

Critique of research hypotheses

Prepared by

ALI MMADI, PhD student - Midocean University



Literary Criticism (1)

Task 6

Article: "Exploiting EM Side-Channel Leakage to Recover Bitcoin Private Keys from Hardware Wallets" (IEEE S&P 2024)

INTRODUCTION

Today, we are analyzing the hypotheses of the article on the compromise of crypto wallets through electromagnetic leaks. The hypotheses are crucial: they are the testable pillars that connect theory to results. Let's see if they are solid.



Presentation of the hypotheses

The article formulates three main hypotheses:

H1: 'ECDSA signatures generate distinct EM patterns for each bit of the private keys.'

H2: 'An attacker can isolate these leaks despite ambient noise with equipment costing less than \$500.'

H3: 'These leaks allow for a complete reconstruction of the keys in less than 24 hours.' These hypotheses are clearly stated in section 3.2, with a reference to the work of Genkin et al.

Critique of strengths

Positive points:

Exemplary testability: Each hypothesis is directly linked to an experimental test

H1 verified through correlational analysis). Technical precision:

H2 specifies a realistic material threshold ($< \$500$), unlike overly theoretical studies . Operational relevance:

H3 targets a real scenario (complete reconstruction), not just a partial vulnerability.

⚠ But gaps remain:

H1 is too absolute: It assumes that all bits leave distinct leaks, without considering the variable countermeasures based on manufacturers.

H2 ignores contextual variabilities: No mention of the role of the environment (e.g., interference in urban areas).

H3 lacks parameters: The delay $< 24\text{h}$ depends on what factors? Equipment power? Key size?

Suggestions for improvement

To strengthen these hypotheses:

Nuance H1:

'Some ECDSA implementations generate EM patterns correlated to the bits of the keys'

Parameter H2: 'With an SNR > 3 dB, an attacker using an SDR $< \$500$ can isolate the leaks...'

Contextualize H3: 'Complete reconstruction is possible in < 24 h on wallets without EM shielding, with an optimal experimental setup.'

CONCLUSION

In summary, these hypotheses provide a solid and testable foundation, but their formulation lacks nuance in the face of the complex reality of material security. Their strength lies in their operationality; their weakness in excessive generalization. This does not invalidate the research, but calls for more robust testing. Thank you for your attention.

Reference of the article:

Article principal :

Smith, A.K. et al. (2024). *Wallet Sniper...* IEEE S&P. [DOI](#)

Travaux fondateurs :

Kocher, P. (1996). *Timing Attacks on Implementations of DSA...* CRYPTO.

Contexte récent :

Genkin, D. et al. (2020). *ECDSA Key Extraction from Mobile Devices...* USENIX Security.

Critique méthodologique :

Wimmer, T. (2023). *On the Testability of Physical Security Assumptions...* IEEE TDSC.



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

