Arithmetic operators for pairing-based cryptography

Jérémie Detrey*

*Computer Security group, B-IT, Bonn, Germany

Since their introduction in constructive cryptographic applications, pairings over (hyper)elliptic curves are at the heart of an ever increasing number of protocols. Software implementations being rather slow, the study of hardware architectures became an active research area. In this talk, I will first describe an accelerator for the η_T pairing over $\mathbb{F}_3[x]/(x^{97}+x^{12}+2)$. Our architecture is based on a unified arithmetic operator which performs addition, multiplication, and cubing over $\mathbb{F}_{3^{97}}$. This design methodology allows us to design a compact coprocessor (1888 slices on a Virtex-II Pro 4 FPGA) which compares favorably with other solutions described in the open literature.

References

[1] Jean-Luc Beuchat, Nicolas Brisebarre, Jérémie Detrey, and Eiji Okamoto. Arithmetic operators for pairing-based cryptography. In P. Paillier and I. Verbauwhede, editors, *9th International Workshop on Cryptographic Hardware and Embedded Systems (CHES'07)*, pages 239–255, Vienna, Austria, September 2007. Springer-Verlag.