Implementation Security In Cryptography

Lecture 09: Composite Field Mapping

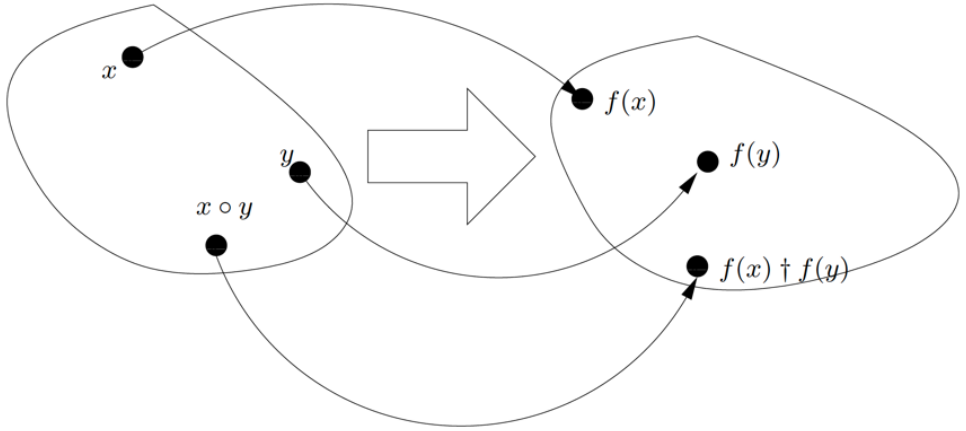
Recap

- In the last lecture
  - Finite Field Isomorphism

Today

- Composite field
- Deeper dive into the inverse implementation

Isomorphism



For two groups G1 and G2, a surjective function G1 to G2 is said to be a homomorphism iff

$$f(x \circ y) = f(x) \dagger f(y).$$

Note, the operators on the left and right are not the same.

An injective (one-to-one) homomorphism is called an isomorphism.

The idea of isomorphism can be extended to rings and fields. In these extensions the only difference is that the latter two are defined wrt. two operators, say (+,.). Thus, we say f: R1→R2 is say a field isomorphism iff: f(a+b)=f(a)+f(b), and f(a.b)=f(a).f(b) for every a and b in R1.

Defining Isomorphism

- The fields are isomorphic and one can establish a mapping between say F_1 and F_2, by computing $c \in F_2,\ st.\ f_1(c) \equiv 0 \left(mod\ f_2\right).$
- The mapping $z \rightarrow c$ is thus used to construct the isomorphism, say T: F1→F2
- An example for c could be $c = z^2 + z$. To verify compute:

$$f_1\left(z^2+z\right) = \left(z^2+z\right)^4 + \left(z^2+z\right) + 1 = z^8 + z^4 + z^2 + z + 1\ (mod\ f_2)$$

Now, note that for $mod\ f_2$, we substitute $z^4 = z^3 + 1.$

$$z^4 = z^3 + 1 \Rightarrow z^5 = z^4 + z = z^3 + z + 1 \Rightarrow z^6 = z^4 + z^2 + z = z^3 + z^2 + z + 1$$

$$\Rightarrow z^8 = z^6 + 1 = z^3 + z^2 + z.$$

$$\text{Thus, } f_1(c) = z^8 + z^4 + z^2 + z + 1 \equiv 0 (\text{mod } f_2)$$

Composite Fields

- The pair of the fields $GF(2^n)$ and $GF(2^n)^m$ is called a composite field.
- If there exists irreducible polynomials, Q(Y) of degree n and P(X) of degree m, which are used to extend GF(2) to $GF(2^n)$, and $GF(2^n)^m$ from $GF(2^n)$.
- The composite field $GF(2^n)^m$ is isomorphic to the field $GF(2^k)$, where $k = m \times n$.

Subfield Mappings

- A very popular design strategy is to implement the AES S-box in the sub-fields.
- The field isomorphisms as follows are exploited:

$$GF(2^8) \cong GF(2^4)^2 \cong GF((2^2)^2)^2$$

- The mappings vary depending on the choice of the basis: **polynomial** or **normal**.

Constructing Isomorphisms between Composite Fields (easy case)

- Let the primitive polynomial used to construct $GF(2^n)$ be denoted by Q(Y).
  - Let ω be the root.
  - Then the elements are $\{0,1,\omega,\omega^2,\cdots,\omega^{2^n-2}\}$
- The primitive polynomial used to construct $GF\left(2^n\right)^m$ is denoted by P(X).
  - Let α be the root.
  - Then the elements are $\{0,1,\alpha,\alpha^2,\cdots,\alpha^{2^{nm}-1}\}$
- Arithmetic in the field $GF\left(2^k\right), k = m \times n$, can be performed by modulo the primitive polynomial $R(z) = z^k + r_{k-1}z^{k-1} + \cdots + 1, r_i \in GF(2)$
- If γ is the root, then the elements can be expressed as: $(1,\gamma,\gamma^2,\cdots,\gamma^{k-1})$.

Mapping from GF(2^k) to GF(2^n)^m, where k=nm

- A simple method to obtain such a conversion is to find the primitive element of both the fields, GF(2^k) and GF(2^n)^m.
- The primitive elements are denoted by γ and α respectively.
- One checks: $R(\gamma) = 0$, and $R(\alpha) mod\ P(X)Q(Y) \equiv 0$.
- Thus, we establish the following mapping from GF(2^k) to GF(2^n)^m: $\gamma \rightarrow \alpha$.
- If the roots do not satisfy the polynomial R, we repeat the test for the next primitive element.
- Subsequent mappings are easy to find:
  - $GF(2^k) \rightarrow GF(2^n)^m : \gamma^i \rightarrow \alpha^i,\ 0 \leq i \leq 2^k - 2$

Algorithm

Input: n, m, Q(Y),P(X),R(Z)

Output: $GF\left(2^k\right) \rightarrow GF\left(2^n\right)^m,\ k = n \times m$

1. Find primitive elements of $GF\left(2^k\right): \gamma$
2. For($\alpha = 1; \alpha < 2^{nm} - 1;$) do

   if(isPrimitive(α)& $R(\alpha) mod\ Q(Y)P(X) \equiv 0$) break;

   end
3. For(i=0;i<$2^{nm} - 1$;i++)

   $a_1 = \alpha^i mod\ Q(Y)P(X),\ b_1 = \gamma^i mod\ R(Z)$

   Map: $b_1 \rightarrow a_1$

Example: $GF(2^4) \rightarrow GF(2^2)^2$

- $R(Z) = Z^4 + Z + 1, Q(Y) = Y^2 + Y + 1, P(X) = X^2 + X + \{2\}$, where $\{2\} \in GF(2^2)$.
- Note, $Q(Y)$ is used to construct $GF(2^2)$, while P(X) is used to extend to the field $GF(2^2)^2$.
- First primitive element $\gamma \in GF(2^4)$ is 2. It can be checked that '2' can be used to generate all the non-zero elements of $GF(2^4)$.
- Likewise, the first primitive element of $GF(2^2)^2$, st. $R(Z) \equiv 0[mod\ Q(Y)P(X)]$ is 4.
- Hence, the map is: $\{2\} \rightarrow \{4\}$. Also, 0 is mapped to 0.

Example Isomorphic Mapping $GF(2^4) \rightarrow GF(2^2)^2$

Proof that {4} $\in GF(2^2)^2$ is the correct choice.

Note, $\{4\} = 0100 = X$

$R(X) = X^4 + X + 1 \; mod \; Q(Y)P(X)$.

$GF(2^4) \rightarrow GF(2^2)^2$	$GF(2^4) \rightarrow GF(2^2)^2$
$\{02\} \rightarrow \{04\}$	$\{04\} \rightarrow \{06\}$
$\{08\} \rightarrow \{0e\}$	$\{03\} \rightarrow \{05\}$
$\{06\} \rightarrow \{02\}$	$\{0c\} \rightarrow \{08\}$
$\{0b\} \rightarrow \{0b\}$	$\{05\} \rightarrow \{07\}$
$\{0a\} \rightarrow \{0a\}$	$\{07\} \rightarrow \{03\}$
$\{0e\} \rightarrow \{0c\}$	$\{0f\} \rightarrow \{0d\}$
$\{0d\} \rightarrow \{09\}$	$\{09\} \rightarrow \{0f\}$
$\{01\} \rightarrow \{01\}$	$\{00\} \rightarrow \{00\}$

$X^2 = X + \{2\} \implies X^3 = 3X + \{2\} \implies X^4 = \{3\}X^2 + \{2\}X = \{3\}(X + \{2\}) + \{2\}X = X + 1 \implies R(4) = 0 \; mod \; Q(Y)P(X$

For checking, $3.2 \; in \; GF(2^2)$, express 3 as Y+1, and 2 as Y. Thus,

with the irreducible polynomial $Q(Y) = Y^2 + Y + 1$, we have

$Y(Y+1) = 1$.

An Efficient Conversion Algorithm

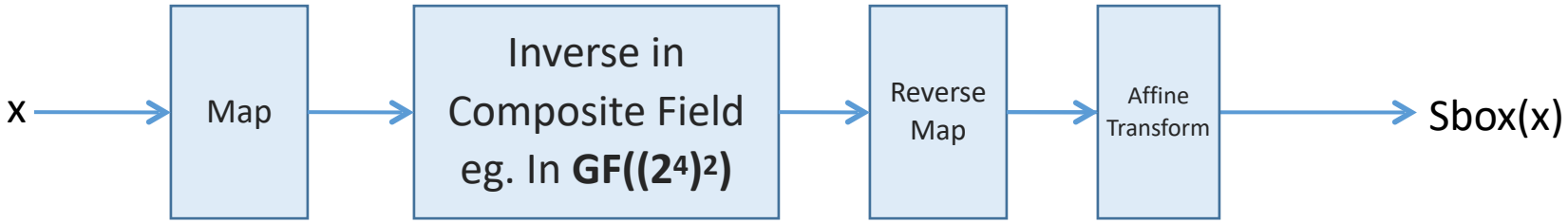
- Maps $GF\left(2^k\right) \rightarrow GF\left(2^n\right)^m,\ k = n \times m$
- Returns a binary $k \times k$, 0-1 matrix T, which performs the mapping.
- Evidently, the inverse of T does the reverse mapping.
- The mapping works by relating only k elements (rather than 2^k).
  - It maps the basis vectors.

The Mapping Matrix

$$T = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

AES in Composite Fields

- AES uses the binary finite field GF(2^8) with irreducible polynomial $x^8 + x^4 + x^3 + x + 1$
- The AES field GF(2^8) is isomorphic to the field GF((2^4)^2) and even GF(((2^2)^2)^2)
  - This means that we could find the inverse of x ∈ GF(2^8) by using a smaller field (eg. GF(2^4))
    - Thus smaller tables or equations required



Transforming GF(2^8) to GF(2^4)^2

- Let the reduction polynomials are as follows:
  - $GF(2^8)$: $Z^8 + Z^4 + Z^3 + Z + 1$
  - $GF(2^4)^2 : Y^2 + \tau Y + \mu$. Here $\mu = \omega^{14}$, where $\omega = (0010)_2$ is a primitive element in $GF\left(2^4\right)$ — just a choice. $\tau = 1$ — again a choice
  - $GF(2^4) : X^4 + X + 1$
- An element in $GF(2^4)^2$ is represented as $\gamma_1 Y + \gamma_0$, where $\gamma_0, \gamma_1 \in GF(2^4)$
- In polynomial basis, the element can be represented as $(\gamma_1 y + \gamma_0)$ where y is a root of $Y^2 + \tau Y + \mu$

Transforming GF(2^8) to GF(2^4)^2

- Previous easy technique works when all field polynomials are primitive.
- However, in case of AES the field polynomial $R(z) = z^8 + z^4 + z^3 + z + 1$ is irreducible but not primitive.
- Since the field is small exhaustive technique can be applied to find a primitive element.
- Basic idea was mapping a primitive element of $GF(2^8)$, say γ to a primitive element of $GF\left(2^4\right)^2$, say α.
- For the remaining elements we map $\gamma^i \rightarrow \alpha^i, \ \forall i \in [0, \cdots, \ 255]$

An Example T from GF(2^8) to GF(2^4)^2

$$T = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Consider $2 \in GF(2^8)$, ie can be denoted as (0000 0010).

Thus, T(2) would be in GF(2^4)^2, ie. (0010 1110)

Atri Rudra, Pradeep K. Dubey, Charanjit S. Jutla, Vijay Kumar, Josyula R. Rao, Pankaj Rohatgi:Efficient Rijndael Encryption Implementation with Composite Field Arithmetic. CHES 2001: 171-184

Pause

- Ok, we have mapped the element to $GF(2^4)^2$ no what??
- Let’s try to see why we did so

Finite Field Inversion in $GF(2^4)^2$

- Let us consider an element $\gamma_1 Y + \gamma_0$ and its inverse $\delta_1 Y + \delta_0$
- Reduction poly is $r(Y) = Y^2 + \tau Y + \mu$
- Then, $(\gamma_1 Y + \gamma_0)(\delta_1 Y + \delta_0) = 1 \ mod \ r(Y)$

Finite Field Inversion in $GF(2^4)^2$

- Let us consider an element $\gamma_1 Y + \gamma_0$ and its inverse $\delta_1 Y + \delta_0$
- Reduction poly is $r(Y) = Y^2 + \tau Y + \mu$
- Then, $(\gamma_1 Y + \gamma_0)(\delta_1 Y + \delta_0) = 1 \ mod \ r(Y)$

$$
\begin{aligned}
(\gamma_1 Y + \gamma_0)(\delta_1 Y + \delta_0) &= \gamma_1\delta_1 Y^2 + (\gamma_1\delta_0 + \gamma_0\delta_1)Y + \gamma_0\delta_0 \\
&= \gamma_1\delta_1(\tau Y + \mu) + (\gamma_1\delta_0 + \gamma_0\delta_1)Y + \gamma_0\delta_0 \\
&= (\gamma_1\delta_0 + \gamma_0\delta_1 + \gamma_1\delta_1\tau)Y + (\gamma_0\delta_0 + \gamma_1\delta_1\mu)
\end{aligned}
$$

Finite Field Inversion in $GF(2^4)^2$

$$\begin{aligned}(\gamma_1 Y + \gamma_0)(\delta_1 Y + \delta_0) &= \gamma_1\delta_1 Y^2 + (\gamma_1\delta_0 + \gamma_0\delta_1)Y + \gamma_0\delta_0 \\ &= \gamma_1\delta_1(\tau Y + \mu) + (\gamma_1\delta_0 + \gamma_0\delta_1)Y + \gamma_0\delta_0 \\ &= (\gamma_1\delta_0 + \gamma_0\delta_1 + \gamma_1\delta_1\tau)Y + (\gamma_0\delta_0 + \gamma_1\delta_1\mu)\end{aligned}$$

- From here, we can write,

$$\begin{aligned}\gamma_1\delta_0 + \gamma_0\delta_1 + \gamma_1\delta_1\tau &= 0 \\ \gamma_0\delta_0 + \gamma_1\delta_1\mu &= 1\end{aligned}$$

Finite Field Inversion in $GF(2^4)^2$

$$\begin{aligned}(\gamma_1 Y + \gamma_0)(\delta_1 Y + \delta_0) &= \gamma_1\delta_1 Y^2 + (\gamma_1\delta_0 + \gamma_0\delta_1)Y + \gamma_0\delta_0 \\ &= \gamma_1\delta_1(\tau Y + \mu) + (\gamma_1\delta_0 + \gamma_0\delta_1)Y + \gamma_0\delta_0 \\ &= (\gamma_1\delta_0 + \gamma_0\delta_1 + \gamma_1\delta_1\tau)Y + (\gamma_0\delta_0 + \gamma_1\delta_1\mu)\end{aligned}$$

- From here, we can write,

$$\begin{aligned}\gamma_1\delta_0 + \gamma_0\delta_1 + \gamma_1\delta_1\tau &= 0 \\ \gamma_0\delta_0 + \gamma_1\delta_1\mu &= 1\end{aligned}$$

$$\begin{aligned}\delta_0 &= (\gamma_0 + \gamma_1\tau)(\gamma_0^2 + \gamma_0\gamma_1\tau + \gamma_1^2\mu)^{-1} \\ \delta_1 &= \gamma_1(\gamma_0^2 + \gamma_0\gamma_1\tau + \gamma_1^2\mu)^{-1}\end{aligned}$$

What just happened?

- Ok, we still have to compute inverse !!
- But?

What just happened?

- Ok, we still have to compute inverse !!
- But, in $GF(2^4)$
- So, overall, we are able to represent a $GF(2^8)$ inverse in terms of $GF(2^4)$ inverses.
- But there are still some multiplications, XORs etc.
- Also, remember that we are still operating in polynomial basis..

Circuit Optimization in Polynomial Basis

- Let the irreducible polynomial of an element in $GF\left(2^4\right)^2$ be $r(Y) = Y^2 + \tau Y + \mu$, and let an element in the composite field be: $\gamma = \left(\gamma_1 Y + \gamma_0\right)$.
- As discussed before,

$$\delta_0 = \left(\gamma_0 + \gamma_1\tau\right)\left(\gamma_0^2 + \gamma_0\gamma_1\tau + \gamma_1^2\mu\right)^{-1}$$

$$\delta_1 = \gamma_1\left(\gamma_0^2 + \gamma_0\gamma_1\tau + \gamma_1^2\mu\right)^{-1}$$

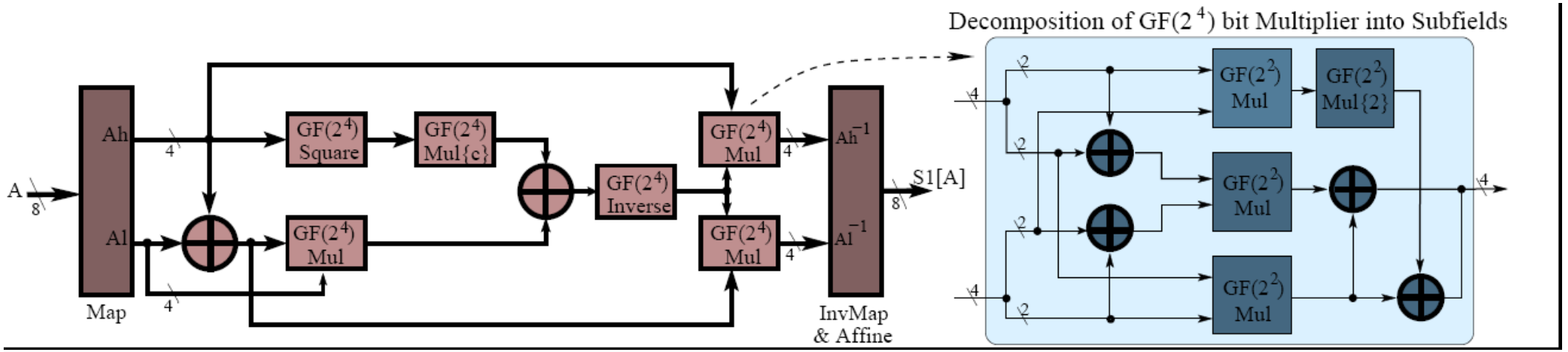
- As τ appears in both equations we set it to 1.

Bases

- Represented using two types of bases:
  - Polynomial base: Let p(x) be an irreducible polynomial over GF(2^m), and let α be the root of p(x). Then the set: $\{1,\alpha, \alpha^2, \cdots, \alpha^{m-1}\}$ is called the polynomial base.
  - Normal base: Let p(x) be an irreducible polynomial over GF(2^m), and let α be the root of p(x). Then the set: $\{\alpha, \alpha^2, \alpha^{2^2}, \cdots, \alpha^{2^{m-1}}\}$ is called the normal base, if the m elements are linearly independent.
    - For $GF(p^k)$: $\left\{\alpha^{p0}, \alpha^{p1}, \cdots, \alpha^{pk-1}\right\}$
    - For $GF(2^4)^2$: $\{\alpha, \alpha^{16}\}$

S-box Based on Composite Fields

S-box Approach



Gate Count for composite Sbox#

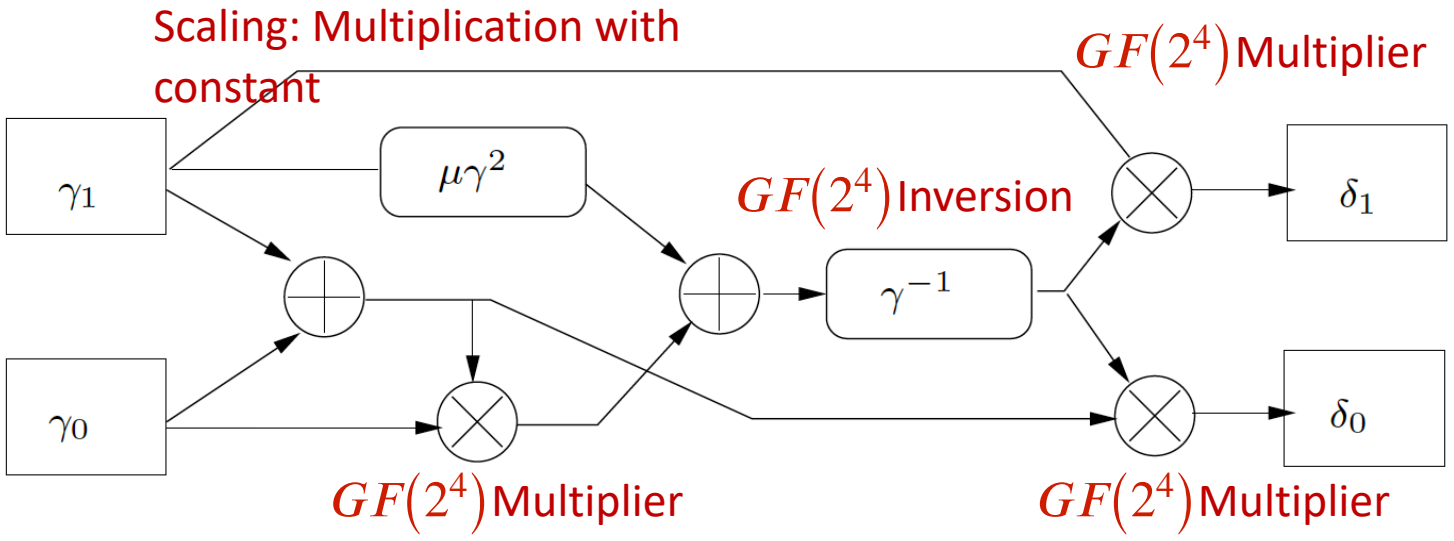
XOR	NAND	NOR	Total Gates in terms of NAND (using std cell lib)
80	34	6	180

Performance of S-boxes on FPGA*

S-box Approach	No. of Slices	Critical Path	Gate Count
table based	64	11.9ns	1128
Composite Field based	30	18.3ns	312

D. Canright, *A Very Compact S-box for AES*, CHES-2005
* Simulation Results using Xilinx ISE

Polynomial $GF(2^8)$ Inverter



$$\delta_0 = (\gamma_0 + \gamma_1)\left(\gamma_0(\gamma_0 + \gamma_1) + \mu\gamma_1^2\right)^{-1}$$

$$\delta_1 = \gamma_1\left(\gamma_0(\gamma_0 + \gamma_1) + \mu\gamma_1^2\right)^{-1}$$

Scaling and Squaring (Implementing $\mu\gamma^2$)

- The products in $GF(2^4)$ is similarly performed by expressing as elements in $GF\left(2^2\right)^2$.
- Consider the product of two elements:
  $\gamma = \Gamma_1 Z + \Gamma_0$, and $\delta = \Delta_1 Z + \Delta_0$, using the irreducible polynomial
  $s(Z) = Z^2 + Z + N$, we have:

$$(\Gamma_1 Z + \Gamma_0)(\Delta_1 Z + \Delta_0) = Z\left(\Gamma_0\Delta_0 + \left(\Gamma_1 + \Gamma_0\right)\left(\Delta_1 + \Delta_0\right)\right) + (\Gamma_0\Delta_0 + N\Gamma_1\Delta_1)$$

- For scaling, proper choices of the constant μ can lead to interesting scopes for optimizations. We set, $\Delta_0 = 0$ in $\mu = \Delta_1 Z + \Delta_0$. Note, $\Delta_1 \neq 0$, as then μ cannot make the polynomial $r(Y)$ irreducible over $GF\left(2^4\right)$.
- Further, we choose $N = \Delta_1^{-1}$, to simplify the scaling operation.

Scaling and Squaring (Implementing $\mu\gamma^2$)

- The choice of N makes the polynomial $s(Z) = Z^2 + Z + N$ irreducible over $GF(2^2)$.
- Thus, N is the root of $t(W) = W^2 + W + 1$, and the roots cannot be 0, 1.
- They are denoted as N, N+1 (note that the sum is 1).
- Depending on the roots chosen for the polynomial basis (W,1), thus either $N = W,$ or $N^2 = N + 1 = W.$
- Note, $N^{-1} = N^2 = N + 1$. This leads to very efficient scaling and squaring circuits.

Scaling and Squaring (Implementing $\mu\gamma^2$)

- $\mu\gamma^2 = \mu\left(\Gamma_1 Z + \Gamma_0\right)^2 = \mu(\Gamma_1^2 Z + \left(\Gamma_0^2 + N\Gamma_1^2\right))$
- Substituting, $\mu = \Delta_1 Z = N^{-1}Z = N^2 Z$, thus we have:
-

$$\mu\gamma^2 = N^2 Z\left(\Gamma_1^2 Z + \left(\Gamma_0^2 + N\Gamma_1^2\right)\right)$$

$$= N^2\Gamma_1^2 Z^2 + Z\left(N^2\Gamma_0^2 + \Gamma_1^2\right) = N^2\Gamma_1^2 Z^2 + Z\left(N^2\Gamma_0^2 + \Gamma_1^2\right)$$

$$= N^2\Gamma_1^2(Z + N) + Z\left(N^2\Gamma_0^2 + \Gamma_1^2\right) = Z\left(N^2\Gamma_1^2 + N^2\Gamma_0^2 + \Gamma_1^2\right) + \Gamma_1^2$$

$$= Z\left(N\Gamma_1^2 + N^2\Gamma_0^2\right) + \Gamma_1^2$$

Operations in $GF(2^2)$

- Reducing with polynomial $t(W) = W^2 + W + 1$.
- Thus we have for $\Gamma = g_1 W + g_0,\ \Delta = d_1 W + d_0,$

$$(g_1 W + g_0)(d_1 W + d_0) = W(g_1 d_1 + g_1 d_0 + g_0 d_1) + (g_1 d_1 + g_0 d_0) = W\Big(g_0 d_0 + (g_1 + g_0)(d_1 + d_0)\Big) + (g_0 d_0 + g_1 d_1)$$

- Note the compact expression above.
- Now the multiplications and additions are in GF(2) and are thus equivalent to AND and XOR gates respectively (Finally!!!)

Squaring and Scaling is Free in $GF(2^2)$

- Like before, we can also combine the squaring and multiplication operations for efficiency.
- Thus, assuming $N = W$,

$$W\Gamma^2 = W(g_1 W + g_0)^2 = W\Big(g_1 W + (g_0 + g_1)\Big) = \Big(g_1 + (g_1 + g_0)\Big)W + g_1 = g_0 W + g_1$$

Thus, we see that the squaring and scaling operation is free in the polynomial basis of $GF(2^2)$!!!

Back to Squaring and Scaling in $GF(2^2)$

- The scaling operation to compute $N\Gamma$ can be computed using the fact $N = W$ or $N = W^2$.
- Assuming, $N = W$ thus:

$$W(g_1W + g_0) = W(g_1 + g_0) + g_1$$
$$W^2(g_1W + g_0) = g_0W + (g_0 + g_1)$$

Final look at the square and scaling in $GF(2^4)$

- $\mu\gamma^2 = Z\left(N\Gamma_1^2 + N^2\Gamma_0^2\right) + \Gamma_1^2 = Z\left(\left\{N\Gamma_1^2\right\} + N\left\{N\Gamma_0^2\right\}\right) + N^2\left\{N\Gamma_1^2\right\}$
- Portions with { } are free!
- Thus the entire operation can be done with one addition and two scaling operations.

Polynomial $GF(2^4)$ Inverter

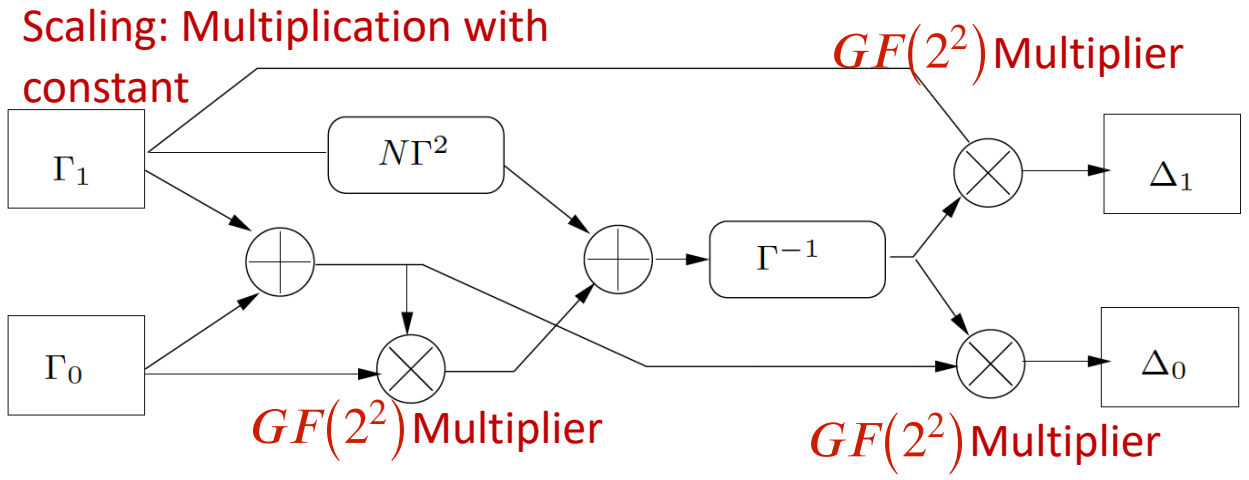
- The inverse of an element in $GF(2^2)^2$ is denoted as:

$$\Delta = (\Gamma_1 Z + \Gamma_0)^{-1} = (\Delta_1 Z + \Delta_0) mod(Z^2 + Z + N)$$

- Thus,

$$\Delta_0 = (\Gamma_0 + \Gamma_1)(\Gamma_0(\Gamma_0 + \Gamma_1) + \Gamma_1^2 N)^{-1}$$

$$\Delta_1 = \Gamma_1(\Gamma_0(\Gamma_0 + \Gamma_1) + \Gamma_1^2 N)^{-1}$$



Inversion in $GF(2^2)$

- Like before, we can obtain the inversion in a similar fashion.
- Thus, for an element in $GF(2^2)$, say $G = g_1 W + g_0$, we have $D = G^{-1} = (d_1 W + d_0),\ d_1, d_0 \in GF(2).$
- The irreducible polynomial is $t(W) = W^2 + W + 1.$
- Thus, $d_0 = (g_0 + g_1)(g_0^2 + g_0 g_1 + g_1^2)^{-1} = (g_0 + g_1)(g_0 + g_0 g_1 + g_1) = (g_0 + g_1)$
  - For $g \in GF(2), g^2 = g,\ g^{-1} = g\,.$
- Similarly, $d_1 = g_1(g_0 + g_0 g_1 + g_1) = g_1$
- Note the special case of inverse of 0, is handled by these equations implicitly by resulting 0 output.

Field Isomorphism between $GF(2^8)$ and $GF((2^2)^2)^2$

- We present another way for this mapping.
- Say an element $g \in GF(2^8)$, which is the standard representation of an element of the state matrix of AES, is denoted by the byte $(g_7 g_6 \cdots g_0)$.
- The polynomial representation is: $g_7 X^7 + g_6 X^6 + \cdots + g_1 X + g_0$.
- We map the element to a new element $(b_7 b_6 \cdots b_0)$ in a new basis.
- In polynomial basis thus for $g \in GF(2^8)/GF(2^4)$, we have

  $g = \gamma_1 Y + \gamma_0, \quad where\ \gamma_1, \gamma_0 \in GF(2^4)/GF(2^2)$

  - That is, for each $\gamma \in GF(2^4)/GF(2^2)$, $\gamma = \Gamma_1 Z + \Gamma_0$.

Field Isomorphism between $GF(2^8)$ and $GF((2^2)^2)^2$

- Further each element $\Gamma \in GF(2^2)$ can be viewed as $(b_1 W + b_0)$, and can be represented as a pair of bits (b_1, b_0).
- Thus the relation between the two byte representations of g is as follows:

$$g_7 X^7 + g_6 X^6 + \cdots + g_1 X + g_0$$

$$= \left[(b_7 W + b_6) Z + (b_5 W + b_4) \right] Y + \left[(b_3 W + b_2) Z + (b_1 W + b_0) \right]$$

$$= b_7(WZY) + b_6(ZY) + b_5(WY) + b_4(Y) + b_3(WZ) + b_2(Z) + b_1(W) + b_0$$

Field Isomorphism between $GF(2^8)$ and $GF((2^2)^2)^2$

- The mapping is decided for a choice of the basis denoted as (Y, Z, W).
- These values are fixed by the choice of the parameters μ and N.
- As an example, consider $\mu = 0XEC,\ N = 0XBC,$ then the basis choices are $Y = 0XFF, Z = 0X5C, W = 0XBD$.
- As an example to justify these values: take N=0XBC=(1011 1100)= $x^7 + x^5 + x^4 + x^3 + x^2$
  - Remember that N has to be a root of the irreducible polynomial of $GF(2^2)$.
  - Substitute N in $W^2 + W + 1$, and perform modulo the AES polynomial $x^8 + x^4 + x^3 + x + 1$

Checking for N

- $N^2 = x^{14} + x^{10} + x^8 + x^6 + x^4$
- $N + 1 = x^7 + x^5 + x^4 + x^3 + x^2$+1
- Using, $x^8 + x^4 + x^3 + x + 1$ as the reduction polynomial, thus we substitute
  $x^8 = x^4 + x^3 + x + 1 \Rightarrow x^9 = x^5 + x^4 + x^2 + x$
- Thus, $x^{10} = x^6 + x^5 + x^3 + x^2$, and
  $x^{14} = x^{10} + x^9 + x^7 + x^6 = \left(x^6 + x^5 + x^3 + x^2\right) + \left(x^5 + x^4 + x^2 + x\right) + x^7 + x^6 = x^7 + x^4 + x^3 + x$
- Thus,

$$N^2 + N + 1$$

$$= x^{14} + x^{10} + x^8 + x^6 + x^4 + x^7 + x^5 + x^4 + x^3 + x^2 + 1$$

$$= x^{14} + x^{10} + x^8 + x^7 + x^6 + x^5 + x^3 + x^2 + 1$$

$$= x^7 + x^4 + x^3 + x + x^6 + x^5 + x^3 + x^2 + x^4 + x^3 + x + 1 + x^7 + x^6 + x^5 + x^3 + x^2 + 1$$

$$= 0$$

Checking for N

$$N^2 + N + 1$$

$$= x^{14} + x^{10} + x^8 + x^6 + x^4 + x^7 + x^5 + x^4 + x^3 + x^2 + 1$$

$$= x^{14} + x^{10} + x^8 + x^7 + x^6 + x^5 + x^3 + x^2 + 1$$

$$= x^7 + x^4 + x^3 + x + x^6 + x^5 + x^3 + x^2 + x^4 + x^3 + x + 1 + x^7 + x^6 + x^5 + x^3 + x^2 + 1$$

$$= 0.$$

The Resultant Mapping

$$\begin{pmatrix} g_7 \\ g_6 \\ g_5 \\ g_4 \\ g_3 \\ g_2 \\ g_1 \\ g_0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} b_7 \\ b_6 \\ b_5 \\ b_4 \\ b_3 \\ b_2 \\ b_1 \\ b_0 \end{pmatrix}$$

D. Canright, *A Very Compact S-box for AES*, CHES-2005

This mapping denoted as X is from the field $GF((2^2)^2)^2$ to $GF(2^8)$. The inverse mapping can be obtained by computing the inverse of the above matrix.