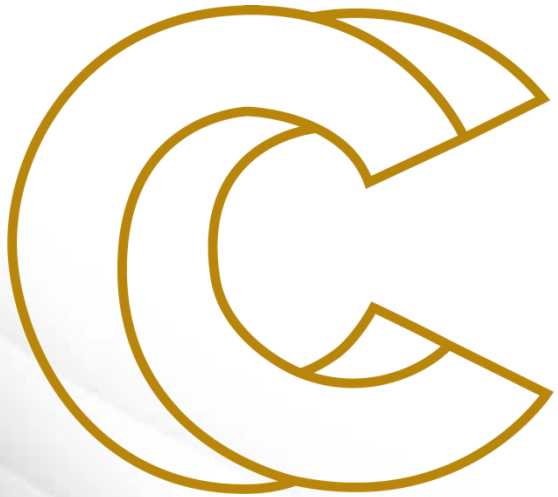


EURO^2

GPU Optimization of Advanced Encryption Standard

Cihangir Tezcan, PhD

Graduate School of Informatics, METU, Ankara

ncc@ulakbim,gov,tr

Lesson 2: Advanced Encryption Standard

Data Encryption Standard (DES)

- Designed by IBM in 1970s, based on an earlier design by Feistel.
- In 1976, NSA tweaked the algorithm by changing its S-boxes.
  - **Block Size:** 64 bits
  - **Key Length:** 56 bits
  - **Rounds:** 16
- Currently known as Data Encryption Algorithm (DEA) since it is no longer a standard.
- Became useless after 1990s since its short key is susceptible to brute force attacks.

Lesson 2: Advanced Encryption Standard

EURO^2

Short Keys

- An attacker that captures a single ciphertext, can try to decrypt it with every possible key to check if it provides a meaningful plaintext.
- Such an attack is called exhaustive search or brute force attack.
- Exhaustive search is a generic attack, i.e. valid for every cipher.
- For a **k**-bit keyed cipher, the attacker is required to perform at most $\mathbf{2^k}$ encryptions/decryptions.
- Thus, security of a block cipher is upper bounded by exhaustive search.

Lesson 2: Advanced Encryption Standard

Short Keys

2^{56} =	72,057,594,037,927,936
2^{80} =	1,208,925,819,614,629,174,706,176
2^{128} =	340,282,366,920,938,463,463,374,607,431,768,211,456
2^{192} =	6,277,101,735,386,680,763,835,789,423,207,666,416,102,355,444,464,034,512,896
2^{256} =	115,792,089,237,316,195,423,570,985,008,687,907,853,269,984,665,640,564,039,457,584,007,913,129,639,936

Lesson 2: Advanced Encryption Standard

Advanced Encryption Standard (AES)

- Rijndael is designed by Joan Daemen and Vincent Rijmen.
- Standardized in 2001 by NIST (winner of the AES competition) and named AES.
  - **Block Size:** 128 bits
  - **Key Length:** 128, 192, 256 bits
  - **Rounds:** 10, 12, 14 (depends on the key length)
  - **Type:** SPN
- Known attacks are ineffective.

Lesson 2: Advanced Encryption Standard

Advanced Encryption Standard (AES)

Byte ordering of AES

0	4	8	12
1	5	9	13
2	6	10	14
3	7	11	15

A byte can be treated in two ways when dealing with AES:

1. A byte can be viewed as a string of 8 bits
2. A byte can be viewed as an element of Galois Field GF(2^8)

Lesson 2: Advanced Encryption Standard

Arithmetic in *GF(2^8)*

- AES uses the Galois Field defined by the irreducible polynomial

$$R_p = X^8 + X^4 + X^3 + X + 1$$

- A byte can be represented by a degree 7 polynomial where the bits of the byte corresponds to coefficients of this polynomial.
- Now we can perform addition and multiplication on these polynomials modulo R_p
- This more mathematical representation is better to understand the security of the cipher

Lesson 2: Advanced Encryption Standard

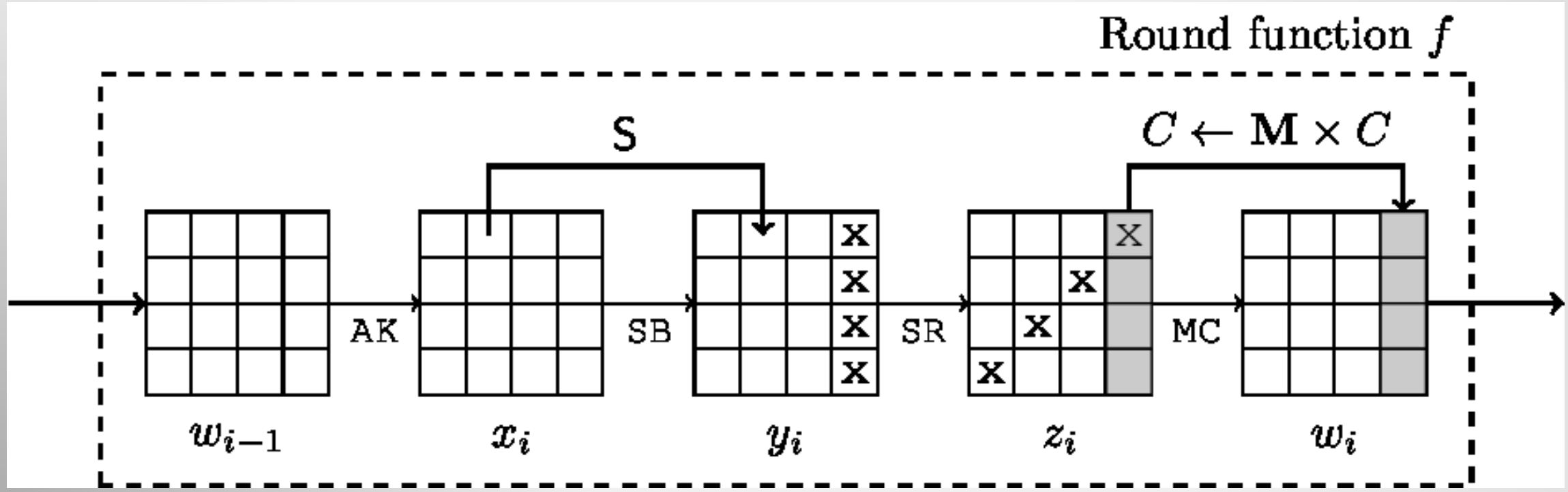
Round Function of AES

Round function of AES contains the following operations:

1. **Key Addition (AK):** XOR the 128-bit round key with the input
2. **Sub Bytes (SB):** Apply 8x8 S-box on 16 bytes
3. **Shift Rows (SR):** Rotate rows to the left
4. **Mix Columns (MC):** Multiply by matrix M

Lesson 2: Advanced Encryption Standard

Advanced Encryption Standard (AES)



Lesson 2: Advanced Encryption Standard

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

S-box of AES

Input $3b$ means the 3rd row and bth column (i.e. $S(3b) = e2$)

Lesson 2: Advanced Encryption Standard

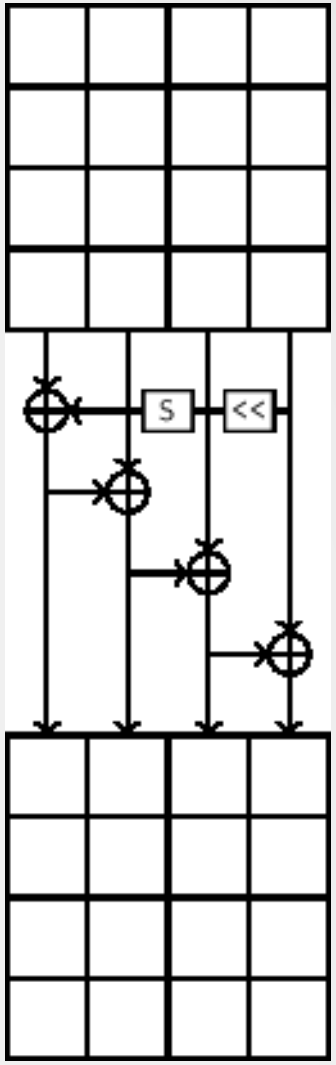
Mix Columns (MC) *(Omitted in the last round!)*

$$M = \begin{pmatrix} 0x02 & 0x03 & 0x01 & 0x01 \\ 0x01 & 0x02 & 0x02 & 0x01 \\ 0x01 & 0x01 & 0x03 & 0x03 \\ 0x02 & 0x01 & 0x01 & 0x02 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{pmatrix}$$

Lesson 2: Advanced Encryption Standard

Key Schedule

- The 128-bit master key is also the first round key
- Next round key is obtained by the previous one by performing:
  1. Byte rotation
  2. Four S-box operation
  3. Round Constant Addition
  4. XOR of 32-bit values



Next lecture

Mode of Operations for Block Ciphers

- When we use a block cipher, we need to choose a mode of operation to determine how we encrypt plaintext that is larger than a single block.
- Some mode of operations are not secure.
- Some mode of operations allow parallelization.

Thanks

This project has received funding from the European High-Performance Computing Joint Undertaking (JU) under grant agreement No 101101903, The JU receives support from the Digital Europe Programme and Germany, Bulgaria, Austria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Greece, Hungary, Ireland, Italy, Lithuania, Latvia, Poland, Portugal, Romania, Slovenia, Spain, Sweden, France, Netherlands, Belgium, Luxembourg, Slovakia, Norway, Türkiye, Republic of North Macedonia, Iceland, Montenegro, Serbia