CHAM 최적화 구현

송민호

유튜브 주소: https://youtu.be/nPxArCx1gHU

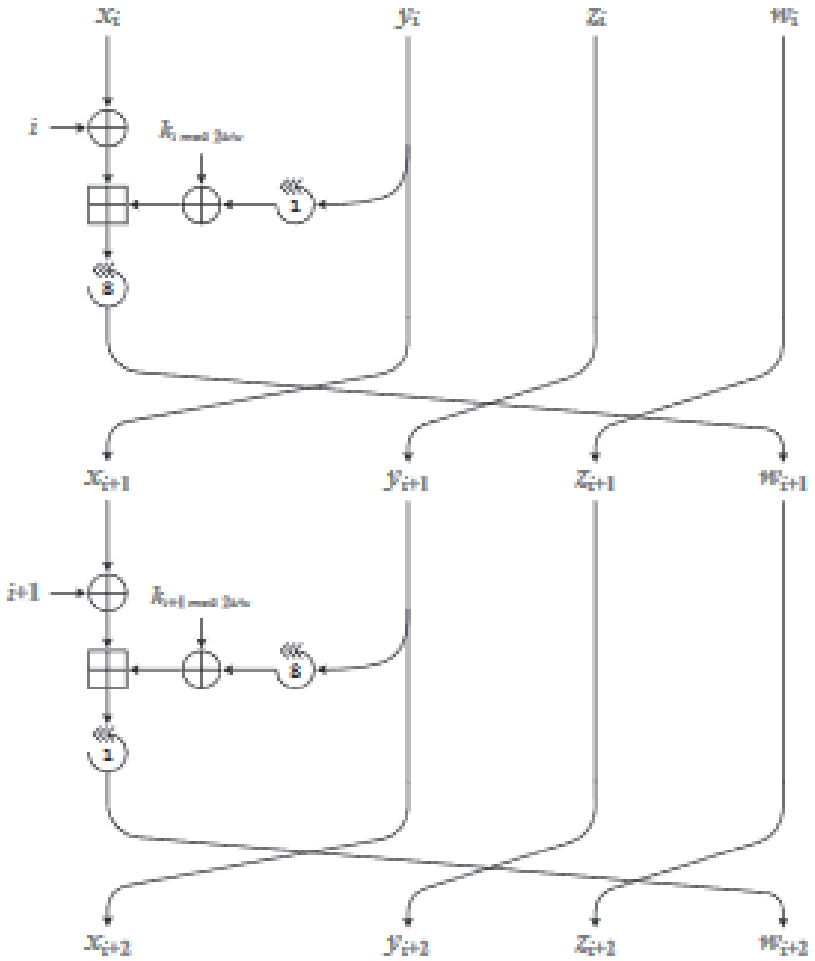
한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

CHAM

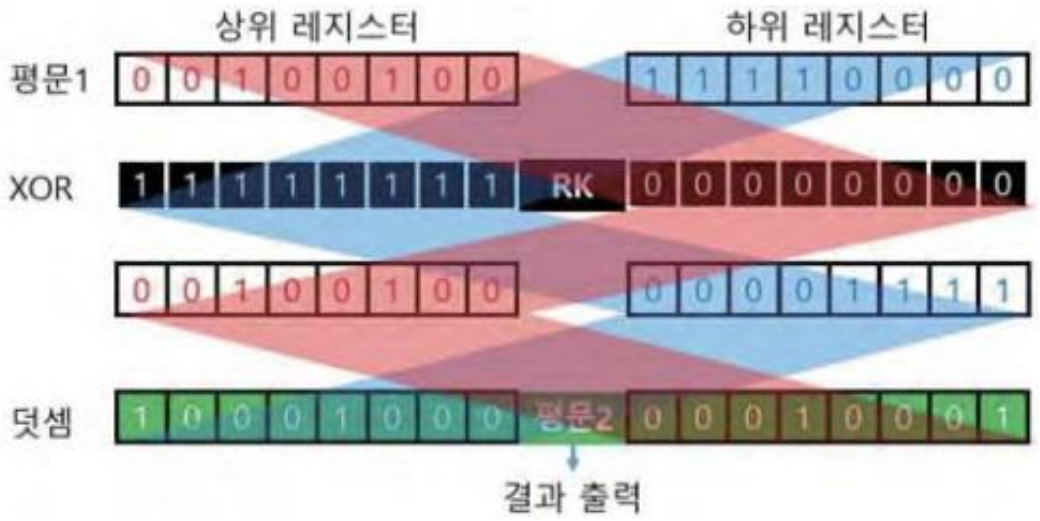
암호화

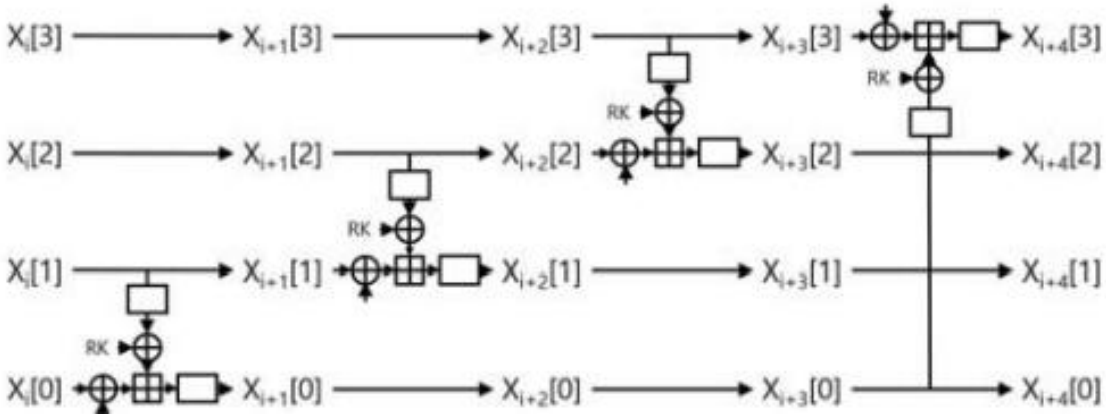
```
for (size_t round = 0; round < CHAM_64_128_ROUNDS; round += 8) {
    blk[0] = rol16((blk[0] ^ (rc++)) + (rol16(blk[1], 1) ^ rk[0]), 8);
    blk[1] = rol16((blk[1] ^ (rc++)) + (rol16(blk[2], 8) ^ rk[1]), 1);
    blk[2] = rol16((blk[2] ^ (rc++)) + (rol16(blk[3], 1) ^ rk[2]), 8);
    blk[3] = rol16((blk[3] ^ (rc++)) + (rol16(blk[0], 8) ^ rk[3]), 1);

    blk[0] = rol16((blk[0] ^ (rc++)) + (rol16(blk[1], 1) ^ rk[4]), 8);
    blk[1] = rol16((blk[1] ^ (rc++)) + (rol16(blk[2], 8) ^ rk[5]), 1);
    blk[2] = rol16((blk[2] ^ (rc++)) + (rol16(blk[3], 1) ^ rk[6]), 8);
    blk[3] = rol16((blk[3] ^ (rc++)) + (rol16(blk[0], 8) ^ rk[7]), 1);
}
```



CHAM

최적화





CHAM

복호화

```
for (size_t round = 0; round < CHAM_64_128_ROUNDS; round += 8) {
     blk[3] = (ror16(blk[3], 1) - (rol16(blk[0], 8) ^ rk[7])) ^ (--rc);
     blk[2] = (ror16(blk[2], 8) - (rol16(blk[3], 1) ^ rk[6])) ^ (--rc);
     blk[1] = (ror16(blk[1], 1) - (rol16(blk[2], 8) ^ rk[5])) ^ (--rc);
     blk[0] = (ror16(blk[0], 8) - (rol16(blk[1], 1) ^ rk[4])) ^ (--rc);

     blk[3] = (ror16(blk[3], 1) - (rol16(blk[0], 8) ^ rk[3])) ^ (--rc);
     blk[2] = (ror16(blk[2], 8) - (rol16(blk[3], 1) ^ rk[2])) ^ (--rc);
     blk[1] = (ror16(blk[1], 1) - (rol16(blk[2], 8) ^ rk[1])) ^ (--rc);
     blk[0] = (ror16(blk[0], 8) - (rol16(blk[1], 1) ^ rk[0])) ^ (--rc);
 }
```

Q & A