Summary of the HAH project - Hardware and Arithmetic for Hyperelliptic Curves Cryptography

HAH consortium

October 2014 - December 2017

Project web page for details: https://h-a-h.cominlabs.u-bretaguenoire.fr/

1. Consortium and Funding

- Lab-STIC laboratory (UMR 6285, MOCS team, since 01.01.2017) and IRISA laboratory (UMR 6074, CAIRN team, before 31.12.2016): Gabriel Gallin (PhD student funded by HAH), Audrey Lucas (PhD student not funded by HAH) and Arnaud Tisserand (DR CNRS).
  
  Institutions: CNRS, University Rennes 1 (UR1), University South Brittany (UBS).
  
  Partial funding: Labex CominLabs and Brittany Région.

- IRMAR laboratory (UMR 6625, GAR Team): Türkü Özlıüm Çelik (PhD student funded by HAH), Sylvain Duquesne (PR Univ. Rennes 1) and Christophe Ritzenhaler (PR Univ. Rennes 1).
  
  Institutions: CNRS, University Rennes 1.
  
  Partial funding: Labex Lebesgue.

2. Introduction

Asymmetric (or public key) cryptography is used for key exchange/agreement (for sharing a common secret key in symmetric cryptosystems), in authentication primitives (of messages, devices, users) and specific cyphering schemes. Asymmetric cryptography was performed using RSA over a long period. But due to works in cryptanalysis and efficient parallel implementations, the size of RSA parameters must increase of lot. For instance, today at least 2048 bits keys, modulus and internal operands are recommended for RSA.

Elliptic curve based cryptography (ECC) was adopted during the last two decades as an efficient alternative to RSA. For instance, ECC requires computations over 256 bits values to achieve a similar security level than RSA with 2048 bits. More recently, hyper-elliptic curve cryptography (HECC) was proposed as a more advanced solution compared to ECC with more efficient computations for the same security level.

Reducing the cost of asymmetric cryptography is a challenge for hardware implementation of embedded systems where silicon area is limited. Hyper-elliptic curve cryptography (HECC) is considered to be an interesting solution compared to elliptic curve cryptography (ECC) and RSA. HECC requires smaller finite fields than ECC at similar security level. Recent HECC solutions based on Kummer surfaces demonstrate promising improvements for embedded software implementations (30 to 70 % clock cycles count reduction compared to the best similar curve based solutions at equivalent security level).

In the HAH project, we study and propose hardware architectures for recent HECC solutions and their FPGA implementations. We study and evaluate the impact of various architecture parameters on the cost and performances: type, size and number of units (arithmetic, memory, internal communications); architecture topology; and exploitation of internal parallelism and security against side channel attacks. We also provide open source code for our hardware (some arithmetic units and accelerator) and software tools (for hardware units generation).
3. Contributions

We first worked on highly optimized operators for multiplication in GF($p$) arithmetic. Then we used those multipliers in various cryptoprocessor for HECC.

3.1 Hardware Modular Multipliers with Hyper-Threading Architecture for HECC

Hardware cryptographic accelerators require efficient arithmetic units over finite fields (128-bit prime ones in this project). The most common and costly finite field operation in HECC is the modular multiplication (MM). Most of MM algorithms over prime fields are derived from Montgomery algorithm. They improve efficiency by interleaving partial products generation and modular reduction steps to reduce the width of intermediate data and to gain some speedup. Over prime fields, it uses dependent partial products and reduction steps. These dependencies make FPGA implementations with fully pipelined DSP blocks difficult to optimize. We propose a new multiplier architecture with hyper-threading capabilities. Several independent multiplications are handled in parallel for efficiently filling the pipeline and overlapping internal latencies by independent computations. It increases the silicon efficiency and leads to a better area / computation time trade-off than current state of the art of efficient modular GF($p$) multipliers operators. One important constraint for hardware implementations comes from strong data dependencies inside the main loop of partial products accumulation and modular reduction. Modern FPGAs embed many dedicated hardware resources for performing small integer multiplications and accumulations (e.g. $18 \times 18 \pm 48$ bits). To reach high frequencies, DSP blocks must use several internal pipeline stages. These stages reduce circuit efficiency with lower utilization of DSP blocks. Finite field elements are decomposed into several words. We propose a new of hardware unit called hyper-threaded modular multiplier (HTMM) to improve efficiency in small hardware units where the modulo $p$ can be selected without constraint at design time. It roughly consists in interleaving independent multiplications in the same hardware resource to fill the pipeline as much as possible. HTMM can be seen as multiple logical multipliers sharing the same physical resource (like in hyperthreaded processors). The iterations for the various multiplications are interleaved in the operator.

As the number of parameters is important and they have very different impact of the best type of architecture, we designed a software generator for HTMM (distributed as open-source code). Based on a small set of parameters and optimization directives, it generates synthesizable VHDL descriptions for various HTMM operators and optimizations targets.

HTMM leads to faster products for about half the cost of the best state of the art solution. In some cases we improve by a factor of 3 to 4 the throughput per area ratio.

Important results:

- Paper at the IEEE Asilomar 2017 Conference (see below)
- Open-source code generator: https://sourcesup.renater.fr/htmm/
- A paper submitted to the journal IEEE Transactions on Computers is under major revision (in october 2018)

3.2 Hardware Accelerators for HECC Scalar Multiplication

A paper presented at CHES 2016 by Rennes et al. (see Links below) proposed a new Kummer-based HECC (KHECC) solution and its implementation on microcontrollers with 30 to 70 % clock cycles count reduction compared to the best similar curve based solutions at equivalent security level. In HAH, we proposed the first hardware architectures for scalar multiplication in KHECC adapted from this paper their FPGA implementations.

KHECC has several advantages:

- smaller finite fields width (half of those for ECC like in typical HECC solutions)
- efficient xDBLADD operation for iterations in the scalar multiplication with a constant time and uniform behavior against some side channel attacks
- large and regular internal parallelism as illustrated in Figure 1

We study and evaluate the impact of various architecture parameters on the cost and performances: type, size and number of units (arithmetic, memory, internal communications); architecture topology; and exploitation of internal parallelism. We explored several configuration of the internal width ($w$) of the
units and internal communications. The field width is 128 bits with prime $p = 2^{127} - 1$. There are several types of resources in our hardware accelerators: arithmetic units for field level operations (F p addition, subtraction and multiplication with generic prime p in this work); memory unit(s) for storing intermediate values (F p elements for points coordinates), curve parameters and constants; a CSWAP unit in charge of scalar management and on-line schedule of operands depending on scalar/key bit values; an internal communication system for data transfers between the units; a control based on a microcode running the architecture.

The best configuration depends on the objective (high speed or low area) and target FPGA. Then exploration tools at architecture level are helpful for designers and users. The obtained results lead to similar speed than the best curve based solutions for embedded systems but with an area almost divided by 2 (-40 % for DSP and RAM blocks and -60 % for logic slices).

**Important results:**
- Paper at the IndoCrypt 2017 Conference (see below)
- Open-source code be will available on the project web page (after the last publication due to anonymous submission)

**Results**

**PhD Theses from the project**
- Gabriel GALLIN. Defense scheduled for the 29th of November 2018. Title: Hardware arithmetic units and crypto-processors for cryptography over hyper-elliptic curves.

**Award, Invitations and Program Chairs**
- Best paper award for the Architecture track at Compas French conference, June 2015, Lille, France, for the paper “Comparaison expérimentale d’architectures de crypto-procéssseurs pour courbes elliptiques et hyper-elliptiques” by Gabriel Gallin, Arnaud Tisserand and Nicolas Veyrat-Charvillon
- Arnaud Tisserand was Program Chair with Julio Villalba of the 2nd IEEE Symposium on Computer Arithmetic (ARITH), June 2015, Lyon, France
- Arnaud Tisserand was Invited Speaker at 19th Workshop on Elliptic Curve Cryptography (ECC), September 2015, Bordeaux, France, on “Hardware Accelerators for ECC and HECC”
- Sylvain Duquesne was Program Chair, with Svetla Petkova-Nikova, of the 6th International Workshop Arithmetic of Finite Fields (WAIFI), July 13-15, 2016 in Ghent, Belgium, LNCS
- Arnaud Tisserand was Invited Speaker at Colloque GDR SOC2, June 2017, Bordeaux, France on “Embedding Crypto in SoCs: Threats and Protections”
- Arnaud Tisserand was Invited Speaker at CRISSIS: 12th International Conference on Risks and Security of Internet and Systems, September 2017, Dinard, France, on “Hardware Support for Physical Security”
- Arnaud Tisserand was the main organizer of CryptArchi 2018: 16th International Workshop on Cryptographic Architectures embedded in logic devices, June 2018, Lorient (Guidel-Plages), France.

**Other Publications**
- Razvan Barbulescu and Sylvain Duquesne: Updating key size estimations for pairings Journal of Cryptology : 2018
- A. Lucas and A. Tisserand: ECC Protections against both Observation and Perturbation Attacks CryptArchi 2017: 15th International Workshops on Cryptographic architectures embedded in logic devices : 2017
- G. Gallin and A. Tisserand: Finite Field Multiplier Architectures for Hyper-Elliptic Curve Cryptography (poster) XIIème Colloque National du GDR SOC2 : 2017
• Lucas Audrey and Arnaud Tisserand: ECC Protections against both Observation and Perturbation Attacks CryptArchi 2017: 15th International Workshops on Cryptographic architectures embedded in logic devices : 2017
• Gabriel Gallin and Arnaud Tisserand: Hardware Architectures for HECC CryptArchi 2017: 15th International Workshops on Cryptographic architectures embedded in logic devices : 2017
• Gabriel Gallin and Turku Ozlum Celik and Arnaud Tisserand: Architecture level Optimizations for Kummer based HECC on FPGAs IndoCrypt: 18th Internat. Conf. on Cryptology in India : 2017
• Gabriel Gallin and Arnaud Tisserand: Hardware Architectures Exploration for Hyper-Elliptic Curve Cryptography 6ème rencontre Crypto’Puces, du composant au système communicant embarqué : 2017
• Md Al-Amin Khandaker, Yuki Nanojo, Loubna Ghammam, Sylvain Duquesnes, Yasuyuki Nogami and Yuta Kodera: Efficient Optimal Ate Pairing at 128-bit Security Level IndoCrypt 2017 - 18th International Conference on Cryptology : 2017
• Sylvain Duquesnes, Yasuyuki Nogami, A. Khandaker and H. Soo: Efficient Scalar Multiplication for Ate Based Pairing over KSS Curve of Embedding Degree 18 WISA : 2017
• Sylvain Duquesnes, Nadia El Mrabet, Safia Haloui and Franck Rondepierre: Choosing and generating parameters for low level pairing implementation on BN curves Applicable Algebra in Engineering, Communication and Computing : 2017
• Sylvain Duquesne and Loubna Ghammam: Memory-saving computation of the pairing final exponentiation on BN curves Groups Complexity Cryptology : 2016
• Pinar Kilicer, Hugo Labrande, Reynald Lercier, Christophe Ritzenthaler, Jeroen Sijsling, Marco Streng: Plane quartics over Q with complex multiplication (Preprint) : 2016
• Christophe Ritzenthaler, Matthieu Romagny: On the Prym variety of genus 3 covers of genus 1 curves (Preprint) : 2016
• Reynald Lercier, Christophe Ritzenthaler, Jeroen Sijsling: Reconstructing plane quartics from their invariants (Preprint) : 2016
• Gabriel. Gallin and Arnaud Tisserand: Comparaison expérimentale d’architectures de crypto-processeurs pour courbes elliptiques et hyper-elliptiques Journées Codage et Cryptographie du GDR IM : 2015
• G. Gallin, A. Tisserand and N. Veyrat-Charvillon: Comparaison expérimentale d’architectures de crypto-processeurs pour courbes elliptiques et hyper-elliptiques ComPAS’2015: Conférence d’informatique en Parallélisme, Architecture et Système : 2015