

Blink: Breaking Parallel Implementation of Crystals-Kyber

王舰, 曹伟琼, 陈华, 李昊远

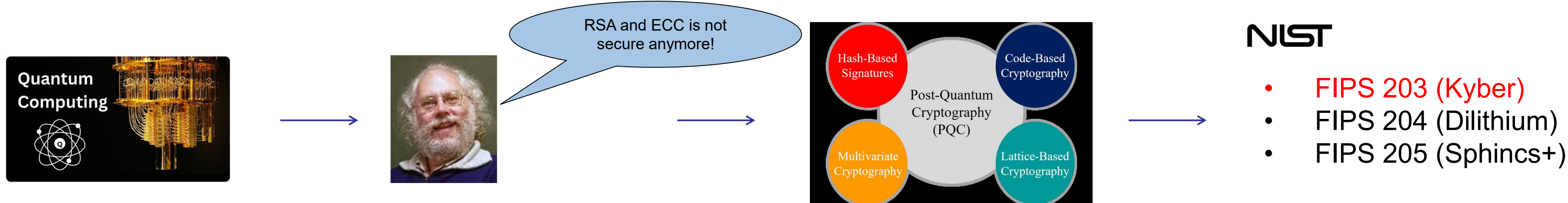
42nd IEEE ICCD, 2024, 105-113.

(CCF-B, Best Paper Nominees (4/277))

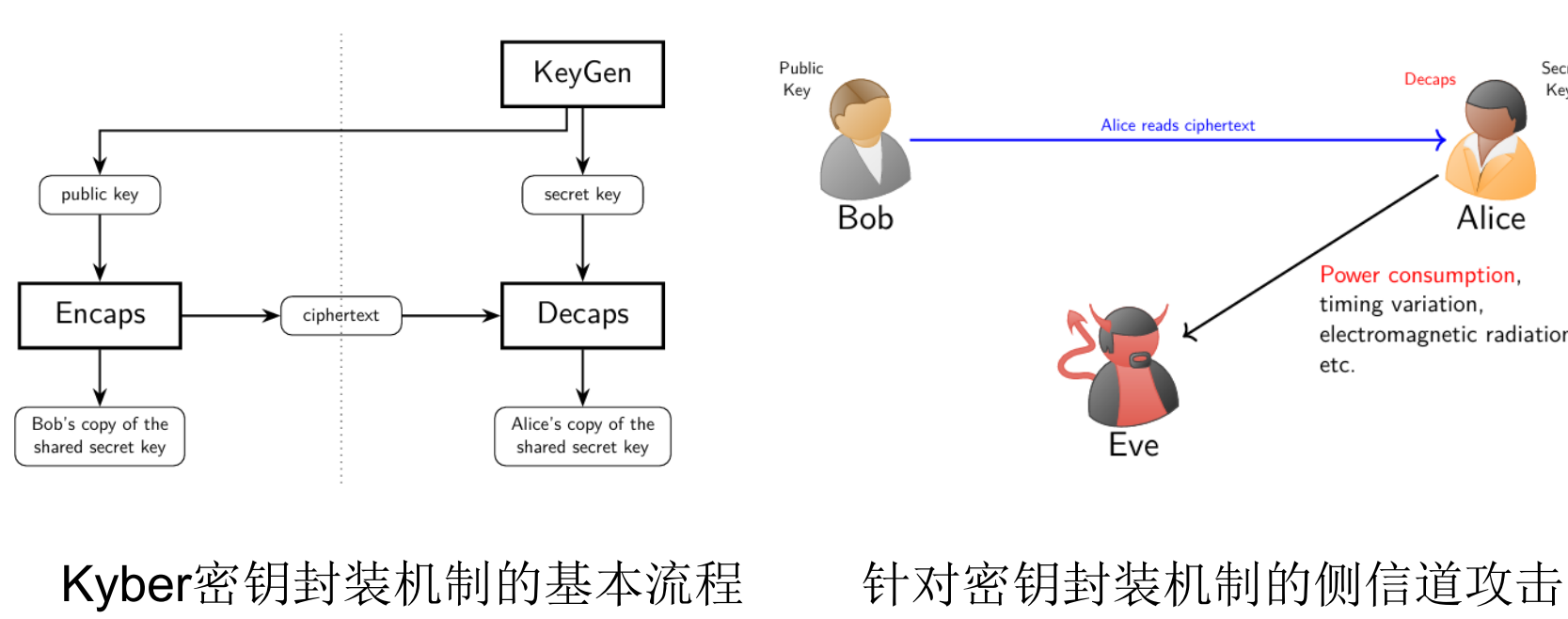
wangjian2019@iscas.ac.cn

引言

为了应对量子计算带来的潜在威胁, 使用后量子密码算法替换经典的公钥密码算法迫在眉睫。当这些新的算法实现在硬件平台上时, 是否存在潜在的侧信道攻击威胁?



基本概念



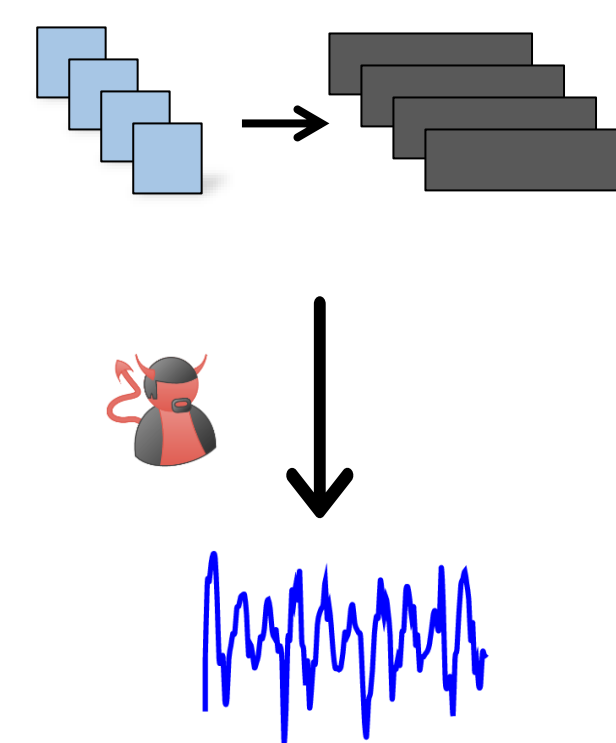
能量泄露模型

针对并行实现的消息编码操作, 构建通用的消息比特能量泄露模型。

$$L = \alpha * hd(nl_i, nr_i) + N_0 + N_1$$

其中, N_0 表示不可避免的采集噪声, 而 N_1 则表示非目标比特消息编码导致的能量消耗信息。

$$N_1 = \sum_{j \neq i} \alpha * hd(nl_j, nr_j)$$



攻击方法

多密文消息恢复策略

对密文 $c = (u, v)$, 令 u 仅包含一个非 0 多项式 $u[j]$, 且

$$u[j] = k_u \in \left(-\frac{q}{4\eta_1}, \frac{q}{4\eta_1}\right],$$

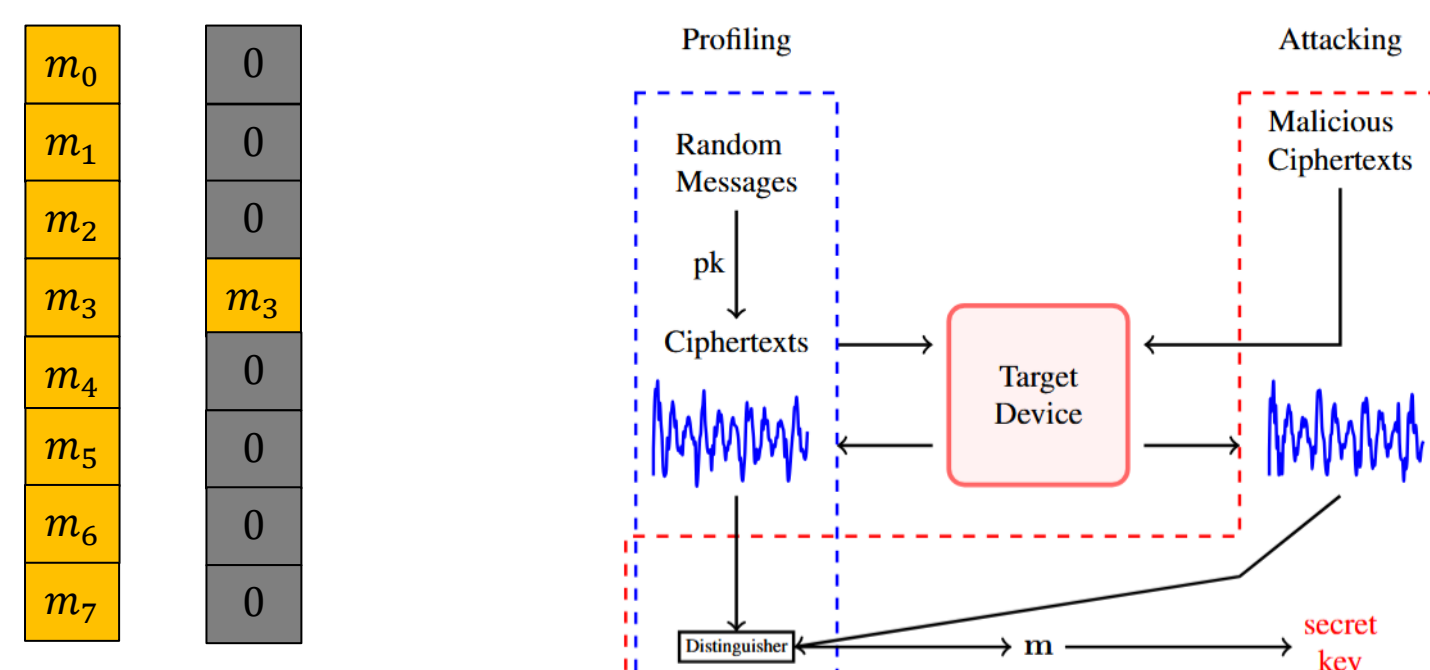
对 p 路并行实现, 针对每 $2p$ 比特中第 t 比特, 令 $v = \sum_{i=0}^{n-1} (k_v * \delta(i))x^i$, 其中

$$\delta(i) = \begin{cases} 1, & \text{if } i = t \bmod 2p; \\ 0, & \text{else.} \end{cases}$$

在该条件下, 有

$$m[i] = \begin{cases} \text{Compress}_1(k_v - k_u * s[j, i]), & \text{if } i = t \bmod 2p; \\ 0, & \text{else.} \end{cases}$$

遍历 $t \in [0, 2p)$ 即可恢复对应一组 (k_u, k_v) 的完整消息。



常规消息 (左) 和结构化密文对应的消息 (右, $p = 4, t = 3$)

密钥恢复攻击流程

最优密钥恢复树

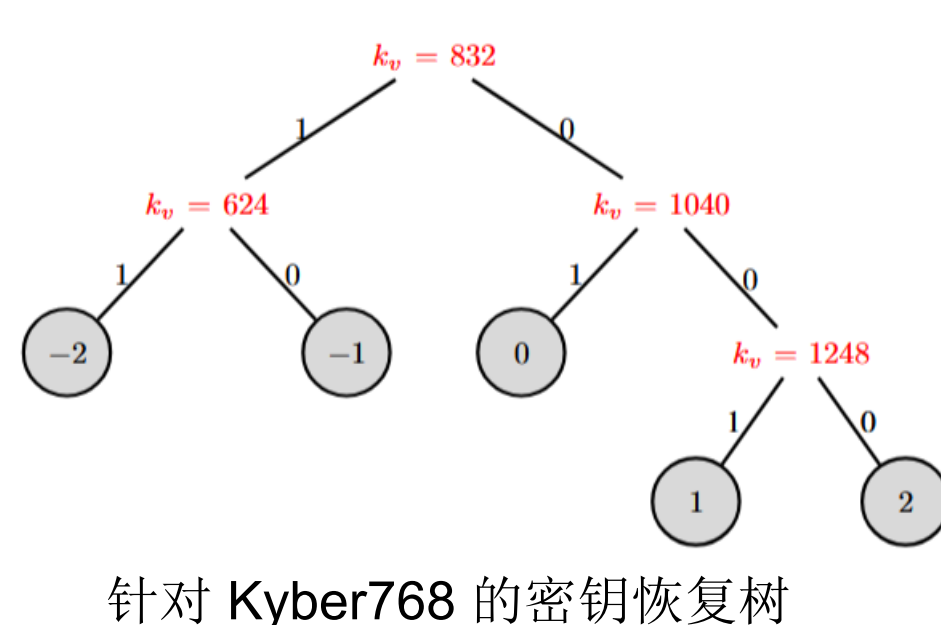
密钥恢复的准确率依赖于消息恢复的准确率

$$P_s = (P_m)^{E_s},$$

由于 $P_m \leq 1$, 在 P_m 一定的情况下, P_s 与 E_s 的值成反比。

利用私钥系数的特殊分布, 本文提出一种基于最优前缀码技术的密文对选择方法, 实现最小化 E_s 的目的。

$$E_s = \sum_{i=0}^{2n_1} P_{S_i} * \text{depth}(S_i)$$



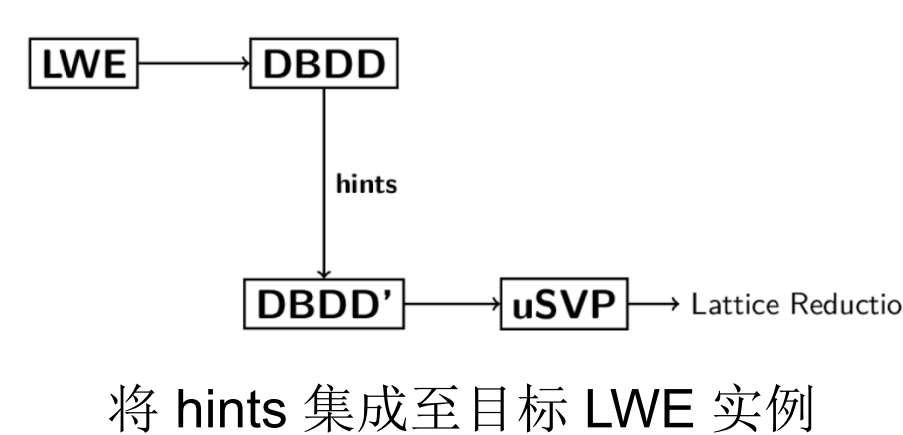
针对 Kyber768 的密钥恢复树

格基约减

依据密钥恢复规则, 将消息的后验概率转换为私钥系数的后验概率

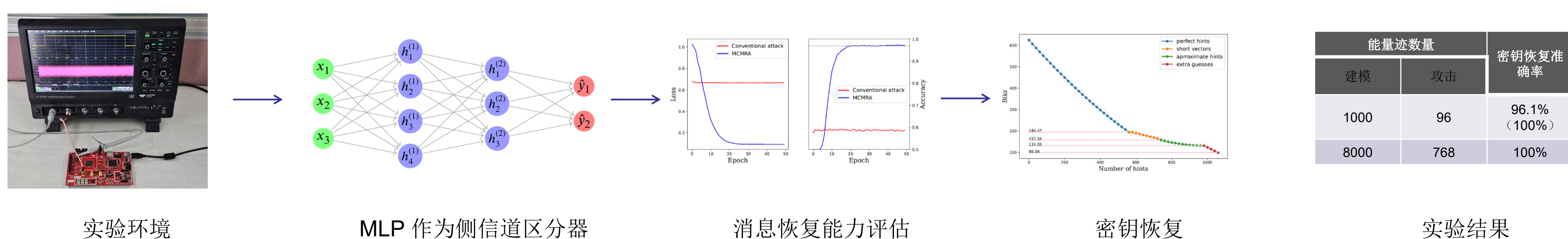
$$P[s_i = \hat{s}|T] = \prod_{l=0}^{Q-1} P[m_{l,i} = \hat{m}_l | T_l = t_l].$$

随后将后验概率作为 hints 集成到目标 LWE 实例中, 降低其求解难度, 进而通过格基约减直接恢复密钥。



将 hints 集成至目标 LWE 实例

攻击结果与防护策略



| 能量流数量 | | 密钥恢复准确率 |
|-------|-----|--------------|
| 建模 | 攻击 | |
| 1000 | 96 | 96.1% (100%) |
| 8000 | 768 | 100% |

为防范该攻击, 可从以下角度设计防护策略: 1) 针对该攻击依赖于结构化密文的特点, 设计恶意密文检测策略; 2) 设计掩码方案, 通过将中间值划分为掩码分量, 打破该攻击构造的特定消息结构; 3) 通过时钟随机化等技术进一步降低信噪比。