Compact implementations of pairings

Anthony Van Herrewege

***Abstract*—The recent discovery of the constructive use of pairings in cryptography has opened up a wealth of new research options into identity-based encryption. In this paper, we will investigate the possible use of pairings in constrained environments. The focus will be on an small, energy efficient ASIC implementation of an accelerator for the Tate pairing over a supersingular curve.**

The results are encouraging for further research. It is possible to obtain an implementation of less than 30k gates. Furthermore, energy efficiency improvements over twenty times compared to other published designs are possible.

***Index Terms*—Identity-based cryptography, elliptic curve cryptography, Tate pairing, hardware accelerator, ASIC.**

I. Introduction

EVER since Shamir's proposal [1] in '86, there's been an interest in identity-based cryptography. Particulary Boneh and Franklin's [2] discovery of the constructive use of pairings for identity-based encryption has helped spur on new research into possible applications and implementations.

Multitudes of protocols have seen the light, however, untill recently the lack of efficient hardware accelerators for the computationally expensive pairings was always kind of a showstopper towards implementing them. Thus most of the published implementations have a focus on speed. Implementations for area- and/or power-constrainted devices were either deemed infeasible or just not interesting enough.

In 2007 Oliveira *et al.* introduced their TinyTate [3] implementation to the world. 2008 saw the light of TinyPBC [4] and NanoECC [5] from the same authors. All three papers present implementations of pairings (either the Tate or η_T) on the AT128Mega microchip of a Mica node [6], designed for deeply embedded networks. Thus it was proven that pairings were indeed feasible for use in constrained environments, such as sensor networks.

In this paper, we will investigate the feasability of a hardware accelerator for the Tate pairing in constrained environments. In Section II necessary parameters will be defined and we will take a look at the pairing arithmetic. Section III consits of a concise overview of the implementation's hardware. Finally, results from ASIC synthesis will be presented in Section IV and from these a conclussion will be drawn in Section V.

II. Parameters and arithmetic for the Tate pairing

Before we can take a look at the arithmetic behind the Tate pairing computation, some parameters need to be set. First and foremost, we decided to define the pairing over a supersingular elliptic curve in a finite field modulo two:

$$E(\mathbb{F}_{2^m}) : y^3 + y = x^3 + x + b,$$

with $b \in \{0,1\}$. We also define [7]:

$$\delta = \begin{cases} b & m \equiv 1,7 \pmod 8 \\ 1-b & m \equiv 3,5 \pmod 8 \end{cases}$$
$$\nu = (-1)^{\delta}$$

The value of b set to whatever value maximizes the order of the curve [7], [8]:

$$\#E(\mathbb{F}_{2^m}) = 2^m + \nu\sqrt{2^{m+1}} + 1.$$

So, before the value of b can be decided on, m is to be set.

Considering that the final implementation should be as small as possible, we settle on $m = 163$, which, according to [9], should still provide reasonable security. If necessary, the hardware which will be proposed in Section III can easily be adapted to larger fields. From [10] the reduction polynomial is chosen to be

$$R = z^{163} + z^7 + z^6 + z^3 + 1.$$

This type of supersingular curve has an embedding degree $k = 4$. The result of the Tate pairing will be an element in $\mathbb{F}_{2^{4m}}$. We define this field by means of tower extensions [11]:

$$\mathbb{F}_{2^{2m}} \cong \mathbb{F}_{2^m}[x]/\left(x^2 + x + 1\right)$$
$$\mathbb{F}_{2^{4m}} \cong \mathbb{F}_{2^{2m}}[y]/\left(y^2 + (x+1)y + 1\right)$$

Zo

III. Hardware implementation

IV. Results

V. Conclussion

References

[1] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proceedings of CRYPTO 84 on Advances in cryptology*. New York, NY, USA: Springer-Verlag New York, Inc., 1985, pp. 47–53.

[2] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," *SIAM J. Comput.*, vol. 32, no. 3, pp. 586–615, 2003.

[3] L. B. Oliveira, D. F. Aranha, E. Morais, F. Daguano, J. López, and R. Dahab, "TinyTate: Computing the Tate Pairing in Resource-Constrained Sensor Nodes," in *Sixth IEEE International Symposium on Network Computing and Applications*. IEEE Computer Society, 2007, pp. 318–323.

[4] L. B. Oliveira, M. Scott, J. López, and R. Dahab, "TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks," in *5th International Conference on Networked Sensing Systems*, 2008, pp. 173–180.

[5] P. Szczechowiak, L. B. Oliveira, M. Scott, M. Collier, and R. Dahab, "NanoECC: Testing the Limits of Elliptic Curve Cryptography in Sensor Networks." *European conference on Wireless Sensor Networks (EWSN08)*, 2008.

Anthony Van Herrewege obtained his B.S. in computer engineering from K.U. Leuven, Leuven, Belgium in 2007. This paper is part of his thesis towards obtaining a M.Sc. in electrical engineering from the same university. Email: anthonyvh@gmail.com.

[6] J. L. Hill and D. E. Culler, “Mica: a wireless platform for deeply embedded networks,” *Micro, IEEE*, vol. 22, no. 6, pp. 12–24, 2002.

[7] J.-L. Beuchat, N. Brisebarre, J. Detrey, E. Okamoto, and F. Rodrguez-Henrquez, “A Comparison Between Hardware Accelerators for the Modified Tate Pairing over $\mathbb{F}_{2^m}$ and $\mathbb{F}_{3^m}$,” in *Lecture Notes in Computer Science*, vol. 5209. Springer, 2008, pp. 297–315.

[8] P. S. L. M. Barreto, H. Y. Kim, B. Lynn, and M. Scott, “Efficient Algorithms for Pairing-Based Cryptosystems,” in *CRYPTO 02: Proceedings of the 22nd Annual International Cryptology Conference on Advances in Cryptology*. Springer-Verlag, 2002, pp. 354–368.

[9] A. K. Lenstra and E. R. Verheul, “Selecting Cryptographic Key Sizes,” *Journal of Cryptology*, vol. 14, pp. 255–293, 2001.

[10] Certicom Corporation, *SEC 2: Recommended Elliptic Curve Domain Parameters*, september 2000. [Online]. Available: http://www.secg.org

[11] G. Bertoni, L. Breveglieri, P. Fragneto, G. Pelosi, and L. Sportiello, “Software implementation of Tate pairing over GF(2^m),” in *DATE 06: Proceedings of the conference on Design, automation and test in Europe*. European Design and Automation Association, 2006, pp. 7–11.