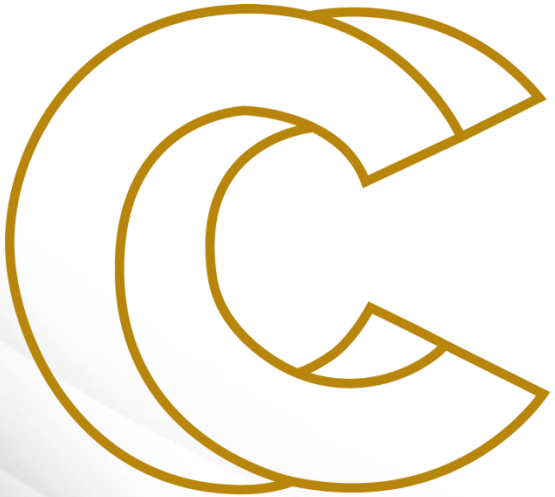


EURO 4SEE

GPU Assisted Brute Force Cryptanalysis of GPRS, GSM, RFID, and TETRA

CihangirTezcan, PhD
Graduate School of Informatics, METU, Ankara

ncc@ulakbim.gov.tr

Lesson 3: KASUMI Block Cipher

KASUMI Block Cipher

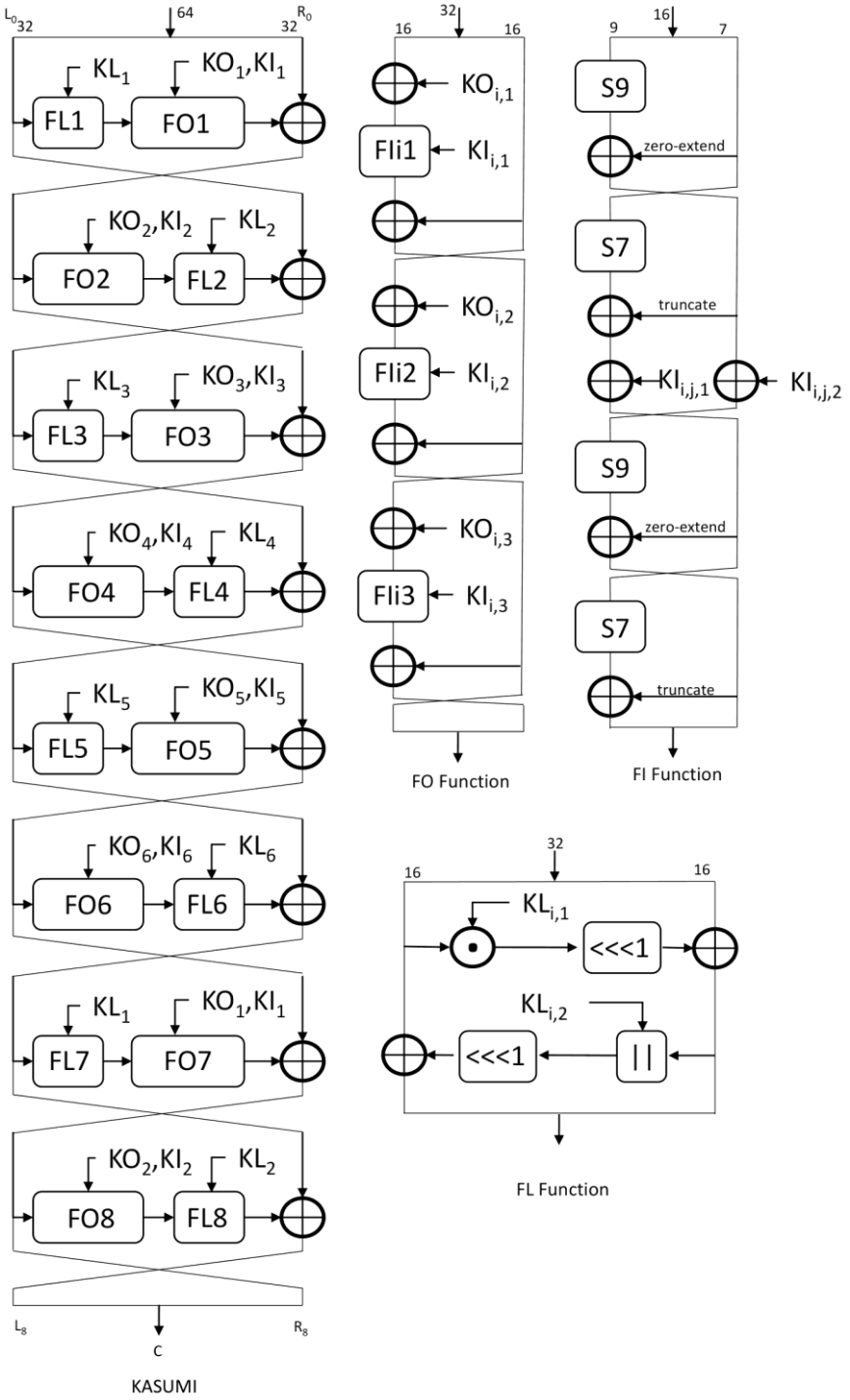
- KASUMI was designed by ETSI SAGE.
- It is a modified version of the block cipher MISTY1.
- It is a *Feistel* block cipher
  - **Number of rounds:** 8
  - **Block size:** 64 bits
  - **Key size:** 128 bits
- The key schedule of KASUMI simply consists of rotations on 16-bit values and XOR with constants.
- The round function of KASUMI contains FO and FL functions where FL function contains AND, OR, and rotation operations and FO function is also a 3-round Feistel structure which contains FI functions in each of its round.
- Moreover, FI functions is a four round Feistel structure which uses two S-boxes of sizes 7x7 and 9x9 consecutively in each round.

Lesson 3: KASUMI Block Cipher

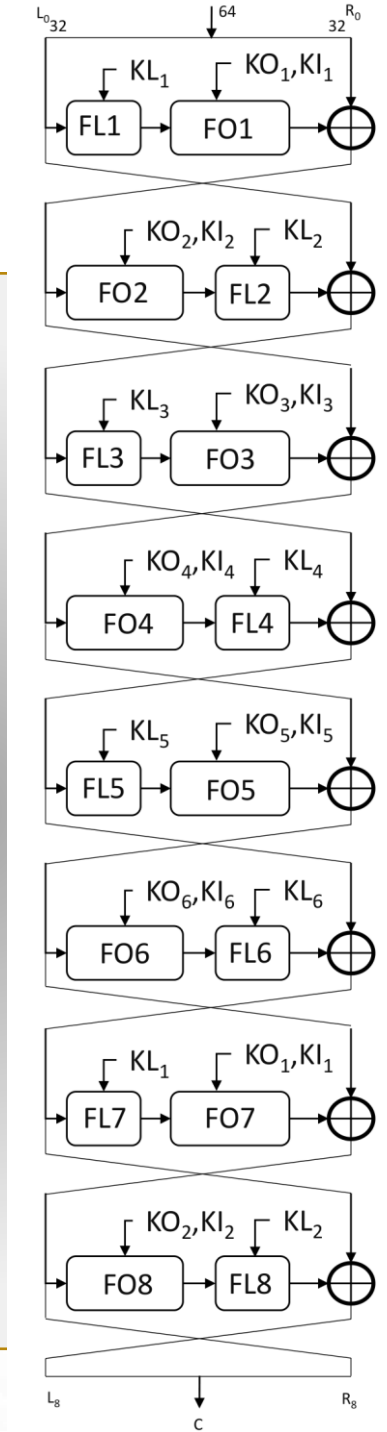
KASUMI Key Schedule

- The 128-bit key ***K*** is divided into eight 16-bit subkeys K_i:
  - $K=K_1||K_2||K_3||K4||K5||K6||K7||K8$
- Additionally a modified key ***K'***, similarly divided into 16-bit subkeys K'_i is used.
- The modified key is derived from the original key by XORing with 0x123456789ABCDEFFEDCBA9876543210
- The round keys are as follows:
  - $KL_{i,1} = ROL(K_{i,1})$
  - $KL_{i,2} = K'_{i+2}$
  - $KO_{i,1} = ROL(K_{i+1,5})$
  - $KO_{i,2} = ROL(K_{i+5,8})$
  - $KO_{i,3} = ROL(K_{i+6,13})$
  - $KI_{i,1} = K'_{i+4}$
  - $KI_{i,2} = K'_{i+3}$
  - $KI_{i,3} = K'_{i+7}$

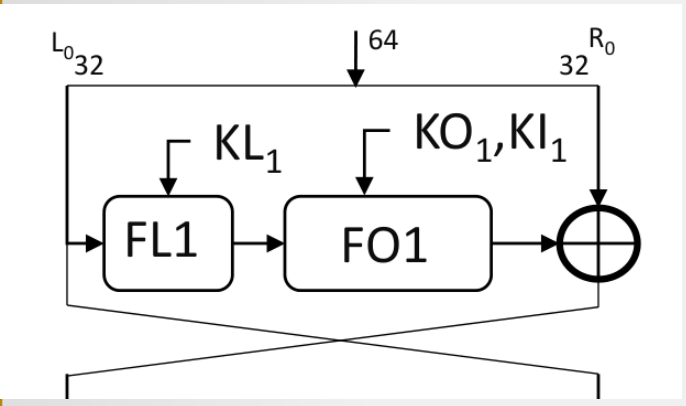
Lesson 3: KASUMI



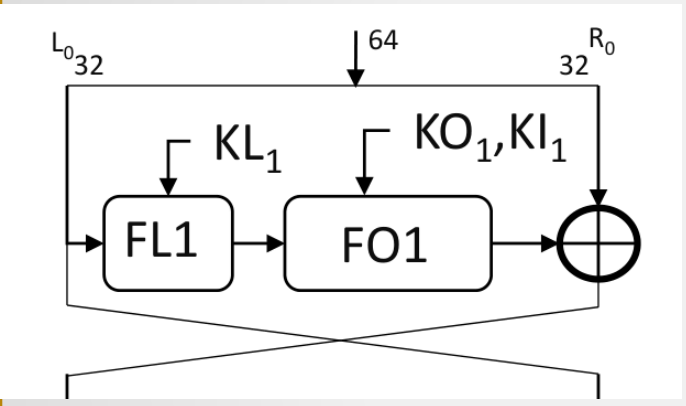
Lesson 3: KASUMI Block Cipher

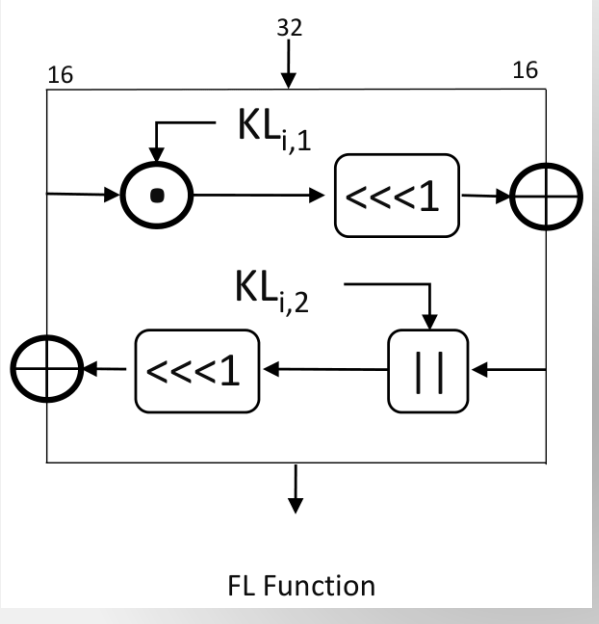


Lesson 3: KASUMI Block Cipher



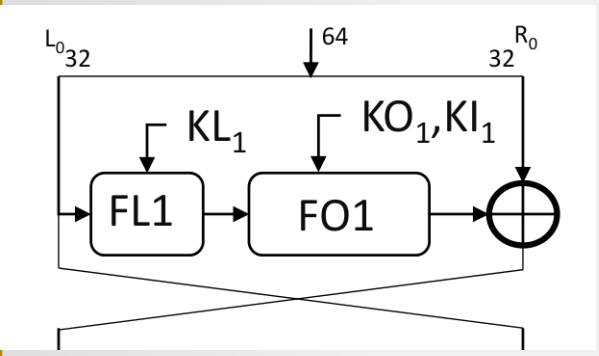
Lesson3:KASUMIBlockCipher

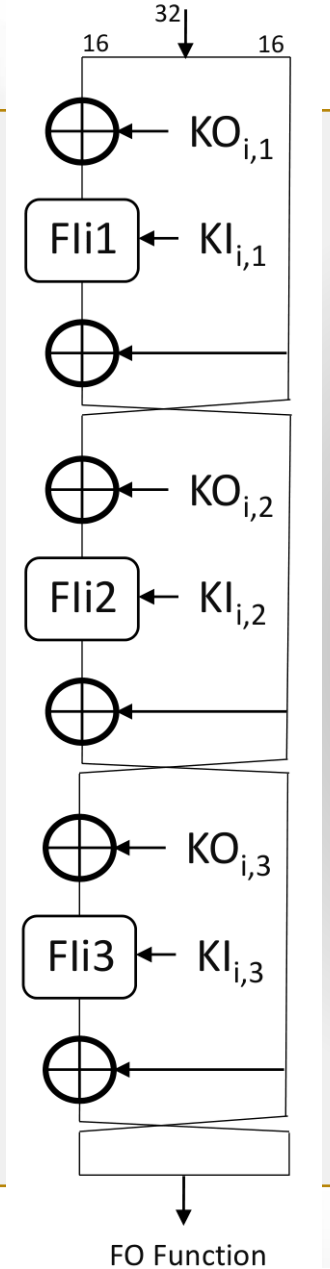




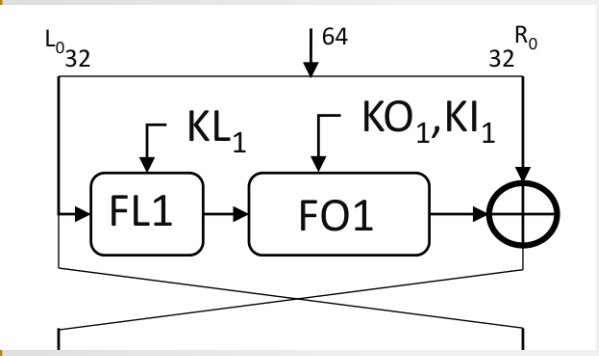
FL Function

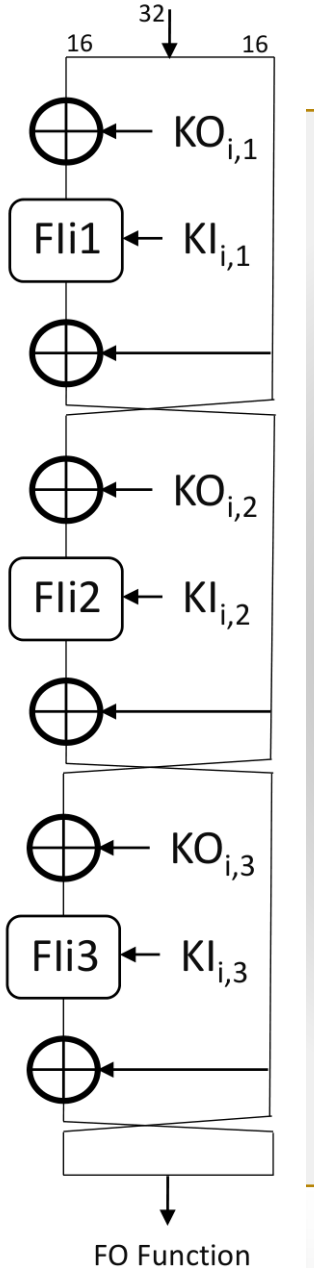
Lesson 3: KASUMI Block Cipher

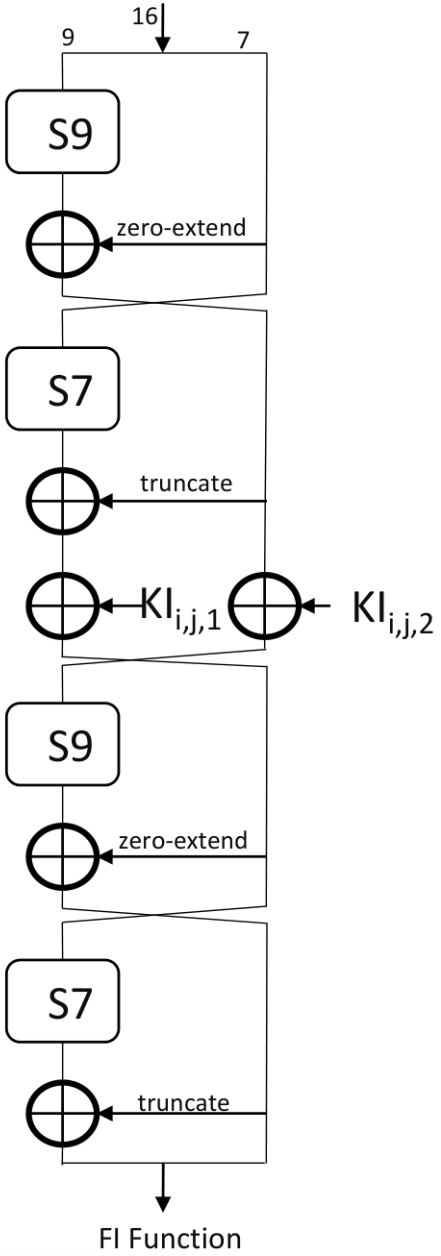




Lesson 3: KASUMI Block Cipher







Lesson 3: KASUMI Block Cipher


```
bit8 S7[128]={
        54,50,62,56,22,34,94,96,38,6,63,93,2,18,123,33,55,113,39,114,21,67,65,12,47,73,46,
        27,25,111,124,81,53,9,121,79,52,60,58,48,101,127,40,120,104,70,71,43,20,122,72,61,
        23,109,13,100,77,1,16,7,82,10,105,98,117,116,76,11,89,106,0,125,118,99,86,69,30,
        57,126,87,112,51,17,5,95,14,90,84,91,8,35,103,32,97,28,66,102,31,26,45,75,4,85,92,
        37,74,80,49,68,29,115,44,64,107,108,24,110,83,36,78,42,19,15,41,88,119,59,3
};
```

Lesson 3: KASUMI Block Cipher

```
bit16 S9[512]={
        167,239,161,379,391,334,9,338,38,226,48,358,452,385,90,397,183,253,147,331,415,340,51,362,306,500,262,
        82,216,159,356,177,175,241,489,37,206,17,0,333,44,254,378,58,143,220,81,400,95,3,315,245,54,235,218,405,
        472,264,172,494,371,290,399,76,165,197,395,121,257,480,423,212,240,28,462,176,406,507,288,223,501,407,
        249,265,89,186,221,428,164,74,440,196,458,421,350,163,232,158,134,354,13,250,491,142,191,69,193,425,152,
        227,366,135,344,300,276,242,437,320,113,278,11,243,87,317,36,93,496,27,487,446,482,41,68,156,457,131,326,
        403,339,20,39,115,442,124,475,384,508,53,112,170,479,151,126,169,73,268,279,321,168,364,363,292,46,499,393,
        327,324,24,456,267,157,460,488,426,309,229,439,506,208,271,349,401,434,236,16,209,359,52,56,120,199,277,
        465,416,252,287,246,6,83,305,420,345,153,502,65,61,244,282,173,222,418,67,386,368,261,101,476,291,195,430,
        49,79,166,330,280,383,373,128,382,408,155,495,367,388,274,107,459,417,62,454,132,225,203,316,234,14,301,91,
        503,286,424,211,347,307,140,374,35,103,125,427,19,214,453,146,498,314,444,230,256,329,198,285,50,116,78,410,
        10,205,510,171,231,45,139,467,29,86,505,32,72,26,342,150,313,490,431,238,411,325,149,473,40,119,174,355,185,
        233,389,71,448,273,372,55,110,178,322,12,469,392,369,190,1,109,375,137,181,88,75,308,260,484,98,272,370,275,
        412,111,336,318,4,504,492,259,304,77,337,435,21,357,303,332,483,18,47,85,25,497,474,289,100,269,296,478,270,
        106,31,104,433,84,414,486,394,96,99,154,511,148,413,361,409,255,162,215,302,201,266,351,343,144,441,365,108,
        298,251,34,182,509,138,210,335,133,311,352,328,141,396,346,123,319,450,281,429,228,443,481,92,404,485,422,
        248,297,23,213,130,466,22,217,283,70,294,360,419,127,312,377,7,468,194,2,117,295,463,258,224,447,247,187,80,
        398,284,353,105,390,299,471,470,184,57,200,348,63,204,188,33,451,97,30,310,219,94,160,129,493,64,179,263,102,
        189,207,114,402,438,477,387,122,192,42,381,5,145,118,180,449,293,323,136,380,43,66,60,455,341,445,202,432,8,
        237,15,376,436,464,59,461
};
```

Lesson 3: KASUMI Block Cipher

KASUMI Block Cipher

- KASUMI is an encryption standard for 3G communications.
- 2G communications initially used ***A5/1*** stream cipher which uses a 64-bit key.
- 64-bit key is too short and it is susceptible to brute-force attacks.
- Moreover, any ***A5/1*** encryption can be broken in real-time via Time-Memory Trade-off (TMTO) attacks.
- For this reason, a modified version of KASUMI which is called ***A5/3*** is added to 2G encryption standards.
- Although KASUMI supports 128-bit keys, ***A5/3*** and ***GEA-3*** both use a session key K_c of 64 bits as 128-bit $K_c \,||\, K_c$ KASUMI key for GSM and GPRS in order to have backward compatibility.

Next lecture

SPECK Family of Block Ciphers

- How SPECK works
- What are the parameters of this family of block ciphers

EURO 4SEE

Thanks!

Co-funded by
the European Union

EuroHPC
Joint Undertaking

This project has received funding from the European High-Performance Computing Joint Undertaking (JU) under grant agreement No 101191697. The JU receives support from the Digital Europe Programme and Germany, Türkiye, Republic of North Macedonia, Montenegro, Serbia, Bosnia and Herzegovina.