An FPGA-based Accelerator for Tate Pairing on Edwards Curves over Prime Fields

Marcin Rogawski Ekawat Homsirikamol **Kris Gaj**

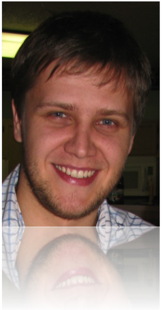
Cryptographic Engineering Research Group (CERG)
Department of ECE, Volgenau School of Engineering
George Mason University, Fairfax, VA, USA

11th CryptArchi Workshop - Fréjus , June 23-26, 2013

Co-authors

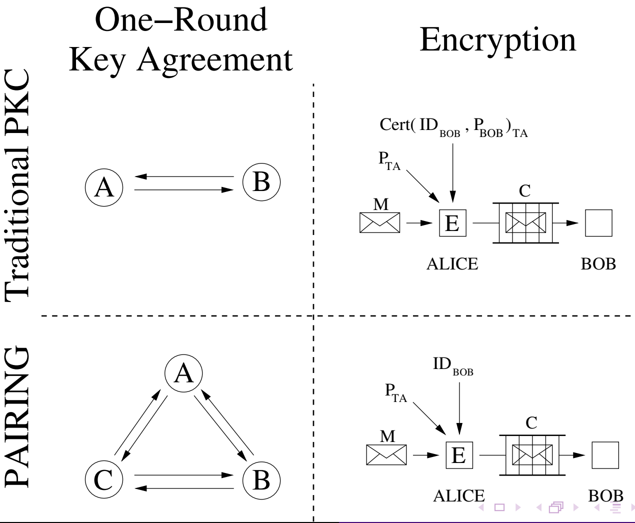
Co-Authors

Marcin Rogawski



Ekawat Homsirikamol a.k.a "Ice"

Pairing Based Cryptography



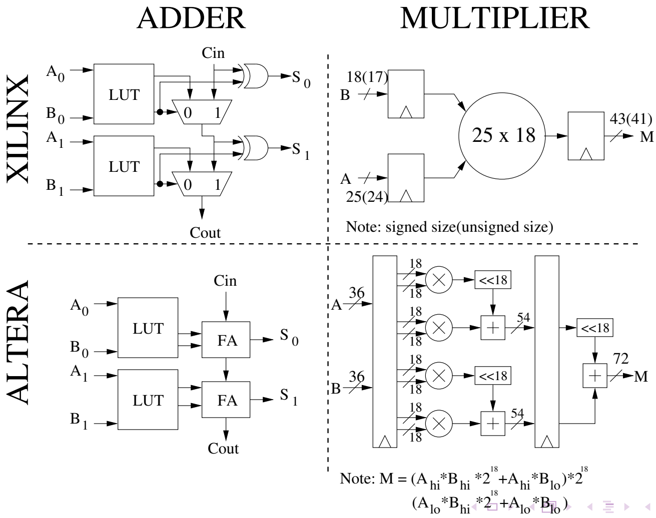
Prime Fields

- Pairing transformations can be defined over multiple fields: binary - GF(2^n), ternary - GF(3^m), and prime fields - GF(p)
- Binary and ternary fields are generally hardware-friendly
- Prime fields are generally better for software implementations and for cross-platform solutions
- The National Security Agency (NSA Suite B Cryptography) and eCRYPT II recommend prime fields

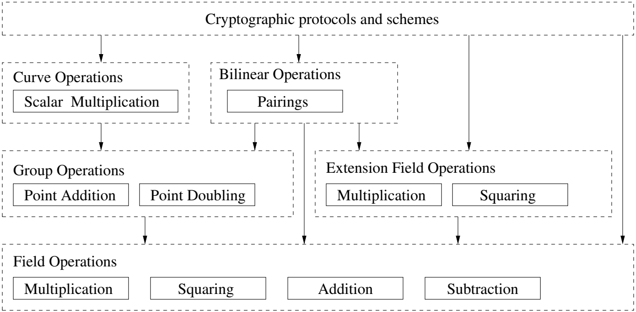
Scope of this work

Efficient implementation of Pairing Based Cryptosystems over prime fields using internal resources of modern FPGAs, such as fast carry chains (carry logic) and DSP units.

Internal Resources of Modern FPGAs



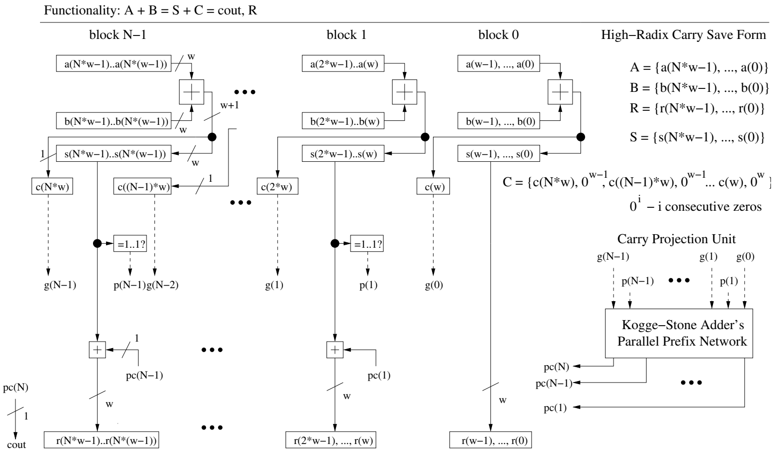
Hierarchy of Operations in Pairing Based Cryptography (PBC)



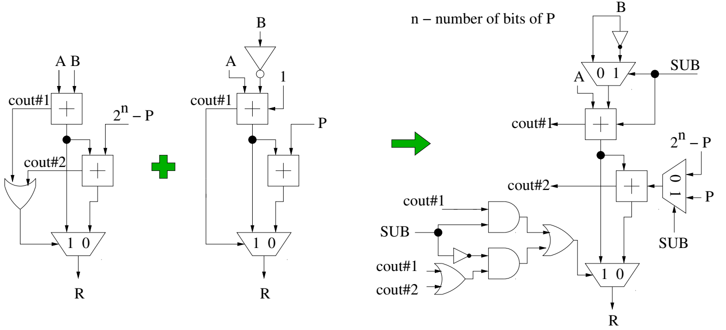
Hardware architecture recipe:

Optimizations on every level CAN NOT be conducted totally independently!

Novel Hybrid high-radix carry save adder with parallel prefix Kogge-Stone network



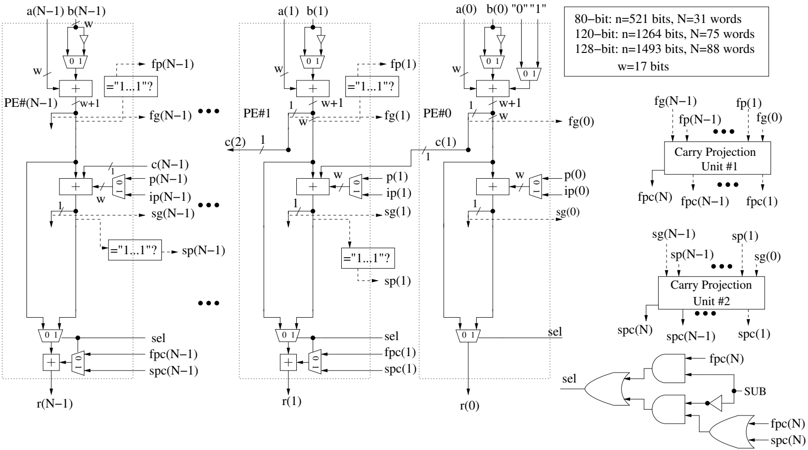
Generic modular adder



- $R = A + B \mod P$, $R = \begin{cases} A + B - P, & \text{if } A + B \geq 2^n \vee A + B - P \geq 0 \\ A + B, & \text{otherwise} \end{cases}$
- $R = A - B \mod P$, $R = \begin{cases} A - B + P, & \text{if } A - B < 0 \\ A - B, & \text{otherwise} \end{cases}$

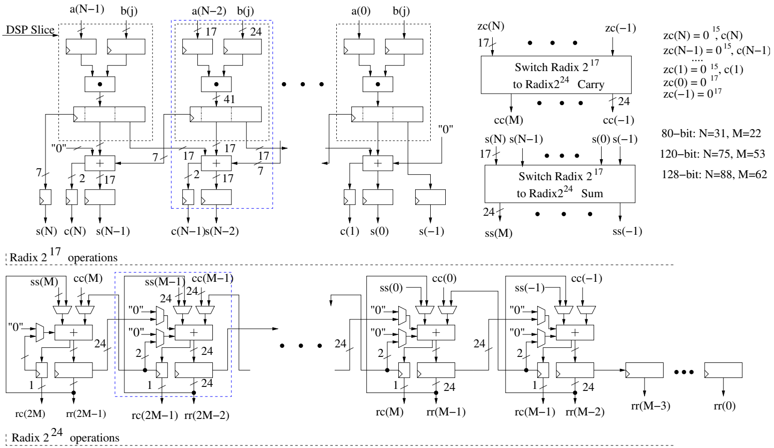
Novel modular adder/subtractor

Functionality: (A + B) mod P = R   A = {a(N−1), ..., a(0)}, B = {b(N−1), ..., b(0)}, P = {p(N−1), ... p(0)}, IP = two's complement of P



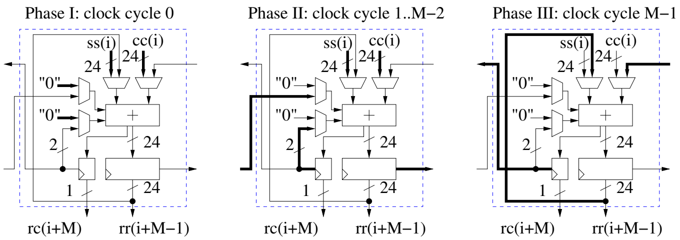
Novel Multiply-and-Add DSP-based multiplier 1/2

Functionality: A * B = (RR, RC), where A = {a(N−1), ..., a(0)}, B = {b(N−1, ...,0}, RR = {rr(2M−1), ..., rr(0)}, RC = {rc(2M−1), ..., rc(0)}



Novel Multiply-and-Add DSP-based multiplier 2/2

Three operational phases of the selected processing element:



Protocol	Xilinx Virtex-6	Altera Stratix IV & V
#bits of A processed per clock cycle	n	n
#bits of B processed per clock cycle	24	36
#clock cycles per multiplication	$\lceil \frac{n}{24} \rceil$	$\lceil \frac{n}{36} \rceil$
#DSP units	$\lceil \frac{n}{17} \rceil$	$\lceil \frac{n}{36} \rceil$
Meaning of DSP unit	DSP48E1 slice	Half-DSP block

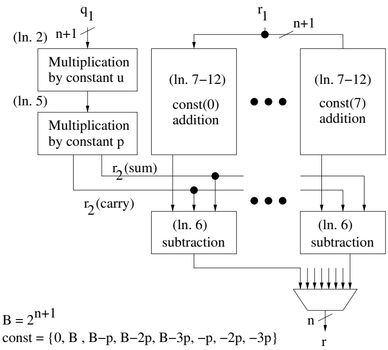
Arithmetic for Special Primes

- Reductions modulo 2^n+1 and modulo 2^n-1 are very efficient. (Problem: Not every number of this form is prime!)
- Primes of a form ($2^a \pm 2^b \pm 1$ and $2^a \pm 2^b \pm 2^c \pm 1$) were introduced by Solinas [NSA'99], Solinas prime's arithmetic is recommended by NIST for digital signature schemes [FIPS-186]!

Comment:

But it is not applicable for all primes in Solinas form!
(e.g.: $2^{520} + 2^{363} - 2^{360} - 1$)

Novel solution: Barrett-based reductor for Solinas primes



Algorithm 1 Barrett modular reduction [Crypto'86]

Require: $x = (x_{2n-1} \ldots x_1, x_0)_2$, $p = (p_{n-1} \ldots p_1, p_0)_2$ $(p_{n-1} \neq 0)$, $\mu = \lfloor 2^{2n} / p \rfloor$

Ensure: $r = x \bmod p$

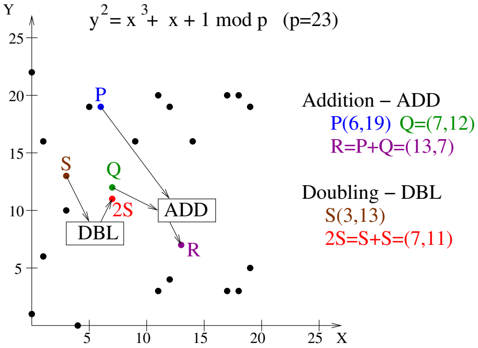
1: $q_1 \leftarrow \lfloor x/2^{n-1} \rfloor$
2: $q_2 \leftarrow q_1 * \mu$
3: $q_3 \leftarrow \lfloor q_2/2^{n+1} \rfloor$
4: $r_1 \leftarrow x \bmod 2^{n+1}$
5: $r_2 \leftarrow q_3 * p \bmod 2^{n+1}$
6: $r \leftarrow r_1 - r_2$
7: **if** $r < 0$ **then**
8: $\quad r \leftarrow r + 2^{n+1}$
9: **end if**
10: **while** $r \geq p$ **do**
11: $\quad r \leftarrow r - p$
12: **end while**
13: **return** r

Comment:

p can be chosen in such a way, that $\mu = 2^{a_{t-1}} + 2^{a_{t-2}} + \ldots + 2^{a_1} + 2^0$, where t is a relatively small number.

Elliptic Curve Cryptography

- Definition: Elliptic curve over $GF(p)$ is a set of points fulfilling equation of the curve and special point ∞.



- $\exists P(generator) : P, 2P, 3P, ...mP = \infty$

Edwards curves + application

- Edwards curve [AmericanMath'07] is a set of points which fulfill equation $x^2 + y^2 = 1 + dx^2y^2$ mod p
- generalized form $ax^2 + y^2 = 1 + dx^2y^2$ mod p - a-twisted Edwards curves proposed by Bernstein et al. [AfricaCrypt'08]
- Extended projective formulae defined by Hisil et al. [AsiaCrypt'08]
- An elliptic curve is called supersingular, if its number of points is equal to $p + 1$
- Edwards curves together with special prime number P-25519 were adopted to digital signatures by Bernstein et al. [CHES'11]

What is Pairing?

Pairing is a mathematical transformation which takes two arguments: two elliptic curve points P and Q from two algebraic groups G_1 and G_2 and it produces an element of the third algebraic group G_T.
The most important properties of these $G_1 \times G_2 \rightarrow G_T$ functions are:

- bilinearity $\forall$ a,b $\in Z_p$:
  $e(aP, bQ) = e(aP, Q)^b = e(P, bQ)^a = e(P, Q)^{ab}$
- non-degeneracy (function $e(P, Q)$ never returns '1'), and
- efficiency in computations.

Pairing on Edwards curves

- Pairing on twisted supersingular $k = 2$ Edwards curve was defined by Das and Sarkar [Pairing'08]
- Pairing on ordinary Edwards curves was defined by Arene et al. [Journal of Cryptology'09]
- So far NO hardware architectures or software implementations for pairing on Edwards curves reported in literature

How to generate secure and computationally-friendly prime numbers? - part I

Security concerns:

- p must be a large prime number, and $p \equiv 3 \pmod 4$
- $p + 1$ must have a large prime divisor r - the discrete logarithm problem in the elliptic curves must be hard (Pollard rho)
- Edwards curves parameters must be $a = 1, d = p - 1$
- k, so called embedding degree, is the smallest number, such that p^{k-1} is divisible by r
- For aforementioned parameters, Edwards curve has $p + 1$ points, embedding degree $k = 2$, and it is called supersingular curve
- p must be a large prime, the discrete logarithm problem in the p^2 must be hard (functional field sieve)

How to generate secure and computationally-friendly prime numbers? - part II

- p and r can have a special form - Menezes and Koblitz [ePrint'06] recommended Solinas primes [NSA'99] $(2^a \pm 2^b \pm 1)$
- **Observation:** Barrett reduction [Crypto'86] requires multiplication by constants: p and $\mu = \lfloor \frac{2^{2 \cdot n}}{p} \rfloor$, and $2^n > p$, and n - number of bits of p.
- we search such for p such that $\mu = 2^{a_{t-1}} \pm ... \pm 1$ and t is relatively a small number $(t < 30)$.
- we were looking for r with a very low Hamming weight $(< 5\%)$

Comment:

The GMP library-based software implementation of the parameters generation algorithm requires significant amount of time to find friendly numbers

Parameters used in our work

Security	Field order - p	Prime divisor - r	# terms of μ
80-bits	$2^{520} + 2^{363} - 2^{360} - 1$	$2^{160} + 2^{3} - 1$	12
120-bits	$2^{1263} + 2^{1037} - 2^{1005} - 1$	$2^{258} + 2^{32} - 1$	28
128-bits	$2^{1492} + 2^{1237} - 2^{1224} - 1$	$2^{268} + 2^{13} - 1$	30
191-bits	$2^{3955} + 2^{3581} + 2^{3573} - 1$	$2^{382} + 2^{8} - 1$	21

Observations:

- The multiplication by p and μ can be replaced by multi-operand addition!
- The prime divisor r $(2^a + 2^b - 1)$ has always a form of **10..01..1** (computationally cheaper - check next slide!).

General algorithm for the modified Tate pairing

Algorithm 2 Miller's algorithm for computing modified Tate pairing

Require: Points P and $\phi(Q)$, prime divisor $r = (r_{l-1} \dots r_0)$, field order p, and embedding degree k, $h_{P,Q}$ a rational function

Ensure: $F = e(P, \phi(Q))$

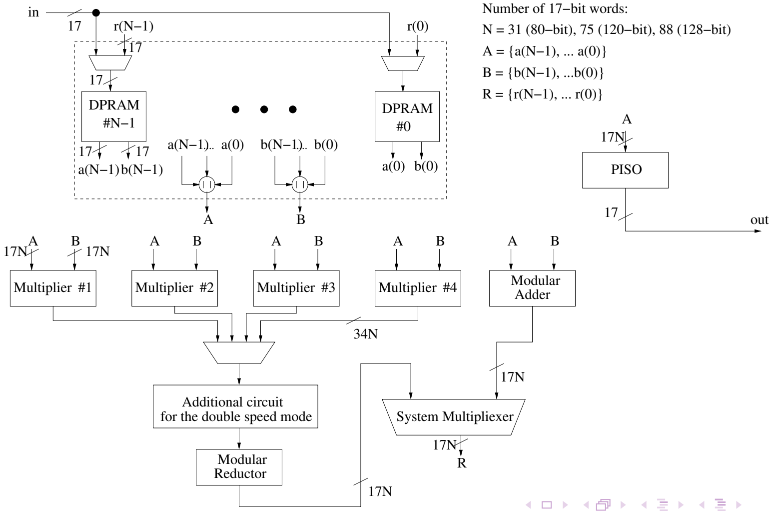
$F = 1$, $R = P$
for $i = l - 2$ downto 0 **do**
  $G \leftarrow h_{R,R}(\phi(Q))$ and $R = 2R$ /* Algorithm 3: 14 multiplications */
  $F = F^2 * G$ /* Algorithm 5 and 6: 2+4 multiplictions */
  if $r_i = 1$ **then**
    $G \leftarrow h_{R,P}(\phi(Q))$ and $R = R + P$ /* Algorithm 4: 24 multiplications */
    $F = F * G$ /* Algorithm 5: 2 multiplications */
  end if
end for
return $F \leftarrow F^{\frac{p^k-1}{r}}$ /* Algorithm 7: next slide */

What if for the substantial number of P and Q the result of $e(P, Q) = 1$?

Distortion maps! $\phi(Q) = (x_Q i, \frac{1}{y_Q})$, where $i^2 = -1$. Consequently, F and G are the complex numbers.

Other names: twists or operations in the extension field $x^2 + 1$, in this case.

The overview of novel coprocessor block diagram



Number of 17−bit words:

N = 31 (80−bit), 75 (120−bit), 88 (128−bit)

A = {a(N−1), ... a(0)}

B = {b(N−1), ...b(0)}

R = {r(N−1), ... r(0)}

FPGA-based hardware architectures - preliminary results Stratix V

- 80-bit security coprocessor: logic - 41471 ALM, memory - 552k, 120 DSPs, 263 MHz, latency: **133μs**
- 120-bit security coprocessor: logic - 120628 ALM, memory - 1327k, 288 DSPs, 257 MHz, latency: **541μs**
- 128-bit security coprocessor: logic - 137484 ALM, memory - 1432k, 336 DSPs, 242 MHz, latency: **697μs**

Reference software implementation results:

- GNU Multiple Precision Arithmetic Library
- Testing platform: Mac OS X 10.6.8, CPU: Intel Core i7 2.8GHz, 8GB 1067 MHz DDR3
- **80-bit**: 5.09ms, **120-bit**: 29.41ms, **128-bit**: 37.11ms

Speed records for the range of 120-128-bits security for the pairing transformations over prime fields

Publication	Curve Type	Security	Type	Platform	Latency
This work	**twisted supersingular Edwards**	**120-bit**	**Tate**	**Stratix V**	**0.54ms**
Cheung et al. [CHES'11]	Barreto-Naehring	126-bit	Opt.-Ate	Virtex-6	0.57ms
This work	**twisted supersingular Edwards**	**128-bit**	**Tate**	**Stratix V**	**0.70ms**
This work	**twisted supersingular Edwards**	**120-bit**	**Tate**	**Stratix IV**	**0.70ms**
Beuchat et al. [Pairing'10]	Barreto-Naehrig	126-bit	Opt.-Ate	Core i7 2.8	0.83ms
This work	**twisted supersingular Edwards**	**128-bit**	**Tate**	**Stratix IV**	**0.88ms**
This work	**twisted supersingular Edwards**	**120-bit**	**Tate**	**Virtex-6**	**1.05ms**
Cheung et al. [CHES'11]	Barreto-Naehrig	126-bit	Opt.-Ate	Stratix III	1.07ms
Fan et al. [Computers'11]	Barreto-Naehrig	128-bit	Opt.-Ate	Virtex-6	1.36ms
This work	**twisted supersingular Edwards**	**128-bit**	**Tate**	**Virtex-6**	**1.05ms**
Fan et al. [Computers'11]	Barreto-Naehrig	128-bit	Ate	Virtex-6	1.60ms
Cheung et al. [CHES'11]	Barreto-Naehrig	126-bit	Opt.-Ate	Cyclone II	1.93ms

Comment:

The fastest reported pairing coprocessor over prime fields for security level above 120 bits!

Major Contributions

- Novel, low latency, generic, optimized for fast carry-chains (FPGA), hybrid adder for big numbers (thousand of bits and more)
- Solinas primes-based, DSP-oriented, modular arithmetic architectures for addition, subtraction and multiplication
- First hardware architectures for 80, 120 and 128-bit pairing on Edwards curves
- Our coprocessor (on Stratix V) computes 120 and 128-bit secure pairing over prime field in less than 0.54 and 0.70 ms, respectively. It is the fastest pairing implementation over prime fields in this security range

Questions

Thank you!

Questions?  Questions?

CERG: http:/cryptography.gmu.edu