The properties of RSA key generation process in software libraries

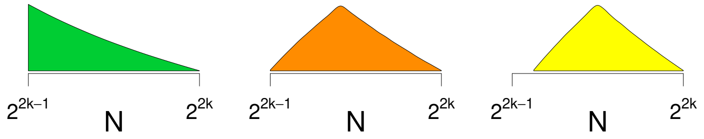
Mgr. Matúš Nemec, supervised by RNDr. Petr Švenda, Ph.D.

Centre for Research on Cryptography and Security, Faculty of Informatics, Masaryk University

Motivation and contributions

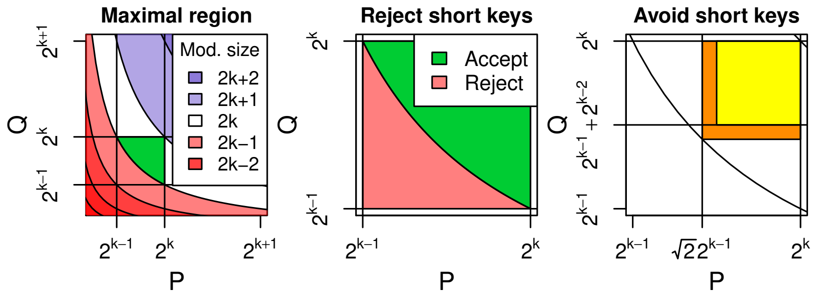
- How different are implementations of RSA keypair generation?
- The keys for the RSA cryptosystem require 2 primes, P and Q; the public modulus N is the product of the primes.
- 18 libraries examined and compared to 6 cryptographic standards.
- 17 methods producing statistically distinct keys found.
- Biased parts identified for 3 levels of knowledge about the keys.

Level 1: Public keys – distribution of the moduli



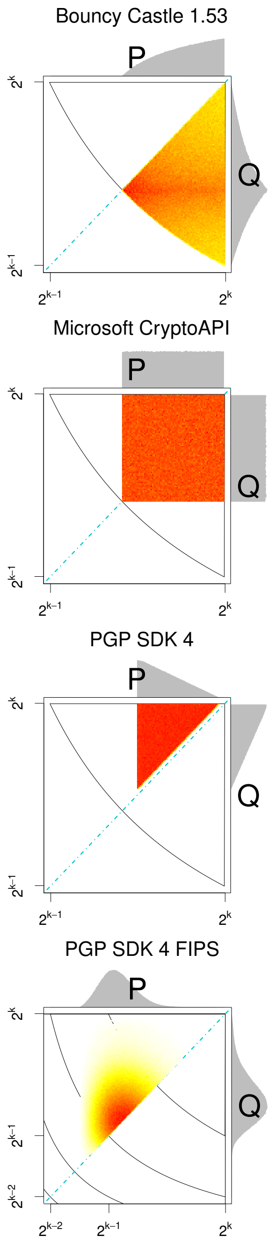
- 3 main distinct distributions of public moduli with many variations were observed, as well as a few unusual methods.
- Software bugs in OpenSSL and GNU Crypto add characteristic properties to the generated keys, effectively fingerprinting them.

Level 2: Private keys – distribution of the prime pairs

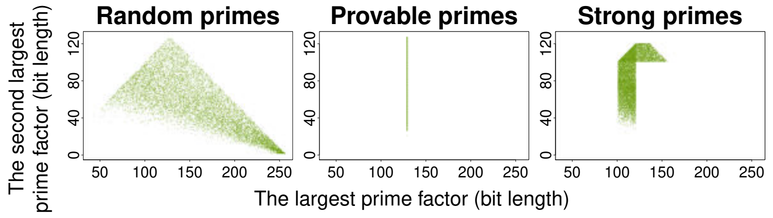


- Both primes are k bits long. Their multiple may be 1 bit shorter than the $2k$-bit modulus. Short keys are rejected or avoided.
- The exact prime generation intervals are revealed – the modulus does not show whether the primes are ordered or not. Similar modulus distributions may hide very different prime regions.

Example prime distributions

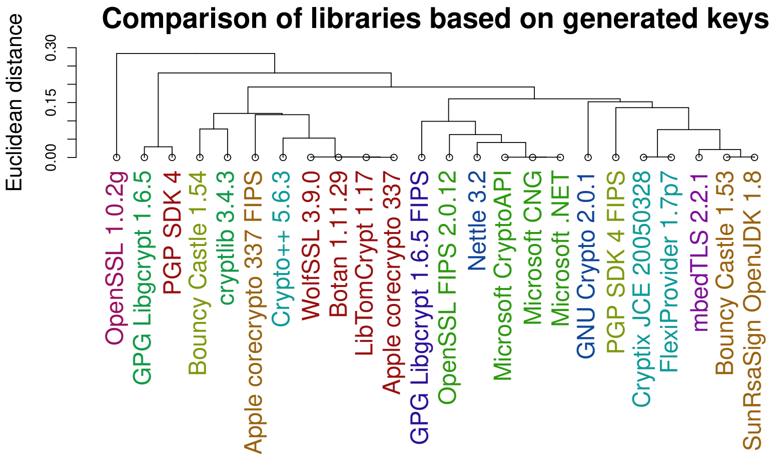


Level 3: Detecting the type of the primes by factorization



- The type of a prime P is revealed by factoring P-1 and $P+1$.
- The libraries use random, provable and "strong" primes, with implications for efficiency and security. Several variations exist.

Results



- The proposed methodology extends well to RSA key sources without published source code (proprietary libraries, smart cards).
- An information leakage vulnerability was revealed, which can be exploited as described in our paper (awarded **Best Paper**).
- P. Švenda, M. Nemec, P. Sekan, R. Kvašňovský, D. Formánek, D. Komárek and V. Matyáš: **The Million-Key Question – Investigating the Origins of RSA Public Keys.** In Proceedings of the 25th USENIX Security Symposium, pages 893–910. 2016.

crcs.cz/rsa

mnemec@mail.muni.cz