

# 认证加密模型 JAMBU 的新分析

田玉丹<sup>1</sup>, 韦永壮<sup>2</sup>

(1. 华东师范大学信息化办公室, 上海 200333;

2. 认知无线电与信息处理省部共建教育部重点实验室(桂林电子科技大学), 广西 桂林 541004)

**摘要:** 根据 JAMBU 模型的结构特点——相关数据和明文可以相互转化, 利用伪造攻击等基本思想提出了“随机数重复利用”的分析方法。结果表明, 该分析所需数据复杂度为  $2^{\frac{n}{2}}$ , 时间复杂度为  $4 \times 2^{\frac{n}{2}}$ 。与已有分析结果相比, 该分析数据复杂度更低。

**关键词:** JAMBU; 伪造攻击; CAESAR; 认证加密

**中图分类号:** TP309.7

**文献标识码:** A

**doi:** 10.11959/j.issn.2096-109x.2017.00177

## New cryptanalysis of the authenticated cipher model JAMBU

TIAN Yu-dan<sup>1</sup>, WEI Yong-zhuang<sup>2</sup>

(1. Information Technology Services Center, East China Normal University, Shanghai 200333, China;

2. Key Laboratory of Cognitive Radio and Information Processing Ministry of Education,  
(Guilin University of Electronic Technology), Guilin 541004, China)

**Abstract:** Based on the characteristic of JAMBU, a forgery attack by using the principle, where the associated data can be transformed into the plaintext was proposed. It is shown that the attack requires a data complexity of about  $2^{\frac{n}{2}}$  chosen plaintext, and a time complexity of about  $4 \times 2^{\frac{n}{2}}$  encryptions. Compared with the previous attack, this attack is more favorable.

**Key words:** JAMBU, forgery attack, CAESAR, authenticated encryption

### 1 引言

认证加密算法可以同时实现信息的加解密和完整性检验这 2 个功能, 已被广泛应用于各种网络安全系统中。2013 年, 世界范围内开启了对认证加密算法的征集活动——CAESAR<sup>[1,2]</sup>; 2014 年, 57 个认证加密算法入选一轮候选算法; 2015 年, 共 29 个认证加密算法入选二轮候选算法; 2016 年, 15 个认证加密算法入选三轮候选算法。Wu 等基于轻量级认证加密的思想, 利用 NIST 的

推荐模型 CFB, 设计出了 JAMBU 模型<sup>[3]</sup>。这一模型具有新颖的结构和设计理念, 并且顺利入选 CAESAR 第三轮候选算法。该模型具有广泛的适用性。例如, 将 SIMONU<sup>[4]</sup>和 AES-128<sup>[5]</sup>算法分别嵌入 JAMBU 模型, 可得到相应的认证加密算法 SIMON-JAMBU 和 AES-JAMBU。

2014 年, Thomas 等在文献[6]中对 JAMBU 的安全性进行分析: 输入 2 个不同的初始随机向量, 会产生不同的内部状态, 然后改变输入的明文值, 可求得内部状态的差分值, 从而达到预测

收稿日期: 2017-05-12; 修回日期: 2017-06-10。通信作者: 韦永壮, walker\_wei@msn.com

基金项目: 广西无线宽带通信与信号处理重点实验室主任基金资助项目 (No.GXKL061510)

**Foundation Item:** Guangxi Wireless Broadband Communication and Signal Processing Laboratory Director of Foundation (No.GXKL061510)

密文的效果。结果表明,该分析所需数据复杂度为  $2 \times 2^{\frac{n}{2}}$  个选择明文,时间复杂度为  $4 \times 2^{\frac{n}{2}}$  次加密模块访问。

2015年,Di在文献[7]中对AES-JAMBU的安全性进行分析,其主要的分析方法包括:穷密钥搜索攻击、暴力破译MAC攻击、密文组插入攻击、密文组删除攻击、密文修改攻击、选择明文攻击。分析结果显示,以上6种攻击方法攻击复杂度最低为  $2^n$ 。

本文根据JAMBU的“相关数据处理阶段和明文加密阶段具有类似的结构”这一特点提出“相关数据和明文相互转化”的新分析。研究表明,新分析通过改变相关数据和明文分组的个数,实现相关数据向明文转化的功能,从而预测密文的输出值。该分析所需数据复杂度为  $2^{\frac{n}{2}}$  个选择明文,时间复杂度为  $4 \times 2^{\frac{n}{2}}$  次加密模块访问。因此,新分析过程在保证时间复杂度未变的前提下,降低了数据复杂度。

## 2 JAMBU 算法介绍

JAMBU 是一个轻量级认证加密模型<sup>[3]</sup>。Wu等将JAMBU模型与SIMON算法结合,设计出了认证加密算法SIMON-JAMBU,将JAMBU模型与AES-128算法结合,设计出了认证加密算法AES-JAMBU。JAMBU模型的输入为  $k$  位密钥,  $n$  位公共随机数  $IV$ , 相关数据  $A$  和明文  $P$ , 生成与明文相同位长的密文  $C$  和  $n$  位标签  $T$ 。

JAMBU 模型的基本运算如下。

$\oplus$ : 按位异或运算。

$\parallel$ : 级联。

JAMBU 的基本符号与常量介绍如下。

$0^a$ :  $a$  位的 0。

$A$ : 相关数据。

$Alen$ : 相关数据的位长 ( $0 \leq Alen \leq 2^{64}$ )。

$IV$ : 初始向量。

$K$ : JAMBU 的密钥。

$E(k)$ : 加密算法, 密钥为  $K$  (如 SIMON 和 AES-128 算法)

$C$ : 密文。

$C_i$ : 第  $i$  个密文分组。

$P$ : 明文。

$P_i$ : 第  $i$  个明文分组。

$m_{len}$ : 明文或密文位长 (其中  $0 \leq m_{len} \leq 2^{64}$ )。

$m_i$ : 数据分组。

$n$ : 半个分组的位长。

$N$ : 相关数据分组和明文分组的总和。

$N_A$ : 相关数据分组个数。

$N_P$ : 明文分组的个数 (其中  $N = N_A + N_P$ )。

$R$ : 加密模型中的外部状态。

$S$ : 加密模型中的内部状态。

$T$ : 认证标签。

$t$ : 认证标签的位长。

JAMBU 模型的认证加密过程共有 5 个阶段: 数据填充、初始化、相关数据处理、明文加密、生成认证标签  $T$ , 如图 1 所示。

### 1) 数据填充阶段

若相关数据  $A$  的最后一个分组是未分组, 则在相关数据  $A$  最后级联  $10^*$ , 即将最后一个分组填充成为满分组。如果相关数据的长度为 0, 那么相关数据处理阶段输入为  $1 \parallel 0^{n-1}$ 。该填充原则同样适用于明文  $P$ 。

### 2) 初始化阶段

如图 1 所示, JAMBU 模型初始化阶段输入为  $n$  位公共初始随机向量  $IV$  和  $n$  位 0。设  $(X, Y)$  表示 2 个  $n$  位状态  $X$  和  $Y$  的组合。初始状态为  $S_{-1} = (0^n, IV)$ , 基本过程如下。

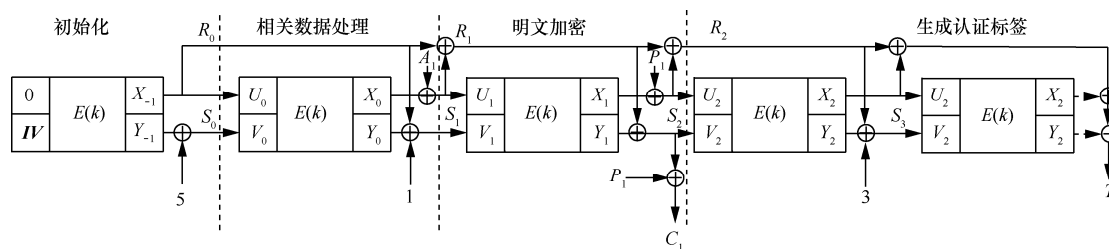


图1 JAMBU 单分组  $A$  和  $P$  的加密过程

$$(X_{-1}, Y_{-1}) = E_k(S_{-1})$$

$$R_0 = X_{-1}$$

$$S_0 = (X_{-1}, Y_{-1} \oplus 5)$$

### 3) 相关数据处理阶段

填充后的相关数据  $A$  划分  $n$  位分组，图 1 给出加密一个分组的相关数据处理过程，多个分组的加密过程如下。

$$(X_i, Y_i) = E(K, S_i)$$

$$U_{i+1} = X_i \oplus A_i$$

$$V_{i+1} = Y_i \oplus R_i \oplus 1$$

$$S_{i+1} = (U_{i+1}, V_{i+1})$$

$$R_{i+1} = R_i \oplus U_{i+1}$$

### 4) 明文加密阶段

将明文划分为  $n$  位分组，图 1 给出加密一个分组的明文加密过程，多个分组的明文加密过程如下（其中  $i$  表示第  $i$  个明文的加密过程）。

$$(X_i, Y_i) = E(K, S_i)$$

$$U_{i+1} = X_i \oplus A_i$$

$$V_{i+1} = Y_i \oplus R_i \oplus 1$$

$$S_{i+1} = (U_{i+1}, V_{i+1})$$

$$R_{i+1} = R_i \oplus U_{i+1}$$

$$R_{i-N_A} = P_{i-N_A} \oplus V_{i+1}$$

### 5) 生成认证标签 $T$ 阶段

认证标签生成阶段如图 1 所示，共有两轮状态更新过程，其过程如下。

$$(X_{N+1}, Y_{N+1}) = E(K, S_{N+1})$$

$$U_{N+2} = X_{N+1}$$

$$V_{N+2} = Y_{N+1} \oplus R_{N+1} \oplus 3$$

$$R_{N+2} = R_{N+1} \oplus X_{N+1}$$

$$S_{N+2} = (X_{N+2}, Y_{N+2})$$

JAMBU 模型的解密过程和加密过程类似，密文在解密之前先进行填充过程，如果密文长度是  $n$  的整数倍，那么在密文的最后添加一个  $n$  位的分组  $1 \parallel 0^{n-1}$ 。解密后生成的标签  $T'$  与加密过程

生成的认证标签  $T$  相比较，如果 2 个值相等，那么表示此次解密有效并返回明文，如果不相等，那么表示此次解密无效，返回值为 **null**。

**引理 1** 由认证加密模型 JAMBU 可知，如果初始向量  $IV$  相同，那么初始化阶段输出的内部状态相同；如果初始向量  $IV$  和相关数据  $A$  相同，那么相关数据处理阶段后的内部状态则完全相同。

## 3 认证加密模型 JAMBU 的分析过程

JAMBU 模型所有阶段所使用的基本加密模块  $E(k)$  完全相同，并且各个模块之间没有明显的界限，只是相差一个异或常数。相关数据处理阶段将  $Y_i$  与常数 1 和  $R_i$  进行异或更新状态  $S_i$ ，而明文加密阶段，更新后的状态  $Y_i$  与  $R_i$  异或之后作为输出的密钥与明文异或得到密文值<sup>[8,9]</sup>。因此，2 个阶段状态更新只差一个常数 1，本文将利用相关数据处理阶段和明文加密阶段的这一特点进行分析，其基本分析过程共分为如下 2 步。

**步骤 1** 如图 2 所示，随机选择一个相关数据  $A_1$ ，进行 2 种不同的加密模块访问（其中  $A_2 = A_1 \oplus \Delta A_1$ ），其输入输出参数如下。

$$(A_1, P_1) \Rightarrow C_1 \quad (1)$$

$$(A_2, P_1) \Rightarrow C_1' \quad (2)$$

其中，这 2 种不同的加密使用相同的初始向量  $IV$ ，即差分  $(\Delta X_0, \Delta Y_0)$  为  $(0, 0)$ ，相关数据处理之前 2 种加密的所有状态完全相同。其中  $\Delta A_1 = A_1 \oplus A_2$ ， $\Delta C_1 = C_1 \oplus C_1'$ ，即  $\Delta A_1$  为输入相关数据的差分， $\Delta C_1$  为输出密文的差分。如图 3 所示，通过尝试  $2^{\frac{n}{2}+1}$  个不同  $A$  的值，可以得到  $2^n$  个输入相关数据差分，同样可以得到  $2^n$  个输出密文差分。因此找到  $C_1' = C_1 \oplus \Delta C_1 = C_1 \oplus 1$  的概率为 1。设当  $\Delta A_1 = \Delta A_1'$  时， $\Delta C_1 = 1$ 。该步骤所需时间复杂度为  $2 \times 2^{\frac{n}{2}}$  次加密模块访问。

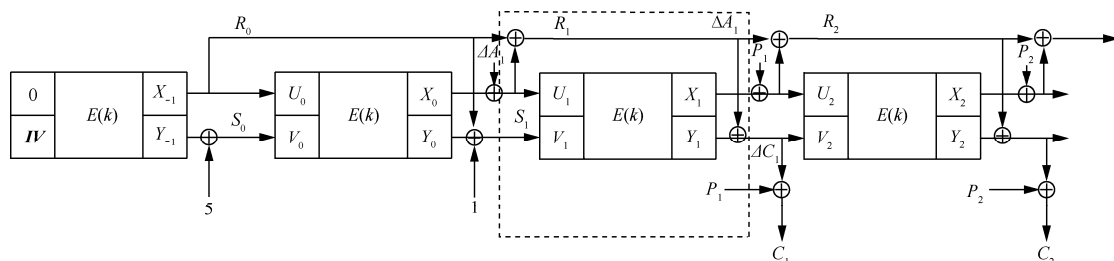


图 2 单分组相关数据  $A_1$  的差分传递

**步骤 2** 如图 3 所示, 随机选择一组数据  $A_1, P_1, P_2$ , 其中式(3)对应图 4(a), 式(4)对应图 4(b), 在相同的初始向量  $IV$  的情况下进行如下 2 种形式的加密。

$$(A_1, P_1, P_2) \Rightarrow (C_1, C_2) \quad (3)$$

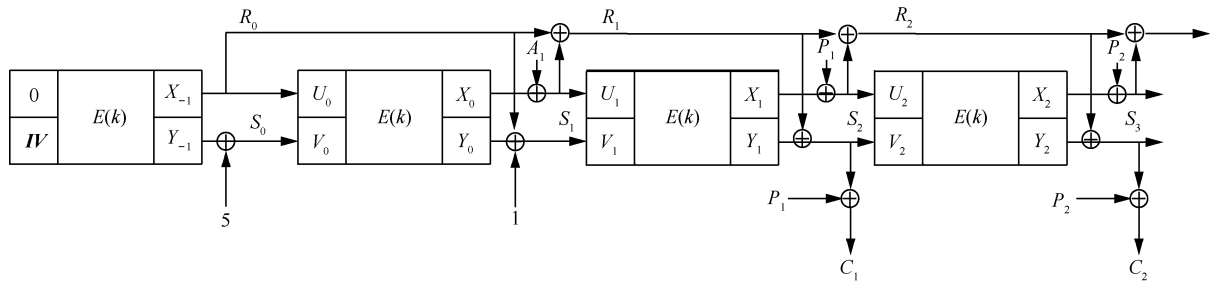
$$(A_1 \oplus \Delta A_1', A_2 = P_1', P_2) \Rightarrow C_1' \quad (4)$$

式(3)输入为 1 个相关数据分组和 2 个明文分组, 式(4)输入为 2 个相关数据分组和 1 个明文分组, 设  $\Delta = P_1 \oplus P_1'$ ,  $\Delta A_1'$  为步骤 1 所求得在  $S_1$  处所注入的相关数据差分值, 根据步骤 1 可知, 该差分

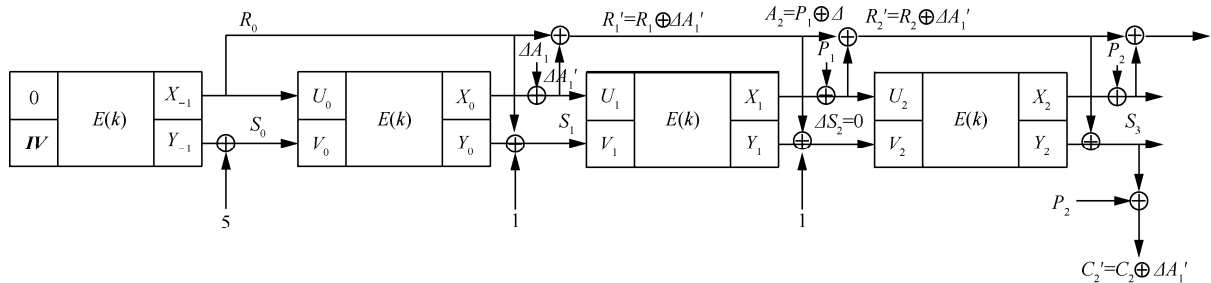
可以使两式加密过程中产生差分  $\Delta R_1 \oplus \Delta Y_1 = 1$ 。由图 4 可知, 图 4(b)在  $Y_1$  处多注入一个 1, 因此  $(\Delta R_1 \oplus \Delta Y_1) \oplus 1 = 0$ , 即  $\Delta V_2 = 0$ 。在第 3 个模块输入端注入差分  $\Delta = P_1 \oplus P_1'$ , 当  $\Delta = \Delta X_1$  时,  $\Delta U_2 = 0$ 、 $\Delta S_2 = 0$ 、 $R_2' = R_2 \oplus \Delta A_1'$ 、 $\Delta X_2 = 0$ 、 $\Delta Y_2 = 0$ 、 $C_1' = C_2 \oplus \Delta A_1'$ 。因此如果输出密文满足  $C_1' = C_2 \oplus \Delta A_1'$ , 则有可能  $\Delta = \Delta X_1$ 。通过  $2 \times 2^{\frac{n}{2}}$  次加密和  $2^{\frac{n}{2}}$  个明文数据即可求出  $\Delta = \Delta X_1$  可能的值 (证明过程与步骤 1 相似)。

| $A_1$                     |           |          | $A_2$                     |           |               | $\Delta A$      |
|---------------------------|-----------|----------|---------------------------|-----------|---------------|-----------------|
| 000...000                 | 000...000 | $\oplus$ | 000...000                 | 000...000 | $\rightarrow$ | ...             |
| 000...000                 | 000...001 |          | 000...001                 | 000...000 |               |                 |
| $\vdots$                  | $\vdots$  |          | $\vdots$                  | $\vdots$  |               |                 |
| 000...000                 | $i$       |          | $j$                       | 000...000 |               | $j \parallel i$ |
| $\vdots$                  | $\vdots$  |          | $\vdots$                  | $\vdots$  |               | ...             |
| 000...000                 | 111...110 |          | 111...110                 | 000...000 |               |                 |
| 000...000                 | 111...111 |          | 111...111                 | 000...000 |               |                 |
| $2^{\frac{n}{2}}$ 个输入相关数据 |           |          | $2^{\frac{n}{2}}$ 个输入相关数据 |           |               | 共 $2^n$ 个相关数据差分 |

图 3 尝试  $2^{\frac{n}{2}+1}$  个不同的  $A$  的值, 可以得到  $2^n$  个输入相关数据差分



(a) 1 个相关数据和 2 个明文的差分传递



(b) 2 个数据和 1 个明文的差分传递

图 4 相关数据  $A_1$  和明文  $P$  的差分状态传递

表 1

JAMBU 分析结果对比

| 攻击类型              | 数据复杂度                      | 时间复杂度                      | 相关文献  |
|-------------------|----------------------------|----------------------------|-------|
| 基于初始向量 $IV$ 的算法分析 | $2 \times 2^{\frac{n}{2}}$ | $4 \times 2^{\frac{n}{2}}$ | 文献[5] |
| 相关数据和明文相互转化的分析    | $2^{\frac{n}{2}}$          | $4 \times 2^{\frac{n}{2}}$ | 本文    |
| AES-JAMBU 的攻击     | $2^n$                      | $2^n$                      | 文献[7] |

## 4 结束语

表 1 将文献[5]和本文结果进行对比。由表可知, 文献[5]改变初始向量的值, 使初始化阶段状态产生差分, 然后注入明文差分, 抵消初始向量带来的差分, 最终内部状态发生碰撞, 所需数据复杂度为  $2 \times 2^{\frac{n}{2}}$  个选择明文, 时间复杂度为  $4 \times 2^{\frac{n}{2}}$  次加密模块访问; 文献[7]提出针对 AES-JAMBU 的分析方法, 分析结果显示数据复杂度和时间复杂度均为  $2^n$ ; 本文采用相同的初始向量值, 通过改变相关数据和明文的界限, 注入相关数据差分, 使内部状态产生差分, 再注入明文差分, 最终内部状态发生碰撞, 从而预测密文, 所需数据复杂度为  $2^{\frac{n}{2}}$  个选择明文, 时间复杂度为  $4 \times 2^{\frac{n}{2}}$  次加密模块访问。因此, 本文所需数据复杂度要小于文献[5]和文献[7], 时间复杂度与文献[5]的复杂度相同并小于文献[7]的复杂度。

## 参考文献:

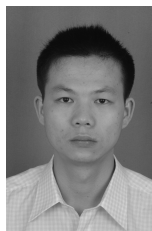
- [1] DANIEL J. CAESAR-competition for authenticated encryption: security, applicability, and robustness[OE/OL]. <http://competitions.cr.ypt.to/caesar.html>.
- [2] FUHR T, LEURENT G, SUDER V. Forgery and key-recovery attacks on caesar candidate marble[J]. *Cryptography & Security*, 2015.
- [3] WU H, HUANG T. JAMBU lightweight authenticated encryption mode and AES-JAMBU (v1)[C]// The CAESAR Competition.2014.
- [4] WU W, ZHANG L. LBlock: a lightweight block cipher[C]//Applied Cryptography and Network Security. 2011: 327-344.

- [5] DERBEZ P, FOUQU A, JEAN J. Improved key recovery attacks on reduced-round AES in the single-key setting[C]//The 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2013: 371-378.
- [6] PEYRIN T, SIM S M, WANG L, et al. Cryptanalysis of JAMBU[J]. *Early Symmetric Crypto ESC*, 2015: 77.
- [7] DI B B. Analysis of one-pass block cipher based authenticated encryption schemes[DB/OL]. [http://eprints.qut.edu.au/87437/1/Binbin\\_Di\\_Thesis.pdf](http://eprints.qut.edu.au/87437/1/Binbin_Di_Thesis.pdf).
- [8] KAVUN E B, YALCIN T. A lightweight implementation of Keccak Hash function for radio-frequency identification applications[M]//Radio Frequency Identification: Security and Privacy Issues. Berlin: Springer, 2010: 258-269.
- [9] 刘彦宾, 韦永壮. PMAC 模式的消息伪造攻击[J]. *计算机工程*, 2009, 35(22): 150-152.
- LIU Y B, WEI Y Z. Message forgery attack of PMAC scheme[J]. *Computer Engineering*, 2009, 35(22): 150-152.

## 作者简介:



田玉丹(1990-), 女, 山东菏泽人, 华东师范大学初级网络安全工程师, 主要研究方向为信息安全。



韦永壮(1976-), 男, 广西田阳人, 博士, 桂林电子科技大学教授, 主要研究方向为信息安全。