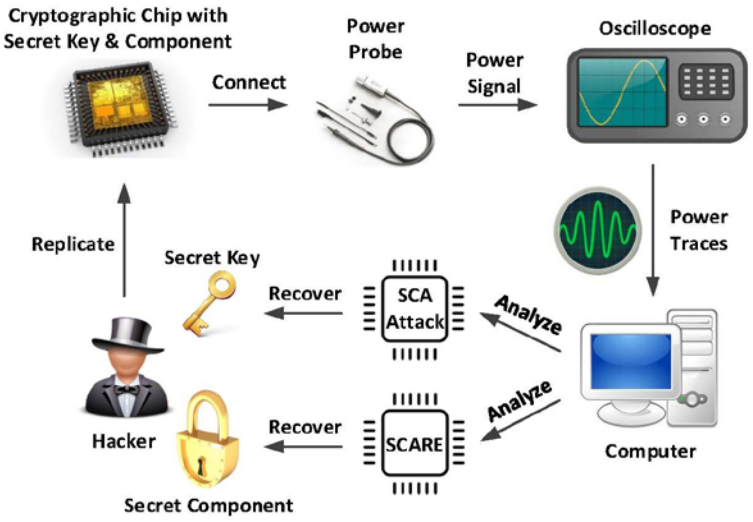
SCARE and power attack on AES-like ciphers with secret S-box

Xin LIU, An WANG, Liehuang ZHU, Yaoling DING, Zeyuan LYU, Zongyue Wang

Frontiers of Computer Science, DOI: 10.1007/s11704-020-0319-z

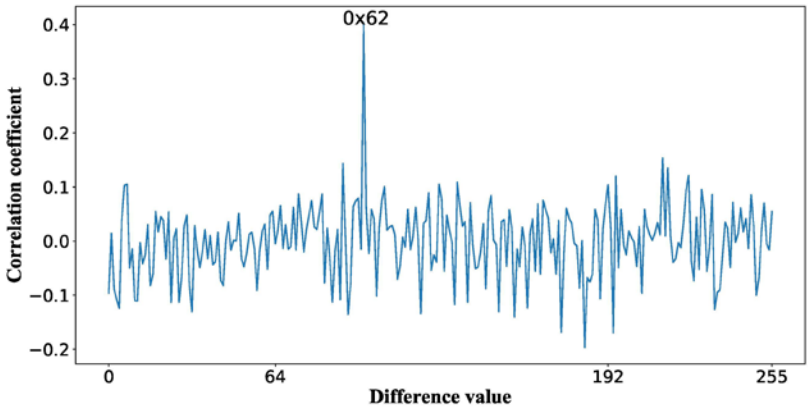
Problems & Ideas

- Previous SCAREs have a few limitations
  - prior knowledge, such as known key, collision point location
  - theoretically feasible only
- Ideas: Practical SCARE on AES-like ciphers with secret S-box
  - key recovery: profiled collision attack
  - S-box reconstruction: intermediate results of MixColumns



Main Contributions

- **Profiled correlation attack**



- **S-box reconstruction**