遗传算法能量分析中初始化与变异机制研究

许一骏[1], 李 圆[2], 唐明环[3], 丁瑶玲[4], 王 安[4]

[1]国家工业信息安全发展研究中心 软件所 北京 中国 100040
[2]北京理工大学 计算机学院 北京 中国 100081
[3]中国工业互联网研究院 安全研究所 北京 中国 100102
[4]北京理工大学 网络空间安全学院 北京 中国 100081

摘要 人工智能与侧信道密码分析相结合, 给密码分析学带来了新的研究方向。近十年来, 遗传算法被引入侧信道分析, 国际上出现了一系列相关研究成果。然而, 现有基于遗传算法的相关能量分析存在局部最优问题, 使整个分析过程的效率偏低。本文旨在建立局部最优与成功率之间的关系, 选取科学的初始化与变异机制, 以显著提升使用人工智能算法开展侧信道分析的效率。我们首先探究了遗传算法能量分析成功、以及陷入局部最优的本质原因, 随后从初始化机制、变异机制两个角度尝试克服局部最优问题, 引入随机初始化、相关能量分析初始化、随机字节变异、基于密钥适应度排名的启发式变异等四种机制进行组合对比。通过参数选取、成功率对比、计算代价对比等多次实验得到结论: 相关能量分析初始化结合随机字节变异的方法具有最高的成功率, 同时计算代价也最小。

与此同时, 本文总结了遗传算法相关能量分析方法不适用于软件实现、难以分析大位宽运算、攻击防护对策时复杂度高、信噪比低时复杂度高等局限性问题, 建议密码硬件计算过程中尽量不要将以字节或比特为单位计算的值存入寄存器, 以防护遗传算法类能量分析攻击, 并对未来工作进行了展望。我们认为, 新方法在分析无防护硬件实现的分组密码算法时具有较高的实用性, 建议应用于实际的侧信道分析测评工作。

关键词 密码学; 能量分析攻击; 遗传算法; 变异机制; 初始化机制
中图法分类号 TP391 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2024.03.05

Initialization and Mutation Mechanism in Genetic-Algorithm-Based Power Analysis

XU Yijun[1], LI Yuan[2], TANG Minghuan[3], DING Yaoling[4], WANG An[4]

[1] Institute for Software, The China Industrial Control Systems Cyber Emergency Response Team (CIC), Beijing 100040, China
[2] School of Computer Science and Technology, Beijing Institute of Technology, Beijing 100081, China
[3] Security Research Institute, China Academy of Industrial Internet (CAII), Beijing 100102, China
[4] School of Cyberspace Science and Technology, Beijing Institute of Technology, Beijing 100081, China

Abstract The combination of artificial intelligence and side-channel analysis brought new research direction to cryptanalysis. In recent ten years, genetic algorithm has been introduced into side channel analysis, and a series of related research results have emerged in the world. However, the existing power analysis based on genetic algorithm had the problem of local optimization and low efficiency. This paper aimed to make a connection between local optimization and success rate, choose better initialization and mutation mechanism, and increase the efficiency of artificial-intelligence-based side-channel analysis. In this paper, we first analyzed the success reason of genetic-algorithm-based power analysis, and then discussed why the existing power analysis method of genetic algorithm fell into the local optimum. Accordingly, we introduced correlation-power-analysis-based initialization, heuristic mutation mechanism, random byte mutation, and random initialization, and then combined and compared them. Through some experiments, such as parameter selection, success rate comparison and calculation cost comparison, it is concluded that the method of correlation-power-analysis-based initialization combined with random byte mutation has the highest success rate and the lowest calculation cost.

At the same time, this paper summarizes the limitations of genetic algorithm-based correlation power analysis method: not suitable for software implementation, difficult to analyze large bit-width operation, high complexity in attack protection countermeasures, high complexity in low signal-to-noise ratio. It is suggested that the value calculated in bytes or bits should not be stored in the register directly during the hardware calculation of cryptographic algorithm, so as to protect against the power analysis attack based on genetic algorithm. At last, the future work is prospected, and we think that the new method has high practicability in analyzing the block cipher algorithm implemented by non-protected hardware, and it

通讯作者: 王安, 理学博士, 研究员, 博士生导师, Email: wanganl@bit.edu.cn。
本文受到国家重点研发计划项目(No. 2022YFB3103800)、国家自然科学基金项目(No. 62302036, No. 62272047)的资助。
收稿日期: 2022-06-05; 修改日期: 2022-08-16; 定稿日期: 2023-11-02

is recommended to be applied to the actual side channel analysis and evaluation.

Key words cryptography; power analysis attack; genetic algorithm; mutation mechanism; initialization mechanism

1 引言

2020 年 1 月 1 日, 《中华人民共和国密码法》[1]正式施行, 其条文中明确提出, 国家鼓励商用密码技术的研究与应用, 制定商用密码检测认证技术规范、规则, 鼓励商用密码从业单位自愿接受商用密码检测认证。然而, 密码技术的使用并不意味着信息的绝对安全, 密码算法本身、密码设备的接口、以及密码运行过程均面临着多种安全威胁。密码分析也称为密码攻击, 是密码技术发展的重要组成部分, 其主要研究如何破译密文或密钥。为了设计出好的密码算法, 需要对其进行深度的密码分析, 发现其算法或实现上存在的薄弱环节, 从而不断完善算法的设计。一直以来密码分析技术的发展极大的推动了密码算法的迭代升级, 促进着以密码算法为核心的相关密码产品的不断完善和创新, 推动了商用密码产业的发展。同时, 针对密码实现的各类分析技术的发展也有力的提升了密码芯片及相关产品检测方面的能力, 为建立健全权威有效的密码检测认证体系奠定了重要的技术基础。

1996 年, Kocher 提出了侧信道密码分析的概念[2], 这是一种根据密码芯片或设备运行过程中泄露的物理信息来恢复密钥的分析方法, 这些物理信息包括能量、电磁、声音、时间等等。由于现实中的 0 和 1 释放的物理信息必然存在差异, 攻击者可以通过这些物理泄露来获得密码实现的敏感信息。其中, 能量分析是实际中最有效的侧信道分析方法之一[3]。

由于噪声的存在, 通过直接对能量波形进行观测的方法一般无法直接恢复密钥。因而实际中攻击者或测评者往往需要采集较多能量波形, 通过统计方法对能量波形中蕴含的信息进行有效提取。在低信噪比条件下, 这种统计方法通常需要用较多波形、进行高复杂度的计算才能完成。2011 年, Hospodar 等人将人工智能中的机器学习技术引入侧信道分析, 使能量分析的能力和效果得到了显著提高[4]。此后, 人们主要聚焦于用卷积神经网络[5]、深度学习[6]等人工智能技术来克服一些防护对策对分析过程带来的影响。这种基于人工智能的侧信道分析的一般流程如图 1 所示。

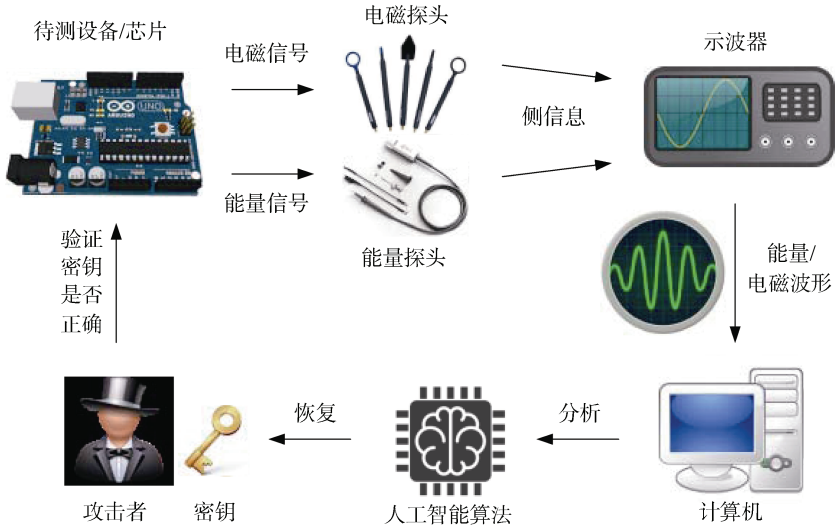

图 1 基于人工智能做侧信道密码分析的一般场景

Figure 1 Common scenarios of artificial-intelligence-based side-channel analysis on cryptographic implementations

2015 年, Zhang 等人[7]提出了一种基于遗传算法的能量分析, 一定程度上解决了并行实现的密码算法在能量分析时噪声显著的问题。2020 年, Ding 等人[8]改进了这一方法, 并将其应用于 AES 算法的 AddRoundKey 运算上。然而, 基于遗传算法的能量分析容易出现收敛慢的现象, 即遗传算法的共性问题——“局部最优”, 从而导致分析效率过低。2019 年, Picek[9]在其人工智能侧信道分析的综述论文中指出, 效率提升是人工智能侧信道分析的首要问题之一。2021 年, Wang 等人[10]尝试用一种高效的遗传算法能量分析框架来克服局部最优问题, 该框架中给出了相关能量分析初始化机制、基于适应度排名

的启发式变异机制。同年, Ding 等人采用多种群遗传算法的思想来做能量分析, 并提出了随机字节变异的概念。然而, Wang 和 Ding 等人的论文中没有对上述多种机制进行公平、细致的对比, 也并没有对局部最优的形成原因进行剖析。

本文分析了现有遗传算法能量分析过程中陷入局部最优的本质原因, 发现种群规模小、变异率低、噪声大、以及启发式变异机制的极值选取策略都可能导致缓慢收敛或局部最优。进而, 针对随机字节变异、启发式变异、随机初始化、相关能量分析初始化四种方法进行了有机组合和效率评估。同时我们发现, 虽然增加种群规模可以提高收敛速度, 但计算复杂度也会随之急剧增长, 进而针对种群规模参数的选取进行了实验, 给出了种群规模的最佳取值。实验表明, 相关能量分析初始化结合随机字节变异的方法在成功率、计算代价方面表现最优, 推荐应用于实际测评。

论文整体结构安排如下: 第二节介绍遗传算法、基于遗传算法的相关能量分析、以及它的改进方法; 第三节归纳了遗传算法能量分析成功和失败的原因, 提出随之待研究的问题, 并研究了启发式变异机制的缺点; 第四节给出了不同变异机制中种群规模参数的选取方法; 第五节采用仿真实验对比了各种变异机制与初始化机制进行组合得到的四种分析方法的成功率及计算代价; 第六节总结了全文, 并展望了未来可以研究的问题。

2 预备知识

2.1 AES 算法与侧信息泄露

本文以 128 位 AES 算法的加密过程为例进行讨论, 该算法的明文、密文、密钥均为 128 比特, 即 16 字节。加密开始时, 16 字节已知明文 p_i 和 16 字节的未知密钥 k_i 进行异或操作, 随后以字节为单位进入 16 个 S-box 运算, 得到 16 个字节 S-box 输出值 y_1 到 y_{16}。后续的运算与本文讨论内容无关, 暂略。

我们假设首轮 S-box 输出值 y_i 存在能量信息泄露如图 2 所示, 即 y_i 的汉明重量 HW(y_i)与能量波形的某个位置具有显著的相关性, 那么攻击者必然可以通过能量波形获得 y_i 的部分信息, 随后结合特定算法、配合已知的明文, 推导出密钥的信息, 这种方法被称为相关能量分析(Correlation Power Analysis, CPA)[11]。

2.2 遗传算法原理

遗传算法是一类解决最优问题的启发式算法, 模拟了自然进化过程, 将问题的最优解看作是进化过程中的最优个体身上携带的基因。遗传算法的流程一般是:

(1) 首先随机生成若干个个体作为初始种群, 并定义为当前代种群。

(2) 为当前代种群中每个个体计算一个适应环境生存的能力——适应度, 并根据个体适应度的值来执行选择算子, 确定该个体是否能够繁殖下一代。

(3) 执行繁殖操作, 即采用交叉算子和变异算子对当前代有繁殖能力的 2 个个体的基因进行组合(模仿生物学的基因重组)和变化(模仿生物学的基因突变), 得到几个子代个体。

(4) 在当前代种群中, 将多对个体执行步骤(3), 得到一定数量的子代个体构成子代种群。随后, 将当前代种群丢弃, 将子代种群定义为当前代种群。

(5) 不断重复步骤(2)～(4)的进化过程, 最后根据某种条件结束繁殖。当结束繁殖时, 末代种群中的最优个体可定义为原问题的近似最优解。

这一过程中, 种群基因能够不断进步、逼近最优解的主要原因是, 适应度高的个体会以更高的几率繁殖下一代, 因而随着时间推移, 各代的适应度将不断提高, 从而产生或逼近最优解。

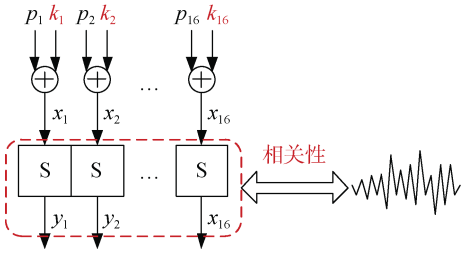

图 2 AES 算法第一轮侧信息泄露假设

Figure 2 Assumption of information leakage in 1st round of AES

2.3 基于遗传算法的 CPA

2015 年, Zhang 等人[7]将遗传算法引入 CPA, 其解决的关键问题是: 在 AES 算法硬件实现、16 个 S-box 并行计算的场景下, 研究一个 S-box 的泄露时, 其余 15 个 S-box 的功耗将被看做噪声; 如果同时研究多个 S-box, 则会指数级增加密钥搜索空间。用遗传算法替代穷搜, 可以完美地解决这个问题, 因而遗传算法 CPA 特别适用于分组密码算法的硬件实现。

Zhang 等人将个体定义为完整的 128 比特密钥的一个猜测, 将个体的适应度定义为该密钥在加密过程中对应的 HW(y_i)与能量波形之间的相关系数, 将选择算子定义为以一定概率(概率大小由适应度大小决定)选出某个个体来繁殖下一代, 将交叉算子定义

为将两个 128 比特密钥的若干比特直接交换, 将变异算子定义为密钥的每一比特均按照一个较小的概率直接翻转。

在上述定义下, 能量分析可自然融合到遗传算法的过程中, 其具体流程如下(如图 3 所示):

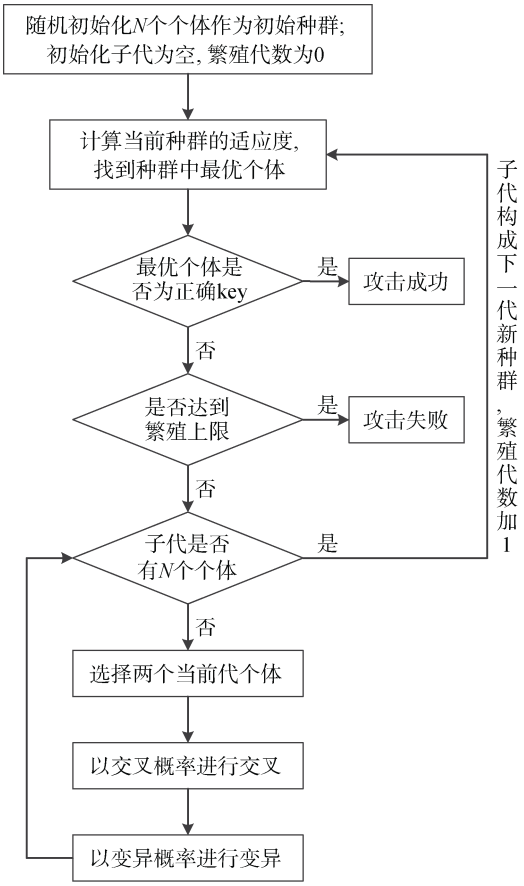

图 3　经典遗传算法能量分析流程

Figure 3　Power analysis flow based on classical genetic algorithm

(1) 初始化阶段, 按照定义 1 随机设定当前代种群, 并令初始化子代为空, 繁殖代数为 0。

定义 1．随机初始化． 随机生成 N 个 128 比特密钥, 作为 N 个个体, 构成进化过程中的初始种群。

(2) 计算当前代种群内所有密钥的适应度(前述的相关系数), 选出其中适应度最高的密钥, 判断是否为正确密钥。如果是, 则密钥恢复成功, 结束程序。如果不是, 判断当前代是否已经达到种群繁殖代数的上限, 若达到, 则终止算法, 密钥恢复失败; 否则, 继续执行下列步骤。

(3) 若子代种群中个体数量不足 N 个, 则循环执行选择、交叉、变异的步骤, 继续生成子代个体。否则, 将子代种群定义为当前代种群, 并清空子代种群, 繁殖代数加 1, 跳转到步骤(2)。

本文主要在 Zhang 方法的基础上开展四个方法的对比实验, 由于 Zhang 等人提出遗传算法 CPA 的原始文献中没有给出选择、交叉的具体方式, 这里说明一下本文中选择、交叉采用的方法: 选择使用的是截断选择的方式, 只从适应度排名靠前的个体中随机选择两个个体用于繁殖下一代的两个个体; 交叉使用的是按字节交叉的方式, 对选择算子得到的两个父代个体以字节为单位, 按照交叉率交换两个父代的字节, 得到两个新的个体。

2.4　遗传算法 CPA 的高效框架

2021 年, Wang 等人[10]给出了遗传算法 CPA 的改进方案, 构成高效的遗传算法能量分析框架, 该框架在原方法的基础上做了下列三种改进:

(1) 基于 CPA 的初始化机制

传统的种群初始化方式通过随机取值产成第一代个体, 新方法采用定义 2 的 CPA 方法进行预计算, 有方向地产生初代个体。

定义 2．CPA 初始化． 通过预先按单字节进行 CPA, 得到 16 个密钥字节对应的 16 组相关系数排名, 每组排名均由 256 个密钥候选值构成。对于待生成的每个初始个体的每个字节, 均在其对应排名中选择一个相关系数较高的取值, 作为其基因片段。

(2) 基于适应度排名的启发式变异

首先引入文献[10]提出的启发式变异的概念, 如定义 3 所示。算法 1 描述了基于适应度排名的启发式变异, 这一过程通过计算适应度来寻找待变异字节的优质基因, 从而使变异不再是随机寻找目标, 而是有方向地取到优质基因。

定义 3．启发式变异． 通过预计算来确定变异的方向, 从而快速获得待变异字节的优质基因。

对于密钥个体 C 的第 i 字节, 首先根据变异率 p_m 决定当前字节是否变异, 即对于每个字节, 均随机生成一个 0～1 之间的数, 若该数小于 p_m, 则发生变异; 否则, 不变异。

若该字节需要变异, 则执行函数 **FindBestByte**(), 其含义为: 在当前密钥个体 C 的 16 字节中, 将第 i 字节遍历 0～255, 其他字节不变, 得到 256 个密钥个体, 分别计算适应度, 从而获得一个适应度排行 R。在排行 R 中选出排名第一的密钥个体, 它通常比现有个体 C 有更优质的基因。最后, 该函数将返回该密钥个体的第 i 字节。

算法 1　基于适应度排名的启发式变异机制

输入: 待变异的 1 个由 16 字节构成的密钥个体 $C=\{c[i]|i\in[1,16]\}$, 变异率 p_m。

输出: 变异后的个体 C。
1: **for** i = 1 to 16
2: $p \leftarrow$ **Random**(0, 1)
3: **if** $p < p_m$ **then**
4: $c[i] \leftarrow$ **FindBestByte**(C, i)
5: **end if**
6: **end for**
7: return C

(3) 密钥枚举

密钥枚举与本文讨论内容无关, 这里不做赘述。

2.5 随机字节变异机制

文献[7]建议按比特进行随机变异, 显然效率太低, 因为 AES 算法是 16 个字节, 若想让一个密钥字节的基因直接转变为最优基因, 按字节进行变异必然是最优的。2021 年, Ding 等人[12]给出了上述两种变异方式存在的问题, 并给出“随机字节变异”方法。

定义 4. 随机字节变异. 以字节为单位对基因进行分段, 分别确定每段是否变异, 变异后的值将从 0～255 之间按均匀分布随机选取。

随机字节变异的具体方法与算法 1 类似, 将算法 1 中的 **FindBestByte** (C, i)函数替换为 **Random** ([0,255])即可。当在取值范围内按均匀分布进行随机字节变异时, 虽然单个字节恰好变异到正确密钥字节取值的概率较小, 但通过增大种群规模、选择合适的变异率, 可显著增加整个种群中出现正确密钥字节取值的概率。由于随机变异出的正确密钥字节所在个体在遗传算法的选择机制下会以更高概率进入下一代, 这使得种群可以不断收敛, 得到最终的正确密钥。

3 遗传算法 CPA 方法与成功率的内在联系剖析

3.1 遗传算法 CPA 实验成功的原因分析

以 AES-128 算法为例, 我们把一个密钥个体的 16 个字节看成是 16 段基因片段, 则遗传算法 CPA 的目标是通过进化得到正确的密钥个体, 该个体的 16 段基因片段都是正确的密钥字节, 我们将其定义为最优基因片段。

执行一次遗传算法 CPA 的目标是使 16 段最优基因片段出现在种群中, 并在进化过程中拼接为一个完整的个体。其中, 拼接可由进化过程自动实现, 而 16 段最优基因片段中的每一片段在进化过程中出现, 只可能来源于下列两种情况:

初始种群中即含有最优基因片段, 该基因片段带来了较高的适应度, 使该基因片段能够以高概率传递下去。

变异产生了最优基因片段, 该基因片段同样因为适应度提升的原因而以较高概率传递到最后。

在上述两种情况中, 种群规模这一参数是决定成功率的关键因素, 这是因为, 在种群规模更大的情况下, 最优基因片段以更高的概率出现在初始种群中, 而在变异时也将有更多的个体发生变异, 从而使最优基因片段以更高的概率出现在当前种群中。然而, 随着种群规模的增加, 计算复杂度也将呈线性增加; 当种群规模增大到一定程度时, 其交叉组合的效果也将接近最优, 而无法获得更高的成功率。因此, 种群规模是遗传算法 CPA 攻击之前需要确定的关键参数, 我们在第 5 节进行讨论。

3.2 遗传算法 CPA 实验失败的原因分析

经典遗传算法 CPA 实验[7]的失败主要归因于存在收敛偏慢、在有限代内无法找到正确密钥的情况, 即局部最优问题, 我们将其本质原因归结为以下几点:

初始代种群随机生成的密钥中, 正确密钥字节较少, 有时几乎没有正确密钥。由于交叉组合无法直接产生正确密钥字节, 故必须通过变异才能出现正确密钥字节。

若变异取值完全随机且变异率偏低, 则会严重滞后正确密钥字节的出现时间。

由于噪声原因, 导致在适应度计算时, 劣质基因的适应度反而高于优质基因的适应度。

尽管遗传算法 CPA 的高效框架[10]给出了 CPA 初始化、启发式变异、密钥枚举等思路来减少实验失败的次数, 但我们仍然认为部分问题尚未得出结论:

(1) 启发式变异每次都朝向最高适应度的基因片段进行变异, 是否仍然(甚至是更)容易出现“局部最优”。

(2) 启发式变异与随机字节变异在成功率上有多大差异。

(3) 与随机初始化相比, CPA 初始化在成功率上带来了多大提升。

我们将在第 3.3 节中解决问题(1), 并在第 5 节中结合实验对问题(2)和(3)的成功率进行评估。

3.3 启发式变异机制的精准度与局部最优问题

在算法 1 中, 启发式变异每次都朝向具有最高适应度的基因片段进行变异, 表面上看它能够加快收敛的速度, 然而, 这个最高的适应度恰恰可能是导致“局部最优”的诱因之一, 本节对这一问题进行研究。

我们以 AES-128 算法为例, 结合实验来验证启发式变异新机制的精准度, 假设 AES 算法 16 个 S-box 的实现方式为硬件并行实现, 信息泄露位置为第一轮 S-box 输出值 y_i 处($i \in [1,16]$)。基于 MATLAB 我们仿真生成了 180 条能量波形, 其信噪比定义为: 128 比特的 $y_1||y_2||y_3||\ldots||y_{16}$ 汉明重量值取 0～128 时, 对应的 129 种能量波形中相邻 2 种波形高度的均值差为 1, 仿真高斯噪声的标准差为 3。

针对仿真波形, 我们基于启发式变异机制实施遗传算法 CPA, 对固定的密钥进行实验, 观察最难恢复的一个密钥字节(正确值为 0xDD)在变异过程中, 其 256 种密钥猜测的平均猜测熵[13](对于某一个密钥猜测, 计算其在多次攻击实验中的猜测熵的平均值)随着繁殖代数的变化。共重复 100 次实验, 其平均结果如图 4 所示。图中红色曲线代表正确猜测 0xDD 的平均猜测熵随着繁殖代数的变化, 255 条蓝色曲线代表密钥字节不等于 0xDD 的 255 种错误猜测的平均猜测熵随着繁殖代数的变化。由图可知, 在排除噪声干扰的前提下, 正确密钥猜测的平均猜测熵总是名列前茅, 因而启发式变异机制中变异的方向大致是有利的。

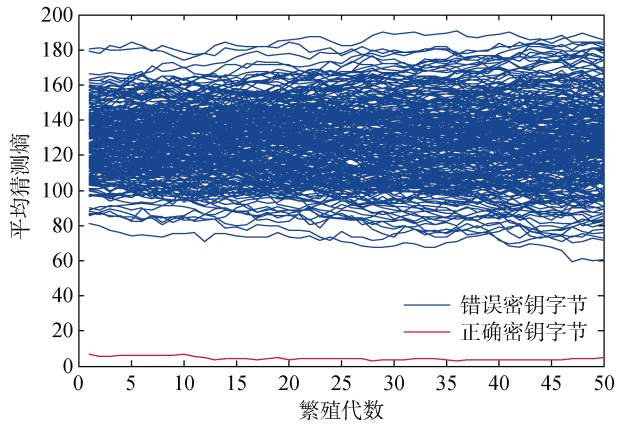

图 4　基于密钥排名的变异方向正确性验证

Figure 4　Mutation direction correctness verification based on key ranking

然而, 上述实验的进化过程中, 正确密钥字节的适应度在密钥候选空间 0～255 的适应度排行中的平均排名约为 5。这说明, 基于适应度排名的启发式变异机制始终朝着适应度排名第一的密钥字节进行取值时, 将大概率取不到正确密钥字节的值。换言之, 当正确密钥字节对应的适应度排名不是第一名时, 启发式变异将无法产生正确密钥字节。该现象足以表明, 启发式变异机制很容易发生局部最优。

3.2 节中问题(1)已解决, 在信息量不充分、正确密钥字节取值的适应度排名不是第一名的情况下, 启发式变异不能通过变异产生正确密钥字节, 故而影响了成功率; 而随机字节变异则可能以相对较高的概率变异产生正确密钥字节, 而非绝对地朝某个方向变异, 故有可能取得更高的成功率。随之而来的是问题(2)中随机字节变异与启发式变异的对比问题, 在后续的两节中, 我们将通过实验手段来研究该问题。

4　种群规模参数的选取

各代种群中个体的数量称为种群规模, 选择足够大的种群规模, 使得候选密钥的数量多、多样性大, 将有利于收敛到正确密钥。在遗传算法不同的实例中, 由于其中的交叉、变异等算子不一样, 所选取的种群规模的合适值也不一样。本文讨论的随机字节变异机制和启发式变异机制有各自不同的特点, 故需首先依据变异机制自身特点选择合适的种群规模, 再对不同方法的效率进行评估。

4.1　随机字节变异机制的种群规模

在随机字节变异机制中, 变异方向为完全随机, 而变异率参数本身又设的很低, 如果种群规模设置得不足够大, 将导致正确密钥字节出现速度太慢。假设种群规模为 1000, 变异率为 0.05, 采用随机字节变异机制, 种群所有个体中某个字节至少有一次出现正确密钥字节取值的概率是 $1-\left(\frac{255}{256}\right)^{1000*0.05} \approx 0.18$。

而当变异率保持不变, 种群规模为 8000 时, 采用随机字节变异机制, 种群所有个体中某个字节至少有一次出现正确密钥字节取值的概率是 $1-\left(\frac{255}{256}\right)^{80000*0.05} \approx 0.79$。

当种群规模足够大时, 正确密钥字节出现在种群中的概率也变大, 有利于收敛到最终的正确密钥。

我们采用经典遗传算法 CPA 对随机字节变异机制进行实验, 以验证上述结论的正确性。实验使用的仿真波形生成方法、信噪比参数均与前一节相同, 共生成了 140 条仿真波形。我们将变异率参数设为 0.05, 种群规模选取 500, 1000, 2000, 3000, 4000, 5000, 6000, 7000, 8000, 9000, 10000 共 11 种取值, 分别进行 400 次实验, 以 10 代为单位, 统计每 10 代中最优个体的正确字节数的平均值, 结果如图 5 所示。图中不同颜色曲线代表不同种群规模取值下每 10 代中最优个体的平均正确字节数, *N_key* 代表种群规模, 从图中可以看出, 随着种群规模增加, 正确密钥字节

数收敛到的值越来越大, 这进一步验证了种群规模的增加使得正确密钥字节出现在种群中的概率增加。当种群规模达到 8000 时, 再继续扩大种群规模, 正确密钥字节数的增加速度与最终收敛的值没有再明显的提升。

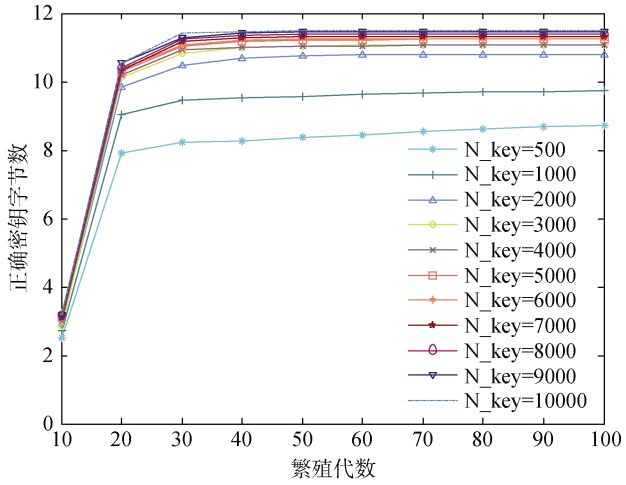

图 5 随机字节变异机制的种群规模与正确密钥字节数的关系

Figure 5 The relationship between the population size and the number of correct key bytes in random byte mutation mechanism

同时, 我们以相关系数的计算次数为依据, 统计随机字节变异机制的计算代价, 得到图 6, 不同颜色数据点代表不同种群规模取值下的计算代价。由图可知, 计算代价始终随着种群规模的增大呈线性增加。因而, 我们选取 8000 作为后续实验中随机字节变异的种群规模。

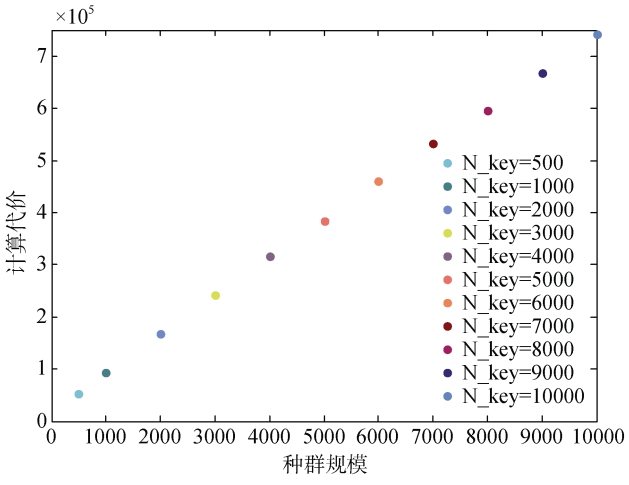

图 6 随机字节变异机制的种群规模与计算代价的关系

Figure 6 Relationship between population size and computational cost in random byte mutation mechanism

4.2 启发式变异机制的种群规模

在基于适应度排名的启发式变异中, 种群的每个个体的变异方向都需要通过遍历各个密钥字节的可能取值、并计算相应适应度得到, 因此, 其种群规模的取值可以比随机字节变异机制的种群规模小的多; 同时, 种群规模的增加同样将带来计算代价的显著增加。

我们采用经典遗传算法 CPA 对启发式变异进行实验, 以验证上述结论的正确性。实验使用的仿真波形生成方法、信噪比参数均与前一节相同, 共生成 140 条仿真波形。我们将变异率参数设为 0.05, 种群规模取 6, 24, 48, 72, 96 共 5 种取值, 分别进行 400 次实验, 以 10 代为单位, 统计每 10 代中最优个体的正确字节数的平均值, 结果如图 7 所示。图中不同颜色曲线代表不同种群规模取值下每 10 代中最优个体的平均正确字节数。

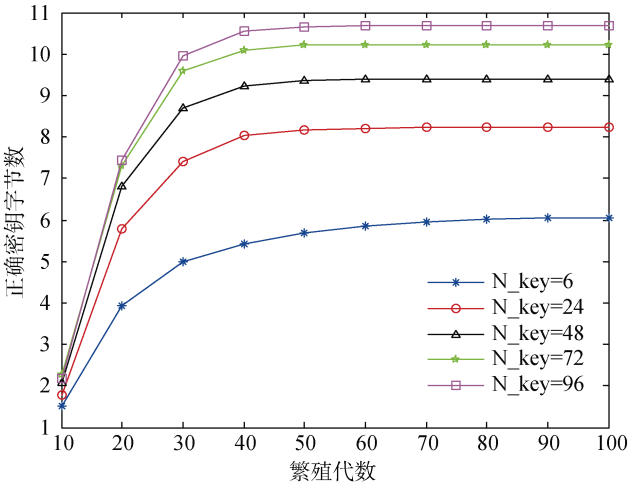

图 7 启发式变异机制的种群规模与正确密钥字节数的关系

Figure 7 The relationship between the population size and the number of correct key bytes in heuristic mutation mechanism

同时, 以相关系数计算次数为依据, 对新方法的计算代价进行统计, 如图 8 所示, 不同颜色数据点代表不同种群规模取值下的计算代价。从两图可知, 随着种群规模增加, 正确密钥字节数收敛到的值越来越大, 然而计算代价也显著增加。对比前一节实验可知, 当随机字节变异的种群规模为 8000 时, 计算代价不足 6×10^5, 正确密钥字节数收敛到的值超过 10; 而当启发式变异的种群规模为 48 时, 计算代价超过 8×10^5, 而正确密钥字节数收敛到的值不足 10。如果继续增加种群规模, 确实可以提高后者的正确密钥字节数, 但与此同时计算代价也将线性增加。因

此, 我们选取 48 作为后续实验中启发式变异机制推荐的种群规模参数。

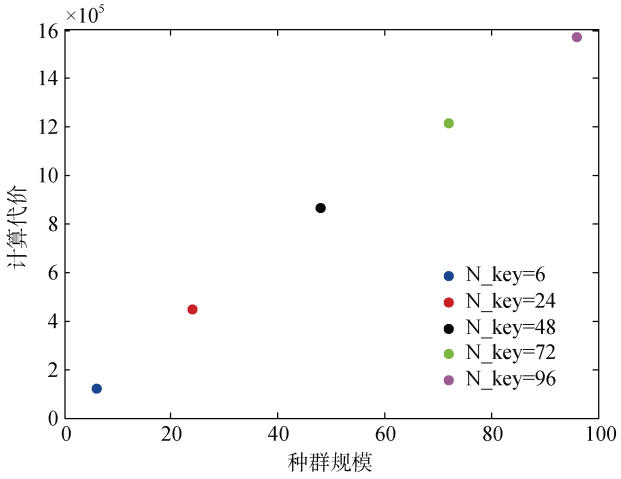

图 8 启发式变异机制的种群规模与计算代价的关系

Figure 8 Relationship between population size and computational cost in heuristic mutation mechanism

5 效率对比与方法讨论

5.1 四种方法的效率对比

在确定种群规模后, 我们将通过实验来对比不同方法的成功率和计算代价这两个指标。为了清晰对比随机初始化与 CPA 初始化、以及启发式变异与随机字节变异之间的差异, 我们对其两两组合, 形成“随机初始化结合启发式变异”、“CPA 初始化结合启发式变异”、“随机初始化结合随机字节变异”、“CPA 初始化结合随机字节变异”共四种方法, 一起进行效率对比。

首先生成 300 条仿真波形, 分别用上述四种方法对其中的 100 条、110 条、120 条、……、300 条进行 1 组分析实验, 得到分析成功或失败的结论。随后将该实验重复 400 组, 统计四种方法的成功率和计算代价, 如图 9 和图 10 所示, 四种颜色曲线分别代表四种方法在不同波形条数下的成功率和计算代价。

从成功率方面看, 为达到成功率 90%的目标, 两种启发式变异的方法所需波形条数约为 190 条, 而两种随机字节变异的方法需约 180 条, 减少了约 5%。从另一个角度来看, 采用 160 条波形曲线进行分析, CPA 初始化结合随机字节变异、随机初始化结合随机字节变异、随机初始化结合启发式变异和 CPA 初始化结合启发式变异这四种方法的成功率分别为 75.5%、66.5%、56.25%和 55.75%。因而我们得到结论: 成功率方面, CPA 初始化结合随机字节变异方法表现最好。

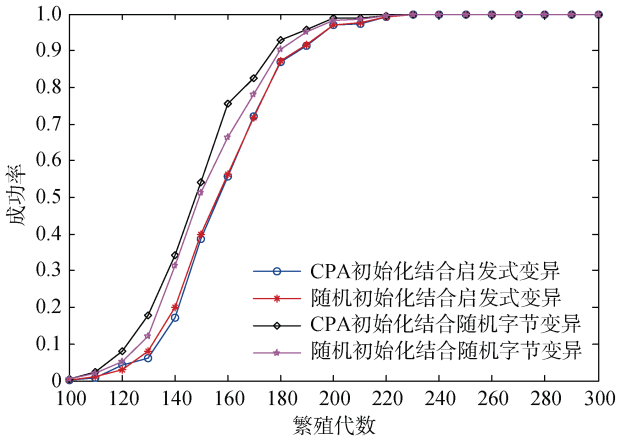

图 9 成功率对比图

Figure 9 Comparison of success rate

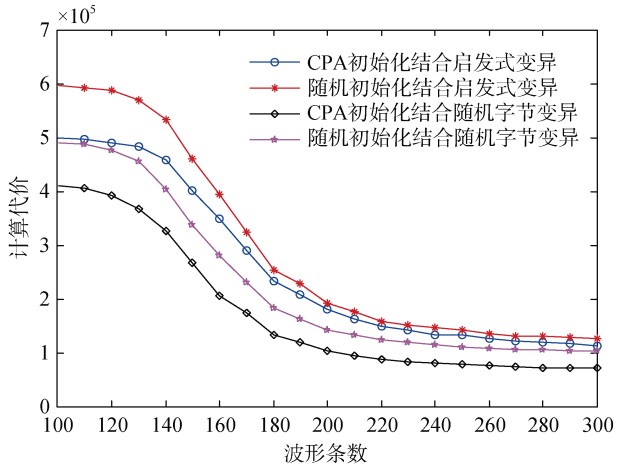

图 10 计算代价对比图

Figure 10 Comparison of computational cost

从计算代价方面看, 在不同波形条数下, CPA 初始化结合随机字节变异方法的计算代价均是四种方法中最低的, 同时结合成功率进行对比, 该方法是上述四种遗传算法 CPA 中表现最好的。因此, 在分组密码芯片测评过程中, 建议将 CPA 初始化、随机字节变异、以及文献[10]给出的密钥枚举三种方法进行结合, 实现遗传算法 CPA 高效的分析。

5.2 讨论

遗传算法 CPA 的现有工作[7,8,10,12]表明, 对硬件并行实现的密码算法开展分析时, 其效率明显高于经典 CPA。这种并行实现的场景主要出现在分组密码的 S-box 输入或输出位置, 因为 S-box 输入值通常以比特为单位泄露、S-box 输出值通常以字节为单位泄露。作为“基因”的密钥比特或字节一旦猜对, 泄露程度就会直接提升, 并以适应度的形式显现出来。

同时, 遗传算法 CPA 也存在下列局限性:

(1) 在分析分组密码算法软件实现时, 遗传算法 CPA 与传统 CPA 相比无明显优势。因为软件实现时各个 S-box 的泄露在时间轴上是分离的, 无需进行全密钥搜索。

(2) 在分析 AES 列混合这类大位宽运算时, 进化速度过慢。这是因为, 当且仅当与列混合对应的 32 比特密钥都猜对时, 适应度才会显著提高, 这种情况发生的概率很低。

(3) 遗传算法 CPA 对随机延时防护对策有一定效果, 例如通过大量样本的统计分析仍可实现密钥恢复。但是, 其对掩码则需要基于遗传算法的流程来实施二阶 CPA, 由于掩码实现的泄露位置未知、二阶 CPA 泄露相对较弱等原因, 其分析复杂度将变得很高。

(4) 遗传算法 CPA 比传统 CPA 增加的处理步骤主要体现在各代中相关系数的计算, 后者的相关系数计算次数是固定的, 例如 AES 算法为 16×256 次, 而前者的相关系数计算则来源于进化过程中适应度的计算(实际进化代数和种群规模的乘积)、CPA 初始化、以及启发式变异。因此, 当信噪比较低、需要较多波形进行分析时, 遗传算法 CPA 运行的复杂度偏高, 分析过程往往需在高性能服务器上完成。

综合上述局限性, 遗传算法 CPA 可以采取一种有效防范思路是: 密码硬件计算过程中, 尽量不要将以字节或比特为单位计算的值存入寄存器。例如, AES 算法可将寄存器安置在列混合输出处, 这种安置方法并不会给 AES 硬件电路带来额外开销。当然, 掩码、随机延时、伪轮、时钟随机化等经典防护对策对增加遗传算法 CPA 攻击难度仍有明显效果。

6 总结

本文剖析了遗传算法 CPA 方法与成功率的内在联系, 引入了随机字节变异机制、启发式变异机制、随机初始化、CPA 初始化并进行组合, 形成 4 种遗传算法 CPA 方法。通过对比 4 种方法的效率, 找到其中成功率最高、计算代价最低的方法, 以有效提升使用人工智能算法开展侧信道分析的效率。

未来工作可以研究遗传算法 CPA 流程中其他组件的优化机制、其他超参数的选取方法, 使整个遗传算法能量分析的执行效率更加优化; 同时, 可针对掩码、伪轮、随机延迟等防护对策开展其普适性研究。此外, 也可采用本文所提新方法面向实际密码芯片开展测评, 发现并解决密码安全性测评与防护设计工作过程中的实际问题。通过对本文工作进一步延伸和改进, 可构建高效、普适、实用的遗传算法 CPA 框架, 从而形成密码芯片物理安全性检测的新工具。

参考文献

[1] Cipher law of the people's Republic of China[OL]. [2020-01-01]. http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74.shtml.
(中华人民共和国密码法[OL]. 2020 年 1 月 1 日).

[2] Kocher P C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and other Systems[M]. *Advances in Cryptology — CRYPTO '96*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996: 104-113.

[3] Kocher P, Jaffe J, Jun B. Differential Power Analysis[M]. *Advances in Cryptology — CRYPTO' 99*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999: 388-397.

[4] Hospodar G, Mulder E, Gierlichs B, et al. Least Squares Support Vector Machines for Side-Channel Analysis[C]. *COSADE 2011*, 2011: 99-104.

[5] Cagli E, Dumas C, Prouff E. Convolutional Neural Networks with Data Augmentation Against Jitter-Based Countermeasures[C]. *International Conference on Cryptographic Hardware and Embedded Systems*, 2017: 45-68.

[6] Timon B. Non-Profiled Deep Learning-Based Side-Channel Attacks with Sensitivity Analysis[J]. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2019: 107-131.

[7] Zhang Z B, Wu L J, Wang A, et al. A Novel Bit Scalable Leakage Model Based on Genetic Algorithm[J]. *Security and Communication Networks*, 2015, 8(18): 3896-3905.

[8] Ding Y L, Shi Y, Wang A, et al. Block-Oriented Correlation Power Analysis with Bitwise Linear Leakage: An Artificial Intelligence Approach Based on Genetic Algorithms[J]. *Future Generation Computer Systems*, 2020, 106: 34-42.

[9] Picek S. Challenges in Deep Learning-Based Profiled Side-Channel Analysis[M]. *Security, Privacy, and Applied Cryptography Engineering*. Cham: Springer International Publishing, 2019: 9-12.

[10] Wang A, Li Y, Ding Y L, et al. Efficient Framework for Genetic Algorithm-Based Correlation Power Analysis[J]. *IEEE Transactions on Information Forensics and Security*, 2021, 16: 4882-4894.

[11] Brier E, Clavier C, Olivier F. Correlation Power Analysis with a Leakage Model[M]. *Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004: 16-29.

[12] Ding Y L, Zhu L H, Wang A, et al. A Multiple Sieve Approach Based on Artificial Intelligent Techniques and Correlation Power Analysis[J]. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 17(2s)Article No. 71,

[13] Standaert F X, Malkin T G, Yung M. A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks[M]. *Advances in Cryptology - EUROCRYPT 2009*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009: 443-461.

许一骏 于 2016 年在电信科学技术研究院信息与通信工程专业获得硕士学位。现任国家工业信息安全发展研究中心高级工程师。研究领域为网络安全。研究兴趣包括: 密码行业应用、密码应用安全性评估、信息技术应用创新。Email: xuyijun@cics-cert.org.cn

唐明环 于 2015 年在北京邮电大学电子科学与技术专业获工学硕士学位。现任中国工业互联网研究院高级工程师。研究领域为工业互联网密码应用。研究兴趣包括: 密码应用、商用密码应用安全性评估等。Email: tangminghuan@china-aii.com

王安 于 2011 年在山东大学信息安全专业获得博士学位。现任北京理工大学研究员。研究领域为密码学。研究兴趣包括: 密码侧信道分析、密码工程。Email: wanganl@bit.edu.cn

李圆 于2021年在北京理工大学计算机科学与技术专业获得硕士学位。现任北京沃东天骏信息技术有限公司工程师。研究领域为密码学。研究兴趣包括: 密码侧信道分析、密码工程。Email: ly18@bit.edu.cn

丁瑶玲 于 2019 年在清华大学计算机科学与技术专业获得博士学位。现任北京理工大学副研究员。研究领域为密码学。研究兴趣包括: 密码侧信道分析、密码工程。Email: dyl19@bit.edu.cn