Thesis Progress Report #6

Christopher A. Wood

May 13, 2013

Agenda

Decompositions of Interest

$$
\begin{tikzcd}
 & & & GF(2^{16}) \arrow[dll] \arrow[d] \arrow[drr] & & \\
 & GF((2^8)^2) \arrow[dl] \arrow[dr] & & GF((2^2)^8) & & GF((2^4)^4) \arrow[dl] \\
GF(((2^4)^2)^2) \arrow[dr] & & GF(((2^2)^4)^2) & & GF(((2^2)^2)^4) & \\
 & GF((((2^2)^2)^2)^2) & & & &
\end{tikzcd}
$$

Basis Towers for Degree 2 Extensions

Let $e(x) = x^2 + x + 1$, $f(x) = x^2 + x + \alpha$, $g(x) = x^2 + x + \lambda$, $\lambda = \alpha^2\beta$

Let $e(\alpha) = 0$, $f(\beta) = 0$, $g(\gamma) = 0$

- Satoh - degree 2 extensions with polynomial basis (compactness)
  - $e(x) = x^2 + x + 1$ with $\{1, \alpha\}$, $f(x) = x^2 + x + \alpha$ with $\{1, \beta\}$, and $g(x) = x^2 + x + \lambda$ with $\{1, \gamma\}$
- Canright - degree 2 extensions with normal basis (compactness)
  - $e(x) = x^2 + x + 1$ with $\{\alpha, \alpha^2\}$, $f(x) = x^2 + x + \alpha$ with $\{\beta, \beta^4\}$, and $g(x) = x^2 + x + \lambda$ with $\{\gamma, \gamma^{16}\}$
- Nogami - degree 2 extensions with mixed basis (shorter critical path)
  - $e(x) = x^2 + x + 1$ with $\{\alpha, \alpha^2\}$, $f(x) = x^2 + x + \alpha$ with $\{1, \beta\}$, and $g(x) = x^2 + x + \lambda$ with $\{\gamma, \gamma^{16}\}$

Inverse Optimizations

With each decomposition, we need an efficient way of computing the multiplicative inverse

- Extended Euclidean algorithm (appropriate for software)
- Field decomposition (see slides from reports 1/2) - $n-1$ squarings and $n-2$ multiplications
- Fermat's Little theorem: $\alpha^{-1} \equiv \alpha^{2^k-2}$
  - $2^k - 2 = 2 + 2^2 + 2^3 + \cdots + 2^{k-1}$
  - $\alpha^{-1} \equiv \alpha^2 \cdot \alpha^{2^2} \cdot \cdots \cdot \alpha^{2^{k-1}}$
- Itoh-Tsujii inversion: $\alpha^{-1} \equiv (\alpha^r)^{-1}\alpha^{r-1}$, $r = (q^k - 1)/(q-1)$

Itoh-Tsujii Inversion Algorithm

Algorithm 1 Itoh-Tsujii Inversion Algorithm

Require: $\alpha \in GF(q^n)$
Ensure: $\alpha^{-1} \in GF(q^n)$
1: $r \leftarrow (q^m - 1)/(q-1)$
2: compute α^{r-1}
3: compute $\alpha^r = \alpha^{r-1}\alpha$
4: compute $(\alpha^r)^{-1}$ in $GF(p)$ (base field)
5: compute $\alpha^{-1} = (\alpha^r)^{-1} \cdot \alpha^{r-1}$
6: **return** α^{-1}

Initially targeted for normal basis to use cyclic shifts for squaring, but can be applied to standard (polynomial) basis as well.

Optimizing the Basis Change Matrices

- Paar showed the first greedy approach to final a locally minimum number of ‘1’s in a basis change matrix
- Satoh used this technique to minimize their basis change matrices
- Canright implemented optimal tree-search algorithm to minimize the complexity of these matrices

Hardware and Software

Demo for polynomial decomposition

Magma feature review

VHDL generation

Action Items

- Literature survey on efficient Galois field arithemtic for $GF(2^8)$ - we need optimal squaring, multiplication, and addition operations
- Implement 16-bit inverse using normal basis extension of Canright's work
- Finish composite field decomposition chapter (overdue)
- Outline of code required to perform exhaustive search over all decompositions using all possible bases

Next meeting: **5/20/13** or **5/27/13**