Wireless Charging Power Side-Channel Attacks

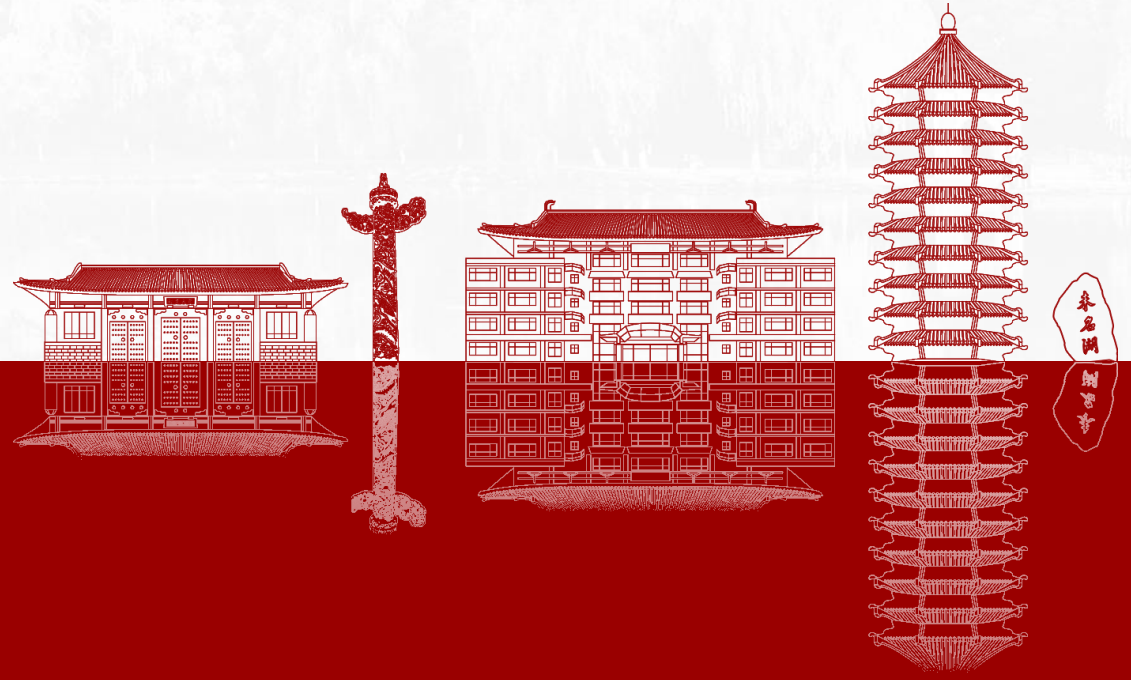
CCS ' 21, November 15–19, 2021, Virtual Event, Republic of Korea

目录
Contents

北京大學
PEKING UNIVERSITY

1 侧信道攻击

Side-channel Attack



侧信道攻击(SCA)

Simple Power Analysis

对能量迹进行直观分析

Differential Power Analysis

基于能量迹之间的相关系数进行分析

Etc.

基于机器学习的侧信道攻击

Timing Attack

```
const pw = "6666"

char str = "";
int i = 0
while(1){
    str = getchar();

    for(i = 0; i < pw.len; i++){
        if(str[i] !== pw(i)){
            break;
        }
    }
    if(i == pw.len){
        login()
    }
}
```

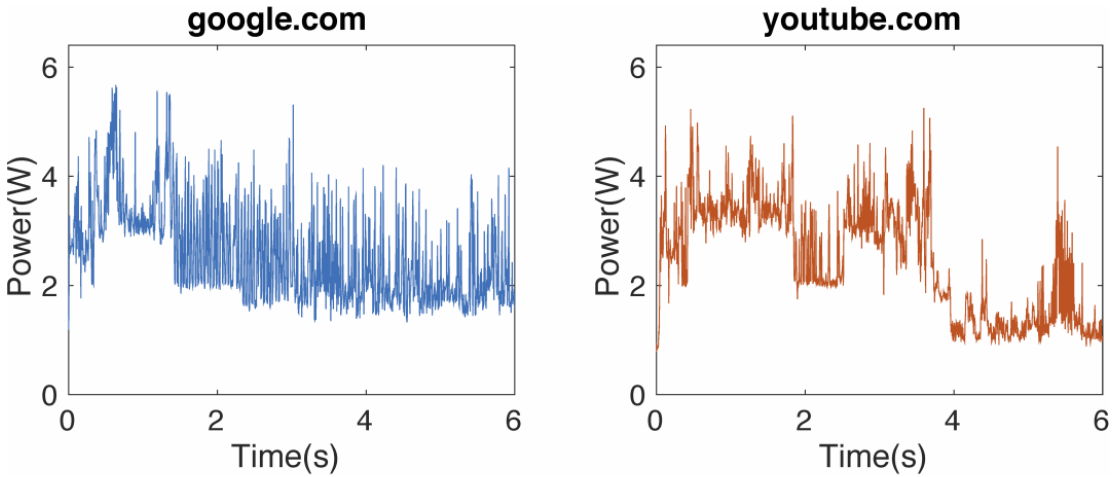
- 暴力破解——指数增长：10 x 10 x 10 x 10
- Timing Attack——线性增长：10 + 10 + 10 + 10

Power Attack （防）

- WattsUpDoc: Power Side Channels to Nonintrusively Discover Untargeted Malware on Embedded Medical Devices --2013, USENIX
  - 医疗设备和SCADA系统
    - 嵌入式设备和通用计算设备：
      - 许多嵌入式设备与传统的基于软件的反恶意软件机制(如反病毒程序或网络入侵检测系统)不兼容：
        - 传统的嵌入式设备通常使用自定义固件或没有防病毒程序的操作系统；
        - 受到严重的资源限制，使得传统的防病毒技术难以实现。
      - 制造商不愿意支持他们没有安装和没有验证的软件；
      - 当防御不明确的威胁会带来不明确的好处时，客户不愿意冒险破坏正在运行的系统。
    - 它们执行定义明确的、重复性的任务，这些任务在每次运行中应该表现出很少的变化；
    - 他们从电源插座上取电，电源插座可以作为未修改硬件的监测点。
  - WattsUpDoc在几种嵌入式设备上检测已知恶意软件的准确率为94+%，检测以前未知的恶意软件的准确率为85+%

Power Attack （攻）

- On Inferring Browsing Activity on Smartphones via USB Power Analysis Side-Channel. –2017, IEEE Transactions on Information Forensics and Security
  - 之前：
    - 攻：充电器偷偷将手机设置为USB传输模式
    - 防：物理层面（Syncstop）中断USB的数据线
  - 有线充电功率侧信道



Power Attack （攻）

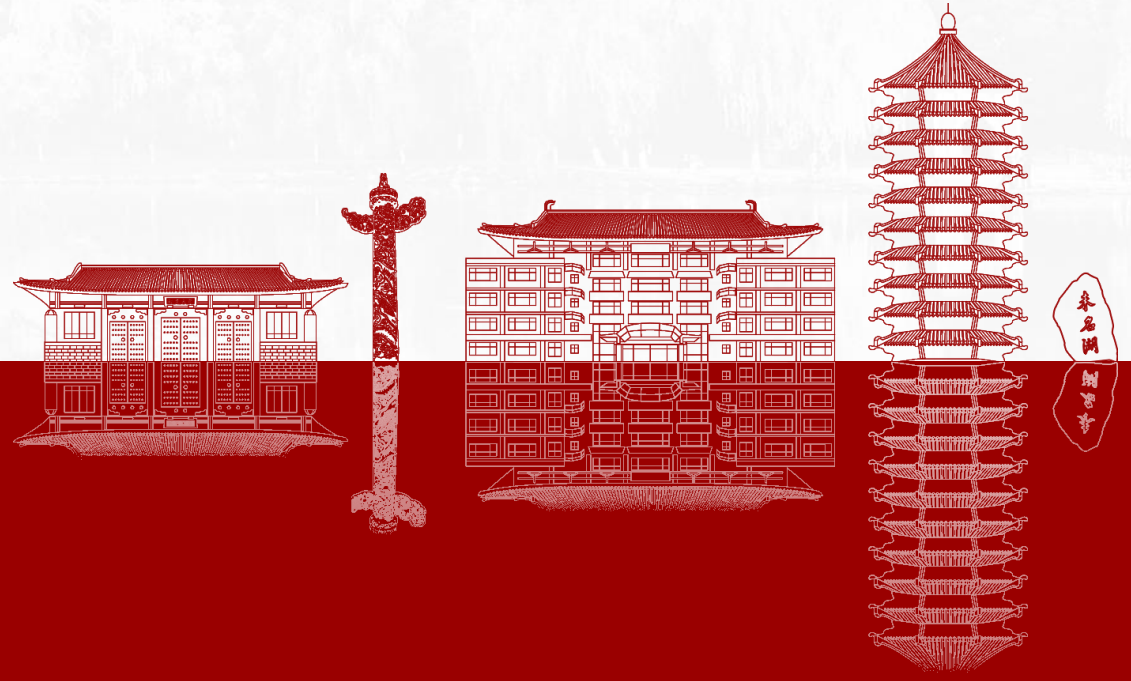
- 时效性：90+%-2.5%（70days）
- 增加训练和测试的功率 trace 持续时间可以提高识别精度；
- 使用 LTE 收集功率 trace，使用 Wi-Fi 来测试，仍能识别网页；
- 使用不同手机进行测试和训练，网页识别准确率显著下降；
- 增加智能手机和服务网页的主机之间的地理距离会降低识别精度，本地网站的识别准确率略高于国外网站；
- 通过安全连接(HTTPS 或者说 TLS)访问网页对识别的准确性没有明显的影响；
- 使用机器学习算法来识别用户从一个封闭的50个网页中访问了哪个网页，实现了2秒追踪时间内高达98.8%的识别准确率。

北京大學
PEKING UNIVERSITY

2

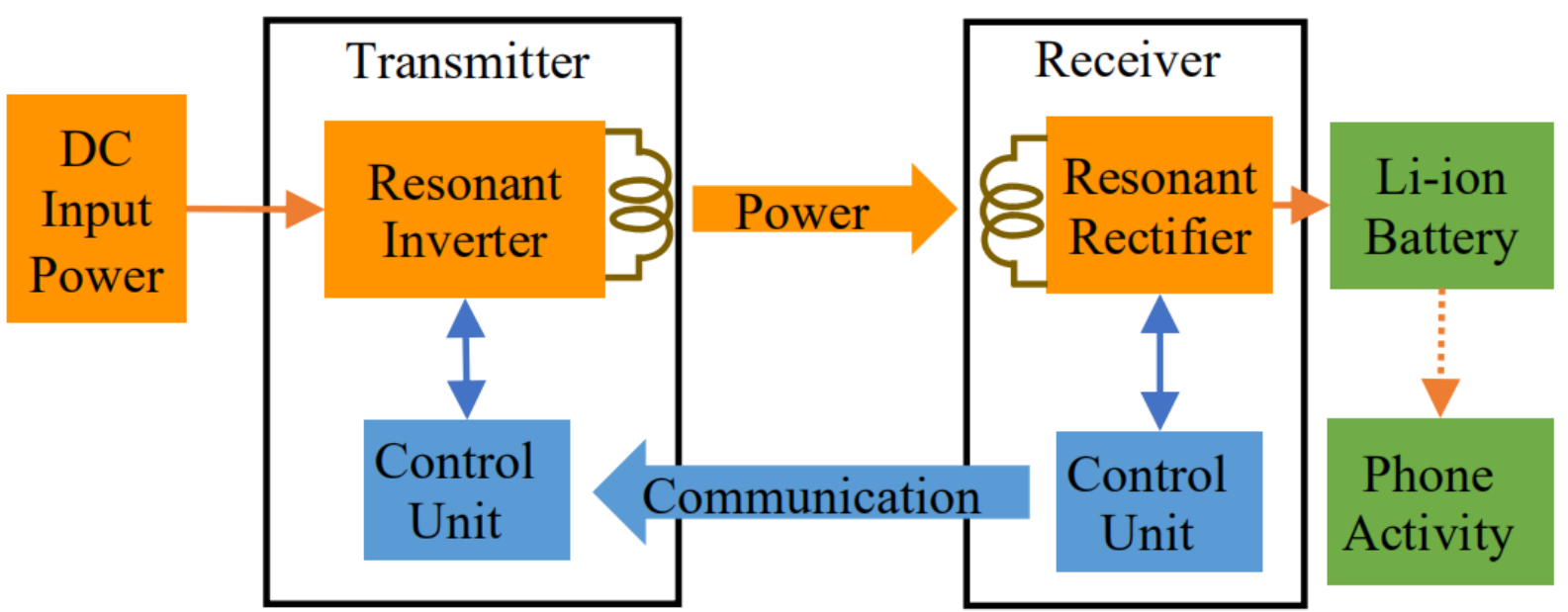
无线充电

无线充电相关原理及标准

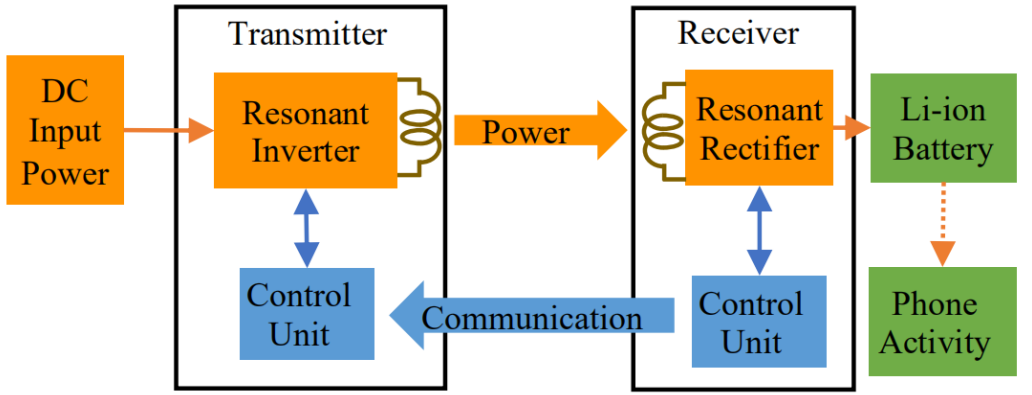


Qi Standard

- Qi标准是目前的主流的无线充电标准，涉及华为、小米、苹果、三星、中兴、诺基亚等多家公司的常见机型，比如熟知的华为mate系列、苹果iphone8以后的机型、小米9之后的机型、微软lumia720之后的机型、三星galaxy note 5之后的机型等。
- 目前支持两种为移动设备充电的功率规格：
  - Qi Baseline Power Profile（提供低于5W的功率）
  - Qi Extended Power Profile（支持高达15W的功率）

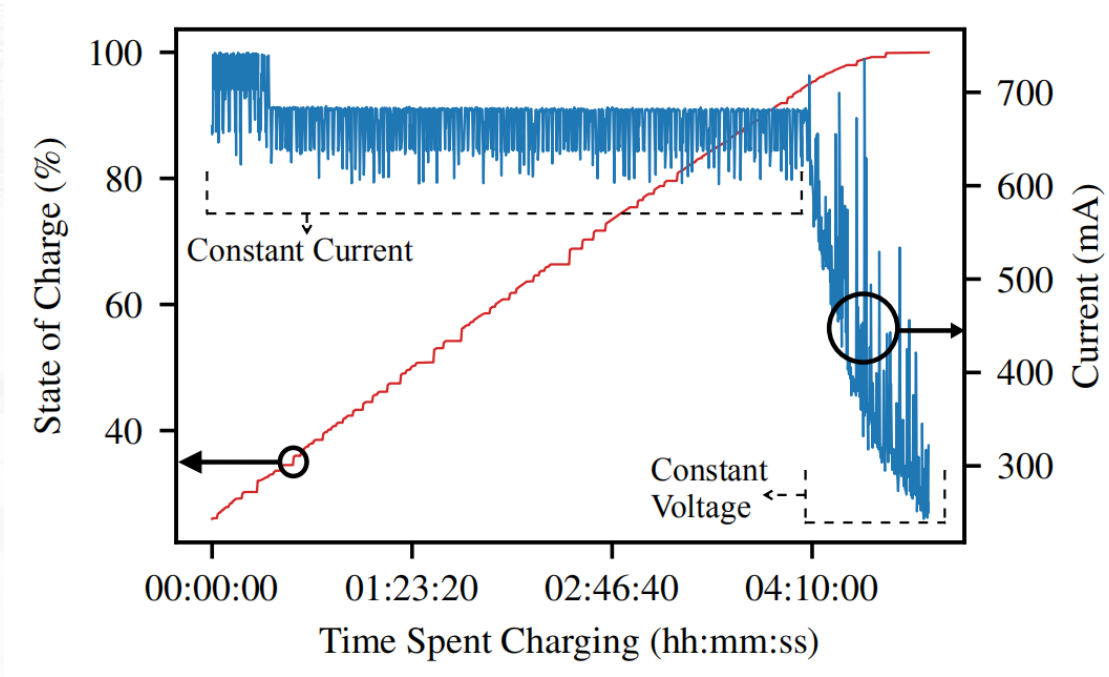


Qi Standard



- 原理：
  - 发射器上的电感线圈（主线圈）和接收器上的另一个线圈（副线圈）相耦合，发射器在其线圈中通交流电，通过法拉第感应定律在接收线圈中感应出一个交流电压。
  - 此外，电容器连接到两个电感线圈，形成LC谐振电路，实现谐振电感耦合，使设备即使在4cm外也能充电。
  - 接收线圈中的感应交变电压被整流并用于电池充电或直接为设备供电。
  - 发射器和接收器之间的通信是通过反向散射调制进行的，并且是单向的，从接收器到发射器。发射线圈由一个谐振式逆变器供电，而接收线圈则为一个谐振式整流器供电。
  - 发射器和接收器都包含通信和控制单元，可主动调节传输的功率，以匹配充电设备要求的数量。
- 步骤：
  - 第一阶段，功率发射器发送一个模拟ping来检测是否有物体存在；
  - 第二阶段，功率发射器发出一个较长的数字ping，让接收器有时间回复一个信号强度的数据包，如果发射器认为该数据包有效，它将继续为其线圈供电并进入下一阶段；
  - 第三阶段，又称识别和配置阶段，由接收方以数据包形式发送信息，以正确配置发射器进行功率传输；
  - 第四阶段，功率传输阶段开始，在此期间，接收器发送控制数据包来修改所提供的功率
  - 第五阶段，接收方停止通信或请求结束电力传输时。

电池充电周期



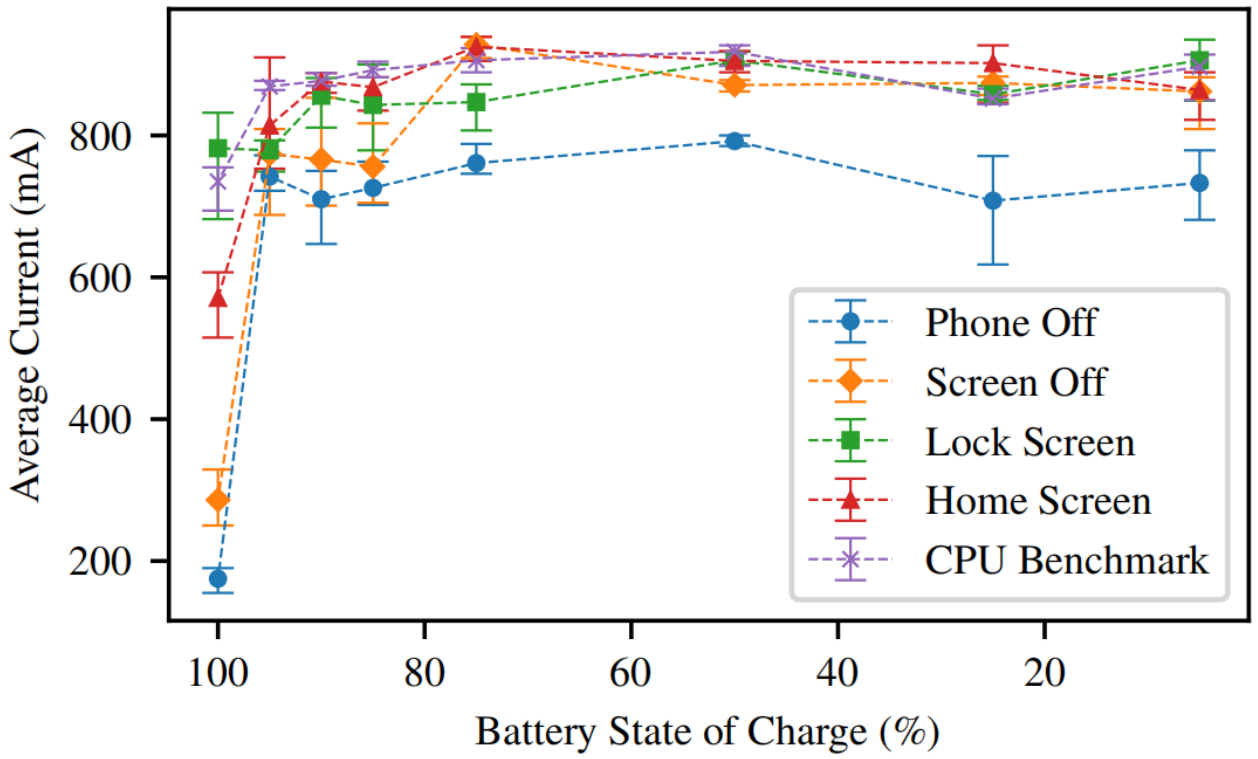
恒流充电

该阶段向电池提供最大的允许电流，稳定地提高其电压，一旦电池电压达到约4.2V，开启第二阶段。

恒压充电

该阶段供应电流下降，以限制电池的最大电压水平，一旦电池SoC(State of Charge)达到100%，充电器将提供顶峰充电，以弥补任何放电，使SoC恢复到100%。

SoC(State of Charge)

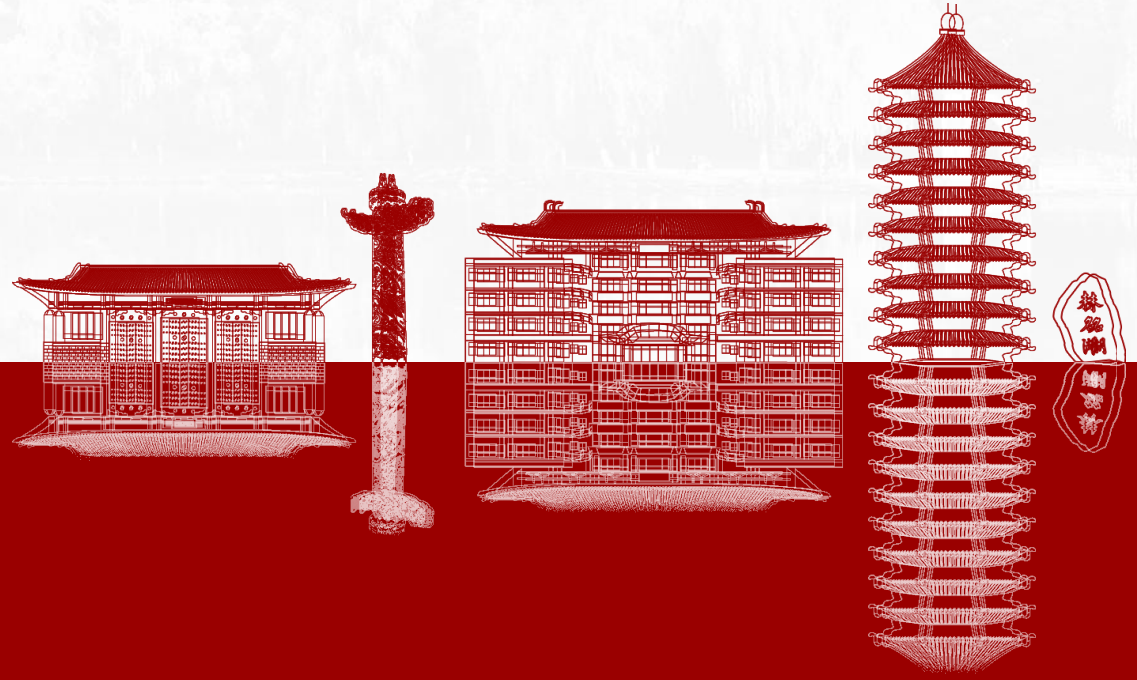


- 在8种不同的电池水平下进行。虽然结果表明，在无线充电时，不同的进程平均消耗不同的电量，但只有当SoC高时，活动之间才会出现明显的差异。
- 原因是，当手机电池充满电时，无线发射器传送的电量完全取决于手机当前使用的电量，因为它无法向已经达到最大容量的电池提供更多的电量。如果电池没有充满电，手机上运行的应用程序的电量消耗可能不会主导充电器的电量消耗，因为大部分电量将用于给电池充电。

北京大学
PEKING UNIVERSITY

3 本文实验内容

本文主要实验内容的介绍



本文工作

- 有线充电的测信道攻击之前已经被证实了，无线充电之前一直被认为是较有线充电而言更安全的，但是本文首次实现了对无线充电的电源测信道攻击，这是一种实质性的攻击，因为该攻击不需要与受害设备进行物理连接，而且不需要用户许可或特别复杂的设备就可进行攻击。

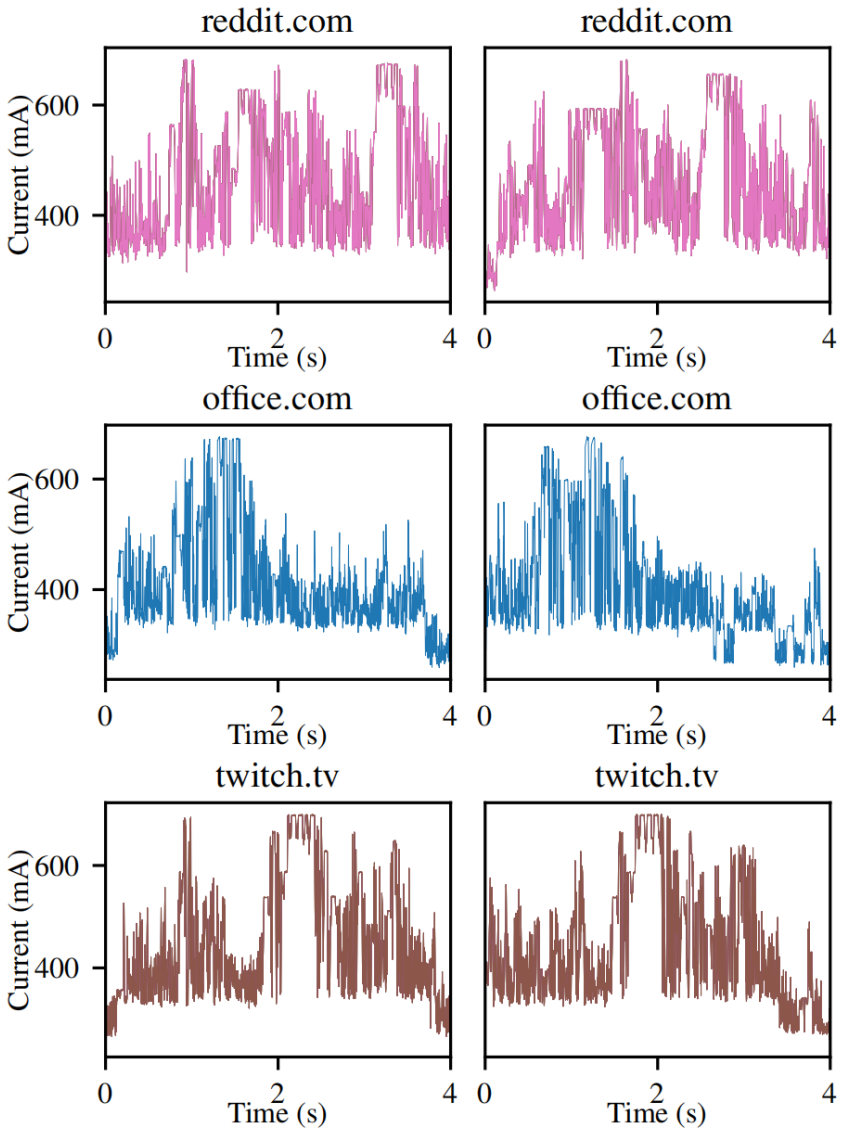
- 智能手机用户一般接触不到无线充电器的电路，因此也就无法识别恶意的充电器。而且，公共无线充电器可以嵌入到桌子和椅子上，有200种智能设备原生支持Qi标准，旧手机也可以通过附件或外壳连接到Qi兼容的接收器来实现该标准，且成本不高，仅需几十块钱，本文展示了对Qi标准（目前主流的无线充电标准）的攻击。

- 首次展示了当今智能手机上存在的一个无线充电电源侧信道，即使有噪音，这个侧信道也会泄露足够的信息，以便进行准确的网站指纹识别。

- 通过实验比较了无线和有线充电侧信道，表明他们泄露了相同的功耗信息。

- 表明充电测信道泄露的信息量很大程度上取决于电池水平。

WEBSITE FINGERPRINTING ATTACK



- 实验网站：美国Alexa top Sites中排名前20和50的非成人网站
- 实验过程
  - 电脑运行一个脚本，在iPhone 11及Pixel 4上连续加载一组网站多达50次；
  - 记录加载一个网站的前10秒的电流trace，在加载每个网站之间，脚本等待4秒；
  - 控制变量：将手机的亮度和音量设置在一个恒定的水平，并启用蓝牙和蜂窝数据。
  - 分类算法：
    - 特征提取：将每个电流轨迹分成代表原始轨迹1秒的片段。在许多小片段而不是整个轨迹上训练有助于增加可用的训练数据量，并使模型更具移位不变性来减少过拟合；
    - 数据以64/16/20的比例分为训练/验证/测试集；
    - 分类器先后用了CNN和Random Forest 。
- 实验结果：
  - To be continued……

实验结果

iPhone 11 有线充电CNN accuracy

Current Trace Type	10 s	6 s	5 s	4 s	2.5 s
Noiseless Wireless Rank-1	94.0	94.5	94.0	87.5	80.5
Wireless Rank-1	N/A	87.0	87.5	87.5	82.0
Noiseless Wired Rank-1	97.0	96.0	96.5	96.0	88.5
Noiseless Wireless Rank-2	96.0	96.5	97.5	94.0	88.0
Wireless Rank-2	N/A	94.0	94.0	89.5	87.0
Noiseless Wired Rank-2	99.0	97.5	98.0	97.0	93.5

iPhone 11 无线充电CNN accuracy

Current Trace Type	10 s	6 s	5 s	4 s	2.5 s
Noiseless Wireless Rank-1	94.0	94.5	94.0	87.5	80.5
Wireless Rank-1	N/A	87.0	87.5	87.5	82.0
Noiseless Wired Rank-1	97.0	96.0	96.5	96.0	88.5
Noiseless Wireless Rank-2	96.0	96.5	97.5	94.0	88.0
Wireless Rank-2	N/A	94.0	94.0	89.5	87.0
Noiseless Wired Rank-2	99.0	97.5	98.0	97.0	93.5

Pixel 4 有线充电CNN accuracy

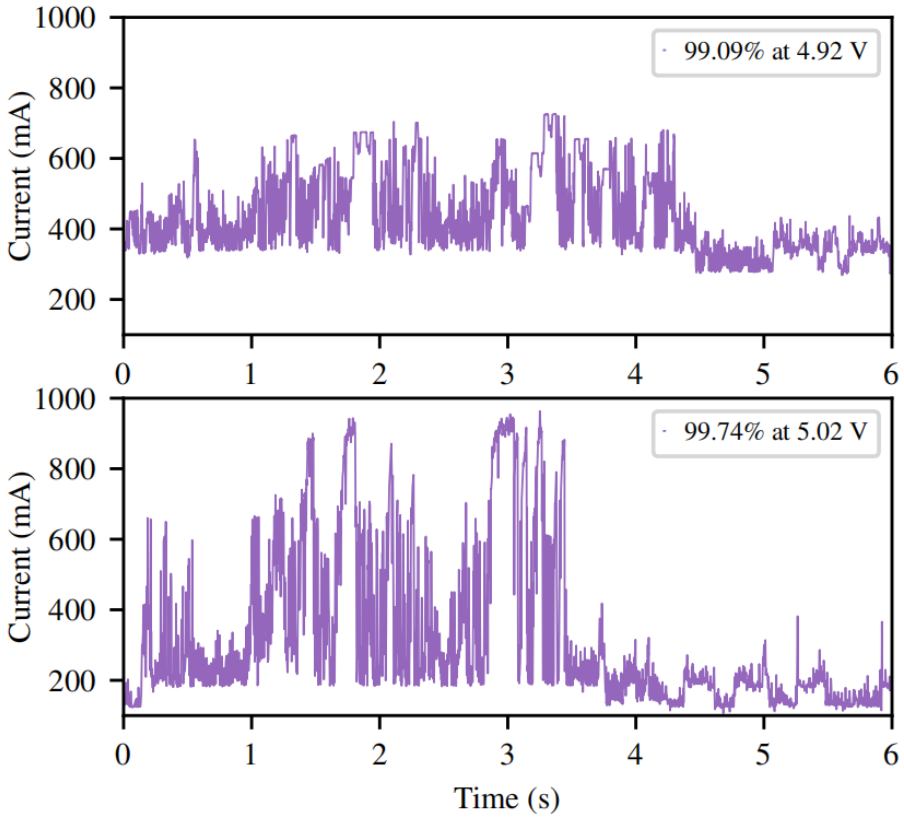
Current Trace Types	6 s	5 s	4 s	2.5 s
Wireless Rank-1	95.0	94.0	95.5	85.5
Wired Rank-1	74.0	75.0	70.5	63.0
Wireless Rank-2	97.5	98.0	96.5	91.5
Wired Rank-2	83.0	85.5	82.5	79.0

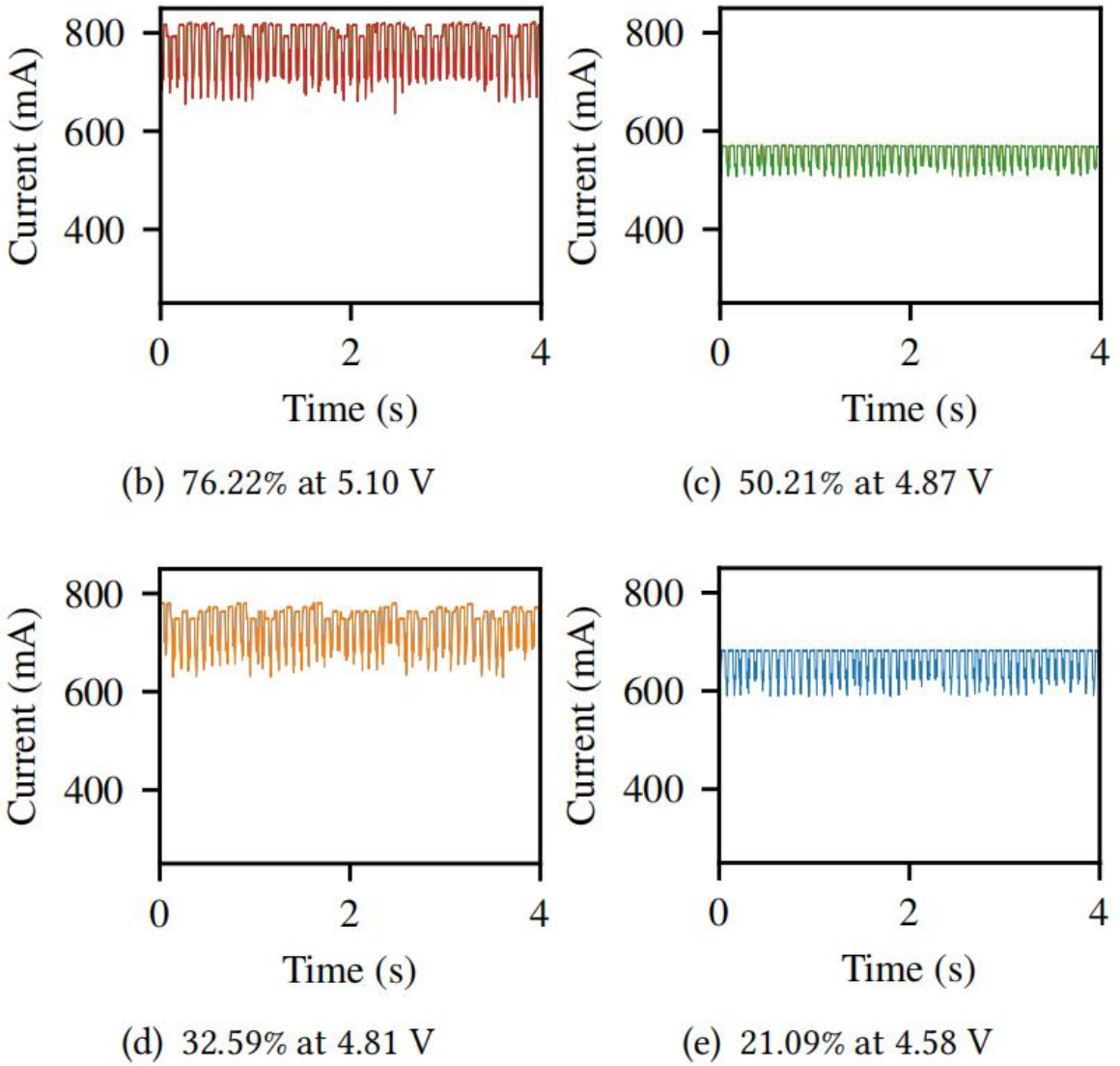
Pixel 4 无线充电CNN accuracy

Current Trace Types	6 s	5 s	4 s	2.5 s
Wireless Rank-1	95.0	94.0	95.5	85.5
Wired Rank-1	74.0	75.0	70.5	63.0
Wireless Rank-2	97.5	98.0	96.5	91.5
Wired Rank-2	83.0	85.5	82.5	79.0

- 有线充电 iPhone 11 比 Pixel 4 识别率更高，但无线充电结果相反
- 时间越长，识别准确率越高

实验结果





(b) 76.22% at 5.10 V

(c) 50.21% at 4.87 V

(d) 32.59% at 4.81 V

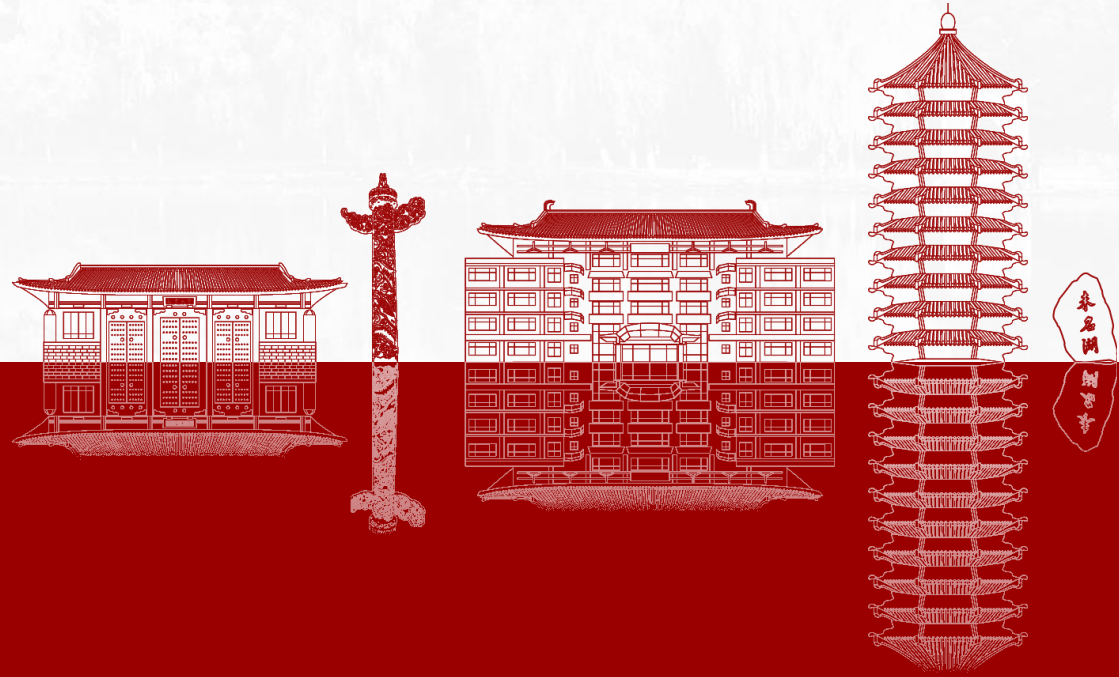
(e) 21.09% at 4.58 V

- 电池电量越高，手机活动的变化越明显
  （前面SoC一节已说明原因）

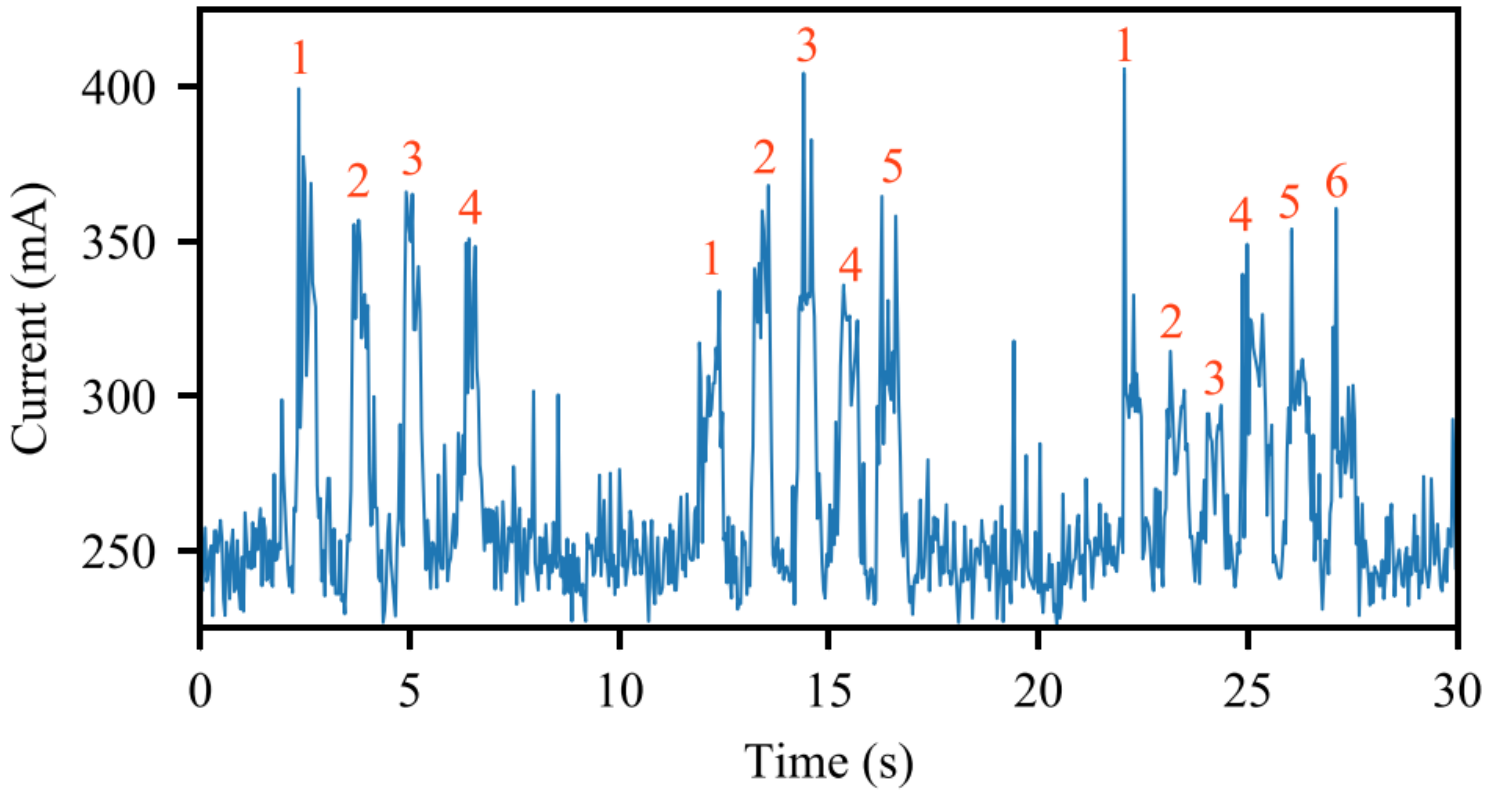
4

其他攻击例子

利用无线充电侧信道的其他攻击手段

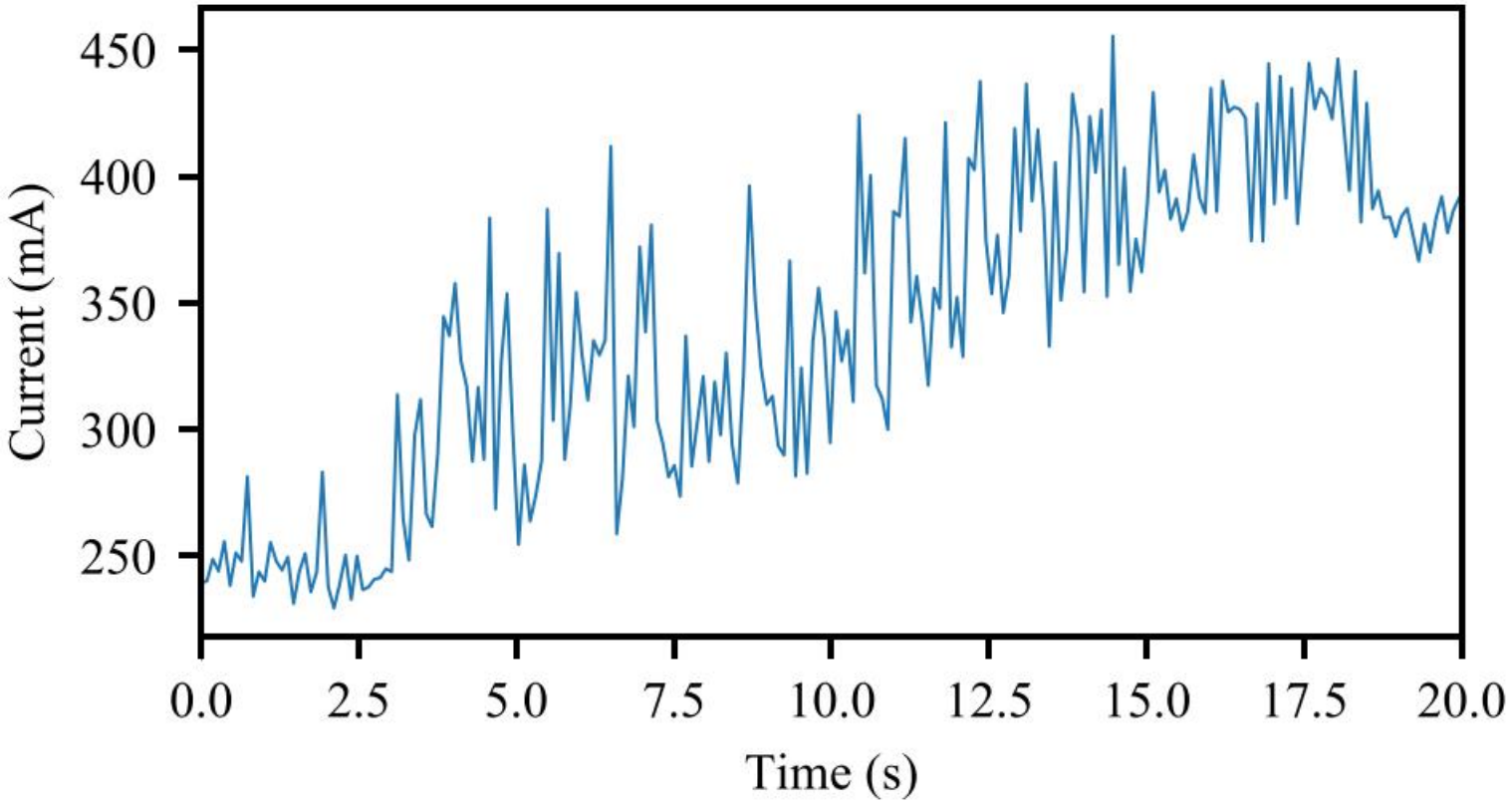


估算密码长度



- 通过点击屏幕输入的密码的每一个数字的电流消耗都会瞬间增加；
- 虽然电流突波不直接显示单个数字，但可以通过计算其包含的突波数，从输入期间收集的电流轨迹直观地识别出密码的长度；
- 知道密码的长度可以大大减少破解密码所需的搜索空间，尤其是在与其他信息提取攻击(如smudge attack，污迹攻击)结合使用时。

OLED屏幕功耗



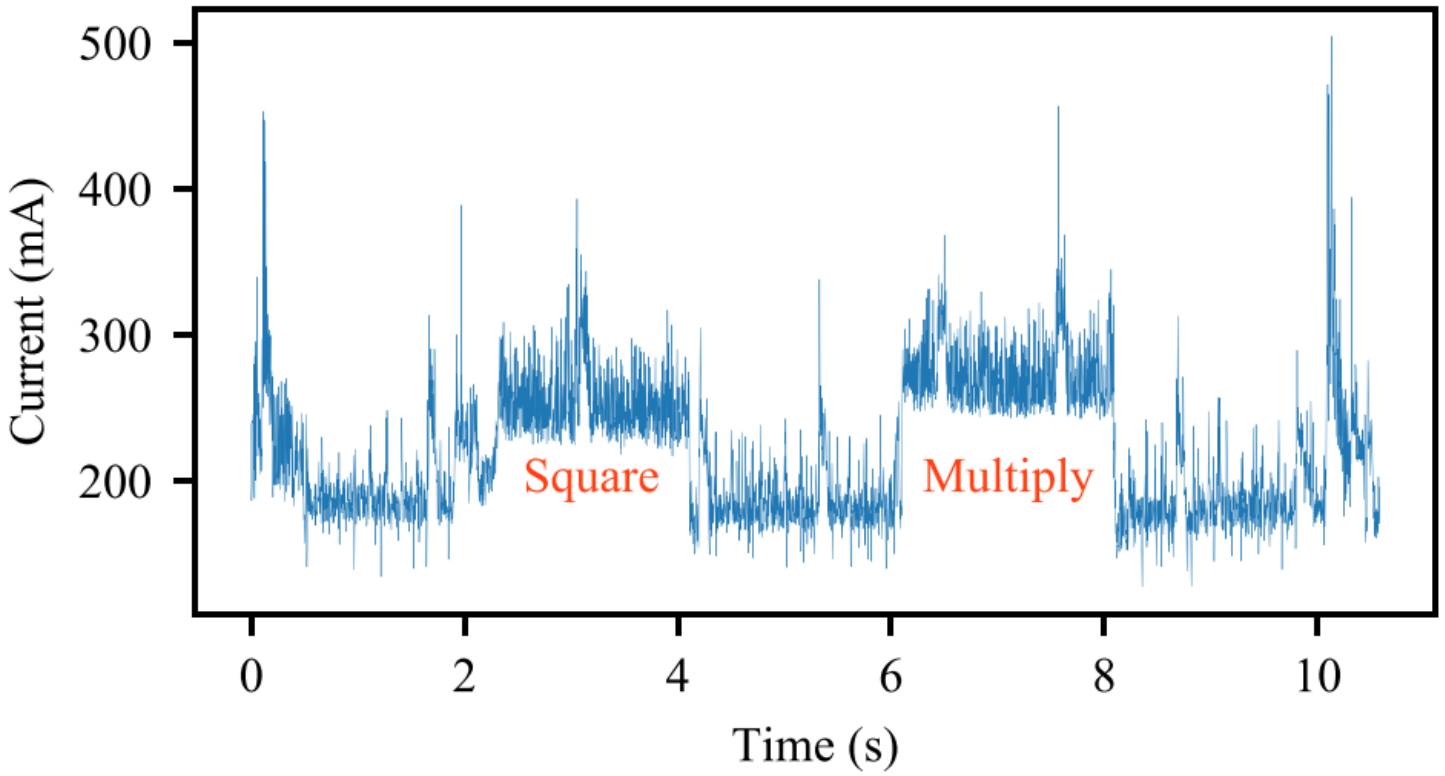
- 以 Pixel 4 的OLED屏幕为例，单一二极管发光，而不是整个屏幕背光（这种类型的显示器通常耗电更少，因为单个像素只有在屏幕内容需要时才会发光）；
- 随时间增加屏幕中白像素的数量（屏幕中间放一个黑色方块，用一个白色方块缓缓滑过来增加白色像素数量）；
- 如果功率测量设备更精确，泄露的信息可能更多。

音频指纹

Current Trace Type	4 s	3 s	2 s	1.5 s
New Traces Rank-1	88.0	88.0	84.0	82.0
New Traces Rank-2	90.0	92.0	88.0	84.0

- 利用类似于网站指纹识别的算法，对 Pixel 4 设备上的10个音频文件进行分析学习
- 之前多是通过分析屏幕亮度不同，功率消耗不同来识别设备活动
- 音频指纹说明熄屏状态下也可能会通过无线充电器泄露信息

加密算法攻击



- 基于微控制器的实验设置只能每1.4ms采样一次功耗，这不足以对快速加密算法进行全面攻击；
- 高端示波器将能够提供更细粒度的功耗测量；
- 本实验仅作为一个概念验证实验，上图显示了无线功率侧信道可以区分CPU空闲和重复运行平方或乘法操作的时间段。

2022

分享完毕 感谢您的聆听

分享人：吕子晗

北京大学
PEKING UNIVERSITY