The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli

Matúš Nemec, Marek Sýs, Petr Švenda, Dušan Klinec, Vashek Matyáš

Centre for Research on Cryptography and Security, Masaryk University

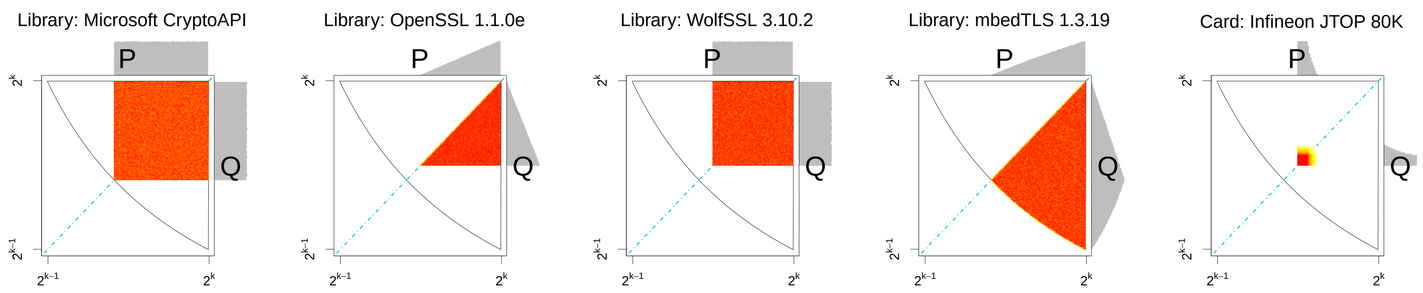
Ca' Foscari University of Venice

Abstract

We discovered an algorithmic flaw in the construction of primes for RSA key generation in a widely-used library of a major manufacturer of cryptographic hardware. The primes suffer from a significant loss of entropy. We proposed a practical factorization method that only requires the value of the public modulus and does *not* depend on a weak or a faulty random number generator. We devised an extension of Coppersmith's factorization attack utilizing an alternative form of the primes in question. The library is found in NIST FIPS 140-2 and CC EAL 5+ certified devices used for a wide range of real-world applications, including identity cards, Trusted Platform Modules, PGP, and tokens for authentication or software signing. The impacted devices are widespread. We responsibly disclosed our findings to the manufacturer of the flawed library. Our work was published at ACM CCS 2017 [1] and received the Real-World Impact Award.

Background – surprising biases in RSA public keys

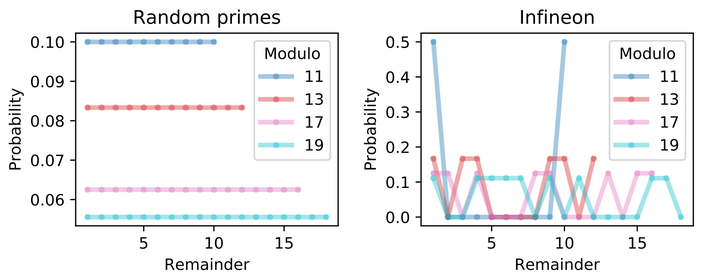
Švenda et al. [2] described how cryptographic libraries generate RSA primes in various ways, introducing subtle biases in the public keys, sufficient to classify the keys based on their origin. Infineon smartcards produced especially biased keys.



The distribution of the most significant bytes of a pair of RSA primes varies for different cryptographic libraries.

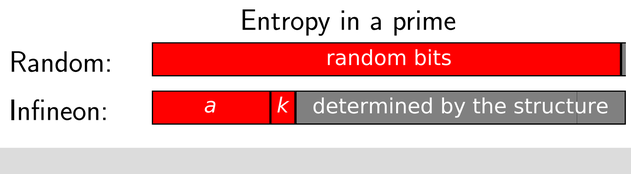
The properties of vulnerable keys

The distribution of the Infineon RSA primes and keys modulo small primes is irregular, unlike randomly chosen primes and keys that are distributed uniformly modulo small primes (left). In fact, the primes belong to a small subgroup modulo a product M of small consecutive primes, what lead us to the discovery of the structure of the primes (right). The primes and RSA moduli suffer from a significant loss of entropy and can be uniquely fingerprinted using a fast discrete logarithm.



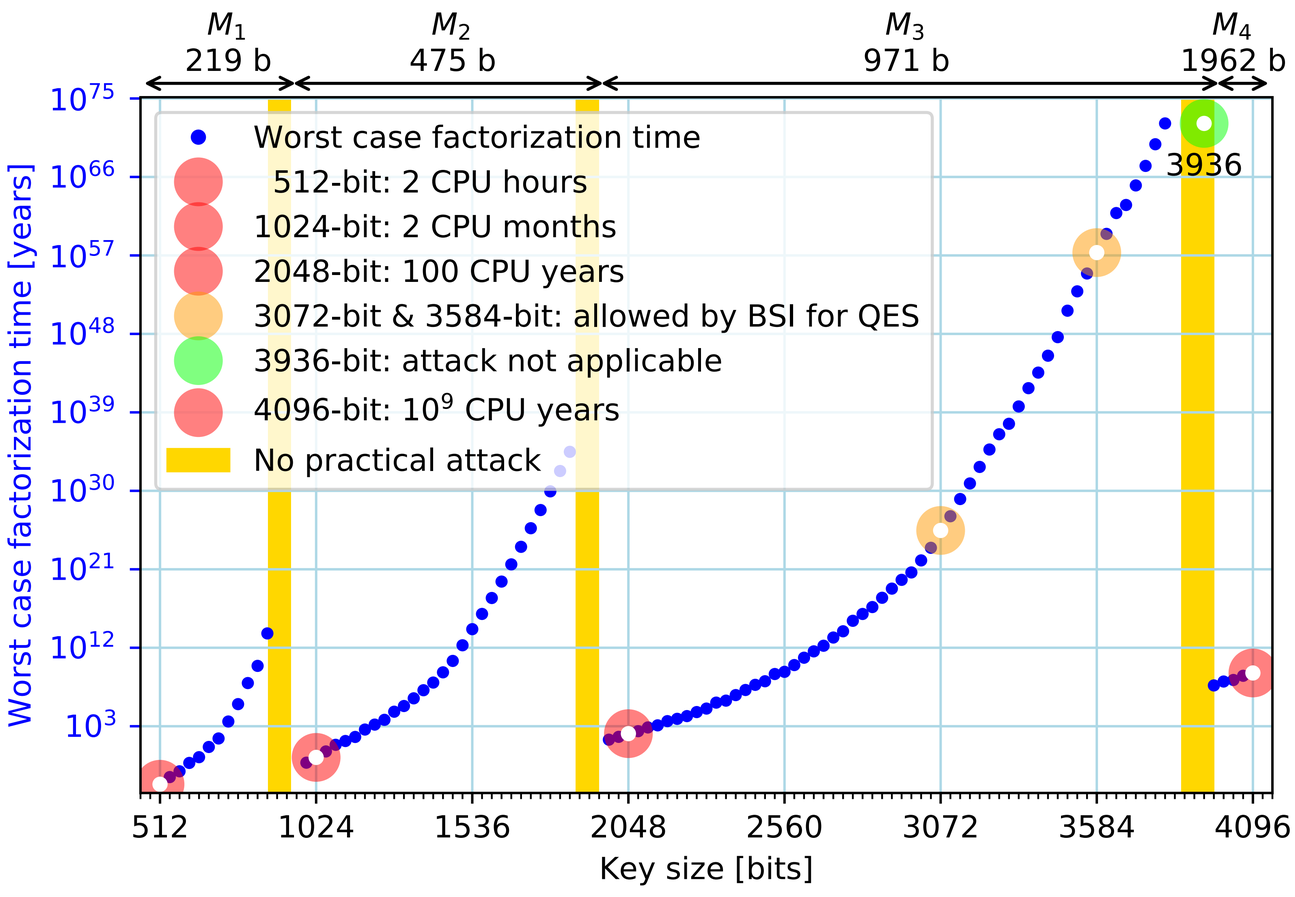
The distribution of RSA keys modulo small primes

$$N = p * q$$
$$p_{ideal} = \text{random prime}$$
$$p_{Infineon} = (k * M + 65537^a \bmod M);\ a, k \in \mathbb{Z}$$
$$M = 2 * 3 * 5 * 7 * \cdots * P_n$$



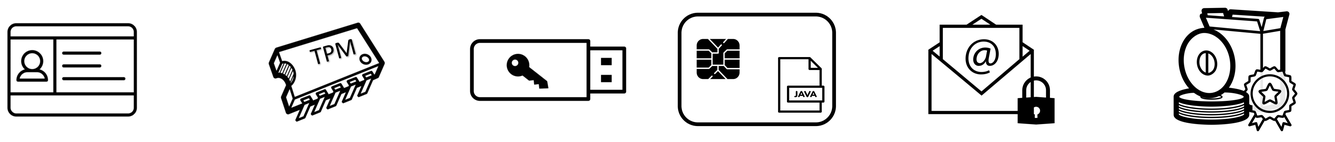
Factorization attack complexity

The complexity of the factorization depends on the size of the keys (horizontal axis). However, due to the different parameters used in their generation (different values of M at the top of the figure), the time required to break a key (vertical axis, blue dots) does not strictly increase. Therefore, some key lengths are more affected, including the common sizes of 1024 bits and 2048 bits. The attack can be easily parallelized with independent processors to achieve a linear speedup.



Impact on real-world applications of cryptographic chips

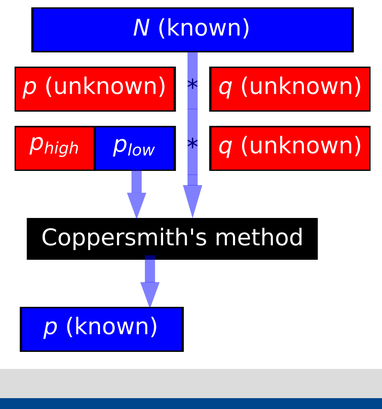
Electronic identity documents (eID) were significantly impacted with Spain, Slovakia, Estonia, Austria, Bulgaria, Brazil, Italy, Kosovo, Malaysia, Poland, and Taiwan affected. Trusted Platform Modules (TPM) used for platform integrity and data encryption (e.g., by Microsoft BitLocker) were vulnerable, as well as authentication tokens and other devices.



Identity documents (eID, eHealth cards) · Trusted Platform Modules · Authentication tokens · Programmable smartcards · Message protection (S-MIME, PGP) · Software signing

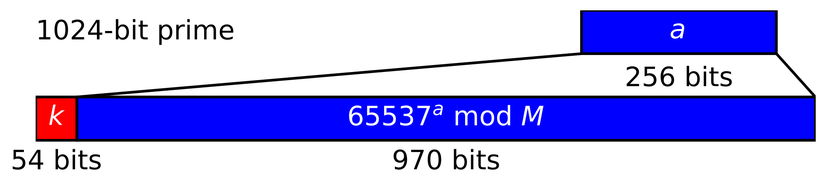
Coppersmith's factorization method

Coppersmith's method uses a partial knowledge of one of the primes to compute the factorization of an RSA modulus. At least half of the bits of the prime must be known. However, the method performs faster with more known bits. We use the method as a black-box tool.

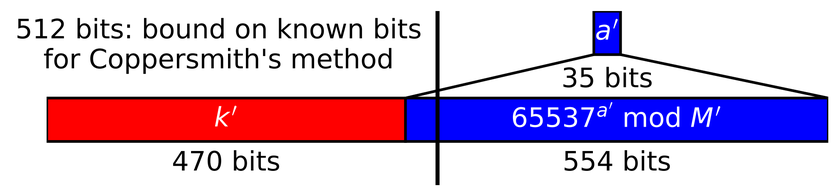


Making the attack practical

To attempt a factorization of a vulnerable RSA key, we guess the value of a and compute the much larger "known" part of the prime as $65537^a \bmod M$. We then try to compute k using Coppersmith's method, what succeeds only if the guess was correct. In the worst case, the attack will require trying half of all the possible values of a.

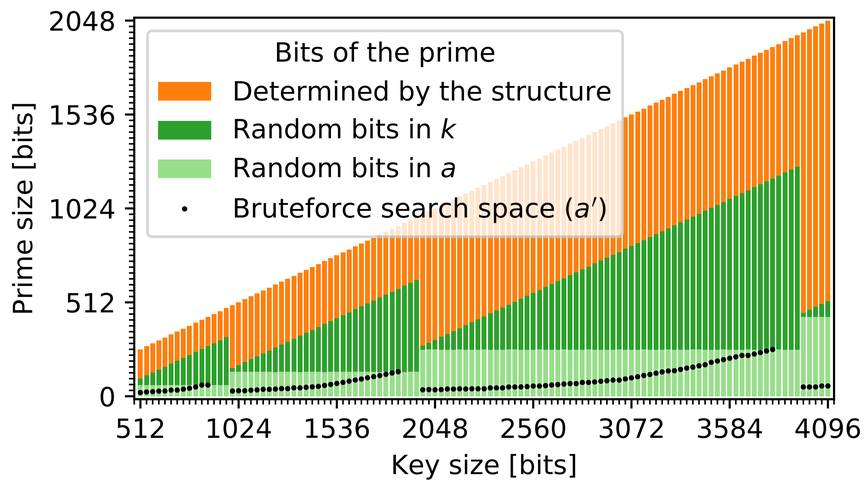


For the majority of RSA key sizes, the bit length of M (and $65537^a \bmod M$) is much larger than the required bound for the attack (one half of the prime's bit length). We find a smaller M' (a divisor of M), such that its size is still sufficient, yet the size of a' is significantly reduced when compared to a.



Entropy in primes

The figure shows the number and origin of random bits in relation to the size of the prime (vertical axis) for keys of given length (horizontal axis). A large portion of prime's bits is determined by the structure (orange) and can be computed from the knowledge of random bits (green). Coppersmith's attack further reduces the required number of known bits even lower (black dots).



The attack optimization process

Smaller values of M' (fewer known bits) require fewer guesses on the value of a'. However, the evaluation of each guess takes more time. We select the parameters corresponding to the minimal overall time of the factorization.

Acknowledgements

This project was supported by the Czech Science Foundation, project GA16-08565S. We greatly appreciate the access to the computing resources of the National Grid Infrastructure MetaCentrum (CESNET LM2015042).

References

[1] Matúš Nemec, Marek Sýs, Petr Švenda, Dušan Klinec, Vashek Matyáš. The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli. In *Proceeding of the 24th ACM Conference on Computer and Communications Security (ACM CCS 2017)*, 2017.

[2] Petr Švenda, Matúš Nemec, Peter Sekan, Rudolf Kvašňovský, David Formánek, David Komárek, Vashek Matyáš. The Million-Key Question – Investigating the Origins of RSA Public Keys. In *Proceeding of the 25th USENIX Security Symposium*, 2016.

roca.crocs.fi.muni.cz

mnemec@mail.muni.cz