# Research Project M2 IPP: trapdooring RSA

Maître de stage: F. MORAIN (LIX)

## 1 Context

RSA is a well known asymmetric cryptosystem. It has resisted to all attacks prior to the invention of the concept of quantum computers. It is still used very much in practice. Building keys involve finding large (probable) primes (around 1024 bits). In some cases, these keys can be built by black-boxes, and it is difficult to prove that they have no trapdoors in them.

## 2 Work to be done

Review attacks on RSA and list the known trapdooring methods. Program them and invent new ones if possible. If time permits, look into trapdoor methods for discrete logarithms based systems.

## 3 Profile

Knowledge of basic asymmetric cryptology, including number theoretic bases. Good experience of programming (Python, C).

## References

[1] Joshua Fried, Pierrick Gaudry, Nadia Heninger, and Emmanuel Thomé. A kilobit hidden SNFS discrete logarithm computation. Cryptology ePrint Archive, Paper 2016/961, 2016.

[2] Adam Young and Moti Yung. The dark side of "black-box" cryptography, or: Should we trust capstone? In *Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings*, volume 1109 of *Lecture Notes in Computer Science*, pages 89–103. Springer, 1996.

[3] Adam Young and Moti Yung. Kleptography: using cryptography against cryptography. In *Proceedings of the 16th Annual International Conference on Theory and Application of Cryptographic Techniques*, EUROCRYPT'97, page 62–74, Berlin, Heidelberg, 1997. Springer-Verlag.

[4] Adam Young and Moti Yung. A space efficient backdoor in rsa and its applications. In Bart Preneel and Stafford Tavares, editors, *Selected Areas in Cryptography*, pages 128–143, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.

[5] Mengce Zheng and Abderrahmane Nitaj. A novel partial key exposure attack on common prime RSA. Cryptology ePrint Archive, Paper 2025/1282, 2025.