Dual AES

Jaroslav Šeděnka

Institute of Mathematics and Statistics
Faculty of Science, Masaryk University

Spring School of Algebra, April 2013

Overview

1. Galois Field $GF(2^8)$
2. Description of AES
3. What operations do you need to compute AES?
4. Dual AES
5. What can you do with dual AES?

Galois Field $GF(2^8)$

Consider the field $GF(2) = \{0, 1\}$.

For any irreducible polynomial $p(x) \in GF(2)[x]$, we can construct the factorring $GF(2^8) := GF(2)[x]/(p(x))$.

Then, $GF(2^8)$ is up to isomorphism the unique finite field with 2^8 elements. Trivially, $GF(2^8)$ is a vector space over $GF(2)$.

The multiplicative group of $GF(2^8)$ is cyclic.

Operations in the $GF(2^8)$

Addition

$a(x) \oplus b(x) = (a_7 \oplus b_7)x^7 + (a_6 \oplus b_6)x^6 + ... + (a_0 \oplus b_0)$, where the $a \oplus b$ denotes XOR of bits a, b.

For example $10100110 \oplus 10000011 = 00100101$.

Operations in the $GF(2^8)$

Multiplication

$$a(x) \bullet b(x) = a(x)b(x) \mod (x^8 + x^4 + x^3 + x + 1)$$

$$10100110 \bullet 10000011 = 01110110$$

Operations in the $GF(2^8)$

Multiplication

$$a(x) \bullet b(x) = a(x)b(x) \mod (x^8 + x^4 + x^3 + x + 1)$$

$10100110 \bullet 10000011 = 01110110$
$(x^7 + x^5 + x^2 + x) \bullet (x^7 + x + 1) =$
$(x^{14} + x^{12} + x^9 + x^7 + x^8 + x^6 + x^3 + x^2 + x^7 + x^5 + x^2 + x)$
$\mod (x^8 + x^4 + x^3 + x + 1) = x^6 + x^5 + x^4 + x^2 + x$

Operations in the $GF(2^8)$

Multiplicative inverse

$a(x)^{-1}$ modulo $(x^8 + x^4 + x^3 + x + 1)$ can be computed using Extended Euclidean Algorithm.

Inverse of 10100110 is ...

Squaring in $GF(2^8)$

Proposition

The function $f(x) = x^2$ is $GF(2)$-linear in $GF(2^8)$.

Proof.

The only scalar multiples are $0, 1$.
Let $a, b \in GF(2^8)$. The characteristic of $GF(2^8)$ is 2, thus
$(a \oplus b)^2 = a^2 \oplus 2ab \oplus b^2 = a^2 \oplus b^2$. $\square$

So, there exists matrix Q with boolean coefficients, such that $Qx = x^2$. Also, the matrix Q is invertible.

Advanced Encryption Standard (AES)

- symmetric block cipher
- current NIST standard
- proposed in 1999 by J. Daemen and V. Rijmen (Rijndael)
- substitution-permutation network
- block size is fixed (128 bits), key size is variable (128, 194 or 256 bits)
- in this lecture, the AES-128 will be described

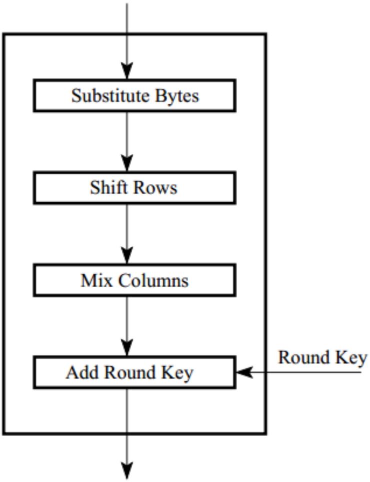
AES State Array

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

Data representation:

- intermediate data block is stored in a 4x4 array of bytes
- Each byte $s_{i,j}$ is interpreted as an element of $GF(2^8) = GF(2)[x]/(x^8 + x^4 + x^3 + x + 1)$
- Example: byte 10100110 is represented as $x^7 + x^5 + x^2 + x$
- Also, 10100110 can be written as $\{A6\}$

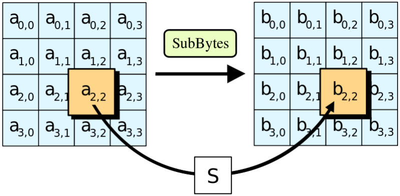
AES Algorithm overview



Encryption Round

- 10 round of AES are performed
- initial and final rounds are slightly different

AES SubBytes



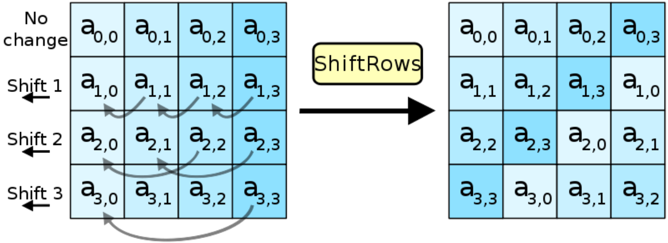
Byte-wise substitution:

- take the multiplicative inverse $b_{i,j} = a_{i,j}^{-1}$ in $GF(2^8)$
- apply an affine transformation $b'_{i,j} = Ab_{i,j} + c$

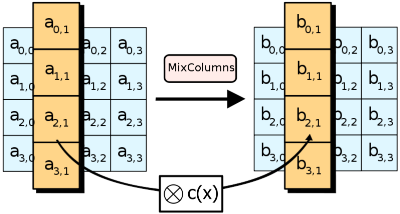
AES SubBytes

$$\begin{bmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \\ b_4' \\ b_5' \\ b_6' \\ b_7' \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

AES ShiftRows



AES MixColumns

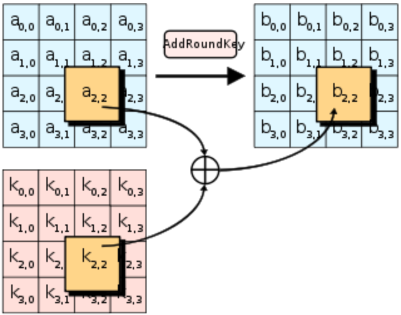


$$b(y) = a(y) \otimes c(y) \mod y^4 + 1$$

as polynomials in $GF(2^8)[y]$.

$$c(y) = \{03\}y^3 + \{01\}y^2 + \{01\}y + \{02\}$$

AES AddRoundKey



Whole state array is XORed with expanded Round key.

What operations do you need to compute AES?

$GF(2^8)$ operations

- addition $x \oplus y$
- XOR with a constant $x \oplus c$
- multiplication $x \bullet y$
- multiplication by a constant $x \bullet c$
- raise to any power in $GF(2^8)$, including to power -1

Non-$GF(2^8)$ operations

- permutation of n-tuples
- $GF(2)$-linear transformation
- table lookup

Let's call these $EGF(2^8)$ *operations*.

Dual cipher

Definition: Dual Ciphers

Two ciphers E, E' are called *dual ciphers*, if there exist invertible functions $f(\cdot)$, $g(\cdot)$ and $h(\cdot)$ such that for each plaintext P and key K

$$f(E_K(P)) = E'_{g(K)}(h(P))$$

Square cipher

Definition: Square Cipher

Given a cipher E that uses only $EGF(2^8)$ operations, we define the cipher E^2 by modifying the constants of E this way:

- whenever there is XOR with c in E, there is XOR with c^2 in E^2
- whenever there is multiplication by c in E, there is multiplication by c^2 in E^2
- whenever there is multiplication by matrix A in E, there is multiplication by QAQ^{-1} in E^2
- whenever there is table lookup $S(x)$ in E, there is $QS(Q^{-1}x)$ in E^2.

Square AES

Theorem

For any cipher E using only operations in $EGF(2^8)$, the ciphers E and E^2 are dual ciphers.

Proof

We need to show the "duality" for all operations in $EGF(2^8)$, that is, $(E_K(P))^2 = E^2_{K^2}(P^2)$ for all P, K. Note that by $(E_K(P))^2$ we mean byte-wise squaring.

- addition: $(x \oplus y)^2 = x^2 \oplus y^2$ is exactly the linearity of squaring in $GF(2^8)$.

Square AES

Theorem

For any cipher E using only operations in $EGF(2^8)$, the ciphers E and E^2 are dual ciphers.

Proof

We need to show the "duality" for all operations in $EGF(2^8)$, that is, $(E_K(P))^2 = E^2_{K^2}(P^2)$ for all P, K. Note that by $(E_K(P))^2$ we mean byte-wise squaring.

- addition: $(x \oplus y)^2 = x^2 \oplus y^2$ is exactly the linearity of squaring in $GF(2^8)$.
- multiplication: $(x \bullet y)^2 = x^2 \bullet y^2$

Square AES

Theorem

For any cipher E using only operations in $EGF(2^8)$, the ciphers E and E^2 are dual ciphers.

Proof

We need to show the "duality" for all operations in $EGF(2^8)$, that is, $(E_K(P))^2 = E^2_{K^2}(P^2)$ for all P, K. Note that by $(E_K(P))^2$ we mean byte-wise squaring.

- addition: $(x \oplus y)^2 = x^2 \oplus y^2$ is exactly the linearity of squaring in $GF(2^8)$.
- multiplication: $(x \bullet y)^2 = x^2 \bullet y^2$
- exponentiation: $(x^k)^2 = (x^2)^k$

Square AES

Theorem

For any cipher E using only operations in $EGF(2^8)$, the ciphers E and E^2 are dual ciphers.

Proof

We need to show the "duality" for all operations in $EGF(2^8)$, that is, $(E_K(P))^2 = E^2_{K^2}(P^2)$ for all P, K. Note that by $(E_K(P))^2$ we mean byte-wise squaring.

- addition: $(x \oplus y)^2 = x^2 \oplus y^2$ is exactly the linearity of squaring in $GF(2^8)$.
- multiplication: $(x \bullet y)^2 = x^2 \bullet y^2$
- exponentiation: $(x^k)^2 = (x^2)^k$
- permutation of n-tuples is trivial

Proof.

- linear transformation: $(Ax)^2 = QAQ^{-1}x^2 = QAx = (Ax)^2$
- table lookup: $S(x)^2 = QS(Q^{-1}x)$.

By structural induction, $(E_K(P))^2 = E^2_{K^2}(P^2)$.

$\square$

In a similar way, any invertible linear transformation can be used to create dual ciphers. Mainly, change of irreducible polynomial $p(x)$ used to construct the Galois Field is also linear.

What can you do with dual ciphers?

- Different dual variants of a cipher may be faster for encryption/decryption
- When the attacker has partial or total access to the encryption process, change of bases during the computatiton can increase security
- The property of cipher being nontrivialy dual to itself can be abused for cryptoanalysis

Thank you for your attention

Questions, comments?

References

Elad Barkan and Eli Biham.
In how many ways can you write rijndael?
In *in Proceedings of Asiacrypt'02*, pages 160–175.
Springer-Verlag, 2002.

Federal Information Processing.
Announcing the advanced encryption standard (aes), 2001.