Multiplication in $GF(2^k)$

The multiplication consists of two phases:

- Polynomial Multiplication

- Reduction with the defining irreducible polynomial $p(x)$.

This is similar to the multiply and reduce method of modular multiplication. Similar algorithms (such as interleaving) can be used.

Especially, Squaring operation can be significantly simplified by judicious selection of the basis. For example, a normal basis can be used (Agnew et al)

By choosing $p(x)$ to have a minimal number of nonzero coefficients, in particular three or five (when $p(x)$ is called trinomial or pentanomial, respectively), the reduction step of polynomial multiplication can be simplified.
Squaring in a Normal Basis

A normal basis of $GF(2^k)$ is a basis of the form

$$\{\beta, \beta^2, \beta^4, \ldots, \beta^{2^{k-1}}\}$$

where $\beta$ is an element of $GF(2^k)$. It is well known that such a basis always exists. Let $A$ be expressed in a normal basis. We have

$$A = (a_{k-1}a_{k-2} \cdots a_1a_0)$$

$$= a_0\beta + a_1\beta^2 + a_2\beta^4 + \cdots + a_{k-1}\beta^{2^{k-1}}$$

We compute the square of $A$ as

$$A^2 = \left( \sum_{i=0}^{k-1} a_i\beta^{2^i} \right) \cdot \left( \sum_{i=0}^{k-1} a_i\beta^{2^i} \right)$$

$$= \sum_{i=0}^{k-1} \left( a_i\beta^{2^i} \right)^2 = \sum_{i=0}^{k-1} a_i\beta^{2^i+1}$$

$$= (a_{k-2}a_{k-3} \cdots a_1a_0a_{k-1})$$

which is a cyclic left shift of $A$.
Squaring in $GF(2^k)$

\[
\left( \sum_{i=0}^{k-1} a_i \beta^{2^i} \right) \cdot \left( \sum_{i=0}^{k-1} a_i \beta^{2^i} \right) = \sum_{i=0}^{k-1} a_i \beta^{2^{i+1}}
\]

The above equality is due to the fact the cross terms cancel out, and $\beta^{2^k} = \beta$. For example, given $A = (a_2 a_1 a_0) \in GF(2^3)$, we have

\[
A = (a_2 a_1 a_0)
\]

\[
A^2 = (a_0 \beta + a_1 \beta^2 + a_2 \beta^4)^2
\]

\[
= a_0 \beta(a_0 \beta + a_1 \beta^2 + a_2 \beta^4) + a_1 \beta^2(a_0 \beta + a_1 \beta^2 + a_2 \beta^4) + a_2 \beta^4(a_0 \beta + a_1 \beta^2 + a_2 \beta^4)
\]

\[
= a_0 a_0 \beta^2 + a_0 a_1 \beta^3 + a_0 a_2 \beta^5 + a_1 a_0 \beta^3 + a_1 a_1 \beta^4 + a_1 a_2 \beta^6 + a_2 a_0 \beta^5 + a_2 a_1 \beta^6 + a_2 a_2 \beta^8
\]

\[
= a_0 \beta^2 + a_1 \beta^4 + a_2 \beta^8
\]

\[
= a_0 \beta^2 + a_1 \beta^4 + a_2 \beta
\]

\[
= a_2 \beta + a_0 \beta^2 + a_1 \beta^4
\]

\[
= (a_1 a_0 a_2)
\]
Multiplication in a Normal Basis

The product $C = AB$ is given as

$$C = \sum_{i=0}^{k-1} C_i \beta^{2i} = \sum_{i=0}^{k-1} \sum_{j=0}^{k-1} A_i B_j \beta^{2i+2j}$$

Since $\beta^{2i+2j}$ is also an element of $GF(2^k)$, it can be expressed as

$$\beta^{2i+2j} = \sum_{r=0}^{k-1} \lambda_{ij}^{(r)} \beta^{2r}$$

where $\lambda_{ij}^{(r)} = 0$ or 1. This yields the formula

$$C_r = \sum_{i=0}^{k-1} \sum_{j=0}^{k-1} A_i B_j \lambda_{ij}^{(r)} \text{ for } 0 \leq r \leq k - 1$$

We also notice that

$$\beta^{2i-s+2j-s} = \sum_{r=0}^{k-1} \lambda_{i-s,j-s}^{(r)} \beta^{2r} = \sum_{r=0}^{k-1} \lambda_{ij}^{(r)} \beta^{2r-s}$$

which implies

$$\lambda_{ij}^{(s)} = \lambda_{i-s,j-s}^{(0)} \text{ for all } 0 \leq i, j, s \leq k - 1$$
Multiplication Formulae

Thus, we have a formula for $C_r$ as

$$C_r = \sum_{i=0}^{k-1} \sum_{j=0}^{k-1} A_{i+r}B_{j+r}\lambda_{ij}$$

Consider a circuit built for computing $C_0$ which receives the inputs as (in this order)

$$A_0, A_1, \ldots, A_{k-2}, A_{k-1}$$
$$B_0, B_1, \ldots, B_{k-2}, B_{k-1}$$

This circuit uses the formula

$$C_0 = \sum_{i=0}^{k-1} \sum_{j=0}^{k-1} A_iB_j\lambda_{ij}$$

to compute $C_0$

The same circuit can be used to compute $C_1$ with the inputs as

$$A_1, A_2, \ldots, A_{k-1}, A_0$$
$$B_1, B_2, \ldots, B_{k-1}, B_0$$
Multiplication Formulae

The number of nonzero $\lambda_{ij}$s determines the complexity of the multiplication circuit

- upper bound is $k^2$

- lower bound is shown to be $2k - 1$

A normal basis with $2k - 1$ nonzero $\lambda$s is called an optimal normal basis. Such a basis exists for certain fields

Thus, a circuit with area $O(k)$ can be built to multiply two elements of $GF(2^k)$ in $k$ clock cycles
Values of $k < 265$ for which there exists an ONB

<table>
<thead>
<tr>
<th>2</th>
<th>18</th>
<th>41</th>
<th>74</th>
<th>100</th>
<th>146</th>
<th>180</th>
<th>226</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>23</td>
<td>50</td>
<td>81</td>
<td>105</td>
<td>148</td>
<td>183</td>
<td>230</td>
</tr>
<tr>
<td>4</td>
<td>26</td>
<td>51</td>
<td>82</td>
<td>106</td>
<td>155</td>
<td>186</td>
<td>231</td>
</tr>
<tr>
<td>5</td>
<td>28</td>
<td>52</td>
<td>83</td>
<td>113</td>
<td>158</td>
<td>189</td>
<td>233</td>
</tr>
<tr>
<td>6</td>
<td>29</td>
<td>53</td>
<td>86</td>
<td>119</td>
<td>162</td>
<td>191</td>
<td>239</td>
</tr>
<tr>
<td>9</td>
<td>30</td>
<td>58</td>
<td>89</td>
<td>130</td>
<td>172</td>
<td>194</td>
<td>243</td>
</tr>
<tr>
<td>10</td>
<td>33</td>
<td>60</td>
<td>90</td>
<td>131</td>
<td>173</td>
<td>196</td>
<td>245</td>
</tr>
<tr>
<td>11</td>
<td>35</td>
<td>65</td>
<td>95</td>
<td>134</td>
<td>174</td>
<td>209</td>
<td>251</td>
</tr>
<tr>
<td>12</td>
<td>36</td>
<td>66</td>
<td>98</td>
<td>135</td>
<td>178</td>
<td>210</td>
<td>254</td>
</tr>
<tr>
<td>14</td>
<td>39</td>
<td>69</td>
<td>99</td>
<td>138</td>
<td>179</td>
<td>221</td>
<td>261</td>
</tr>
</tbody>
</table>
Inversion in $GF(2^k)$

An efficient algorithm for computing an inverse of an element of $GF(2^k)$ was proposed by Itoh, Teechai, and Tsujii (see Agnew et al)

If $a \in GF(2^k)$ and $a \neq 0$, then

$$a^{-1} = a^{2^k-2} = \left(a^{2^{k-1}-1}\right)^2$$

For $k$ even or odd, we have

**odd:** $2^{k-1} - 1 = (2^{(k-1)/2} - 1) \cdot (2^{(k-1)/2} + 1)$

**even:** $2^{k-1} - 1 = 2 \cdot (2^{k-2} - 1) + 1$
$= 2 \cdot (2^{(k-2)/2} - 1) \cdot (2^{(k-2)/2} + 1) + 1$

These formulae yield an algorithm for computing the inverse by a series of squarings, exponentiations and multiplications.
Example of Inverse Computation

Consider the field $GF(2^{155})$

\[
\begin{align*}
2^{155} - 2 &= 2 \cdot (2^{77} - 1) \cdot (2^{77} + 1) \\
2^{77} - 1 &= 2 \cdot (2^{38} - 1) \cdot (2^{38} + 1) + 1 \\
2^{38} - 1 &= (2^{19} - 1) \cdot (2^{19} + 1) \\
2^{19} - 1 &= 2 \cdot (2^9 - 1) \cdot (2^9 + 1) + 1 \\
2^9 - 1 &= 2 \cdot (2^4 - 1) \cdot (2^4 + 1) + 1 \\
2^4 - 1 &= (2^2 - 1) \cdot (2^2 + 1) \\
2^2 - 1 &= (2^1 - 1) \cdot (2^1 + 1)
\end{align*}
\]

It requires 10 multiplications to compute an inverse in $GF(2^{155})$ (and many squarings, which are essentially free)

In general, the method requires

$$\lceil \log_2(k - 1) \rceil + H(k - 1) - 1$$

multiplications
Properties of $GF(p^k)$ Arithmetic

$GF(p^k)$ is a $k$-dimensional vector space over the field $GF(p)$ hence, the elements of $GF(p^k)$ are represented by vectors $(a_{k-1}a_{k-2}\cdots a_1a_0)$ where $a_i \in GF(p)$.

- A carefully chosen $p$ admits efficient reduction in the ground field operations.

- Bailey and Paar proposed the use of a pseudo-Mersenne prime of the form $p = 2^m \pm c$ with $\log_2 c < \lfloor \frac{m}{2} \rfloor$. This construction is also called Optimal extension field.
Properties of $GF(p^k)$ Arithmetic

- Addition is performed component-wise with modulo $p$ arithmetic.

- The usual multiply-reduce methodology is used for multiplication.

- Observe that we are considering two types of reduction: the first one is modulo $p$ reduction that we perform on the components where the second one is reducing the degree of the polynomials by using the defining polynomial.