PV204 Security technologies

Team projects

Petr Švenda
Faculty of Informatics, Masaryk University, Brno, CZ

CROCS
Centre for Research on
Cryptography and Security

Project idea

Improve existing cryptographic libraries

1. Select existing open-source cryptographic library
2. Generate large number of RSA and ECC keys
3. Analyze cryptographic operations for side-channel leakage
4. Implement support for hardware tokens
5. (Try to push changes to upstream repository)

Teams

- 3 people per team
  - Formed today (within group), available in IS
- Teams must use GitHub for cooperation
  - Distribute work load evenly between all members
  - Contribution from all team members must be visible in git (git commits from each member)
  - Your evaluation will be partially based on your participation
- Teams may use existing code, but must make clear attribution to the original author(s)

Basic hints on successful team work

- Form team from people with similar expectations
  - intended effort, final mark, interactions…
- Plan your work (GitHub milestones + issues)
- Don’t overcommit and fulfil your promises
- Agree on 4 personal session to work on project (at least 1 hour each) and block time in your calendar
  - Mail me the dates
- Every seminar 10 minutes reserved for team sync
  - Update your GitHub project milestones…

Projects – timeline (details on next slides)

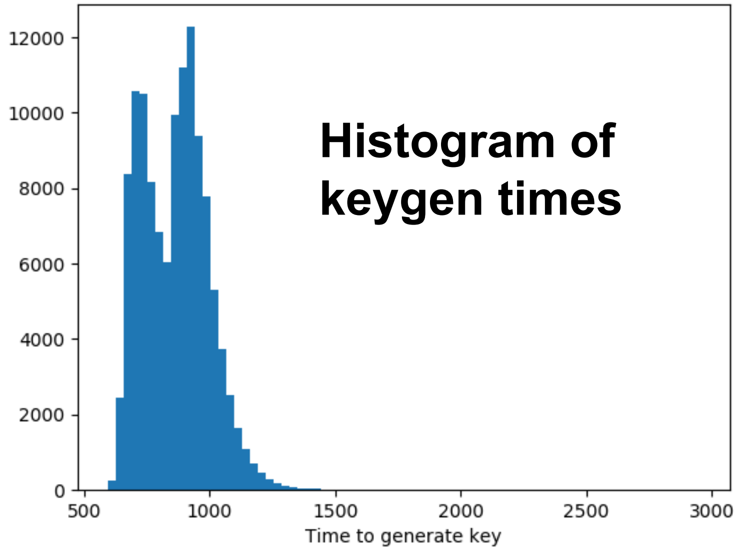
1. Select target library, fork/create repository (4.3.2019)
   - No duplicate libraries allowed, predefined list, FIFO, mail me!
2. Collect 1 million RSA and 1 million ECC keys: 5 points (14.3.2019)
   - Store resulting keys (public and private, primes…) + measured timing + graphs
   - Plot graphs: histogram of MSB and LSB, histogram timing
   - Keygen code, keys, report (max. 2 pages A4) + presentation (your seminar)
3. Analyze crypto operations for side-channel leakage: 7 points (4.4.2019)
   - Time side-channel (random inputs, mostly zeroes, mostly binary ones…)
   - Bonuses: cache-based side-channel; pull requests with fix
   - Report (max. 4 pages A4) + presentation (your seminar group)
4. Implement support for hardware tokens: 8 points (19.4.2019)
   - Key generation in hardware token (PKCS#11, JavaCard…)
   - Sign & encrypt operation using key stored inside token

- At least **10 points** (total) from the project required

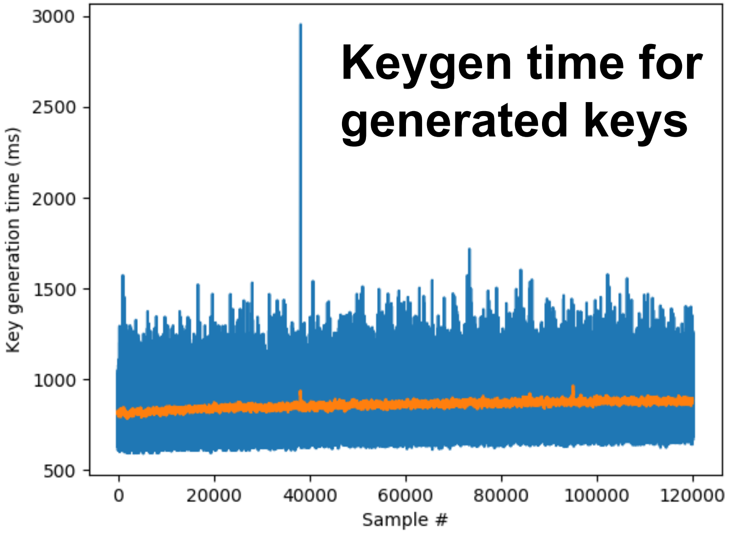
PROJECT: KEY COLLECTION

Collect 1 million RSA and ECC keys

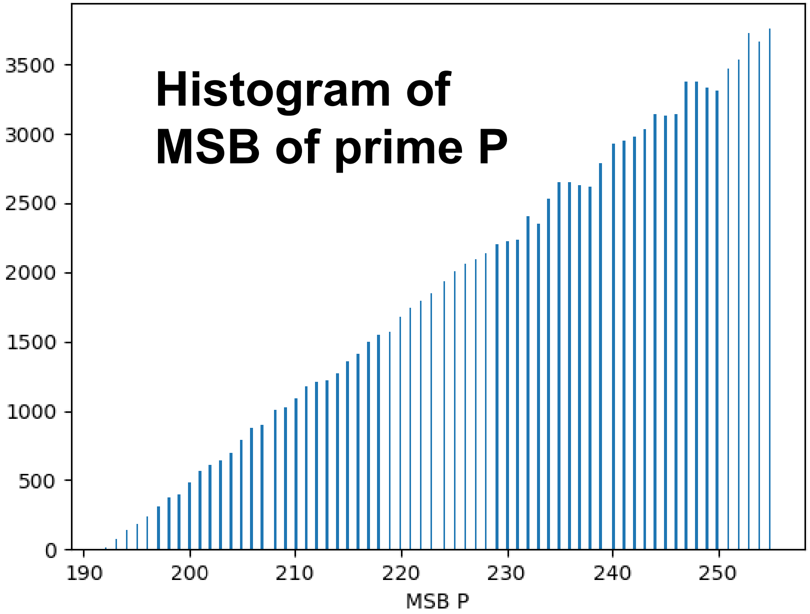
- Investigate library code, locate key generation methods
- Write small program collecting generated keypairs
  - 10^6 RSA-512b keys
  - 10^4 RSA-1024b, 10^4 RSA-2048b
  - 10^6 ECDSA (NIST P-256) keys
  - Store resulting keys (format on next slides)
- Plot graphs using generated keys
  - histogram of MSBs and LSB, timing histogram



Histogram of keygen times

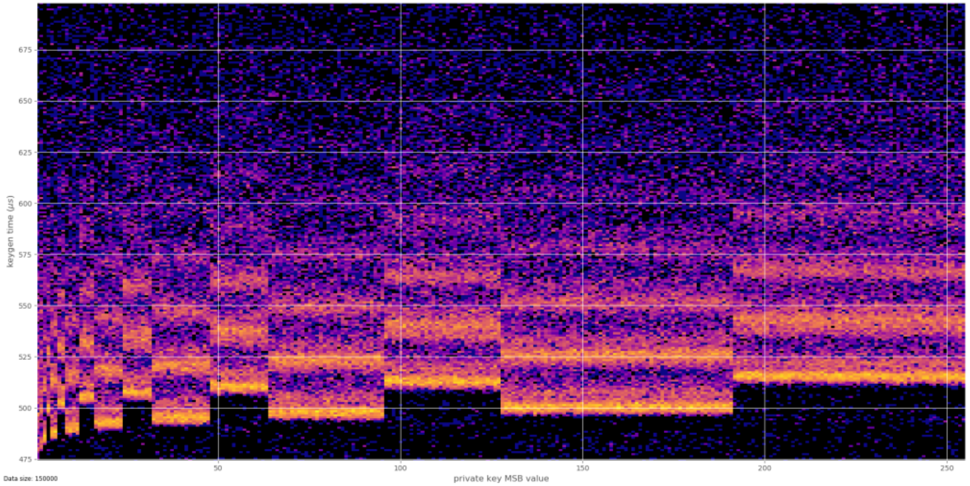


Keygen time for generated keys



Histogram of MSB of prime P

Heatmap of private keys MSB to keygen time



RSA key format

- CSV Format, hexadecimal coding
- **id;n;e;p;q;d;t1;**
- id – simple counter: 1, 2 ….
- n – modulus
- e – public exponent
- p – first prime
- q – second prime
- d – private exponent
- t1 – time to generate key (ns)

ECC key format

- CSV Format, hexadecimal coding
- **id;e;d;t1;**
- id – simple counter: 1, 2 ….
- e – public key
- d – private key
- t1 – time to generate key (ns)

LIBRARIES AVAILABLE FOR SELECTION

- BearSSL
  - https://bearssl.org/
  - Michal Čech, Šimon Doucha a Martin Bulák
- BoringSSL
  - http://www.boringssl.com/
  - Mária Micháliková, Darek Cidlinský, + one other
- Amazon s2n
  - https://github.com/awslabs/s2n
  - Jan Kvapil, Vladmír Sedláček, Ondřej Krčma
- Apple coretls
  - https://opensource.apple.com/tarballs/coreTLS/
  - ??
- Apple corecrypto
  - https://developer.apple.com/security/
  - Tomáš Šlancar, Xichu Zhang + one other

mbedTLS
Pedro Gomes

- GO language crypto
  - https://golang.org/
  - ??
- Mozilla NSS
  - https://hg.mozilla.org/projects/nss
  - ??
- GNU TLS
  - https://gnutls.org/
  - Martin Frian, Pedro Gomes, Peter Sekan
- WolfSSL
  - https://www.wolfssl.com/
  - Daniel Filakovsky, Antonin Dufka, Jakub Bartolomej
- LibreSSL
  - https://www.libressl.org/
  - Natália Gregušková (422562), Daniela Belajová (445323), Nikola Šedivcová (433396)
- Nettle
  - http://www.lysator.liu.se/~nisse/nettle/
  - Richard Kalinec, Ondřej Zoder a Filip Gontko