针对 AES-128 算法的密钥优势模板攻击

樊昊鹏[1,2],袁庆军[1,2],王向宇[1,2],王永娟[1,2],王 涛[1,2]
(1. 战略支援部队信息工程大学,河南郑州 450001; 2. 河南省网络密码技术重点实验室,河南郑州 450001)

摘 要: 模板攻击分为模板刻画和密钥恢复两个阶段. 针对 AES-128 算法,模板攻击为每一字节密钥构建 256 个模板,当攻击者仅获得 1000 条左右的能量迹时将面临两个问题:一是模板刻画不具有适用性,二是无法恢复正确的密钥. 针对这些问题,本文在模板刻画阶段为 S 盒输出值的汉明重量构建 9 个模板,利用 Panda 2018 数据集提供的 600 条能量迹进行建模;在密钥恢复阶段提出密钥优势叠加的方法,仅需约 10 条相同密钥加密所产生的能量迹即可有效区分正确密钥,降低了攻击的难度并提高了攻击的成功率.

关键词: 模板攻击; AES-128 算法; 密钥优势; 汉明重量模型
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2020)10-2003-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2020.10.018

Key Advantage Template Attack Against AES-128 Algorithm

FAN Hao-peng[1,2], YUAN Qing-jun[1,2], WANG Xiang-yu[1,2], WANG Yong-juan[1,2], WANG Tao[1,2]
(1. *Information Engineering University, Zhengzhou, Henan* 450001, *China*;
2. *Henan Key Laboratory of Network Cryptography, Zhengzhou, Henan* 450001, *China*)

Abstract: Template attack is divided into two stages: template description and key recovery. For AES-128 algorithm, when the attacker only got 1000 energy traces, he would face two problems: one was that the template description would not be applicable, the other was that the correct key would not be recovered. To solve these problems, this paper constructed 9 templates for Hamming weight of S-box output value in the template description stage, and used 600 energy traces provided by panda 2018 data set to build the model; in the key recovery stage, this paper proposed the method of key advantage superposition, which only needed about 10 energy traces encrypted to distinguish the correct key. This method reduces the number of energy traces required in the template description stage and key recovery stage, lowered the difficulty of template attack, and improved the success rate of template attack.

Key words: template attack; AES-128 algorithm; key advantage; Hamming weight model

1 引言

在上世纪末,Kocher 提出了侧信道攻击技术[1]破解密码体制,即利用加密设备在运行时所产生的时间、功率、能量或电磁辐射等侧信道信息的泄露来获知密钥信息,并且可以分段恢复密钥. 侧信道攻击技术具有极高的实用性和破坏性,给密码设备带来了严重的威胁.

2002 年,Chari 团队针对 8 比特的标准 S-box,根据其输入值的汉明重量而建立起 9 个模板,然后将实际获得的信息与模板匹配,从而获取中间信息[2]. 2005 年,Rechbeger 团队提出了特征提取、能量迹预处理和实验分类等方法显著减少了计算量,使得模板攻击拥有更高的效率[3]. 2005 年,Agrawal 团队提出增强的差分能量分析(DPA,Differential Power Analysis)模板攻击,成功实现了传统 DPA 攻击与单比特模板的结合[4]. 2006 年,Archambeau 团队提出了主成分分析和线性判别两种特征提取方法,进一步提高了攻击效率[5]. 同年,Gierlichs 提出了 T 检验的方法,也可以提取能量迹中的特征数据. 之后,大量的研究者将模板攻击应用到实践中,成功实现了对 RC4[6]、AES[7] 和 3DES[8] 等密码算法的破解. 2012 年,王安团队提出相关-模板-诱导攻击[9],其对相关攻击和模板攻击都有良好的纠错能力,并且利用 8051 单片机给出了具体的实验结果. 2013 年,Lerman

收稿日期:2019-07-05;修回日期:2020-06-07;责任编辑:孙瑶
基金项目:国家自然科学基金(No. 61872381);河南省网络密码技术重点实验室开放基金(No. LNCT2019-S02)

团队将欧氏距离和曼哈顿距离应用到模板攻击中,在此基础上,根据极大似然原则,与能量迹匹配程度最高的模板为正确的模板[10]. 2015 年,张海龙团队将马哈拉诺比斯距离相似测度(MDSM)引入模板攻击,提高了模板攻击的密钥恢复效率[11]. 2016 年,Fan 团队提出归一化模板攻击,但在具体计算和效率方面仍需提升[12]. 2018 年,Karimi 团队发现当训练设备和目标设备之间老化程度不匹配时模板攻击更加困难[13]. 2019 年,张海龙副教授利用信息论的相关原理对模板攻击的工作效率和安全性进行了评估[14]. 同年,张海龙副教授从理论上分析了模板攻击与不同参数值之间的精确关系,并在模拟和实际情况下对理论分析的合理性进行了验证[15]. 2019 年,Batina 团队提出在线模板攻击,并证明在线模板攻击可以应用于多种标量乘法算法[16].

模板攻击分为模板刻画和密钥恢复两个阶段. 模板刻画阶段要求攻击者拥有 10000 条以上的能量迹,否则攻击者所刻画的模板将难以进行有效的攻击;在密钥恢复阶段,攻击者恢复正确的密钥仍需要约 100 条能量迹. 针对这两个问题,本文将汉明重量模型应用于模板攻击,使得攻击者仅拥有 600 条能量迹的情况下进行模板攻击. 此外,在密钥恢复阶段,本文创新性的提出了密钥优势叠加的方法,使用约 10 条相同密钥加密所产生的能量迹即可有效区分 AES-128 加密算法的密钥. 实验所使用的数据来源于 Panda 2018 数据集[17]所提供的能量迹,Panda 2018 数据集是标准 AES-128-ECB 的软件实现,曲线采集的是 AES 加密运算过程中第一轮的能量泄露波形,能量曲线的采集平台为 8051 单片机. 实验证明基于汉明重量模型的密钥优势模板攻击操作简单,效率高,具有一定的实用性.

2 模板攻击原理

2.1 主要思想和实现

模板攻击利用了这样一个事实:能量消耗依赖于设备正在处理的数据. 模板攻击使用多元正态分布刻画能量迹的特征,从而捕获能量迹泄露的密钥信息. 在刻画模板的过程中,为了得到被攻击设备输出的侧信道信息,攻击者需要一台与同类的设备进行输出,因此模板攻击是一种选择明文攻击.

模板攻击分为模板刻画和密钥恢复两个阶段. 在模板刻画阶段,攻击者根据已获得的侧信道信息,计算出不同密钥对应的能量迹的特征,如均值向量和协方差矩阵;在密钥恢复阶段,攻击者将能量迹与模板进行匹配,获得对应的匹配概率,一般匹配概率最大的模板对应的密钥即为正确密钥.

在模板刻画阶段,假设攻击者获得 AES-128 密码设备加密产生的 n 条能量迹 $\boldsymbol{T}_1,\boldsymbol{T}_2,\cdots,\boldsymbol{T}_n$,每条能量迹上有 t 个特征点. 将这 n 条能量迹分为 256 个集合 $A_1,A_2,\cdots,A_{256}$,$|A_i|=n_i$ 其中第 i 个集合 A_i 是密钥为 i 时加密所产生的能量迹.

定义第 i 个猜测密钥的均值向量 $\boldsymbol{m}_i$ 为

$$\boldsymbol{m}_i=\frac{\sum_{\boldsymbol{T}_j\in A_i}\boldsymbol{T}_j}{n_i} \tag{1}$$

定义第 i 个猜测密钥的协方差矩阵 $\boldsymbol{C}_i$ 为

$$\boldsymbol{C}_i=\frac{1}{n_i-1}\sum_{\boldsymbol{T}_j\in A_i}(\boldsymbol{T}_j-\boldsymbol{m}_i)(\boldsymbol{T}_j-\boldsymbol{m}_i)' \tag{2}$$

我们将$(\boldsymbol{m}_i,\boldsymbol{C}_i)$称为第 i 个猜测密钥对应的模板.

在密钥恢复阶段,攻击者利用特征刻画了模板$(\boldsymbol{m}_i,\boldsymbol{C}_i)$之后,针对给定的一个被攻击设备的能量迹 $\boldsymbol{Trace}$,计算如下概率:

$$p(\boldsymbol{Trace};(\boldsymbol{m}_i,\boldsymbol{C}_i)=\frac{\exp(-0.5*(\boldsymbol{Trace}-\boldsymbol{m}_i)'\boldsymbol{C}_i^{-1}(\boldsymbol{Trace}-\boldsymbol{m}_i)}{\sqrt{(2\pi)^t\cdot\det(\boldsymbol{C}_i)}} \tag{3}$$

概率值反映了模板与给定能量迹的匹配程度. 概率值越大,则模板与给定能量迹的匹配程度越高.

2.2 存在的问题

模板攻击简单易行,成本低廉,因此获得了广泛的应用. 但是,如下几条缺点限制了模板攻击的适用范围和效果:

(1)模板刻画需要大量能量迹. 针对 AES-128 算法,攻击者需要对某一字节密钥构建 256 个模板,因此需要 10000 条以上的能量迹. 当攻击者获得的能量迹不足时,如 Panda 2018 提供的 600 条能量迹,攻击者无法建立有效的模型,因此无法进行模板攻击.

(2)密钥恢复需要 100 条能量迹. 针对 Panda 2018 数据集,模板攻击由单条能量迹破解密钥信息的概率为 2%. 因此,需要对多条能量迹与密钥匹配的概率进行叠加,才能破解最终的密钥. 经过实验验证,密钥恢复所需能量迹约为 100 条. 当攻击者获得的能量迹数目少于 100 条时,将很难恢复正确的密钥.

根据模板攻击存在的问题,本文将汉明重量模型应用于模板攻击,只需建立 9 个模板即可进行模板攻击. 因此模板攻击在攻击者所获得能量迹仅有 1000 条左右时也可以使用,扩大了模板攻击的适用范围. 其次,本文创新性的在密钥恢复阶段提出了密钥优势叠加的方法,使用约 10 条相同密钥加密所产生的能量迹即可有效区分正确密钥密钥. 具体的原理和实验将在第 3 节与第 4 节中详细介绍.

3 密钥优势模板攻击

密钥优势模板攻击的主要思想和实现方法如下所述.

针对第 2 节所提出的问题,本文对模板攻击的步骤加以完善,具体步骤如图 1 所示.

图1　基于汉明重量模型的密钥优势模板攻击流程图

在选取特征点阶段,由式(2)可知,协方差矩阵 $\boldsymbol{C}_i$ 的大小与能量迹点数的平方成正比. 为了提高计算效率,本文采用差分和技术[2]和 T 检验技术[7]两种技术选取与密码算法中间值相关程度最高的几个特征点,在不影响实验效果的基础上显著的减少了运算量.

在模板构建阶段,模板攻击需要构建 256 个模板,因此需要大量的能量迹. 当攻击者得到的能量迹较少时(如 600 条),无法有效构建 256 个模板,因此需要对模板攻击进行改进. 针对 AES-128 算法,假设第一字节明文为 d,第一字节密钥为 k,则经过第一轮 S 盒的输出 $v=S(d\oplus k)$. 攻击者可以将密码算法的密码算法中间值 v 映射到其汉明重量 $HW(v)$,即构建 9 个模板.

假设攻击者获得 AES-128 密码设备加密产生的 n 条能量迹 $\boldsymbol{T}_1,\boldsymbol{T}_2,\cdots,\boldsymbol{T}_n$,对应密码设备的密码算法中间值为 $v_1,v_2,\cdots,v_n$. 将这 n 条能量迹分为 9 个集合 $B_1,B_2,\cdots,B_9$,$|B_i|=n_i$ 其中集合 B_i 中的能量迹 $\boldsymbol{T}_j$ 满足 $HW(v_j)=i$.

定义猜测汉明重量为 i 的均值向量 $\boldsymbol{m}_i$ 为

$$\boldsymbol{m}_i=\frac{\sum\limits_{T_j\in B_i}\boldsymbol{T}_j}{n_i} \tag{4}$$

定义猜测汉明重量为 i 的协方差矩阵 $\boldsymbol{C}_i$ 为

$$\boldsymbol{C}_i=\frac{1}{n_i-1}\sum_{T_j\in B_i}(\boldsymbol{T}_j-\boldsymbol{m}_i)(\boldsymbol{T}_j-\boldsymbol{m}_i)' \tag{5}$$

我们将$(\boldsymbol{m}_i,\boldsymbol{C}_i)$称为汉明重量 i 对应的模板. 在汉明重量恢复阶段,根据式(3)与式(4)、式(5)两式计算的模板,可以得到给定的能量迹 $\boldsymbol{T}_i$ 与 9 个模板$(\boldsymbol{m}_w,\boldsymbol{C}_w)$的匹配概率 $p_w,w=0,1,\cdots,8$.

将汉明重量 w 对应的明文通过第一轮 S 盒的输出值(以下简称为中间值)的集合记为 D_w. 显然有$|D_w|=C_8^w$. 将密钥空间记为 K_w,并记 S^{-1}为 S 盒的逆变换,则对任意 $d\in D_w$,存在 $k\in K_w$,使得 $k\oplus m=S^{-1}(d)$,其中 m 为明文是攻击者已知的. 此过程如图 2 所示.

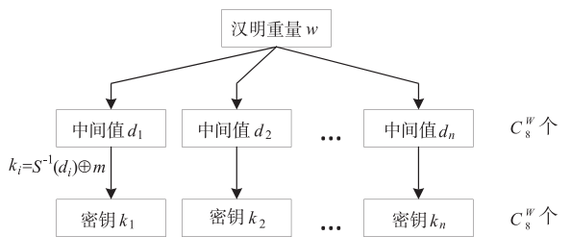

图2　通过汉明重量求出对应的密钥集合

密钥优势叠加:首先将所有预测密钥的优势记为 0. 设正确密钥为 k_s,中间值的汉明重量为 w_s,攻击者对所有集合 K_j 中预测密钥的优势增加对数值 $\ln p_j(j=0,1,\cdots,8)$,这里使用概率的对数值进行计算以避免指数爆炸问题. 密钥 k_s 加密产生的多条能量迹与模板$(\boldsymbol{m}_{w_s},\boldsymbol{C}_{w_s})$的匹配概率 p_s 大于与其他模板匹配的概率. 经过多轮叠加,正确密钥的优势会远高于其他密钥.

4　实验结果

4.1　特征点的选取

为了提高计算效率,我们需要选取能量迹中与中间值有关的一部分特征点进行计算. 特征点的选取可以用以下两种方法.

差分和技术:假设有 n 条能量迹 $\boldsymbol{T}_1,\boldsymbol{T}_2,\cdots,\boldsymbol{T}_n$,将这 n 条能量迹按照其对应的中间值的汉明重量分为 9 组,对每组能量迹的集合计算:

$$\boldsymbol{M}_i=\frac{\sum\limits_{j=1}^{n_i}\boldsymbol{T}_j}{n_i},\boldsymbol{SOD}=\sum_{i_1=0}^{7}\sum_{i_2=i_1+1}^{8}(\boldsymbol{M}_{i_1}-\boldsymbol{M}_{i_2}) \tag{6}$$

然后选择使得 $\boldsymbol{SOD}$ 取值最大的时间点作为特征点.

T 检验技术:T 检验技术是在计算 $\boldsymbol{M}_i$ 的基础之上,计算:

$$\boldsymbol{V}_i=\frac{\sum\limits_{j=1}^{n_i}(\boldsymbol{T}_j-\boldsymbol{M}_i)^2}{n_i},\quad \boldsymbol{TTest}=\sum_{i_1=0}^{7}\sum_{i_2=0}^{8}\frac{(\boldsymbol{M}_{i_1}-\boldsymbol{M}_{i_2})^2}{\frac{\boldsymbol{V}_{i_1}}{n_{i_1}}-\frac{\boldsymbol{V}_{i_2}}{n_{i_2}}} \tag{7}$$

然后选择使得 $\boldsymbol{TTest}$ 取值最大的时间点作为特征点[14].

差分和技术各个时间点的取值如图 3 所示.

T 检验技术各个时间点的取值如图 4 所示.

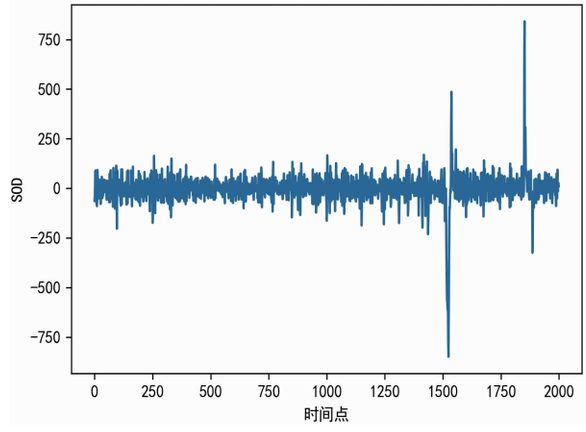

图3　差分和方法选取特征点

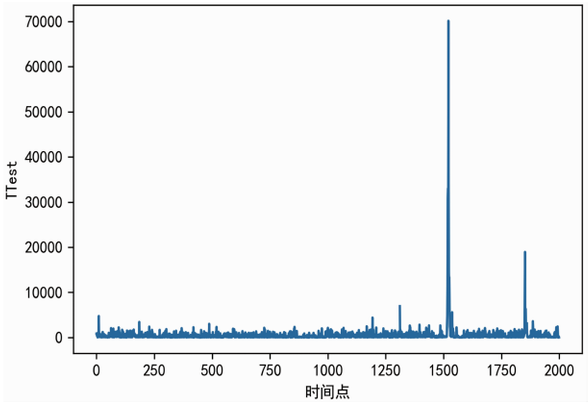

图4 T检验方法选取特征点

二者所得到的特征点相同,因此本文选取 1518、1519、1520、1521、1522、1523、1524、1525、1851、1852 十个点作为特征点.

4.2 模板构建与密钥恢复

由于 AES-128 算法是以字节为单位进行加密运算,因此本节以第一字节为例演示破解结果.

将 600 条能量迹按照对应的中间值的汉明重量分为 9 个集合. 由式(4)和式(5)计算均值向量 $\boldsymbol{m}_i$ 和协方差矩阵 $\boldsymbol{C}_i$,得到 9 个模板$(\boldsymbol{m}_i,\boldsymbol{C}_i)$,$i=0,1,\cdots,8$.

为了避免指数爆炸所产生的计算问题,用 $\ln p(\boldsymbol{Trace};(\boldsymbol{m}_i,\boldsymbol{C}_i)$代替 $p(\boldsymbol{Trace};(\boldsymbol{m}_i,\boldsymbol{C}_i)$计算给定的能量迹 $\boldsymbol{Trace}$ 与每个模板的匹配程度,计算公式如下:

$$\begin{aligned}&\ln p(\boldsymbol{Trace};(\boldsymbol{m}_i,\boldsymbol{C}_i)\\&=-0.5*[t\ln(2\pi)+\ln\det(\boldsymbol{C}_i)\\&\quad+(\boldsymbol{t}-\boldsymbol{m})'\boldsymbol{C}_i^{-1}(t-m)]\end{aligned}\tag{8}$$

根据极大似然法则,正确的中间值的汉明重量 i 所对应的能量迹与模板$(\boldsymbol{m}_i,\boldsymbol{C}_i)$代入式(6)计算出的概率应是最大值. 为了验证模型的正确性,本节选取了中间值的汉明重量为 1 ~ 7 的能量迹与模板进行匹配,这 7 条能量迹与建模所使用的 600 条能量迹是不同的. 使用式(6)计算出的结果如图 5 所示.

从图 5 中可以看出,汉明重量 $w_i(i=1,2,\cdots,7)$对应的能量迹与其模板$(\boldsymbol{m}_{w_i},\boldsymbol{C}_{w_i})$的匹配程度都是最大值,因此模型具有正确性. 又因为所选能量迹与建模所使用的能量迹并不相同,所有模型具有普遍性. 至此,模型构建完成.

在密钥恢复阶段,对于给定的能量迹,攻击者可以计算出能量迹与 9 个模板的匹配程度,得到中间值的汉明重量为 w_s 的概率 $p_s,s=0,1,\cdots,8$,随后对汉明重量 w_s 对应的密钥集合 K_s 中预测密钥的优势增加对数值 $\ln p_s,s=0,1,\cdots,8$. 当能量迹有 10 条时,密钥 7E 的优势已经十分明显,攻击者可以有效区分正确的密钥,如图 6 所示.

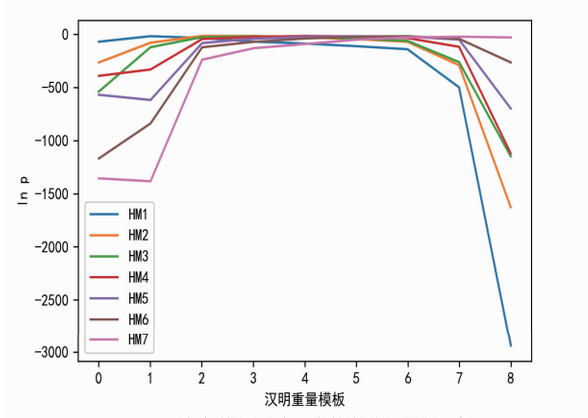

图5 给定能量迹与9个模板的匹配程度

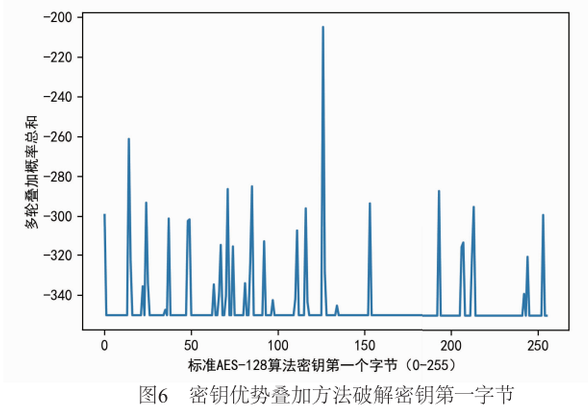

图6 密钥优势叠加方法破解密钥第一字节

由于图中优势最大的点为 7E,故破解密钥的第一字节为 7E.

对密钥其余 15 个字节进行同样的操作,最终得到 128 比特密钥为:

7E BD 52 1B 4F E1 5B 89 4E 8C 96 F6 4E 00 51 6B

为了验证基于汉明重量模型的密钥优势模板攻击的准确性,从测试集中随机抽取 n 条能量迹,判断由此 n 条能量迹恢复的密钥是否为正确密钥,得到正确率与能量迹条数的关系如图 7 所示.

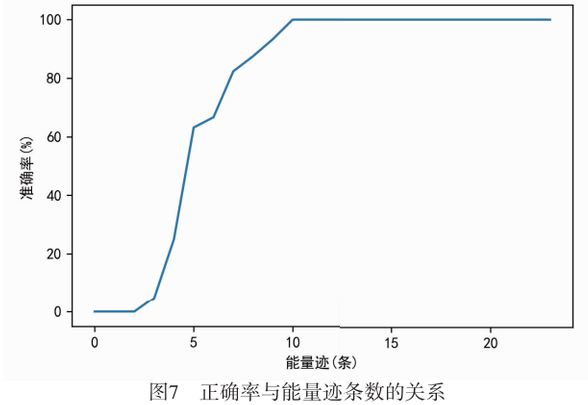

图7 正确率与能量迹条数的关系

当随机选取的能量迹在 10 条以上时,攻击者有 100% 的概率恢复出正确的密钥. 因此基于汉明重量的密钥优势模板攻击是准确且高效的.

4.3 方案对比

为了说明基于汉明重量模型的密钥优势模板攻击的优势,本小节将此方法与针对 AES-128 算法的模板攻击以及近几年对模板攻击的一些改进方法——针对 AES 的快速模板攻击[18]、基于汉明重量模型的密码设备放大模板攻击[19]和基于公共协方差矩阵的实用模板攻击[20]进行比较,比较结果如表 1 所示.

表 1　模板攻击方案对比

攻击方案	被攻击算法	建模所需能量迹	密钥恢复所需能量迹
密钥优势模板攻击	AES-128	600 条	10 条
模板攻击	AES-128	10000 条	100 条
快速模板攻击	AES-128	8000 条	43 条
放大模板攻击	AES-128	450 条	48 条
实用模板攻击	AES-128	10000 条	500 条

由表 1 可以看出,基于汉明重量模型的密钥优势模板攻击在模板构建阶段所用的能量迹较少,降低了模板攻击的难度;同时,在密钥恢复阶段仅需 10 条能量迹便以 100% 的概率恢复正确密钥,显著提高了攻击的成功率. 因此在实际应用中,基于汉明重量模型的密钥优势模板攻击具有一定的优越性.

5 结论

针对 AES-128 算法,本文利用 600 条能量迹为 S 盒输出值的汉明重量构建 9 个模板,在攻击者仅获得 600 条能量迹的情况下也可以使用模板攻击,拓宽了模板攻击的应用范围. 在成功恢复汉明重量的基础上,本文提出密钥优势叠加的方法,使得攻击者仅需使用约 10 条相同密钥加密所产生的能量迹即可有效区分正确的密钥. 本文的方法减少了攻击者所需的能量迹数目,提高了密钥破解的成功率. 除了破解 AES-128 加密算法的密钥之外,本文提出的方法可以应用到任何一个 SPN 结构的加密算法中,更一般地说,如果加密算法中有包含密钥信息的已知可逆映射,攻击者都可以用密钥优势叠加的方法破解密钥. 本文的方法在模板攻击的密钥恢复阶段提供了新思路.

参考文献

[1] Kocher P C. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems[A]. Annual International Cryptology Conference[C]. Berlin, Heidelberg: Springer, 1996. 104 – 113.

[2] Chari S, Rao J R, Rohatgi P. Template attacks[A]. International Workshop on Cryptographic Hardware and Embedded Systems[C]. Berlin, Heidelberg: Springer, 2002. 13 – 28.

[3] Rechberger C, Oswald E. Practical template attacks[A]. International Workshop on Information Security Applications[C]. Berlin, Heidelberg: Springer, 2004. 440 – 456.

[4] Agrawal D, Rao J R, Rohatgi P, et al. Templates as master keys[A]. International Workshop on Cryptographic Hardware and Embedded Systems[C]. Berlin, Heidelberg: Springer, 2005. 15 – 29.

[5] Archambeau C, Peeters E, Standaert F X, et al. Template attacks in principal subspaces[A]. Proceedings of the 8th International Conference on Cryptographic Hardware and Embedded Systems[C]. USA: ACM, 2006. 1 – 14.

[6] DENG Gao-ming, ZHANG Peng, ZHAO Qiang. Formal analysis for cipher chip's security against template attack[A]. Proceedings of the 2009 First IEEE International Conference on Information Science and Engineering[C]. USA: IEEE, 2009. 1741 – 1744.

[7] Gierlichs B, Lemke-Rust K, Paar C. Templates vs stochastic methods[A]. International Workshop on Cryptographic Hardware and Embedded Systems[C]. Berlin, Heidelberg: Springer, 2006. 15 – 29.

[8] Oswald D, Paar C. Breaking mifare DESFire MF3ICD40: power analysis and templates in the real world[A]. International Workshop on Cryptographic Hardware and Embedded Systems[C]. Berlin, Heidelberg: Springer, 2011. 207 – 222.

[9] WANG An, et al. Overcoming significant noise: correlation-template-induction attack[A]. International Conference on Information Security Practice and Experience[C]. Berlin, Heidelberg: Springer, 2012. 393 – 404.

[10] Lerman L, Medeiros S F, Veshchikov N, et al. Semi-supervised template attack[A]. International Workshop on Constructive Side-Channel Analysis and Secure Design[C]. Berlin, Heidelberg: Springer, 2013. 184 – 199.

[11] ZHANG H, FENG D, ZHOU Y. Mahalanobis Distance Similarity Measure Based Distinguisher for Template Attack[M]. USA: John Wiley & Sons, Inc. 2015.

[12] FAN G, ZHOU Y, ZHANG H, et al. Towards optimal leakage exploitation rate in template attacks[J]. Security and Communication Networks, 2016, 9(16): 3116 – 3126.

[13] Karimi N, Guilley S, Danger J L. Impact of aging on template attacks[A]. Proceedings of the 2018 on Great Lakes Symposium on VLSI[C]. USA: ACM, 2018. 455 – 458.

[14] ZHANG H, ZHOU Y. Template attack vs stochastic model: An empirical study on the performances of profiling attacks in real scenarios[J]. Microprocessors and Microsys-

tems,2019,66(4):43 – 54.
[15] ZHANG H. On the exact relationship between the success rate of template attack and different parameters[J]. IEEE Transactions on Information Forensics and Security,2019,15(7):681 – 694.
[16] Batina L,Chmielewski Ł,Papachristodoulou L,et al. Online template attacks[J]. Journal of Cryptographic Engineering,2019,9(1):21 – 36.
[17] 樊昊鹏. Panda 2018 数据集[OL]. https://github.com/kistoday/Panda2018/tree/master/challeng1,2019-7-1.
[18] 崔琦,王思翔,段晓毅,等. 一种 AES 算法的快速模板攻击方法[J]. 计算机应用研究,2017,34(6):1801 – 1804.
CUI Qi, WANG Si-xiang, DUAN Xiao-yi, et al. A fast template attack method for AES algorithm[J]. Computer Application Research,2017,34(6):1801 – 1804. (in Chinese)
[19] 欧长海,王竹,黄伟庆,等. 基于汉明重量模型的密码设备放大模板攻击[J]. 密码学报,2015,2(5):477 – 486.
OU Chang-hai, WANG Zhu, HUANG Wei-qing, et al. Amplification template attack of cryptographic device based on Hamming weight model[J]. Journal of Cryptography,2015,2(5):477 – 486. (in Chinese)
[20] 刘飚,孙莹. 基于公共协方差矩阵的实用模板攻击[J]. 计算机应用研究,2016,33(1):236 – 239.
LIU Biao, SUN Ying. Practical template attack based on common covariance matrix[J]. Computer Application Research,2016,33(1):236 – 239. (in Chinese)

作者简介

樊昊鹏 男,1997 年 4 月出生,河南新密人. 现为战略支援部队信息工程大学硕士研究生,主要研究方向为网络空间安全,侧信道分析技术.
E-mail:fanhaopeng15gc@sina.com

袁庆军 男,1993 年出生,河北衡水人. 硕士、讲师,研究方向为网络空间安全、侧信道分析技术.
E-mail:gcxyuan@outlook.com