

密码旁路分析原理与方法

2014年5月

提纲

- 1 为什么研究？密码旁路分析研究背景
- 2 现状怎么样？国内外研究现状及分析
- 3 攻击怎么干？典型攻击原理与实例分析
- 4 未来怎么走？未来研究热点分析与展望
- 5 我们怎么办？总结与建议

信息时代中，密码是确保信息安全的核心和基础。

计算机



通信



“信息时代”



信息安全

密码学

公钥密码

分组密码

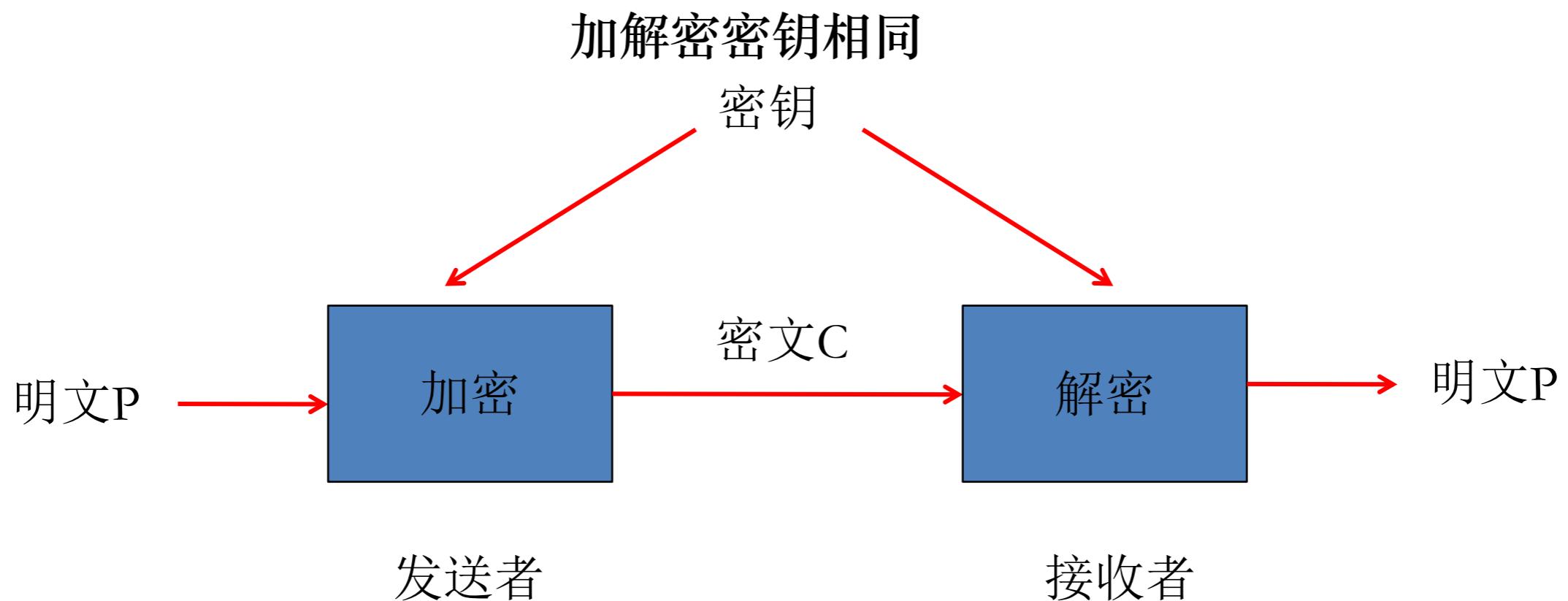
序列密码

哈希函数

...

对称密码体制

源于Shannon于1949年发表的论文《保密系统的通信理论》，根据加密方式不同可分为序列密码算法和分组密码算法两种。密钥管理复杂，对于n个用户的计算机网络通信需管理 $n(n-1)/2$ 种不同的密钥。

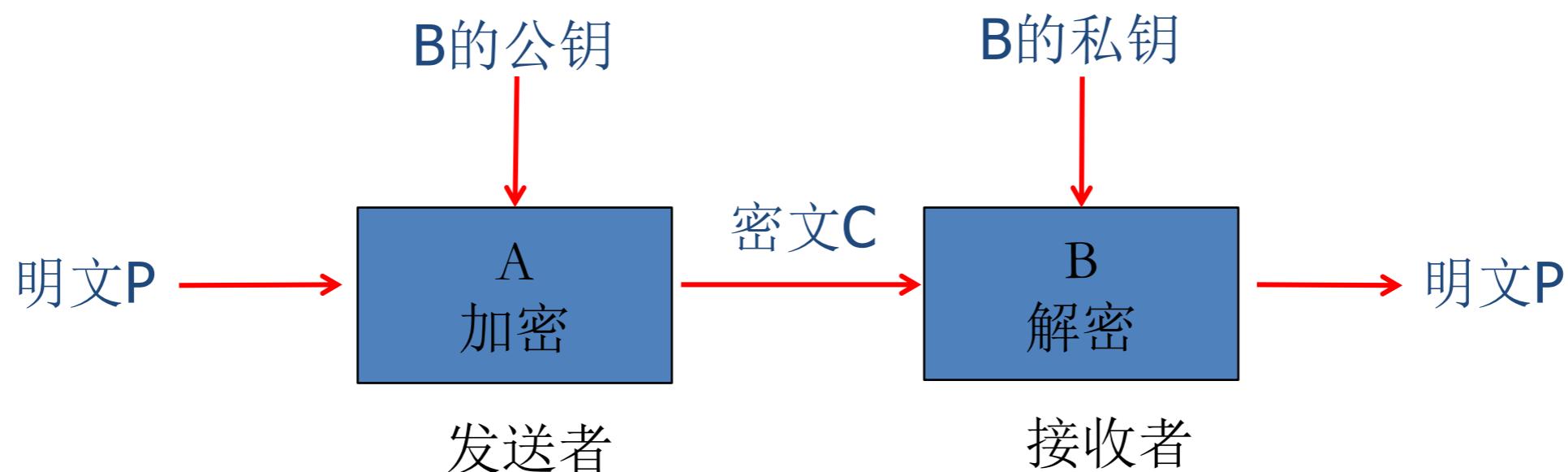


通过多轮迭代混淆（线性变换+非线性变换）确保安全性

非对称（公开）密码体制

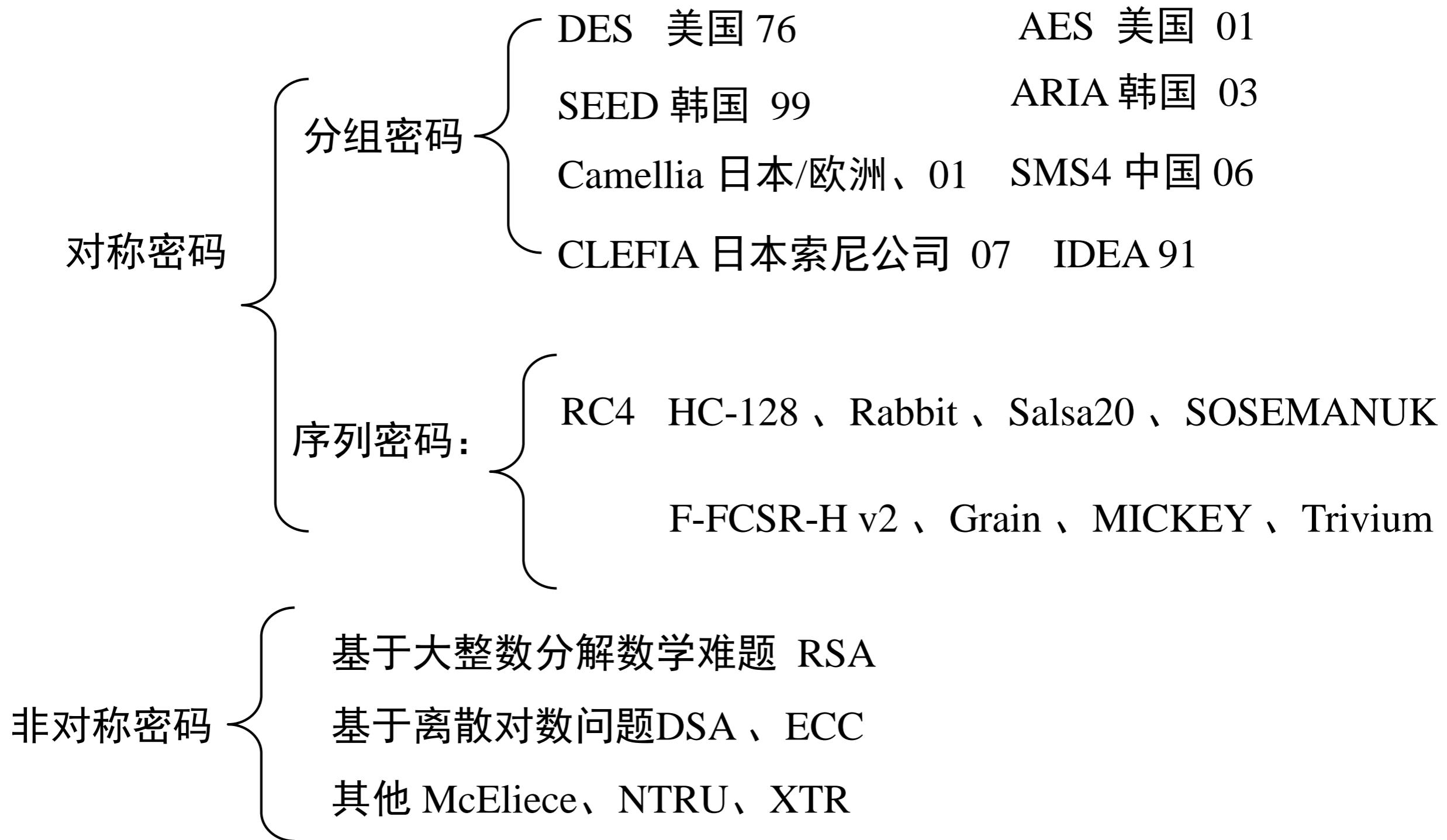
源于Diffie和Hellman于1976年发表的论文《密码编码学新方向》，使得使用不同密钥进行加解密成为可能，解决了在发送者和接收者之间无密钥传输的难题，开创了公钥密码学的新纪元。

加解密密钥不同

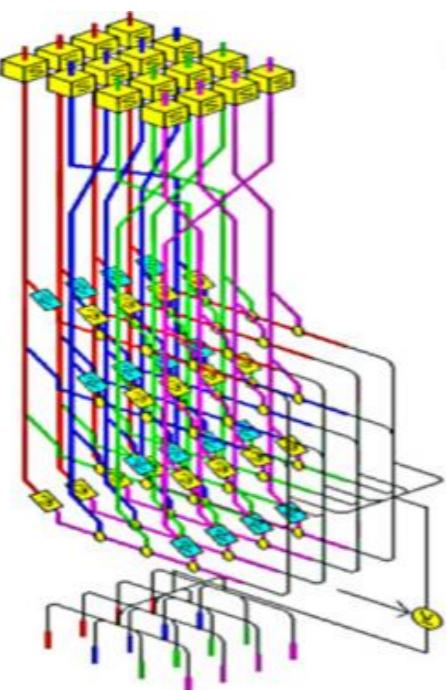


通过数学问题求解的计算复杂性确保安全性

典型密码算法



传统密码分析方法



针对算法的设计安全性进行分析

传统密码分析

强力攻击

穷举攻击

字典攻击

折中攻击

数学分析

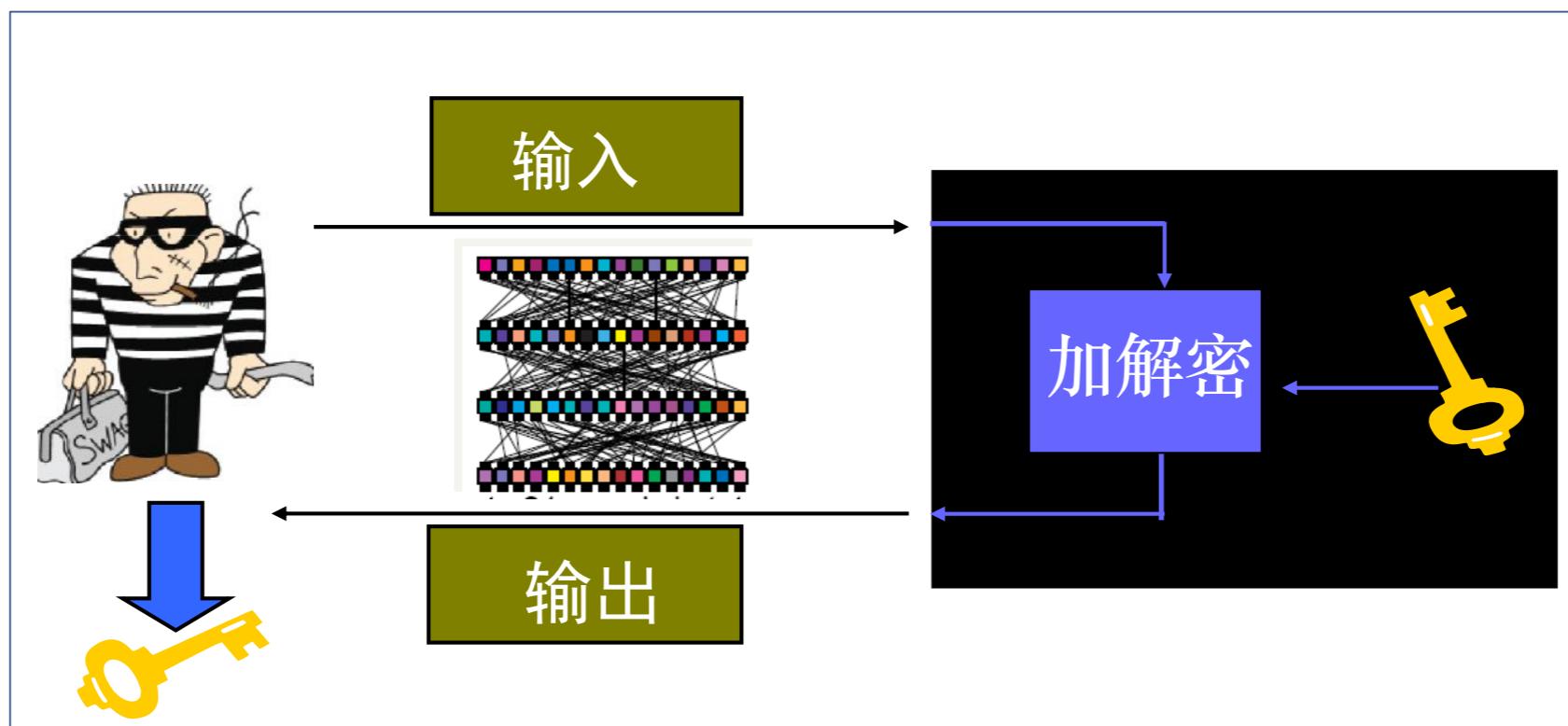
差分分析

线性分析

相关分析

代数分析

传统密码分析方法



攻击者只能获取密码系统输入和输出

传统密码分析方法

密钥作为一个整体进行穷举



00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

FF FF

2128

密码强力攻击



由FPGA阵列组成的密码分析机COPACOBANA, DES破译需要8.7天
AES? ? ? ? ? ?

密码强力攻击



EPFL: 用于攻击ECCp-112的机器阵列，200台，3.5月破解

密码分析芯片

密码强力攻击

RSA-768, 2009年12月9日历时两年被分解， RSA 1024仍较为安全！

n=:

12301866845301177551304949583849627207728535695953347921973224521517264005
07263657518745202199786469389956474942774063845925192557326303453731548268
50791702612214291346167042921431160222124047927473779408066535141959745985
6902143413.

=

3347807169895689878604416984821269081770479498371376856891
2431388982883793878002287614711652531743087737814467999489

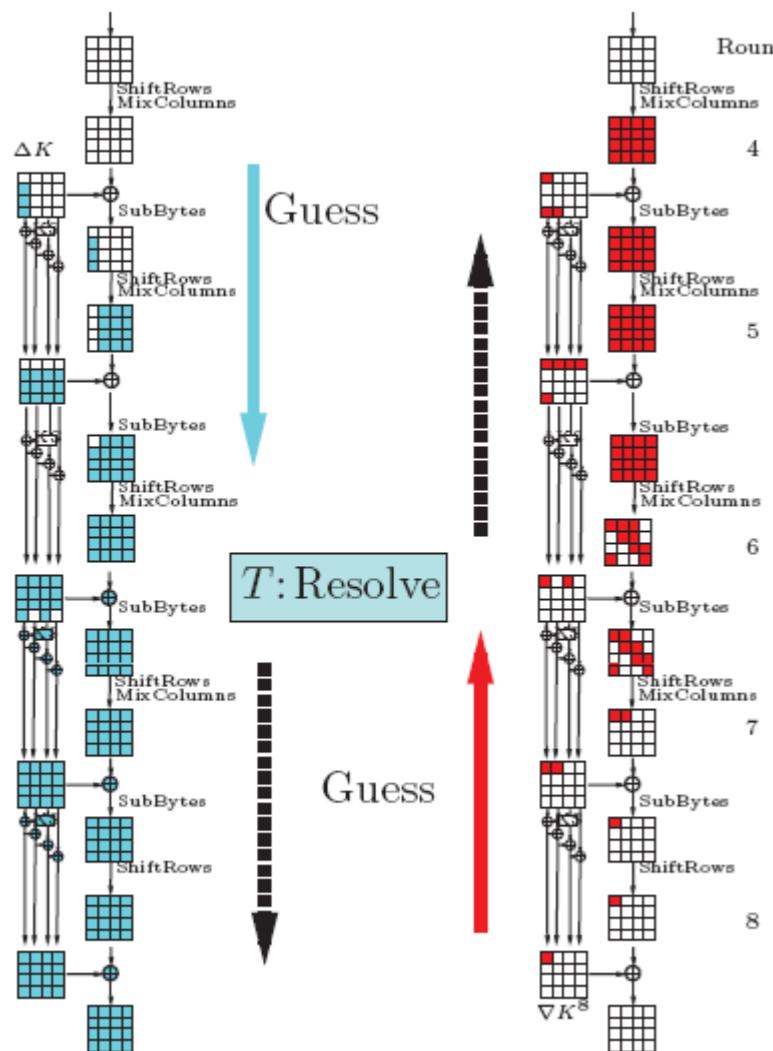
*

3674604366679959042824463379962795263227915816434308764267
6032283815739666511279233373417143396810270092798736308917

密码数学分析

评估密码算法理论上可提供的密钥安全性？

AES密码Biclique分析



评估密码算法理论上可提供的密钥安全性？

AES-128, 实际密钥安全性 126.1位

AES-192, 实际密钥安全性 189.7位

AES-256, 实际密钥安全性 254.4位



随着密码设计水平的提高，传统密码分析方法已经难以对密钥安全性构成现实威胁！

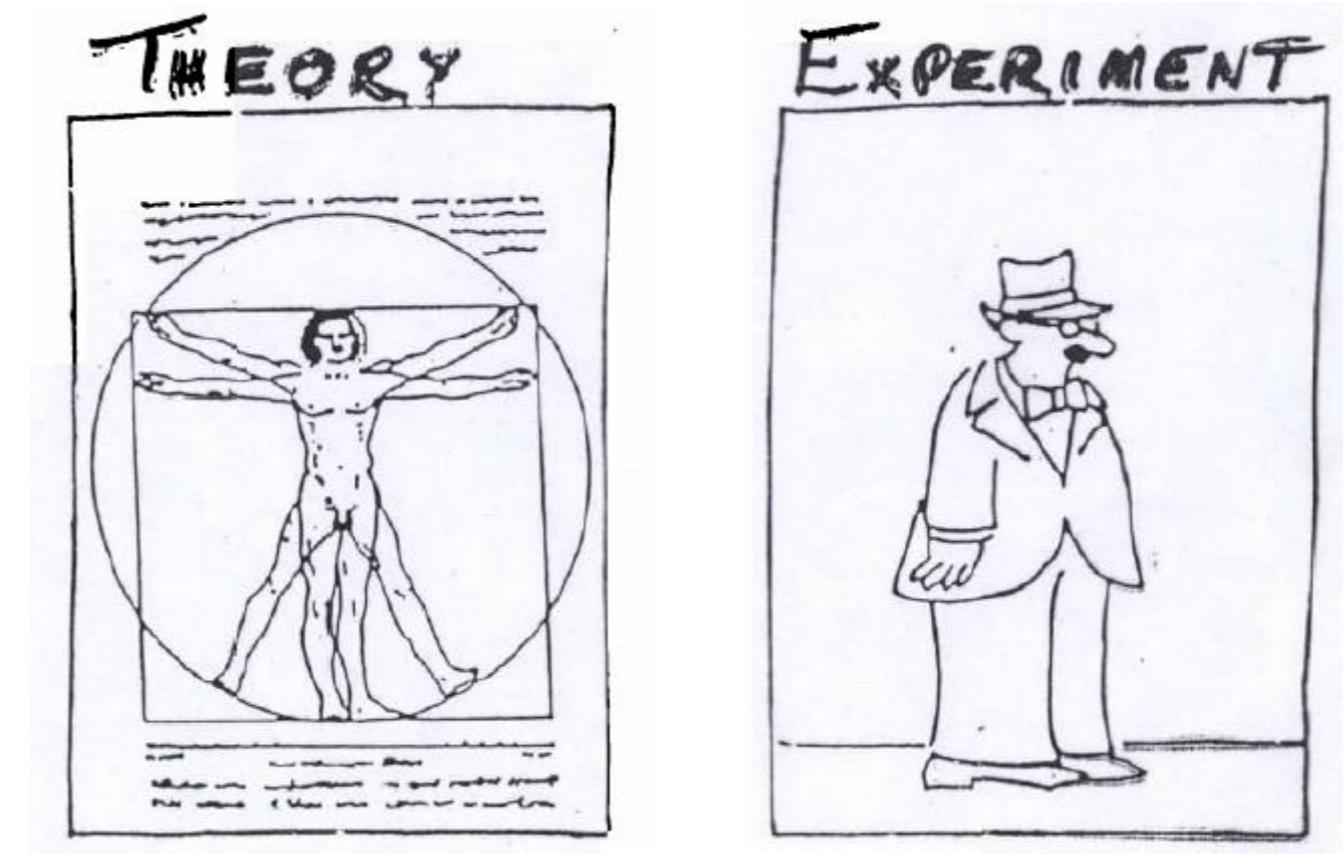


攻击者就缴械了吗？

密码安全遵循木桶效应

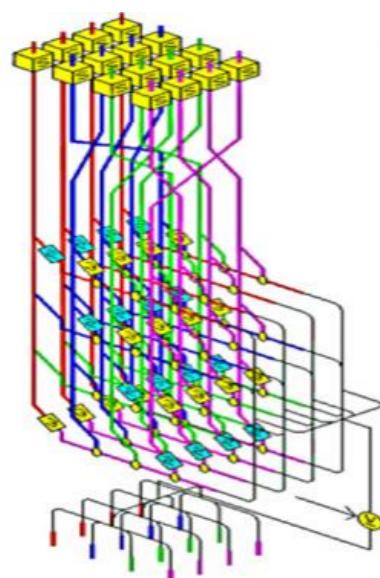


理论安全 不等价于 实际安全

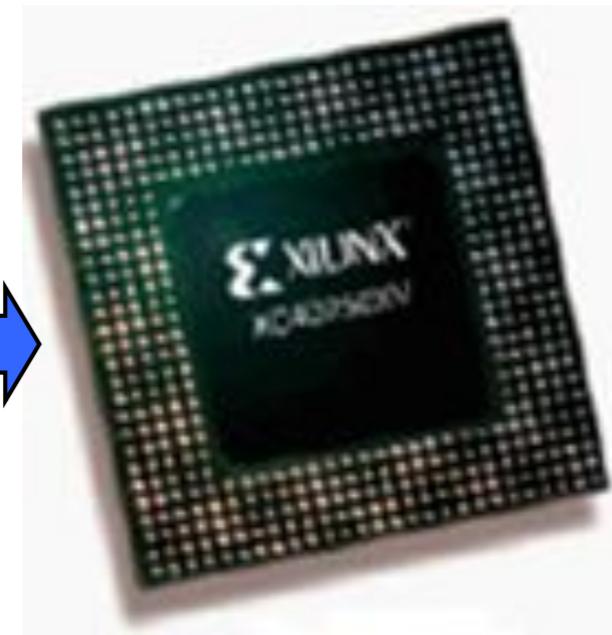


攻击者的能力远比理论模型要强大

- 1、任何密码算法都需依赖物理平台实现
- 2、密码算法设计安全不等价于实现安全
- 3、基于密码芯片实现安全性的密钥分析？



密码算法



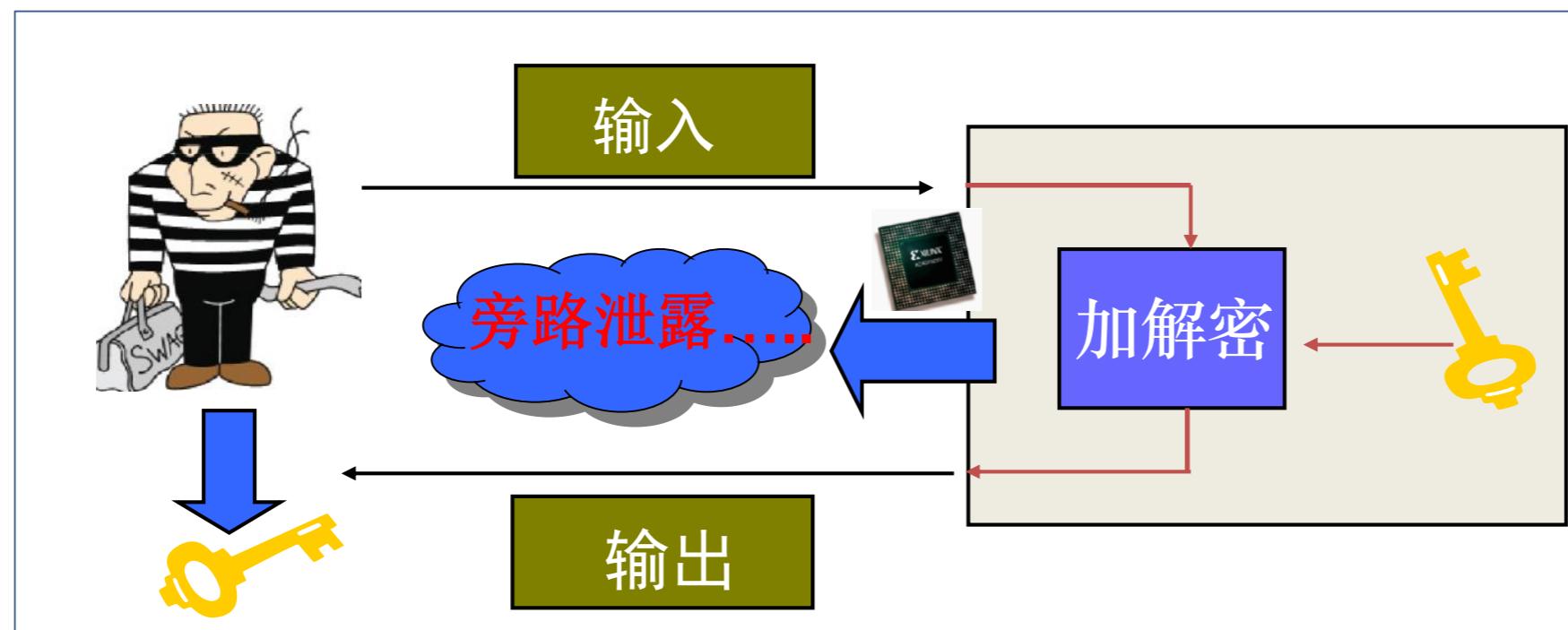
密码芯片



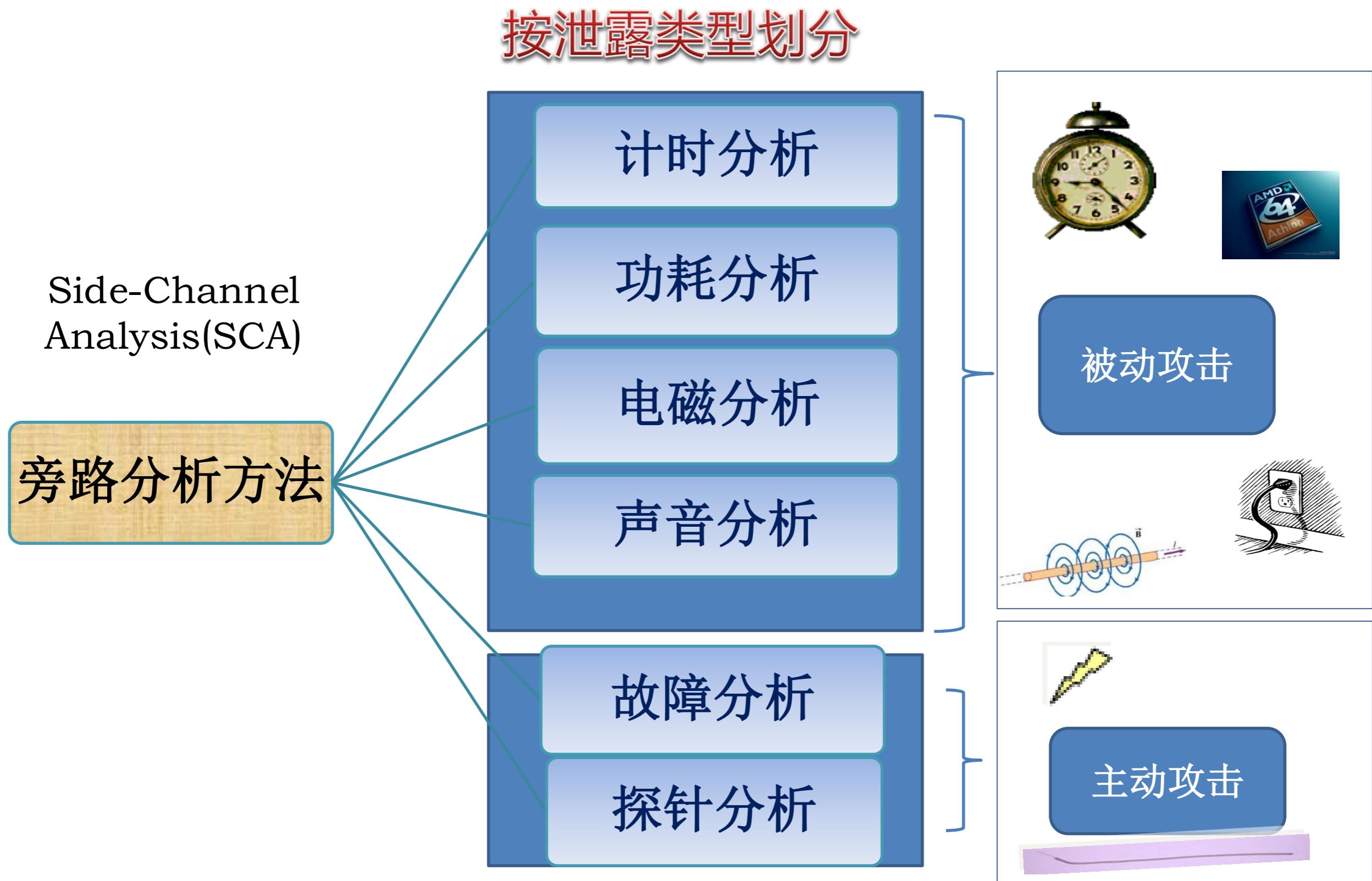
密码旁路分析方法

密码旁路分析方法

攻击者可利用除了输入、输出以外的第三类信息：旁路泄露
旁路泄露是密码运行中间状态的直接反映，可用于密钥破解

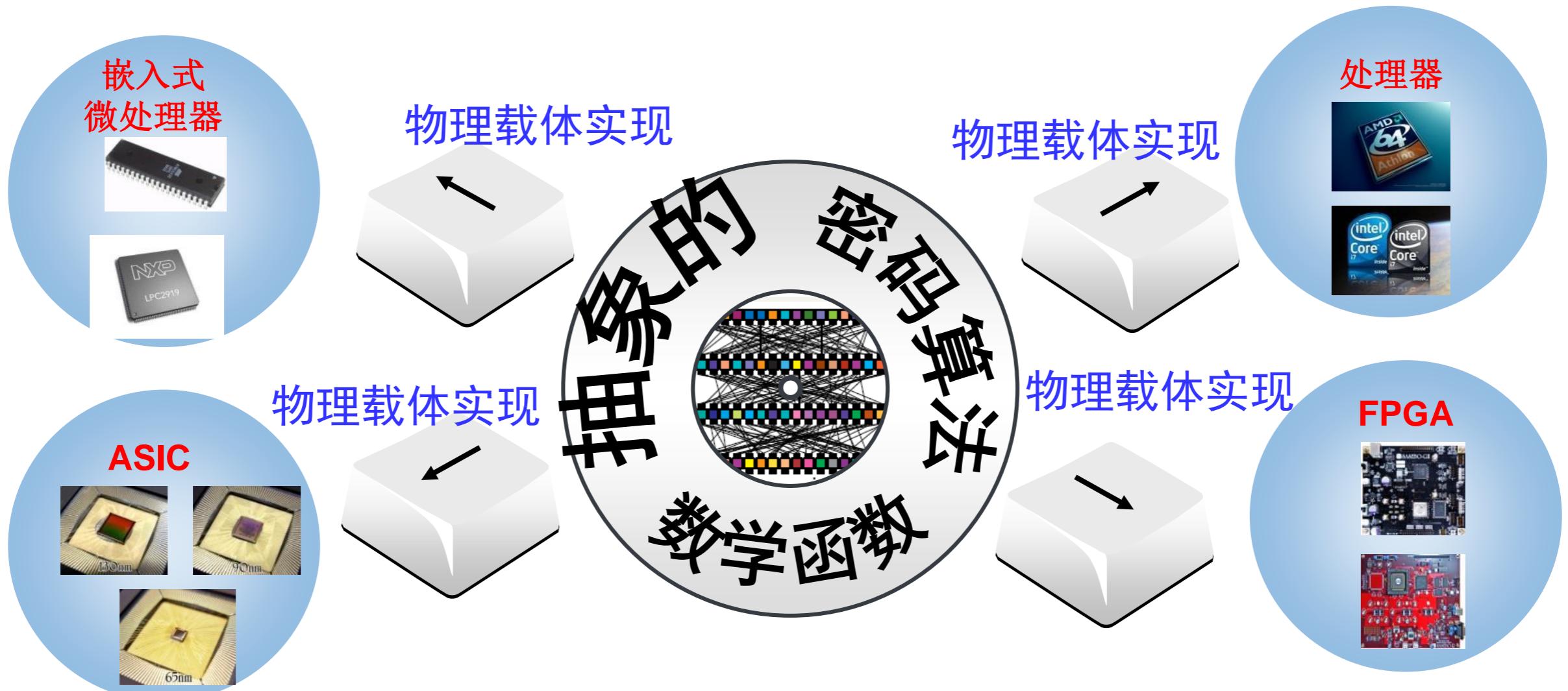


旁路分析是一种利用密码执行的时间、功耗、电磁辐射、故障输出等物理特征泄露，结合输入和输出进行秘密信息分析的一种方法。



密码旁路分析原理：密钥分而治之

1、任何密码算法都要依附一个载体平台，即密码芯片来运行；



密码旁路分析原理：密钥分而治之

2、密码算法在密码芯片上实现时，总会产生旁路泄露；



密码 芯片 实现	微控制器	微处理器	处理器	FPGA	ASIC

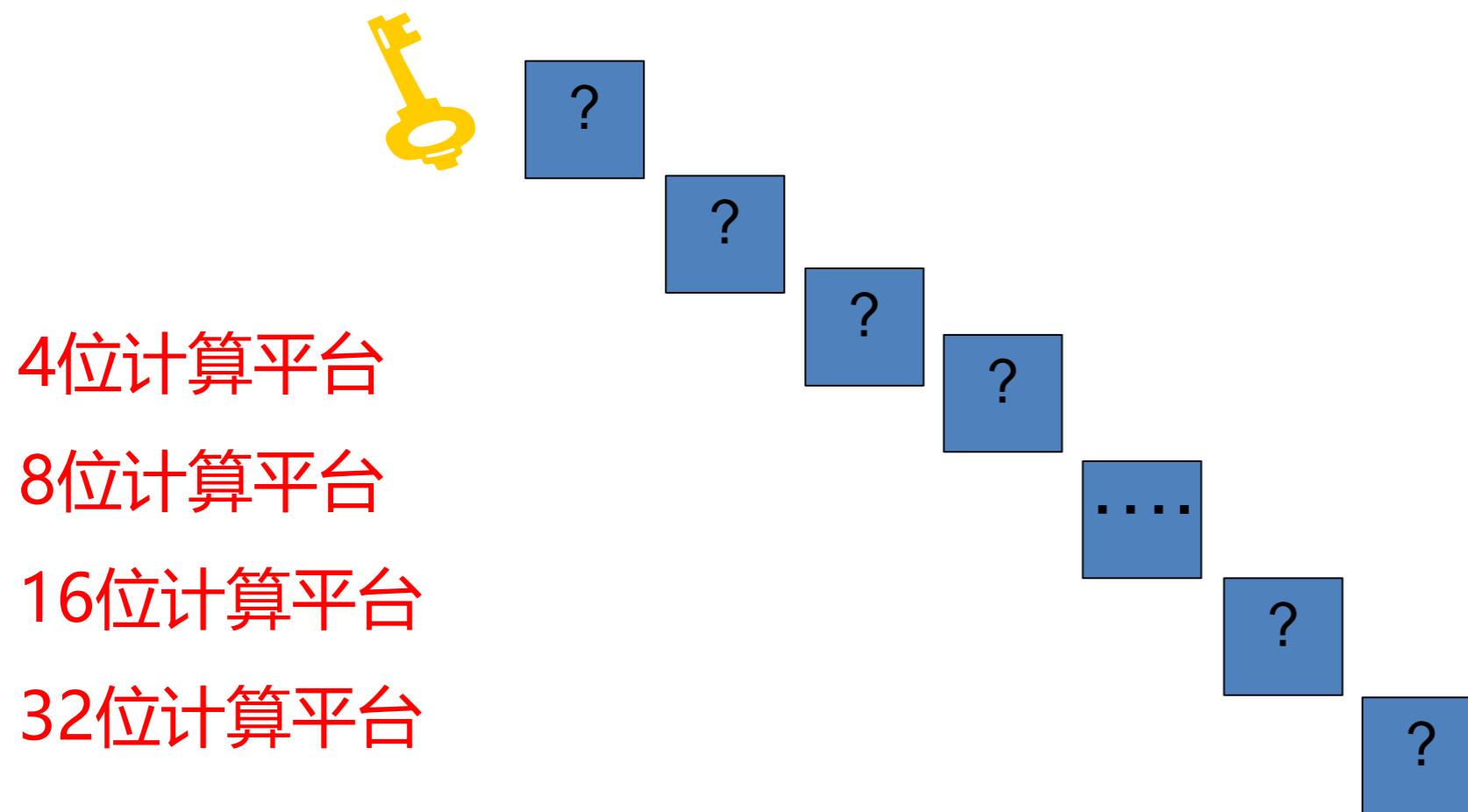
(1) 门电路翻转状态变换需要运动；

0 → 1 (2) 运动过程中会产生能量消耗；

1 → 0 (3) 能量又可转化为电压、电流、电磁辐射、声音等瞬时旁路泄露；同时又可转化为时间等累积旁路泄露。

密码旁路分析原理：密钥分而治之

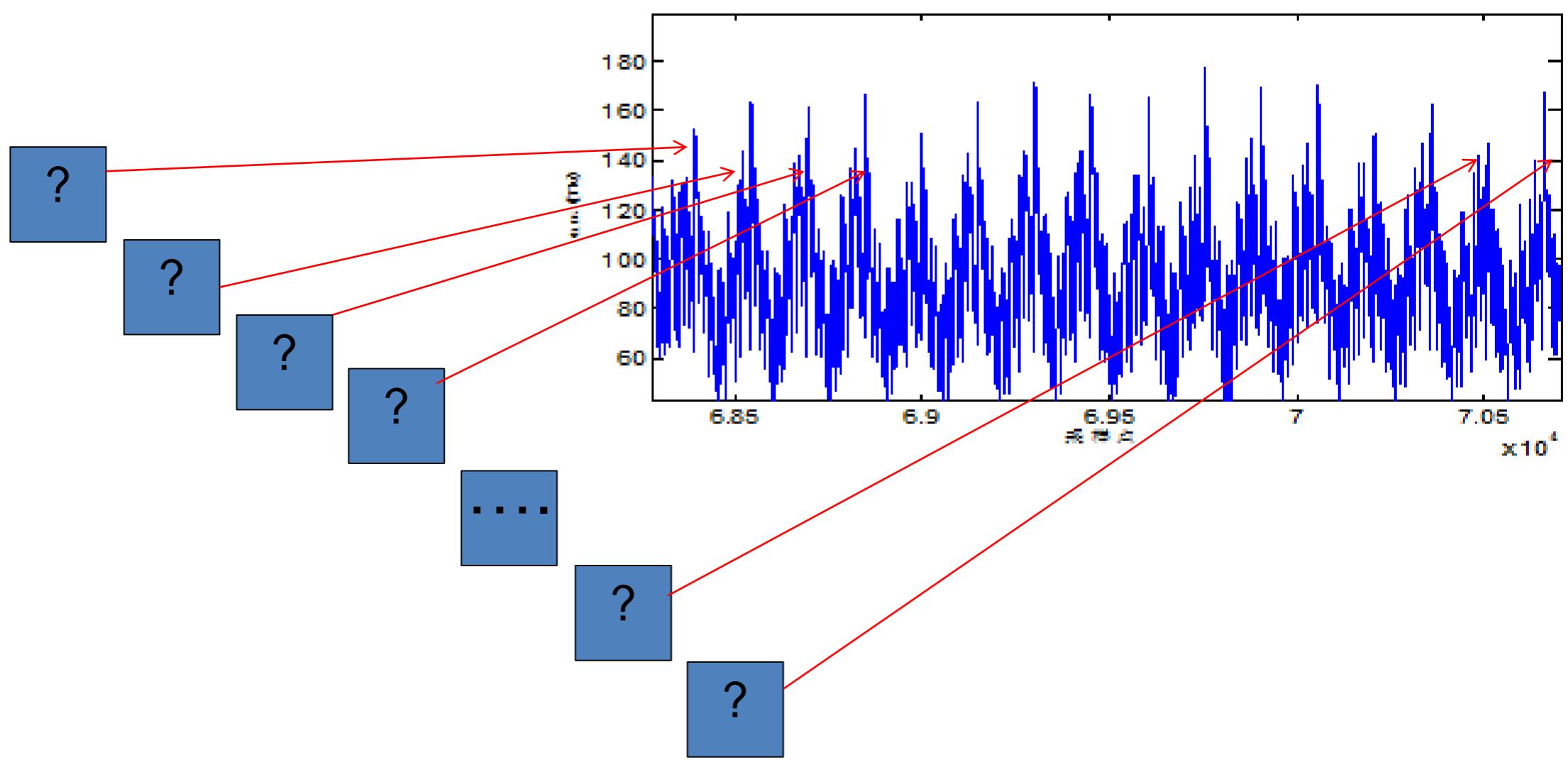
3、受计算资源和处理能力限制，密码芯片处理密钥时大都切割为若干密钥片段分开参与运算；



密码旁路分析原理：密钥分而治之

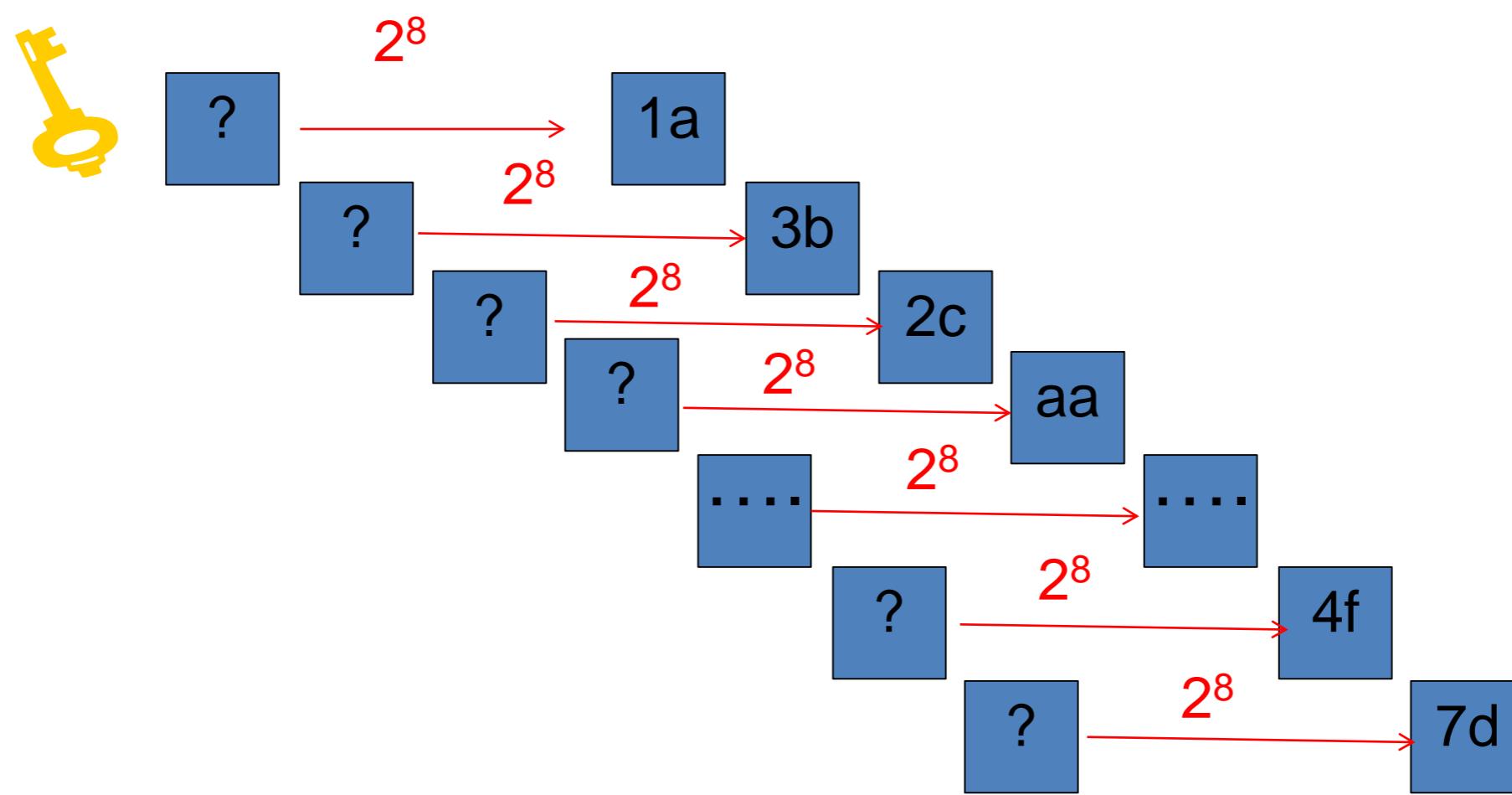
4、不同时机处理这些密钥片段的旁路泄露可被攻击者采集到；

以功耗为例



密码旁路分析原理：密钥分而治之

5、攻击者通过分析每段旁路泄露同密钥片段的相关性，穷举这些密钥片段的有限候选值，利用一定的分析方法恢复出密钥片段值；



密码旁路分析原理：密钥分而治之

6、恢复出足够的密钥片段，结合密钥扩展设计恢复完整密钥。



1a	3b	2c	aa	34	4f	8a	3d	dd	ac	4a	1d	de	2f	4f	7d
----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

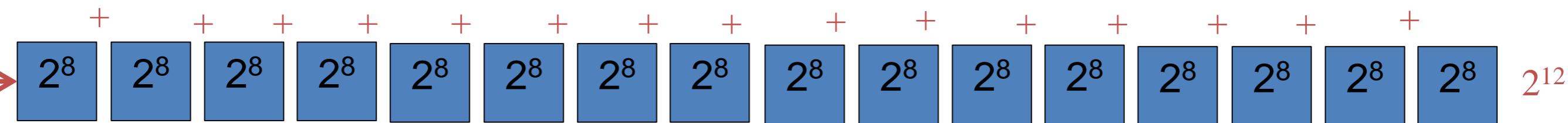
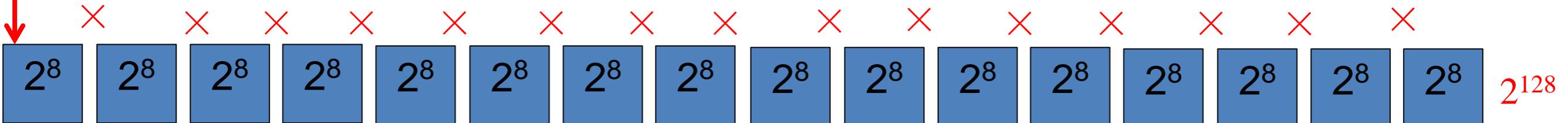
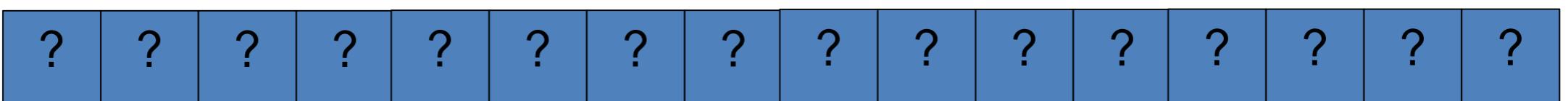
密钥穷举复杂度分析

密钥长度 m 比特，切割为 n 个密钥片段，每次处理一个片段（ l 比特）；

传统密码分析的密钥穷举复杂度为 $2^l \times 2^l \times \dots \times 2^l = 2^m$ (n 个 2^l 相乘)

密码旁路分析的密钥穷举复杂度为 $2^l + 2^l + \dots + 2^l = 2^l \times n$ (n 个 2^l 相加)

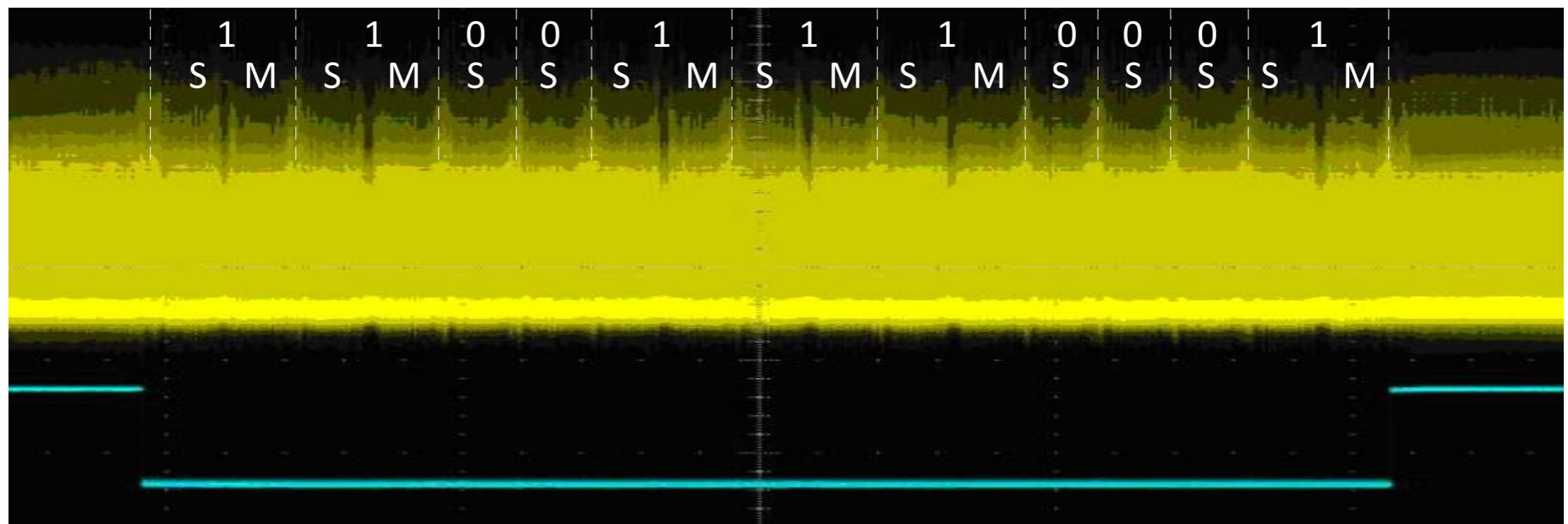
AES-128



旁路分析复杂度实现了灵巧降维，现实威胁更大！

1024位密钥按位“分而治之”，拼接恢复主密钥！

RSA
功耗
分析
示例

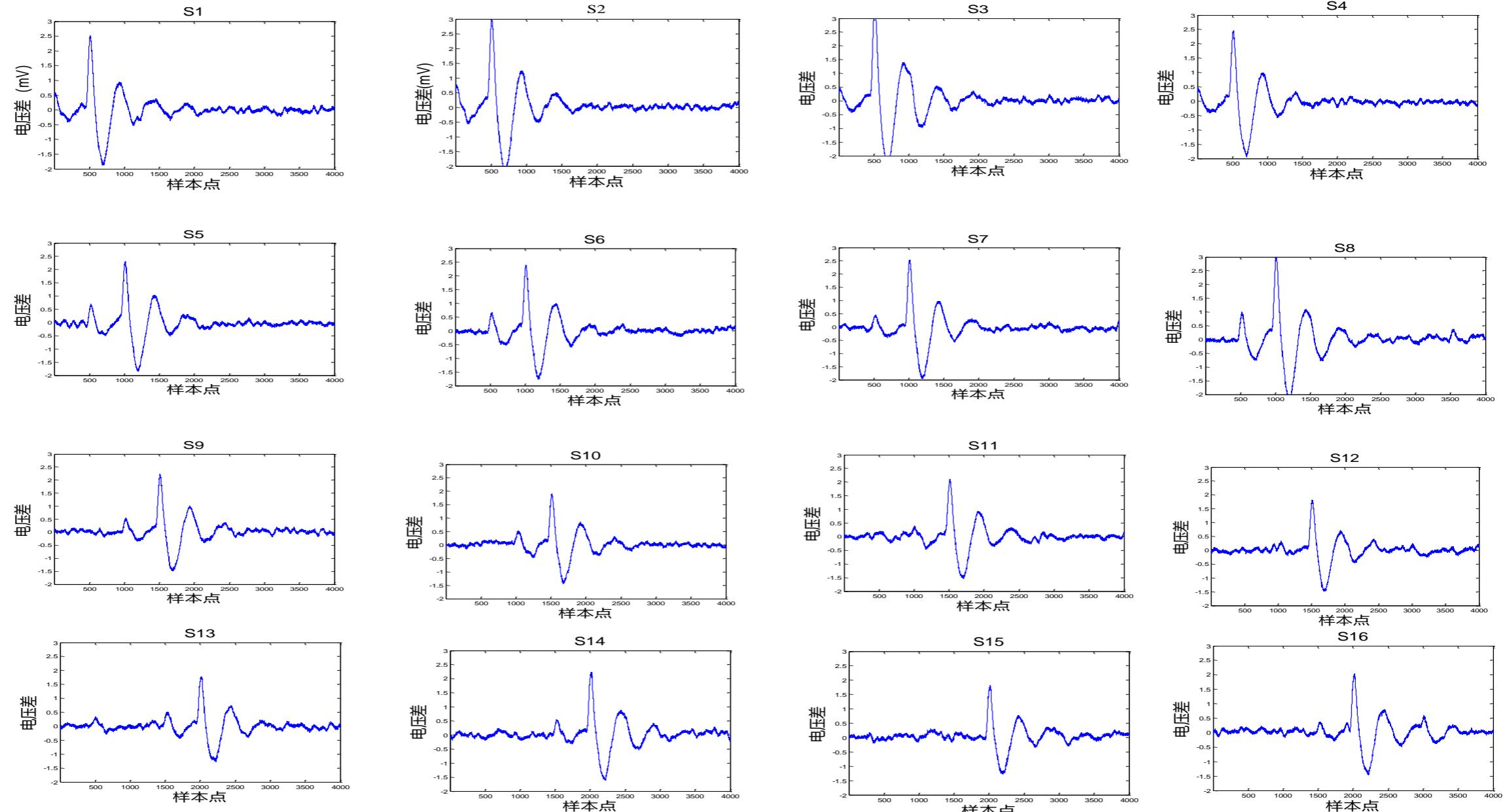


1条功耗曲线分析，根据密钥位为0和1的功耗差异，可直接读取所有密钥位

密钥穷举复杂度： $2^{1024} \rightarrow 2^1 \times 1024 = 2^{11}$

128位密钥按字节“分而治之”，拼接恢复主密钥！

AES
功耗
分析
示例



100条功耗曲线分析，正确密钥字节猜测分析曲线会出现峰值

密钥穷举复杂度： $2^{128} \rightarrow 2^8 \times 16 = 2^{12}$

发展动因分析

■ 攻击对象

- 设计安全性 ≠ 实现安全性
- 密码运行总会产生泄露
- 旁路泄露同密码运算相关

■ 攻击者

- 既能采集无意泄露
- 又能主动诱导泄露
- 还可参与密码体制

■ 测试计量手段

- 支持采集新型旁路泄露
- 泄露采集精度大大提高
- 泄露采集速度大大加快

■ 密码产业发展

- 密码算法的标准化
- 密码算法设计公开化
- 密码芯片安全产业需求

旁路分析技术提出绝非偶然，是密码分析学发展的必然结果！

提纲

1

为什么研究？密码旁路分析研究背景

2

现状怎么样？国内外研究现状及分析

3

攻击怎么干？典型攻击原理与实例分析

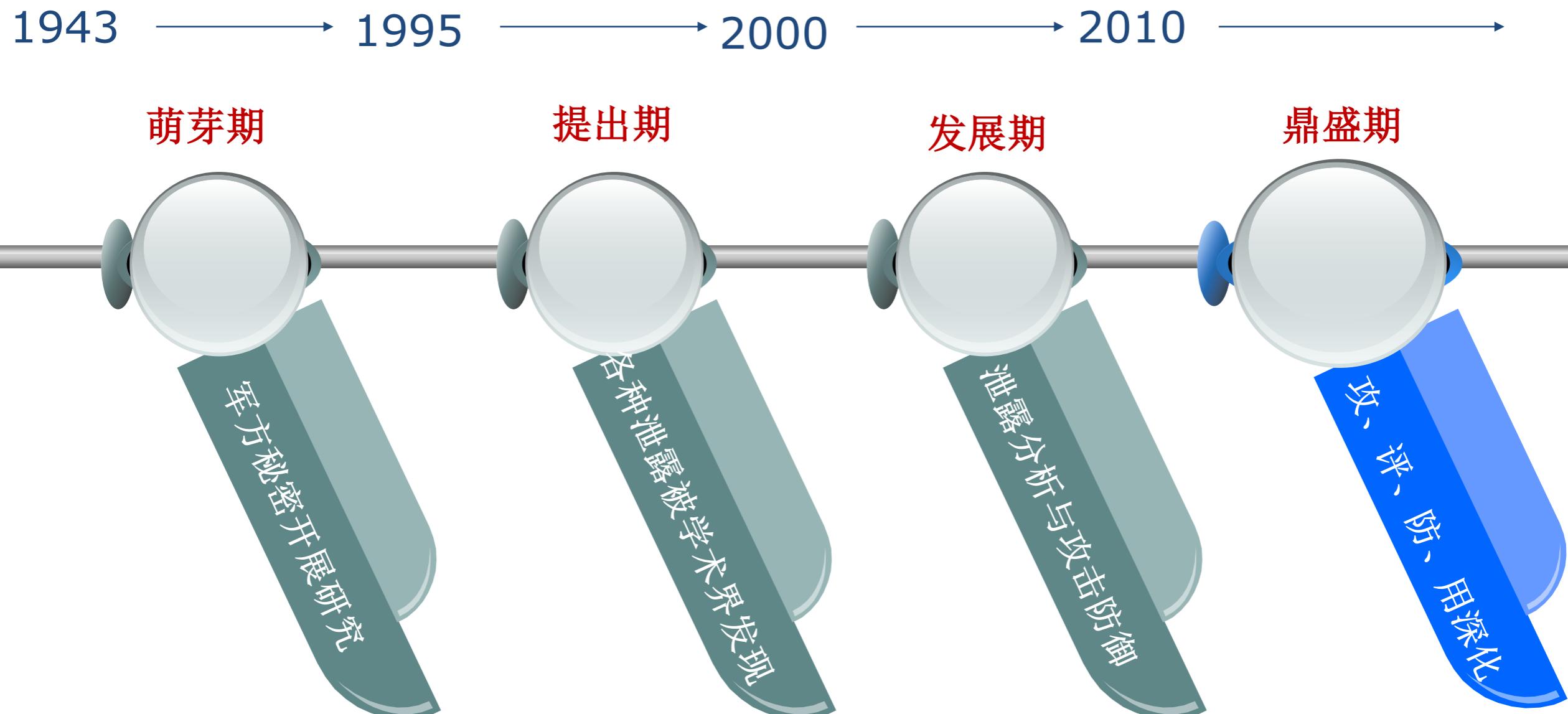
4

未来怎么走？未来研究热点分析与展望

5

我们怎么办？总结与建议

2.1 发展历程



2.1 发展历程

萌芽期：军方率先发现电子设备运行旁路泄露问题，并秘密开展研究

（1）瞬态电磁脉冲辐射监测技术研究

早在1943年，美国军方在调试加密电传终端（贝尔电话131-B2）时，就发现电子设备的杂散电磁脉冲辐射会导致敏感信息泄露，并认为这将成为信息对抗的新领域，展开了瞬态电磁脉冲辐射监测技术（Transient Electromagnetic Pulse Emanation Surveillance Technology: TEMPEST）研究。



Bell 131-B2

1960年，英国情报人员在英国加入欧共体的谈判中也发现了泄漏发射问题。德国、加拿大、荷兰、澳大利亚等国也逐渐认识到这一问题，相继投入研究，但都是秘密进行的。

TEMPEST研究直至1995年才被美国正式解密。

2.1 发展历程

萌芽期：军方率先发现电子设备运行旁路泄露问题，并秘密开展研究

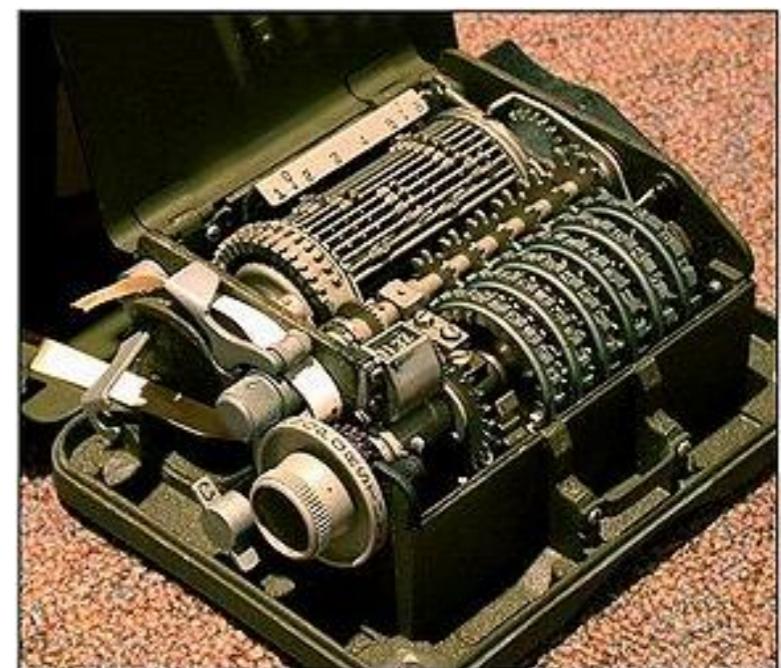
(2) 声音分析技术研究

1956年，英国情报部门军情五处特工Peter Wright利用声音分析手段，执行了代号为“咽吞”的计划，将监听器放至埃及驻伦敦大使馆Hagelin密码机旁边的电话机中，通过秘密监听密码机齿轮滚动的咔喀声，成功破译了当时埃及驻伦敦大使馆所用的密钥。通过执行“咽吞”计划，英国在整个苏伊士运河危机时期得到了埃及方面的大部分情报。

Peter
Wright



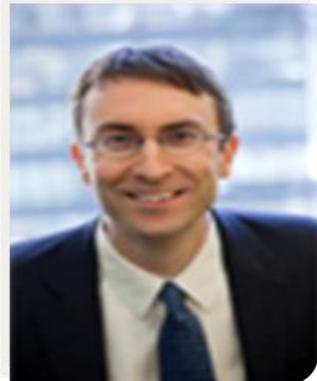
Hagelin
M-209



2.1 发展历程

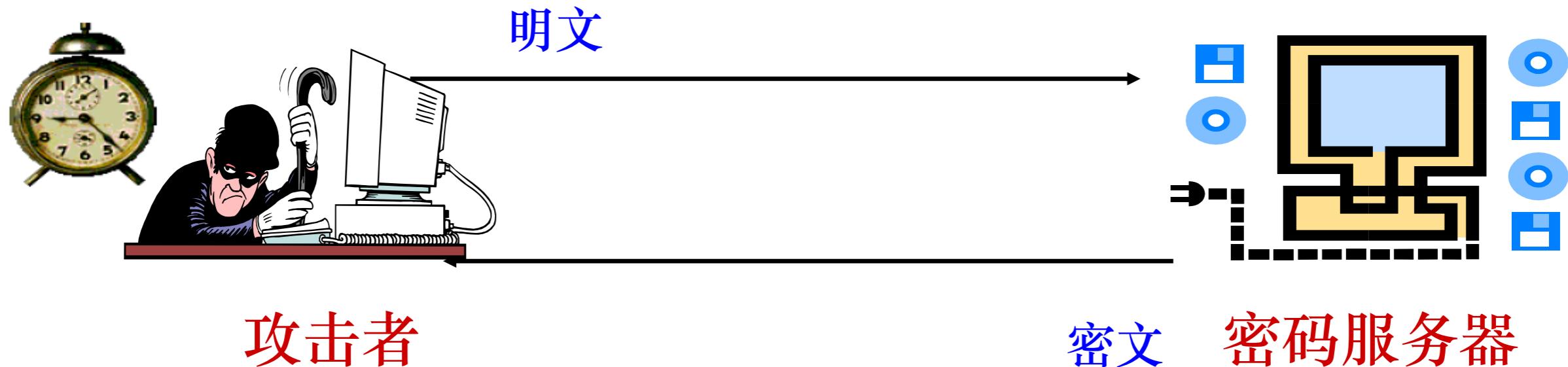
提出期：不同类型的旁路泄露被学术界陆续发现并用于密钥分析

(1) 时间旁路泄露1996年被发现



P. Kocher

Cryptography Research公司总裁兼首席科学家，率先提出旁路分析的思想，并利用计时分析方法对RSA密钥进行了分析。



2.1 发展历程

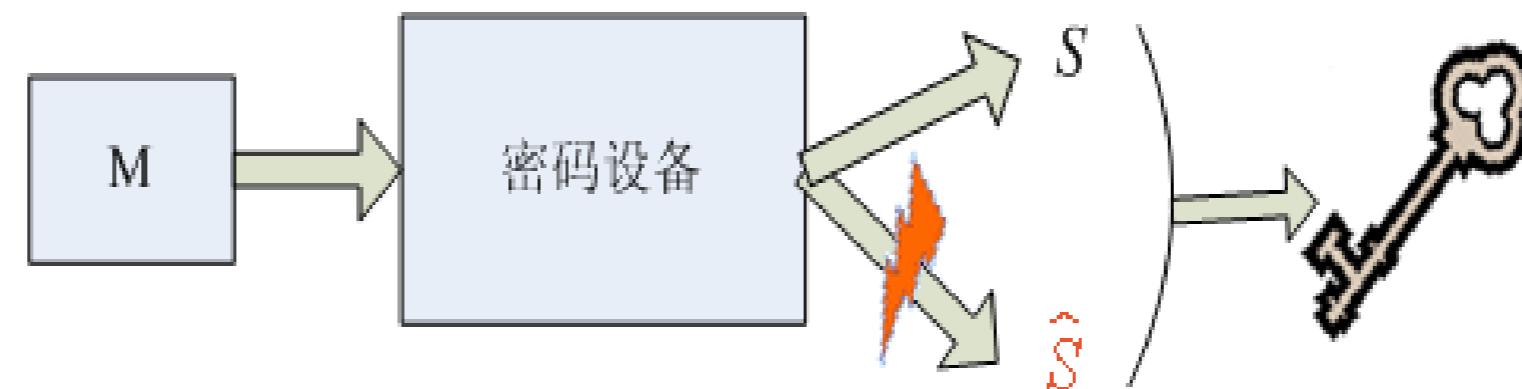
提出期：不同类型的旁路泄露被学术界陆续发现并用于密钥分析

(2) 故障泄露1997年被发现



D. Bone

美国斯坦福大学的教授，发现智能卡上密码算法执行过程可能会受到干扰产生故障（或错误）输出用于密钥恢复，成功对RSA密码算法进行了故障分析。



2.1 发展历程

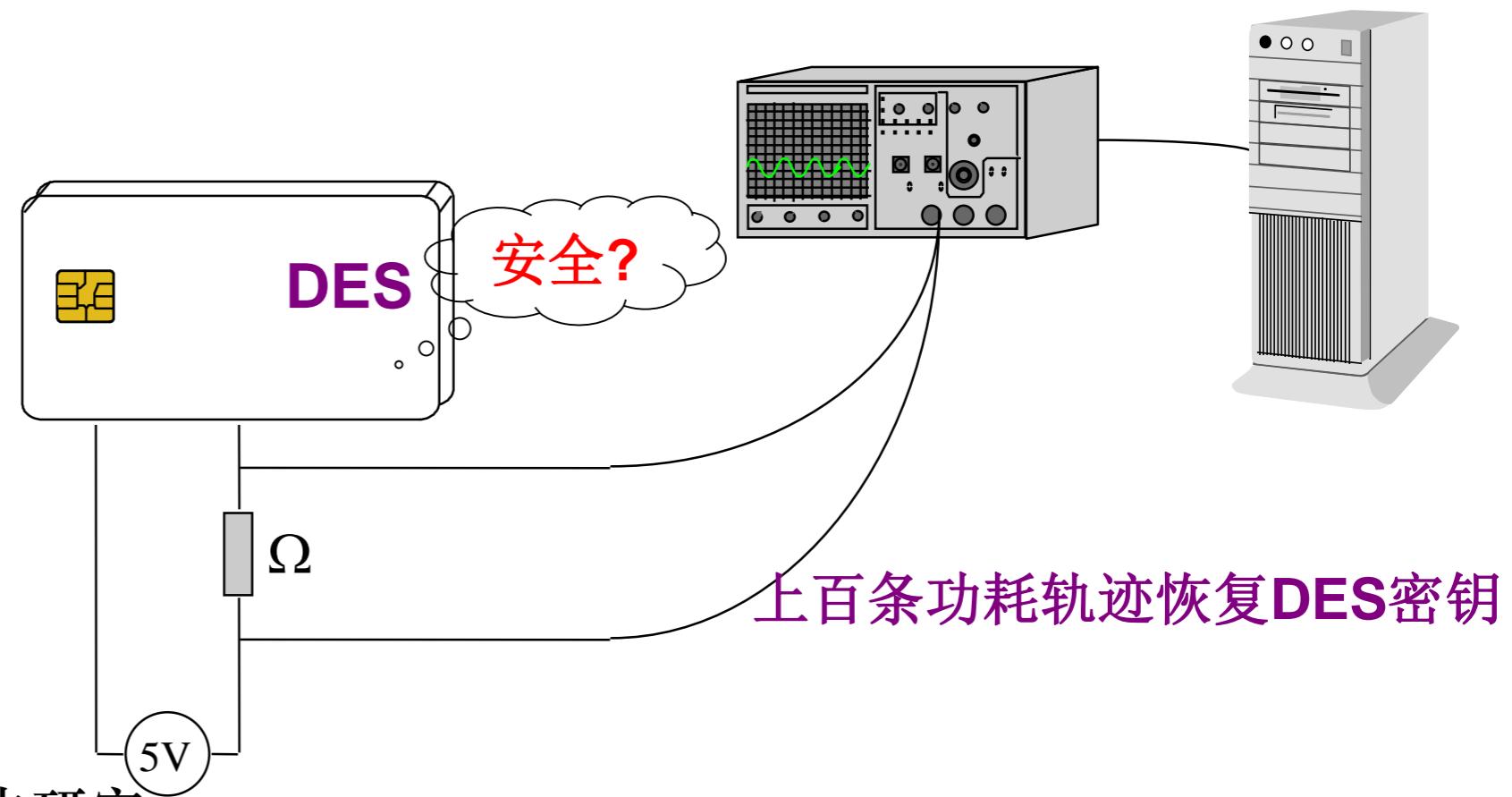
提出期：不同类型的旁路泄露被学术界陆续发现并用于密钥分析

(3) 功耗旁路泄露1998年被发现

发现智能卡中DES运行存在功耗泄露，
对DES进行了密钥恢复。



P. Kocher



2009年，P. Kocher因对旁路攻击研究
的杰出贡献，被评为美国工程院院士。

2.1 发展历程

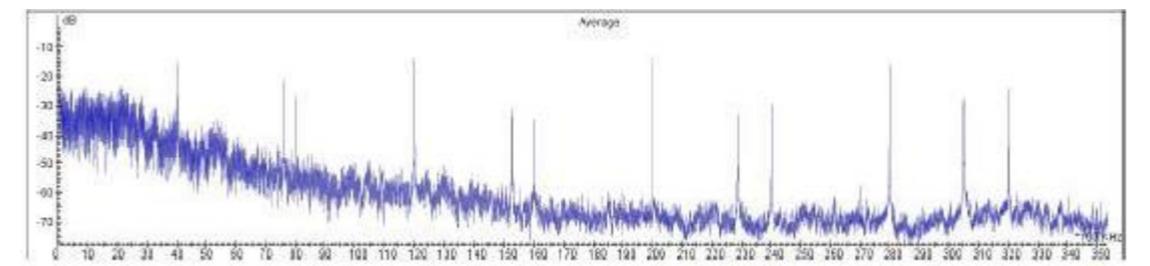
提出期：不同类型的旁路泄露被学术界陆续发现并用于密钥分析

(4) 电磁旁路泄露2000年被发现



J. Quisquater

发现电磁泄露也可用于密钥恢复，分析方法同功耗分析类似。



2.1 发展历程

发展期：各种旁路分析方法蓬勃发展，旁路分析评估、防御及应用得到重视

时间	旁路分析研究进展
2001	高阶差分功耗分析方法被提出
2002	Cache访问特征旁路泄露被发现
2003	模板分析方法、多道旁路分析方法、碰撞旁路分析方法被提出
2004	声音旁路泄露被发现、相关功耗分析方法被提出
2005	随机模型分析方法、频域旁路分析方法、访问驱动Cache计时分析方法被提出
2006	基于旁路的智能卡代码逆向方法被提出
2007	欧洲学者撰写的第一本功耗旁路分析书籍公开出版
2008	欧洲和日本联合举办的旁路分析竞赛DPAContest开始，互信息分析方法、旁路立方体分析方法被提出
2009	旁路分析评估框架被首次提出，硬件木马旁路分析方法、代数旁路分析方法、代数故障分析方法被提出
2010	通用的旁路分析模型和方法研究成为研究热点，光子旁路分析方法、旁路水印方法、故障灵敏度分析方法、相关性碰撞分析方法被提出

2.1 发展历程

鼎盛期：旁路分析、评估、防御、应用研究将更加深化

■旁路信息采集

- 采集泄露类型更多
- 泄露采集速度更快
- 泄露采集精度更高

■旁路分析方法

- 防御的密码攻击
- 现有分析方法优化
- 新型分析方法提出

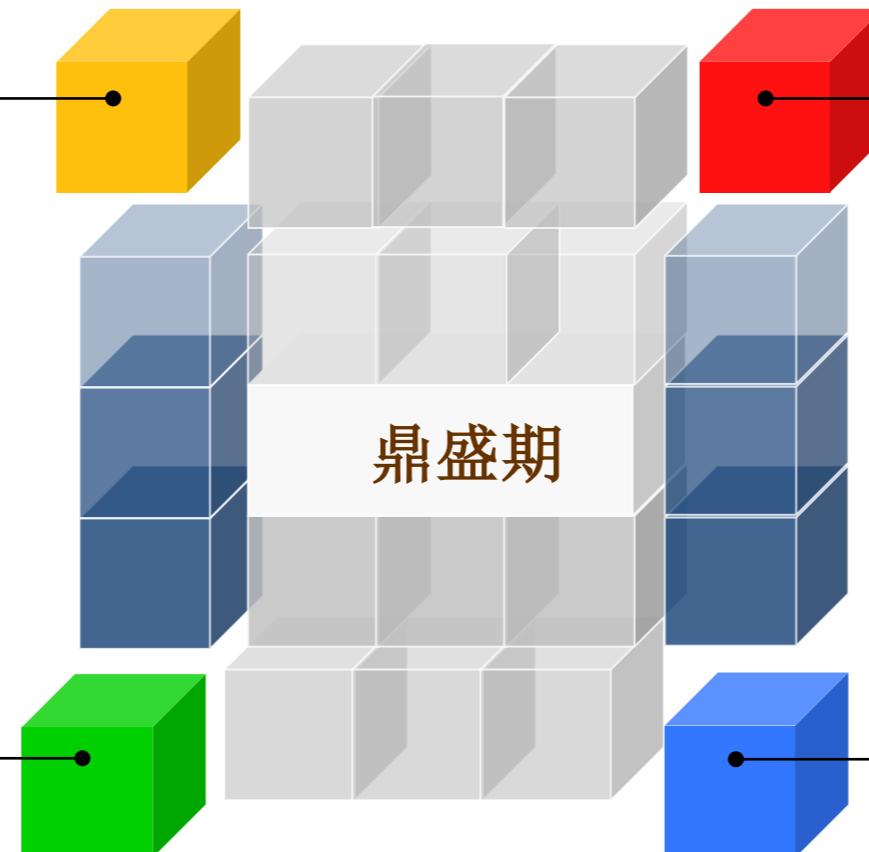
鼎盛期

■旁路分析防御

- 设计方式科学化
- 实现方法灵活化
- 部署应用体系化

■旁路分析应用

- 分析应用通用化
- 分析应用广泛化
- 分析应用交叉化



2.2 各国发展现状

美国

不论是早期的TEMPEST研究、1976年DES分组密码、1977年RSA公钥密码、1992年SHA杂凑算法、1997年AES分组密码、2008年SHA-3杂凑算法征集，还是密码实现攻击研究，美国一直是密码学领域的主导者。

计时攻击、功耗攻击均为美国人Kocher首次提出，声音攻击则由斯坦福大学MIT实验室教授Adi Shamir和学生Eran Tromer提出，此后，美国许多密码研究机构在此基础上进行了进一步的深入研究。

2.2 各国发展现状

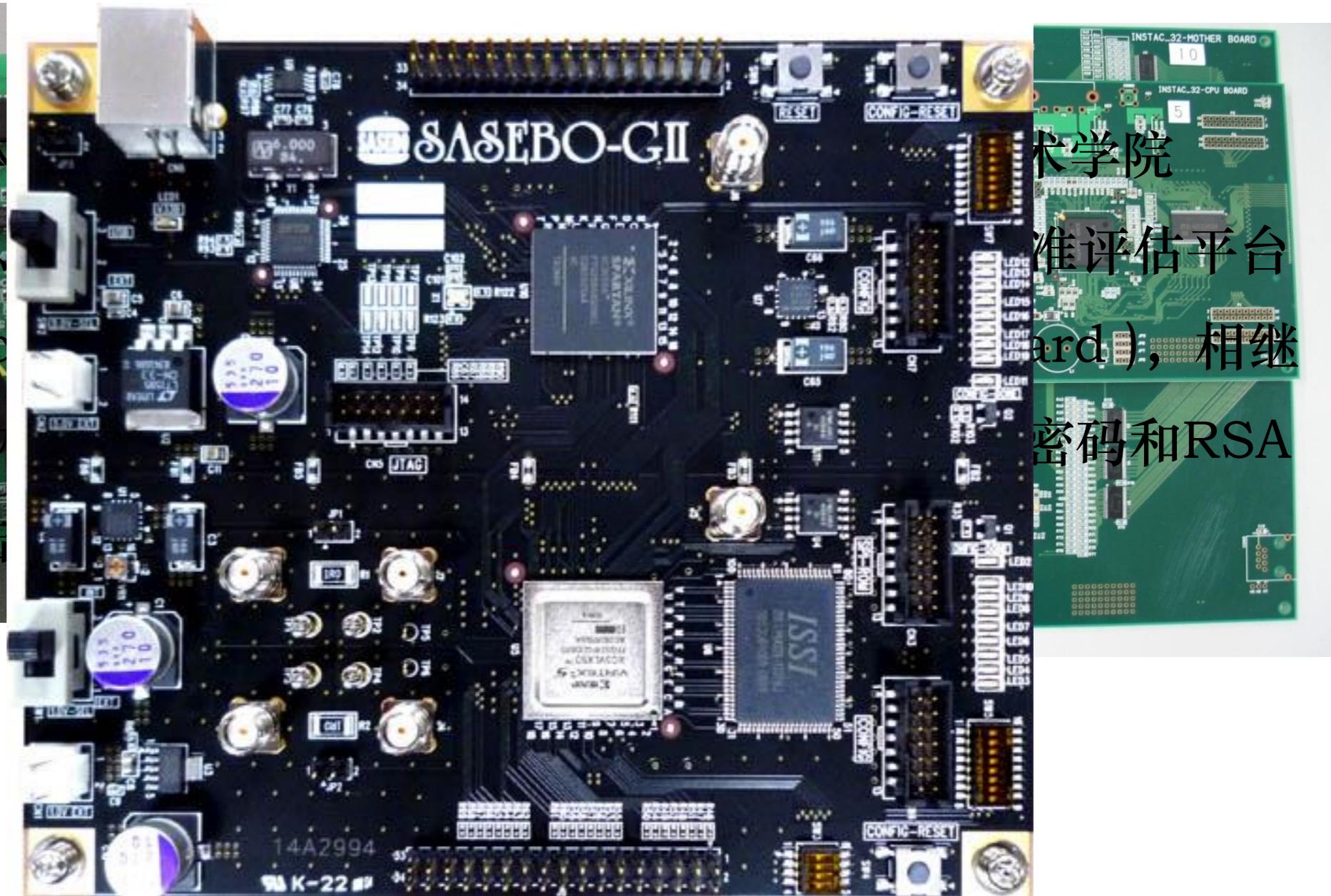
欧洲

近
参与
密码学
计划，
已能够
计时、
采集和



2.2 各国发展现状

日本



2.2 各国发展现状

中国

单位	计时攻击	功耗攻击	电磁攻击	Cache攻击	故障攻击	旁路硬件木马	旁路逆向工程
中国科学院		●			●		
上海交通大学		●	●		●		
西安电子科技大学		●	●		●		
电子科技大学		●	●				
国防科技大学		●			●	●	
清华大学		●			●		
中国科技大学		●					
武汉大学		●			●		●
解放军信息工程大学		●	●		●		
总参第五十四研究所	●	●	●	●	●	●	●

同国外研究比较

- 研究起步较晚，实验条件差，物理实验少；
- 自主测试仪器少，旁路泄露数据采集困难；
- 测试密码芯片少，主要技术受国外垄断。

2.3 攻击威胁分析

威胁对象



不同密码
算法、协议

算法

分组密码

序列密码

公钥密码

IPSec

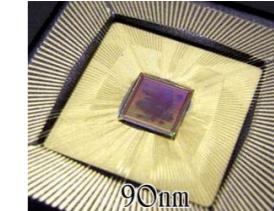
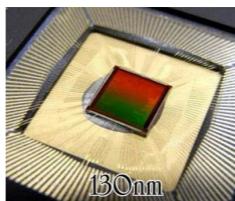
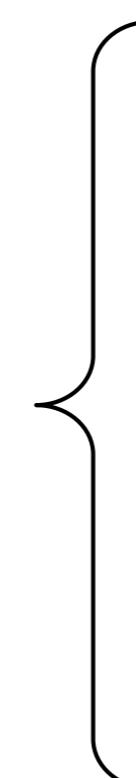
SSL

PKCS

协议



不同密码
实现



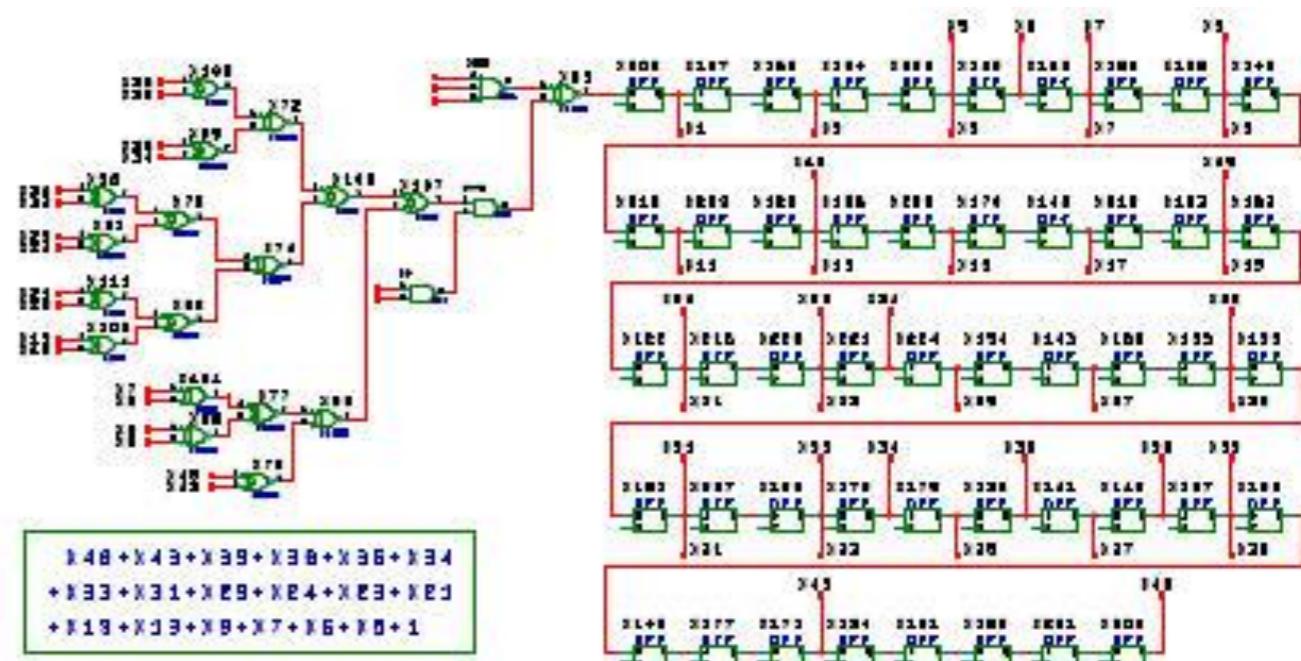
2.3 攻击威胁分析

威胁领域



密钥安全

算法安全



2.3 攻击威胁分析

威胁场景



已知明文密文

未知明文密文

已知算法设计

未知算法设计

2.3 攻击威胁分析

威胁场景



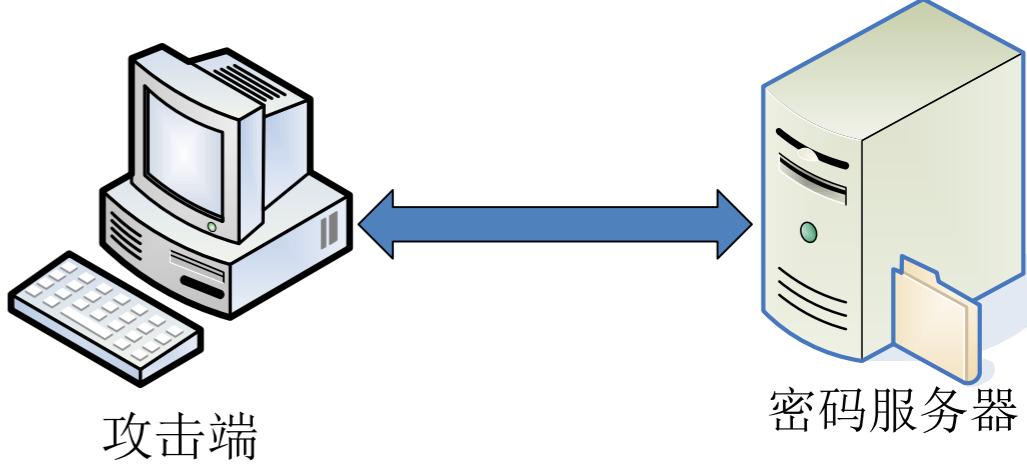
物理接触式



近距离非接触式

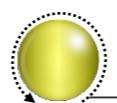


远程非接触式



提纲

- 1 为什么研究？密码旁路分析研究背景
- 2 现状怎么样？国内外研究现状及分析
- 3 攻击怎么干？典型攻击原理与实例分析
- 4 未来怎么走？未来研究热点分析与展望
- 5 我们怎么办？总结与建议

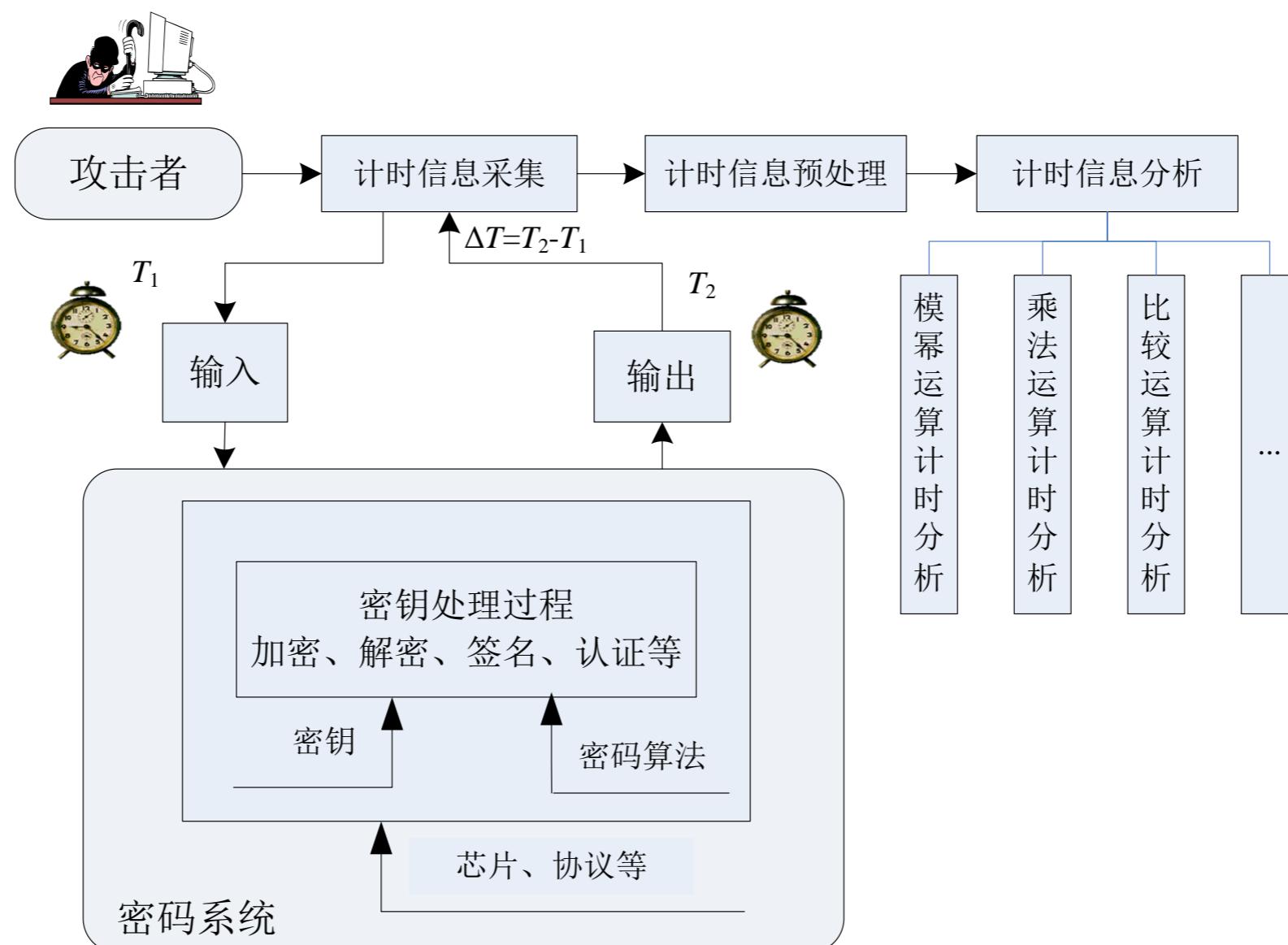


3.1 计时攻击原理与实例分析

3.1 计时攻击原理与实例分析

(1) 基本原理

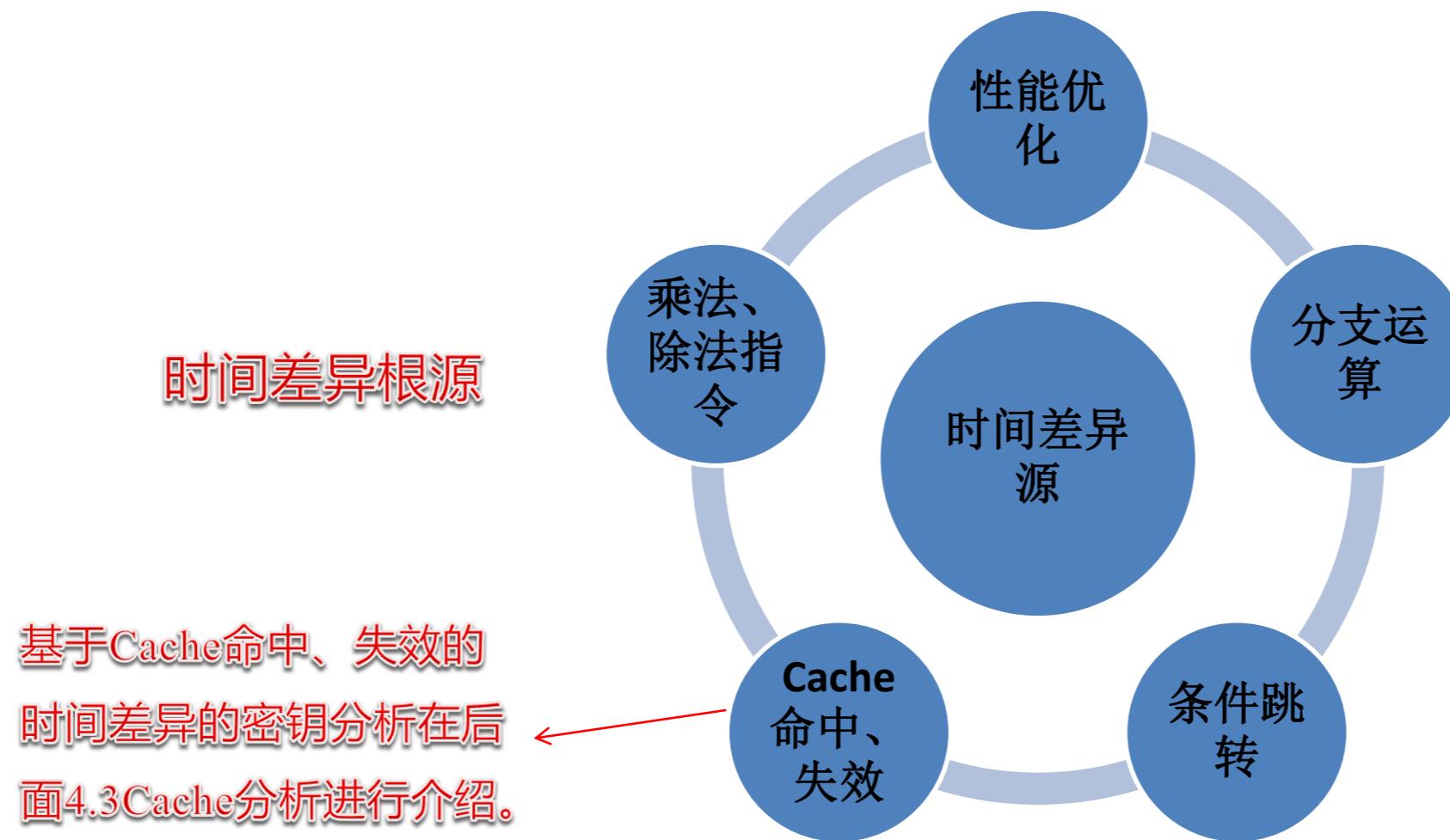
通过采集和分析密码不同输入的执行时间差异实现密钥破解。



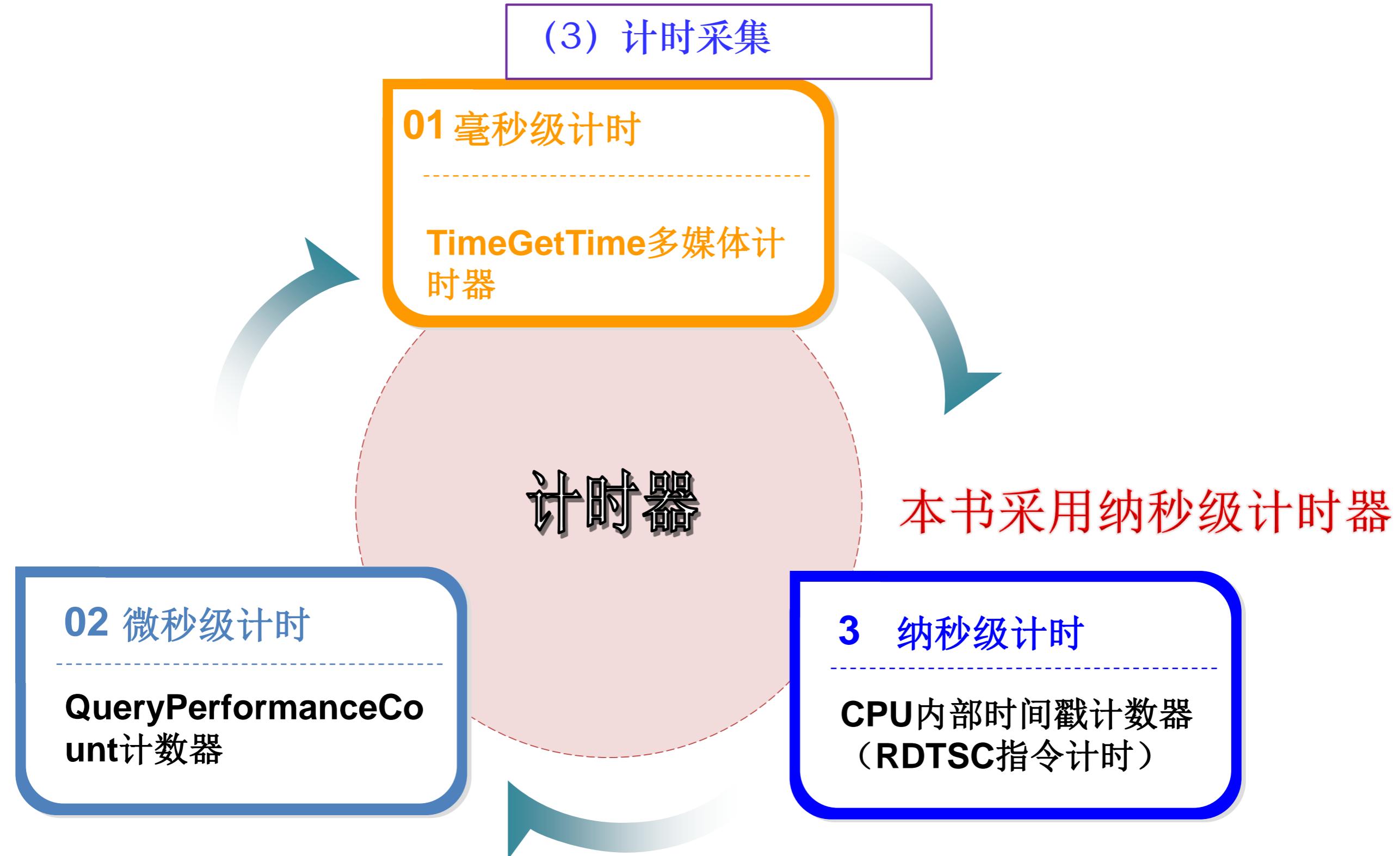
3.1 计时攻击原理与实例分析

(2) 适用范围

密码算法处理不同秘密信息时，指令的执行时间存在差异。



4.1 计时分析



3.1 计时攻击原理与实例分析

(4) 攻击方法与实例

- 1、基于模幂运算时间差异的RSA密钥攻击
- 2、基于乘法运算时间差异的AES密钥攻击

3.1 计时攻击原理与实例分析

(4) 攻击方法与实例

1、基于模幂运算时间差异的RSA密钥攻击

- RSA算法

选定密钥

- 随机选取两个大素数p和q。
- 计算 $n=pq$, $\varphi(n)=(p-1)(q-1)$
- 随机选取正整数d, 满足 $0 < d < \varphi(n)$, $\gcd(d, \varphi(n))=1$
- 计算 $e=d^{-1} \bmod \varphi(n)$ 。
- 公开e和n作为用户A的公钥。保密d, 以及p和q。d是用户A的私钥。

加密

- 对消息M, 假设 $0 < M < n$ 。
- 计算 $C=M^e \bmod n$

解密

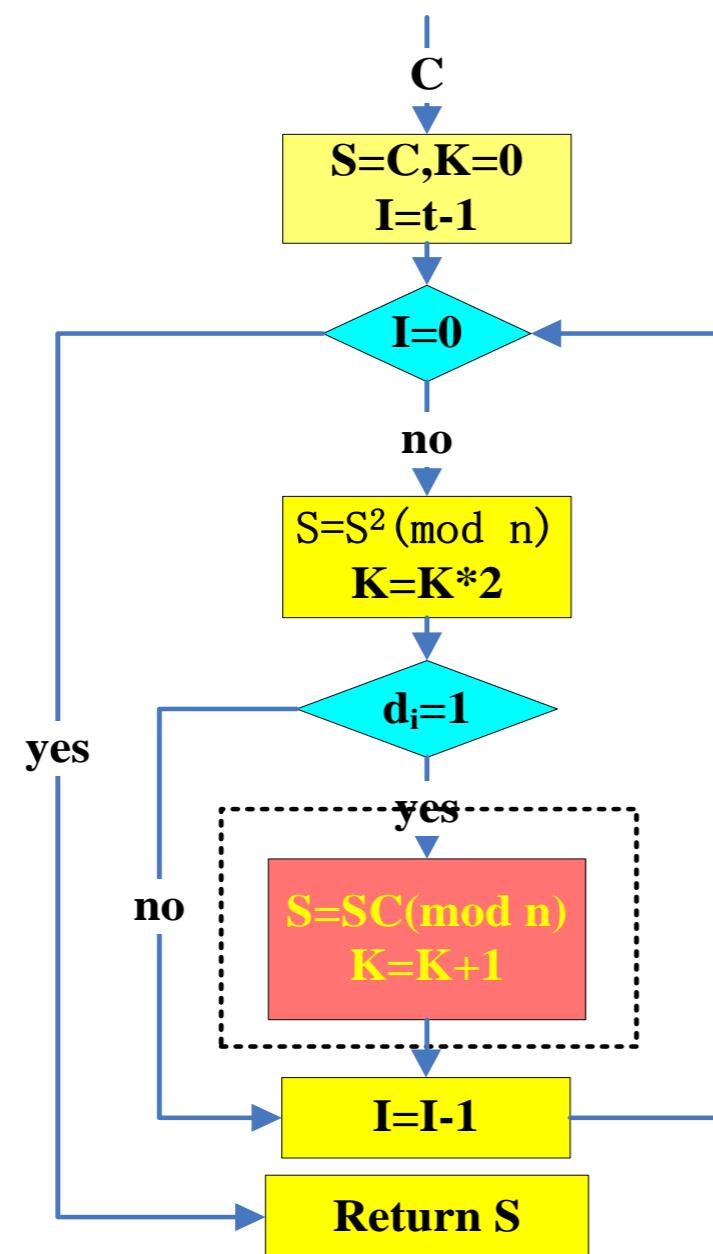
- 计算 $P=C^d \bmod n$

3.1 计时攻击原理与实例分析

(4) 攻击方法与实例

1、基于模幂运算时间差异的RSA密钥攻击

$C^d \bmod n$ 平方和乘法实现的RSA模幂运算

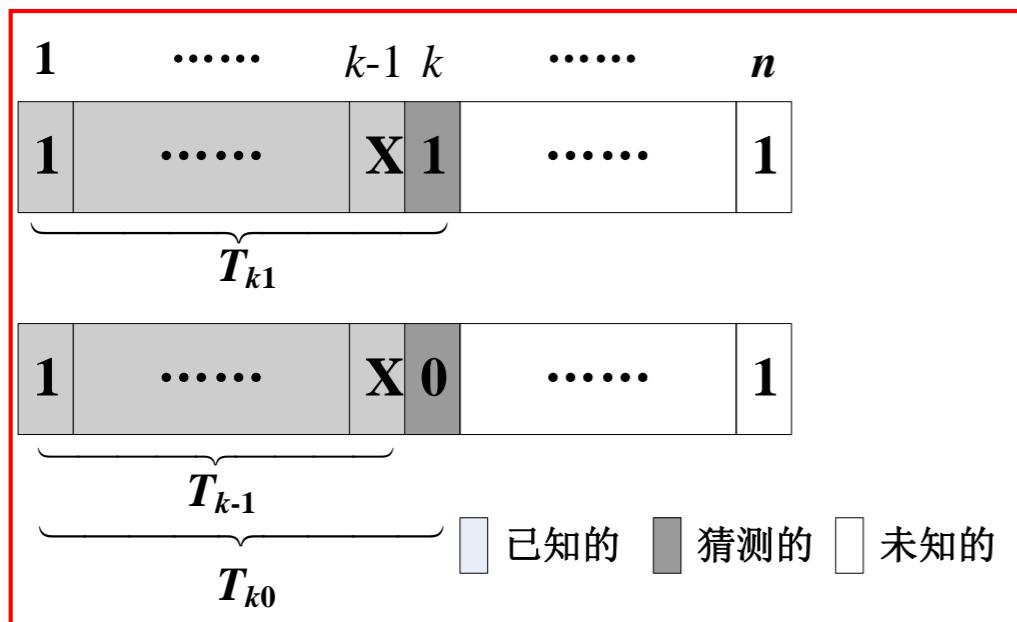


RSA密码采用平方和乘法操作进行模幂运算的时候，当密钥d的1个比特值为1的时候，比为0要多进行一步乘法操作，执行时间要长，如图中虚框所示。

3.1 计时攻击原理与实例分析

(4) 攻击方法与实例

1、基于模幂运算时间差异的RSA密钥攻击



假设前面k-1已知，猜测第k位是否为1？

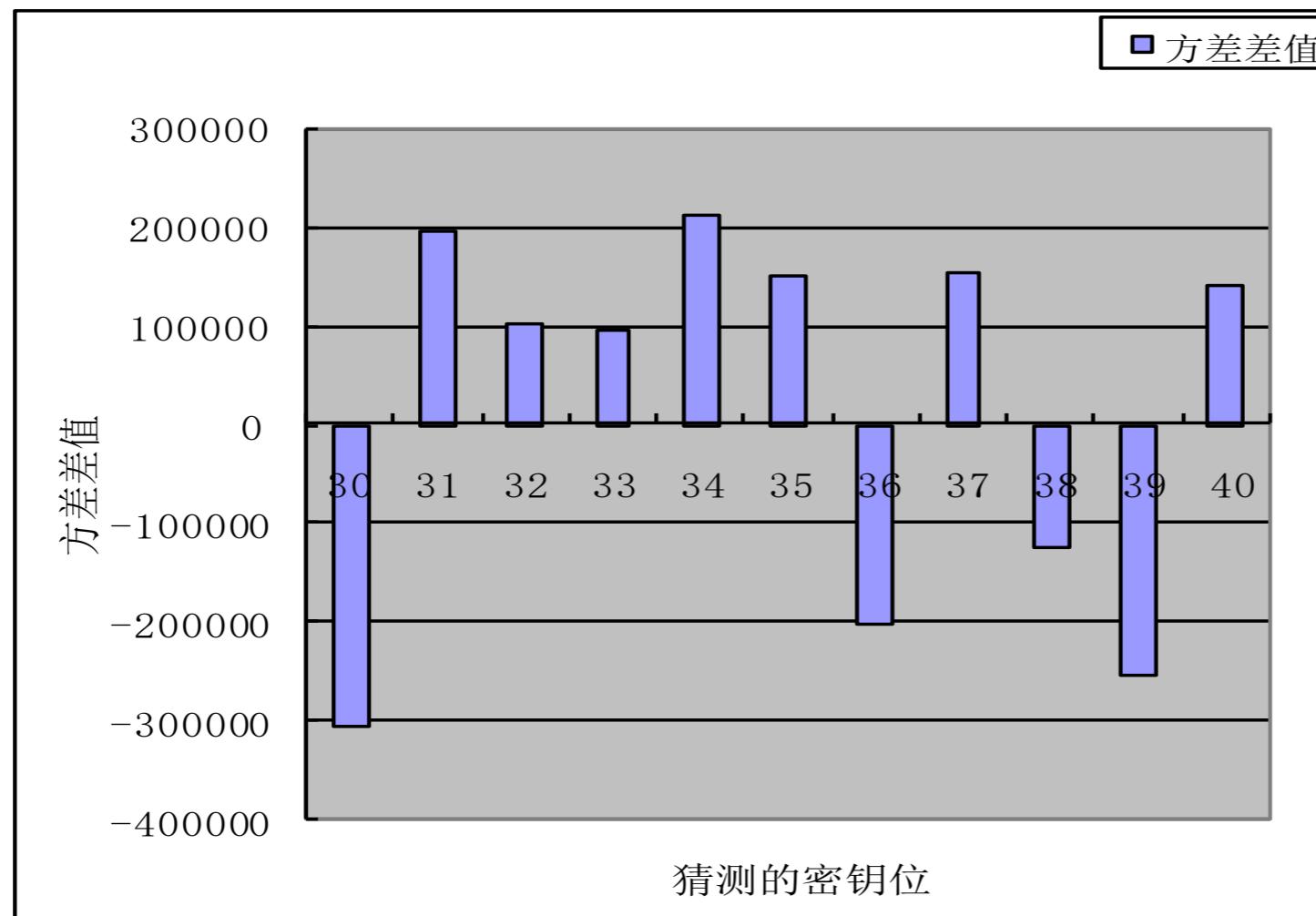
- 如果猜测正确，那么
- $\text{Var}(\{T_i - T_{i,k}\}) = \text{Var}(e + \sum_{j=1}^n t_j - \sum_{j=1}^k t_j) = \text{Var}(e + \sum_{j=k+1}^n t_j) = \text{Var}(e) + (n-k) \text{Var}(t)$
- 如果猜测错误，那么
- $\text{Var}(\{T_i - T_{i,k}\}) = \text{Var}(e + \sum_{j=1}^n t_j - \left[t_k + \sum_{j=1}^{k-1} t_j \right]) = \text{Var}(-t_k + \sum_{j=k}^n t_j) = \text{Var}(e) + (n-k)\text{var}(t) + 2\text{var}(t)$

显然猜测正确时，对应的方差值较小。重复执行获取 d_{k+1} 值，直到获取完整密钥 d 。

3.1 计时攻击原理与实例分析

(4) 攻击方法与实例

1、基于模幂运算时间差异的RSA密钥攻击



方差差值为负，对应的密钥位为1，为正的对应为0。
得到第30-40位密钥值为 $(1000\ 0010\ 110)_2$

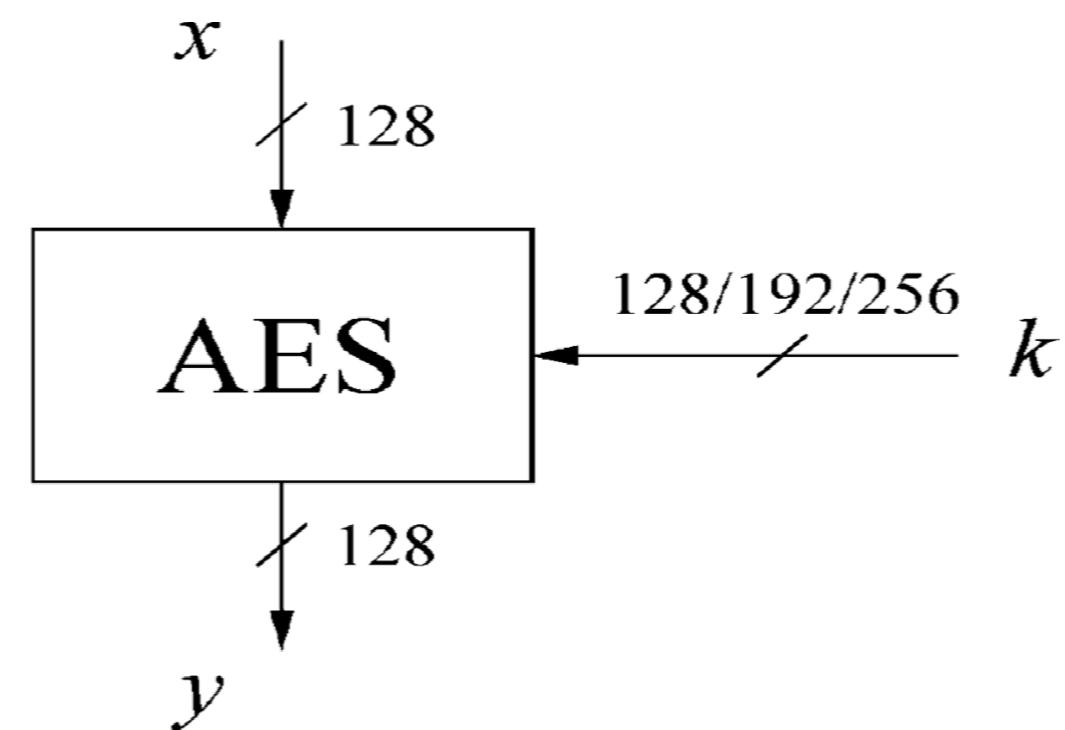
3.1 计时攻击原理与实例分析

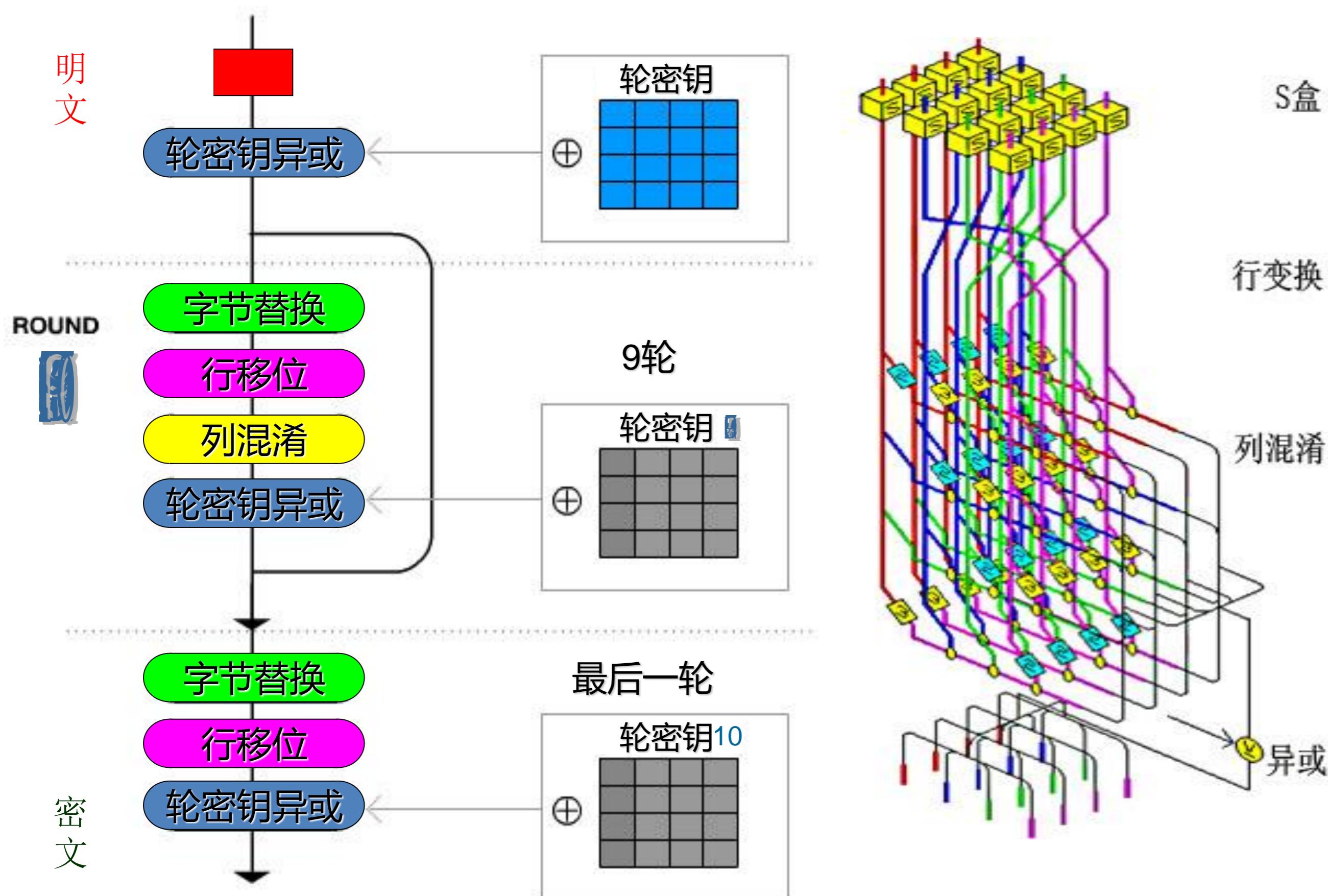
(4) 攻击方法与实例

2、基于乘法运算时间差异的AES密钥攻击

AES——Advanced Encryption Standard

- 2001年11月，美国国家标准技术研究所（NIST）正式公布AES分组密码为美国国家标准。
- 分组长度128，密钥长度为128、192或256。





3.1 计时攻击原理与实例分析

(4) 攻击方法与实例

2、基于乘法运算时间差异的AES密钥攻击

AES在执行列混淆操作时，常用xtime函数来实现，对于一个输入字节x，首先对x执行左移1位操作，**如果左移后最高位x7=1，则比为0时多执行一个异或0x1B操作，执行时间长。**

xtime函数

输入：字节x = (x₇, x₆, …, x₀)₂

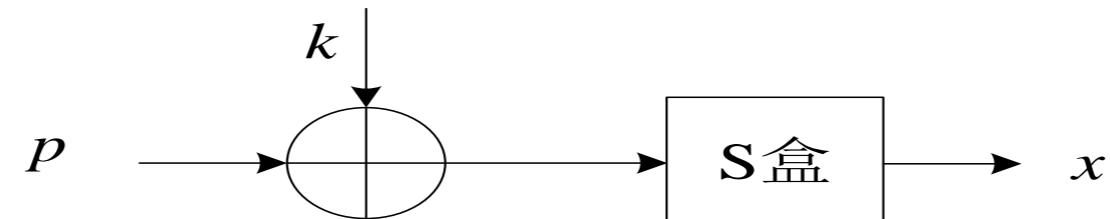
输出：字节y = xtime(x)

1. y ← (x << 1) ⊕ 0xFF
2. if x₇ = 1
3. y ← y ⊕ 0x1B
4. end if
5. return y

3.1 计时攻击原理与实例分析

(4) 攻击方法与实例

2、基于乘法运算时间差异的AES密钥攻击



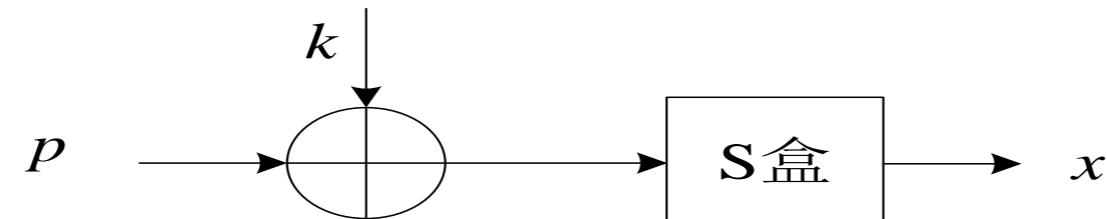
p, k, x 分别表示明文、密钥、查S盒结果，攻击 k 过程如下：

1. 产生随机明文，执行加密，并采集加密执行时间；
2. 攻击者穷举 k ，计算出所有明文对应的 x 值，然后对所有 x 左移一位，将最高位为1和0对应的明文 p 分别划为一个聚类，分别计算两个聚类对应的加密平均时间，然后得出二者之差；
3. 对于正确的 k 猜测，因为最高位为1对应的加密时间总是大于为0的加密时间，则对应的聚类平均加密时间差应该较大；对于错误的 k 猜测， x 左移后最高位对 p 的划分是随机的，则聚类平均加密时间差应该趋近于0。

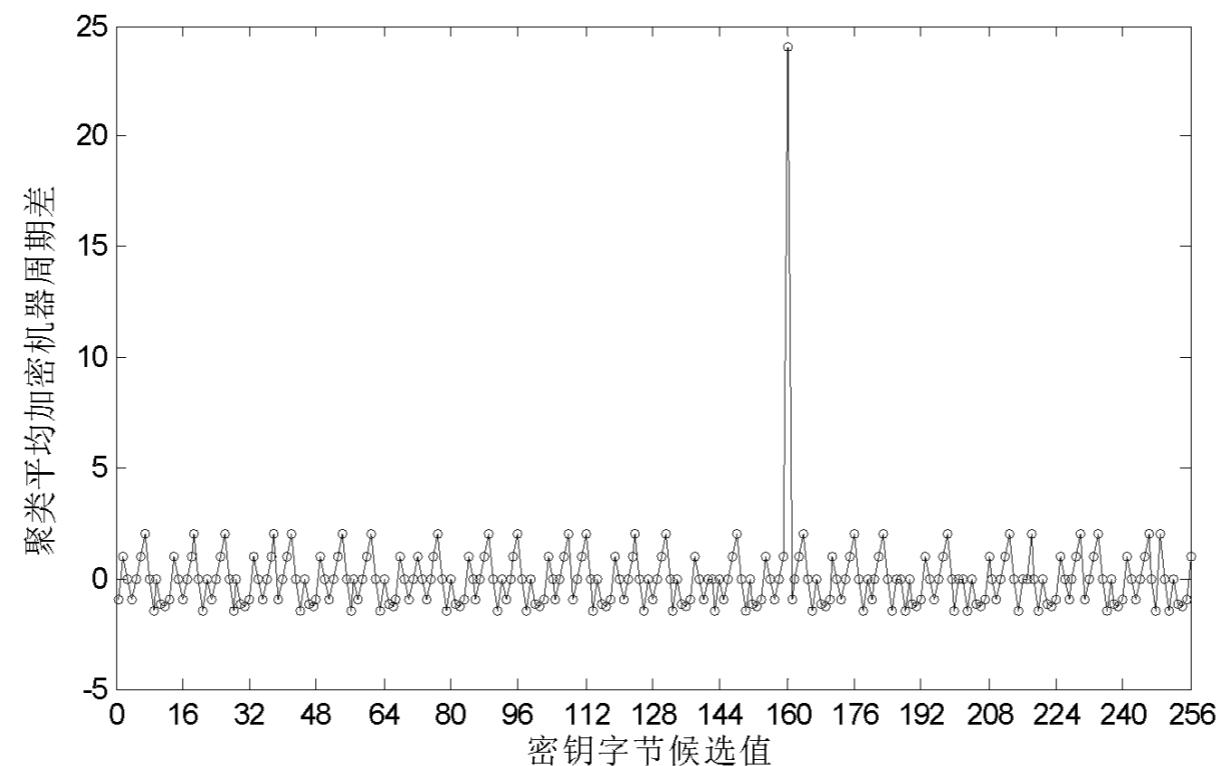
3.1 计时攻击原理与实例分析

(4) 攻击方法与实例

2、基于乘法运算时间差异的AES密钥攻击



NIST颁布在FIPS - 197上的AES算法在8051单片机上的实现



对于一个密钥字节攻击，正确的密钥字节猜测对应的平均加密机器周期长。

3.1 计时攻击原理与实例分析

(5) 攻击总结

攻击优
点

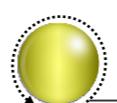
- 软件实现。可在本地和远程环境中实施。
- 适用性强。可对软件、硬件等各种密码算法实现实施。

攻击难
点

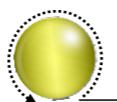
- 计时精度问题。高精度计时指令执行不稳定。
- 计时干扰问题。本地攻击系统进程存在干扰，远程攻击网络传输时延干扰。

防御方
法

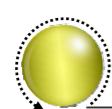
- 在密码执行过程中加入随机时延。
- 修改密码实现算法，使得不同密钥处理的执行时间相同。



3.1 计时攻击原理与实例分析



3.2 功耗/电磁攻击原理与实例分析



3.2 功耗/电磁攻击原理与实例分析

(1) 基本原理

通过采集和分析密码不同输入的功耗或电磁泄露差异实现密钥破解。

现代密码设备大部分使用VLSI设计，而VLSI中占统治地位的是数字CMOS逻辑电路。当集成电路内部处理的数据发生变化时，反映在CMOS电路上就是状态的变化，导致CMOS电路功率消耗（电磁辐射）。

$$P_{total} = P_{dyn} + P_{short} + P_{leak}$$

P_{dyn} 动态切换占到80%左右。

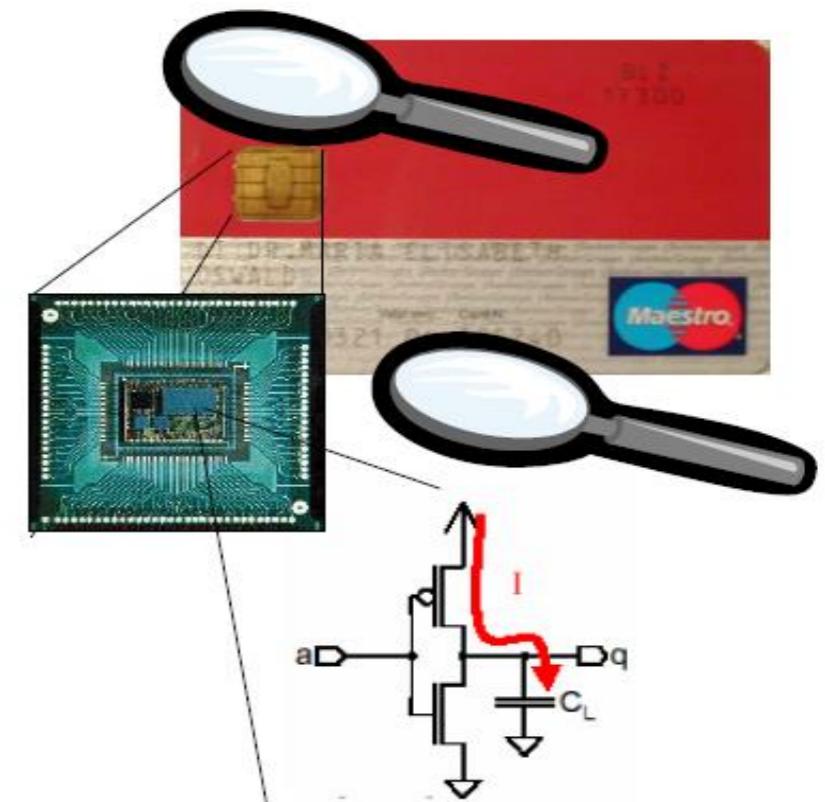
这样，如果CMOS门电路发生翻转时，就会有较大功耗（电磁辐射）。

0->0 低功耗（电磁辐射） 静态消耗

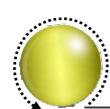
1->1 低功耗（电磁辐射） 静态消耗

0->1 高功耗（电磁辐射） 静态+动态消耗（放电）

1->0 低功耗（电磁辐射） 静态+动态消耗（充电）



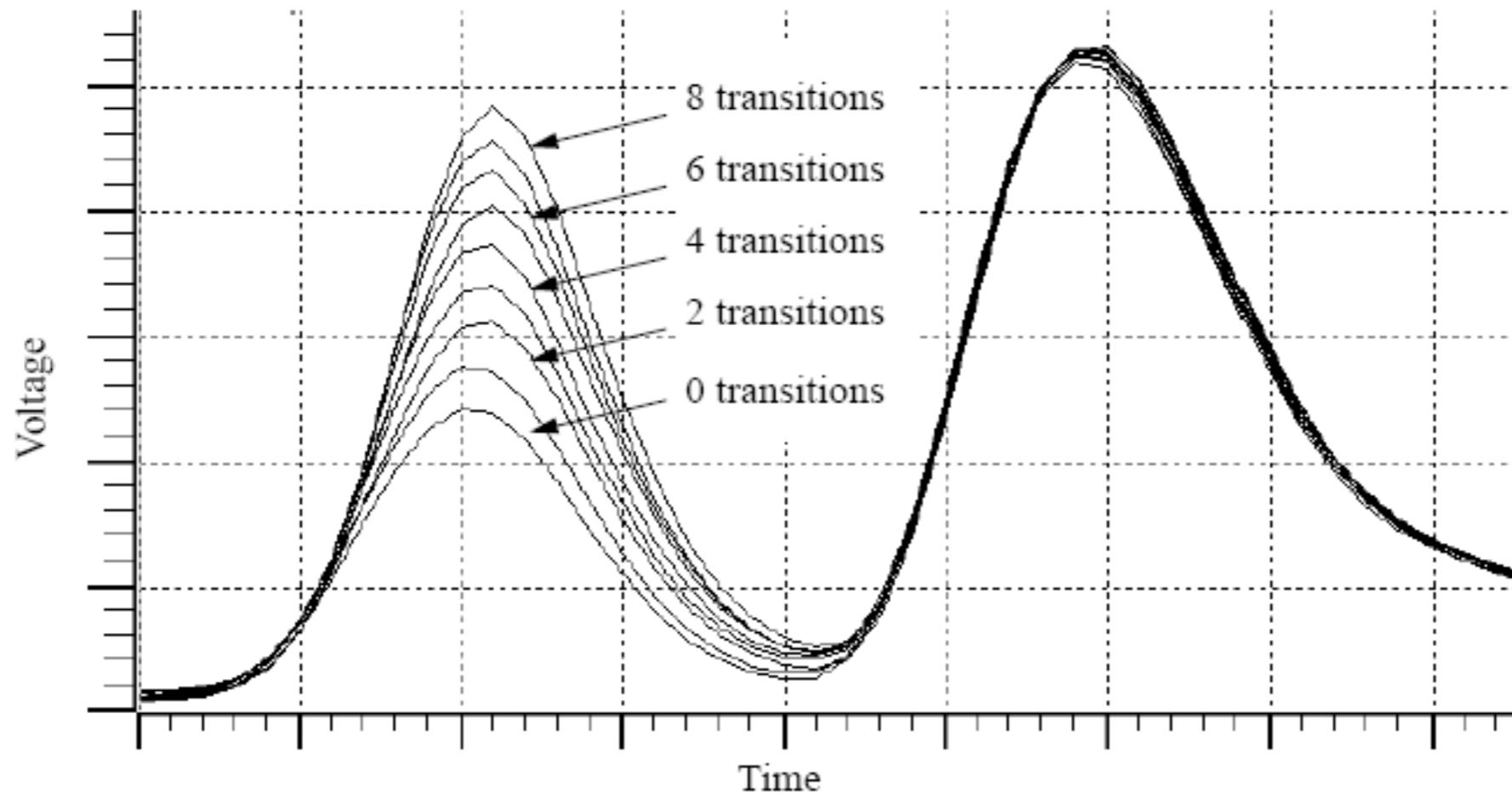
VLSI中CMOS逻辑电路充放电



3.2 功耗/电磁攻击原理与实例分析

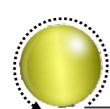
(2) 泄露模型

- 1) 汉明重量模型(HW)
- 2) 汉明距离模型(HD)



功耗大小同汉
明距离成正比

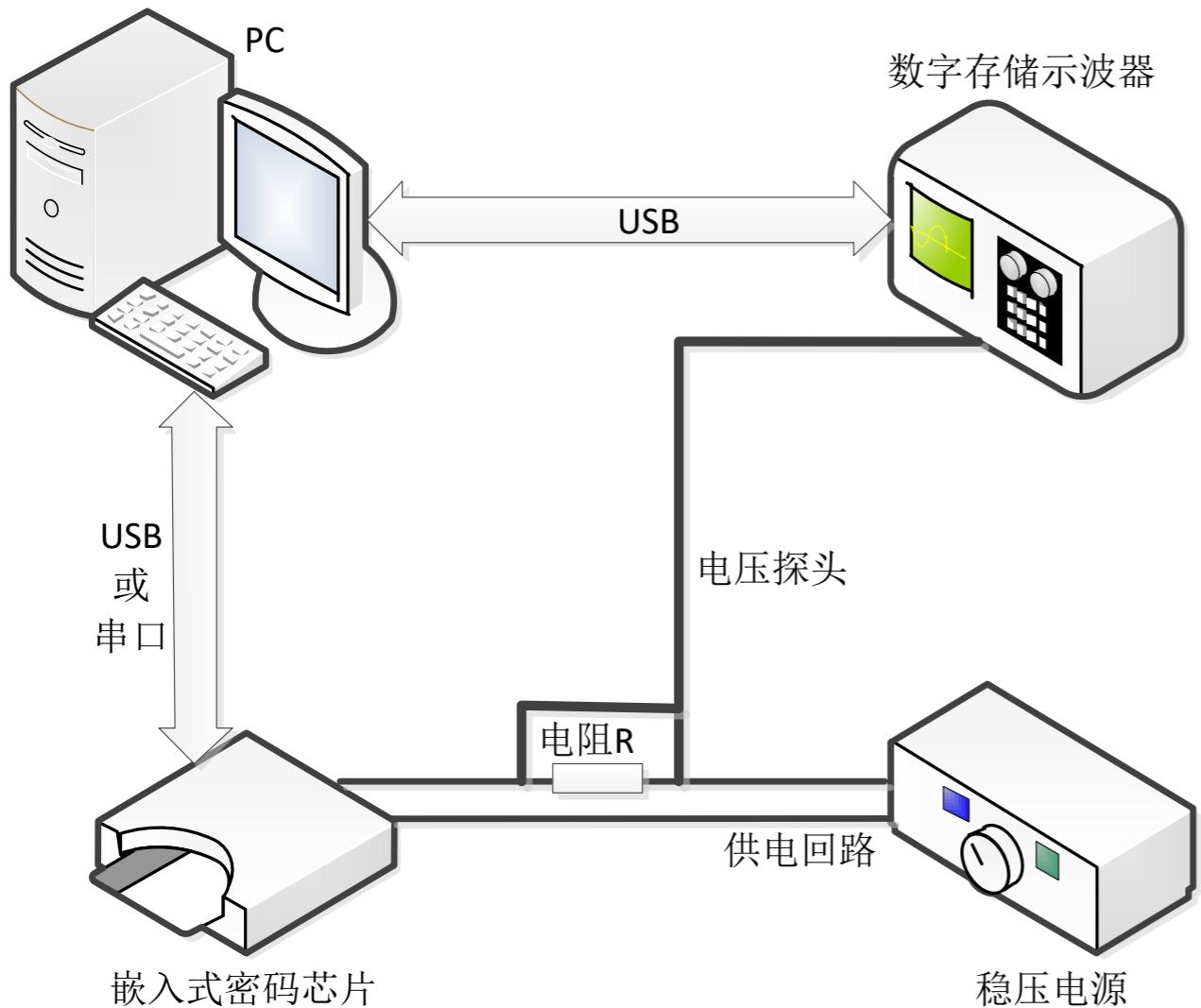
不同汉明距离对应功耗大小



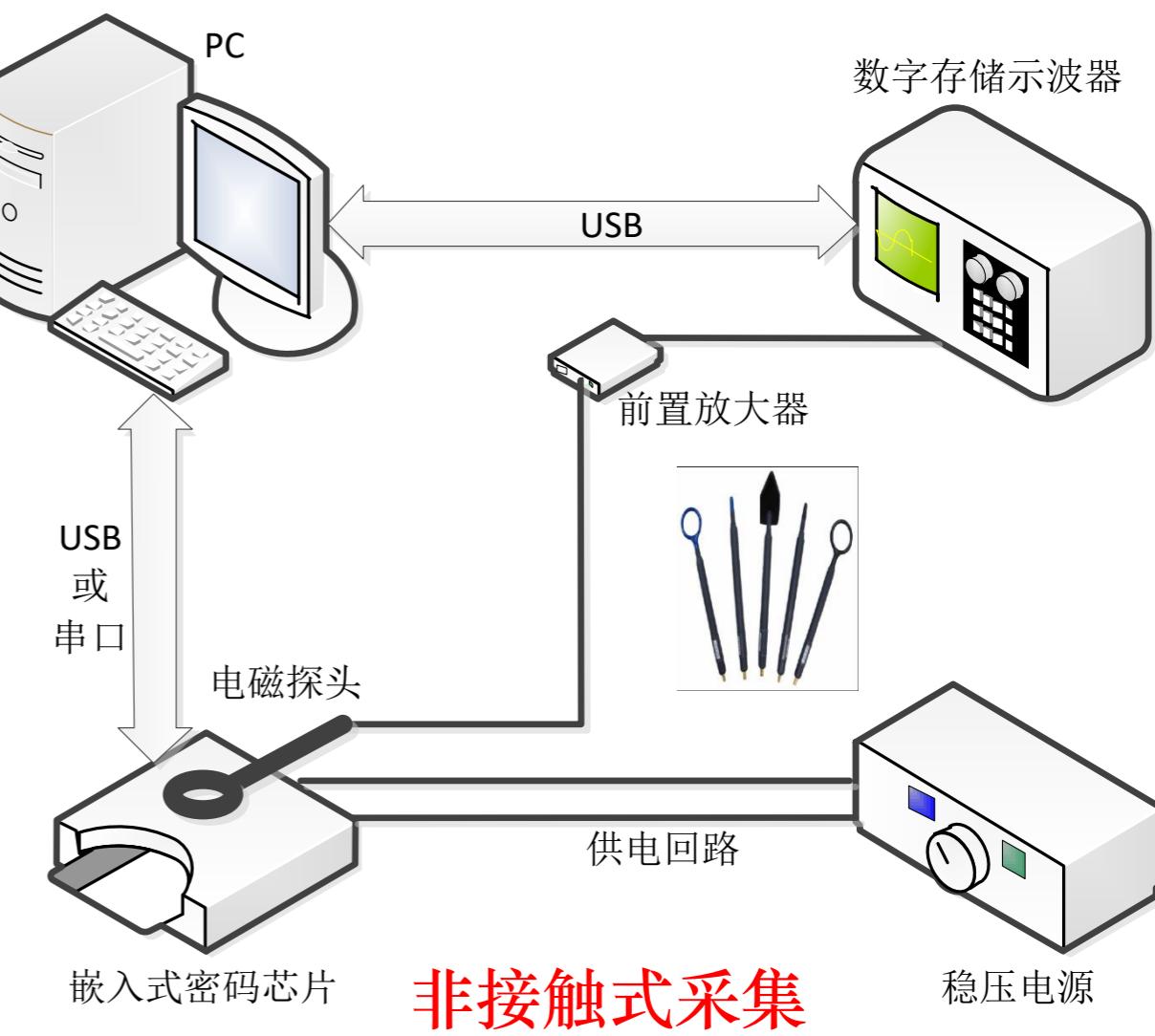
3.2 功耗/电磁攻击原理与实例分析

(3) 泄露采集

功耗泄露采集



电磁泄露采集



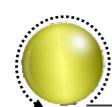
4.2 功耗/电磁分析

(4) 攻击方法与实例

1、RSA密码简单功耗攻击

2、AES密码差分功耗攻击

3、RC4密码电磁模板攻击

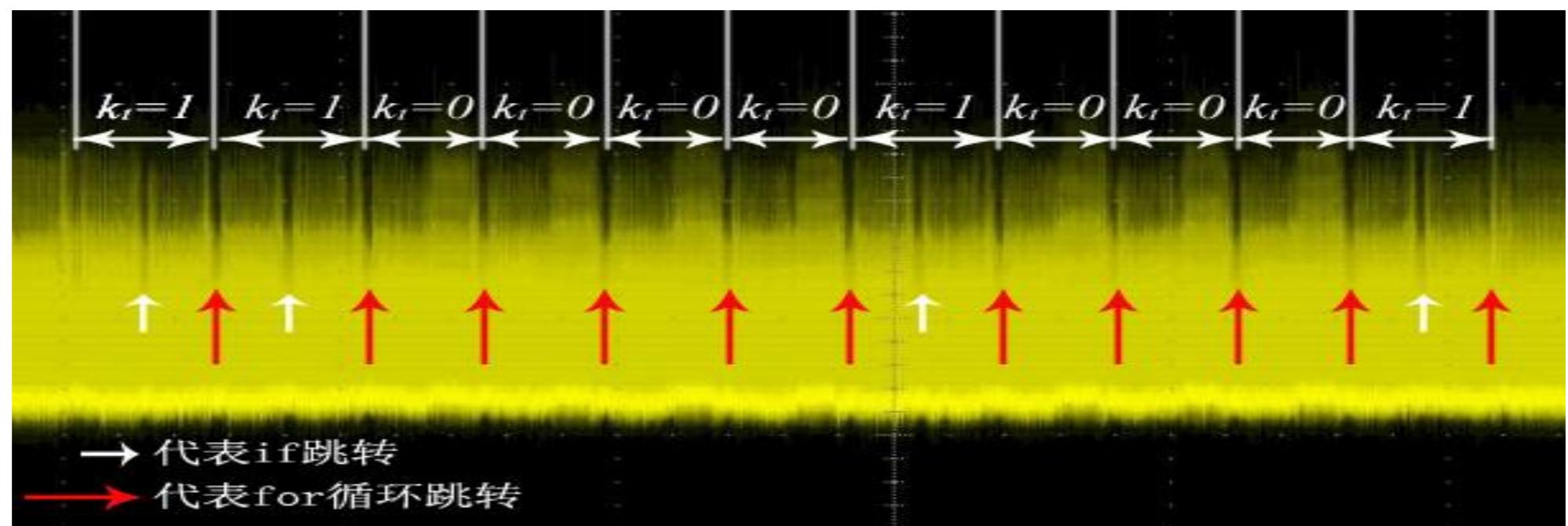


3.2 功耗/电磁攻击原理与实例分析

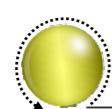
(4) 攻击方法与实例

1、RSA密码简单功耗攻击

简单功耗分析（Simple Power Analysis, SPA），采集单条功耗曲线，直接推断密钥位值。适用于使用一些和密钥相关跳转指令且功耗消耗差别较大密码算法，如RSA、ECC。



1条RSA功耗曲线，密钥为1比0多执行1个乘法操作，可以直接目视读取密钥位。

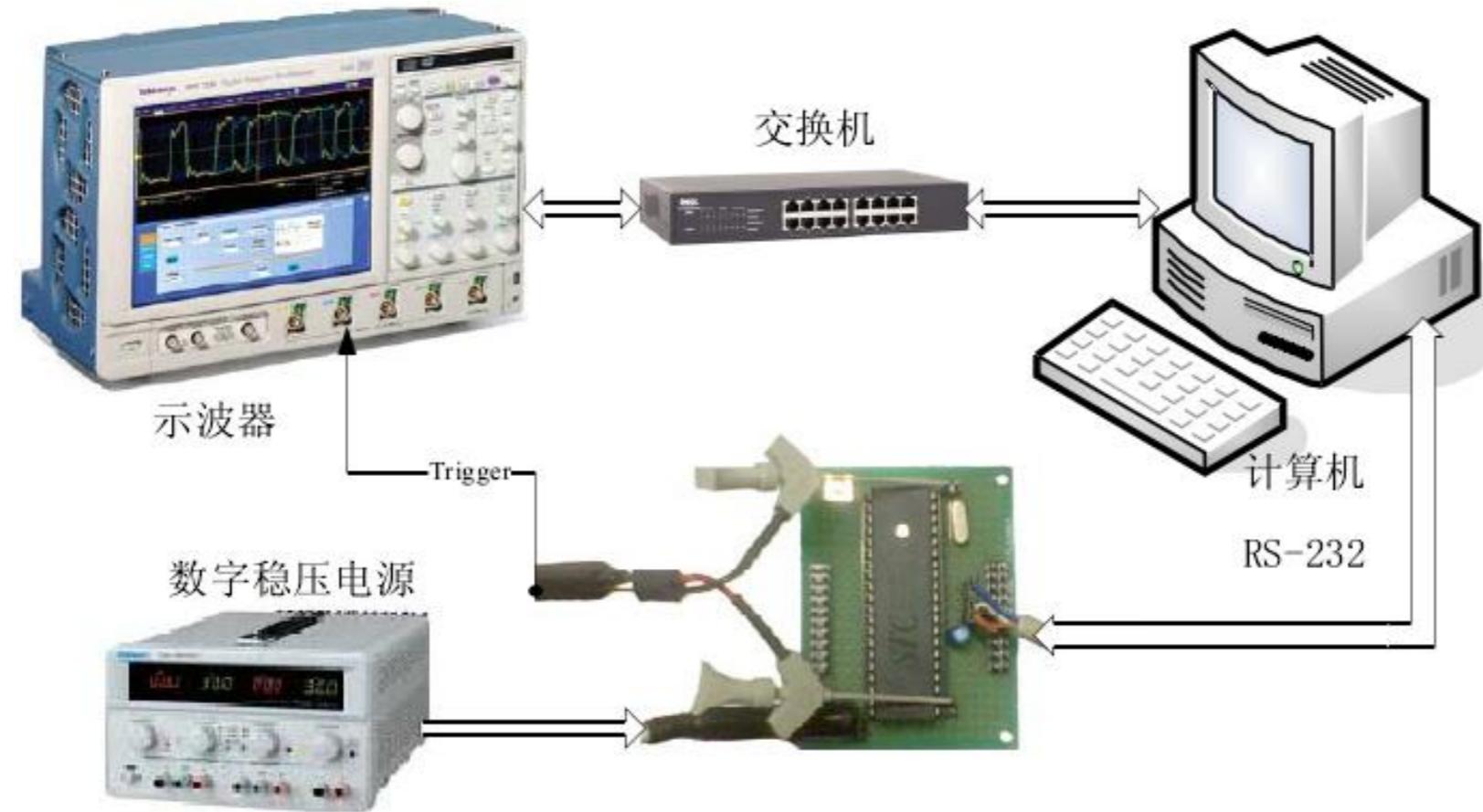


3.2 功耗/电磁攻击原理与实例分析

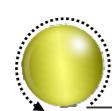
(4) 攻击方法与实例

2、AES密码差分功耗攻击

差分功耗分析（Differential Power Analysis, DPA），采集多条功耗曲线，猜测每个密钥字节得到中间状态的1比特值，并根据它对功耗曲线划分聚类，计算聚类功耗均值差，正确密钥字节对应曲线中出现**尖峰**，反之则比较**平缓**。



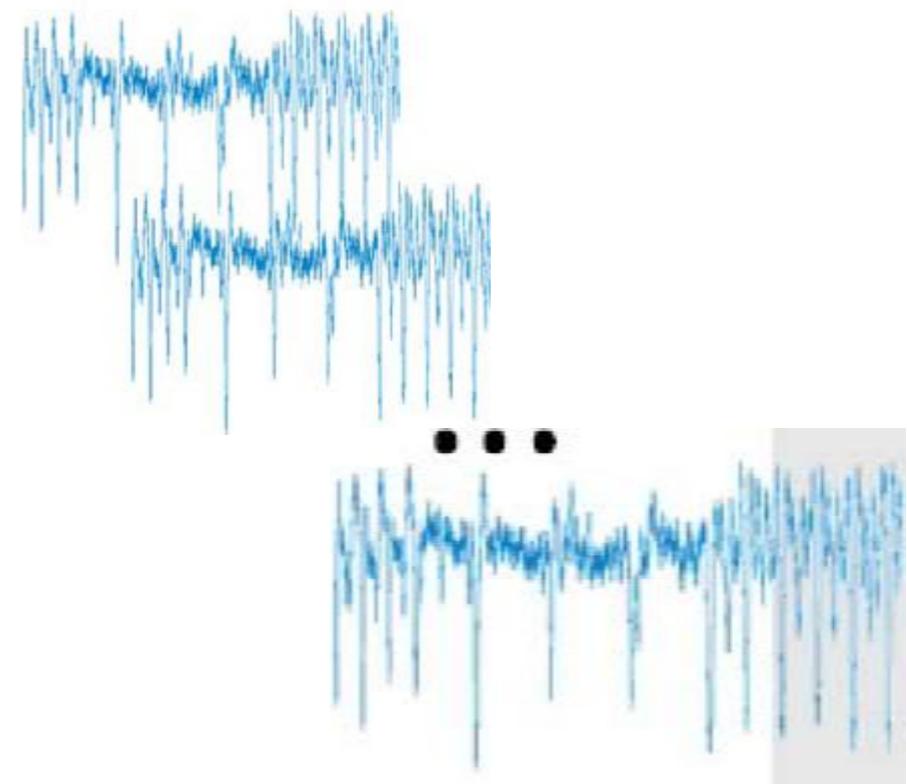
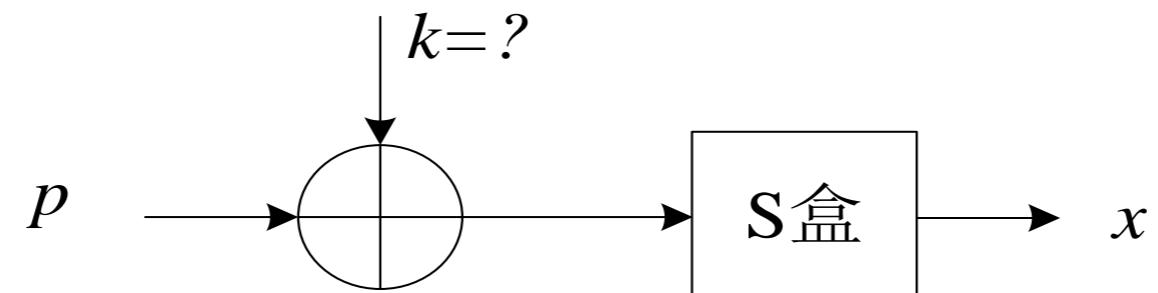
目标，获取单片机上的AES密钥。



3.2 功耗/电磁攻击原理与实例分析

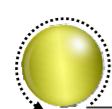
(4) 攻击方法与实例

2、AES密码差分功耗攻击



步骤1、攻击者采集 l 条加密功耗曲线

$D = \text{LSB}(x)$ 表示 x 的最低位值



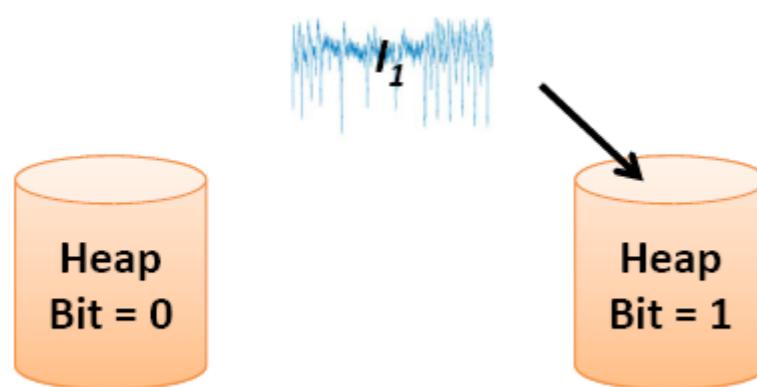
3.2 功耗/电磁攻击原理与实例分析

(4) 攻击方法与实例

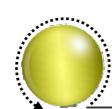
2、AES密码差分功耗攻击

步骤2、攻击者猜测一个密钥字节，根据某样本计算出的D值将曲线分堆
 $k=0x00??$

样本	1	2	3	4	5	6	7...
p	0x70						
x	0x51						
D	1						



LSB(x



3.2 功耗/电磁攻击原理与实例分析

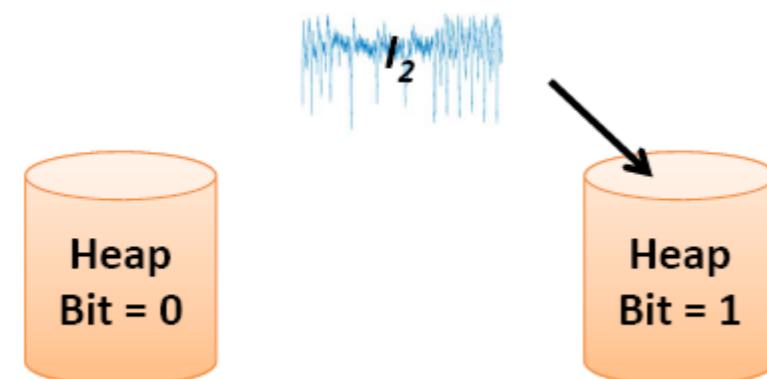
(4) 攻击方法与实例

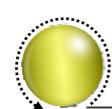
2、AES密码差分功耗攻击

步骤2、攻击者猜测一个密钥字节，根据某样本计算出的D值将曲线分堆

k=0x00??

样本	1	2	3	4	5	6	7...
p	0x70	0x22					
x	0x51	0x93					
D	1	1					





3.2 功耗/电磁攻击原理与实例分析

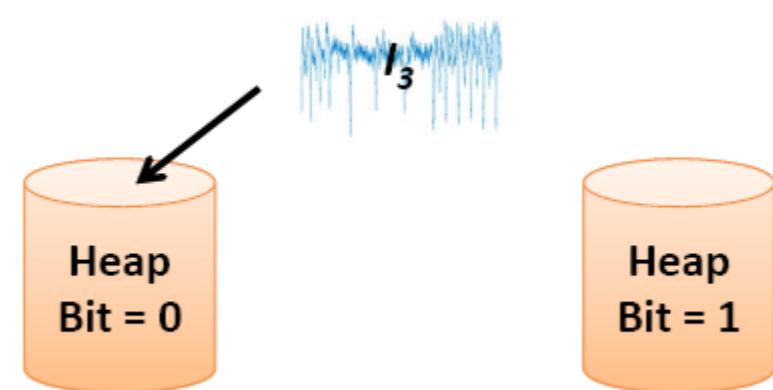
(4) 攻击方法与实例

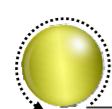
2、AES密码差分功耗攻击

步骤2、攻击者猜测一个密钥字节，根据某样本计算出的D值将曲线分堆

k=0x00??

样本	1	2	3	4	5	6	7...
p	0x70	0x22	0xAB				
x	0x51	0x93	0x62				
D	1	1	0				





3.2 功耗/电磁攻击原理与实例分析

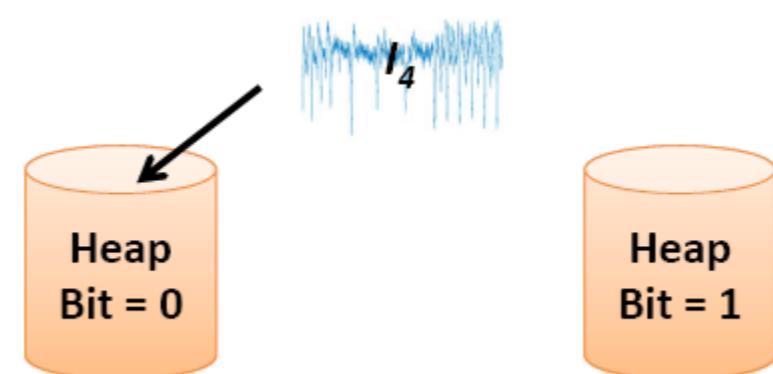
(4) 攻击方法与实例

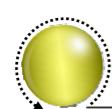
2、AES密码差分功耗攻击

步骤2、攻击者猜测一个密钥字节，根据某样本计算出的D值将曲线分堆

$k=0x00??$

样本	1	2	3	4	5	6	7...
p	0x70	0x22	0xAB	0xFF			
x	0x51	0x93	0x62	0x16			
D	1	1	0	0			





3.2 功耗/电磁攻击原理与实例分析

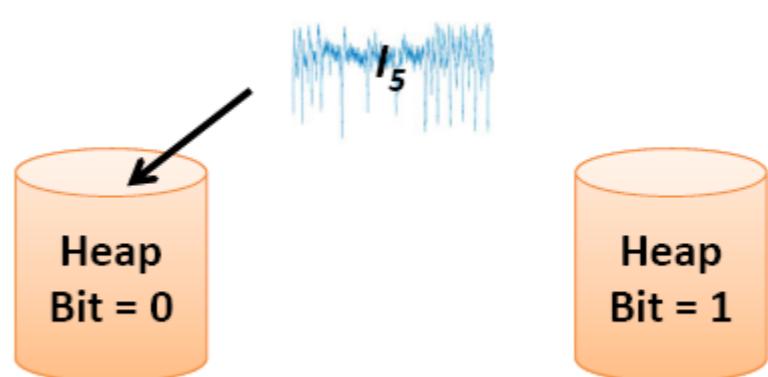
(4) 攻击方法与实例

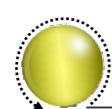
2、AES密码差分功耗攻击

步骤2、攻击者猜测一个密钥字节，根据某样本计算出的D值将曲线分堆

k=0x00??

样本	1	2	3	4	5	6	7...
p	0x70	0x22	0xAB	0xFF	0x01		
x	0x51	0x93	0x62	0x16	0x7C		
D	1	1	0	0	0		





3.2 功耗/电磁攻击原理与实例分析

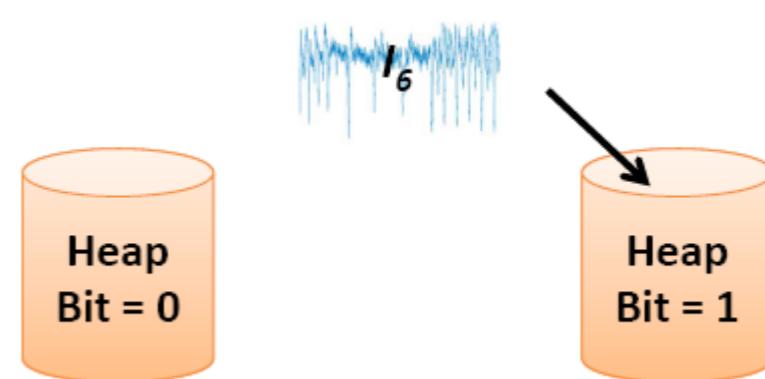
(4) 攻击方法与实例

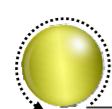
2、AES密码差分功耗攻击

步骤2、攻击者猜测一个密钥字节，根据某样本计算出的D值将曲线分堆

$k=0x00??$

样本	1	2	3	4	5	6	7...
p	0x70	0x22	0xAB	0xFF	0x01	0x32	...
x	0x51	0x93	0x62	0x16	0x7C	0x23	...
D	1	1	0	0	0	1	...





3.2 功耗/电磁攻击原理与实例分析

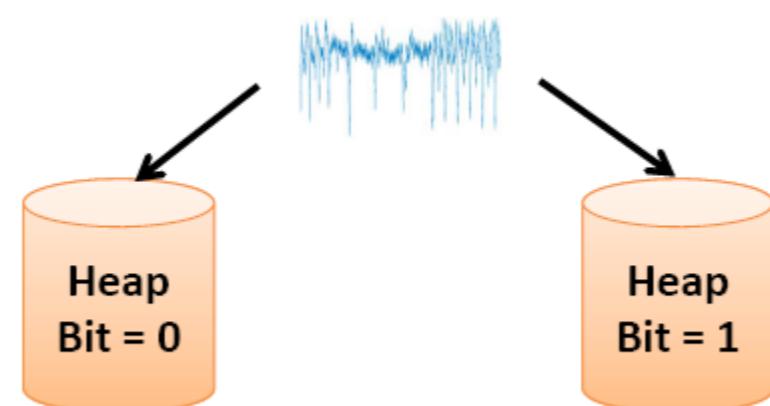
(4) 攻击方法与实例

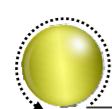
2、AES密码差分功耗攻击

步骤2、攻击者猜测一个密钥字节，根据某样本计算出的D值将曲线分堆

k=其他字节一直到0xFF??

样本	1	2	3	4	5	6	7...
p	0x70	0x22	0xAB	0xFF	0x01	0x32	...
x	0x73	0xC1	0x20	0x63	0xBB	0xCD	...
D	1	1	0	1	1	1	...



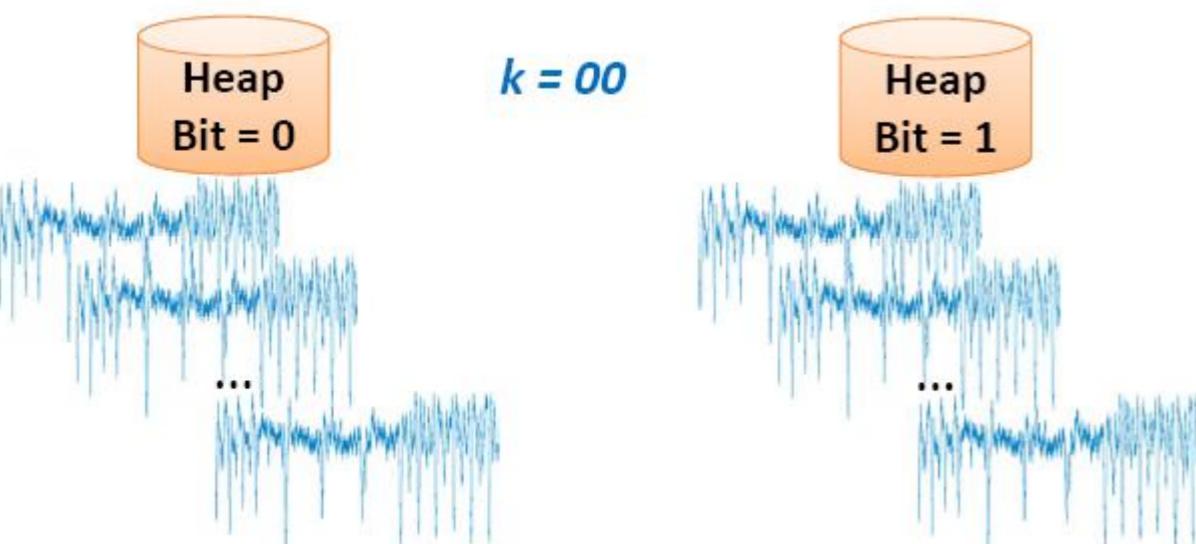


3.2 功耗/电磁攻击原理与实例分析

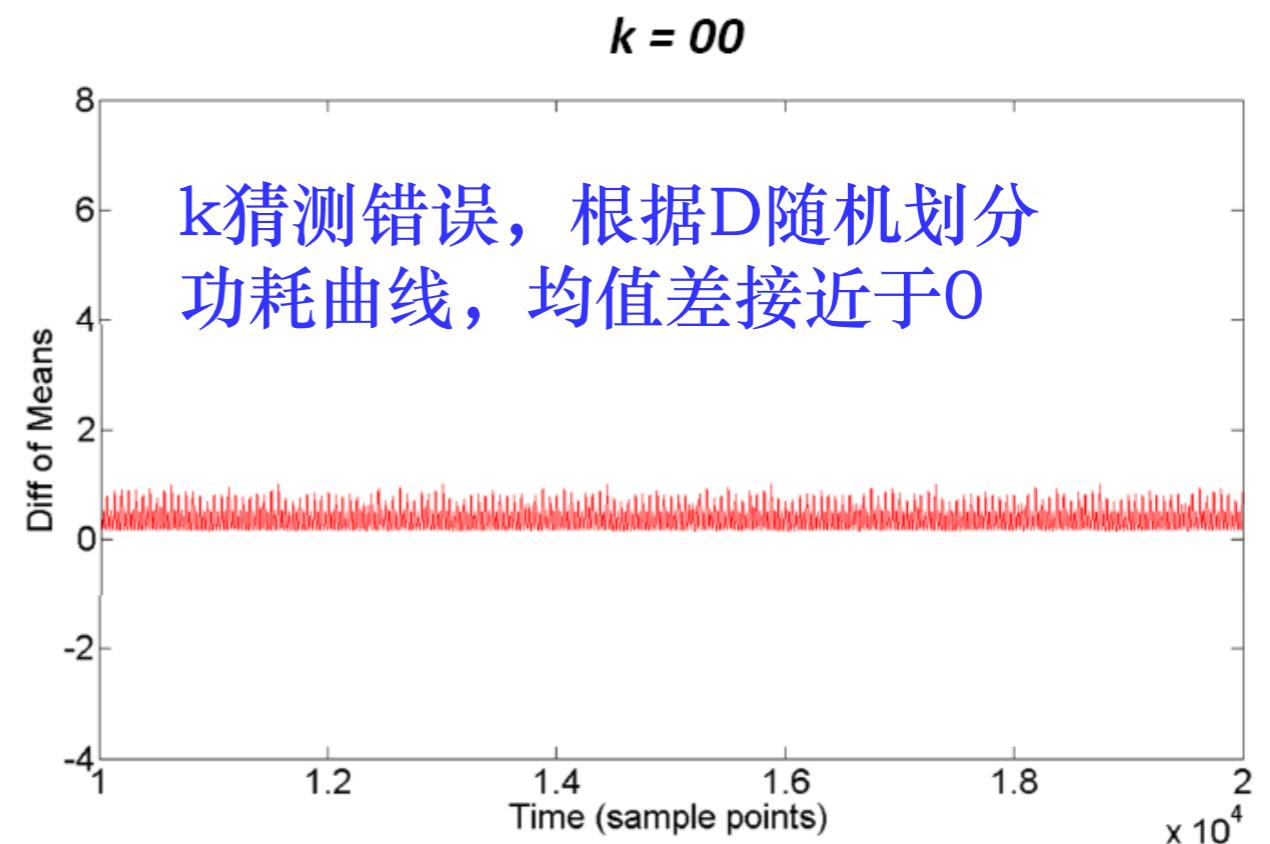
(4) 攻击方法与实例

2、AES密码差分功耗攻击

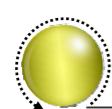
步骤3、攻击者计算某个密钥猜测D值两堆的功耗曲线均值差



D值两堆的功耗曲线



功耗曲线均值差

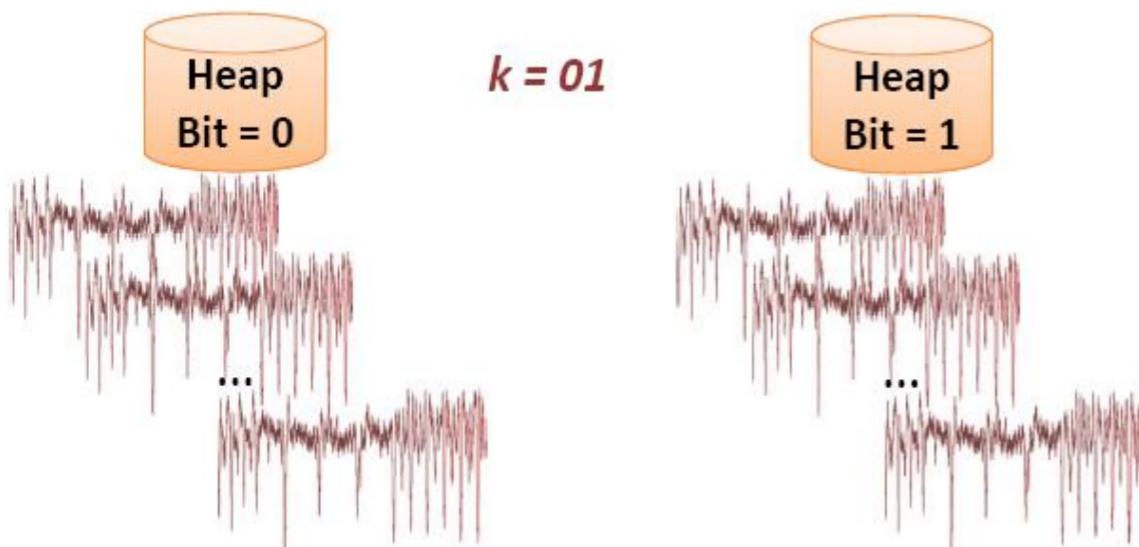


3.2 功耗/电磁攻击原理与实例分析

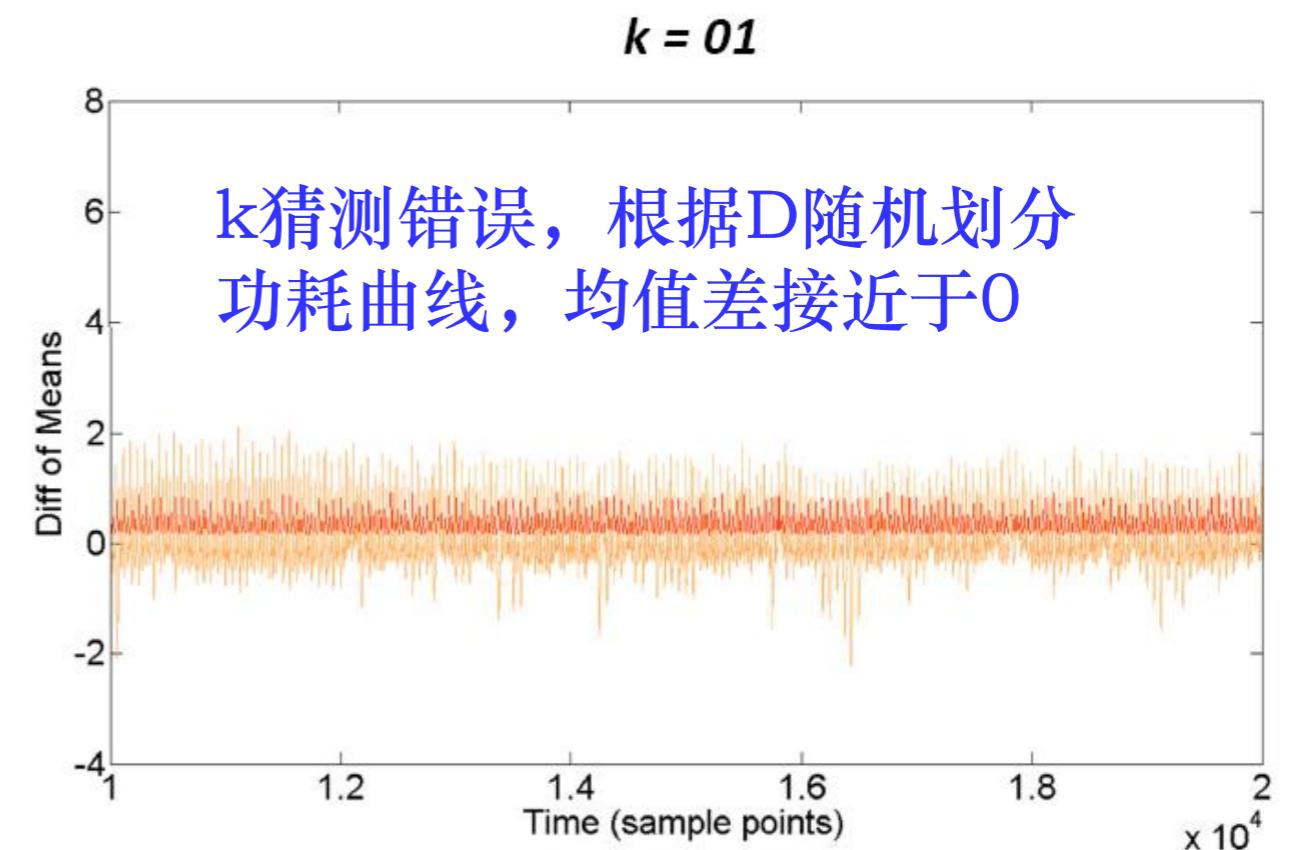
(4) 攻击方法与实例

2、AES密码差分功耗攻击

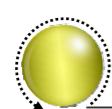
步骤3、攻击者计算某个密钥猜测D值两堆的功耗曲线均值差



D值两堆的功耗曲线



功耗曲线均值差



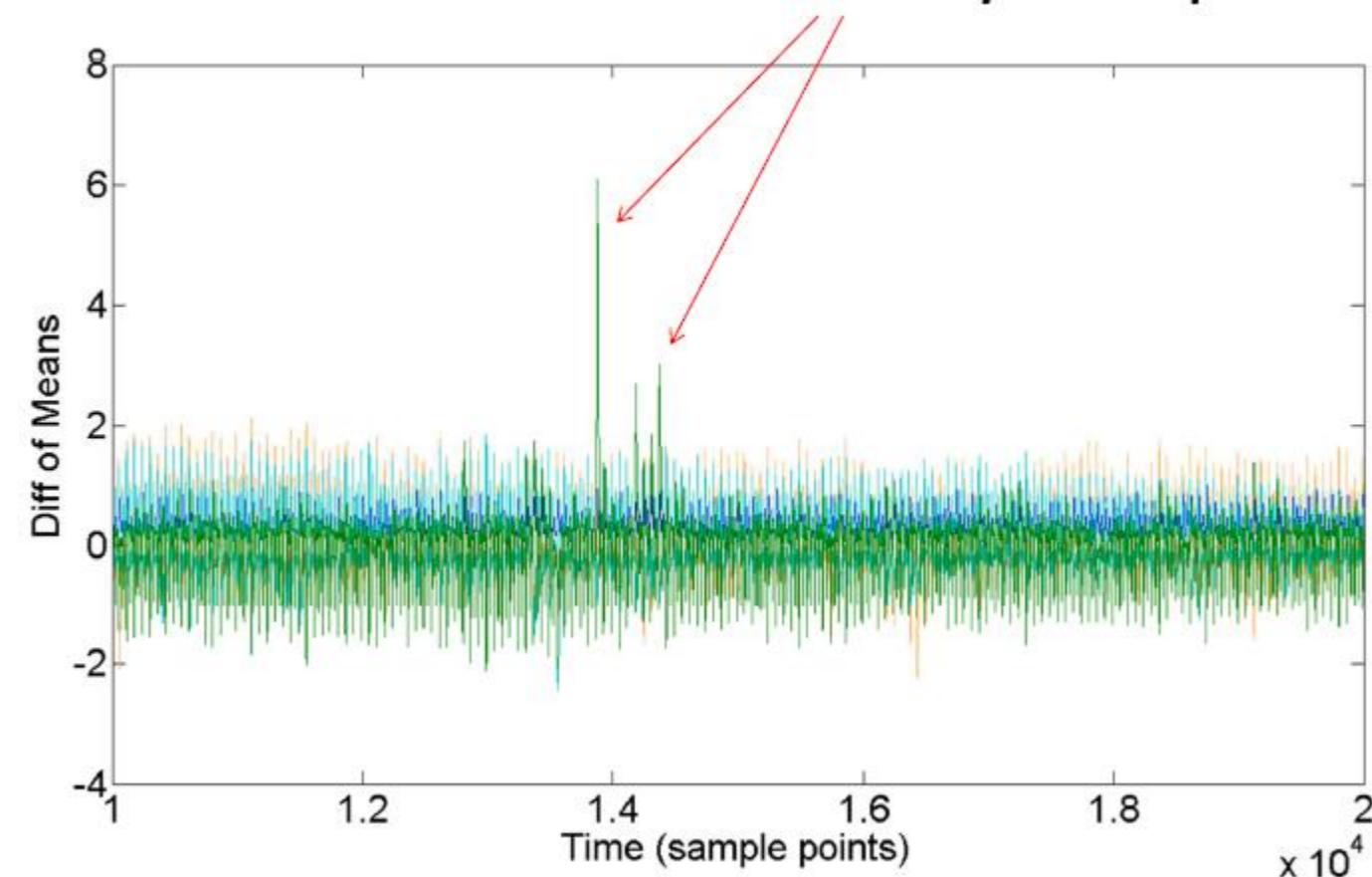
3.2 功耗/电磁攻击原理与实例分析

(4) 攻击方法与实例

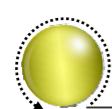
2、AES密码差分功耗攻击

步骤3、攻击者计算某个密钥猜测D值两堆的功耗曲线均值差

k猜测正确，根据D划分功耗曲线0和1分别划分到对应的堆，二者均值差接近于0和1的功耗，不为0



功耗曲线均值差



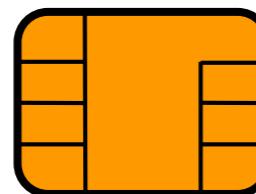
3.2 功耗/电磁攻击原理与实例分析

(4) 攻击方法与实例

3、RC4密码电磁模板攻击

模板分析（Template Analysis, TA），攻击者首先获取一个可控芯片采集不同密钥字节的旁路泄露搭建模板，然后采集目标芯片的1条泄露曲线，计算不同模板与泄露曲线的匹配度，匹配度最大对应正确密钥片段。

模板构建阶段

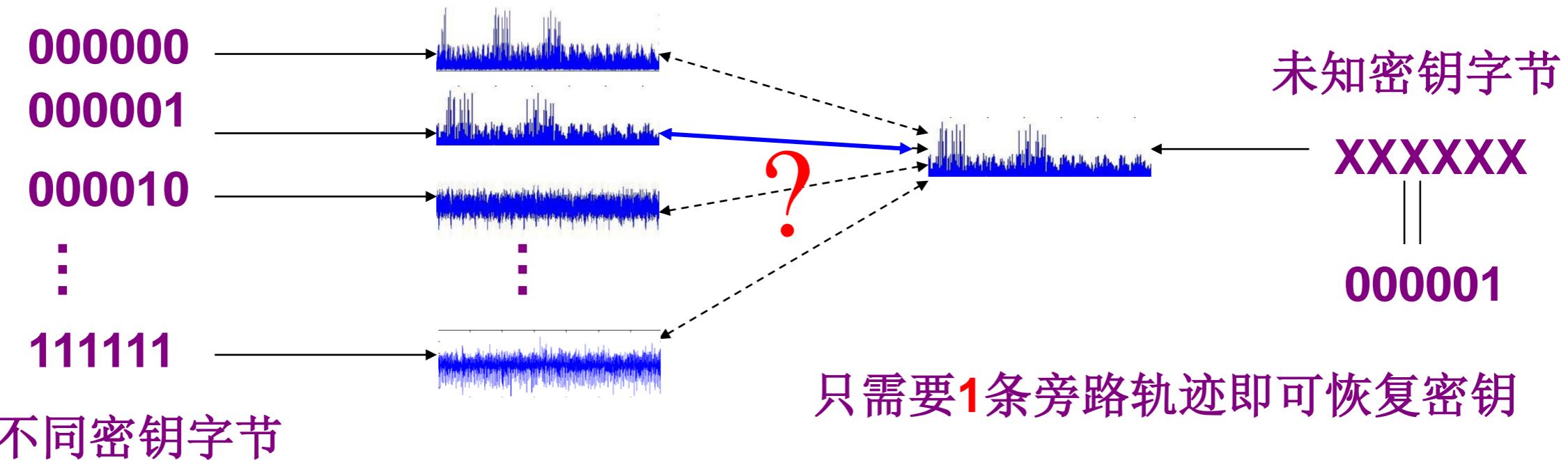


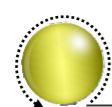
可控芯片

模板匹配阶段



被攻击芯片





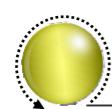
3.2 功耗/电磁攻击原理与实例分析

(4) 攻击方法与实例

3、RC4密码电磁模板攻击

RC4 是Ron Rivest在1987年为RSA数据安全公司开发的可变密钥长度的序列密码。1994年源代码被公开。加密速度很快（DES的10倍），已被广泛应用于各种嵌入式密码系统中，如IEEE802.11b中定义的WEP和IEEE802.11i中定义的TKIP。

RC4以输出反馈（OFB）方式工作：密钥序列与明文相互独立。其密钥长度从1到2048位可变，常用的为40到256位。加密算法包含两个部分：一个称为KSA 密钥扩展算法和一个称为PRGA伪随机数产生算法。PRGA算法产生的伪随机数序列R用于与明文异或产生密文(加密)，或者与密文异或产生明文(解密)。

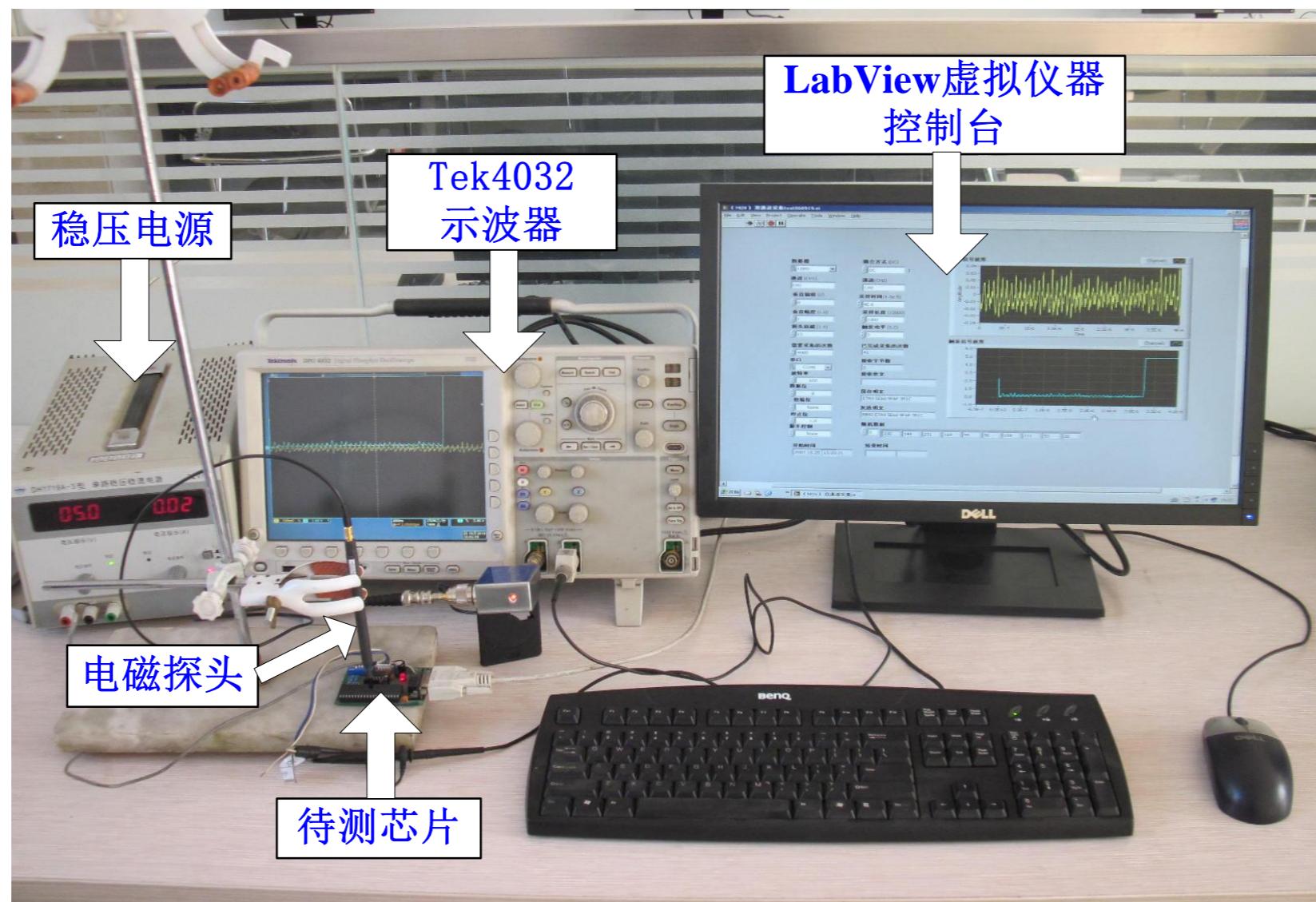


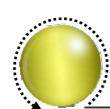
3.2 功耗/电磁攻击原理与实例分析

(4) 攻击方法与实例

3、RC4密码电磁模板攻击

攻击目标为KSA算法中的密钥，攻击策略将完整密钥按字节实施模板攻击。





3.2 功耗/电磁攻击原理与实例分析

(4) 攻击方法与实例

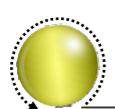
3、RC4密码电磁模板攻击

无防护

匹配密钥 原始密钥	时域模板匹配结果				频域模板匹配结果			
	00000000	10010001	10111101	11111111	00000000	10010001	10111101	11111111
00000000	0.85	0.64	0.23	0.08	0.79	0.46	0.33	0.01
10010001	0.15	0.79	0.18	0.11	0.25	0.65	0.18	0.15
10111101	0.18	0.24	0.85	0.15	0.20	0.33	0.70	0.26
11111111	0.03	0.12	0.34	0.89	0.02	0.21	0.45	0.77

插入时延防护

匹配密钥 原始密钥	时域模板匹配结果				频域模板匹配结果			
	00000000	10010001	10111101	11111111	00000000	10010001	10111101	11111111
00000000	0.24	0.25	0.32	0.03	0.72	0.31	0.18	0.09
10010001	0.23	0.43	0.43	0.12	0.33	0.77	0.24	0.07
10111101	0.08	0.16	0.33	0.20	0.17	0.25	0.80	0.34
11111111	0.02	0.12	0.27	0.69	0.12	0.15	0.33	0.79



3.2 功耗/电磁攻击原理与实例分析

(5) 攻击总结

攻击优
点

- 泄露信息丰富。
- 攻击适用性好。

攻击难
点

- 功耗信号预处理问题。
- 电磁信号远场采集问题。

防御方
法

- 在密码执行过程中加入随机时延。
- 在密码执行过程中增加随机掩码。
- 在门电路设计过程中使用平衡电路



3.1 计时攻击原理与实例分析

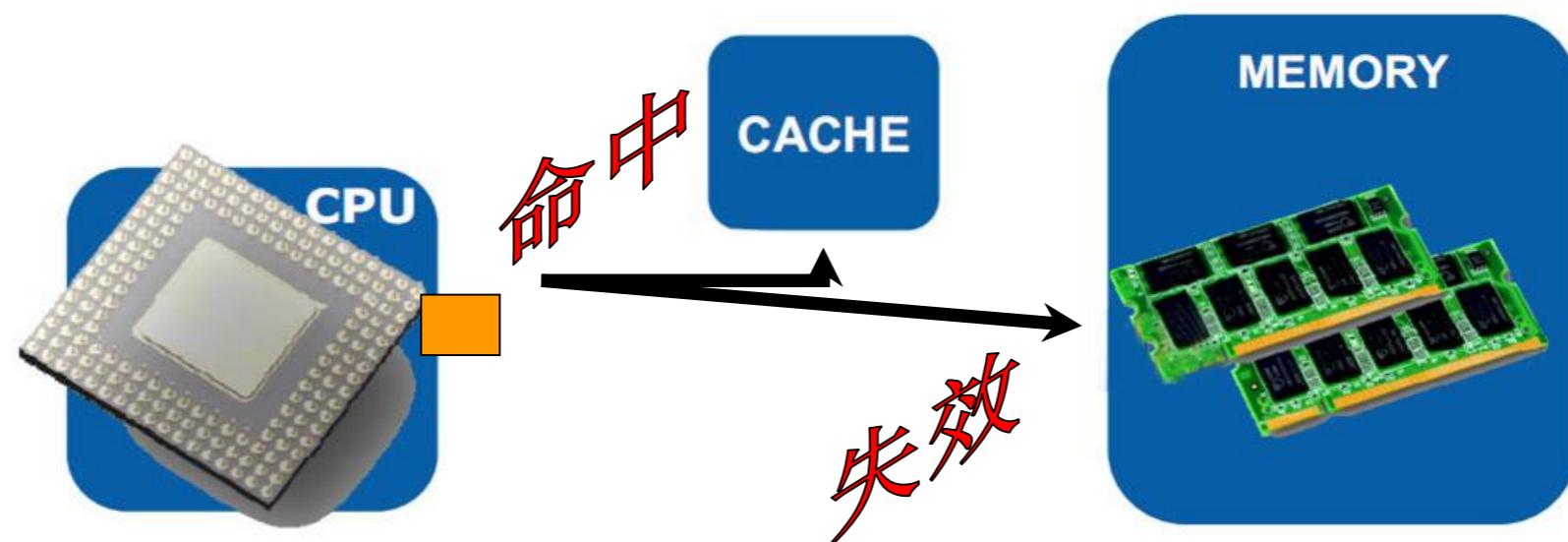
3.2 功耗攻击原理与实例分析

3.3 Cache攻击原理与实例分析

3.3 Cache攻击原理与实例分析

(1) 基本原理

利用密码访问Cache命中和失效产生的时间、功耗（电磁等）旁路泄露差异进行密钥破解。



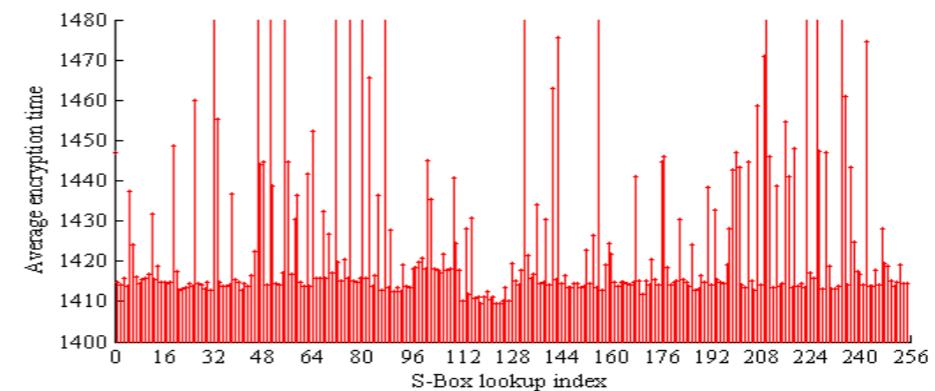
一般来说，Cache命中所需的时间短、功耗（电磁辐射）小。

3.3 Cache攻击原理与实例分析

(2) 信息泄露分类

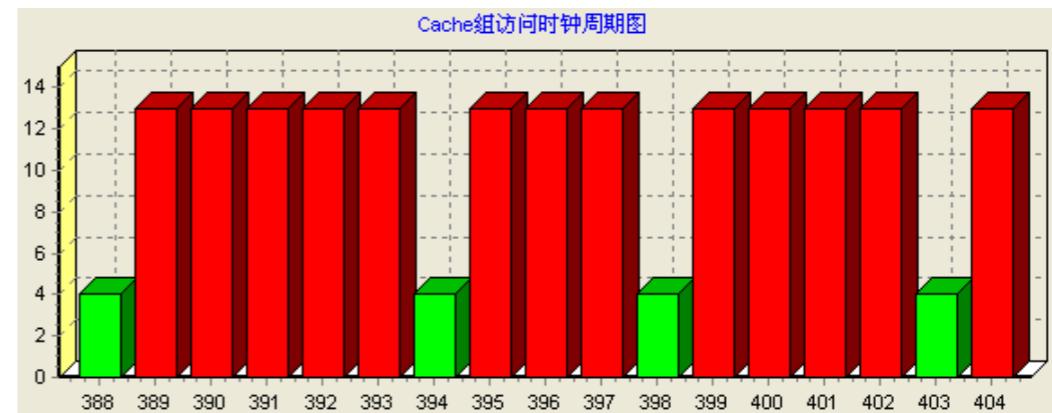
时序驱动攻击

测量密码整体执行时间



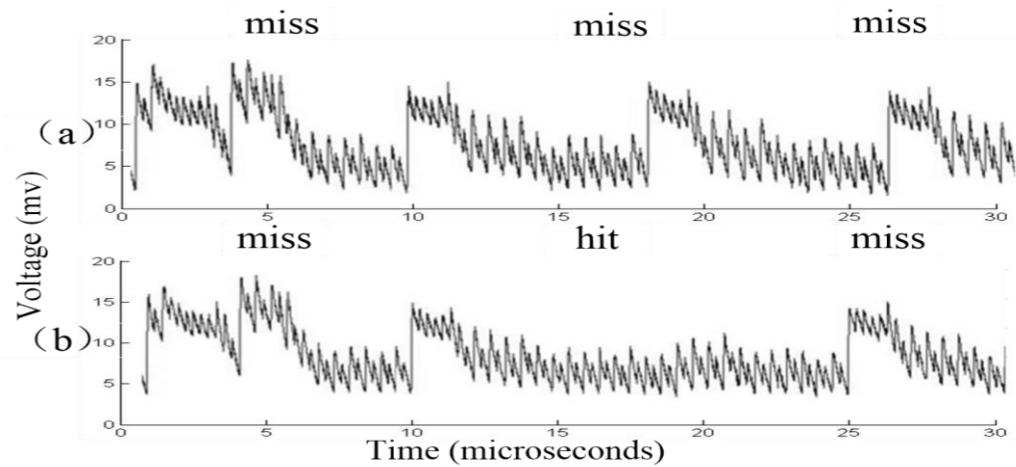
访问驱动攻击

采集密码访问Cache组地址



踪迹驱动攻击

采集密码执行踪迹

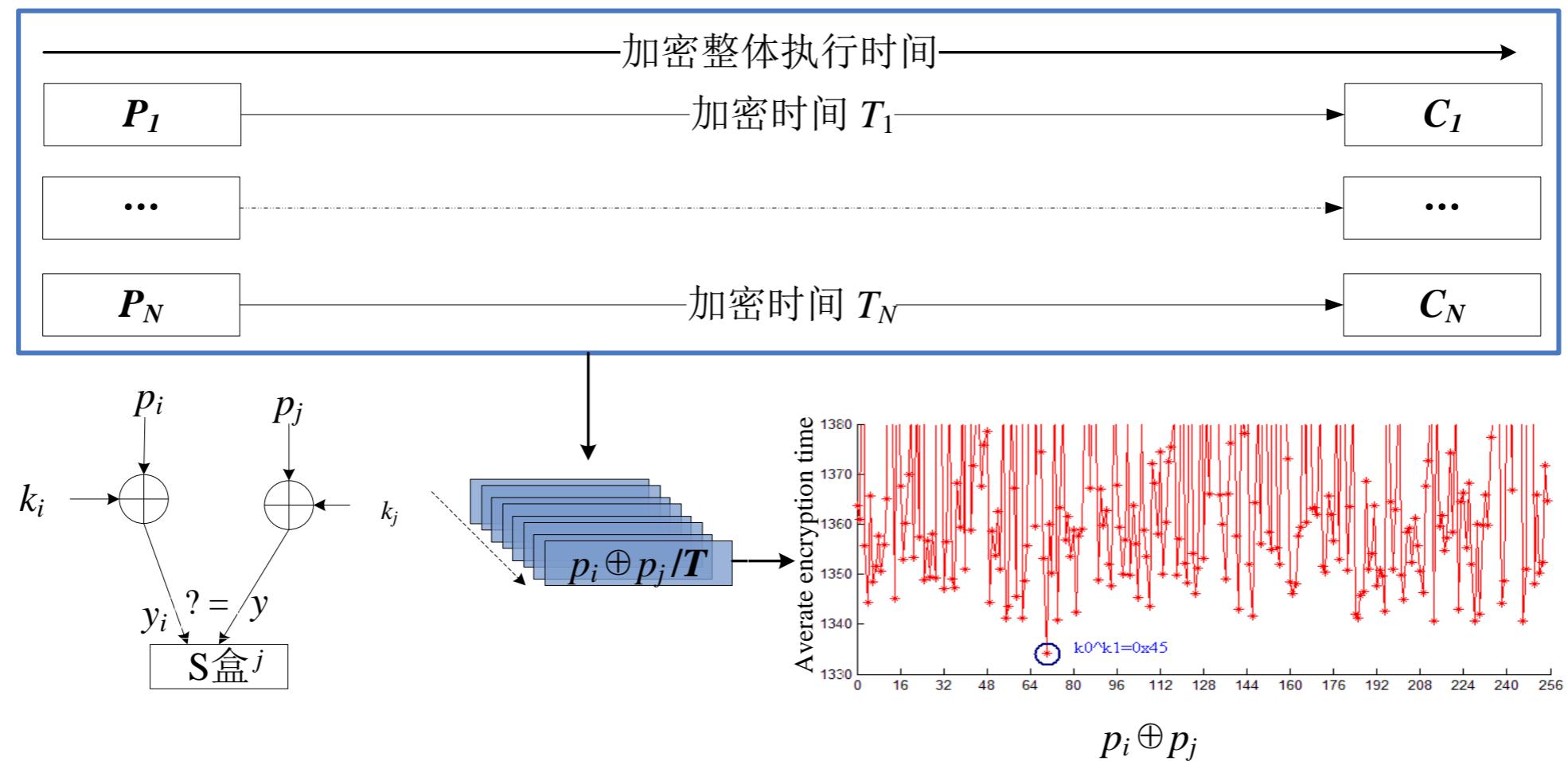


3.3 Cache攻击原理与实例分析

(3) 密钥分析方法

1) Cache碰撞计时分析（时序驱动Cache攻击）

利用密码算法两次查同一个表时第二次访问产生的Cache命中和失效对密码整体执行时间差异的影响来进行密钥分析。

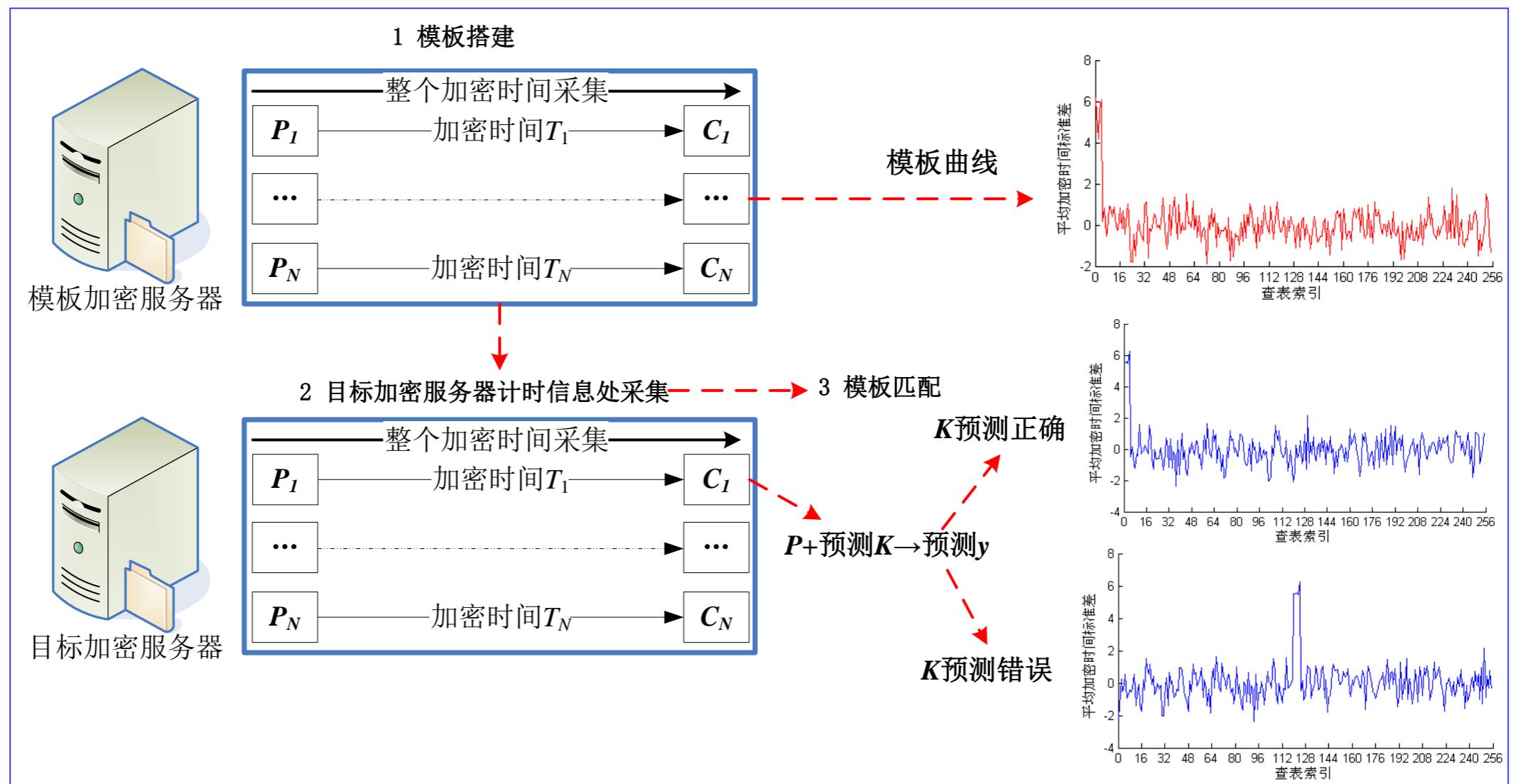


3.3 Cache攻击原理与实例分析

(3) 密钥分析方法

2) Cache计时模板分析（时序驱动Cache攻击）

密码加密查找表访问不同索引的执行时间差异可以建立模板，可通过观测整体执行时间得到该模板，并进行密钥分析。

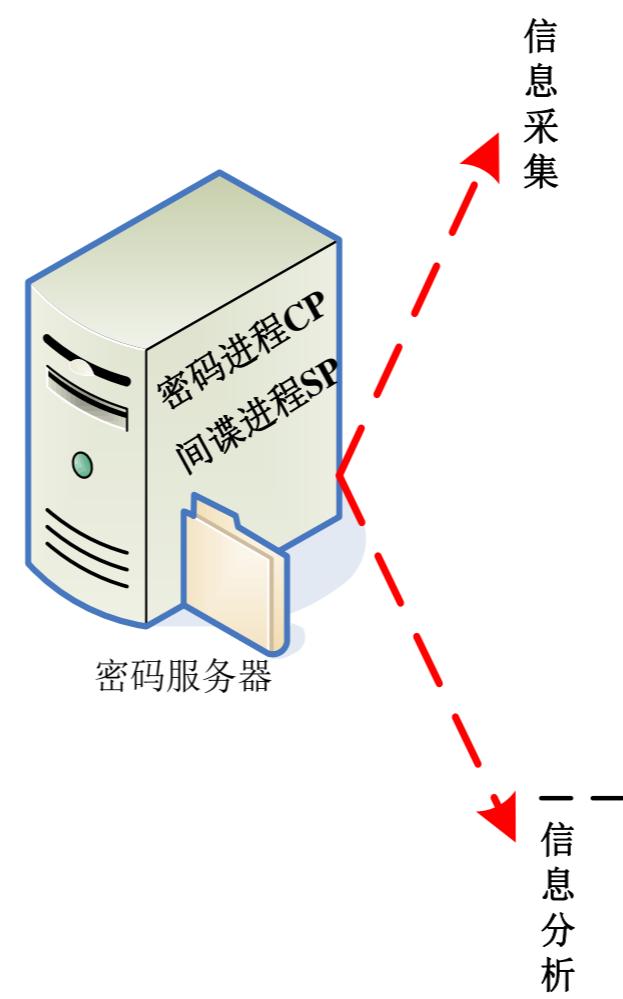


3.3 Cache攻击原理与实例分析

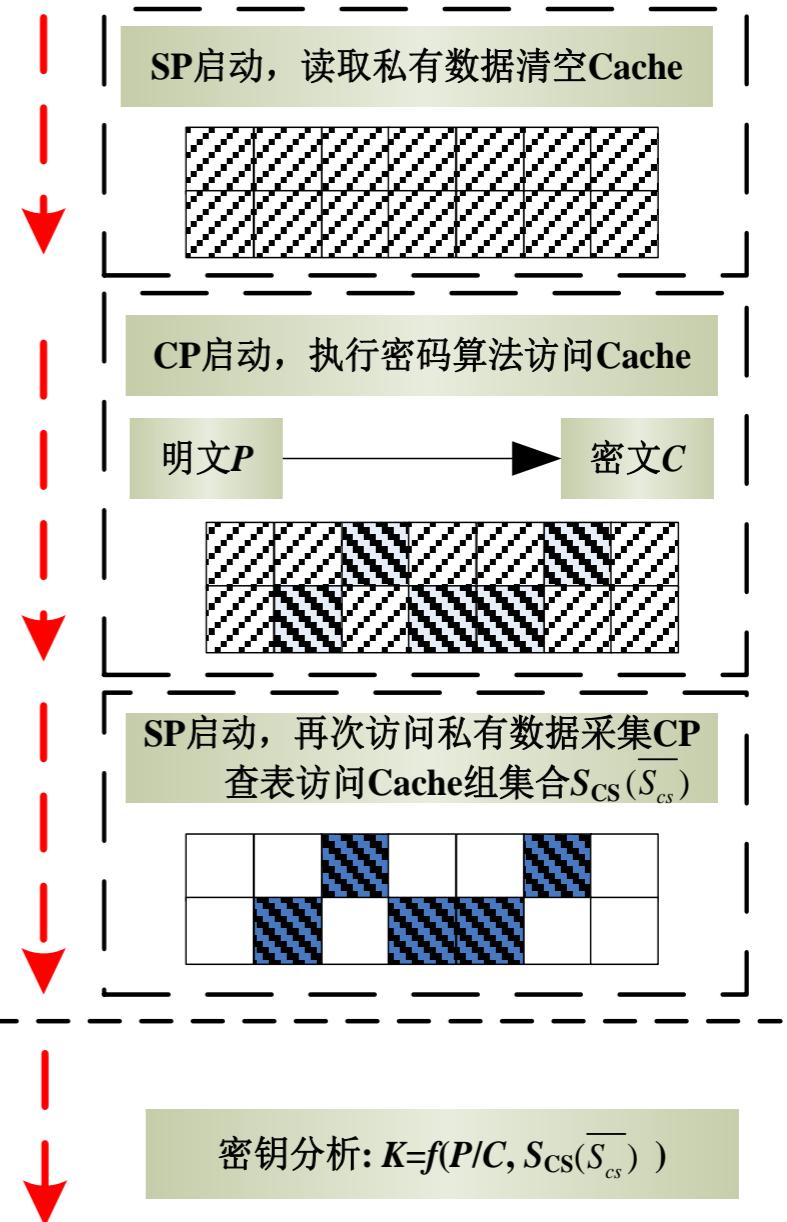
(3) 密钥分析方法

3) 访问驱动Cache分析

不同进程的数据有可能被映射到同一Cache组中，共享Cache存储空间。攻击者可设计间谍进程同密码进程同步执行，间谍进程通过对私有数据Cache访问发生的命中和失效事件来监测密码进程访问的Cache组地址，在此基础上进行密钥破解。



■ CP数据块 ■ SP数据块 □ 命中 ■ 失效

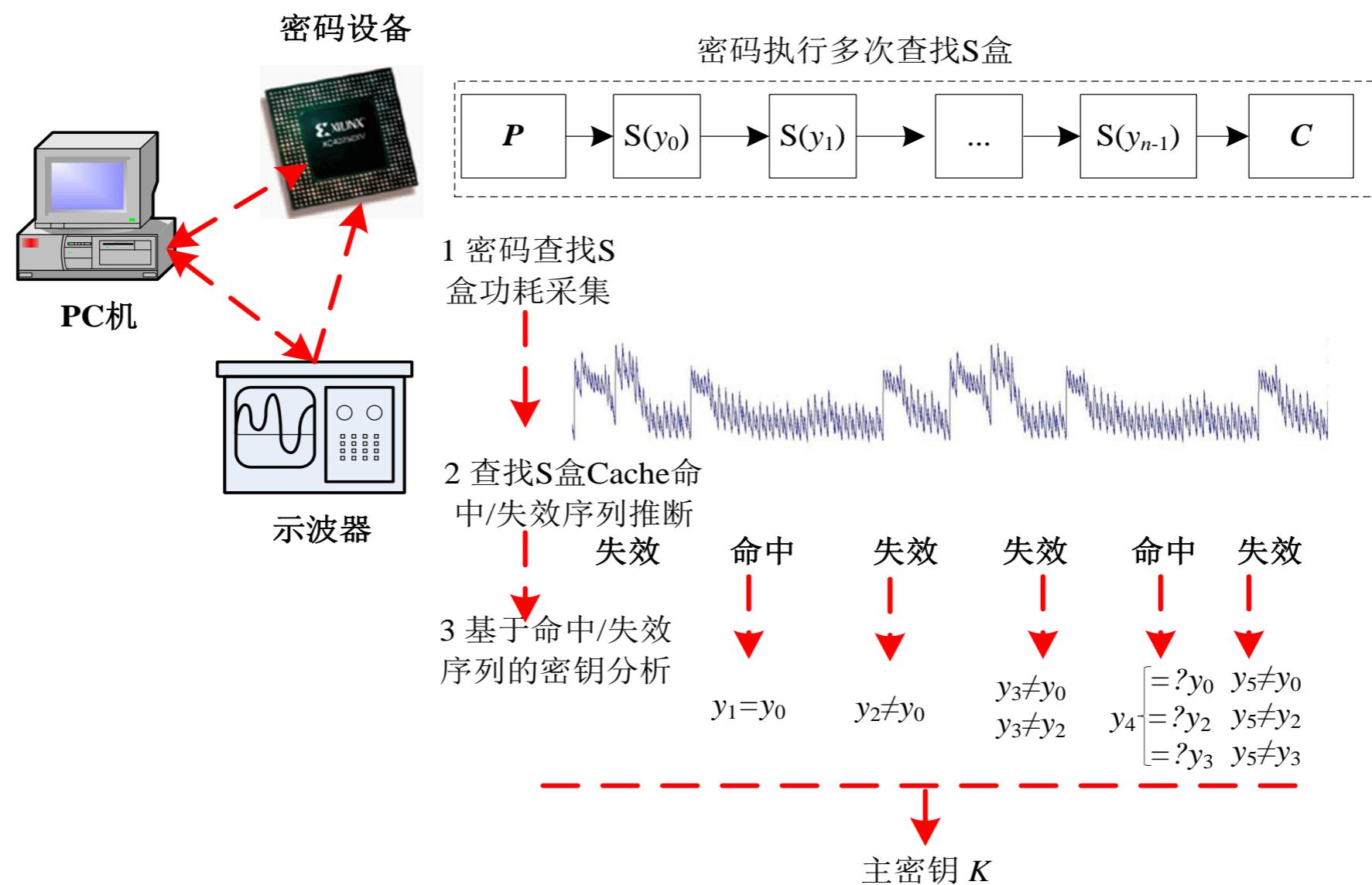


3.3 Cache攻击原理与实例分析

(3) 密钥分析方法

4) 基于Cache命中和失效踪迹的分组密码Cache分析

通过功耗/电磁手段推断出分组密码加密每次查表访问Cache的命中和失效序列，在此基础上进行密钥恢复。

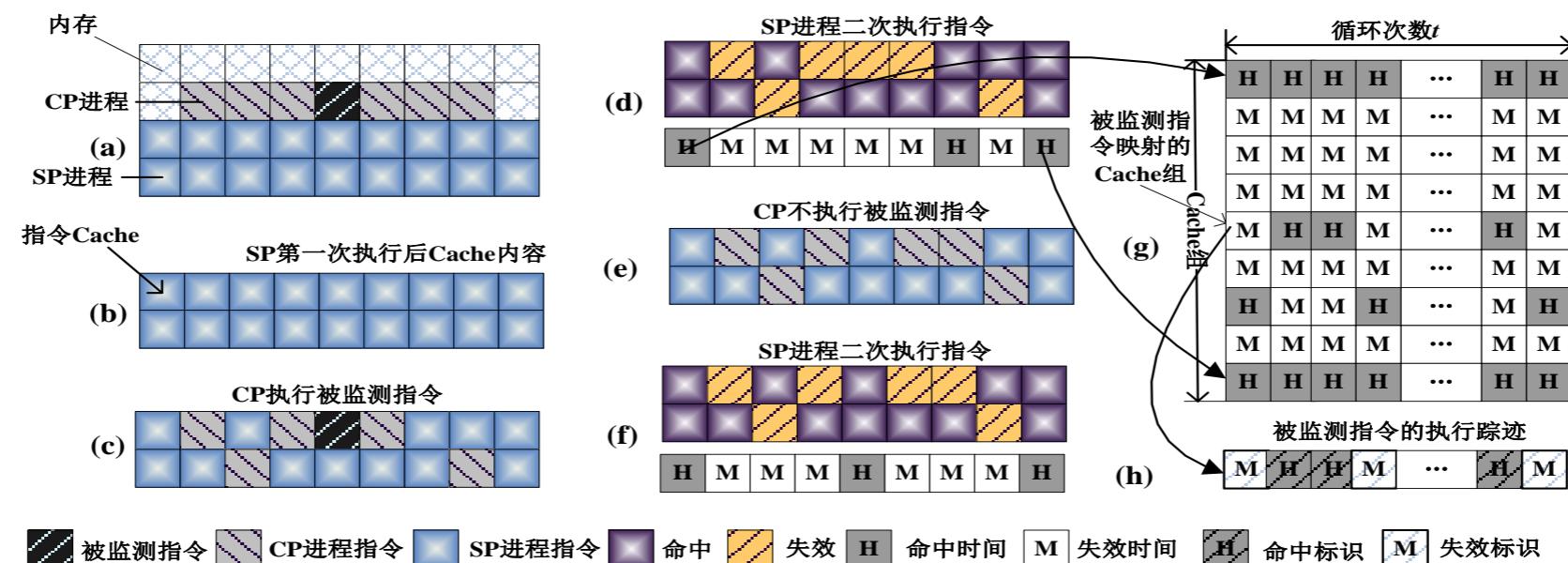


3.3 Cache攻击原理与实例分析

(3) 密钥分析方法

5) 基于平方和乘法踪迹的公钥密码Cache分析

通过访问驱动手段采集公钥密码加密平方和乘法操作序列，在此基础上进行密钥恢复。



密钥序列

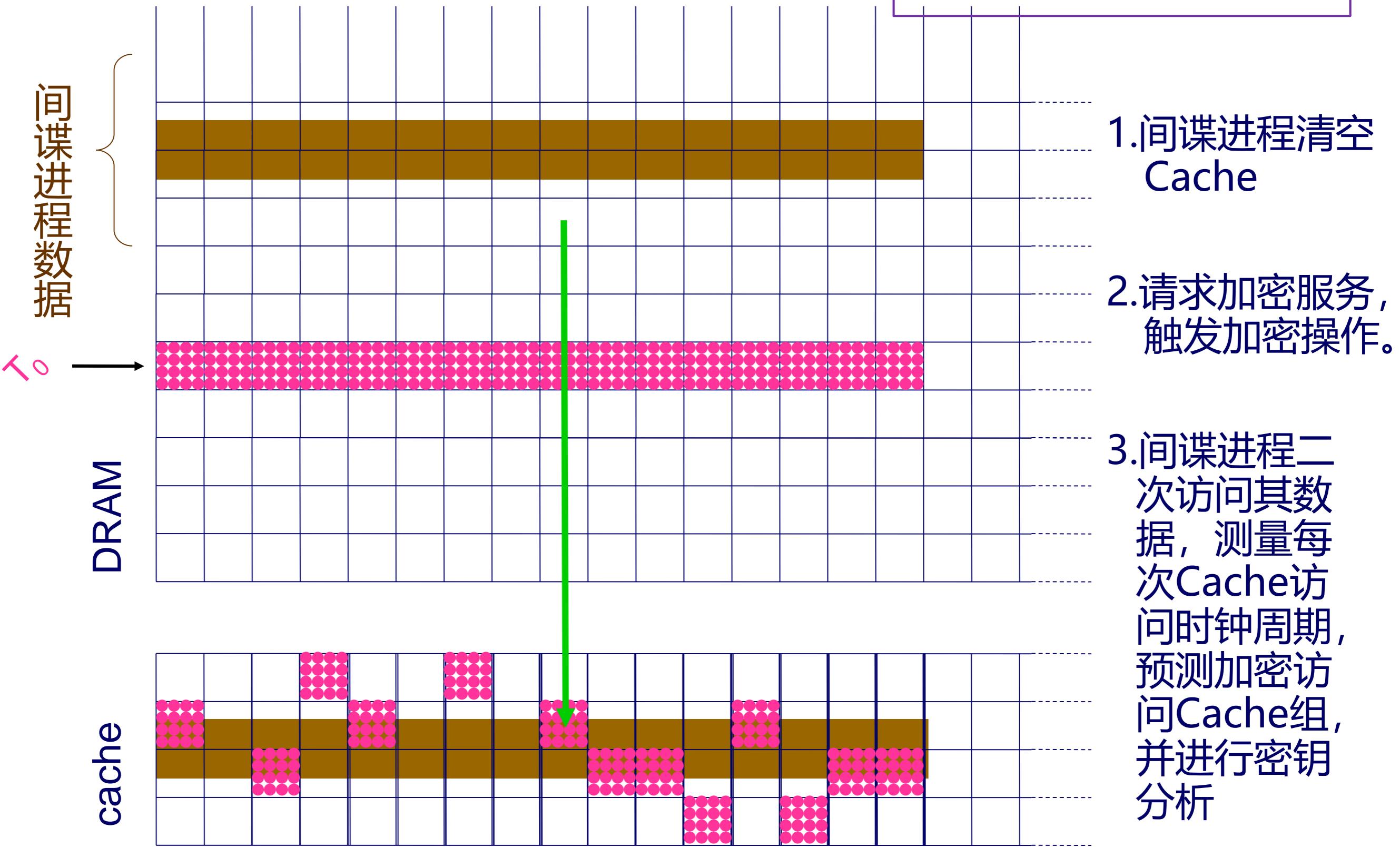
1	0	1	1	0	1	0	1	1	0
---	---	---	---	---	---	---	---	---	---

平方乘法
序列

SM	S	SM	SM	S	SM	S	SM	SM	S
----	---	----	----	---	----	---	----	----	---

3.3 Cache攻击原理与实例分析

(4) 访问驱动攻击示例



3.3 Cache攻击原理与实例分析

(4) 访问驱动攻击示例

AES密码访问驱动Cache攻击

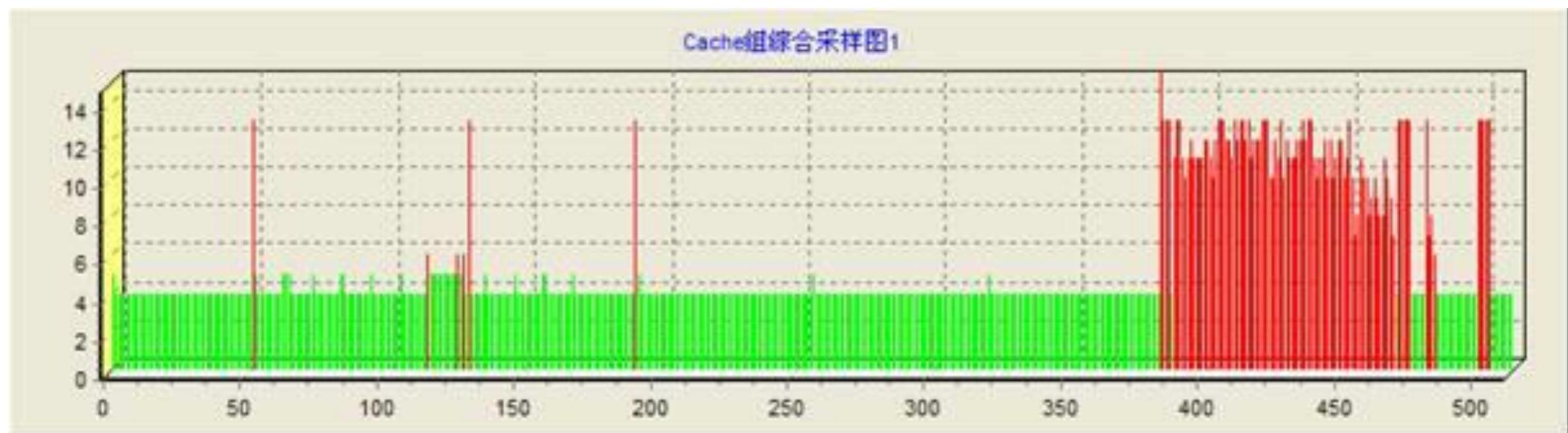


设定待攻击的密钥

3.3 Cache攻击原理与实例分析

(4) 访问驱动攻击示例

AES密码访问驱动Cache攻击

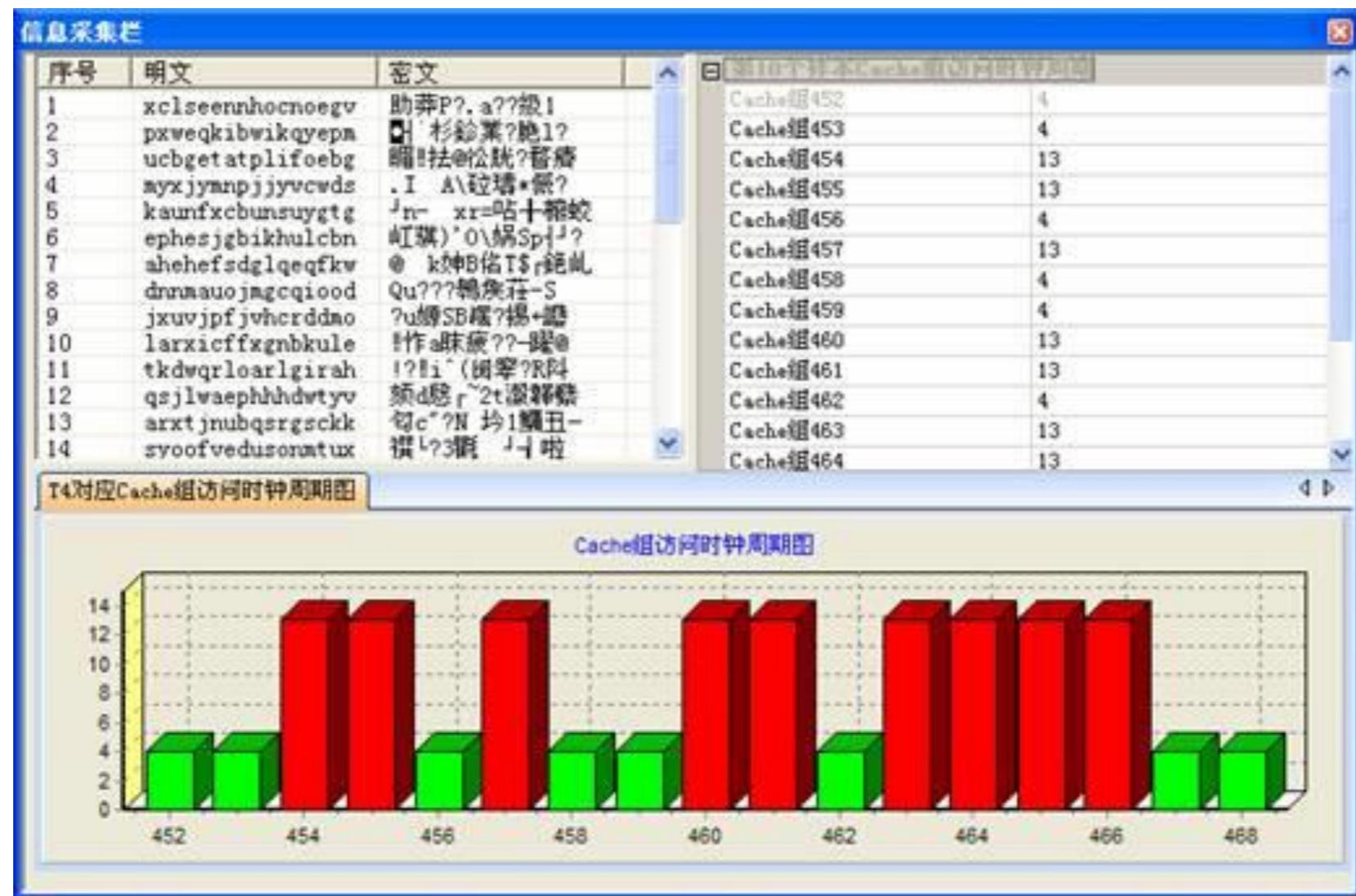


定位AES密码查找表在Cache中的位置

3.3 Cache攻击原理与实例分析

(4) 访问驱动攻击示例

AES密码访问驱动Cache攻击

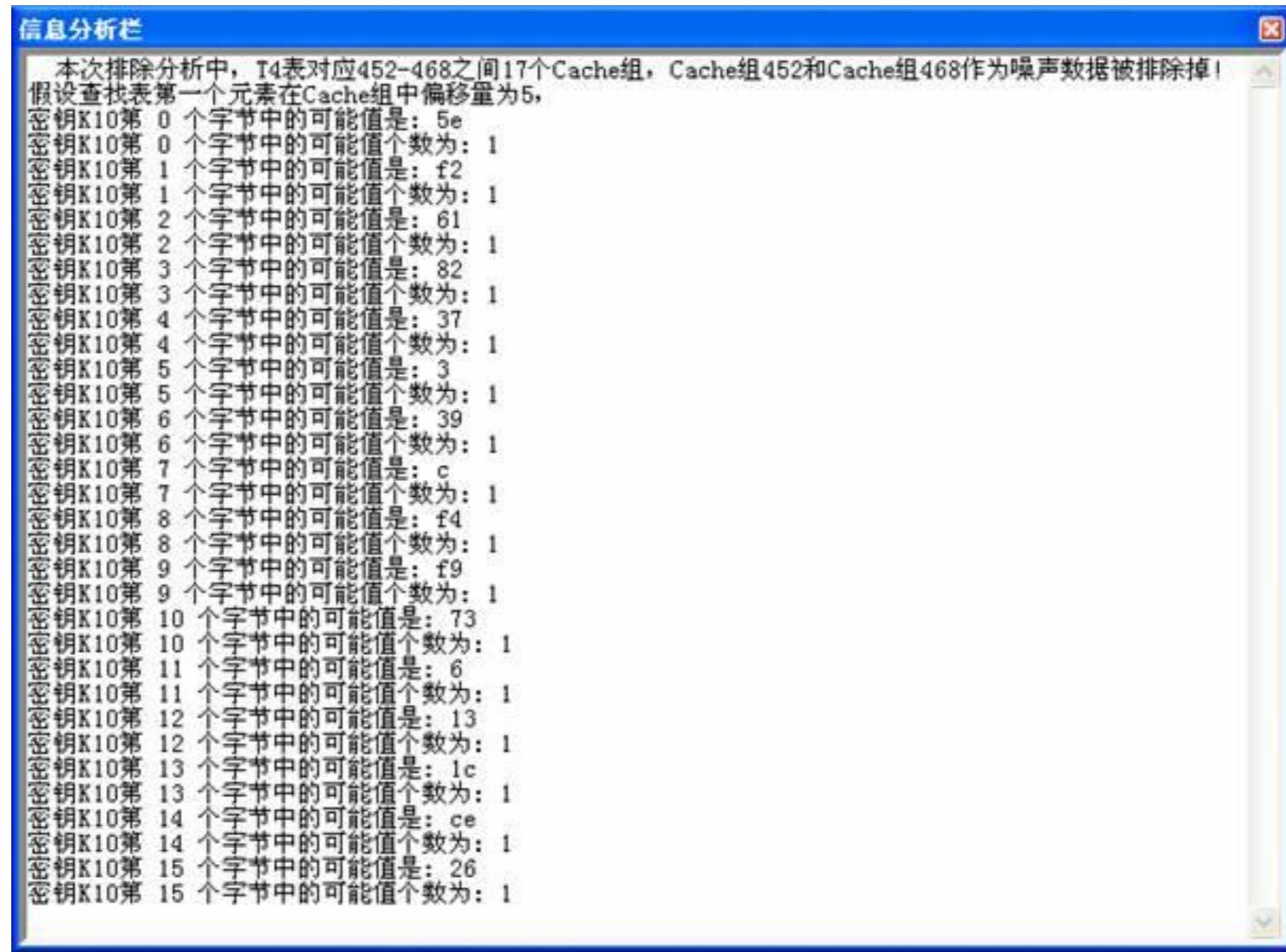


采集某次加密AES密码查表访问的Cache组集合
绿色表示加密没有访问过的Cache组地址

3.3 Cache攻击原理与实例分析

(4) 访问驱动攻击示例

AES密码访问驱动Cache攻击

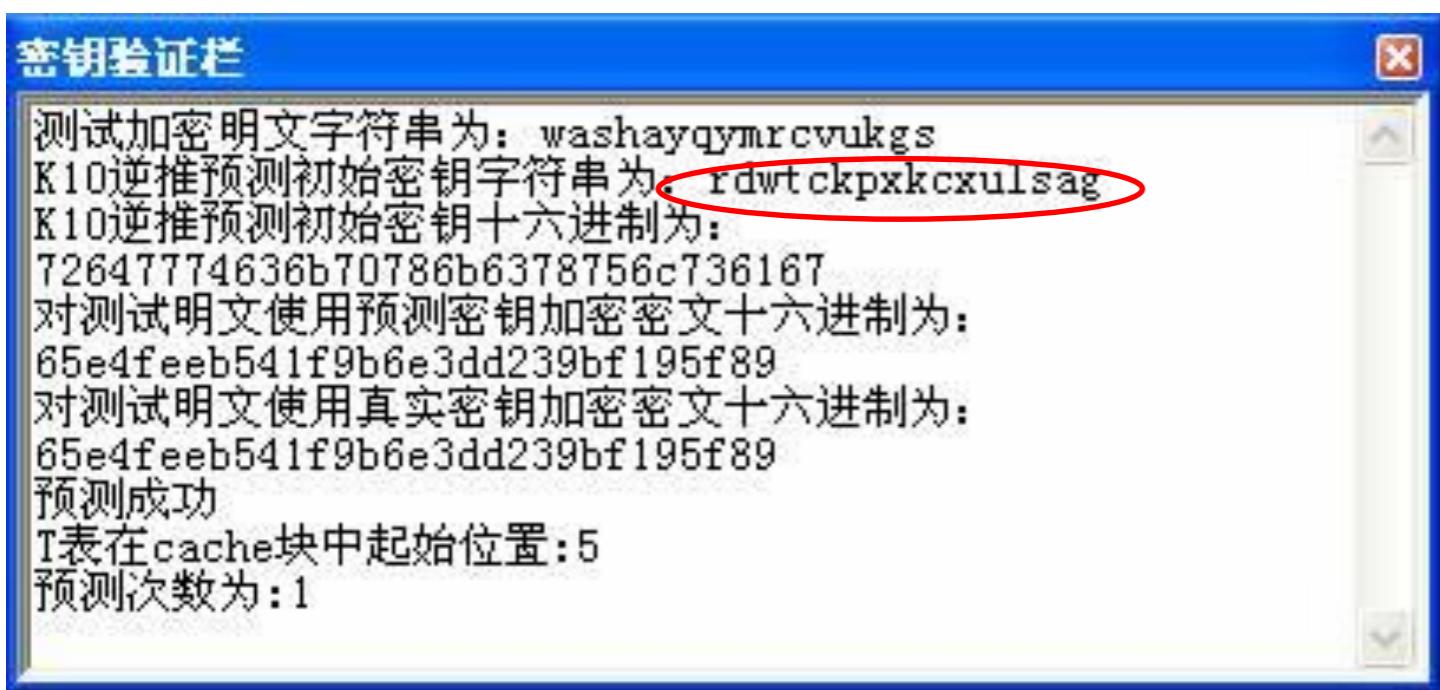


将AES16个字节的密钥分别恢复出来

3.3 Cache攻击原理与实例分析

(4) 访问驱动攻击示例

AES密码访问驱动Cache攻击

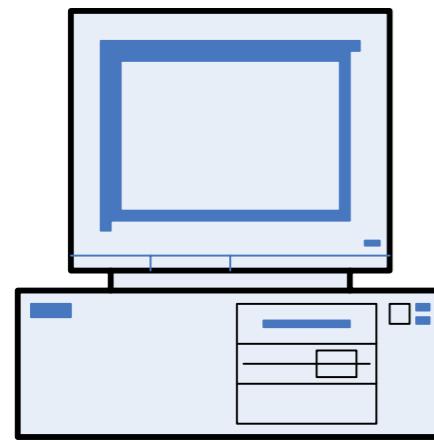


密钥正确性验证

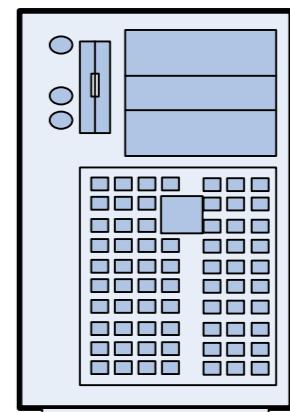
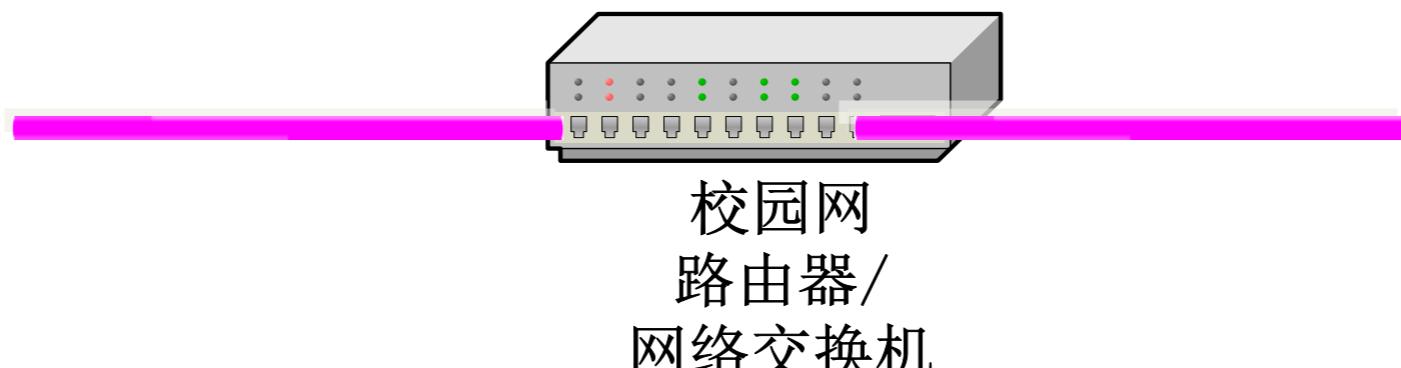
3.3 Cache攻击原理与实例分析

(4) 访问驱动攻击示例

远程攻击也可成功实现



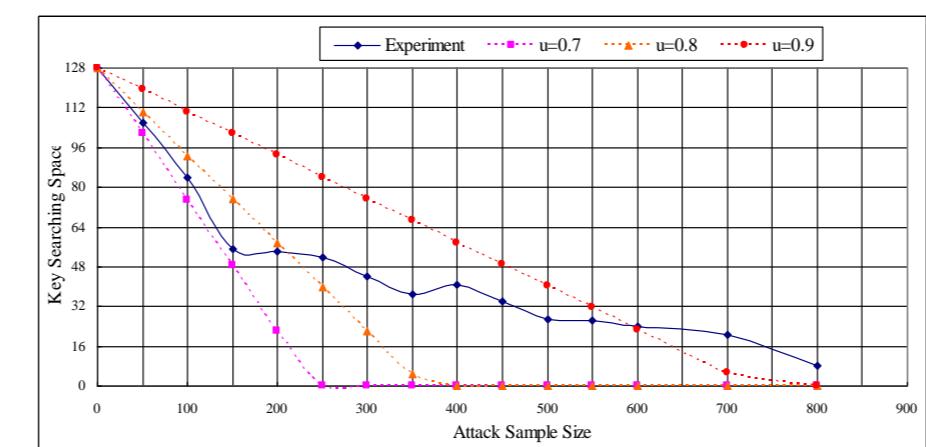
攻击端



密码服务器



校园风光



AES第一轮攻击, 750个样本



3.3 Cache攻击原理与实例分析

(5) 攻击总结

攻击优
点

- 适用于使用了Cache的各种软件实现。
- 攻击可利用时间、功耗、电磁等多种旁路泄露。

攻击难
点

- Cache访问命中和失效的高精度采集。
- 网络传输时延、发包/拆包给攻击带来的噪声。
- 间谍进程如何在一次密码加密过程中多次采集泄露

防御方
法

- 在密码执行前进行Cache预热。
- 在密码执行前插入随机时延。
- 密码加密不再访问Cache，如Intel推出的AES-NI设计



3.1 计时攻击原理与实例分析

3.2 功耗攻击原理与实例分析

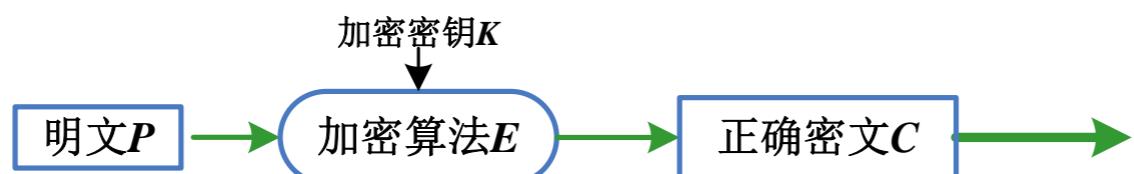
3.3 Cache攻击原理与实例分析

3.4 故障攻击原理与实例分析

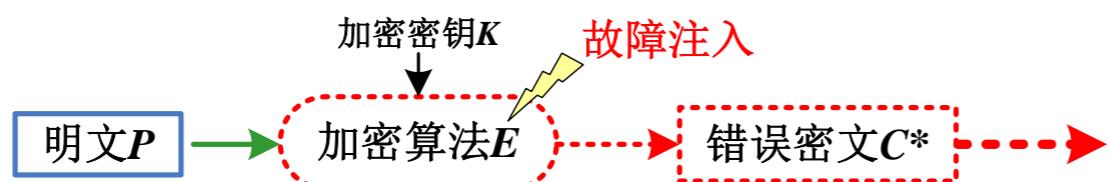
3.4 故障攻击原理与实例分析

(1) 基本原理

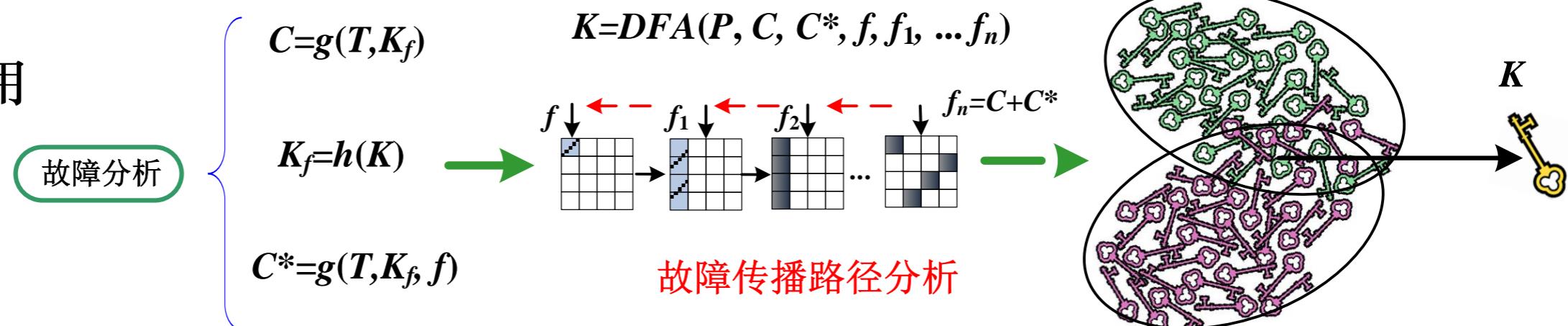
通过修改密码芯片工作条件使得其产生故障进行密钥恢复。



故障注入



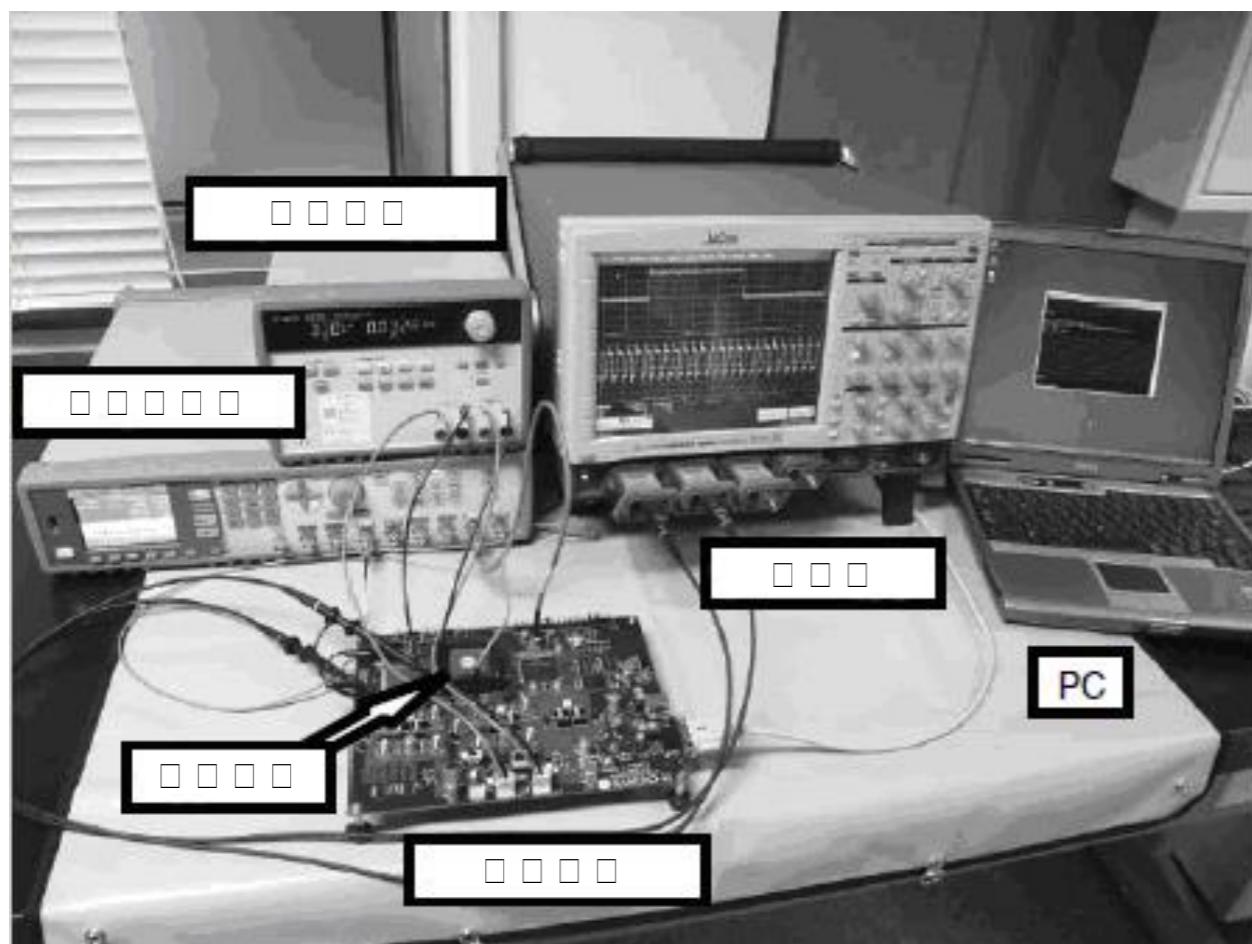
故障利用



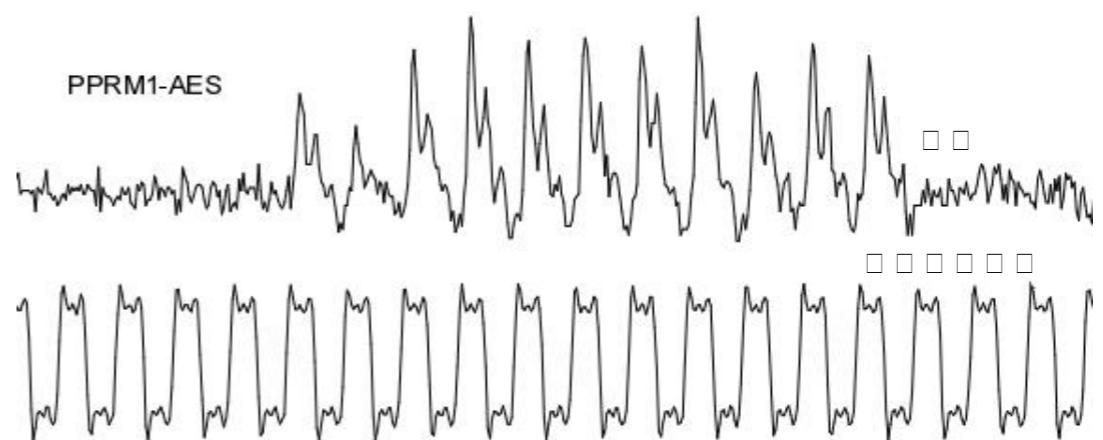
3.4 故障攻击原理与实例分析

(2) 故障注入

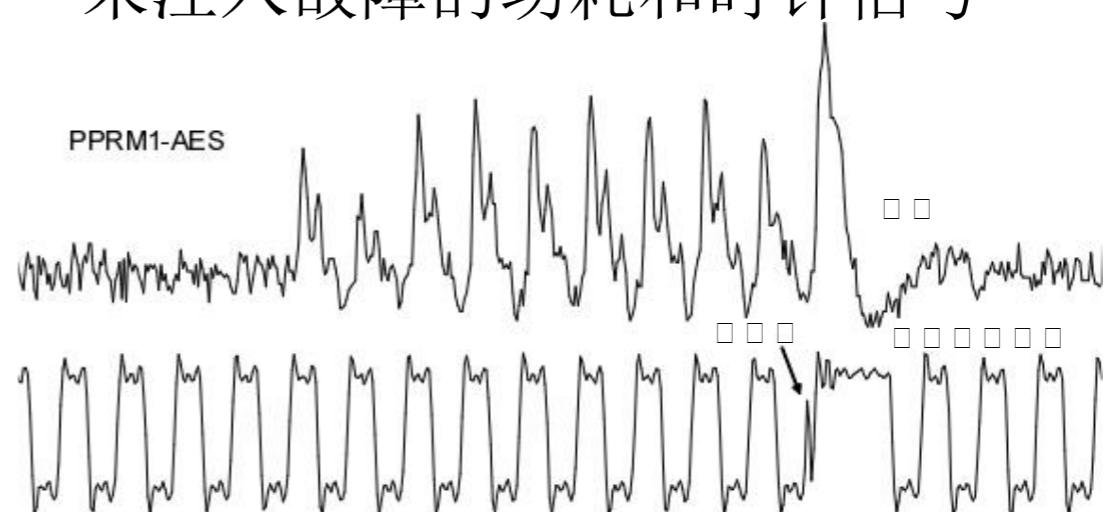
非侵入式故障注入



触发“脉冲产生器”在加密某时刻产生高于密码板卡正常工作频率的脉冲



未注入故障的功耗和时钟信号



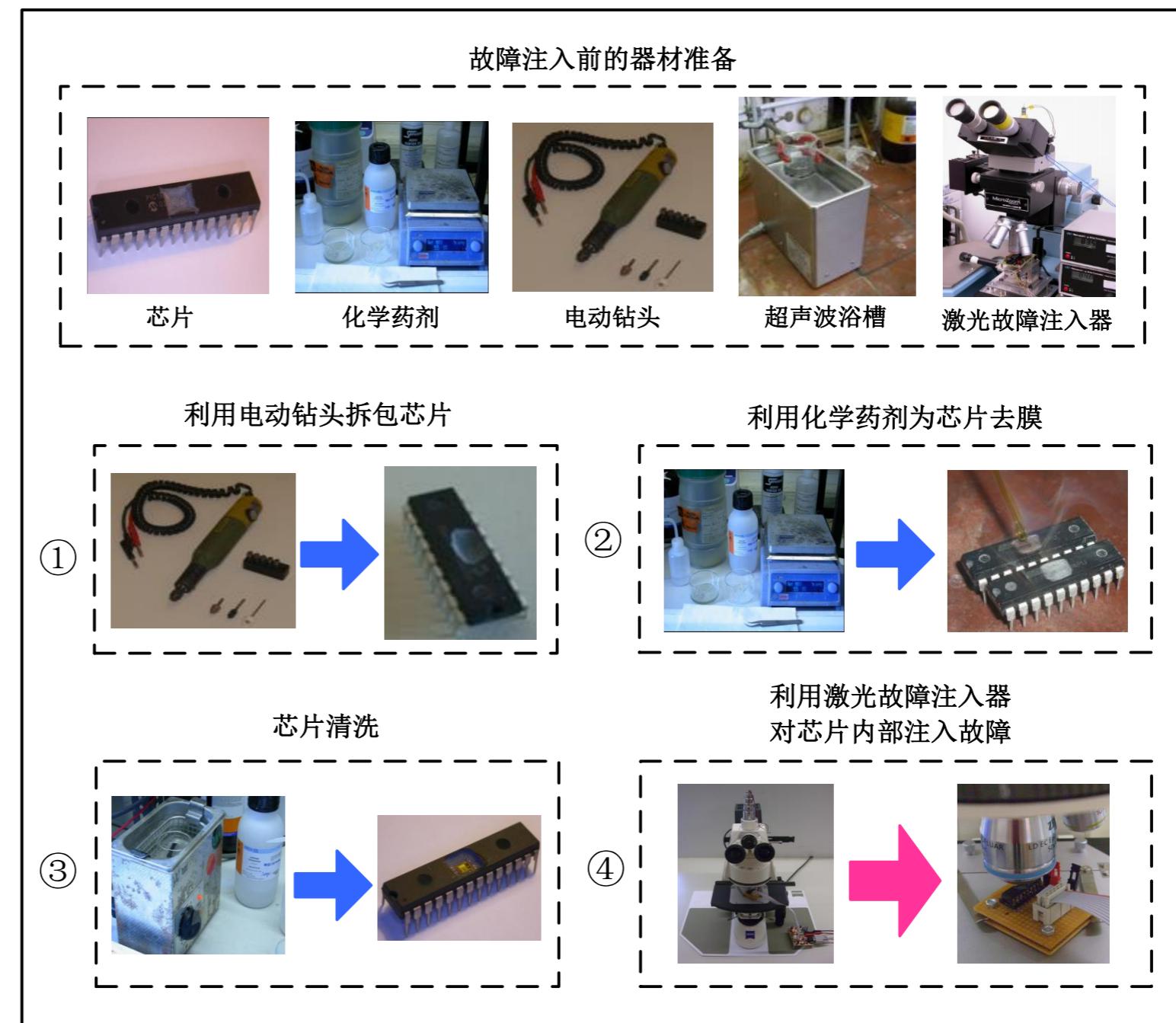
注入故障的功耗和时钟信号

3.4 故障攻击原理与实例分析

(2) 故障注入

半侵入式故障注入

需要直接接触设备，但是**不损害设备的钝化层**，如通过激光手段注入故障。

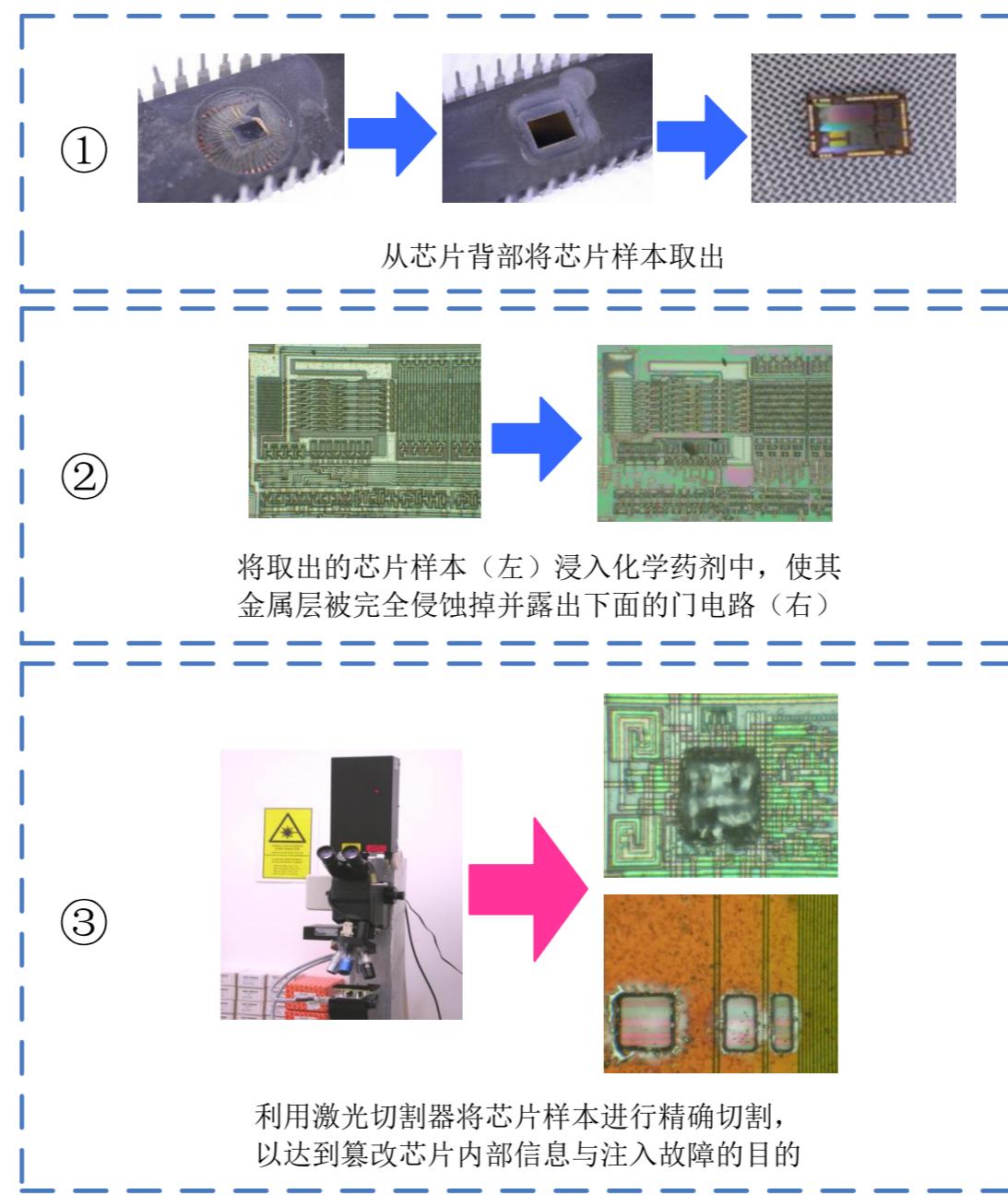


3.4 故障攻击原理与实例分析

(2) 故障注入

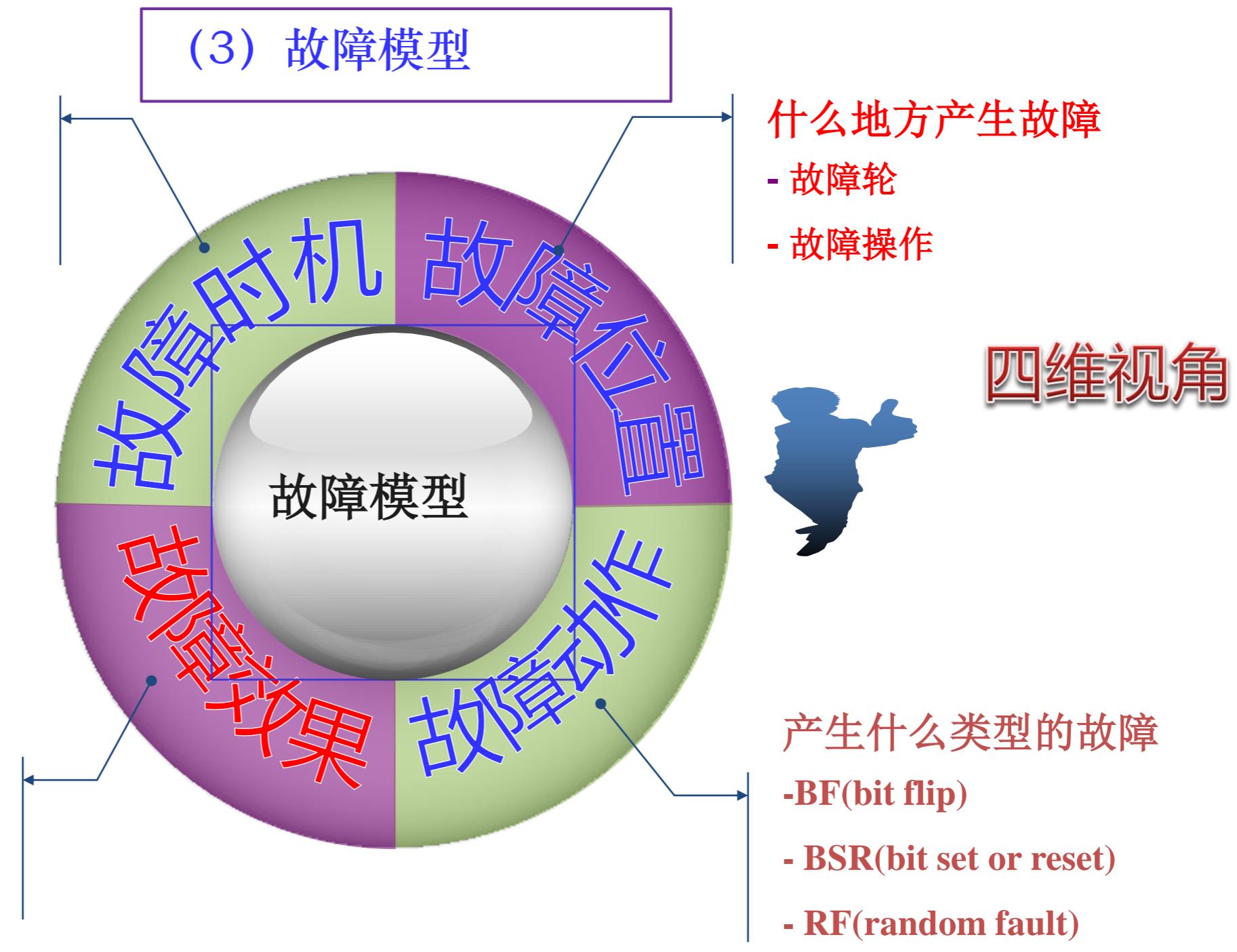
侵入式故障注入

在半侵入式故障注入的基础上，对密码芯片进行更深一层的剖片，去除门电路上面的金属层，使得每个门电路都能够裸露出来，再进行进一步的故障注入。



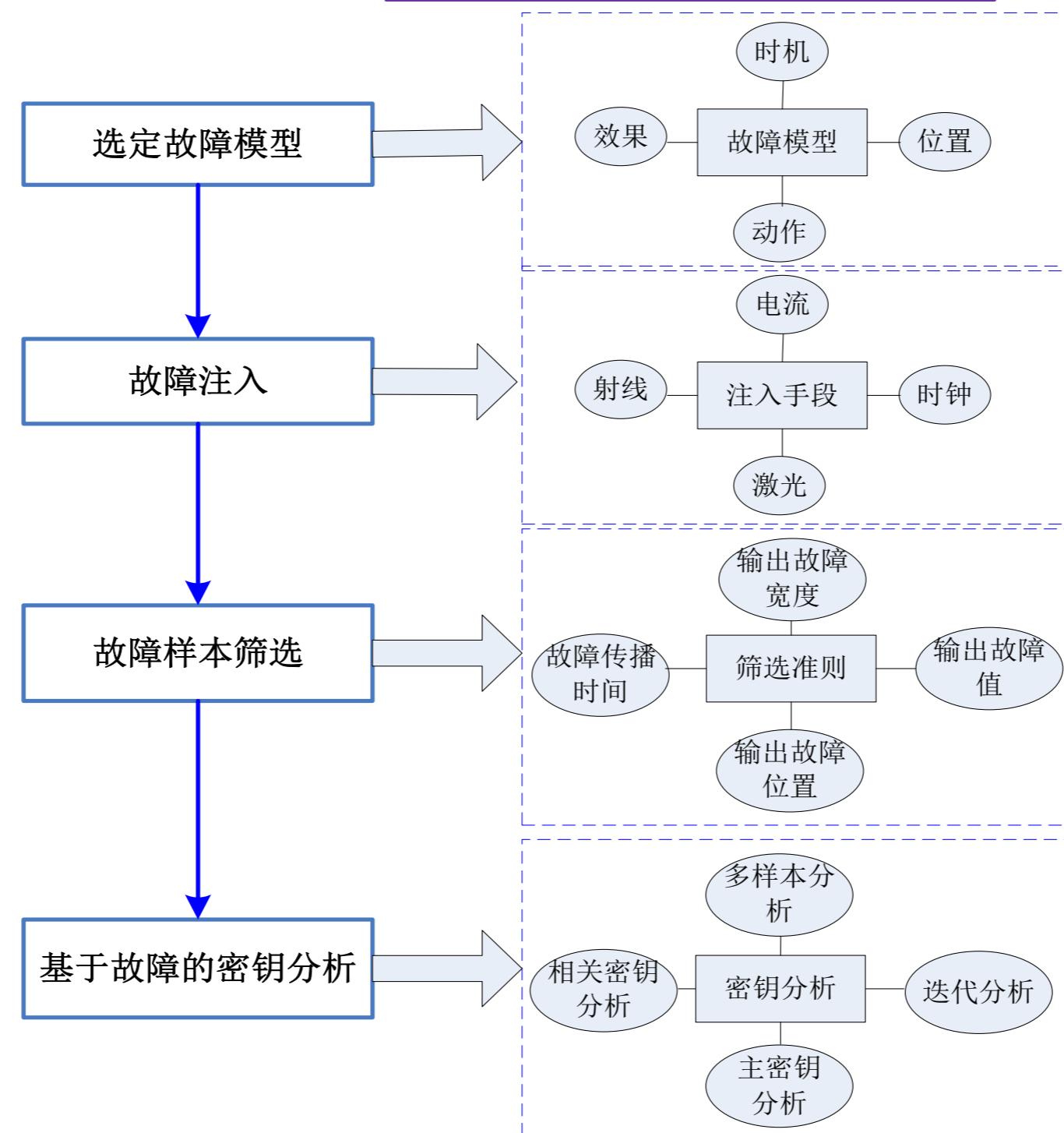
3.4 故障攻击原理与实例分析

什么时候产生故障
-运算在某个指定步骤
-运算在某个指定范围



3.4 故障攻击原理与实例分析

(4) 故障分析流程



3.4 故障攻击原理与实例分析

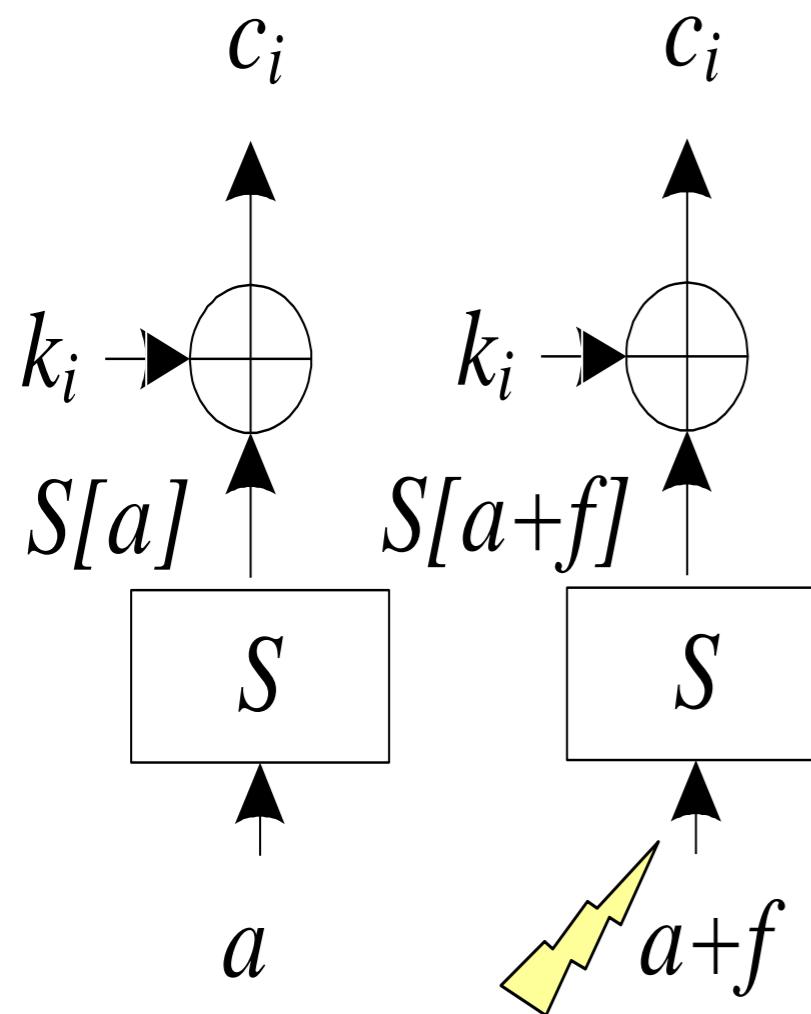
(5) 分组密码故障分析方法

将分组密码故障分析归结为求解查找S盒输入和输出故障差分问题。

$$S[a] \oplus S[a + f] = f'$$



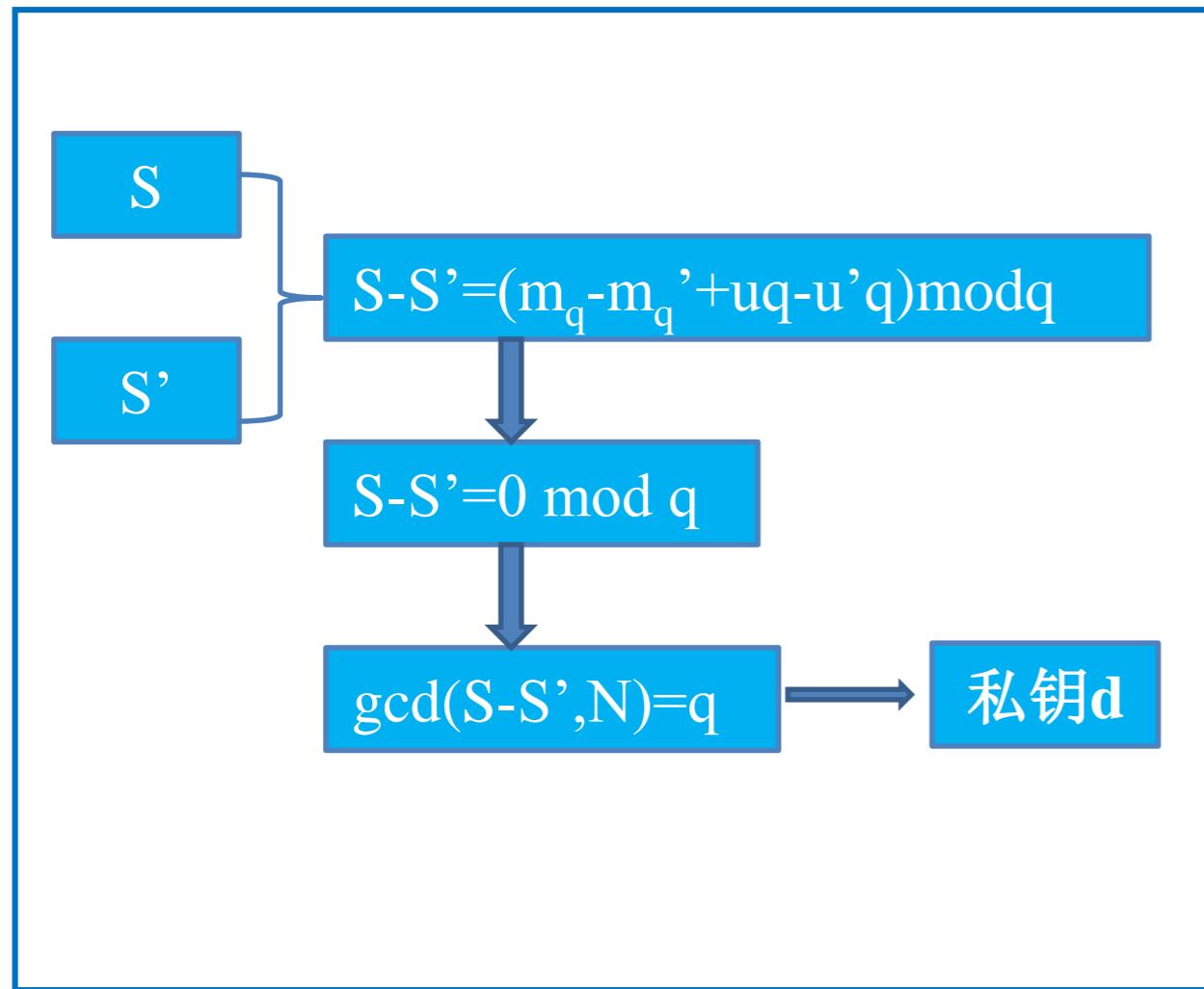
问题本质抽取：S盒输出差分 f' 一般可从密文差分得到，关键在于计算S盒输入差分 f ，根据上式得到 a 的值，并结合密文分析进一步得出密钥 k_i 。



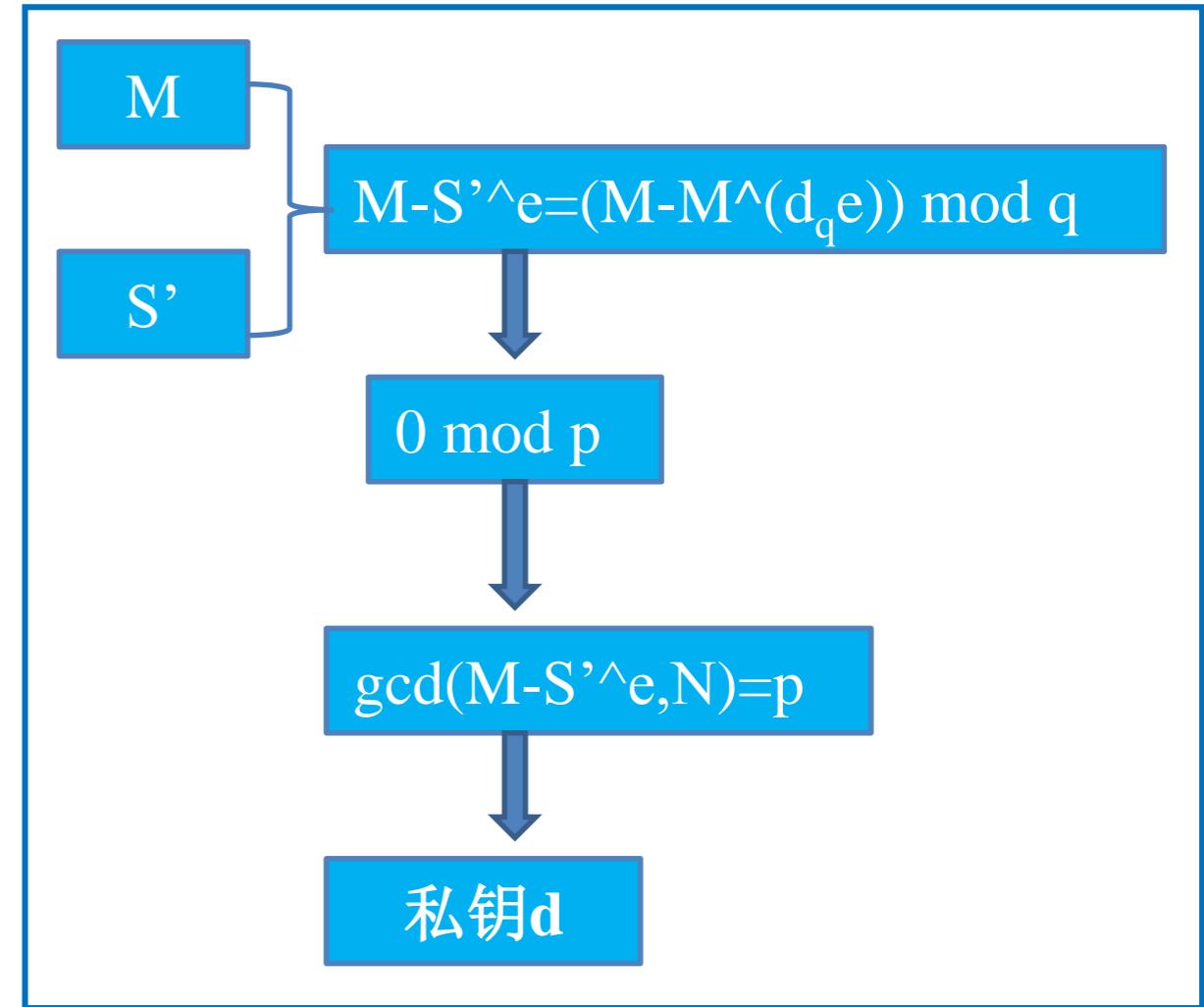
3.4 故障攻击原理与实例分析

(6) 公钥密码故障分析方法

一次RSA正确和故障签名即可恢复密钥。



一次RSA故障签名即可恢复密钥。



基于故障公式推导的密钥恢复

3.4 故障攻击原理与实例分析

(7) AES密码故障分析示例

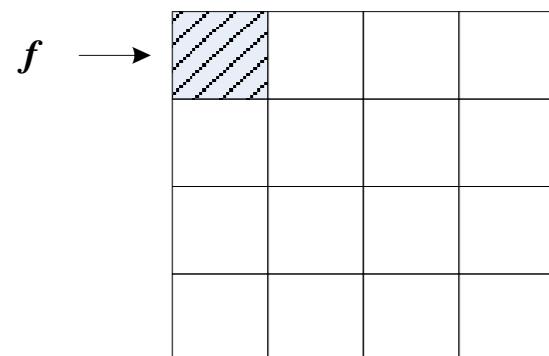
- (1) 攻击者能够选择一个明文P并对其进行AES加密，得到正确密文C；
- (2) 攻击者选择同样一个明文P，在AES加密第8轮字节代换过程中导入单字节随机故障 f , f 位置和数值未知，得到错误密文 C^* .
- (3) 攻击者根据正确密文C和错误密文 C^* ,利用分组密码故障分析模型，得到AES加密第10轮查找S盒输入有限候选值；
- (4) 多次执行步骤 (1) – (3) , 恢复AES加密第10轮查找S盒输入值，结合密文计算出最后一轮扩展密钥 K_{10} ，然后经密钥逆推恢复初始密钥。

3.4 故障攻击原理与实例分析

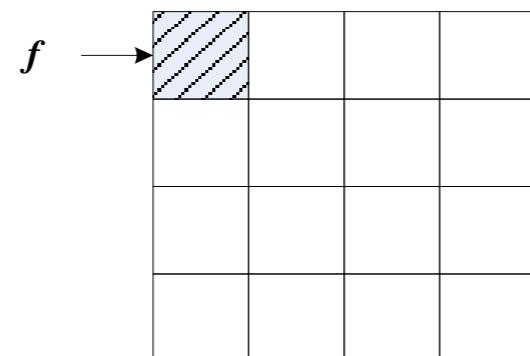
(7) AES密码故障分析示例

第八轮单字节故障传播示意图

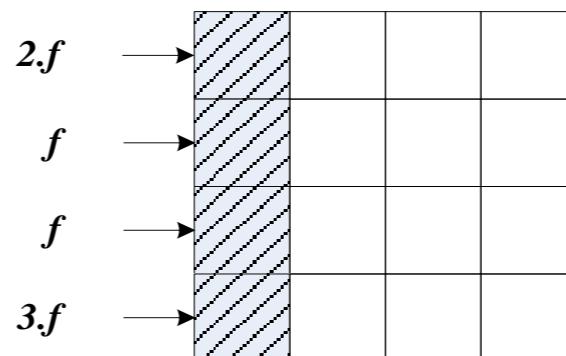
第8轮字节代换



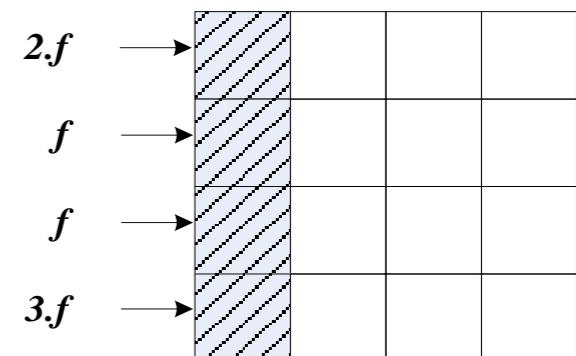
第8轮行移位



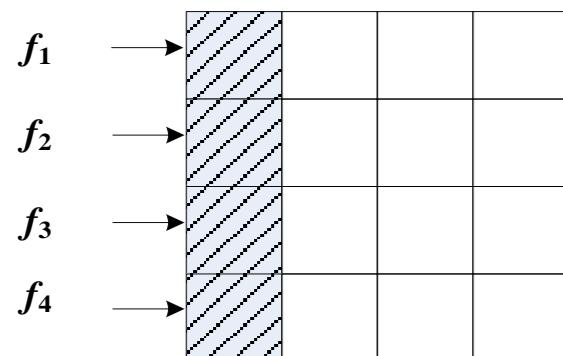
第8轮列混淆



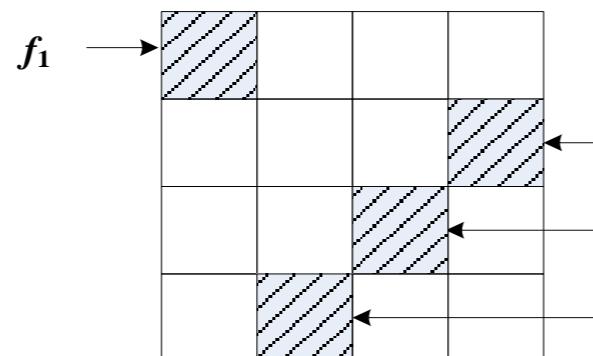
第8轮和轮密钥加



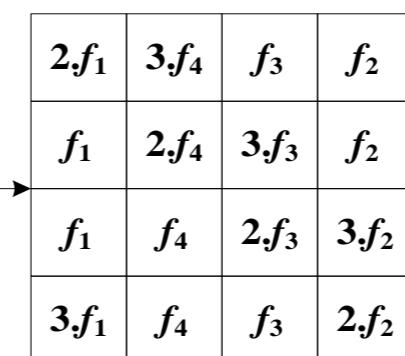
第9轮字节代换



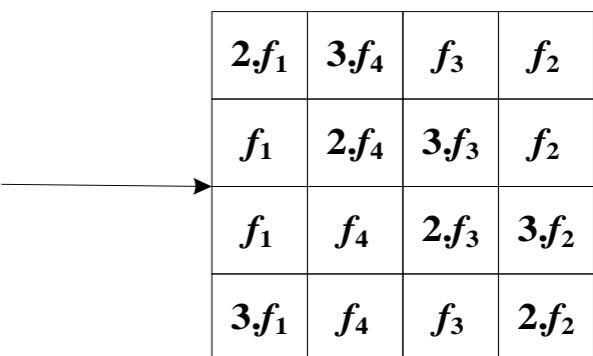
第9轮行移位



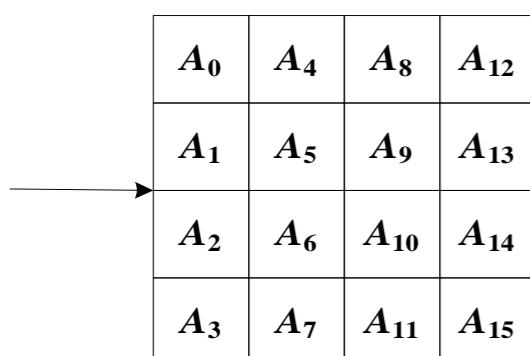
第9轮列混淆



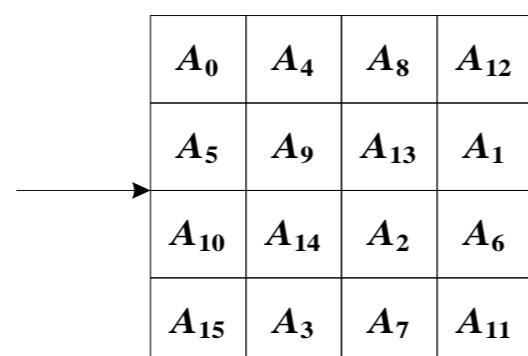
第9轮和轮密钥加



第10轮字节代换



第10轮行移位



第10轮和轮密钥加



3.4 故障攻击原理与实例分析

(7) AES密码故障分析示例

K^{10} 密钥空间 2^{128}

通过在第8轮第1个字节导入1次故障，可恢复240个 K_0^{10} , K_{13}^{10} , K_{10}^{10} , K_7^{10} 组合值，
 240个 K_8^{10} , K_5^{10} , K_2^{10} , K_{15}^{10} 组合值，
 240个 K_{12}^{10} , K_9^{10} , K_{14}^{10} , K_6^{10} , K_3^{10} 组合值。

如果再次对该字节导入1次故障，又分别恢复四组组合值，
 由于正确的 K^{10} 组合值肯定在这两次故障分析得到的密钥组合
 值集合中，那么这两次故障分析得到的对应密钥组合值集合
 的交集即为正确的密钥组合值，经分析即可恢复极其有限的
 密钥组合值，如图所示。

实验中，一般可直接获取唯一的密钥组合值，然后再经密
 钥逆推可恢复初始密钥K。

3.4 故障攻击原理与实例分析

(7) AES密码故障分析示例

任意选择明文和加密密钥如下：

明文 P : 69 77 78 79 73 6a 6c 71 6c 79 69 65 6f 77 74 69

加密密钥 K : 71 67 71 74 61 63 76 70 71 67 76 68 76 6d 67 6d

攻击实验数据如下：

正确密文 C : 73 88 03 4b 28 2b 84 e0 7d ef 8c f2 0d 3c ea 38

第1个错误密文 C^*1 : 49 b0 34 12 08 2d e0 42 e3 19 90 a5 c7 cf 88 5a

第2个错误密文 C^*2 : d8 4c 45 dc 13 e8 a8 f0 94 23 b1 38 aa 59 e2 d3

恢复 K_{10} 密钥: 79 aa cf 1a fb f9 24 a4 31 23 c8 ff ea 2d 98 85

恢复初始密钥 K : 71 67 71 74 61 63 76 70 71 67 76 68 76 6d 67 6d

第10轮字节 代换预测输 入差分值 ⁺	恢复密钥 字节 ⁺	候选值 ⁺
19 29 39 ⁺ 4a 50 54 ⁺ 70 7c 85 ⁺ 89 94 ad ⁺ ae d8 f5 ⁺	K_0^{10} , K_{13}^{10} , K_{10}^{10} , K_7^{10} ⁺	ad,97;08,fb;9b,87;b4,16 05,3f;2b,d8;c4,d8;11,b3 82,b8;8f,7c;ac,b0;84,26 c4,fe;7a,89;bc,a0;93,3e 6b,51;97,64;23,3f;1f,fd 90,aa;c6,35;5b,17;3f,9d ⁺ 02,38;16,e5;04,18;38,9a d1,eb;0e,fd;8b,97;01,a3 17,2d;91,62;2f,33;aa,08 56,6c;aa,59;e3,ff;94,36 c3,f9;47,b4;7c;60;18;ba 44,7e;10,e3;08,14;2f,8d ⁺ ec,d6;c0,33;4b,57;28,8a 43,79;de,2d;d4,c8;06,a4 85,bf;41,b2,70,6c,ad,0f ⁺
04 05 14 ⁺ 52 55 6e ⁺ 85 a5 ac ⁺ b3 ba bc ⁺ bf d7 f9 ⁺	K_{14}^{10} , K_{11}^{10} , K_4^{10} , K_1^{10} ⁺	d3,b1;ee,b9;42,62;f8,c0 d7,b5;d9,8e;2f,0f;69,51 8d,ef;91,c6,f1,a6;06,26;7a,42 ⁺ 10,72;70,27;8c,ac;89,b1 5b,39;61,36;15,35;e3,db a0,c2;80,d7;d2,f2;b9,81 ⁺ 9c,fe;c8,9f;96,b6;3b,03 c6,a4;b7,e0;9f,bf;28,10 4a,28;58,0f;85,a5;9a,a2 ⁺ 01,63;49,1e;1c,3c;c8,f0 67,05;7e,29;71,51;59,61 5f,3d;01,56;78,58;72,4a ⁺ 4e,2c;38,6f;e8,c8;0b,33 98,fa;a8,ff;db,fb;92,aa 14,76;47,10;e1,c1;20,18 ⁺
07 22 45 ⁺ 4d 68 76 ⁺ 82 99 9a ⁺ b1 d2 d4 ⁺ d9 df e9 ⁺	K_8^{10} , K_5^{10} , K_2^{10} , K_{15}^{10} ⁺	79,e7;d8,de;8f,b8;d0,b2 31,af;f9,ff;cf,f8;85,e7...a9,37;11,17;b2,85;53,31 ⁺ 0c,92;07,01;3c,0b;fc,9e f5,6b;97,91;d3,e4;77,15 e1,7f;30,36;f2,c5;64;06 ⁺ bd,23;b0,b6;93,a4;22,40 25,bb;5e,58;d9,ee;f4,96 6d,f3;79,7f;ae,99;c3,a1 ⁺ ce,50;87,81;6a,5d;ba,d8 44,da;26,20;4b,7c;cb,a9 42,dc;c8,ce;01;36;7f,1d ⁺ 56,c8;69,6f;20,17;0e,6c 86,18;a6,a0;2a,1d;ef,8d 0a,94;ef,e9;41,76;2a;48 ⁺
02 1c 3b ⁺ 3f 40 97 ⁺ 9e a0 ba ⁺ cb cf d6 ⁺ d8 de df ⁺	K_3^{10} , K_6^{10} , K_{12}^{10} , K_9^{10} ⁺	a0,f9;20,44;1d,d7;d6,20 e1,b8;7d,19;f3,39;C3,35...c8,91;7a,1e;3c,f6;38,ce ⁺ 8a,d3;da,be;bd,77;9a,6c 89,d0;43,27;d2,18;db,2d 30,69;de,ba;80,4a;6f,99 ⁺ fa,a3;dd,b9;b8,72;61,97 bb,e2;80,e4;9c,56;74,82 6a,33;47,23;25,ef;d8,2e ⁺ 72,2b;7e,1a;01,cb;cd,3b 1a,43;24,40;20,ea;d5,23 19,40;bd,d9;4f,85;62,94 ⁺ 5b,02;79,1d;ce,04;c0,36 01,58;84,e0;a1,6b;77,81 cb,92;e3,87;99,53;8f,79 ⁺

第1个错 误密文恢 复密钥

第2个错误密文恢复密钥

第10轮字节代换预测输入差分值	恢复密钥字节	候选值		
0c 12 1b ⁺ 29 33 36 ⁺ 74 76 9d ⁺ a1 ba e2 ⁺ e4 fb fd ⁺	K_0^{10} , K_{13}^{10} , K_{10}^{10} , K_7^{10}	60,cb;51,34;40,7d;04,14 79,d2;48,2d;c8,f5;a4,b4 4f,e4;0a,6f;2e,13;38,28 a5,oe;be,db;a0,9d;6a,7a 17,bc;c2,a7;28,15;ca,da	56,fd;13,76;9b,a6;88,98 51,fa;eb,8e;61,5c;d1,c1 a2,09;46,23;67,5a;23,33 cc,67;cc,a9;ba,87;4d,5d 94,3f;04,61;bc,81;bf,af	d5,7e;d5,b0,0f;32,fd,ed ⁺ 93,38;fc,99;46,7b;f6,e6 ⁺ 21,8a;80,e5;d2,ce;46,56 ⁺ e3,48;97,f2;d4,e9;71,61 ⁺ 8d,26;1d,78;09,34;1f,0f ⁺
23 2e 34 ⁺ 41 51 5c ⁺ 61 62 8d ⁺ c7 ca cd ⁺ e1 e7 fb ⁺	K_{14}^{10} , K_{11}^{10} , K_4^{10} , K_1^{10}	bb,b3;fe,34;f4,cf;74,b0 e5,ed;3e,f4;cc,f7;19,dd 98,90;35,ff;fb,c0;aa,6e d7,df;9b,51;73,48;42,86 c7,cf;d1,1b;21,1a;41,85	e4,ec;d0,ea;15,2e;9f,5b 88,80;b5,7f;a9,92;6d,a9 aa,a2;5a,90;44,7f;f1,35 de,d6;75,bf;aa,91;c4,00 ba,b2;da,10;2d,16;36,f2	a3,ab;b4,7e;9d,a6;b3,77 ⁺ c6,ce;f5,3f;c3,f8;c7,03 ⁺ 91,99;db,11;19,22;2c,e8 ⁺ fd,f5;74,be;9e,a5;1a;de ⁺ fc,f4;50,9a;47,7c;58,9c ⁺
0d 15 23 ⁺ 27 38 4b ⁺ 53 6f 74 ⁺ 8b c1 c4 ⁺ d6 f2 f6 ⁺	K_8^{10} , K_5^{10} , K_2^{10} , K_{15}^{10}	27,ce;4c,8f;2f,69;18,f3 ac,45;f3,30;ce,88;46,ad bd,54;94,57;fc,ba;c8,23 83,6a;42,81;27,61;98,73 df,36;e8,2b;5b,1d;7d,96	84,6d;90,53;f5,b3;8b,60 19,f0;59,9a;f4,b2;48,a3 42,ab;e2,2e;5a,1c;55,be .7c,95;f7,34;c7,81;ee,05 ba,53;85,46;2e,68;db,30	e1,08;fd,3e;c6,80;c6,2d ⁺ 20,c9;5d,9e;fd,bb;e0,0b ⁺ d8,31;3a,f9;cf,89;6e,85 ⁺ 92,7b;25,e6;53,15;fd,16 ⁺ 0f,e6;2f,ec;52,14;d5,3e ⁺
0a 18 1f ⁺ 82 87 88 ⁺ 8a a3 b7 ⁺ bd c6 c9 ⁺ d7 e5 fc ⁺	K_3^{10} , K_6^{10} , K_{12}^{10} , K_9^{10}	57,c0;22,0e;b7,10;76,ba d7,40;8d,a1;25,82;77,bb b4,23;20,0c;96,31;de,12 cb,5c;c9,e5;4f,e8;e8,24 4b,dc;66,4a;dd,7a;25,e9	65,f2;cd,e1;33,94;15,d9 a8,3f;48,64;fc,5b;41,8d 34,a3;a3,8f;a3,04;df,13 11,86;e3,cf;b5,12;bd,71 72,e5;4e,62;a1,06;d8,14...f9,6e;26,0a;6c,cb;8b,47 ⁺	06,91;60,4c;80,27;bc,70 ⁺ ee,79;a5,89;fe,59;8a,46 ⁺ 1.a,8d;24,08;4d,ea;ef,23 ⁺ 9a,0d;a7,8b;78,df;22,ee ⁺ f9,6e;26,0a;6c,cb;8b,47 ⁺

3.4 故障攻击原理与实例分析

(7) AES密码故障分析示例

实验结果表明，一次故障导入可将AES密钥空间由 2^{128} 降低到 $2^{31.63}$ ，两次故障导入无需任何暴力破解，可直接恢复128位AES密钥。

3.4 故障攻击原理与实例分析

(8) 攻击总结

攻击优
点

- 攻击所需样本量极少。
- 可用于攻破抗其他旁路攻击的密码实现。

攻击难
点

- 如何精确的在密码运行过程中注入故障。
- 如何从故障输出中提取出故障分析有用的样本。
- 如何对深轮的故障进行有效分析。

防御方
法

- 在密码芯片层面增强设备工作条件感知能力。
- 在密码运行过程中进行错误校验。

提纲

1 为什么研究？密码旁路分析研究背景

2 现状怎么样？国内外研究现状及分析

3 攻击怎么干？典型攻击原理与实例分析

4 未来怎么走？未来研究热点分析与展望

5 我们怎么办？总结与建议

热门的旁路分析方向?



4.1 新的旁路泄露发现与利用研究

4.2 新型密码旁路分析方法研究

4.3 旁路攻击综合防御体系研究

4.4 旁路攻击形式化模型研究

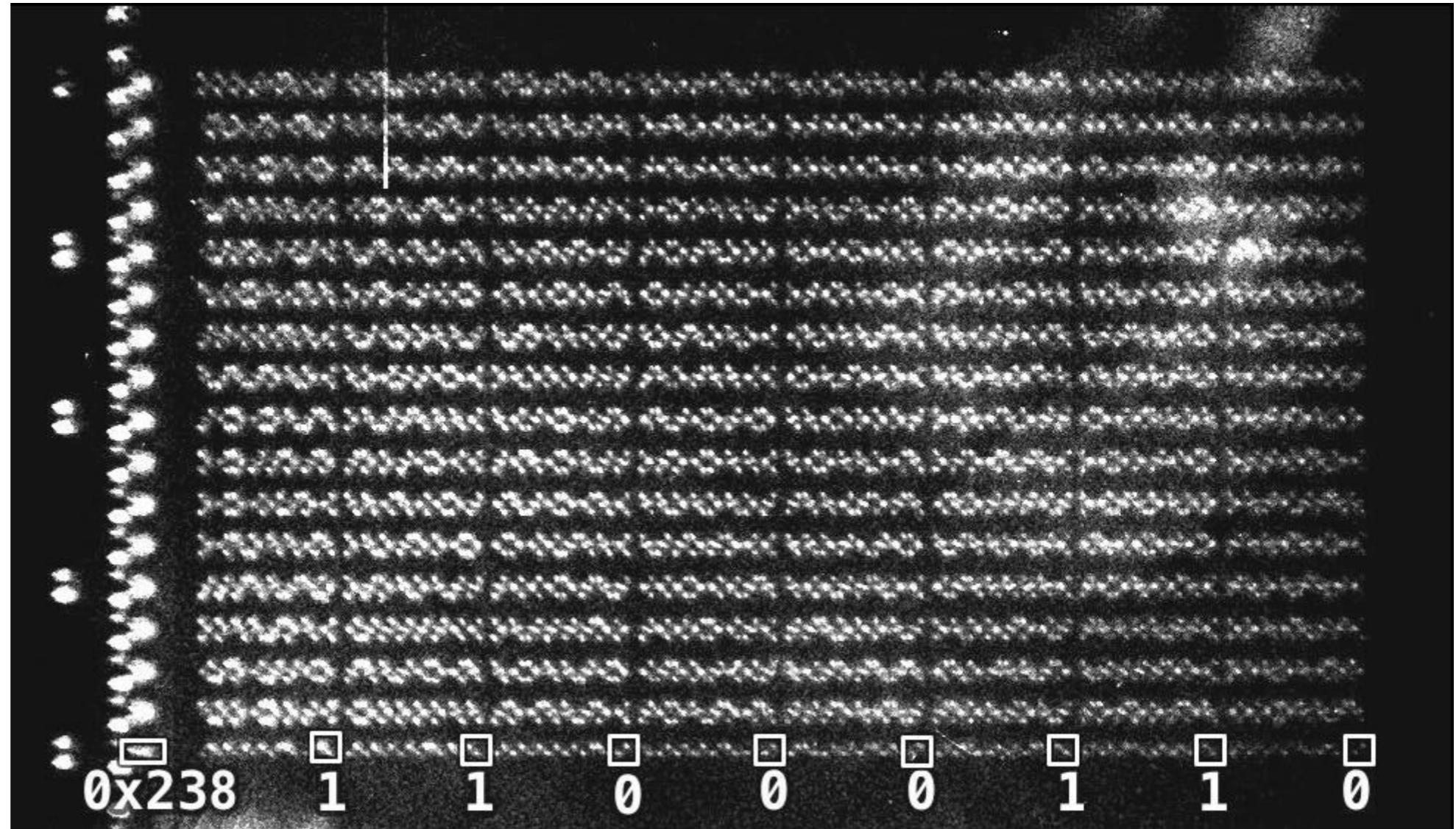
4.5 旁路分析一体化平台研制

4.6 抗旁路分析密码安全标准制定

4.7 旁路分析新型应用研究

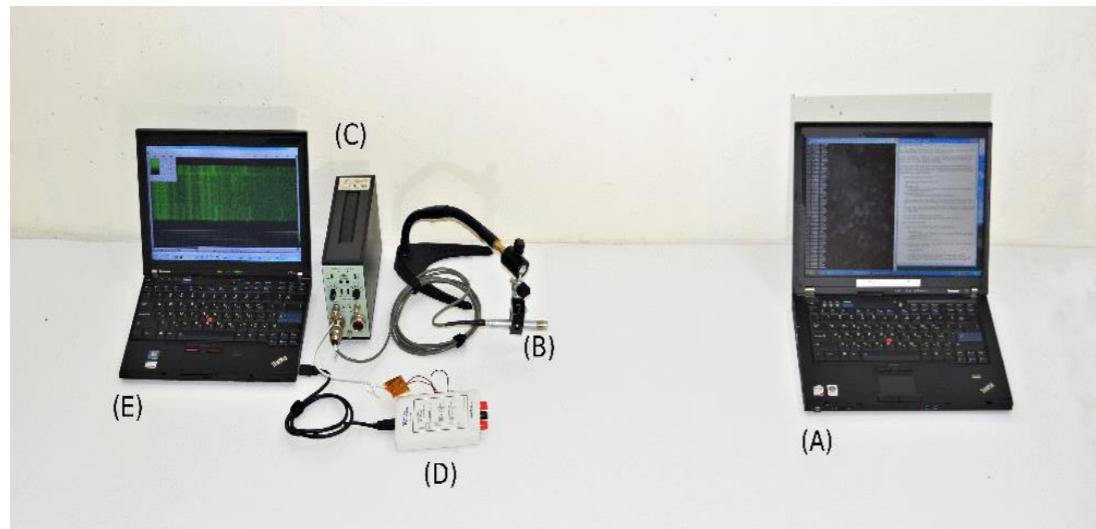
4.1 新的旁路泄露发现与利用研究

(1) 基于光子泄露的旁路分析技术研究 (2011)

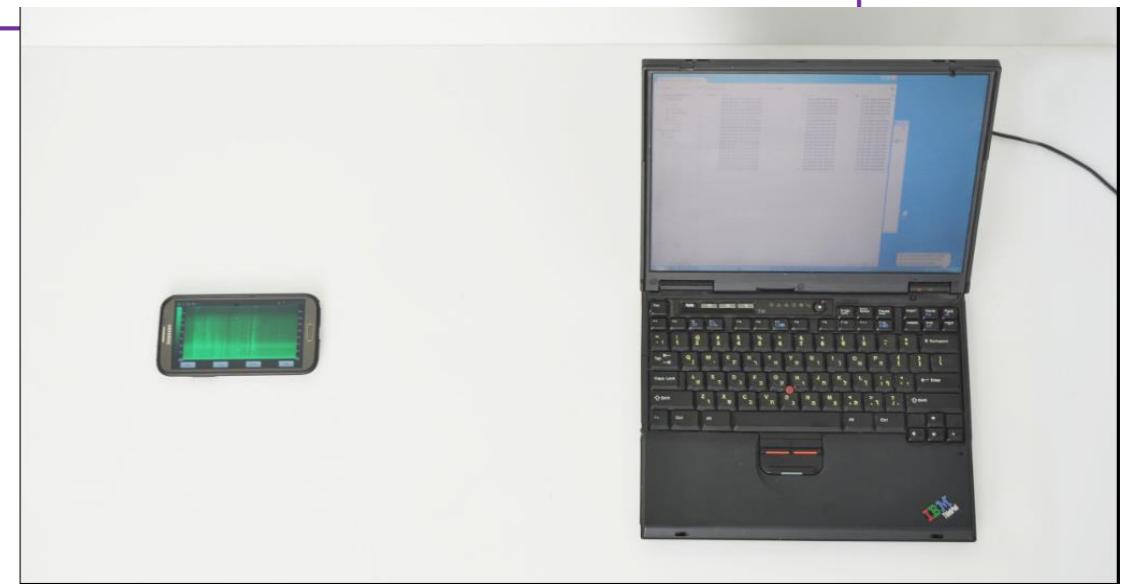


4.1 新的旁路泄露发现与利用研究

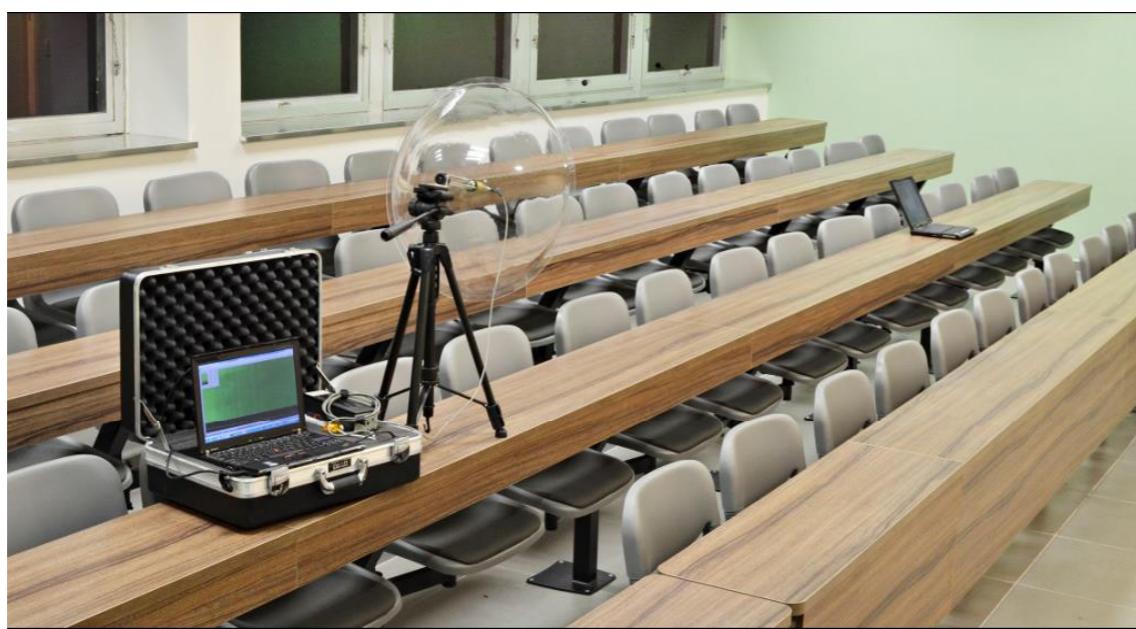
(2) 基于声音泄露的旁路分析技术研究 (2013.12)



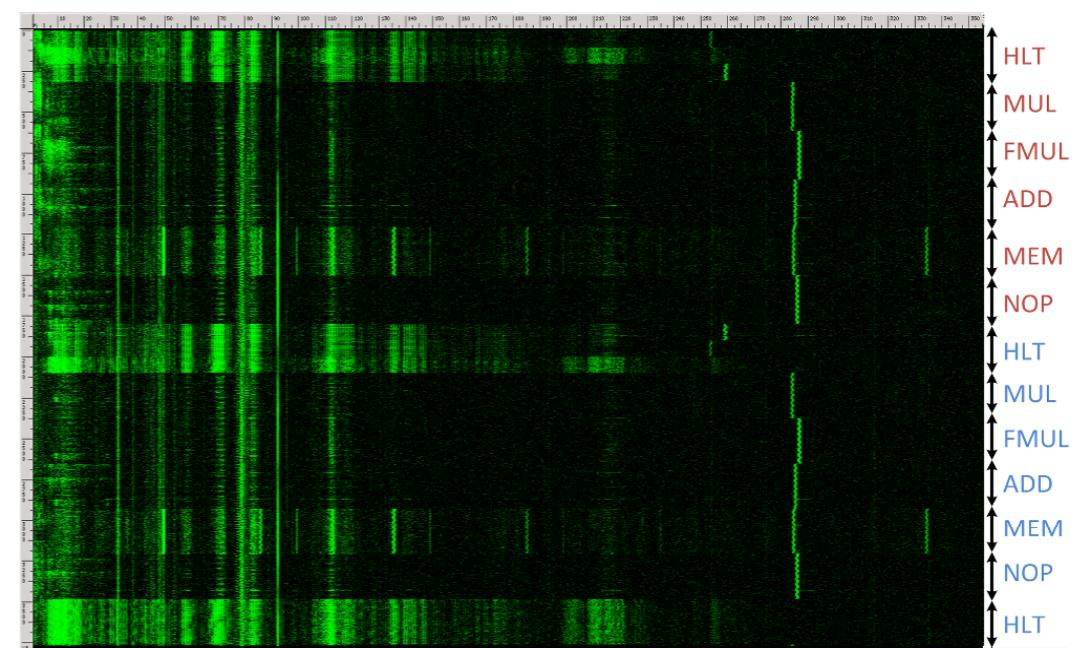
攻击配置1



攻击配置2



攻击配置3



频谱信息

4.1 新的旁路泄露发现与利用研究

(3) 基于? ? ? 泄露的旁路分析技术研究 (201X)

让我们共同期待

4.2 新型密码旁路分析方法研究

1、高阶差分旁路分析

2、随机过程模型旁路分析

3、互信息旁路分析

4、频域旁路分析

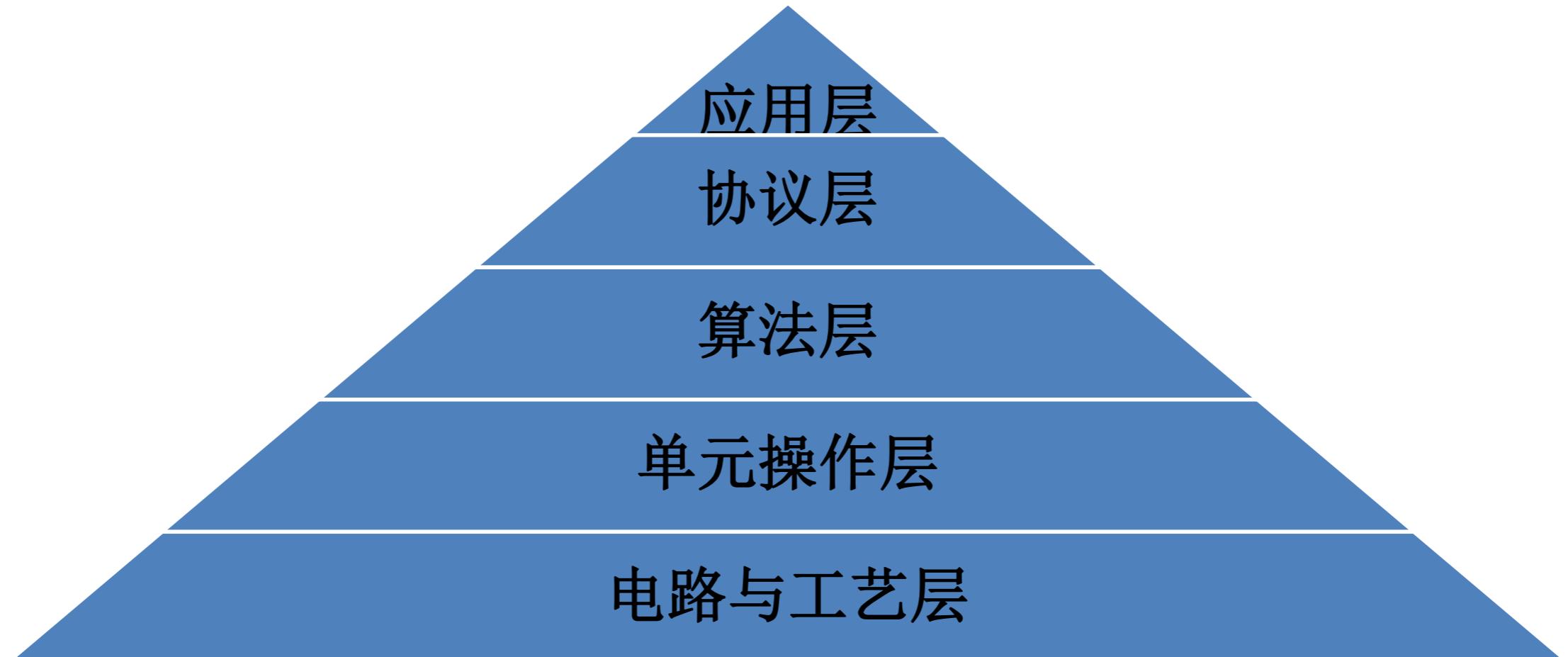
5、碰撞旁路分析

6、多道旁路分析

.....

4.3 旁路攻击综合防御体系研究

根据木桶理论和短板效应，密码系统的实际安全性取决于最薄弱环节。



单防御措施抗多种密码旁路攻击研究

多防御措施抗多种密码旁路攻击的组合性研究

4.4 旁路攻击形式化模型研究

对密码方案或协议的安全性作出“担保”，给出形式化模型，是近年来密码安全领域研究的热点问题。现有研究大部分基于传统黑盒分析，并没有涵盖针对密码旁路攻击灰盒分析。虽然目前也有部分研究结构给出了一些初步研究成果，但争议依然很大。因此，实用的密码旁路攻击形式化模型一直是当前该领域的研究重点和难点。

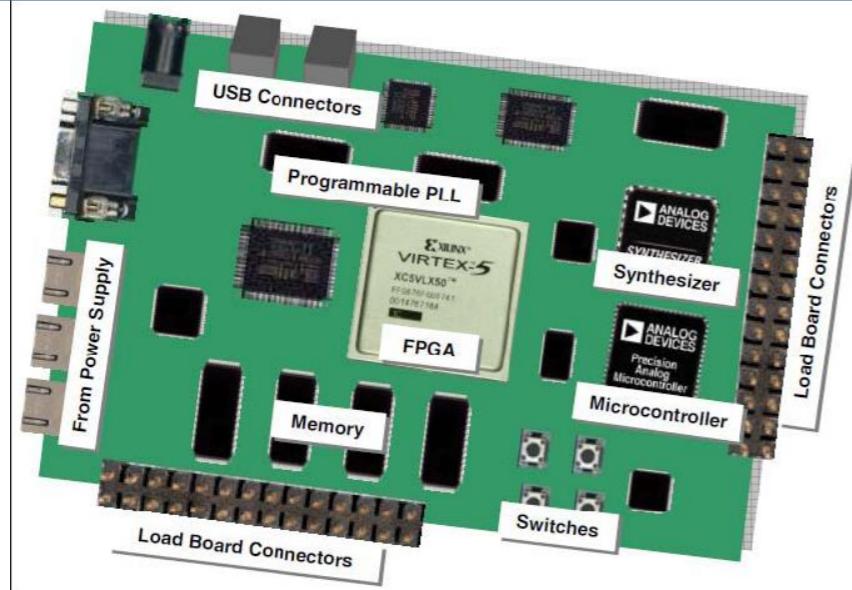
1、物理可观测密码术模型

2、敌手攻击能力评估模型

3、信息熵评价模型

4.5 旁路分析一体化平台研制

1、多种密码芯片接入能力



2、多种旁路泄露采集能力

时间、功耗、电磁、故障、声音等旁路泄露采集能力

3、专用物理泄露采集设备

如功耗、电磁分析不再使用传统示波器和探头，而是使用专用采集板卡，以提高采样速度和精度。

4、多种旁路泄露分析能力

将计时分析、功耗分析、电磁分析、故障分析、组合分析等方法集成到平台中。

4.5 旁路分析一体化平台研制

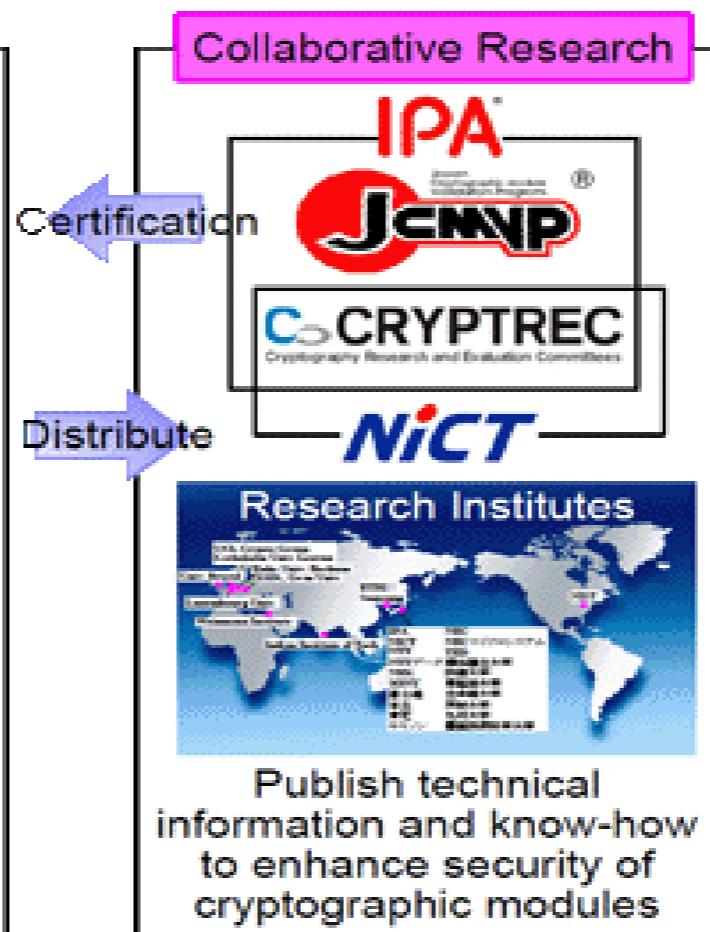
- (1) 美国Cryptography Research公司研发的功耗分析平台DPA Workstation
- (2) 荷兰Riscure公司研发的旁路攻击平台Inspector SCA和Inspector FI
- (3) 日本Tohoku大学开发了5种旁路攻击标准评估开发板，目前SASEBO已支持智能卡、FPGA、ASIC三类芯片
- (4) 中国? ? ? ? ? ?

4.6 抗旁路分析密码安全标准制定

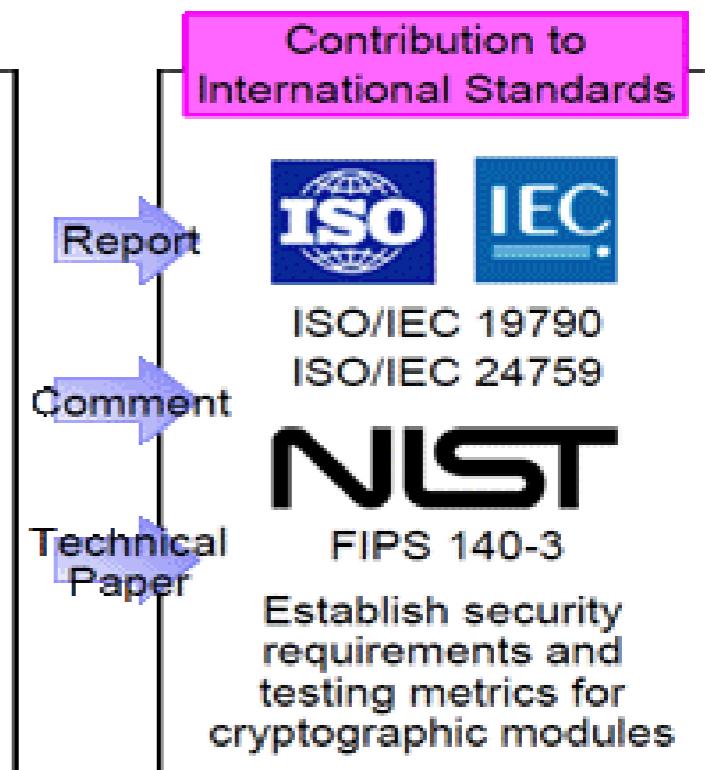
开发平台



联合评估



形成标准



日本研究战略值得借鉴!

4.7 旁路分析新型应用研究

1、基于旁路分析的密码协议系统攻击

2、基于旁路分析的生物密钥系统攻击

3、基于旁路分析的硬件木马设计

4、基于旁路分析的硬件木马检测

5、基于旁路分析的数字水印设计

6、基于旁路分析的逆向工程研究

.....

提纲

1 为什么研究？密码旁路分析研究背景

2 现状怎么样？国内外研究现状及分析

3 攻击怎么干？典型攻击原理与实例分析

4 未来怎么走？未来研究热点分析与展望

5 我们怎么办？总结与建议

5.1 研究总结

- 密码算法的设计安全性不等价于实现安全性；
- 密码系统实际安全性遵循木桶理论和短板效应；
- 旁路分析为密码分析学开辟了新的研究领域；
- 密码旁路分析是密码分析学发展的必然结果；
- 密码旁路分析已对密码安全性构成严峻的威胁；
- 我国急需开展旁路分析攻、防、评、测研究。

5.2 几点建议

付
诸
行
动

泄露可采

- 基础环境建设（泄露采集平台搭建）

泄露可用

- 研究旁路泄露的对齐、选点等预处理方法，确保后续分析的旁路泄露信息可信

深入分析

- 深入挖掘所采集泄露与秘密信息相关性

攻防结合

- 以攻查漏、以防阻攻、以攻验防

理论提升

- 在攻防基础上加强密码旁路攻击领域理论分析，形成相关标准

注意三多

- 多投入、多交流（国内外交流，跨学科交流）、多深入（提高攻击实用性）

謝

謝

