Information Security

2018 Project 1

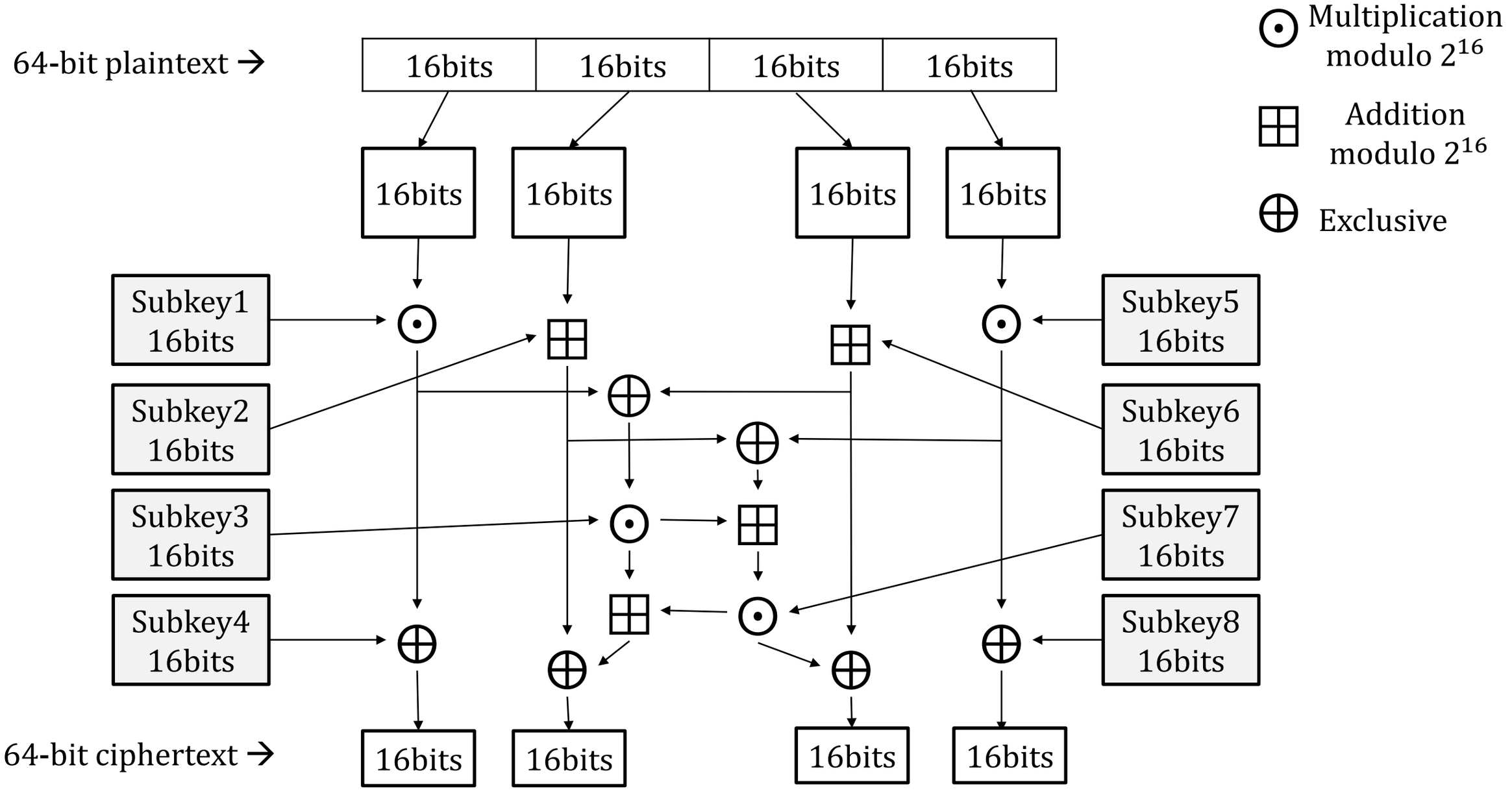
Prof. Junbeom Hur
TA. Changhee Hahn, Hyeong-seob Kim
Department of Computer Science and Engineering
Korea University

Project Overview

- You are given
  - A one-round symmetric-key block cipher
  - Plaintext-ciphertext pairs

- Goal is to find the key
  - Use the pairs to check whether your answer is correct

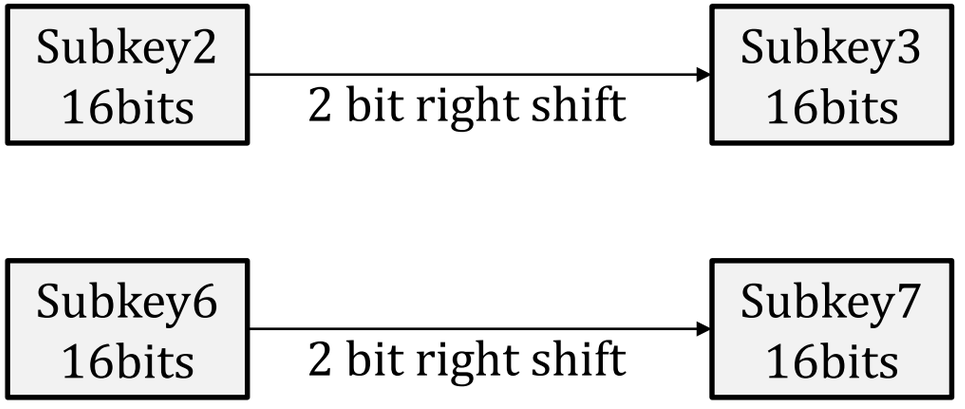
Encryption Workflow



Key Scheduling

- All Subkeys are chosen randomly (except Subkey3 and Subkey7)

- Subkey 3 and 7 are generated from Subkey 2 and 6 by performing bit-wise right shift by 2-bit, respectively



Given Information

- You are given four plaintext-ciphertext pairs
  - (0x6018 E590 FDA5 84A9, 0x3AC5 37CD 9CD1 724E)
  - (0x0A81 ECF1 281E DA5A, 0x192C 94BE C3CA 69ED)
  - (0x2E70 91D3 0AF3 45A0, 0x0B2D A334 CD6F D8F7)
  - (0xF778 A320 1457 4AB1, 0x7BA5 5825 5367 2DF6)

- Find the eight Subkeys

Submission Guideline

1. Source code (e.g., C or Java)
2. Report (e.g., .doc, .hwp, …)
   - Approach to find the key
   - Comment to your source code
     - Explain what functions, variables, etc., you use in your source code do
   - Screen capture of the running program
     - Explain what the captured images mean
   - Answer
     - List the values of eight Subkeys
3. Executable file
   - Project_1.exe, etc.

Grading Criteria

- 0 if at least one is not submitted
- +3 for each Subkey
- +6 for report
- −9 for late submission
- 30 as the maximum score

Submission

- Due date
  - 2018. Nov. 2, 23:59

- Upload into Blackboard