MPHELL: a fast and robust library with unified arithmetic for elliptic curves cryptography

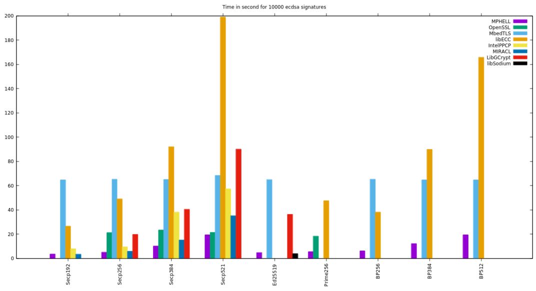
Titouan Coladon, Philippe Elbaz-Vincent, and Cyril Hugounenq

Univ. Grenoble Alpes, CNRS, IF, 38000 Grenoble, France

March 1, 2019

Key Words: C library, Elliptic Curve Cryptography (ECC), Unified arithmetic, SPA resistance.

Creating secure implemantations for elliptic curves arithmetic while preserving performances is not an easy task as shown by the attacks [11, 4, 2, 3] on OpenSSL [10] and GnuPG[6]. We propose a new versatile ECC library based on unified arithmetics with a focus on protection against simple power analysis and an abstract layer for easy customisations. It has been extensively tested on x86-64, ARM 32bits and STM32 architectures and also in real-world applications. Our library has the advantage to propose standard elliptic curves (all those from [9]) but gives also the possibility to use curves in different settings such as Weierstrass form in co-Z coordinates, Jacobi quartic or Edwards forms (as well as their associated conversion functions)[1]. The number arithmetic used in MPHELL is inherited from GMP [7] and has some improvement using Montgomery representation [8] and windowing techniques. Part of this library and the mathematics behind it were described in [1]. In the figure below ECDSA signatures[2] timings are shown for different elliptic curves without taking into account specificity of the curves (as in OpenSSL for instance).



To illustrate the abstraction layer for ground fields and curves, we will also show implemantations based on randomized arithmetic.

Our library will be released under LGPL v3 [5].

This work is supported by ANR-15-IDEX-02, ANR ARRAND (ANR-15-CE39-0002) and SECURIOT-2-AAP FUI 23.

[1] The formulas used are mainly available in the Elliptic Curve Formula Database.

[2] Time in seconds for 10 000 ECDSA signatures

References

[1] M.-A. Cornélie. *Implantations et protections de mécanismes cryptographiques logiciels et matériels.* PhD thesis, Université Grenoble Alpes, 2016.

[2] D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer. Stealing Keys from PCs using a Radio: Cheap Electromagnetic Attacks on Windowed Exponentiation. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 207–228. Springer, 2015.

[3] D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer. ECDH Key-Extraction via Low-Bandwidth Electromagnetic Attacks on PCs. In *Cryptographers' Track at the RSA Conference*, pages 219–235. Springer, 2016.

[4] D. Genkin, L. Pachmanov, I. Pipman, E. Tromer, and Y. Yarom. ECDSA Key Extraction from Mobile Devices via Nonintrusive Physical Side Channels. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 1626–1638. ACM, 2016.

[5] GNU. Gnu general public license, 2015.

[6] GnuPG. GNU privacy guard, 1998.

[7] T. Granlund and the GMP development team. *GNU MP: The GNU Multiple Precision Arithmetic Library*, 2016. Version 6.1.2 `http://gmplib.org/`.

[8] P. L. Montgomery. Modular multiplication without trial division. *Mathematics of computation*, 44(170):519–521, 1985.

[9] N. I. of Standards and T. (NIST). FIPS 186-4: Digital Signature Standard (DSS). *online*, 2013.

[10] T. OpenSSL software foundation. The OpenSSL project, 1999.

[11] J. Van de Pol, N. P. Smart, and Y. Yarom. Just a little bit more. In *Cryptographers' Track at the RSA Conference*, pages 3–21. Springer, 2015.