An FPGA-based Accelerator for Tate Pairing over Prime Fields

Marcin Rogawski, Ekawat Homsirikamol, and Kris Gaj
George Mason University

Abstract

Pairing-based cryptography has emerged as an important alternative and supplement to traditional public key cryptography. Pairing-based schemes can be used for identity-based encryption, short signatures, identity-based signatures, tripartite key exchange protocols, cryptanalysis, and many other important applications. Compared to other popular public key cryptosystems, such as Elliptic Curve Cryptography (ECC) and RSA, pairing-based schemes are much more computationally intensive. Therefore, hardware acceleration based on modern high-performance FPGAs is an important implementation option.

Pairing-schemes over prime fields are considered particularly resistant to cryptanalysis, but at the same time, the most challenging to implement in hardware. One of the most promising optimization options is taking advantage of embedded resources of modern FPGAs. Practically all FPGA vendors incorporate in modern FPGAs, apart from basic reconfigurable logic blocks, also embedded components, such as DSP units, Fast Carry Chain Adders, and large memory blocks. These hardwired FPGA resources, together with meticulously selected prime numbers, such as Mersenne, Fermat, or Solinas primes, can serve as a basis of an efficient hardware implementation.

In this paper, we demonstrate a novel high-speed architecture for Tate pairing over prime fields, based on the use of Solinas primes, Fast Carry Chains, and DSP units of modern FPGAs. Our architecture combines Booth recoding, Barrett modular reduction, and the high-radix carry-save representation in the new design for modular multiplication over Solinas primes. Similarly, a low-latency modular adder, based on high-radix carry save addition, Fast Carry Chains, and the Kogge-Stone architecture, has been proposed. The modular multiplier and adder based on the aforementioned principles have been used as basic building blocks for a higher level application - a high-speed hardware accelerator for Tate pairing on twisted supersingular Edwards curves over prime fields.

Our design has been implemented using two high-speed FPGA families: Altera Stratix IV and Xilinx Virtex 6. All architectures have been first modeled in VHDL-93, and their functionality verified using software implementations in C and Magma. The coprocessor was then synthesized, mapped, placed, and routed using tools of the respective vendor. The tool options were selected in such a way, that the embedded resources, such as DSP units and block memories, were inferred during implementation. The fastest version of our design calculates Tate pairing at 80, 120 and 128-bit security over prime fields in less than 0.2, 0.5 and 0.7 ms, respectively.

Experimental measurements of our designs, based on the use of high-performance FPGA boards from PLDA Inc., supporting the PCI Express Gen 2 protocol, are currently in progress, and their results will be incorporated in the final version of the paper.