标题*

作者一[1], 作者二[1,2], 作者三[1,2]

1. XX 大学, 北京 100190
2. XXX 研究院, 北京 100190

通信作者: 作者一, E-mail: zuozhe1@net.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: 关键词 1; 关键词 2

Title

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

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

Corresponding author: ZUO Zhe-Yi, E-mail: zuozhe1@net.cn

Abstract: XXX.

Key words: keyword 1; keyword 2

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. □

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.

* 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: 2024-xx-xx　　定稿日期: 2024-xx-xx

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
```

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.

$$a^2 + b^2 = c^2 \tag{1}$$

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

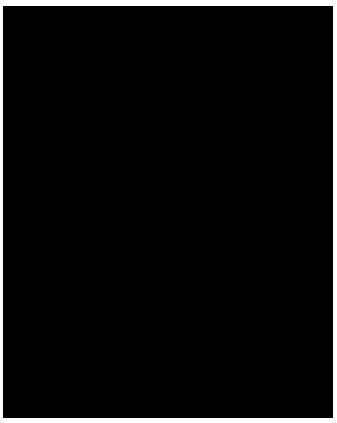

图 1 示例

Figure 1 Example

参考文献

[1] WANG X, YIN Y L, YU H. Finding collisions in the full SHA-1[C]. Advances in Cryptology–CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005. Proceedings 25. Springer Berlin Heidelberg, 2005: 17-36. [DOI: 10.1007/11535218_2]

[2] WANG X Y, LIU M J. Survey of Lattice-based Cryptography[J]. Journal of Cryptologic Research, 2014, 1(1): 13-27. [DOI: 10.13868/j.cnki.jcr.000002]
王小云, 刘明洁. 格密码学研究 [J]. 密码学报, 2014, 1(1): 13-27. [DOI: 10.13868/j.cnki.jcr.000002]