课程作业：侧信道分析调研

杨一凡
520021911080
上海交通大学

日期：2023 年 5 月 20 日

1 侧信道分析调研出处

1. **论文出处：**2022 年密码学报，针对 SNOW3G 流密码算法的侧信道分析。
2. **侧信道分析对象：**以 SNOW3G 算法实现为研究对象，使用 CPA（相关性能量分析）的方法对其在装有 ATMega128A 芯片的单片机上运行产生的能量消耗信息进行分析。

2 SNOW3G 算法在单片机上的侧信道分析

目前针对 SNOW3G，仅存在少量的侧信道相关的工作，因此为了进一步验证 SNOW3G 抵御侧信道攻击的能力，使用相关性能量分析研究 SNOW3G 的安全性。

2.1 侧信道分析

侧信道分析利用密码设备运行过程中产生的物理信息，如运行时间、能量消耗、电磁辐射等信息，恢复密码设备的中间状态，进一步恢复密码设备中的敏感信息。能量分析攻击是侧信道攻击的一种，其主要关注密码设备运行过程中产生的能量消耗信息，能量分析攻击可以分为简单能量分享（SPA）、差分能量分析（DPA）以及相关性能量分析（CPA）。

1. **SPA：**直接对密码算法执行过程中所采集到的能量消耗信息进行分析的方法，其目标是通过观察密码算法中不同操作引起的能量消耗差异来恢复设备中的密钥信息。
2. **DPA：**记录密码设备对大量不同数据分组进行加密或解密操作所产生的能量消耗信息，通过分析设备的能量消耗与对应的敏感中间值的关系，来恢复出密码设备中的密钥。
3. **CPA：**通过对比猜测密钥可能产生的能量消耗与设备实际产生的能量消耗之间的相关性来推测算法中密钥信息，其一般的攻击流程如下：
   - 选取合适的中间值函数 $f = S(k, d)$，其中 k 是密钥的一部分，d 为已知可变明文，将每一个猜测密钥 $k_i \in \{k_1, k_2, \cdots, k_K\}$ 与每一个 $d_j \in \{d_1, d_2, \cdots, d_D\}$ 代入中间值函数计算得到大小为 $D \times K$ 的中间值矩阵 V；
   - 选择合适的能量消耗模型（如汉明重量模型），将 V 中每一个假设的中间值映射为对应的能量消耗值，得到能量消耗矩阵 H；
   - 采集每一个 $d_j \in \{d_1, d_2, \cdots, d_D\}$ 时密码设备产生的能量消耗曲线，每条曲线包含 R 个采样点，得到实际的能量消耗矩阵 T，计算 H 和 T 中每一列值的相关性，得到大小为 $K \times D$ 的相关系数矩阵 R；
   - R 中每一行表示对应猜测密钥理论上的能量消耗与密码设备实际的能量消耗曲线上各点之间的相关性，选取绝对值最大的相关系数作为猜测密钥和正确密钥的相关系数；

- 对于得到的 K 个相关系数，其中值最大的意味着这个猜测密钥和正确密钥具有最大的相关性，将该密钥作为最佳猜测密钥。

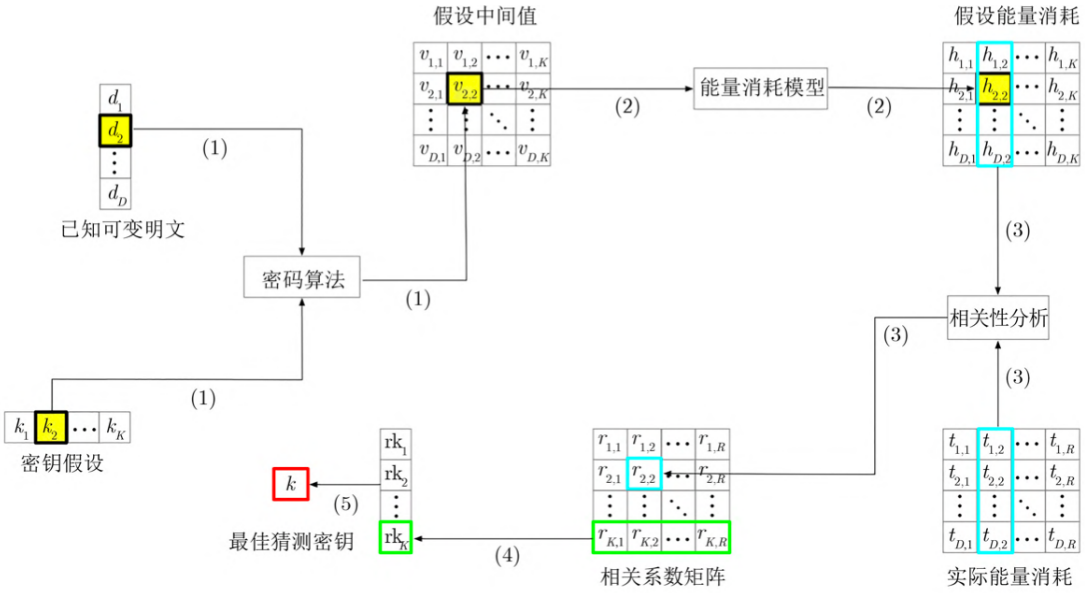

图 1: 相关性能量攻击流程

2.2 SNOW3G 流密码算法

SNOW3G 是一种以字为单位的流密码算法。该算法主要由一个线性反馈移位寄存器（LFSR）和一个有限状态机（FSM）组成。线性反馈移位寄存器由 16 个 32bit 的寄存器 $(s_0, s_1, \cdots, s_{15})$ 和一个反馈回路组成，有限状态机由 3 个 32bit 的寄存器 (R_1, R_2, R_3) 和 2 个 32×32 大小的 SBox(S_1, S_2) 组成。其结构如图 2 所示，其中符号 $\oplus$ 表示按位异或操作，符号 $\boxplus$ 表示整数模 2^32 加法操作。

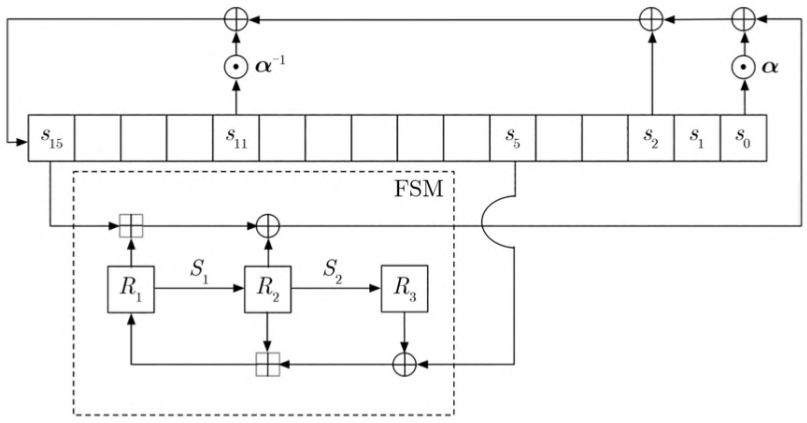

图 2: SNOW3G 算法

算法的运行过程主要分为两个阶段：初始化阶段和密钥流生成阶段。其中算法的初始化过程如下：

- 使用状态值初始化算法中各个寄存器；
- 计算 $F = (s_{15} \boxplus R_1) \oplus R_2$；
- 计算 $r = (R_3 \oplus s_5) \boxplus R_2$；
- 令 $(R_3, R_2, R_1) = (S_2(R_2), S_1(R_1), r)$，其中 S_2, S_1 分别为对应的 SBox 字节替换操作；

- 计算 $s_{16} = (s_{0,1}||s_{0,2}||s_{0,3}||0x00) \oplus MUL\alpha(s_{0,0}) \oplus s_2 \oplus (0x00||s_{11,0}||s_{11,1}||s_{11,2}) \oplus DIV\alpha(s_{11,3}) \oplus F$;
- 令 $(s_{15}, s_{14}, \cdots, s_0) = (s_{16}, s_{15}, \cdots, s_1)$
- 重复步骤 2 至步骤 6 的过程 32 次。

算法中的两个 SBox(S_1, S_2) 的结构如图 3 所示，其中 S_R 和 S_Q 分别对应两个 8×8 大小的 SBox。每次对 R 使用 S_1/S_2 进行字节替换操作时，先将 32bit 的 R 分为 8bit 的 r_0, r_1, r_2 和 r_3，然后用 S_R/S_Q 进行字节替换，再经过后续的操作最终完成 R 到 R' 到映射。

3 针对 SNOW3G 的侧信道分析

侧信道攻击主要采用分而治之的思想，每次仅恢复娃整密钥中的一小部分，但密钥流生成阶段密钥的各个部分已经充分混淆，每一个寄存器状态中都包含着完整的密钥信息，因此主要关注算法的初始化阶段。

3.1 攻击思路

攻击目标是 SNOW3G 流密码算法，由于该算法在使用过程之中，加解密双方需要通过传递 IV 值来同步算法的内部状态，并且出于安全的目的，每次使用的 IV 值不能重复，与 CPA 攻击的典型应用场景十分匹配。因此可以多次采集算法再同步过程中产生的能量消耗信息，结合明文传送的 IV ，来实现对算法的攻击。

3.2 攻击后果

尽管 SNOW3G 能够抵御传统的密码分析攻击，但仍可能遭受到侧信道攻击。可以利用算法 SBox 处的能量泄漏，仅需采集 2000 条能量消耗曲线在 1 小时内即可完整恢复出算法中使用的密钥信息。针对侧信道攻击目前已有一些成熟的防御措施，如向算法中添加掩码以及使用抗功耗分析的逻辑单元，在未来工作中可以结合 SNOW3G 中存在的能量泄漏的特点来设计相应的防护方案，提高算法抗侧信道攻击的能力。

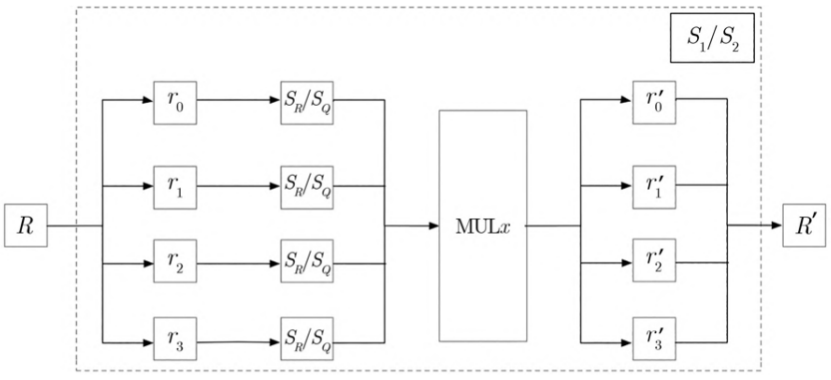

图 3: SBox 结构示意图