密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research, 2020, 7(1): 1–3

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

AES 算法研究*

作者一[1], 作者二[1,2], 作者三[1,2]

1. xxx 大学 XXXX 实验室, 济南 250100
2. XXX 研究院, 北京 100190

通信作者: 作者一, E-mail: xxx@mail.xx.edu.cn

摘 要: 本刊要求来稿摘要内容详实, 字数不少于 400 字, 能全面表述稿件的主要观点和结论, 便于读者通过阅读摘要了解到作者的研究内容、方法和主要成果, 同时要求英文摘要对照准确.

关键词: AES 算法; 差分攻击

中图分类号: TP309.7 **文献标识码:** A DOI: 10.13868/j.cnki.jcr.000XXX

中文引用格式: 作者一, 作者二, 作者三. AES 算法研究[J]. 密码学报, 2020, 7(1): 1–3. [DOI: 10.13868/j.cnki.jcr.000XXX]

英文引用格式: ZUO Z Y, ZUO Z E, ZUO Z S. Research on AES[J]. Journal of Cryptologic Research, 2020, 7(1): 1–3. [DOI: 10.13868/j.cnki.jcr.000XXX]

Research on AES

ZUO Zhe-Yi[1], ZUO Zhe-Er[1,2], ZUO Zhe-San[1,2]

1. Academy of XXXX, Beijing 100190, China
2. Academy of XXXX, Beijing 100190, China

Corresponding author: ZUO Zhe-Yi, E-mail: xxx@mail.xx.edu.cn

Abstract: XXX.
Key words: AES; differential cryptanalysis

1 一级标题 1

正文部分 [1]. 文献 [1] 说了什么

2 一级标题 2

2.1 二级标题 1

2.1.1 三级标题 1

定理 1 定理内容.

证明: 证明过程. □

* 基金项目: 国家重点研发计划 (XXXX); 国家自然科学基金 (XXXX)
Foundation: National Key Research and Development Program of China (XXXX); National Natural Science Foundation of China (XXXX)
收稿日期: 2019-05-01 定稿日期: 2019-09-01

定义 1 定义内容.

引理 1 引理内容.

推论 1 推论内容.

命题 1 命题内容.

注 1 备注内容.

例 1 例子内容.

假设 1 假设条件.

算法 1 算法内容.

算法 1 AES 算法

```
Input: input parameters A, B, C
Output: output result
for condition do
    only if;
    if condition then
        1;
    end
end
```

$$\deg(g_{y_1}) \leq \min \{\mathrm{DEG}(y_{t-r_C-r_B-1}) + \mathrm{DEG}(z_{t-r_C}), \tag{1}$$

$$\mathrm{DEG}(y_{t-r_C-r_B+1}) + \mathrm{DEG}(z_{t-r_C-1}), \tag{2}$$

$$\mathrm{DEG}(y_{t-r_C-r_B-1}) + \mathrm{DEG}(y_{t-r_C-r_B}) + \mathrm{DEG}(y_{t-r_C-r_B+1})\} \tag{3}$$

$$\triangleq d1. \tag{4}$$

$$\tag{5}$$

3 一级标题 3

公式示例. 结论性公式没有必要全部编号, 后面要引用才需编号.

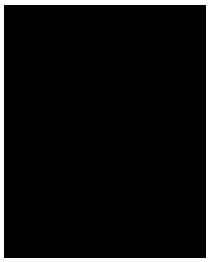
$$a^2 + b^2 = c^2 \tag{6}$$

参考文献

[1] DE CANNIÈRE C, DUNKELMAN O, KNEŽEVIĆ M. KATAN and KTANTAN—a family of small and efficient hardware-oriented block ciphers[C]. In: Cryptographic Hardware and Embedded Systems—CHES 2009. Springer Berlin Heidelberg, 2009: 272–288. [DOI: 10.1007/978-3-642-04138-9_20]

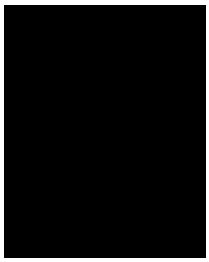
[2] LI Q, FENG D G, ZHANG L W, et al. Enhanced attribute-based authenticated key agreement protocol in the standard model[J]. Chinese Journal of Computers, 2013, 36(10): 2156–2167. [DOI: 10.3724/SP.J.1016.2013.02156]
李强, 冯登国, 张立武, 等. 标准模型下增强的基于属性的认证密钥协商协议 [J]. 计算机学报, 2013, 36(10): 2156–2167. [DOI: 10.3724/SP.J.1016.2013.02156]

作者信息



xxx (1993–), 山东济南人, 硕士生在读. 主要研究领域为应用密码学, 文档安全分析.
xiangxinguo@mail.ustc.edu.cn

作者二 (1982–), 山东济南人, 教授. 主要研究领域为对称, 密码算法的安全性分析.
zuozhe2@net.cn



作者三 (1989–), 北京人, 副研究员. 主要研究领域为对称, 密码算法的安全性分析.
zuozhe3@net.cn

附: 图、表模板

表 **1** 三线式表格
Table 1 Three lines table

列 1	**列 2**	**列 3**	**列 4**
行 1	XX	XX	XX
行 2	XX	XX	XX
行 3	XX	XX	XX
行 4	XX	XX	XX

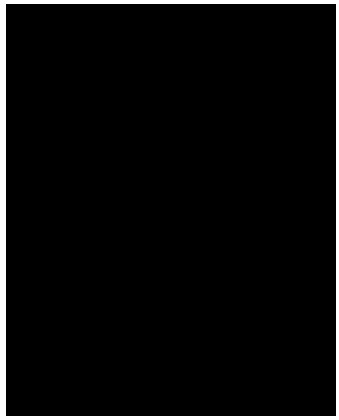


图 1 示例
Figure 1 Example