

基于 SAT 方法进一步加速差分特征的搜索

许峥^{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)

摘 要: 回顾了孙等使用 Matsui 边界条件加速差分特征搜索的方法, 为了进一步提高搜索效率, 改进了 Matsui 边界条件以及利用 Matsui 边界条件加速差分特征自动化搜索的方法, 并提出了一种改进的方法来搜索分组密码的最优差分特征。研究了线程数和询问条件的加速效果并提出了选择线程数以及询问条件的策略。使用 STP 和 CryptoMiniSat 分别搜索概率为 2^{-24} 、 2^{-25} 、 2^{-26} 的 8 轮 SPECK96 差分特征以及概率为 2^{-39} 的 11 轮 HIGHT 差分特征, 并比较了在不同线程数和询问条件下求解 SAT/SMT 问题的耗时。研究发现线程数对搜索差分特征的耗时影响较大, 而询问条件对搜索差分特征的耗时影响较小, 从而提出了一种如何选择线程数和询问条件的策略。根据所提策略, 使用改进的边界条件和方法搜索 HIGHT 的 11 轮最优差分特征, 并首次获得了 HIGHT 的 11 轮最优差分特征的紧致概率, 即 2^{-45} 。现有的 11 轮 HIGHT 最优差分特征概率的最紧致边界是 $P_{\text{opt}}^{11} \geq 2^{-45}$ 。这就意味着, 利用现有 11 轮 HIGHT 最优差分特征概率的最紧致边界无法给出 11 轮 HIGHT 抗差分分析安全性的精确评估。因此, 所提策略的结果是目前已知的最优结果。

关键词: 差分分析; 差分特征; 自动化搜索; SAT 求解器

中图分类号: TP309.7

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2022066

Further accelerating the search of differential characteristics based on the SAT method

XU Zheng^{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

Abstract: Sun et al.'s method of using Matsui's bounding conditions to accelerate the search of differential characteristics was reviewed. Matsui's boundary conditions and Sun et al.'s method of using Matsui's bounding conditions to accelerate the search of differential characteristics were improved for better search efficiency. Then an improved method to search for the optimal differential characteristics in block ciphers was proposed. Besides, the

收稿日期: 2021-11-15; 修回日期: 2022-03-30

通信作者: 许峥, xuzheng@iie.ac.cn

基金项目: 国家自然科学基金 (61772516, 61772517)

Foundation Item: The National Natural Science Foundation of China (61772516, 61772517)

引用格式: 许峥. 基于 SAT 方法进一步加速差分特征的搜索[J]. 网络与信息安全学报, 2022, 8(5): 129-139.

Citation Format: XU Z. Further accelerating the search of differential characteristics based on the SAT method[J]. Chinese Journal of Network and Information Security, 2022, 8(5): 129-139.

accelerating effects of the number of threads and the query condition were investigated, and a strategy for choosing the number of threads and the query condition were proposed. STP and CryptoMiniSat were used to search for 8-round SPECK96 differential characteristics with probabilities of 2^{-24} , 2^{-25} , 2^{-26} and 11-round HIGHT differential characteristics with a probability of 2^{-39} , then the time-consuming of solving SAT/SMT problems under different number of threads and query conditions were compared. It was found that the number of threads has a great effect on the time consumption of searching for differential characteristics, while the query condition may have little effect on the time consumption of searching for differential characteristics. Then, a strategy on how to select the number of threads and the query condition was proposed. Furthermore, it was found that STP can affect the overall efficiency of the search. According to the proposed strategy, the 11-round optimal differential characteristics of HIGHT were searched by using the improved bounding conditions and improved method. A tight bound for the probability of the 11-round optimal differential characteristics of HIGHT was obtained for the first time, i.e. 2^{-45} . To the best of our knowledge, the existing tightest bound of the optimal 11-round HIGHT is $P_{\text{Opt}}^{11} \geq 2^{-45}$. This means that using the existing tightest bound of the optimal 11-round HIGHT cannot give an accurate evaluation of the security of 11-round HIGHT against differential cryptanalysis. Therefore, the result is the best-known result.

Keywords: differential cryptanalysis, differential characteristics, automatic search, SAT solver

0 引言

20 世纪 90 年代初, Biham 和 Shamir 提出了差分分析^[1]。差分分析最初是一种用于评估 DES 分组密码安全性的密码分析方法, 后来被用于评估各种分组密码的安全性。对于对称密码原语的密码分析, 差分分析是评估对称密码原语安全性的最强技术之一。此外, 抗差分分析是现代分组密码算法的主要设计标准。

对于差分分析, 一个关键的步骤是找到高概率的差分特征。目前, 使用自动化方法搜索差分特征已成为一种新趋势。在 1994 年欧密会议上^[2], Matsui 提出了一种分支定界算法来自动化搜索基于 S 盒的分组密码的最优差分特征。后来, Matsui 的算法被用于自动化搜索 ARX 密码的差分特征^[3-6]。

21 世纪初期, 自动化工具由于在搜索分组密码的差分特征方面表现出优越的性能而备受关注。最重要的自动化工具之一是基于混合整数线性规划 (MILP) 的方法。Mouha 等^[7]首次引入了该方法, 并用其评估了差分、线性活跃 S 盒数量的下界。后来, 上述方法被改进并应用于搜索面向比特的分组密码的 (相关密钥) 差分特征。此外, MILP 方法被进一步应用于搜索各种类型的区分器^[8-11]。

另一种备受关注的自动化工具是基于布尔可满足性问题 (SAT) 的方法。2013 年, Mouha 等^[12]首次引入了该方法, 并将其用于搜索 Salsa20 的 3 轮最优差分特征。后来, 在 2015 年美密会议上, Kölbl 等^[13]使用上述方法搜索 SIMON 的最优差分特征和线性特征。此外, SAT 方法被进一步应用于搜索各种类型的区分器^[14-18]。

为了使用上述自动化工具搜索差分特征, 密码分析者只需要将差分传播转化为相应的不等式或约束条件, 这极大地简化了密码分析者的工作, 并最大限度地减少了人为错误的可能性。然而, 上述两种自动化工具在搜索阶段的执行效率取决于第三方求解器的性能、差分性质的等式/不等式的表示方式以及一些优化策略。

为了提高 MILP 方法的效率, 密码分析者提出了多种优化策略。2017 年, Sasaki 和 Todo^[19]对于描述 S 盒的差分传播提出了一种确保不等式数量最少的方法。在 2018 年 ISC 会议上, Zhang 等^[20]通过将 Matsui 边界条件加入 MILP 模型中来加速差分特征的搜索。2019 年, Zhou 等^[21]利用差分特征概率与活跃 S 盒数量之间的关系优化差分特征的搜索。2020 年, Boura 和 Coggia^[22]对于 SPN 结构的 S 盒以及线性层提出了高效的 MILP 模型, 以提高搜索效率。

然而, 与 MILP 方法效率的提高相比, 使用

SAT 方法对自动化搜索加速的研究相对滞后。2016 年, Song 等^[23]提出了一种启发式的方法搜索 ARX 密码更好的差分特征。2021 年, Sun 等^[24]通过将 Matsui 边界条件加入 SAT 方法中来加速差分特征的搜索。

当密码分析者利用 SAT 方法搜索分组密码的最优差分特征时, 他们经常使用 STP^[25]以及 CryptoMiniSat^[26]。由于 CryptoMiniSat 支持多线程且 STP 支持多种询问条件, 本文提出以下两个问题。① 使用多线程是否可以加速搜索? ② 使用不同的询问条件是否会影响搜索的耗时? 因此, 研究线程数和询问条件的加速效果是十分重要的。

本文改进了文献[24]中的方法, 并且研究了线程数和询问条件的加速效果, 主要贡献有以下 3 方面。

(1) 改进的边界条件

在文献[24]中, Sun 等将 Matsui 边界条件转化为合取范式 (CNF) 的形式并将其加入 SAT 方法中来加速差分特征的搜索。由于搜索空间可以被进一步减小, 他们的方法可以被优化。为了进一步提高搜索效率, 本文改进了 Matsui 边界条件并提出了一种改进的方法搜索分组密码的最优差分特征。

(2) 选择线程数以及询问条件的策略

为了研究线程数和询问条件的加速效果, 本文使用 STP 和 CryptoMiniSat 分别搜索 SPECK96 和 HIGHT 的差分特征, 并比较了在不同线程数和询问条件下求解 SAT/SMT 问题的耗时。本文的实验结果表明, 线程数对搜索差分特征的耗时影响较大, 而询问条件对搜索差分特征的耗时影响较小。从而, 本文提出了一种如何选择线程数和询问条件的策略, 并发现 STP 会影响搜索的整体效率。

(3) 自动化搜索 HIGHT 的 11 轮最优差分特征

根据所提策略, 本文使用改进的边界条件和方法搜索 HIGHT 的 11 轮最优差分特征, 并首次获得了 HIGHT 的 11 轮最优差分特征的紧致概率, 即 2^{-45} 。由于现有的 11 轮 HIGHT 最优差分特征概率的最紧致边界是 $P_{\text{Opt}}^{11} \geq 2^{-45}$ ^[6], 因此, 本文的结果是目前已知的最优结果。

1 符号、预备知识及算法简介

1.1 符号

本文使用的符号及含义如表 1 所示。

表 1 符号及含义
Table 1 Notations and descriptions

符号	含义
$x \parallel y$	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 加模 2^n
$\bar{x}$	x 的逐比特取反
$wt(x)$	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 $\Delta x = x \oplus x'$

1.2 预备知识

定义 1 加法模 2^n ^[27]

令 $x, y \in \mathbb{F}_2^n$, 则 $x \boxplus y = x \oplus y \oplus \text{carry}(x, y)$, 其中 $\text{carry}(x, y) = (c[n-1], \dots, c[1], c[0]) \in \mathbb{F}_2^n$ 是 $x \boxplus y$ 的进位比特向量, 其递归的定义为 $c[0] = 0; c[i+1] = (x[i] \wedge y[i]) \oplus (x[i] \wedge ci[i]) \oplus ((y[i] \wedge c[i]), 0 \leq i \leq n$ 。

定义 2 模加的异或差分概率^[27]

加法模 2^n 上的一组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。那么, 模加的异或差分概率被定义为

$$P(\alpha, \beta \mapsto \gamma) = \frac{\#\{(x, y) \mid (x \boxplus y) \oplus ((x \oplus \alpha) \boxplus (y \oplus \beta)) = \gamma\}}{\#\{(x, y)\}} \quad (1)$$

在文献[27]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

$$\text{eq}(\alpha \ll 1, \beta \ll 1, \gamma \ll 1) \wedge (\alpha \oplus \beta \oplus \gamma \oplus (\beta \ll 1)) = 0 \quad (2)$$

其中

$$\text{eq}(x, y, z) = (\bar{x} \oplus y) \wedge (\bar{x} \oplus z) \quad (3)$$

下文将式(2)和式(3)称为 L-M 条件 (L-M conditions)。此外, 如果 $(\alpha, \beta \mapsto \gamma)$ 是有效的, 则模加的异或差分概率可以按式(4)计算。

$$P(\alpha, \beta \mapsto \gamma) = 2^{-\text{wt}(\text{eq}(\alpha, \beta, \gamma) \wedge \text{mask}(n-1))} \quad (4)$$

其中 $\text{mask}(n-1)$ 表示 $0 \| 1^{n-1}$ 。

1.3 SPECK 简介

2013 年, 美国国家安全局 (NSA) 发布了 SPECK 族分组密码算法^[28]。根据算法的分组长度 (32 bit、48 bit、64 bit、96 bit 以及 128 bit), SPECK 共包括 5 种分组密码算法 (SPECK32、SPECK48、SPECK64、SPECK96 以及 SPECK128)。通常, $\text{SPECK}_{2n/mn}$ 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 轮的输出计算如下。

$$\begin{aligned} L_i &\leftarrow (L_{i-1} \ggg \alpha) \boxplus R_{i-1} \oplus K_i \\ R_i &\leftarrow (R_{i-1} \lll \beta) \boxplus L_i \end{aligned} \quad (5)$$

其中 K_i 表示轮密钥。当分组长度是 32 bit 时, $(\alpha, \beta) = (7, 2)$, 否则 $(\alpha, \beta) = (8, 3)$ 。SPECK 的轮函数如图 1 所示。

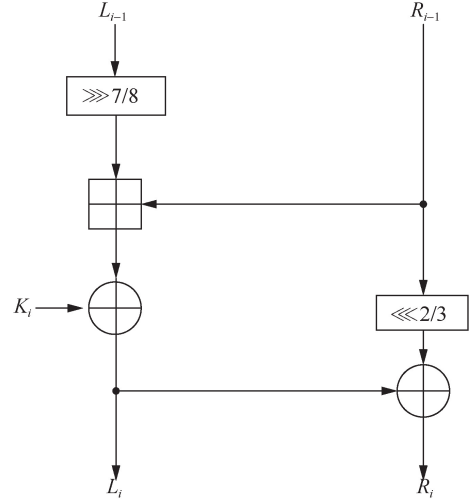


图 1 SPECK 轮函数

Figure 1 The round function of SPECK

1.4 HIGHT 简介

HIGHT 是一个 8 分支 (每个分支都是 8 bit 长) 的广义 Feistel 结构的迭代型分组密码算法, 迭代轮数为 32 轮^[29]。HIGHT 轮函数如图 2 所示, 其中 $(X_7^i \| X_6^i \| \dots \| X_0^i)$ 和 $(SK_{4i+3} \| SK_{4i+2} \| SK_{4i+1} \| SK_{4i})$ 分别表示第 i 轮的 64 bit 输入以及 32 bit 轮密钥。 SK_{4i+1} 和 SK_{4i+3} 以模加的方式注入, 另外两个轮密钥以异或的方式注入。 F_0 和 F_1 是两个 8 bit 输入、8 bit 输出的线性函数。

$$F_0(x) = (x \lll 1) \oplus (x \lll 2) \oplus (x \lll 7)$$

$$F_1(x) = (x \lll 3) \oplus (x \lll 4) \oplus (x \lll 6) \quad (6)$$

2 改进 Matsui 边界条件

在 1994 年的欧密会议上, Matsui 提出了一种分支定界的自动化方法来搜索分组密码的最优差分特征。令 P_{Opt}^i 表示分组密码的 i 轮最优差分特征

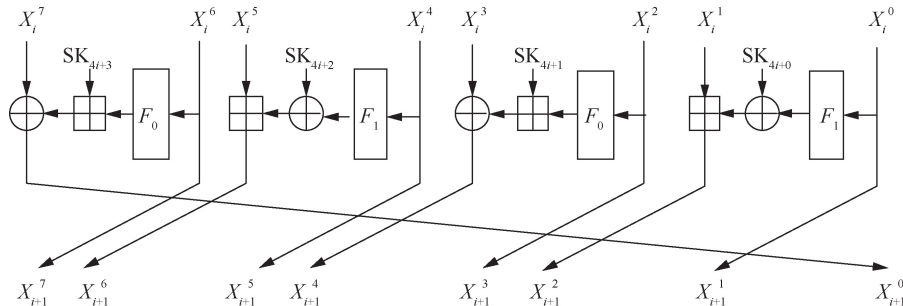


图 2 HIGHT 轮函数

Figure 2 The round function of HIGHT

概率，其中 $1 \leq i \leq R-1$ 。密码学家可以利用 Matsui 算法通过 P_{Opt}^i 派生出 R 轮最优差分特征概率，即 P_{Opt}^R 。令 w_{Opt}^i 表示 P_{Opt}^i 的以 2 为底数的对数的绝对值，其中 $1 \leq i \leq R-1$ 。假设 $w_{\text{Opt}}^R \leq k$ ，对于 $2 \leq r \leq R+1$ ，有

$$\sum_{i=1}^{r-1} w^i + w_{\text{Opt}}^{R-r+1} \leq k \quad (7)$$

其中， w^i 表示 P_i （即 R 轮最优差分特征中第 i 轮差分特征的概率）的以 2 为底数的对数的绝对值。下文将式(7)称为边界条件。

2.1 改进边界条件

在文献[24]中，Sun 等将 Matsui 边界条件转化为合取范式（CNF）的形式并将其加入 SAT 模型中来加速差分特征的搜索。对于 $1 \leq i \leq R-1$ ，假设最优差分特征概率 P_{Opt}^i 已知，则可以使用 Sun 等的方法搜索分组密码的 R 轮最优差分特征。搜索过程如算法 1 所示。

算法 1 Sun 等方法的搜索过程

输入 最优差分特征 P_{Opt}^i ，其中 $1 \leq i \leq R-1$

输出 P_{Opt}^R

1) flag $\leftarrow 1$;

2) for $i \in \{1, 2, \dots, R-1\}$ do

3) $w_{\text{Opt}}^i \leftarrow -\log_2 P_{\text{Opt}}^i$;

4) end for

5) 令 $k \leftarrow w_{\text{Opt}}^{R-1}$;

6) for $2 \leq r \leq R+1$ do

7) 令 $\sum_{i=1}^{r-1} w^i + w_{\text{Opt}}^{R-r+1} \leq k$;

8) end for

9) 将边界条件以及 L-M 条件转化为 CNF 形式;

10) while flag = 1 do

11) 调用 SAT 求解器 CaDiCaL 来确定是否存在 R 轮最优差分特征;

12) if 存在 R 轮最优差分特征 then

13) flag $\leftarrow 0$;

14) end if

15) if 不存在 R 轮最优差分特征 then

16) $k \leftarrow k+1$;

17) end if

18) end while

19) $P_{\text{Opt}}^R = 2^{-k}$;

20) return P_{Opt}^R

根据算法 1，每次调用 SAT 求解器时，如果没有有效的 R 轮差分特征，则 k 的值会增加 1。因此，对于 $w_{\text{Opt}}^R \leq k$ ，如果没有有效的 R 轮差分特征，仅需要在条件 $w_{\text{Opt}}^R = k+1$ 下搜索 R 轮差分特征而不需要在条件 $w_{\text{Opt}}^R \leq k+1$ 下搜索。

此外，由于 $w_{\text{Opt}}^{R-1} \leq w_{\text{Opt}}^R$ ，则当 SAT 求解器被首次调用时，仅需要在条件 $w_{\text{Opt}}^R = w_{\text{Opt}}^{R-1}$ 下搜索 R 轮差分特征而不需要在条件 $w_{\text{Opt}}^R \leq w_{\text{Opt}}^{R-1}$ 下搜索。

然而，如果使用 Sun 等的方法，每次调用 SAT 求解器时，都需要在条件 $w_{\text{Opt}}^R \leq k$ 下搜索 R 轮差分特征。

因此，对于 $2 \leq r \leq R$ ，可以利用如下公式进一步提高搜索效率。

$$\begin{cases} w_{\text{Opt}}^R = k \\ \sum_{i=1}^{r-1} w^i + w_{\text{Opt}}^{R-r+1} \leq k \end{cases} \quad (8)$$

其中， w^i 表示 P_i （即 R 轮最优差分特征中第 i 轮差分特征的概率）的以 2 为底数的对数的绝对值。下文将式(8)称为改进的边界条件。改进后的带改进的边界条件的搜索过程如算法 2 所示。

算法 2 改进后的带改进的边界条件的搜索过程

输入 最优差分特征 P_{Opt}^i ，其中 $1 \leq i \leq R-1$

输出 P_{Opt}^R

1) flag $\leftarrow 1$;

2) for $i \in \{1, 2, \dots, R-1\}$ do

3) $w_{\text{Opt}}^i \leftarrow -\log_2 P_{\text{Opt}}^i$;

4) end for

5) 令 $k \leftarrow w_{\text{Opt}}^{R-1}$;

6) 令 $w_{\text{Opt}}^R \leftarrow k$;

7) for $2 \leq r \leq R$ do

8) 令 $\sum_{i=1}^{r-1} w^i + w_{\text{Opt}}^{R-r+1} \leq k$;

9) end for

```

10) 将改进的边界条件以及 L-M 条件转化为
CNF 形式;
11) while flag = 1 do
12) 调用 SAT 求解器来确定是否存在  $R$  轮
最优差分特征;
13) if 存在  $R$  轮最优差分特征 then
14) flag  $\leftarrow$  0;
15) end if
16) if 不存在  $R$  轮最优差分特征 then
17)  $k \leftarrow k + 1$ ;
18) end if
19) end while
20)  $P_{\text{Opt}}^R = 2^{-k}$ ;
21) return  $P_{\text{Opt}}^R$ 

```

3 线程数和询问条件的加速效果

当密码分析者利用 SAT 方法搜索分组密码的最优差分特征时, 密码分析者需要将搜索差分特征的问题转化为布尔可满足性问题 (即 SAT 问题)。然而, SAT 问题仅包含布尔变量以及布尔操作 (AND、NOT 以及 OR), 因此上述转化过程十分复杂。相比之下, 可满足性模理论 (即 SMT) 问题支持比特向量变量以及常用的比特向量操作。此外, SMT 问题是 SAT 问题的推广且 SMT 公式可以用更丰富的逻辑表达。因此, 密码分析者通常将搜索差分特征的问题转化为 SMT 问题, 并使用 SMT 求解器进行求解, 过程如下。

- 1) 将搜索差分特征的问题转化为 SMT 问题。
- 2) 利用 SMT 求解器将 SMT 问题转化为 SAT 问题。
- 3) 利用 SMT 求解器调用 SAT 求解器求解 SAT 问题。

STP^[25]是一种典型的 SMT 求解器, 本文利用 STP 求解所有的 SMT 问题。

3.1 线程数的加速效果

STP 的默认 SAT 求解器是 MiniSAT^[30]。然而, STP 同样支持其他的 SAT 求解器, 如 CryptoMiniSat^[26]。由于 CryptoMiniSat 支持多线程且支持异或操作以及高斯消元, 密码学者经常利用 CryptoMiniSat 作为后端 SAT 求解器来求解 SAT 问题。因此, 使用多线程是否可以加速搜索成为一个

很自然的问题。

为了研究线程数的加速效果, 本文使用 STP 和 CryptoMiniSat 分别搜索 SPECK96 和 HIGHT 的差分特征。

3.2 询问条件的加速效果

为了将搜索差分特征的问题转化为 SMT 问题, 密码分析者经常使用 CVC 语言描述异或差分传播。当搜索差分特征时, 一个常用的搜索策略是询问在当前概率约束下是否存在有效的差分特征。上述策略所对应的询问条件为 QUERY (FALSE), COUNTEREXAMPLE。

上述询问条件被称为错误询问。当 STP 返回 Invalid 以及一条差分特征时, 代表在当前概率约束下至少有一条有效差分特征。

直观上看, 使用上述搜索策略是很耗时的, 尤其是在当前概率约束下没有有效差分特征时。因此, 替换询问条件是否可以加速搜索成为一个很自然的问题。

当使用算法 2 搜索差分特征时, 如果 STP 返回 Valid, 则代表无论输入差分为何值, 在当前概率约束下都没有有效的差分特征。因此, 对于一个分组长度为 n 比特的分组密码, 如果利用询问条件 QUERY($\Delta x = \alpha$)代替错误询问, 则在当前概率约束下没有有效差分特征时, STP 将返回 Invalid。其中, Δx 表示输入差分且 $\alpha = 1^n$, 即在限定输入差分等于全 1 向量的条件下进行差分特征的搜索, 将上述询问条件称为输入询问。为了研究线程数和询问条件的加速效果, 本文使用 STP 和 CryptoMiniSat 分别搜索 SPECK96 和 HIGHT 的差分特征。

3.3 线程数和询问条件加速效果的实验测试

3.3.1 追踪差分传播

(1) 追踪 SPECK96 中的差分传播

利用如下约束条件追踪 SPECK96 中的差分传播。

$$\begin{aligned}
 0 &= \text{eq}(\alpha_{i-1} \ll 1, \beta_{i-1} \ll 1, \gamma_{i-1} \ll 1) \wedge \\
 &(\alpha_{i-1} \oplus \beta_{i-1} \oplus \gamma_{i-1} \oplus (\beta_{i-1} \ll 1)) \\
 \Delta L_i &= \gamma_{i-1} \\
 \Delta R_i &= \Delta L_i \oplus (\Delta R_{i-1} \lll 3)
 \end{aligned} \tag{9}$$

其中, $(\alpha_{i-1}, \beta_{i-1}, \gamma_{i-1}) = (\Delta L_{i-1} \ggg 8, \Delta R_{i-1}, \Delta L_i)$ 且 $1 \leq i \leq R$ 。如果上述传播是有效的, 则第 i 轮的

概率为 $2^{-w_d^{j-1}}$ ，其中

$$w_d^{j-1} = wt(\overline{eq(\alpha_{i-1}, \beta_{i-1}, \gamma_{i-1})} \wedge \text{mask}(n-1)) \quad (10)$$

利用如下约束条件将 R 轮差分特征概率限制为 2^{-k} 。

$$\sum_{i=1}^R w_d^{j-1} = k \quad (11)$$

(2) 追踪 HIGHT 中的差分传播

利用如下约束条件追踪 HIGHT 中的差分传播。

$$\begin{aligned} 0 &= eq(\alpha_i^0 \lll 1, \beta_i^0 \lll 1, \gamma_i^0 \lll 1) \wedge \\ &\quad (\alpha_i^0 \oplus \beta_i^0 \oplus \gamma_i^0 \oplus (\beta_i^0 \lll 1)) \\ 0 &= eq(\alpha_i^1 \lll 1, 0^8 \lll 1, \gamma_i^1 \lll 1) \wedge \\ &\quad (\alpha_i^1 \oplus 0^8 \oplus \gamma_i^1 \oplus (0^8 \lll 1)) \\ 0 &= eq(\alpha_i^2 \lll 1, \beta_i^2 \lll 1, \gamma_i^2 \lll 1) \wedge \\ &\quad (\alpha_i^2 \oplus \beta_i^2 \oplus \gamma_i^2 \oplus (\beta_i^2 \lll 1)) \\ 0 &= eq(\alpha_i^3 \lll 1, 0^8 \lll 1, \gamma_i^3 \lll 1) \wedge \\ &\quad (\alpha_i^3 \oplus 0^8 \oplus \gamma_i^3 \oplus (0^8 \lll 1)) \end{aligned} \quad (12)$$

$$\begin{aligned} \Delta X_{i+1}^1 &= \Delta X_i^0 \\ \Delta X_{i+1}^2 &= \gamma_i^0 \\ \Delta X_{i+1}^3 &= \Delta X_i^2 \\ \Delta X_{i+1}^4 &= \Delta X_i^3 \oplus \gamma_i^1 \\ \Delta X_{i+1}^5 &= \Delta X_i^4 \\ \Delta X_{i+1}^6 &= \gamma_i^2 \\ \Delta X_{i+1}^7 &= \Delta X_i^6 \\ \Delta X_{i+1}^0 &= \Delta X_i^7 \oplus \gamma_i^3 \end{aligned}$$

其中，

$$\begin{aligned} (\alpha_i^0, \beta_i^0) &= \\ &((\Delta X_i^0 \lll 3) \oplus (\Delta X_i^0 \lll 4) \oplus (\Delta X_i^0 \lll 6), \Delta X_i^1) \\ \alpha_i^0 &= (\Delta X_i^2 \lll 1) \oplus (\Delta X_i^2 \lll 2) \oplus (\Delta X_i^2 \lll 7) \\ (\alpha_i^2, \beta_i^2) &= \\ &((\Delta X_i^4 \lll 3) \oplus (\Delta X_i^4 \lll 4) \oplus (\Delta X_i^4 \lll 6), \Delta X_i^5) \\ \alpha_i^3 &= (\Delta X_i^6 \lll 1) \oplus (\Delta X_i^6 \lll 2) \oplus (\Delta X_i^6 \lll 7) \end{aligned}$$

$$1 \leq i \leq R \quad (13)$$

如果上述传播是有效的，则第 i 轮的概率为 $2^{-w_d^i}$ ，其中

$$w_d^i = \sum_{j=0}^3 wt(\overline{eq(\alpha_i^j, \beta_i^j, \gamma_i^j)} \wedge \text{mask}(n-1)) \quad (14)$$

利用如下约束条件将 R 轮差分特征概率限制为 2^{-k} 。

$$\sum_{i=1}^R w_d^i = k \quad (15)$$

3.3.2 线程数和询问条件加速效果的实验测试

本节分别利用 1~30 个线程搜索 SPECK96 以及 HIGHT 的差分特征并记录耗时，从而实验测试线程数的加速效果。此外，分别利用错误询问以及输入询问搜索 SPECK96 以及 HIGHT 的差分特征并记录耗时，从而实验测试询问条件的加速效果。

3.3.2.1 搜索 SPECK96 的差分特征

令 $R=8$ 且 $k=24$ ，测试线程数以及询问条件的加速效果（以单线程+错误询问为基准）。

(1) 线程数的加速效果

① 当询问条件是错误询问时

时间消耗随着线程数增加的变化趋势是：先减少，再增多，最后减少并趋于平稳。两个转折点分别是 4 线程以及 11 线程。

② 当询问条件是输入询问时

时间消耗随着线程数增加的变化趋势是：先减少，再增多并趋于平稳，最后减少并趋于平稳。两个转折点分别是 5 线程以及 13 线程。

(2) 询问条件的加速效果

当线程数不为 5 或者 8 时，利用错误询问搜索差分特征的耗时与利用输入询问搜索差分特征的耗时之间没有明显的差距。实验结果如图 3 所示。

令 $R=8$ 且 $k=25$ ，测试线程数以及询问条件的加速效果（以单线程+错误询问为基准）。

(1) 线程数的加速效果

① 当询问条件是错误询问时

当线程数不超过 11 时，时间消耗随线程数增加没有明显变化的规律：时间消耗从减少到增多的转折点分别为 2、4、6 和 10 线程；时间消耗从增多到减少的转折点分别为 3、5 和 8 线程。当线

程数超过 11 且不超过 20 时, 时间消耗随着线程数的增加而减少。当线程数超过 20 且不超过 30 时 (除了 26), 时间消耗随着线程数的增加几乎不变。当线程数为 26 时, 时间消耗最少。

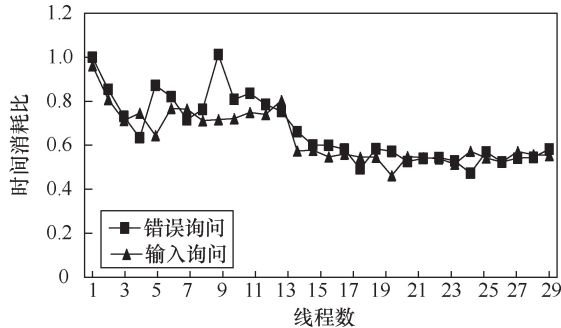


图 3 搜索 SPECK96 的概率为 2^{-24} 的 8 轮差分特征的时间消耗比
Figure 3 The time consumption ratio of searching for 8-round differential characteristics with a probability of 2^{-24} of SPECK96

② 当询问条件是输入询问时

当线程数不超过 13 时, 时间消耗随线程数增加没有明显变化的规律: 时间消耗从减少到增多的转折点分别为 2、6、9 和 12 线程; 时间消耗从增多到减少的转折点分别为 4、7 和 11 线程。当线程数超过 13 且不超过 19 时, 时间消耗随着线程数的增加先减少后增多, 且转折点为 18 线程。当线程数超过 19 且不超过 30 时, 时间消耗随着线程数的增加几乎不变。

(2) 询问条件的加速效果

尽管在大多数情况下, 利用错误询问搜索差分特征的耗时少于利用输入询问搜索差分特征的耗时, 然而, 耗时之间的差距并不十分明显。实验结果如图 4 所示。

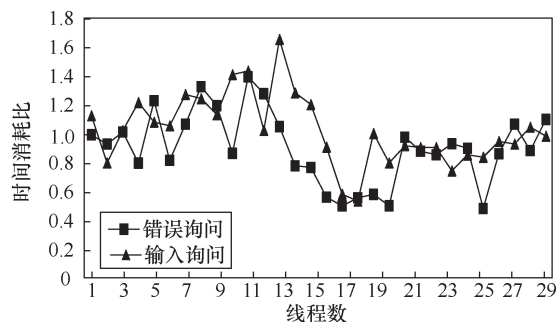


图 4 搜索 SPECK96 的概率为 2^{-25} 的 8 轮差分特征的时间消耗比
Figure 4 The time consumption ratio of searching for 8-round differential characteristics with a probability of 2^{-25} of SPECK96

令 $R=8$ 且 $k=26$, 测试线程数以及询问条件的加速效果 (以单线程+错误询问为基准)。

(1) 线程数的加速效果

① 当询问条件是错误询问时

时间消耗随着线程数增加的变化趋势分为 5 个阶段 (减少→增多→减少→增多→减少并趋于平稳)。4 个转折点分别是 2、7、10 以及 13 线程。

② 当询问条件是输入询问时

当线程数不超过 6 时, 时间消耗随线程数增加没有明显变化的规律: 时间消耗从减少到增多的转折点分别为 3 线程和 5 线程; 时间消耗从增多到减少的转折点为 4 线程。当线程数超过 6 时, 时间消耗随着线程数增加的变化趋势是: 先减少并趋于平稳, 后增多。转折点为 25 线程。

(2) 询问条件的加速效果

尽管在大多数情况下, 利用错误询问搜索差分特征的耗时少于利用输入询问搜索差分特征的耗时, 然而, 耗时之间的差距并不十分明显。实验结果如图 5 所示。

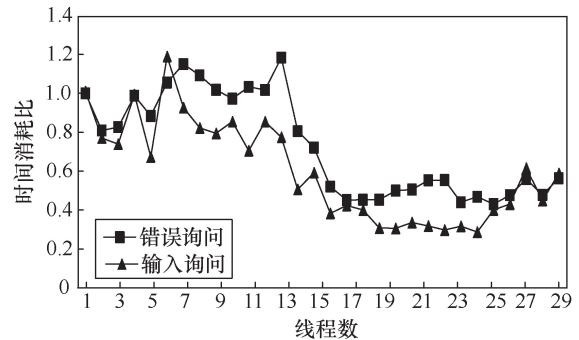


图 5 搜索 SPECK96 的概率为 2^{-26} 的 8 轮差分特征的时间消耗比
Figure 5 The time consumption ratio of searching for 8-round differential characteristics with a probability of 2^{-26} of SPECK96

3.3.2.2 搜索 HIGHT 的差分特征

令 $R=11$ 且 $k=39$, 测试线程数以及询问条件的加速效果 (以单线程+错误询问为基准)。

(1) 线程数的加速效果

① 当询问条件是错误询问时

时间消耗随着线程数增加的变化趋势是: 先减少并趋于平稳, 再增多, 最后减少并趋于平稳。两个转折点分别是 11 线程以及 12 线程。

② 当询问条件是输入询问时

时间消耗随着线程数增加的变化趋势分为 5 个阶段 (减少→增多→减少并趋于平稳→增多→减少并趋于平稳)。4 个转折点分别是 2、3、9 以及

11 线程。

(2) 询问条件的加速效果

当线程数不在集合 $\{1, 2, 5, 9\}$ 中时, 利用错误询问搜索差分特征的耗时少于利用输入询问搜索差分特征的耗时; 并且, 当线程数不为 3 时, 耗时之间的差距并不十分明显。实验结果如图 6 所示。

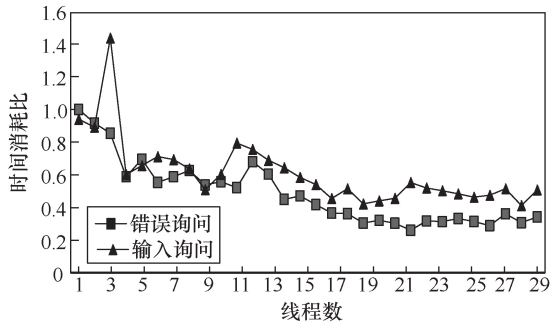


图6 搜索 HIGHT 的概率为 2^{-39} 的 11 轮差分特征的时间消耗比
Figure 6 The time consumption ratio of searching for 11-round differential characteristics with a probability of 2^{-39} of HIGHT

根据实验结果发现, 线程数对搜索差分特征的耗时影响较大, 而询问条件对搜索差分特征的耗时影响较小。对于相同的分组密码, 尽管时间消耗随着线程数增加变化的总体趋势是减少的, 但“使用较多线程数导致较高耗时”的情况并不罕见, 因此, 盲目地选择较多的线程数可能会导致更低的搜索效率。并且, 对于不同的分组密码, 线程数的加速效果是不同的。此外, 利用两个线程搜索差分特征的耗时基本低于利用单线程搜索差分特征的耗时。因此, 对于某个特定的分组密码, 如果密码分析者在搜索差分特征之前没有实验测试线程数的加速效果 (如同本文所做的实验), 利用两个线程搜索差分特征将是一个较好的选择。

对于上述 4 组实验, 有对应的 4 组 SMT 问题。需要注意的是, 每组 SMT 问题中的两个 SMT 问题仅询问条件不同。利用 STP 将这 8 个 SMT 问题转化为对应的 8 个 SAT 问题。然而, 每组 SAT 问题中的两个 SAT 问题是完全相同的。这就意味着, 仅改变询问条件将不会影响 CryptoMiniSat 的求解效率。因此, 利用错误询问搜索差分特征的耗时与利用输入询问搜索差分特征的耗时之间的差距是 STP 引起的。这意味着 STP 会影响搜索的整体效率。

在上述实验中, 时间消耗随着线程数的增加先减少后增加的情况多次出现。然而, 上述现象出现的线程数位置以及范围均无明显规律, 可能与以下两个原因有关: 线程增加导致线程调度时间开销增加; 第三方求解器的内部优化逻辑不够完善。此外, 线程数增加到一定数量时, 时间消耗趋于平缓而无法进一步降低, 可能与以下原因有关: 采用多线程进行搜索时, 多个线程要操作同一个数据集, 线程状态将频繁改变, 导致在线程数达到某个阈值时, 线程数的增加无法进一步提高程序的性能。

4 自动化搜索 HIGHT 的 11 轮最优差分特征

根据第 3 节的实验结果, 利用 27 个线程以及错误询问搜索 HIGHT 的差分特征耗时较短。因此, 本节利用 27 个线程以及错误询问搜索 HIGHT 的 11 轮最优差分特征。利用如算法 2 所示的搜索策略, 首次获得了 HIGHT 的 11 轮最优差分特征的紧致概率, 即 $P_{\text{Opt}}^{11} = 2^{-45}$ 。现有的 11 轮 HIGHT 最优差分特征概率的最紧致边界是 $P_{\text{Opt}}^{11} \geq 2^{-45}$ [6]。

在文献[6]中, Liu 等利用 Matsui 类算法搜索 11 轮 HIGHT 的最优差分特征。然而, 由于搜索算法的效率问题, Liu 等无法证明 11 轮 HIGHT 是否存在概率高于 2^{-45} 的差分特征。这就意味着 Liu 等的方法无法证明具有概率 $P_{\text{Opt}}^{11} = 2^{-45}$ 的 11 轮 HIGHT 差分特征是证明最优的。因此, 利用 Liu 等所提方法派生出的 11 轮 HIGHT 抗差分分析安全性的评估均无法被证明是精确的。利用本文提出的方法, 首次证明了 11 轮 HIGHT 最优差分特征的紧致概率 $P_{\text{Opt}}^{11} = 2^{-45}$, 即首次证明了本文给出的 11 轮 HIGHT 差分特征是证明最优的。这意味着, 首次给出了 11 轮 HIGHT 抗差分分析安全性的精确评估。因此, 本文的结果是目前已知的最优结果。利用本文方法找到的 HIGHT 的 11 轮最优差分特征如表 2 所示。

5 结束语

本文尝试利用 SAT 方法进一步加速差分特征的搜索, 通过改进边界条件从而降低搜索空间。密码分析者经常使用 STP 以及 CryptoMiniSat 搜索差分特征, 因此本文研究了线程数以及询问条

表 2 HIGHT 的 11 轮最优差分特征
Table 2 The 11-round optimal differential characteristic of HIGHT

r	ΔX_r^7	ΔX_r^6	ΔX_r^5	ΔX_r^4	ΔX_r^3	ΔX_r^2	ΔX_r^1	ΔX_r^0	w'_d
1	0x00	0x00	0x08	0xE5	0x28	0xE9	0x80	0x00	0
2	0x00	0x00	0xE5	0xA8	0xE9	0x80	0x00	0x00	1
3	0x00	0x00	0xA8	0x2C	0x80	0x00	0x00	0x00	8
4	0x00	0x00	0x2C	0x80	0x00	0x00	0x00	0x00	2
5	0x00	0x00	0x80	0x00	0x00	0x00	0x00	0x00	3
6	0x00	0x80	0x00	0x00	0x00	0x00	0x00	0x00	0
7	0x80	0x00	0x00	0x00	0x00	0x00	0x00	0xC3	3
8	0x00	0x00	0x00	0x00	0x00	0x72	0xC3	0x80	4
9	0x00	0x00	0x00	0x0C	0x72	0xE9	0x80	0x00	9
10	0x00	0xA3	0x0C	0xF2	0xE9	0x80	0x00	0x00	3
11	0xA3	0x00	0xF2	0x2A	0x80	0x00	0x00	0x08	7
12	0x00	0x79	0x2A	0x80	0x00	0xC2	0x08	0xA3	5

件的加速效果, 并实验测试了线程数以及询问条件的加速效果。根据实验结果发现, 线程数对搜索差分特征的耗时影响较大, 而询问条件对搜索差分特征的耗时影响较小。此外, 本文提出了一种选择线程数的策略, 利用该搜索策略, 首次获得了 HIGHT 的 11 轮最优差分特征的紧致概率, 且结果是已有最优的结果。希望本文提出的搜索策略不仅有助于评估分组密码抗差分分析的安全性, 而且有助于分组密码的设计。

参考文献:

- [1] BIHAM E, SHAMIR A. Differential cryptanalysis of DES-like cryptosystems[J]. Journal of Cryptology, 1991, 4(1): 3-72.
- [2] MATSUI M. On correlation between the order of S-boxes and the strength of DES[C]//Workshop on the Theory and Application of Cryptographic Techniques. 1994: 366-375.
- [3] BIRYUKOV A, ROY A, VELICHKOV V. Differential analysis of block ciphers SIMON and SPECK[C]//International Workshop on Fast Software Encryption. 2014: 546-570.
- [4] BIRYUKOV A, VELICHKOV V, LE C Y. Automatic search for the best trails in ARX: application to block cipher speck[C]//International Conference on Fast Software Encryption. 2016: 289-310.
- [5] LIU Z B, LI Y Q, WANG M S. Optimal differential trails in SIMON-like ciphers[J]. IACR Transactions on Symmetric Cryptology, 2017: 358-379.
- [6] 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.
- [7] MOUHA N, WANG Q J, GU D W, et al. Differential and linear cryptanalysis using mixed-integer linear programming[C]//International Conference on Information Security and Cryptology. 2011: 57-76.
- [8] FU K, WANG M Q, GUO Y H, et al. MILP-based automatic search algorithms for differential and linear trails for speck[C]//International Conference on Fast Software Encryption. 2016: 268-288.
- [9] XIANG Z J, ZHANG W T, BAO Z Z, et al. Applying MILP method to searching integral distinguishers based on division property for 6 lightweight block ciphers[C]//International Conference on the Theory and Application of Cryptology and Information Security. 2016: 648-678.
- [10] CUI T T, JIA K T, FU K, et al. New automatic search tool for impossible differentials and zero-correlation linear approximations[J]. Cryptology ePrint Archive, 2016.
- [11] SASAKI Y, TODO Y. New impossible differential search tool from design and cryptanalysis aspects[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2017: 185-215.
- [12] MOUHA N, PRENEEL B. Towards finding optimal differential characteristics for ARX: application to Salsa20[J]. IACR Cryptology ePrint Archive, 2013, (2013): 328.
- [13] KÖLBL S, LEANDER G, TIESSEN T. Observations on the SIMON block cipher family[C]//Annual Cryptology Conference. 2015: 161-185.
- [14] ANKELE R, KÖLBL S. Mind the gap—a closer look at the security of block ciphers against differential cryptanalysis[C]//International Conference on Selected Areas in Cryptography. 2018: 163-190.
- [15] ROH D Y, KOO B W, JUNG Y H, et al. Revised version of block cipher CHAM[C]//International Conference on Information Security and Cryptology. 2019: 1-19.
- [16] 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.
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.
- [17] LIU Y W, WANG Q J, RIJMEN V. Automatic search of linear trails

- in ARX with applications to SPECK and Chaskey[C]//International Conference on Applied Cryptography and Network Security. 2016: 485-499.
- [18] SUN L, WANG W, WANF M Q. Automatic search of bit-based division property for ARX ciphers and word-based division property[C]//International Conference on the Theory and Application of Cryptology and Information Security. 2017: 128-157.
- [19] SASAKI Y, TODO Y. New algorithm for modeling S-box in MILP based differential and division trail search[C]//International Conference for Information Technology and Communications. 2017: 150-165.
- [20] ZHANG Y J, SUN S W, CAI J H, et al. Speeding up MILP aided differential characteristic search with Matsui's strategy[C]//International Conference on Information Security. 2018: 101-115.
- [21] ZHOU C N, ZHANG W T, DING T Y, et al. Improving the MILP-based security evaluation algorithm against differential/linear cryptanalysis using a divide-and-conquer approach[J]. IACR Transactions on Symmetric Cryptology, 2019: 438-469.
- [22] BOURA C, COGGIA D. Efficient MILP modelings for Sboxes and linear layers of SPN ciphers[C]//IACR Transactions on Symmetric Cryptology. 2020: 327-361.
- [23] SONG L, HUANG Z J, YANG Q Q. Automatic differential analysis of ARX block ciphers with application to SPECK and LEA[C]//Australasian Conference on Information Security and Privacy. 2016: 379-394.
- [24] SUN L, WANG W, WANG M Q. Accelerating the search of differential and linear characteristics with the SAT method[C]//IACR Transactions on Symmetric Cryptology. 2021: 269-315.
- [25] GANESH V, DILL D L. A decision procedure for bit-vectors and arrays[C]//International Conference on Computer Aided Verification. 2007: 519-531.
- [26] SOOS M, NOHL K, CASTELLUCCIA C. Extending SAT solvers to cryptographic problems[C]//International Conference on Theory and Applications of Satisfiability Testing. 2009: 244-257.
- [27] LIPMAA H, MORIAI S. Efficient algorithms for computing differential properties of addition[C]//International Workshop on Fast Software Encryption. 2001: 336-350.
- [28] BEAULIEU R, SHORS D, SMITH J, et al. The SIMON and SPECK lightweight block ciphers[C]//Proceedings of the 52nd Annual Design Automation Conference. 2015: 1-6.
- [29] HONG D J, SUNG J C, HONG S H, et al. HIGHT: a new block cipher suitable for low-resource device[C]//International Workshop on Cryptographic Hardware and Embedded Systems. 2006: 46-59.
- [30] EÉN N, SÖRENNSSON N. An extensible SAT-solver[C]//International Conference on Theory and Applications of Satisfiability Testing. 2003: 502-518.

[作者简介]



许峥（1992—），男，河南郑州人，中国科学院信息工程研究所博士生，主要研究方向为分组密码的分析与设计。