Curve41417: Karatsuba revisited

Chitchanok Chuengsatiansup

Technische Universiteit Eindhoven

August 10, 2014

Joint work with Daniel J. Bernstein and Tanja Lange

Karatsuba

- Goal: Compute $P = AB$
  given $A = a_0 + a_1 t^n$ and $B = b_0 + b_1 t^n$
- Method1: schoolbook
  $P = a_0 b_0 + (a_0 b_1 + a_1 b_0) t^n + a_1 b_1 t^{2n}$
- Method2: Karatsuba
  $P = a_0 b_0 + ((a_0 + a_1)(b_0 + b_1) - a_0 b_0 - a_1 b_1) t^n + a_1 b_1 t^{2n}$
- Method3: refined Karatsuba
  $P = (a_0 b_0 - a_1 b_1 t^n)(1 - t^n) + (a_0 + a_1)(b_0 + b_1) t^n$

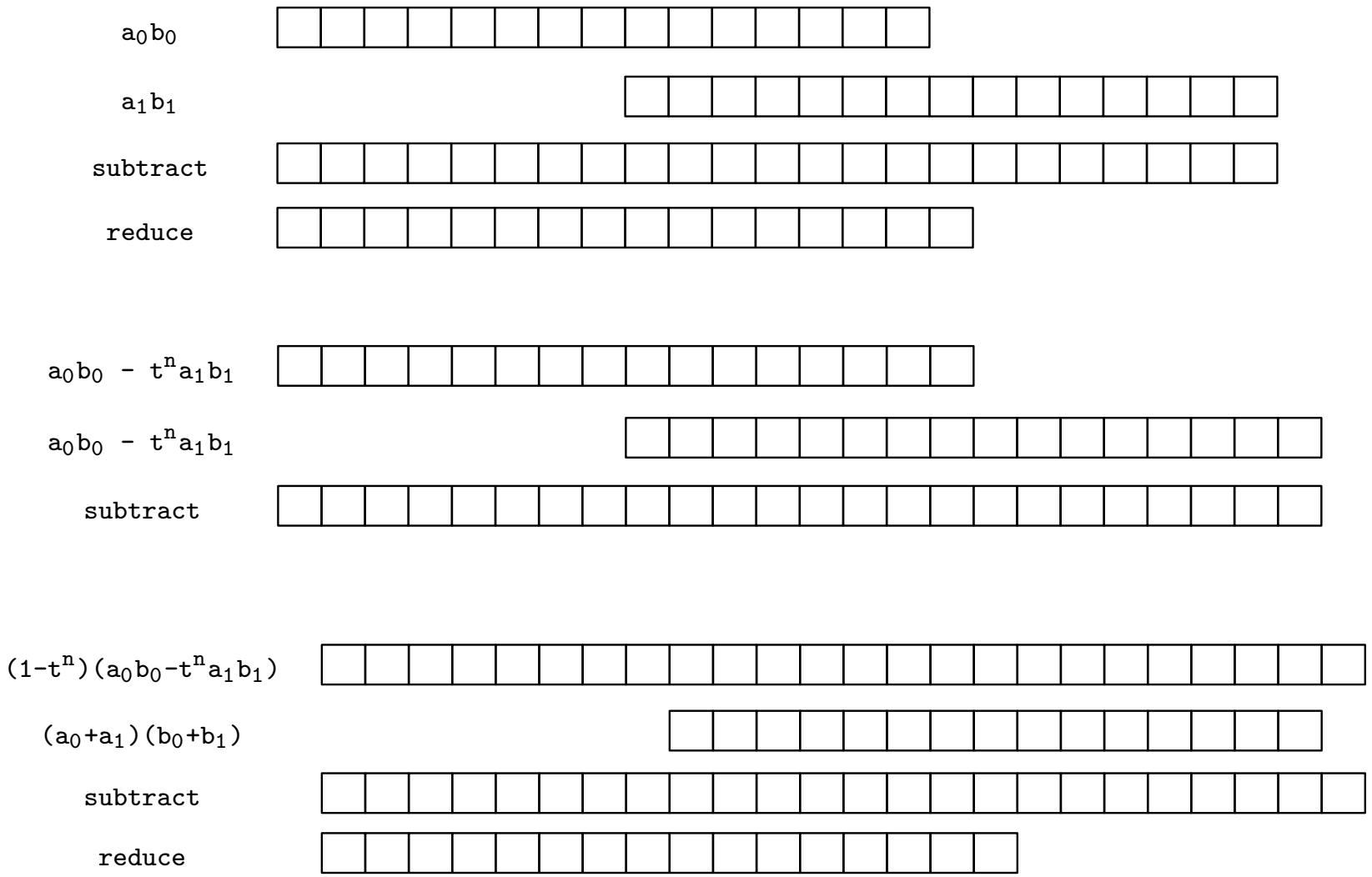
Karatsuba

- Goal: Compute $P = AB \mod Q$
  given $A = a_0 + a_1 t^n$ and $B = b_0 + b_1 t^n$
- Method1: schoolbook
  $P = a_0 b_0 + (a_0 b_1 + a_1 b_0) t^n + a_1 b_1 t^{2n} \mod Q$
- Method2: Karatsuba
  $P = a_0 b_0 + ((a_0 + a_1)(b_0 + b_1) - a_0 b_0 - a_1 b_1) t^n + a_1 b_1 t^{2n} \mod Q$
- Method3: refined Karatsuba
  $P = (a_0 b_0 - a_1 b_1 t^n)(1 - t^n) + (a_0 + a_1)(b_0 + b_1) t^n \mod Q$

Karatsuba

- Goal: Compute $P = AB \bmod Q$
  given $A = a_0 + a_1 t^n$ and $B = b_0 + b_1 t^n$
- Method1: schoolbook
  $P = a_0 b_0 + (a_0 b_1 + a_1 b_0) t^n + a_1 b_1 t^{2n} \bmod Q$
- Method2: Karatsuba
  $P = a_0 b_0 + ((a_0 + a_1)(b_0 + b_1) - a_0 b_0 - a_1 b_1) t^n + a_1 b_1 t^{2n} \bmod Q$
- Method3: refined Karatsuba
  $P = (a_0 b_0 - a_1 b_1 t^n)(1 - t^n) + (a_0 + a_1)(b_0 + b_1) t^n \bmod Q$
- Method4: reduced refined Karatsuba (new)
  $P = (a_0 b_0 - a_1 b_1 t^n \bmod Q)(1 - t^n) + (a_0 + a_1)(b_0 + b_1) t^n \bmod Q$

Reduced refined Karatsuba



Cost comparison, e.g., 16 words

- Schoolbook
  $16 \times 16 = 256$
- One-level Karatsuba
  $16 \times 16 \to 3 \cdot (8 \times 8) +$ some additions
  $= 192 +$ some additions
- Two-level Karatsuba
  $3 \cdot (8 \times 8) \to 3 \cdot (3 \cdot (4 \times 4)) +$ even more additions
  $= 144 +$ even more additions
- What is the cutoff?
  - gmp cutoff: 832 bits on ARM Cortex-A8
  - but cutoff is reduced by improvements to Karatsuba
  - and cutoff is reduced by redundant representation

Target application: Curve41417

- High security curve for paranoid cryptographers (at the request of Silent Circle)
- Defined over prime field $\mathbf{F}_p$ where $p = 2^{414} - 17$
- In Edwards curve form

$$x^2 + y^2 = 1 + 3617x^2y^2$$

- Large prime order subgroup (cofactor 8)
- Large embedding degree
- Twist secure, i.e., twist of Curve41417 also secure

Performance budget

Performance budget

- OpenSSL
  - `secp160-r1` (least secure option supported by OpenSSL)
  - $\approx$ 2.1 million cycles on FreeScale i.MX515
  - $\approx$ 2.1 million cycles on TI Sitara

Performance budget

- OpenSSL
  - `secp160-r1` (least secure option supported by OpenSSL)
  - $\approx$ 2.1 million cycles on FreeScale i.MX515
  - $\approx$ 2.1 million cycles on TI Sitara
- Curve41417
  - 1.648409 million cycles on FreeScale i.MX515
  - 1.775804 million cycles on TI Sitara

- Full presentation at CHES 2014 !

www.chesworkshop.org

- Online version
  http://cr.yp.to/ecdh/curve41417-20140706.pdf