# 文献阅读：Decrypting Without Keys: The Case of the GlobalPlatform SCP02 Protocol

研究目标:

如题所言，对 SCP02 协议下的无密钥解密方法的探讨。这里，作者对于该研究的必要性的探讨十分有趣。他提到，尽管早在 2018 年 SCP02 在作者初步研究结果的影响下就被 GlobalPlatform 弃用，但考虑到智能卡行业的生命周期，SCP02 仍是现存智能卡上被部署最多的安全通道，因而对它的攻击方式的研究依旧十分有意义。

主要贡献:

由于作者的工作是基于大量其他研究成果发展而来的，而我又并不具有将其完全分清的阅读能力，因此我选择不加分别地全部描述。

作者介绍了如何对 SCP02 协议执行 padding oracle 攻击，并解释了如何利用不同的统计技术来利用这些 cards 提供的 timing side channel。其展示了在不同类型的卡和设备进行的实际实验的结果，用以表明真实世界的攻击场景确实是可能的。当然，作者也给出了他的对策。

内容描述:

常规的 padding oracle 攻击的核心逻辑在于：如果在加密过程中使用了填充数据，并且必须在解密过程中验证填充数据。而这就给了攻击机会，用最简单的情形举例：加密方案中为了识别填充部分，在填充的一串 00 中以 80 为开头，这样攻击者便可以构建多字节的明文攻击序列，此时序列的后续位会在解密时呈现为 00 串，而首位则会进行遍历，当其遍历至真实值时，其解密结果会是 80。唯有此时，系统响应为正确的解码结果，其余为错误结果。

当然，真实情况并不会如此简单，实际的部件会无论正确与否仅输出错误代码。而作者选择进行侧信道攻击——响应时间。当 padding 数据有效时，卡片的响应时间（反映卡片的计算时间）比 padding 数据无效时要长。不过由于不同设备上，该时间差或极小或显著，作者给出了两套统计方法用于计算出攻击有效的时间戳。

应对策略上，作者给出了一套双重解密方案，这样该 orcale 仅能获得加密后的明文数据。

我的思考:

1、现实场景很重要，作者的理论攻击方案早在 2017 年便已经初具雏形，但他还是做了现实场景的攻击尝试。

2、侧信道好有用，该论文的时间差异攻击和我在网安实践课程上学到的无反馈网站密码破译方案简直一摸一样，在绕过常规防备上，时间温度这类非网络数据形式的

信息超乎寻常的好用。

3、所谓跨学科，此次论文中，最让我印象深刻的是作者的统计方法设计。概统知识的运用自然不必多说，里面还包含一部分物理实验的逻辑，对于过小的时间差异，可以数次累加再做分析，这和物理实验里多次实验便于误差分析如出一辙。

[0] Avoine, G., Ferreira, L. Decrypting Without Keys: The Case of the GlobalPlatform SCP02 Protocol. J Cryptol 38, 9 (2025). https://doi.org/10.1007/s00145-024-09528-z