ECDSA Attack with partial knowledge for the Nonce

Laurent Imbert and Thomas Roche

1 Subject

ECDSA is certainly the most common digital signature scheme (standardized under [2]) in the world. It is well known that, in theory (see [4]) and in practice (see *e.g.* [1,3]), the knowledge of few consecutive bits of the Nonce (the so-called ephemeral key of ECDSA protocol) for several signatures is enough to recover the long-term secret key. However the number of known bits for a practical attack (6-7 bits for [1], 5 bits for [3]) does not reach the theoretical bound (2 bits are enough [4]). In two very similar recent works (https://minerva.crocs.fi.muni.cz/ and http://tpm.fail/), the gap between theory and practice is reduced.

The student will work on these recent improvements, first by reproducing the attack (in an idealized scenario), which involves both understanding and implementing the key-recovery attack. Then the study can follow different paths, including – but not limited to – (1) the effect of errors in the known bits (problem that always appear in practice), (2) when the known bits position is not the most significant bits of the Nonce, (3) the application of the attack on a real device.

The output of the internship will be a set of tools for ECDSA long-term secret key recovery with partial knowledge of the Nonce.

2 Information

The student should have a good experience in C, C++ or Python and have studied public key cryptography.

The 4 to 6 months internship will take place in an exciting scientific context, in Montpellier, France, at the LIRMM (laboratory of computer science, robotics and microelectronics of the university of Montpellier). It will be supervised by Dr. Laurent Imbert, CNRS researcher in the ECO Team (https://www.lirmm.fr/lirmm_eng/research/teams/eco), and Dr. Thomas Roche, co-founder of the company NinjaLab (https://ninjalab.io).

Depending on the internship outcomes, a PhD student position will be open.

Contact info:
Laurent Imbert (laurent.imbert@lirmm.fr)
Thomas Roche (thomas@ninjalab.io)

References

[1] B. B. Brumley and N. Tuveri. Remote timing attacks are still practical. Cryptology ePrint Archive, Report 2011/232, 2011. https://eprint.iacr.org/2011/232.

[2] FIPS PUB 186-3. *Digital Signature Standard.* National Institute of Standards and Technology, Mar. 2006. Draft.

[3] E. D. Mulder, M. Hutter, M. E. Marson, and P. Pearson. Using bleichenbacher"s solution to the hidden number problem to attack nonce leaks in 384-bit ECDSA. In *Cryptographic Hardware and Embedded Systems - CHES 2013 - 15th International Workshop, Santa Barbara, CA, USA, August 20-23, 2013. Proceedings*, pages 435–452, 2013.

[4] P. Nguyen and I. Shparlinski. The Insecurity of the Elliptic Curve Digital Signature Algorithm with Partially Known Nonces. In *Designs, Codes and Cryptography*, 2003.