文章编号：2095-2163(2023)01-0072-05 中图分类号：TP393.4 文献标志码：A

认证加密算法 SUNDAE-GIFT 的故障分析

朱晓铭
(东华大学 计算机科学与技术学院，上海 201620)

摘 要：SUNDAE-GIFT 算法是以 GIFT-128 为底层分组密码的认证加密算法，入选了美国国家标准与技术研究院(NIST)举办的轻量级标准化项目的第二轮评选，能够保护数据传输时的机密性、完整性并认证数据源，可以广泛应用于物联网中射频识别标签、智能卡、传感器等资源受限的嵌入式设备。本文结合 SUNDAE-GIFT 密码的设计结构和实现特点，实现了 SUNDAE-GIFT 的故障分析，在加密过程中的底层分组密码 GIFT-128 中注入故障，并分析密文破译密码。这是首次针对 SUNDAE-GIFT 的统计故障分析，实验表明，SEI、HW 和 MLE 区分器分别需要 768、576 和 608 个故障即可在短时间内破译 SUNDAE-GIFT 的 128 比特主密钥。研究表明，故障分析对 SUNDAE-GIFT 密码构成了严重威胁，为其它的认证加密算法的安全性分析提供了重要参考。

关键词：SUNDAE-GIFT；物联网；故障分析

Fault analysis of the authenticated encryption algorithm SUNDAE-GIFT

ZHU Xiaoming
(School of Computer Science and Technology, Donghua University, Shanghai 201620, China)

【Abstract】 The SUNDAE-GIFT is an authenticated encryption algorithm with GIFT-128 as the underlying block cipher. It was selected in the second round of the lightweight project organized by the National Institute of Standards and Technology(NIST). It can protect the confidentiality, integrity and data source authentication of data transmission. It is widely used in resource-constrained embedded devices such as radio frequency identification tags, smart cards, and sensors in the Internet of Things(IoT). By Combining the design structure and implementation characteristics of SUNDAE-GIFT, this paper realizes the fault analysis of SUNDAE-GIFT. The attackers can inject faults into the underlying block cipher GIFT-128 in the encryption process, and analyze the ciphertexts to break the cipher. This is the first statistical fault analysis of SUNDAE-GIFT. As the experiment shows, SEI, HW and MLE distinguishers require 768, 576 and 608 faults, respectively, to recover the 128-bit master key of SUNDAE-GIFT. It shows that the fault analysis poses a serious threat to the SUNDAE-GIFT. The research provides an important reference for the security of other authenticated encryption algorithms.

【Key words】 SUNDAE-GIFT; Internet of Things; fault analysis

0 引 言

随着信息产业的快速发展，一些软硬件资源受限的设备，如射频识别标签和智能卡等，正在广泛应用于智能农业、智慧医疗、智慧建筑等生活领域，需要密码保护的范围也因此变得更加广阔[1]。但是早期的认证工作模式由于对资源有较高的要求，不再适用于资源受限的设备中。轻量级的认证加密算法在保证数据机密性、完整性和消息鉴别功能的基础上，又降低了对资源的需求，因此受到国内外学者的高度关注，不同模式的轻量级认证加密算法的设计与分析成为研究的重点[2]。

SUNDAE-GIFT 是由 Banik 等学者提出的基于 SUNDAE(Small Universal Deterministic Authenticated Encryption)模式，并采用 GIFT-128 为底层分组密码的轻量级认证加密算法，入选美国国家标准与技术研究院(NIST)启动的轻量级密码标准化项目的第二轮评选[3]。相较于 PRESENT，轻量级密码 GIFT 更加安全和高效，甚至优于轻量级密码 SKINNY 和 SIMON[4]。相较于传统的认证加密模式，SUNDAE-GIFT 具有低功耗，高效率等特点，适合 RFID 和智能卡网络等资源受限设备。

基金项目：国家自然科学基金(61772129,61932014)。

作者简介：朱晓铭(1998-)，男，硕士研究生，主要研究方向：轻量级密码的故障分析。

收稿日期：2022-03-31

1997 年，Boech 等学者首次利用故障分析破译 RSA 算法[5]。后来，通过结合传统密码分析和故障分析，逐渐衍生出差分故障攻击、不可能故障分析、代数故障分析和统计故障分析等分析方法，具备不同的分析优势[6]。目前，故障分析已经成为对密码进行安全性分析的重要方法。

自从 SUNDAE-GIFT 被提出以来，已经有学者利用故障分析研究其安全性。2021 年，Sun 等[7]对 SUNDAE-GIFT 进行了 17 轮的线性故障分析，成功破译了 128 比特的主密钥；同年，Liu 等[8]使用碰撞故障分析，仅以 128 个错误密文恢复密钥。

2013 年，Fuhr 等[6]首次提出了针对 AES 密码算法的统计故障分析；2016 年，Dobraunig 等[9]提出了针对基于随机数的认证加密算法模式的统计故障分析思想；2017 年，Li 等[10]首次针对轻量级分组算法 LED 统计故障分析；2018 年，Ramezanpour 等[11]首次通过统计故障分析对认证加密算法进行安全性分析。本文对 SUNDAE-GIFT 进行了统计故障分析，证明了分组密码工作模式类的认证加密算法存在设计上的安全问题，为轻量级认证加密算法的安全设计提供了重要思路。故障分析的结果对比见表 1，表明 SUNDAE-GIFT 在故障数方面更具优势。

表 1　统计故障分析破译部分子密钥的结果对比

Tab. 1　Comparison of statistical fault analysis on a partial subkey

区分器	AES		LED		Ascon		SUNDAE-GIFT	
	模型	故障数	模型	故障数	模型	故障数	模型	故障数
SEI	Byte	320	Nibble	70	Nibble	66	Nibble	48
HW	Byte	288	Nibble	39	-		Nibble	36
MLE	Byte	224	Nibble	40	-		Nibble	38

1　SUNDAE-GIFT 算法

1.1　符号说明

设 Z_2^e 为 e 比特的二进制向量集。

记 $M \in (Z_2^4)^{32}$ 为明文，$C \in (Z_2^4)^{32}$ 为密文，$A \in (Z_2^4)^{32}$ 为关联数据，$B \in (Z_2^4)^{32}$ 为初始数据块，$T \in (Z_2^4)^{32}$ 为标签，E_K 为底层加密函数；

记 $X \in (Z_2^4)^{32}$ 为 E_K 的输入，$Y \in (Z_2^4)^{32}$ 为 E_K 的输出，$K \in (Z_2^4)^{32}$ 为 128 比特主密钥，$k_j \in (Z_2^4)^4$ 是 K 的第 j 个字节，$RK_i \in (Z_2^4)^{16}$ 为第 i 轮子密钥，其中 $i \in [1,40]$，$j \in [0,7]$；

记 SC、SC^{-1} 为 S 盒和 S 盒的逆，PB、PB^{-1} 为 P 置换和 P 置换的逆，ARK 为子密钥加；

记 $S_{SC}^i \in (Z_2^4)^{16}$ 为第 i 轮 S 盒前的状态，其中 $i \in [1,40]$，记~为元素的实验值符号；Q_n 为中间状态的实际概率；n 为错误中间状态值；hw_n 为二进制字符串的汉明重量；V_n 表示中间状态实际个数；f 为故障数；P_n 为中间状态的理论概率。

1.2　SUNDAE-GIFT 密码

SUNDAE-GIFT 是以 GIFT-128 为底层密码的 SUNDAE 结构的认证加密算法。输入包括初始块 B、关联数据 A、明文 M 和密钥 K，输出包含标签 T 和密文 C，分组长度为 128 比特，算法结构如图 1 所示。

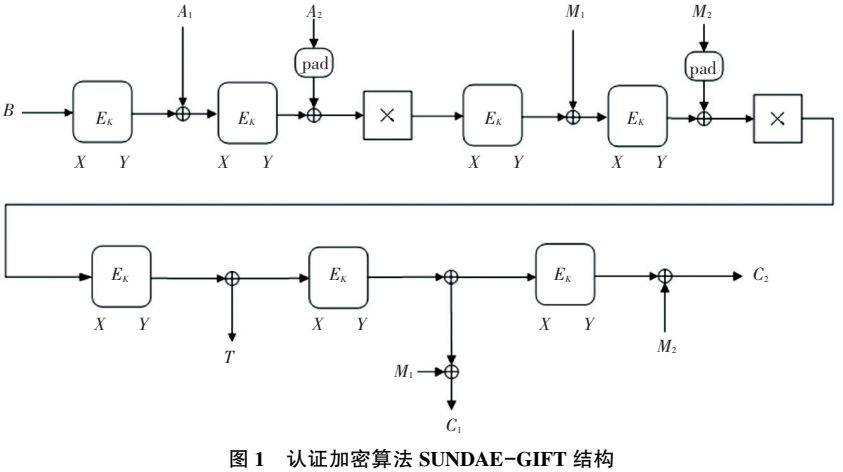

图 1　认证加密算法 SUNDAE-GIFT 结构

Fig. 1　The structure of authenticated encryption algorithm SUNDAE-GIFT

GIFT 是一种 SPN 结构的轻量级分组密码。GIFT-128 是其中的一个版本,其密钥长度为 128 位,分组长度为 128,轮数为 40 轮,每一轮的轮函数包括 S 盒、P 置换和轮密钥加,算法结构如图 2 所示。

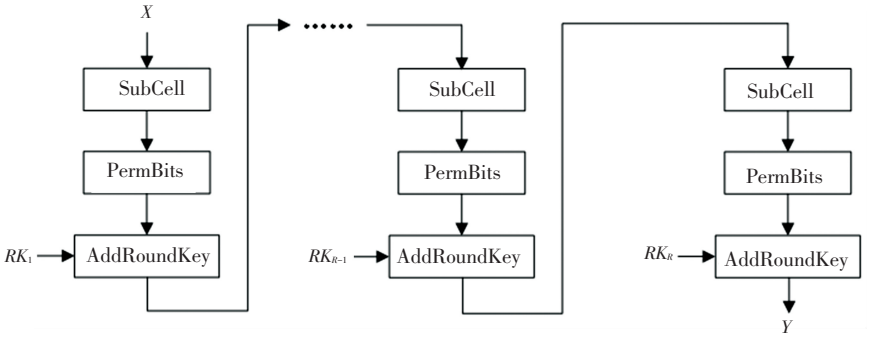

图 2 GIFT-128 算法结构

Fig. 2 The structure of GIFT-128

1.3 故障模型

本文采取的故障模型是半字节随机“与”故障模型,通过在加密过程中的某一轮注入半字节随机“与”故障,影响中间状态值的分布律产生偏移,而不注入故障的中间状态值的分布律呈现均匀分布。半字节中间状态在注入故障后理论分布律如图 3 所示。

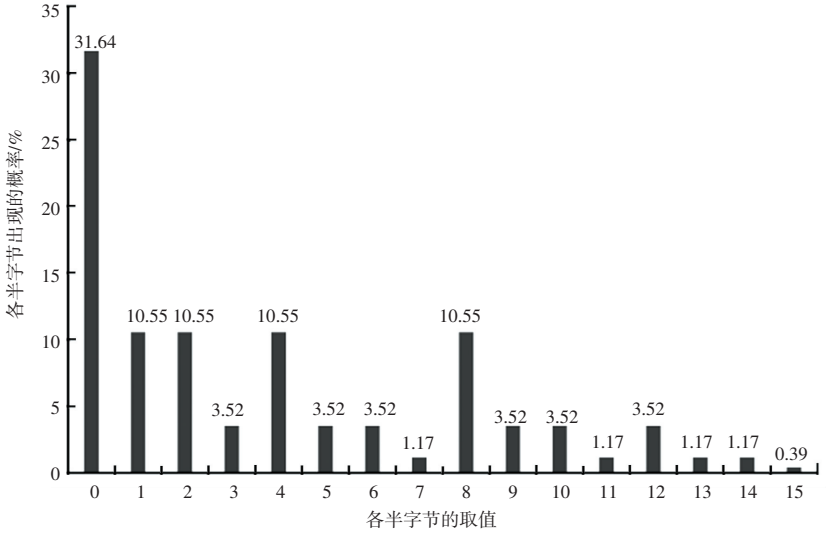

图 3 半字节的理论分布律

Fig. 3 The theoretical distribution of a nibble

1.4 攻击步骤

本文使用统计故障分析破译 SUNDAE-GIFT 算法的主密钥,主要包括以下步骤:

步骤 1 故障注入。攻击者在生成密文阶段通过在底层密码 GIFT-128 的第 39 轮注入随机“与”故障,使半字节中间状态值的分布律产生偏移,最后故障扩散并生成错误标签,故障扩散路径如图 4 所示。攻击者在故障扩散后收集错误密文样本,为后续的密钥破译提供数据基础。

步骤 2 计算中间状态值。攻击者依据公式(1)逆推错误标签样本集,穷举最后两轮子密钥中的 10 比特作为候选密钥值样本集,解密计算得出半字节错误中间状态样本集合为

$$S_{SC}^{40} = SC^{-1}(PB^{-1}(\tilde{T} \oplus RK_{40})) \quad (1)$$

步骤 3 区分器选取。攻击者按照步骤 1、2 操作,取得候选密钥和对应的半字节错误中间状态样本集,并通过区分器进行统计分析,筛选出实验分布律最接近理论分布律的半字节错误中间状态所对应的密钥候选值,即正确子密钥。

步骤 4 主密钥恢复。重复步骤 1~步骤 3,直至破译 RK_{39} 和 RK_{40} 的全部比特。再依据公式(2)和公式(3)中的密钥编排方案恢复主密钥。

$$RK_{39} = (k_1 \ggg 4) \| (k_0 \ggg 8) \| (k_5 \ggg 2) \| (k_4 \ggg 12) \quad (2)$$

$$RK_{40} = (k_3 \ggg 4) \| (k_2 \ggg 8) \| (k_7 \ggg 2) \| (k_6 \ggg 12) \quad (3)$$

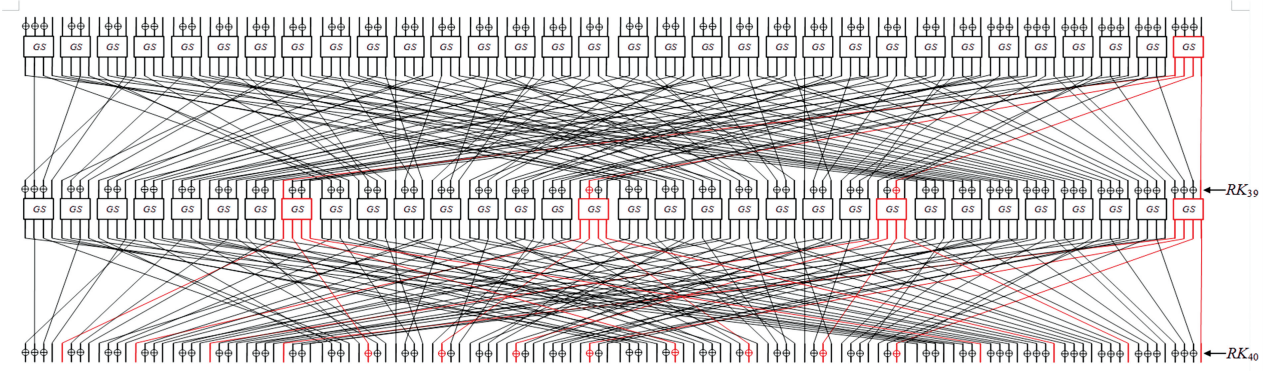

图 4　SUNDAE-GIFT 的故障扩散路径

Fig. 4　Fault diffusion path of SUNDAE-GIFT

1.5　区分器

区分器主要用于计算样本集的分布律，利用统计学的知识对样本集进行分析并筛选出正确密钥。本文采用 Fuhr 等[6]统计故障分析 AES 时使用的 SEI、HW 和 MLE 3 个区分器对 SUNDAE-GIFT 算法进行分析。3 个区分器对应的公式和选取的极值见表 2。

表 2　不同区分器的计算公式和所取极值

Tab. 2　The formulas and extreme values of different distinguishers

区分器	公式	极值
SEI	$\sum_{n=0}^{N}\left(Q_n-\frac{1}{16}\right)^2$	最大值
HW	$\frac{1}{f}\sum_{n=0}^{N} hw_n \cdot V_n$	最小值
MLE	$\prod_{n=0}^{N}(P_n)^{V_n}$	最大值

2　实验分析

本文实验利用计算机软件模拟随机故障导入，使用 Java 语言编程进行分析。本文基于成功率、故障数、耗时和复杂度等指标评测不同区分器和两种故障分析方法的效果。

2.1　成功率

成功率是指不同区分器破译密码的概率。各个区分器恢复 10 比特子密钥时，不同故障数对应的成功率如图 5 所示，3 个区分器均能够在故障数少于 50 时，成功率达到 100%。

2.2　故障数

故障数是指不同区分器以最大概率破译密码所需最少故障数。统计故障分析在恢复 SUNDAE-GIFT 密码主密钥时的故障数见表 3，SEI、HW 和 MLE 3 个区分器的故障数分别为 768、576 和 608。

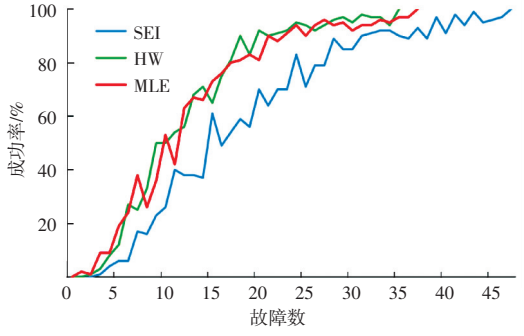

图 5　不同区分器恢复部分子密钥的成功率

Fig. 5　The probability of recovering a partial sub key with different distinguishers

表 3　不同区分器破译主密钥的故障数

Tab. 3　The faults of breaking the master key with different distinguishers

区分器	故障数	成功率
SEI	768	≥99%
HW	576	≥99%
MLE	608	≥99%

2.3　耗时

耗时是指破译 SUNDAE-GIFT 算法所需要的时间，包括故障导入、密钥猜测和统计分析等过程。采用各个区分器恢复子密钥时，不同故障数对应的时间如图 6 所示。其中，横轴与纵轴分别表示故障数和时间堆积。当成功率达到最高时，SEI、HW 和 MLE 的耗时分别为 7.98、5.80 和 6.13 s。

2.4　复杂度

复杂度是指破译 SUNDAE-GIFT 算法主密钥所需的时间复杂度和数据复杂度，用于衡量统计故障分析的效率和占用的资源。不同区分器在破译 SUNDAE-GIFT 时的时间复杂度和数据复杂度见表 4，均表现优秀，其中 F 表示故障数，S 表示密钥搜索

空间且 $S = 2^{10}$。

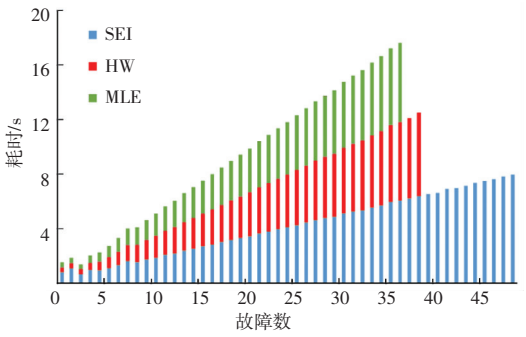

图 6 不同区分器恢复部分子密钥的耗时

Fig. 6 The time of recovering a partial subkey with different distinguishers

表 4 不同区分器破译主密钥的复杂度

Tab. 4 The complexity of breaking the master key with different distinguishers

区分器	时间		数据	
	公式	复杂度	公式	复杂度
SEI	$F*S*16$	$2^{23.58}$	$F*S$	$2^{19.58}$
HW	$F*S*17$	$2^{23.26}$	$F*S$	$2^{19.17}$
MLE	$F*S*17$	$2^{23.19}$	$F*S$	$2^{19.25}$

3 结束语

本文实现了针对 SUNDAE-GIFT 认证加密算法的统计故障分析,是首次针对分组密码工作模式类的认证加密算法的统计故障分析。实验结果表明,统计故障分析对 SUNDAE-GIFT 认证加密密码具有较大威胁性。在物联网中使用 SUNDAE-GIFT 时,应考虑对密码加以更多保护,该结果为轻量级认证加密算法抵御故障分析提供了有价值的参考。

参考文献

[1] 王莹. 物联网在智慧农业中的现状及发展趋势研究[J]. 技术与市场, 2022, 29(1): 111-113.

[2] 吴文玲, OTHERS. 认证加密算法研究进展[J]. 密码学报, 2018, 5(1): 70-82.

[3] BANIK S, BOGDANOV A, PEYRIN T, et al. SUNDAE-GIFT [J]. Submission to Round, 2019, 1(1): 157-161.

[4] BANIK S, PANDEY S K, PEYRIN T, et al. GIFT: A Small PRESENT [C]//International Conference on Cryptographic Hardware and Embedded Systems. Taipei: Springer, 2017: 321-345.

[5] BONEH D, DEMILLO R A, LIPTON R J. On the Importance of Checking Cryptographic Protocols for Faults [C]//International Conference on the Theory and Applications of Cryptographic Techniques. Konstanz: Springer, 1997: 37-51.

[6] FUHR T, JAULMES E, LOMNE V, et al. Fault Attacks on AES with Faulty Ciphertexts Only[C]//Workshop on Fault Diagnosis and Tolerance in Cryptography. Washington DC: IEEE, 2013: 108-118.

[7] SUN L, WANG W, WANG M. Linear Cryptanalyses of Three AEADs with GIFT-128 as Underlying Primitives [J]. IACR Transactions on Symmetric Cryptology, 2021: 199-221.

[8] LIU S, GUAN J, HU B. Fault Attacks on Authenticated Encryption Modes for GIFT[J]. IET Information Security, 2022, 16(1):51-63.

[9] DOBRAUNIG C, EICHLSEDER M, KORAK T, et al. Statistical Fault Attacks on Nonce-Based Authenticated Encryption Schemes [M]. CHEON J H, TAKAGI T, eds.//Advances in Cryptology-ASIACRYPT 2016. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016: 369-395.

[10] LI W, LIAO L, GU D, et al. Ciphertext-Only Fault Analysis on the LED Lightweight Cryptosystem in the Internet of Things[J]. IEEE Transactions on Dependable and Secure Computing, 2019, 16(3): 454-461.

[11] RAMEZANPOUR K, AMPADU P, DIEHL W. A Statistical Fault Analysis Methodology for the Ascon Authenticated Cipher[C]// IEEE International Workshop on Hardware-Oriented Security and Trust. Tysons: IEEE, 2019:41-50.

(上接第 71 页)

[4] CAO X, WANG Z, ZHAO Y, et al. Scale aggregation network for accurate and efficient crowd counting[C]//Proceedings of the European Conference on Computer Vision (ECCV). 2018: 734-750.

[5] LIU N, LONG Y, ZOU C, et al. Adcrowdnet: An attention-injective deformable convolutional network for crowd understanding[C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2019: 3225-3234.

[6] LIU W, SALZMANN M, FUA P. Context-aware crowd counting [C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2019: 5099-5108.

[7] ZHU L, ZHAO Z, LU C, et al. Dual path multi-scale fusion networks with attention for crowd counting [J]. arXiv preprint arXiv:1902.01115, 2019.