Robust identification metadata for certified smartcards

JCAlgTest

SCAN ME

Research question

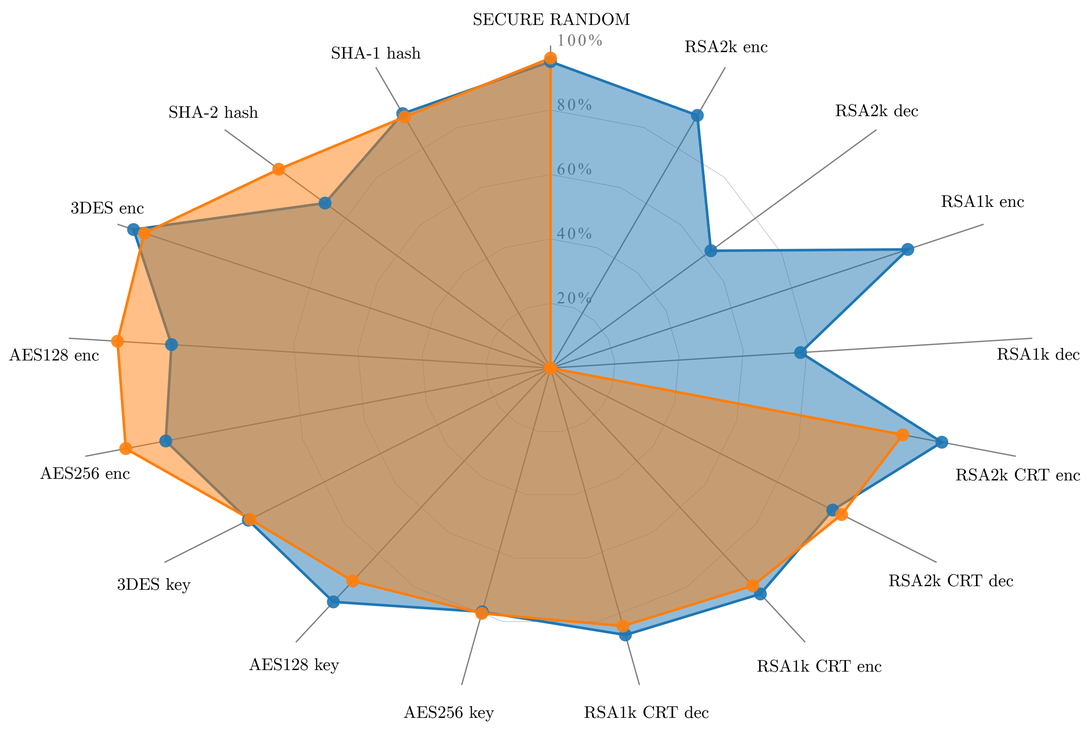
"Can we build a robust profile of a cryptographic smartcard from its behavioral characteristics?"

Method

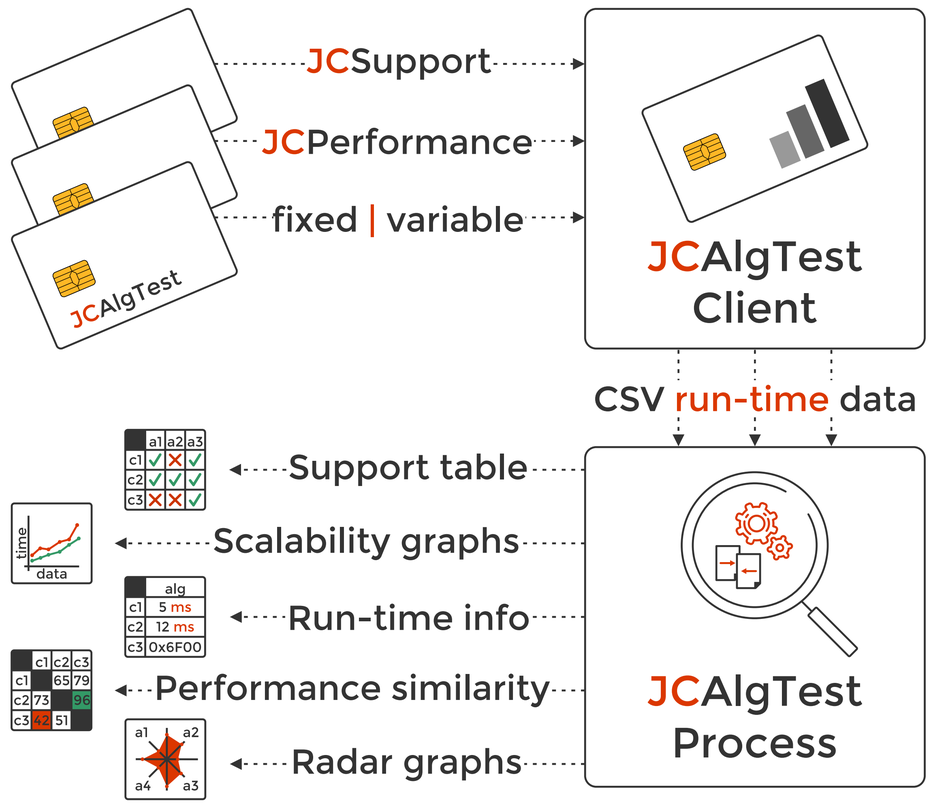
- Set of tools developed to construct metadata profile
- More than 100 types of cryptographic smartcards profiled (CRoCS laboratory & community provided)
- Extract insight from two decades of card production

Modules developed and used

- **ATR and CPLC collection module**
  ICFabricator, ICType, OSID, ICFabDate...
- **Supported JavaCard algorithms module**
  All constants from JavaCard API v2.0 (2000) up to v3.1 (2019) extracted from the specification
  More than 360 cryptographic algorithms, key lengths and padding options tested
- **Performance profiling module**
  More than 2300 combinations of {`algorithm`, `method`, `data_length`} benchmarked
  Sub-millisecond measurement resolution achievable despite missing on-card timer
- **Installed javacard packages module**
  Scan for support of 89 `java.*`, `javacard*.*`, `org.globalplatform.*` and `visa.openplatform.*` packages via purpose-crafted *.cap file
- **RSA/ECC keys collection module**
  Automatic on-card RSA & ECC key generation
  Millions of keys generated, exported, and analyzed
- **Presentation module**
  Build interactive web pages from the data collected

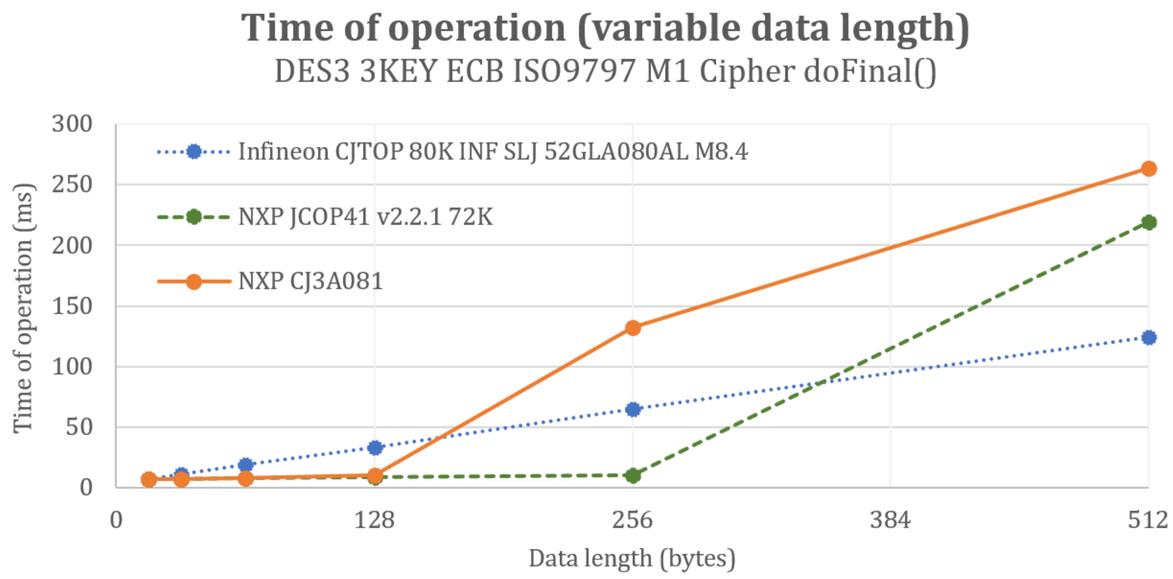


Performance comparison of basic crypto algs (2 cards)



Some facts from smartcard ecosystem

- Every tested card offers truly random number generator (TRNG) and DES & 3DES algorithms
- Adoption of newer algorithms is relatively slow
  First card with AES six years after standardization
  Still no card with SHA-3 support among tested
- Stronger security is supported via ECC than via RSA
  Most newer cards (3.0.4 or higher) support key lengths up to 521b (ECC), very few 4096b (RSA)
- The performance varies widely among the cards
  Up to 10-100x, but stable for the same type
- Internal buffers influence speed dramatically
  Processing time increases linearly only until the internal buffer size is reached
- Hardware co-processors matters
  AES in hardware can be hundreds times faster than software-only on the same card



Biggest JavaCard open-source database

- More than 110 profiled cryptographic smartcards
- All freely available at **http://jcalgtest.org**
- Thank you FOSS community!

Petr Švenda, Rudolf Kvašňovský, Imrich Nagy, Antonín Dufka

svenda@fi.muni.cz

Centre for Research on Cryptography and Security, Masaryk University

MASARYK UNIVERSITY