# Revised CHAM

IT융합공학부 권혁동

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB
https://crypto.modoo.at

# Contents



CryptoCraft LAB

# CHAM

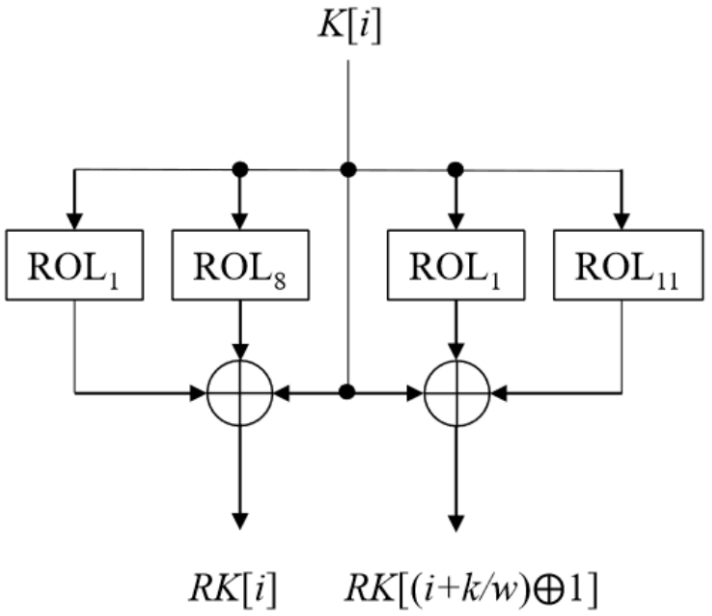
- CHAM은 ICISC'17에서 발표한 **국산 초경량 블록암호**
- ARX 연산
  - Addition
  - Rotation
  - XOR
- Feistel 구조
- 8비트 등의 초소형 **마이크로컨트롤러를 지원**하기 위해 개발

# CHAM

| cipher | $n$ | $k$ | $r$ | $w$ | $k/w$ |
|---|---|---|---|---|---|
| CHAM-64/128 | 64 | 128 | 80 | 16 | 8 |
| CHAM-128/128 | 128 | 128 | 80 | 32 | 4 |
| CHAM-128/256 | 128 | 256 | 96 | 32 | 8 |

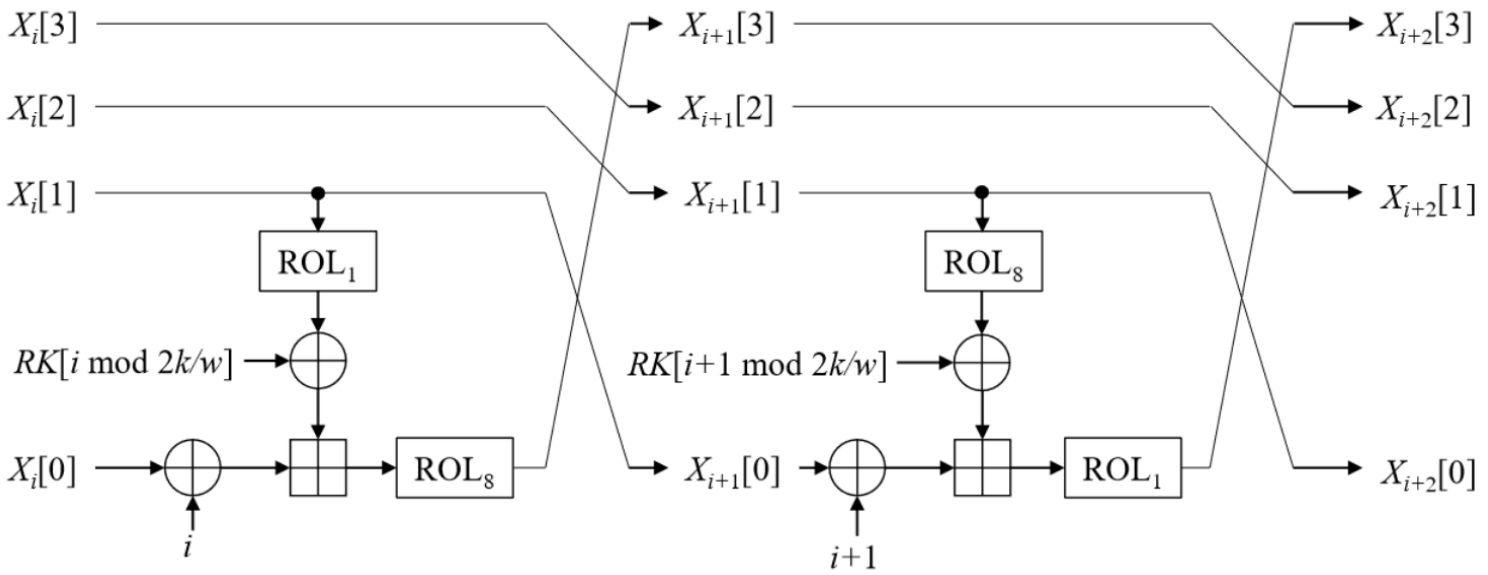
- CHAM은 세 가지 규격을 제공
- n: 블록 크기
- k: 키 크기
- r: 라운드
- w: 워드 크기

# CHAM




$$RK[i] \leftarrow K[i] \oplus \mathrm{ROL}_1(K[i]) \oplus \mathrm{ROL}_8(K[i]),$$
$$RK[(i + k/w) \oplus 1] \leftarrow K[i] \oplus \mathrm{ROL}_1(K[i]) \oplus \mathrm{ROL}_{11}(K[i]),$$

# CHAM




- 라운드 함수를 거치면서 암호화 진행
  - Feistel 구조를 사용하지만 **짝수, 홀수 라운드마다 다른 연산** 수행

$$X_{i+1}[3] \leftarrow \mathrm{ROL}_8((X_i[0] \oplus i) \boxplus (\mathrm{ROL}_1(X_i[1]) \oplus RK[i \bmod 2k/w])),$$
$$X_{i+1}[j] \leftarrow X_i[j+1] \text{ for } 0 \le j \le 2,$$

$$X_{i+1}[3] \leftarrow \mathrm{ROL}_1((X_i[0] \oplus i) \boxplus (\mathrm{ROL}_8(X_i[1]) \oplus RK[i \bmod 2k/w])),$$
$$X_{i+1}[j] \leftarrow X_i[j+1] \text{ for } 0 \le j \le 2,$$

# Revised CHAM

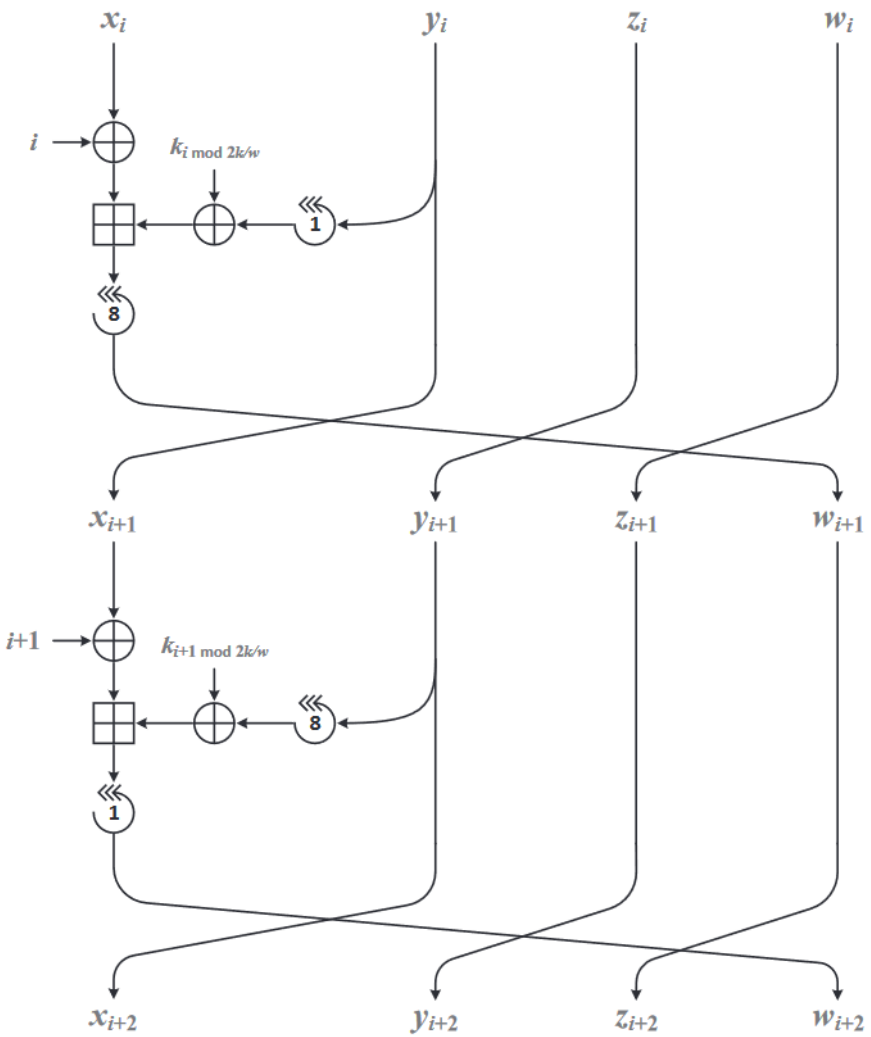
- ICISC'19에서 발표된 **CHAM의 개량형**
- **라운드 수를 바꾼 것**으로 보안성을 향상
  - 충족 가능성 문제
- 구현에 있어서 추가적인 자원 소모 없음

# Revised CHAM

| Cipher | $n$ | $k$ | $w$ | $r_{\text{old}}$ | $r$ |
|---|---|---|---|---|---|
| CHAM-64/128 | 64 | 128 | 16 | 80 | 88 |
| CHAM-128/128 | 128 | 128 | 32 | 80 | 112 |
| CHAM-128/256 | 128 | 256 | 32 | 96 | 120 |

- 기존 CHAM에서 라운드 수를 약간 증가
  - 64/128:  80라운드 -> 88라운드
  - 128/128: 80라운드 -> 112라운드
  - 128/265: 96라운드 -> 120라운드

# Revised CHAM




$$(x_{i+1}, y_{i+1}, z_{i+1}, w_{i+1}) \longleftarrow (y_i, z_i, w_i, ((x_i \oplus i) \boxplus ((y_i \lll \alpha_i) \oplus rk_{i \bmod 2k/w})) \lll \beta_i)$$

where $\alpha_i = 1$ and $\beta_i = 8$ when $i$ is even and $\alpha_i = 8$ and $\beta_i = 1$

- 표현 형식은 다르지만 기존 CHAM과 동일

# Revised CHAM

```
for(int i = 0 ; i < 80 ; i++)
{
    if(i % 2)
    {
        a = 8;
        b = 1;
    }
    else
    {
        a = 1;
        b = 8;
    }

    temp0 = ROL(X1, a);
    temp1 = temp0 ^ RK[i % 16];
    temp2 = X0 ^ i;
    temp3 = temp1 + temp2;
    temp4 = ROL(temp3, b);

    X0 = X1;
    X1 = X2;
    X2 = X3;
    X3 = temp4;
}
```

Original CHAM

```
for(int i = 0 ; i < 88 ; i++)
{
    if(i % 2)
    {
        a = 8;
        b = 1;
    }
    else
    {
        a = 1;
        b = 8;
    }

    temp0 = ROL(X1, a);
    temp1 = temp0 ^ RK[i % 16];
    temp2 = X0 ^ i;
    temp3 = temp1 + temp2;
    temp4 = ROL(temp3, b);

    X0 = X1;
    X1 = X2;
    X2 = X3;
    X3 = temp4;
}
```

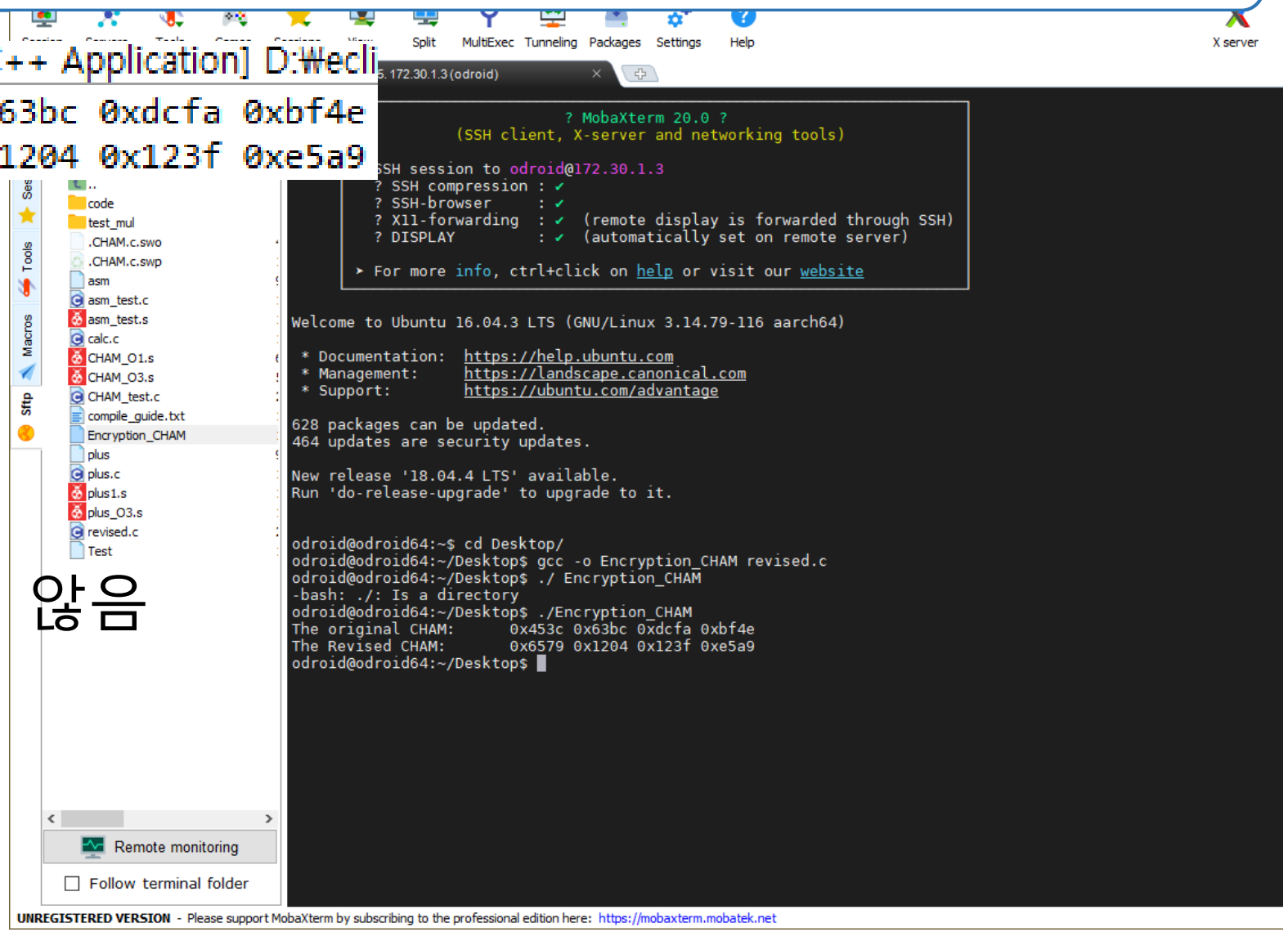
Revised CHAM

- 기존 CHAM과 동일하게 구현
  - 64/128 규격
- 기존 64/128: 80라운드
- **개량 64/128: 88라운드**

# Revised CHAM

```
<terminated> (exit value: 0) cham.exe [C/C++ Application] D:₩ecli
The original CHAM:      0x453c 0x63bc 0xdcfa 0xbf4e
The Revised CHAM:       0x6579 0x1204 0x123f 0xe5a9
```

- 동일한 결과가 반환되지 않음



# Revised CHAM

| $n/k$ | Cipher | Bit-serial Area[1] | Bit-serial Tput.[2] | Round-based Area[1] | Round-based Tput.[2] | Tech. | Ref. |
|---|---|---|---|---|---|---|---|
| 64/128 | Revised CHAM | 665 | 4.5 | 852 | 72.7 | IBM130 | This paper |
| | Original CHAM | 665 | 5.0 | 852 | 80.0 | IBM130 | [22] |
| | Revised CHAM | 728 | 4.5 | 985 | 72.7 | UMC90 | This paper |
| | Revised CHAM | 859 | 4.5 | 1,110 | 72.7 | UMC180 | This paper |
| | SIMON | 944 | 4.2 | 1,403 | 133.3 | IBM130[3] | [34] |
| | SIMON | 958 | 4.2 | 1,417 | 133.3 | IBM130 | [4] |
| | SPECK | 996 | 3.4 | 1,658 | 206.5 | IBM130 | [4] |
| 128/128 | Revised CHAM | 1,057 | 3.6 | 1,499 | 114.3 | IBM130 | This paper |
| | Original CHAM | 1,057 | 5.0 | 1,499 | 160.0 | IBM130 | [22] |
| | Revised CHAM | 1,086 | 3.6 | 1,691 | 114.3 | UMC90 | This paper |
| | SIMON | 1,234 | 2.9 | 2,090 | 182.9 | IBM130 | [4] |
| | SPECK | 1,280 | 3.0 | 2,727 | 376.5 | IBM130 | [4] |
| | Revised CHAM | 1,295 | 3.6 | 1,899 | 114.3 | UMC180 | This paper |
| | LEA | 2,302 | 4.2 | 3,826 | 76.2 | UMC130 | [20] |
| | AES | - | - | 2,400 | 57.0 | UMC180 | [26] |
| 128/256 | Revised CHAM | 1,179 | 3.3 | 1,622 | 106.7 | IBM130 | This paper |
| | Original CHAM | 1,180 | 4.2 | 1,622 | 133.3 | IBM130 | [22] |
| | Revised CHAM | 1,260 | 3.3 | 1,864 | 106.7 | UMC90 | This paper |
| | Revised CHAM | 1,481 | 3.3 | 2,086 | 106.7 | UMC180 | This paper |
| | SIMON | 1,782 | 2.6 | 2,776 | 168.4 | IBM130 | [4] |
| | SPECK | 1,840 | 2.8 | 3,284 | 336.8 | IBM130 | [4] |

- 기존과 GE가 같음
- 라운드 빼고 모두 같음을 명시
- 구현의 잘못된 부분??

We compare the software performance of the revised CHAM and other ciphers via the same method used in the aforementioned study [22]. The implementation method is also identical to that in the earlier work [22] except for the numbers of rounds.