boxplus (y \oplus \beta)) = \gamma\}}{\#\{(x,y)\}}.$$

在文献 [6] 中, Lipmaa 和 Moriai 研究了模加的异或差分概率, 并证明了一个异或差分三元组 $(\alpha, \beta \mapsto \gamma)$ 是有效的当且仅当

$$\mathrm{eq}(\alpha \ll 1, \beta \ll 1, \gamma \ll 1) \wedge (\alpha \oplus \beta \oplus \gamma \oplus (\beta \ll 1)) = 0, \tag{1}$$

其中

$$\mathrm{eq}(x, y, z) = (\overline{x} \oplus y) \wedge (\overline{x} \oplus z). \tag{2}$$

则, 如果 $(\alpha, \beta \mapsto \gamma)$ 是有效的, 模加的异或差分概率可以被如下计算:

$$P(\alpha, \beta \mapsto \gamma) = 2^{-\mathrm{wt}(\overline{\mathrm{eq}(\alpha,\beta,\gamma)} \wedge \mathrm{mask}(n-1))},$$

其中 $\mathrm{mask}(n-1)$ 表示 $0\|1^{n-1}$. 在下文中, 称公式 (1) 和公式 (2) 为 Lipmaa-Moriai 限制条件.

定义 3 (符号差分 [22–24]) 符号差分 $\Delta^\pm x$ 可以将异或差分分为三种情况:

(i) $\Delta^{\pm}x[i]=0$, 若 $x[i]=x'[i]$;

(ii) $\Delta^{\pm}x[i]=+1$, 若 $x[i]=1$ 且 $x'[i]=0$;

(iii) $\Delta^{\pm}x[i]=-1$, 若 $x[i]=0$ 且 $x'[i]=1$.

一个符号差分 $\Delta^{\pm}x$ 对应一个异或差分 Δx 以及一个加法差分 $\Delta^{+}x$:

$$\begin{aligned}\Delta x &= \bigoplus_{i=0}^{n-1} |\Delta^{\pm}x[i]| \cdot 2^i,\\ \Delta^{+}x &= \sum_{i=0}^{n-1} \Delta^{\pm}x[i] \cdot 2^i \bmod 2^n.\end{aligned} \tag{3}$$

根据公式 (3), 有如下推论.

推论 1 令 $x,x',y,y',z,z' \in \mathbb{F}_2^n$, $z = x \boxplus y$ 且 $z' = x' \boxplus y'$. 对于一个有效的异或差分三元组 $(\Delta x, \Delta y \mapsto \Delta z)$, $\Delta^{\pm}x$、$\Delta^{\pm}y$、$\Delta^{\pm}z$ 之间有如下关系:

$$\sum_{i=0}^{n-1} \Delta^{\pm}x[i] \cdot 2^i \bmod 2^n \boxplus \sum_{i=0}^{n-1} \Delta^{\pm}y[i] \cdot 2^i \bmod 2^n = \sum_{i=0}^{n-1} \Delta^{\pm}z[i] \cdot 2^i \bmod 2^n.$$

2.3 Alzette 简介

在 2020 年美密会议上, Beierle 等人 [2] 提出了一种名为 Alzette 的 64 比特基于 ARX 的 S 盒. 它是一种具有两个分支的 4 轮 SPECK 类结构, 并且由一个任意的常数 $c \in \mathbb{F}_2^{32}$ 来参数化. Alzette 的描述如算法 1、图 1 所示.

算法 1 Alzette 实例 A_c

Input: $(x,y) \in \mathbb{F}_2^{32} \times \mathbb{F}_2^{32}$
Output: $(u,v) \in \mathbb{F}_2^{32} \times \mathbb{F}_2^{32}$

$x \leftarrow x \boxplus (y \ggg 31)$;
$y \leftarrow y \oplus (x \ggg 24)$;
$x \leftarrow x \oplus c$;
$x \leftarrow x \boxplus (y \ggg 17)$;
$y \leftarrow y \oplus (x \ggg 17)$;
$x \leftarrow x \oplus c$;
$x \leftarrow x \boxplus (y \ggg 0)$;
$y \leftarrow y \oplus (x \ggg 31)$;
$x \leftarrow x \oplus c$;
$x \leftarrow x \boxplus (y \ggg 24)$;
$v \leftarrow y \oplus (x \ggg 16)$;
$u \leftarrow x \oplus c$;
return (u,v);

2.4 SPECK 简介

美国国家安全局 (NSA) 于 2013 年发布了 SPECK 族轻量分组密码算法 [27]. 根据算法的分组长度 (32、48、64、96 以及 128 比特), 共包括 5 类分组密码算法: SPECK32、SPECK48、SPECK64、SPECK96 以及 SPECK128. 通常, SPECK2n/mn 表示具有 $2n$ 比特分组长度以及 mn 比特密钥长度的 SPECK 算法, 其中 $n \in \{16,24,32,48,64\}$、$m \in \{2,3,4\}$ 且依赖于 n 的取值. 令 (L_{i-1}, R_{i-1}) 表示第 i 轮的输入, 则第 i 轮的输出如下计算:

$$\begin{aligned}L_i &\leftarrow (L_{i-1} \ggg \alpha) \boxplus R_{i-1} \oplus K_i,\\ R_i &\leftarrow (R_{i-1} \lll \beta) \oplus L_i,\end{aligned}$$

其中 K_i 表示轮密钥. 当分组长度是 32 比特时, $(\alpha,\beta)=(7,2)$, 否则 $(\alpha,\beta)=(8,3)$. SPECK 的轮函数如图 2 所示.

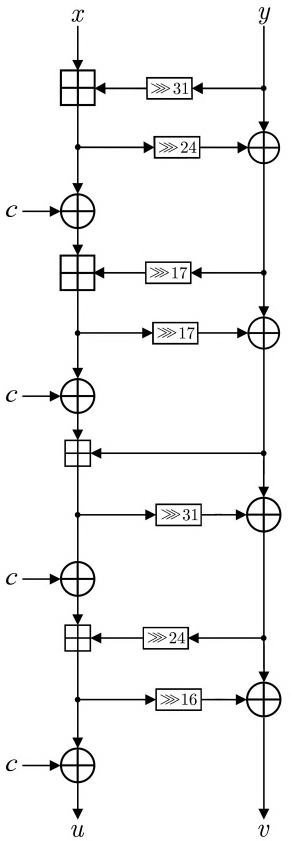

图 1 Alzette 实例 A_c
Figure 1 Alzette instance A_c

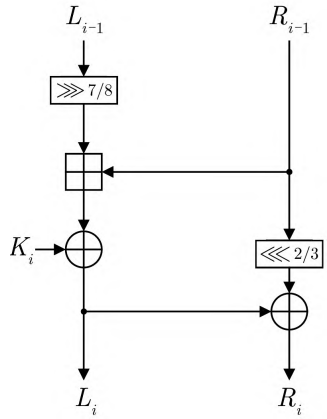

图 2 SPECK 轮函数
Figure 2 Round function of SPECK

3 基于 SAT/SMT 求解器的 ARX 结构不可能差分区分器自动化搜索工具

在本节中, 我们提出了一种新的基于 SAT/SMT 求解器的 ARX 结构不可能差分区分器自动化搜索工具. 由于该自动化工具不仅包含了传统搜索方法所包含的约束条件 (Lipmaa-Moriai 限制条件), 还包含了传统搜索方法未包含的约束条件 (符号差分比特约束条件), 因此, 该自动化工具能够更好地过滤无效的差分路径, 并找到被传统搜索方法所遗漏的有效的不可能差分区分器。

3.1 构建基于 SAT/SMT 求解器的 ARX 结构不可能差分区分器自动化搜索工具

在文献 [20] 中, Mouha 等人利用 SAT/SMT 求解器自动化搜索 3 轮 Salsa20 的最优差分路径. 尽管他们发现了一些差分路径是无效的, 但他们的搜索模型中仅包含了 Lipmaa-Moriai 限制条件以及异或差分的传播, 这意味着他们的模型无法自动地过滤那些满足 Lipmaa-Moriai 限制条件以及异或差分传播的无效差分路径.

为了自动地过滤这些特殊的差分路径, 本文提出的自动化搜索工具不仅包含了传统搜索方法所包含的约束条件, 还包含了符号差分的传播以在异或差分传播中添加值传播的信息.

本文将搜索不可能差分区分器的问题转化为布尔可满足性问题 (Boolean satisfiability problem, SAT), 然后利用 SAT 求解器进行求解. 然而, ARX 结构所包含的都是 n 比特向量上的操作, 但是 SAT 问题仅能包含布尔变量以及与 (AND)、或 (OR)、非 (NOT) 操作. 由于 SMT 问题支持比特向量变量以

及比特向量操作, 且 SMT 问题是 SAT 问题的推广, 因此本文使用 SMT 问题来代替 SAT 问题. 一旦一个 SMT 问题被建立, SMT 求解器可将 SMT 问题转化为 SAT 问题, 并利用 SAT 求解器进行求解. STP 求解器 [28] 是一个典型的 SMT 求解器, 我们利用 STP 求解器求解本文中所有的 SMT 问题.

本文采用 Mouha 等人的方法来描述 Lipmaa-Moriai 限制条件以及异或差分传播, 详情请参阅文献 [20]. 在下文中, 不失一般性的, 假设所有的异或差分变量 Δa 的字长都为 n.

为了描述符号差分, 对每一个异或差分变量 Δa 创建集合 $\mathcal{A} = \{a_0^s, a_1^s, \cdots, a_{n-1}^s\}$, 其中 $a_0^s, a_1^s, \cdots, a_{n-1}^s \in \mathbb{F}_2^m$. 于是, 可以用 a_i^s 来表示 $\Delta^{\pm}a[i]$. 然而, 由于 SAT/SMT 问题中不包含带符号的变量, 无法直接表示符号差分. 为了克服这个问题, 当 $\Delta^{\pm}a[i] = -1$ 时, 本文用 a_i^s 的补码来表示 $\Delta^{\pm}a[i]$, 其中 $0 \le i \le n-1$. 此外, 由于循环移位以及移位操作可能会将异或差分变量的最高有效比特移动至其他位置, 则 $\Delta^{\pm}a[n-1] = -1$ 与 $\Delta^{\pm}a[n-1] = 1$ 是不同的. 因此, 需要令 $m > n$. 于是, 我们有

$$a_i^s = \begin{cases} 0^m, & \text{if } \Delta^{\pm}a[i] = 0, \\ 1^{m-i} \parallel 0^i, & \text{if } \Delta^{\pm}a[i] = -1, \\ 0^{m-i-1} \parallel 1 \parallel 0^i, & \text{if } \Delta^{\pm}a[i] = 1, \end{cases}$$

其中, $0 \le i \le n-1$. 我们将 $a_0^s, a_1^s, \cdots, a_{n-1}^s$ 命名为比特符号差分变量.

为了处理模加的符号差分传播, 本文对每个模加的每个输入、输出变量创建一个新的变量, 这些新变量的字长都是 n. 我们分别将这些新变量命名为 MAI 符号差分变量以及 MAO 符号差分变量. 每一个 MAI 符号差分变量以及 MAO 符号差分变量的值等于其对应的比特符号差分变量的加法和模 2^n. 对于每一个模加操作, 其对应 MAO 符号差分变量的值还需等于对应的两个 MAI 符号差分变量的加法和模 2^n. 例如: 假设 $\mathcal{A} = \{a_0^s, a_1^s, \cdots, a_{n-1}^s\}$、$\mathcal{B} = \{b_0^s, b_1^s, \cdots, b_{n-1}^s\}$、$\mathcal{C} = \{c_0^s, c_1^s, \cdots, c_{n-1}^s\}$ 表示一个模加操作的输入、输出比特符号差分变量的集合, 且 $\mathcal{SUM}_{\mathcal{A}}$、$\mathcal{SUM}_{\mathcal{B}}$、$\mathcal{SUM}_{\mathcal{C}}$ 表示该模加操作的 MAI 符号差分变量以及 MAO 符号差分变量. 那么, 如果以下等式成立, 则 $\mathcal{A}$、$\mathcal{B}$、$\mathcal{C}$ 的赋值是有效的.

$$\begin{cases} \mathcal{SUM}_{\mathcal{A}} = \sum\limits_{i=0}^{n-1} a_i^s \bmod 2^n, \\ \mathcal{SUM}_{\mathcal{B}} = \sum\limits_{i=0}^{n-1} b_i^s \bmod 2^n, \\ \mathcal{SUM}_{\mathcal{C}} = \sum\limits_{i=0}^{n-1} c_i^s \bmod 2^n, \\ \mathcal{SUM}_{\mathcal{C}} = \mathcal{SUM}_{\mathcal{A}} \boxplus \mathcal{SUM}_{\mathcal{B}}. \end{cases}$$

对于一个变量分支与一个常数的异或操作的符号差分传播, 由于输出符号差分的取值依赖于常数, 本文用定理 1 处理这种情况.

定理 1 令 $x, x', y, y', z, z' \in \mathbb{F}_2^n$. 对于 $z = x \oplus C$ 以及 $z' = x' \oplus C$, 假设 C 是常数, 则有 $\Delta z = \Delta x$ 以及如下符号差分比特之间的关系:

$$\Delta^{\pm}z[i] = \begin{cases} \Delta^{\pm}x[i], & \text{if } C[i] = 0 \\ -\Delta^{\pm}x[i], & \text{if } C[i] = 1, \end{cases} \tag{4}$$

其中, $0 \le i \le n-1$.

我们可以用公式 (4) 来描述一个变量分支与一个常数的异或操作的符号差分传播.

对于循环移位的符号差分传播, 尽管循环移位对符号差分的影响与其对异或差分的影响相同, 但它们在 STP 中的描述方式有很大差别. 在此, 我们只关注如何处理循环左移的情况. 对循环右移的处理方法可以很容易地从处理循环左移的方法中导出. 对于一个 n 比特的异或差分变量 Δa, 假设它是循环左移 t 比特操作的输入异或差分, 根据前述方法, 我们有 n 个字长为 m 比特的比特符号差分变量 a_i^s, 其中

$0 \le i \le n-1$. 令 $b_i^s \in \mathbb{F}_2^m$ 表示 $a_i^s \lll t$ 对应的输出比特符号差分变量, 其中 $0 \le i \le n-1$. 那么需要分两种情况处理循环左移 t 比特操作.

(1) 当 $0 \le i \le n-1-t$ 时, 有

$$b_{i+t}^s = a_i^s \lll t.$$

(2) 当 $n-t \le i \le n-1$ 时, 有

$$b_{i+t-n}^s = \begin{cases} a_i^s \gg n-t, & \text{if } \Delta^{\pm} a[i] \neq -1, \\ 1^{m+n-i-t} \| 0^{i+t-n}, & \text{if } \Delta^{\pm} a[i] = -1. \end{cases}$$

使用上述方法, 可以构建一个描述 Lipmaa-Moriai 限制条件、异或差分传播以及符号差分传播的 SAT/SMT 求解模型. 如果对 ARX 结构的输入差分 (InD) 以及输出差分 (OutD) 进行赋值, 则可以得到指定输入差分到指定输出差分是否是一个可能的映射, 即: $\mathtt{InD} \nleftrightarrow \mathtt{OutD}$ 或者 $\mathtt{InD} \leftrightarrow \mathtt{OutD}$. 通过在本文提出的搜索模型中添加以下两条命令, 即可完成该映射的可能性判断:

QUERY(FALSE),

COUNTEREXAMPLE.

当 STP 返回 Valid 时, 则 $\mathtt{InD} \nleftrightarrow \mathtt{OutD}$, 即找到一个不可能差分区分器; 当 STP 返回一条差分路径时, 则 $\mathtt{InD} \leftrightarrow \mathtt{OutD}$, 且该差分路径是有效的.

至此, 我们可以通过以上完整的架构来构建用于搜索 ARX 结构不可能差分区分器的自动化工具. 该自动化工具可以有效地过滤不符合 Lipmaa-Moriai 限制条件以及符号差分比特约束条件的无效差分路径.

4 自动化搜索 Alzette 和无密钥注入的 SPECK64 不可能差分区分器

在本节中, 我们将第 3 节中提出的自动化工具用于搜索 Alzette 和无密钥注入的 SPECK64 不可能差分区分器, 并找到了被传统搜索方法忽略的不可能差分区分器.

在文献 [2] 中, Alzette 的设计者宣称, Alzette 的设计安全性指标之一是两步 Alzette (即 8 轮) 的差分界与线性界要强于 8 轮 SPECK64. 在 Alzette 以及 SPARKLE 的设计文档中, 设计者仅通过搜索不同步数 Alzette 的最优 (或次优) 差分路径来评估其抗差分分析的安全性. 除了上述设计文档外, 唯一对 Alzette 的安全性分析结果发表在 2021 年欧密会议上 [29]. 然而, 文献 [29] 中的安全性分析是关于差分-线性密码分析的. 到目前为止, 还没有任何对 Alzette 不可能差分区分器的公开分析结果. 由于 Alzette 是一个 S 盒, 因此最直接的分析其抗差分类分析安全性的方法是计算它的差分分布表 (difference distribution table, DDT). 然而, 由于 Alzette 是操作在 64 比特上的 S 盒, 计算其 DDT 是无法实现的. 因此, 需通过间接的方法评估其差分的分布情况. 对于任意操作在 n 比特上的 S 盒, 对于任意给定的输入差分, 有如下性质:

$$\sum_{i=0}^{2^n-1} P(\mathtt{InD} \to \mathtt{OutD}_i) = 1,$$

其中 $\mathtt{OutD}_i$ 表示 $\mathtt{OutD} = i$. 因此, 若一个 S 盒的 DDT 中为 0 的项越少, 该 S 盒的差分呈现较为均匀分布的概率越高, 则该 S 盒能够较好抗差分类分析的概率越高. 由此可见, 搜索 Alzette 的不可能差分区分器对评估 Alzette 抗差分类分析的安全性是十分有意义的.

由于 Alzette 没有密钥注入, 为了更好地对比 Alzette 与 SPECK64 的安全性, 本文搜索无密钥注入的 SPECK64 不可能差分区分器. 其次, 由于每一步 Alzette 使用不同的常数进行实例化, 而无论几轮的无密钥注入 SPECK64 都相当于使用全 0 密钥进行实例化, 因此搜索一步 Alzette 与 4 轮 SPECK64 的不可能差分区分器能够更好地对比 Alzette 与 SPECK64 的安全性.

4.1 自动化搜索 Alzette 不可能差分区分器

在搜索一步 Alzette 不可能差分区分器时, 本文选择常数 $c = \texttt{0xb7e15162}$ (SPARKLE 使用的 8 个常数之一) 来实例化 Alzette.

(1) 在 $\mathrm{wt}(\texttt{InD}) = 1$ 且 $\mathrm{wt}(\texttt{OutD}) = 1$ 的限制条件下, 利用本文提出的自动化工具, 我们找到了 4096 个不可能差分区分器; 利用传统搜索方法, 我们同样找到了 4096 个不可能差分区分器.

(2) 在 $\mathrm{wt}(\texttt{InD}) = 2$ 且 $\mathrm{wt}(\texttt{OutD}) = 1$ 的限制条件下, 利用本文提出的自动化工具, 我们找到了 128 993 个不可能差分区分器; 利用传统搜索方法, 我们仅找到 128 767 个不可能差分区分器.

上述结果说明, 利用仅包含 Lipmaa-Moriai 限制条件以及异或差分传播的传统方法搜索 ARX 结构不可能差分区分器, 可能会遗漏一些有效的不可能差分区分器; 然而, 利用本文提出的自动化工具, 我们可以搜索到这些区分器.

4.2 自动化搜索无密钥注入 SPECK64 不可能差分区分器

为了更好地对比 Alzette 与 SPECK64 的安全性, 本文搜索 4 轮无密钥注入 SPECK64 的不可能差分区分器.

在 $\mathrm{wt}(\texttt{InD}) = 2$ 且 $\mathrm{wt}(\texttt{OutD}) = 1$ 的限制条件下, 利用本文提出的自动化工具, 我们找到了 128 976 个不可能差分区分器; 利用传统搜索方法, 我们仅找到 128 018 个不可能差分区分器.

我们发现, 无论利用本文提出的自动化工具还是利用传统方法, 一步 Alzette 不可能差分区分器的数量都多于 4 轮无密钥注入 SPECK64 不可能差分区分器的数量. 因此, 如果从搜索不可能差分区分器的角度来评估 ARX 结构的差分分布, Alzette 抗差分分析的安全性可能弱于 SPECK64, 这与 Alzette 设计者的结论相反. 尽管 Alzette 的设计者利用两步 Alzette 最优差分路径的概率小于 8 轮 SPECK64 来证明 Alzette 抗差分分析的安全性强于 SPECK64, 但是由于 Alzette 是一个 S 盒, 因此, 只能通过差分的概率而不是差分路径的概率来评估其安全性. 然而, Alzette 与 SPECK64 的差分概率之间的大小关系无法由最优差分路径概率之间的大小关系导出. 因此, Alzette 设计团队的安全性评估是不够全面的. 据我们所知, 这是首次利用不可能差分性质评估 Alzette 的安全性.

5 结论

本文研究了 Alzette 抗差分类分析的安全性. 对于模加操作上的有效异或差分, 通过利用符号差分的概念, 本文给出了符号差分比特之间关系的比特向量表示. 通过将 Lipmaa-Moriai 限制条件以及符号差分比特约束条件转化为 SMT 问题, 本文提出了一种基于 SAT/SMT 求解器的 ARX 结构不可能差分区分器自动化搜索工具. 该自动化工具是首个利用 Lipmaa-Moriai 限制条件以及符号差分搜索 ARX 结构不可能差分区分器的自动化工具. 利用该工具可以发现被传统搜索方法忽略的有效的不可能差分区分器. 利用上述自动化工具以及传统方法搜索 Alzette 的不可能差分区分器, 我们发现, 该自动化工具能够发现更多的不可能差分区分器, 证明该自动化工具能够更好地过滤无效差分路径. 此外, 将该自动化搜索工具用于搜索 4 轮无密钥注入 SPECK64 不可能差分区分器, 我们发现 4 轮无密钥注入 SPECK64 不可能差分区分器的数量少于 Alzette 不可能差分区分器的数量, 说明 Alzette 设计团队的安全性评估是不够全面的. 据我们所知, 这是首次利用不可能差分性质评估 Alzette 的安全性. 我们希望本文提出的方法有助于评估 ARX 结构抗差分类分析的安全性并有助于 ARX 密码的设计.

参考文献

[1] NIST. Lightweight Cryptography Standardization Process[S]. 2017. https://csrc.nist.gov/projects/lightweight-cryptography.

[2] BEIERLE C, BIRYUKOV A, DOS SANTOS L C, et al. Alzette: A 64-bit ARX-box—(Feat. CRAX and TRAX)[C]. In: Advances in Cryptology—CRYPTO 2020, Part III. Springer Cham, 2020: 419–448. [DOI: 10.1007/978-3-030-56877-1_15]

[3] BIHAM E, SHAMIR A. Differential cryptanalysis of DES-like cryptosystems[J]. Journal of Cryptology, 1991, 4(1): 3–72. [DOI: 10.1007/BF00630563]

[4] BIHAM E, BIRYUKOV A, SHAMIR A. Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials[C]. In: Advances in Cryptology—EUROCRYPT '99. Springer Berlin Heidelberg, 1999: 12–23. [DOI: 10.1007/3-540-48910-X_2]
[5] KNUDSEN L R. DEAL: A 128-bit block cipher[R]. Technical Report 151, Department of Informatics, University of Bergen, Bergen, Norway, 1998.
[6] LIPMAA H, MORIAI S. Efficient algorithms for computing differential properties of addition[C]. In: Fast Software Encryption—FSE 2001. Springer Berlin Heidelberg, 2001: 336–350. [DOI: 10.1007/3-540-45473-X_28]
[7] MOUHA N, VELICHKOV V, CANNIÈRE C D, et al. The differential analysis of S-functions[C]. In: Selected Areas in Cryptography—SAC 2010. Springer Berlin Heidelberg, 2010: 36–56. [DOI: 10.1007/978-3-642-19574-7_3]
[8] AZIMI S A, RANEA A, SALMASIZADEH M, et al. A bit-vector differential model for the modular addition by a constant[C]. In: Advances in Cryptology—ASIACRYPT 2020, Part I. Springer Cham, 2020: 385–414. [DOI: 10.1007/978-3-030-64837-4_13]
[9] LAI X J, MASSEY J L, MURPHY S. Markov ciphers and differential cryptanalysis[C]. In: Advances in Cryptology—EUROCRYPT '91. Springer Berlin Heidelberg, 1991: 17–38. [DOI: 10.1007/3-540-46416-6_2]
[10] BIRYUKOV A, ROY A, VELICHKOV V. Differential analysis of block ciphers SIMON and SPECK[C]. In: Fast Software Encryption—FSE 2014. Springer Berlin Heidelberg, 2014: 546–570. [DOI: 10.1007/978-3-662-46706-0_28]
[11] BIRYUKOV A, VELICHKOV V, CORRE Y L. Automatic search for the best trails in ARX: Application to block cipher SPECK[C]. In: Fast Software Encryption—FSE 2016. Springer Berlin Heidelberg, 2016: 289–310. [DOI: 10.1007/978-3-662-52993-5_15]
[12] LIU Z B, LI Y Q, JIAO L, et al. A new method for searching optimal differential and linear trails in ARX ciphers[J]. IEEE Transactions on Information Theory, 2020, 67(2): 1054–1068. [DOI: 10.1109/TIT.2020.3040543]
[13] LIU Z B, LI Y Q, WANG M S. Optimal differential trails in SIMON-like ciphers[J]. IACR Transactions on Symmetric Cryptology, 2017, 2017(1): 358–379. [DOI: 10.13154/tosc.v2017.i1.358-379]
[14] FU K, WANG M Q, GUO Y H, et al. MILP-based automatic search algorithms for differential and linear trails for SPECK[C]. In: Fast Software Encryption—FSE 2016. Springer Berlin Heidelberg, 2016: 268–288. [DOI: 10.1007/978-3-662-52993-5_14]
[15] ZHOU C N, ZHANG W T, DING T Y, et al. Improving the MILP-based security evaluation algorithms against differential cryptanalysis using divide-and-conquer approach[J/OL]. IACR Cryptology ePrint Archive, 2019: 2019/19. https://eprint.iacr.org/2019/19.pdf
[16] ANKELE R, KÖLBL S. Mind the gap—A closer look at the security of block ciphers against differential cryptanalysis[C]. In: Selected Areas in Cryptography—SAC 2018. Springer Cham, 2018: 163–190. [DOI: 10.1007/978-3-030-10970-7_8]
[17] ANKELE R, LIST E. Differential cryptanalysis of round-reduced Sparx-64/128[C]. In: Applied Cryptography and Network Security—ACNS 2018. Springer Cham, 2018: 459–475. [DOI: 10.1007/978-3-319-93387-0_24]
[18] HAN Y. Automatically Search for Three Types of Block Cipher Distinguishers Based on SAT/SMT Solver[D]. Beijing: University of Chinese Academy of Sciences, 2018.
韩亚. 基于 SAT/SMT 自动搜索三类分组密码区分器研究 [D]. 北京: 中国科学院大学, 2018.
[19] KÖLBL S, LEANDER G, TIESSEN T. Observations on the SIMON block cipher family[C]. In: Advances in Cryptology—CRYPTO 2015, Part I. Springer Berlin Heidelberg, 2015: 161–185. [DOI: 10.1007/978-3-662-47989-6_8]
[20] MOUHA N, PRENEEL B. Towards finding optimal differential characteristics for ARX: Application to Salsa20[J/OL]. IACR Cryptology ePrint Archive, 2013: 2013/328. https://eprint.iacr.org/2013/328.pdf
[21] ROH D Y, KOO B W, JUNG Y H, et al. Revised version of block cipher CHAM[C]. In: Information Security and Cryptology—ICISC 2019. Springer Cham, 2019: 1–19. [DOI: 10.1007/978-3-030-40921-0_1]
[22] WANG X Y, LAI X J, FENG D G, et al. Cryptanalysis of the hash functions MD4 and RIPEMD[C]. In: Advances in Cryptology—EUROCRYPT 2005. Springer Berlin Heidelberg, 2005: 1–18. [DOI: 10.1007/11426639_1]
[23] WANG X Y, YIN Y L, YU H B. Finding collisions in the full SHA-1[C]. In: Advances in Cryptology—CRYPTO 2005. Springer Berlin Heidelberg, 2005: 17–36. [DOI: 10.1007/11535218_2]
[24] WANG X Y, YU H B. How to break MD5 and other hash functions[C]. In: Advances in Cryptology—EUROCRYPT 2005. Springer Berlin Heidelberg, 2005: 19–35. [DOI: 10.1007/11426639_2]
[25] LEURENT G. Analysis of differential attacks in ARX constructions[C]. In: Advances in Cryptology—ASIACRYPT 2012. Springer Berlin Heidelberg, 2012: 226–243. [DOI: 10.1007/978-3-642-34961-4_15]
[26] YU H B, CHEN J Z, JIA K T, et al. Near-collision attack on the step-reduced compression function of Skein-

256[J/OL]. IACR Cryptology ePrint Archive, 2011: 2011/148. https://eprint.iacr.org/2011/148.pdf
[27] BEAULIEU R, SHORS D, SMITH J, et al. The SIMON and SPECK families of lightweight block ciphers[J/OL]. IACR Cryptology ePrint Archive, 2013: 2013/404. https://eprint.iacr.org/2013/404.pdf
[28] GANESH V, DILL D L. A decision procedure for bit-vectors and arrays[C]. In: Computer Aided Verification—CAV 2007. Springer Berlin Heidelberg, 2007: 519–531. [DOI: 10.1007/978-3-540-73368-3_52]
[29] LIU Y W, SUN S W, LI C. Rotational cryptanalysis from a differential-linear perspective—Practical distinguishers for round-reduced FRIET, Xoodoo, and Alzette[C]. In: Advances in Cryptology—EUROCRYPT 2021, Part I. Springer Cham, 2021: 741–770. [DOI: 10.1007/978-3-030-77870-5_26]

作者信息

许峥 (1992–)，河南郑州人，博士．主要研究领域为对称密码的安全性分析．
xuzheng@iie.ac.cn

王明生 (1967–)，四川绵阳人，研究员．主要研究领域为对称密码算法的安全性分析与设计．
wangmingsheng@iie.ac.cn

李永强 (1982–)，吉林集安人，副研究员．主要研究领域为对称密码算法的安全性分析与设计．
yongq.lee@gmail.com