

Recent Implementations of PKC on ATmega128L using NesC

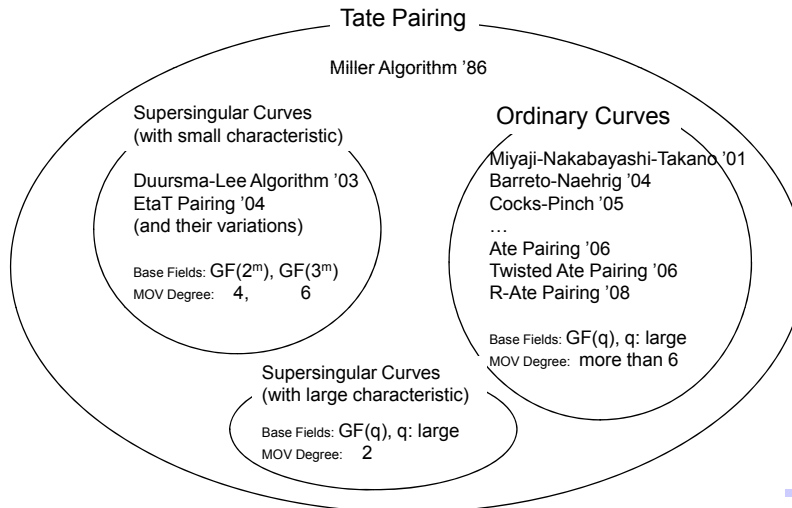
- **TinyPK, 14.5 sec, Watro et al. 2004**
RSA cryptosystem with $e=3$, n : 1024 bits, NesC
- **TinyECC, 1.9 sec, Liu et al. 2005**
ECC, SECG curve over $GF(q)$, q : 160-bit prime, NesC+Assembly
- **TinyECCK, 1.1 sec, Chung et al. 2007**
ECC, Koblitz curve over $GF(2^{163})$, Nesc
- **TinyTate, 30.2 sec, Oliveira et al. 2007**
Tate pairing, Supersingular curves $GF(q)$, q : 256-bit prime, NesC
- **TinyPBC, 5.5 sec, Oliveira et al. 2007**
 η_T pairing, supersingular curves $GF(2^{271})$, NesC
- **Ours, 5.8 sec, Ishiguro et al. 2007**
 η_T pairing, supersingular curves $GF(3^{97})$, NesC

Type of Pairing

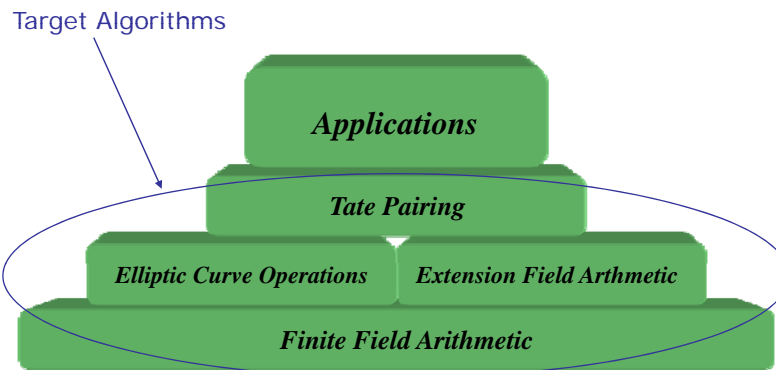
Pairing $e: G_1 \times G_2 \rightarrow G_T$

- **Symmetric Pairing**
There is an efficient homomorphism $\varphi: G_1 \rightarrow G_2$ (or $G_1 = G_2$).
- **Asymmetric Pairing**
There is no efficient homomorphism $\varphi: G_1 \rightarrow G_2$ (and $G_1 \neq G_2$).
- **Composite Order Pairing**
 $G_1 = G_2$ has a subgroup of composite order, e.g. RSA modulus.
- **Hyperelliptic Curve Pairing**
pairing using hyperelliptic curves.

Several Pairings using Elliptic Curves



Implementation of PBC



η_T Pairing (2004)

- Input: $P = (x_p, y_p), Q = (x_q, y_q) \in E(GF(3^m))$
- Output: $\eta_T(P, Q) \in GF(3^{6m})$

```

y_p ← -y_p, f ← y_qσ - y_p + y_p(-x_q + ρ - x_p)
for i ← 0 to (m-1)/2 do
    u ← x_p + x_q + 1
    g ← y_p y_q σ - u2 - uρ - ρ2
    f ← f · g
    x_p ← x_p1/3, y_p ← y_p1/3, x_q ← x_q3, y_q ← y_q3
end for
return f(33m-1)(3m+1)(3m-3(m+1)/2+1)
    
```

Initialization

Addition (+), Subtraction (-),

Main loop

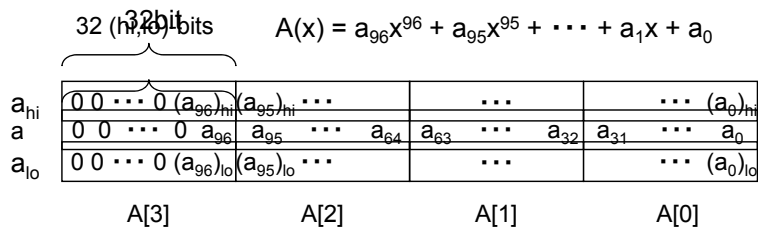
Final exponentiation

Finite Fields $GF(3^m)$ (or F_{3^m})

- Arithmetic of $GF(3^m)$
 - Addition/Subtraction (A), Multiplication (M), Cubing (C), Inversion (I)
 - We can implement them using AND,OR,XOR.
- Extension Fields $GF(3^{6m})$
 - We can implement it using (A,M,C,I) of $GF(3^m)$
 - Elements $A = (a_5, a_4, a_3, a_2, a_1, a_0)$
 $= a_5\sigma\rho^2 + a_4\sigma\rho + a_3\sigma + a_2\rho^2 + a_1\rho + a_0$
 $(a_i \in GF(3^m), \rho^3 = \rho + 1, \sigma^2 = -1)$

Polynomial Base (m=97)

- Polynomial Base $GF(3^m) = GF(3)[x]/(x^{97}+x^{16}+2)$
- $GF(3)$ is represented by (hi,lo)-bit.
 - $a = (a_{hi}, a_{lo})$, a in $GF(3)=\{0,1,2\}$.
 - $0 = (0,0)$, $1 = (0,1)$, $2 = (1,0)$



Addition

$A(x), B(x)$ in $GF(3^{97})$

$C(x) = A(x) + B(x)$

$$= (a_{97}+b_{97}) x^{97} + (a_{96}+b_{96}) x^{96} + \dots + (a_0+b_0)$$

Algorithm

- $t = (a_{hi} | a_{lo}) \& (b_{hi} | b_{lo})$
- $c_{hi} = t \wedge (a_{hi} | b_{hi})$
- $c_{lo} = t \wedge (a_{lo} | b_{lo})$

Boolean Gates: AND(&), OR(|), XOR(^)

Multiplication

Input: $a(x) = a_{96}x^{96} + a_{95}x^{95} + \dots + a_0x^0 \in GF(3^{97})$
 $b(x) = b_{96}x^{96} + b_{95}x^{95} + \dots + b_0x^0 \in GF(3^{97})$
 $f(x) = x^{97} + x^{12} + 2$

Output: $c(x) = a(x) \times b(x) \bmod f(x)$

$\left(\begin{array}{l} a_i, b_i \in GF(3) \\ i = 0, 1, \dots, 96 \end{array} \right)$

1: Multiplication of polynomials

$$c'(x) = a(x) \times b(x)$$

$$= a_{96}b_{96}x^{192} + (a_{95}b_{96} + a_{96}b_{95})x^{191} + \dots + a_0b_0x^0$$

2: Reduction

$$c(x) = c'(x) \bmod f(x)$$

Shift-Add Method

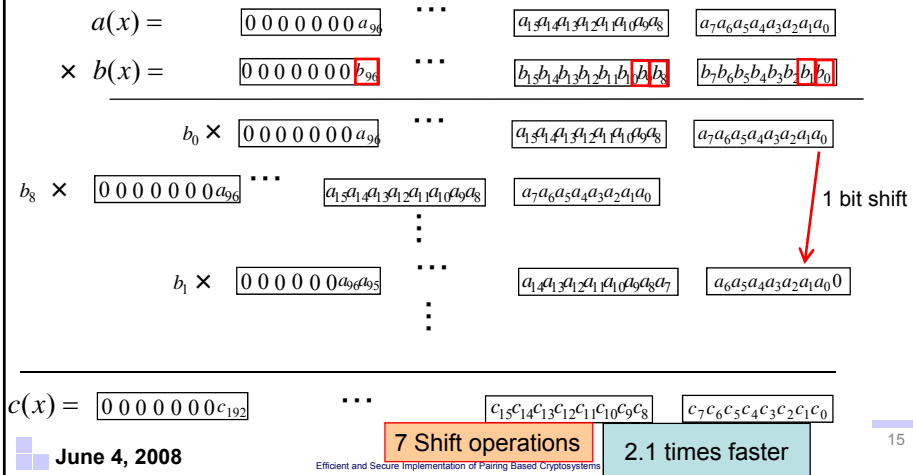
Shift-Add Method

$a(x) =$	0 0 0 0 0 0 0 a_{96}	...	$a_1 a_4 a_7 a_{10} a_{13} a_{16} a_{19} a_{22} a_{25} a_{28} a_{31} a_{34} a_{37} a_{40} a_{43} a_{46} a_{49} a_{52} a_{55} a_{58} a_{61} a_{64} a_{67} a_{70} a_{73} a_{76} a_{79} a_{82} a_{85} a_{88} a_{91} a_{94} a_{97}$...	$a_7 a_6 a_5 a_4 a_3 a_2 a_1 a_0$
$\times b(x) =$	0 0 0 0 0 0 0 b_{96}	...	$b_1 b_4 b_7 b_{10} b_{13} b_{16} b_{19} b_{22} b_{25} b_{28} b_{31} b_{34} b_{37} b_{40} b_{43} b_{46} b_{49} b_{52} b_{55} b_{58} b_{61} b_{64} b_{67} b_{70} b_{73} b_{76} b_{79} b_{82} b_{85} b_{88} b_{91} b_{94} b_{97}$...	$b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0$
$b_0 \times$	0 0 0 0 0 0 0 a_{96}	...	$a_1 a_4 a_7 a_{10} a_{13} a_{16} a_{19} a_{22} a_{25} a_{28} a_{31} a_{34} a_{37} a_{40} a_{43} a_{46} a_{49} a_{52} a_{55} a_{58} a_{61} a_{64} a_{67} a_{70} a_{73} a_{76} a_{79} a_{82} a_{85} a_{88} a_{91} a_{94} a_{97}$...	$a_7 a_6 a_5 a_4 a_3 a_2 a_1 a_0$
$b_1 \times$	0 0 0 0 0 0 0 $a_{96} a_{95}$...	$a_4 a_7 a_{10} a_{13} a_{16} a_{19} a_{22} a_{25} a_{28} a_{31} a_{34} a_{37} a_{40} a_{43} a_{46} a_{49} a_{52} a_{55} a_{58} a_{61} a_{64} a_{67} a_{70} a_{73} a_{76} a_{79} a_{82} a_{85} a_{88} a_{91} a_{94} a_{97}$...	$a_6 a_5 a_4 a_3 a_2 a_1 a_0 0$
		⋮			
$b_{96} \times$	$a_7 a_6 a_5 a_4 a_3 a_2 a_1 a_0$...	0 0 0 0 0 0 0 0
$c(x) =$	0 0 0 0 0 0 0 c_{192}	...	$c_1 c_4 c_7 c_{10} c_{13} c_{16} c_{19} c_{22} c_{25} c_{28} c_{31} c_{34} c_{37} c_{40} c_{43} c_{46} c_{49} c_{52} c_{55} c_{58} c_{61} c_{64} c_{67} c_{70} c_{73} c_{76} c_{79} c_{82} c_{85} c_{88} c_{91} c_{94} c_{97}$...	$c_7 c_6 c_5 c_4 c_3 c_2 c_1 c_0$

↓ 1 bit shift
↓ 1 bit shift

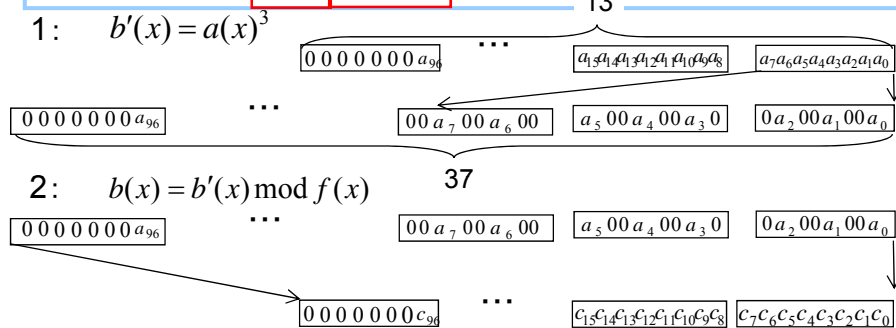
Comb Method

Comb Method



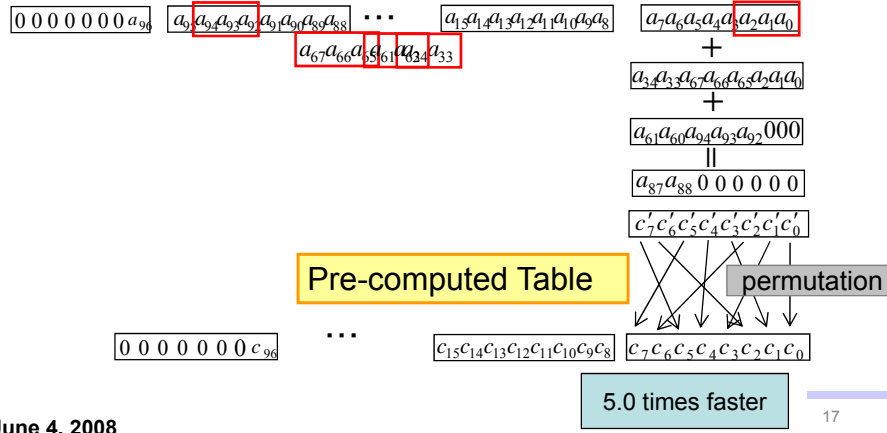
Cubing

- Input: $a(x) = a_{96}x^{96} + a_{95}x^{95} + \dots + a_0x^0 \in GF(3^{97})$
 - Output: $b(x) = a(x)^3 \bmod f(x)$
- $f(x) = x^{97} + x^{16} + 2$ $(a_i \in \{0,1,2\})$
 $(i = 0,1,\dots,96)$



Faster Cubing

Reduction trinomial $x^{97}+x^{16}+2$ allows us a simple pre-computation.



Timing

[IST07] Tsukasa Ishiguro, Masaaki Shirase, Tsuyoshi Takagi, "Efficient Implementation of the Pairing on ATmega128L", IPSJ Computer Security Symposium, CSS 2007, Nara, pp.187-192, October, 2007.

	MICAz (non-improved)	MICAz (improved)	PC (improved)
addition	0.047ms	0.047ms	0.12μs
multiplication	14ms	6.2ms	5.91μs
Cubing	2ms	0.4ms	0.32μs
Inversion	108ms	96ms	670.9μs
Pairing	≈ 30s	5.8s	5.41ms

MICAz, NesC
CPU: ATmega128L 7.37MHz
RAM: 4kB

PC, gcc
CPU: Core2Duo6300 1.87GHz
RAM: 1GB

Timing for larger degrees

	F_3^{97}	F_3^{167}	F_3^{193}	F_3^{239}
Addition	0.047	0.076	0.084	0.092
Cube	0.40	0.069	1.15	1.16
Multiplication	6.2	18.2	25.5	35.75
Inversion	96	1.6890	1.4480	2.3040
η_T Pairing (sec)	5.8	15.3	34.6	60.2

[milliseconds]

MICAz, NesC
CPU: ATmega128L 7.37MHz

Comparison

	TinyPK	TinyECC	TinyECCK	TinyTate	TinyPBC	Ours
Language	NesC	NesC,asm	NesC	NesC	NesC	NesC
Cryptosystem	RSA	ECC (char. p)	ECC (char. 2)	Tate (char.p)	η_T (char. 2)	η_T (char. 3)
ROM (bytes)	12,408	13,858	5,592	18,384	47,948	17,284
RAM (bytes)	1,167	1,440	1,002	1,831	368 (Stack 2,867)	628
Timing (sec)	14.5	1.9	0.9	30.2	5.5	5.8

Conclusion

- We implemented the η_T pairing of char. 3 on sensor node.
- The implementation is optimized for ATmega128L.
- The timing for $GF(3^{97})$ is about 5.8 seconds.

Future works

- Implementation by inline assembly
- Cryptographic applications using pairing