A Low-Power Design for an Elliptic Curve Digital Signature Chip

Rich Schroeppel, Tim Draelos, Russell Miller,
Rita Gonzales, Cheryl Beaver

{rschroe;tjdrael;rdmille;ragonza;cbeaver}@sandia.gov

Sandia National Laboratories

Aug. 14, 2002

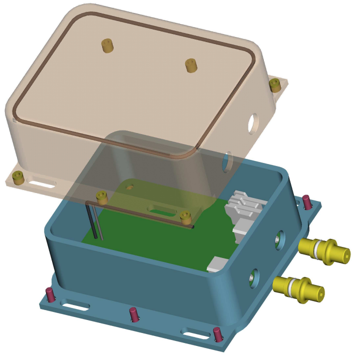
Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.

Motivation

- Public key authentication in resource constrained environments
  - E.g. Battery operated, unattended sensor-based monitoring
  - Low power for signature generation
- Design choices balance between power, size, and speed
- Short signatures (356 bits)
- Low Bandwidth
- Standalone chip, or piece of larger chip
- Bump-in-the-wire option

Application Concept

- Nuclear Material Monitoring & Inventory Application
  - Fiber Optic Tamper Indication
  - Motion, Temperature sensors
  - Two-way wireless communication
  - Message authentication/encryption
  - Battery life in excess of 5 years
  - Reduced size (1.5”x 4.1”x 4.6”)
  - Low cost module ($550 estimate)



Design Choices

- Elliptic Curve Optimal El Gamal Signatures
  - No modular reciprocals
- Elliptic Curve (EC) uses characteristic 2 field, GF(2^{178})
- VHDL for portability
- Designed-in power management

Algorithm Components

- Elliptic Curve operations for signature
  - Point multiplication
    - Halve&Add Method
    - Signed Sliding Window multiplication
    - Pre-compute 3P,5P,7P
- Finite Field Operations
  - Elliptic curve operations are built up from finite field primitives such as multiplication, reciprocal, and solving a quadratic equation

Algorithm Optimizations

- EC Point halving
  - Point-slope form
- Field Towers
- Almost Inverse Algorithm
  - Fast degree comparison, fast shift, fast fix-up
- Quadratic Solve circuit design
- Field multiplication – radix 16
- Trinomial field basis

The Signature Scheme

- Parameters
  - Public: Elliptic Curve **E**, Point **$G=(x_G,y_G)$** of order **r**, Field = **GF(2^n)**, Public Key **W** = sG
  - Private: long term private key **s**, $0 < s < r$
- Signature: On message, M
  - f=Hash(M).
  - Choose per message random, v.
  - Compute $V = vG = (x_V,y_V)$.
  - $c = x_V \pmod r$
  - $d = cfs+v \pmod r$
  - Signature is (c,d)
- Verification: On received input (M,c,d)
  - If $c <= 0$ or $c > r-1$, output “reject” and stop
  - f = Hash(M)
  - $h = cf \pmod r$
  - $P = dG - hW = (x_P,y_P)$
  - $c' = x_P \bmod r$
  - If c = c’ then output “accept” else “reject”

Point Halving

- 3 times faster than doubling
- No reciprocals
- E: $y^2 + xy = x^3 + ax^2 + b$
- Use point in (x,r) format (r = y/x) (point-slope)
- Input $P = (x_P,r_P)$; Output = $Q = (x_Q , r_Q)$ where 2Q=P

```
1. Mh = Qsolve($x_P$+a)
2. T = $x_P(r_P$+Mh)
3. If parity(tm&T)=0 then
     » Mh = Mh + 1; T = T + $x_P$
     » tm is a trace mask depending on the field
4. $x_Q = \sqrt{T}$; $r_Q$ = Mh + $x_Q$ + 1
```

Field Towers

$$\begin{tikzcd}
GF(2^{178}) = GF(2^{89}) / (V^2+V+1) \arrow[d, dash, "2"] \\
GF(2^{89}) = GF(2) / (u^{89}+u^{38}+1) \arrow[d, dash, "89"] \\
GF(2)
\end{tikzcd}$$

$$\alpha = a_1 V + a_0 \in GF(2^{178}); \quad a_i \in GF(2^{89})$$

Write $\alpha = (a_1, a_0)$

Field Towers

- Arithmetic based in GF(2^{89}),
  e.g.

$$\alpha + \beta = (a_1 + b_1, a_0 + b_0)$$

- E: $y^2 + xy = x^3 + ax^2 + b$
  - Fixed a = (1,0) for simplicity
  - b variable
- Main optimizations done over GF(2^{89})
- Order of G ~ 177 bits is equivalent to 1500 bit RSA
- Not subject to known field tower attacks

Quadratic Solution

- Qsolve(a) = z where $z^2 + z = a$
- Qsolve for GF(2^{89}):
  - Input a = ($a_{00}, a_{01}, \ldots, a_{88}$), output z = ($z_{00}, \ldots, z_{88}$)

$$\text{a even bits}: a_{00} \ldots a_{36}: \quad a_{2n} = z_{2n} \oplus z_n \oplus z_{n+70}$$

$$a_{38} \ldots a_{74}: \quad a_{2n} = z_{2n} \oplus z_n \oplus z_{n+51}$$

$$a_{76} \ldots a_{88}: \quad a_{2n} = z_{2n} \oplus z_n$$

$$\text{a odd bits}: a_{01} \ldots a_{37}: \quad a_{2n+1} = z_{2n+1} \oplus z_{n+45}$$

$$a_{39} \ldots a_{87}: \quad a_{2n+1} = z_{2n+1} \oplus z_{n+45} \oplus z_{n+26}$$

- Compute odd $z_{01} \ldots z_{19}$ directly
- Solve equations for other z_n:

$$a_{01} = z_{01} \oplus z_{46} \qquad \Rightarrow \qquad z_{46} = a_{01} \oplus z_{01}$$

Gate-Depth Tradeoff

XOR Gates	Depth	
3872	6	
387	35	selected
287	65	

- Developed special circuit with relatively small number of XOR gates (387) and depth (35)
- Faster with more gates, but traded speed for size

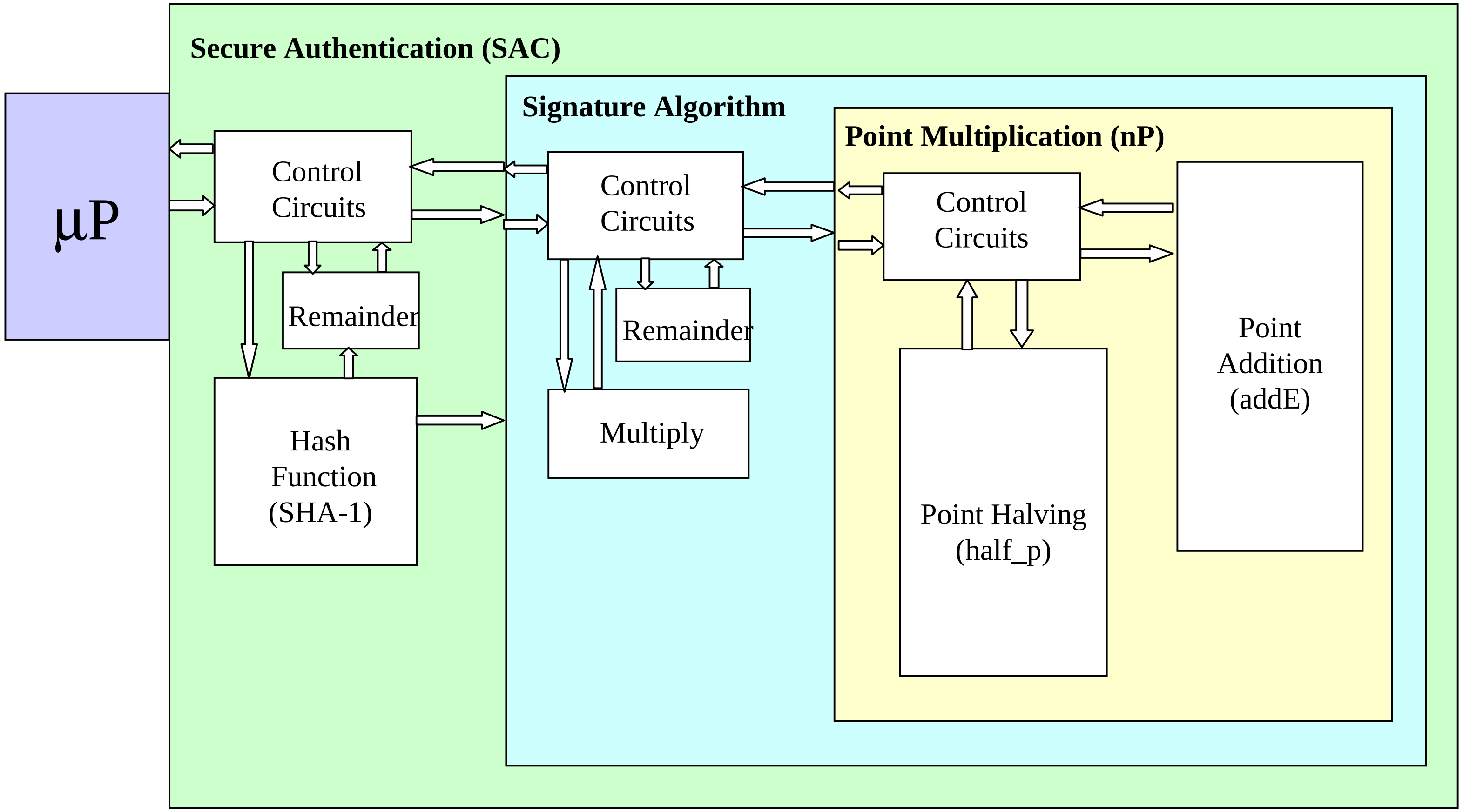
Hardware Architecture & Design

- Full VHDL implementation that can be targeted to FPGA or ASIC
  - Bottom up approach
- I/O Interface – intended to be used as a memory-mapped device
  - Hang off of microprocessor bus
    - 16-bit address bus
    - 8-bit data bus
  - Control Signals
    - Interrupt signals used to indicate signature status, error or signature completion

Hardware Architecture & Design

- Functionality
  - Signature, SHA-1 Hash Algorithm, Pseudo-random number generation
- Flexibility
  - Input message or hash of message
  - Input random per-message nonce, or seed for a pseudo-random nonce
  - Parameters: private key, generating point (Curve equation)
  - Output: signature, message hash, public key

Secure Signature Chip Design



Gate counts

- Chip: 191,000
  - Control: 27,000
  - SHA-1: 13,000
  - Remainder: 6,700
  - Signature Algorithm: 143,000
    - Control: 15,000
    - Multiply: 6,200
    - Remainder: 6,800
    - Point Multiplication: 112,000
      - Register & Control: 30,000
      - Point Addition: 52,000
      - Point Halving: 29,000

Power control in hardware design

- Clock gating
  - Inactive portion of chip turned off
    - Point halver
    - Point adder
    - Remainder
    - Multiplier
  - Finer granularity possible

Other Hardware Optimizations

- SHA-1 shift register to reduce area & power
- Radix 16 field multiplication
- Almost Inverse
  - Fast degree comparison
  - Fast radix 4 low-order 1 circuit
  - Fast radix 256 fix up step

Results

- Complete Register-Transfer-Level VHDL Design - fully transferable
- Final Synthesized Gate Count: 191,000
- Signature Sign Time: 4.4ms at 20Mhz
  - Initialization 0.25 ms
- Nominal Operating Speed: 20Mhz
- Nominal conditions: CMOS library 5V, .5μm 25°C
- Power Estimation: 150mW while signing, 6uW while idle
- Improved performance with more advanced technology

Future Work

- Counter side channel attacks
- Improve worst case path (remainder)
- Additional improvements to point multiplication
- Verification algorithm
- Tech transfer: VHDL available
- More applications