JavaCards at CRoCS

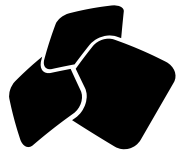
Centre for Research on
Cryptography and Security

Ján Jančár[*†]
jan@neuromancer.sk

Masaryk University
Brno, Czech Republic

SummerSchool on Real World
Crypto and Privacy
18.06.2019

[*]In collaboration with many people.
[†]Disclaimer: Opinions presented are mine, not of CRoCS or the University.



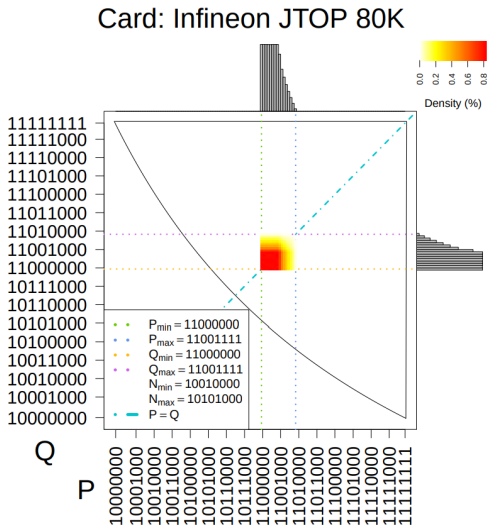
JavaCards

- Very popular programmable smart cards (est. 20 billion units)
- *Applets* written for Java-like environment, ISO 7816-4 APDUs
- Used in security critical applications
  - Credit/Debit cards
  - SIM cards
  - Electronic ID & passport
  - Cryptocurrency wallets
- Offer nice crypto:
  - ECDH/ECDSA ($\mathbb{F}_p$,$\mathbb{F}_{2^m}$) $\sim$ 100ms, custom curves!
  - RSA
  - AES
  - SHA-1/SHA-2
- ! Very industry oriented and secretive space (NDAs, only certs - no info, ...)

The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli (ACM CCS '17)

Matúš Nemec, Marek Sýs, Petr Švenda, Dušan Klinec, Vashek Matyas **(not me)**

- Analyzing bias in RSA public keys
- Noticed a bit too much bias on one of the cards (Infineon)
- Recovered structure of the generated primes $\Longrightarrow$ low entropy
- Figured out a way to attack this to get practical factoring (Coppersmith's method)
- **Huge impact:**
  - eID cards (Estonian, Slovak, ?Spanish?)
  - TPM chips
  - ?Who knows where else?
- OPSEC works



What we do

- RSA key analysis - Properties of RSA public keys & classification
- JCAlgTest - Support and performance
- ECTester **(me)** - Testing of ECC for correctness and security
- APDU fuzzing - Using power traces to guide fuzzing
- MPC from smartcards - High assurance from untrusted components
- PYECSCA **(me)** - Extracting ECC implementation information from SCA: curve model, coordinates, formulas, scalar mult
- Other tools: profiling, low-level math from primitives
- Building a community!

What you can do

- Do you have access to cards? $\Longrightarrow$ JCAlgTest + ECTester
- See if JavaCards offer something for your crypto needs
- Develop with them (please make it open-source)
- Come up with new ideas to attack/analyze/secure them
- Talk to me afterwards

Thanks!

J08nY | </> neuromancer.sk | jan@neuromancer.sk

- `https://crcs.cz` | `https://github.com/crocs-muni`
- `https://www.fi.muni.cz/~xsvenda/jcalgtest/`
- `https://crocs-muni.github.io/ECTester/`
- ROCA:
  `https://crocs.fi.muni.cz/public/papers/rsa_ccs17`
- MPC:
  `https://crocs.fi.muni.cz/public/papers/mpc_ccs17`
- RSA key analysis:
  `http://crcs.cz/rsa`
- PYECSCA:
  `https://neuromancer.sk/pyecsca/`
- More to come!