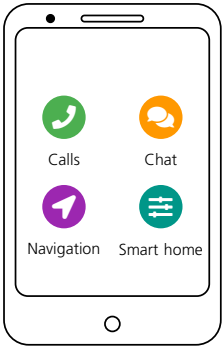
Side-Channel Analysis (SCA) on Smartphones: Challenges and Practicality

Nisha Jacob Kabakci, Felix Oberhansl, Marc Schink, January 20th, 2026

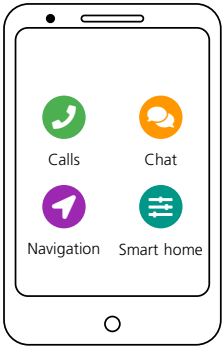
Smartphones: From Everyday Utility to Critical Infrastructure

Everyday apps

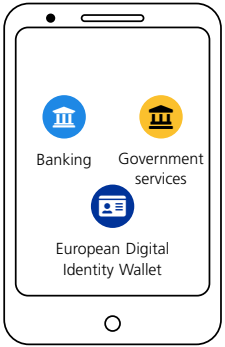


Smartphones: From Everyday Utility to Critical Infrastructure

Everyday apps



Critical apps

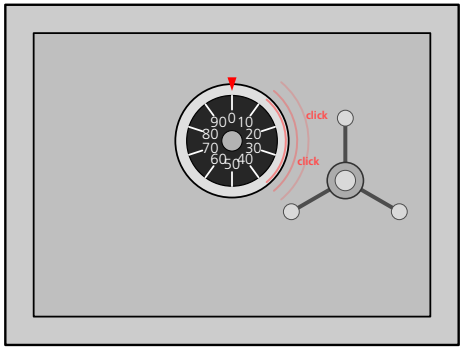


High concentration of sensitive data → Growing security concerns

Security Threats to Smartphones

- Typical threats are software exploits
- Physical access to the devices → Physical SCA
  - Attacks on modern smartphone not widely investigated
  - Hardware cannot be changed → Software updates alone might not be sufficient
  - TEE powerful against software threats, does not protect against physical SCA

What is Physical Side Channel Analysis?

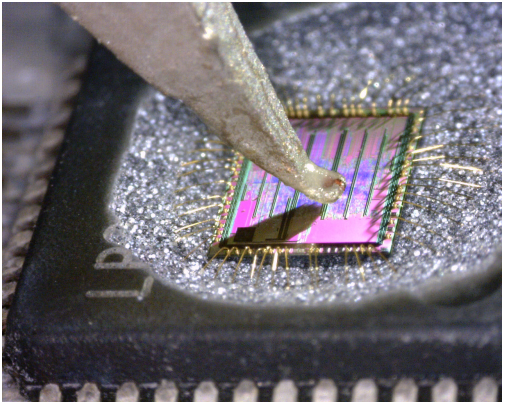


Using „clicking“-sounds to brake mechanic locks

What is Physical Side Channel Analysis?

- Physical characteristics e.g., power, timing, EM to extract secrets
- Significant threat for devices in hostile environments
- Not easily solved in software (e.g. TEE)

- Established testing schemes for Smart Cards
- Complexity of smartphones significantly increased
- Impact on physical attacks unclear



Our Goals

- Understand the practicality and risks of physical attacks on smartphones
- Analyse common cryptographic libraries on smartphones

Attack Scenarios

1. Device screen is locked

   $\rightarrow$ Attacker cannot bypass screen-lock

Attack Scenarios

1. Device screen is locked
   → Attacker cannot bypass screen-lock

2. Attacker is able to unlock the screen lock
   → Device theft (Evil-maid scenario) + weak screen-lock

Target device

- **Fairphone 4** (2020)
  - Snapdragon 750 5G SoC
    Samsung A52 5G, Xiaomi Mi 10T Lite use same SoC
  - 8nm chip with frequencies up to 2.21 GHz
  - 8 CPU cores: 2x Cortex-A77 + 6x Cortex-A55
  - Does not include Secure Element

Attack Strategy

Nonce@Once Attack

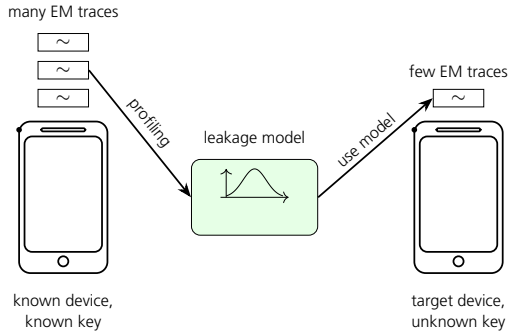
- EM attack on the ECDSA implementation of OpenSSL
- Recover k from the scalar-by-point multiplication $k \cdot G$
- Knowing (parts of) k allows to recover secret key d
- Many side-channel attacks on scalar-by-point multiplication algorithms exist, including Nonce@Once (Alam et al., 2021)

So why is it interesting for us?

Attack Strategy

Nonce@Once Attack

- Nonce@Once affects constant-time multiplication routines relying on conditional swap operations
- Libraries: OpenSSL, Libgcrypt (adopted minor countermeasures)
- Profiled side-channel attack



Attack Strategy

Attack Execution

I. Exploration and profiling
   1. Device preparation to gain access to the chip
   2. Die shot using IR camera
   3. Photon emission to identify cores
   4. Measurement of profiling traces
   5. Training the neural network

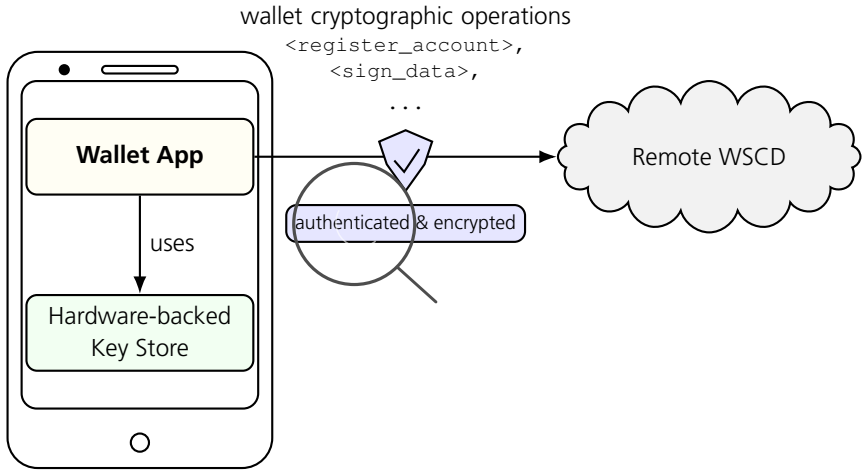
II. Attack phase
   1. Device preparation to gain access to the chip
   2. Measurement of attack traces
      Two signature are sufficient
   3. Analyses of the traces to extract secret

Attack Strategy

Demo

Attack Demo

Impact on Smartphone Security



Impact on Smartphone Security

- Attack shows the risk of physical attacks on modern Smartphones
- Software only countermeasures might not be sufficient against hardware attacks
- Open questions
  - Invasiveness: Where can we place the probe?
  - Transferability of the attack
- Certified hardware for sensitive data should be considered in the long run

Pre-print of Our Work

Breaking ECDSA with Electromagnetic Side-Channel Attacks: Challenges and Practicality on Modern Smartphones

Felix Oberhansl, Marc Schink, Nisha Jacob Kabakci, Michael Gruber, Dominik Klein, Sven Freud, Tobias Damm, Michael Hartmeier, Ivan Gavrilan, Silvan Streit, Jonas Stappenbeck, Andreas Seelos Zankl

2025

Pre-print available on `arXiv (cs.CR)`:
`https://arxiv.org/abs/2512.07292`

Contact Information

Dr. Nisha Jacob Kabakci

Head of Department Hardware Security

Fraunhofer-Institute for
Applied and Integrated Security (AISEC)

Address: Lichtenbergstraße 11
85748 Garching (near Munich)
Germany
Internet: https://www.aisec.fraunhofer.de

Phone: +49 89 3229986-116
E-Mail: nisha.jacob@aisec.fraunhofer.de