A Very Compact AES

Abhishek Bajpai

November 7, 2016

Contents

Abstract

1 AES

A round in AES comprised of following functions

1. **AddRoundKey** : $S \oplus Rk$ where S is state matrix
2. **SubBytes** : $AT(s^{-1})$ where s id element of state matrix and AT is affine transform
3. **ShiftRow** : Permutation in rows (not important)
4. **MixColumn**: $c(x) = 3x^3 + x^2 + x + 2$
$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

Now SubBytes can be optimised be doing inverse in sub field $(GF(2^4)^2)$. Let's say δ emplies $GF(2^8)$ to $GF(2^4)^2$ transformation matrix and δ^{-1} emplies $GF(2^4)^2$ to $GF(2^8)$

then SubBytes can be implemented as:

$AT(\delta^{-1} \times (\delta \times s)^{-1}) \Rightarrow M \times (\delta^{-1} \times (\delta \times s)^{-1}) \oplus C$

if we some how do the AT in subfield then implementation would be

$\Rightarrow \delta^{-1} \times (M' \times (\delta \times s)^{-1} \oplus C')$

I can derive M' and C' as

$M' = \delta \times M \times \delta^{-1}$

$C' = \delta \times C$

now as shift row is just a row permutation then

$$
\begin{aligned}
Round &\Rightarrow MixColumn(ShiftRow(SubBytes(addroundkey(S)))) \\
&\Rightarrow MixColumn(ShiftRow(SubBytes(Rk \oplus S))) \\
&\Rightarrow MixColumn(ShiftRow(\delta^{-1} \times (M' \times (\delta \times s)^{-1} \oplus C'))) \\
&\text{where s is element of S} \\
&\Rightarrow MixColumn(\delta^{-1} \times (ShiftRow(M' \times (\delta \times s)^{-1} \oplus C'))) \qquad (1) \\
&\text{Now we know that mixcolumn also works in same } GF(2^8) \\
thus &\Rightarrow \delta^{-1} \times (MixColumn'(ShiftRow(M' \times (\delta \times s)^{-1} \oplus C'))) \\
&\text{further } \delta \times s \text{ emplies element of } \delta \times S \oplus \delta \times Rk \\
&\Rightarrow \delta^{-1} \times Round(\delta \times S)
\end{aligned}
$$

where $MixColumn'$ is $MixColumn$ in $GF((2^4)^2)$

This suggests that we can do all the round calculations in subfield while doing so we can eleminate implementing δ and δ^{-1} in each round. further decreasing latency.