



Minerva

A Ladder has no Windows but can Still Leak
minerva.crocs.fi.muni.cz


Ján Jančár Vladimír Sedláček
Petr Švenda Marek Sýs
jan@neuromancer.sk




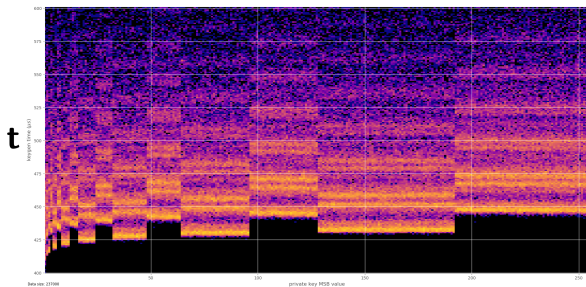
Centre for Research on
Cryptography and Security

Masaryk University
Brno, Czech Republic


Workshop on Elliptic Curve
Cryptography
02.11.2019


-  **ECTester**: black-box testing of cards and libraries

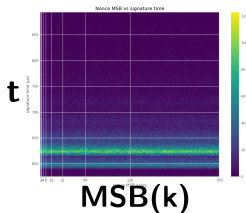
-  **ECTester**: black-box testing of cards and libraries
- 2018 - Timing leakage in EC keygen in Botan 2 library




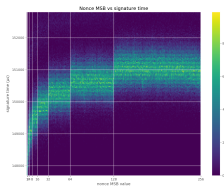
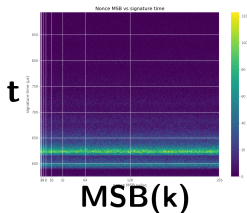
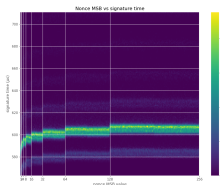
MSB


-  **ECTester**: black-box testing of cards and libraries
- 2018 - Timing leakage in EC keygen in Botan 2 library
- 2019 - Let's test ECDSA!

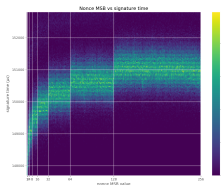
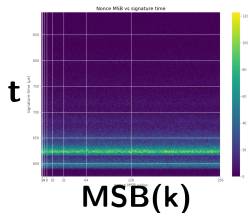
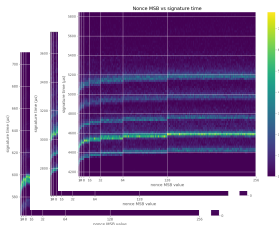
-  **ECTester**: black-box testing of cards and libraries
- 2018 - Timing leakage in EC keygen in Botan 2 library
- 2019 - Let's test ECDSA!




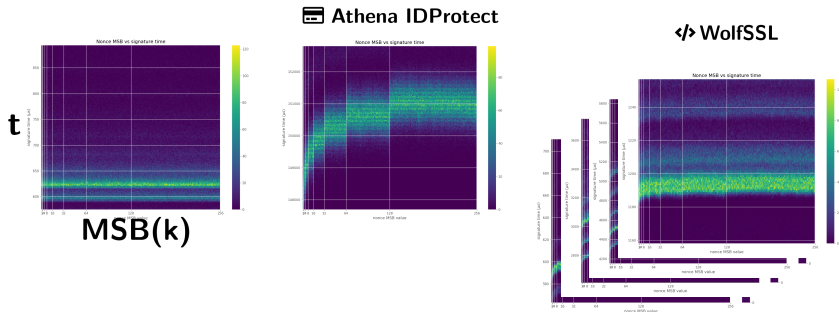
-  **ECTester**: black-box testing of cards and libraries
- 2018 - Timing leakage in EC keygen in Botan 2 library
- 2019 - Let's test ECDSA!


 **Athena IDProtect**

 **SunEC/Java**


-  **ECTester**: black-box testing of cards and libraries
- 2018 - Timing leakage in EC keygen in Botan 2 library
- 2019 - Let's test ECDSA!

 **Athena IDProtect**

 **MatrixSSL**


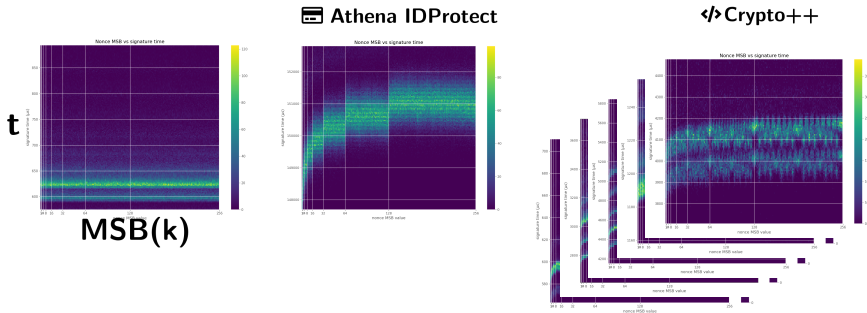
-  **ECTester**: black-box testing of cards and libraries
- 2018 - Timing leakage in EC keygen in Botan 2 library
- 2019 - Let's test ECDSA!



-  **ECTester**: black-box testing of cards and libraries
- 2018 - Timing leakage in EC keygen in Botan 2 library
- 2019 - Let's test ECDSA! \implies 1 card + 5 libraries leak +



TPM-FAIL



- **Attack:** Measure N signatures, take d of the fastest.
- Assume some bounds l_i : $k_i = |xt_i - u_i|_n < n/2^{l_i}$
- **HNP:** Given d of the above, find secret x .
- Construct a lattice, reduce it, find a short vector, get the private key.

- Our minimal $N = 500; 1400; 2200$, far from theoretical minimum
- Montgomery ladder leaked (incomplete formulas)

compatibility (EMI/EMC); self-tests; and design assurance. An additional area concerned with the mitigation of other attacks is currently not tested but the vendor is required to document implemented controls (e.g., differential power analysis, and TEMPEST). Table 1 summarizes the security requirements in each of these areas.



Note

* The **Fast** functions of M10.3, M10.4, M10.5, M10.7, M10.8, M10.9, do not offer any DPA/SPA protection and **must** not be used for secure data.



Thanks!

🐦 J08nY | `</>` neuromancer.sk | ✉️ jan@neuromancer.sk

- <https://crcs.cz> | <https://github.com/crocs-muni>
- <https://minerva.crocs.fi.muni.cz>
- <https://crocs-muni.github.io/ECTester/>