CHAM에 대한 CPA공격 및 마스킹 적용 방안

IT융합공학부 안규황

https://youtu.be/m0zwNH65igM

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

Contents

CryptoCraft LAB

1 CHAM 구동 방식

2017년 국가보안기술연구소 소속 팀에 의해 만들어진 초 경량 블록암호

CHAM은 3가지 암호화 모드를 제공

CHAM은 암호화 및 복호화에 있어, ARX구조를 따른다.
→ Addition, Rotation, eXclusie-or만 사용

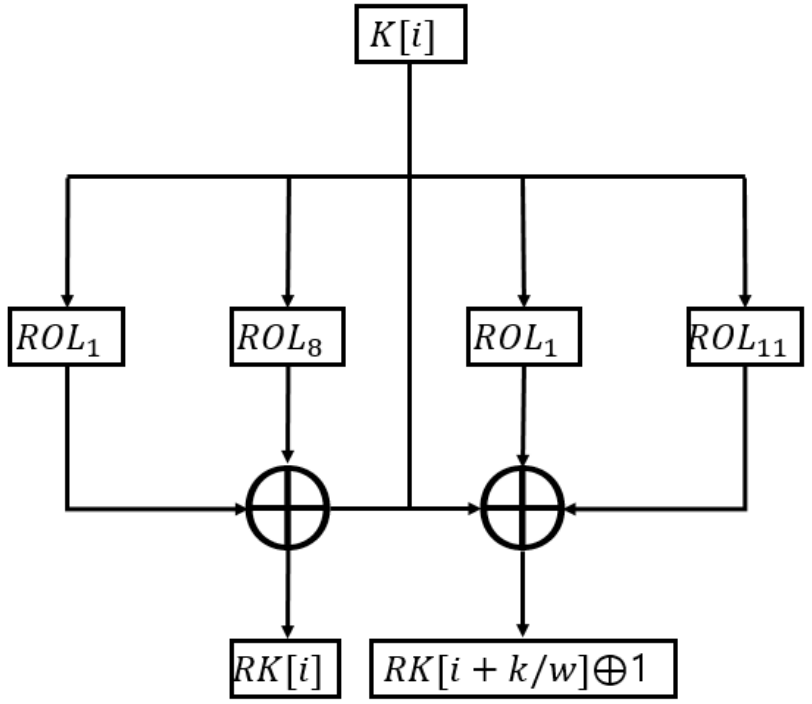
n: 평문 블록의 비트 길이, k: 키의 비트 길이
r: 라운드 횟수, k/w: 분할 된 키 워드의 수

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

B.W. Koo, D. Roh, H. Kim, Y. Jung, D. G. Lee, D. Kwon, "CHAM: A Family of Lightweight Block Ciphers for Resource-Constrained Devices." *International Conference on Information Security and Cryptology*. Springer, Cham, 2017.

1 CHAM 구동 방식

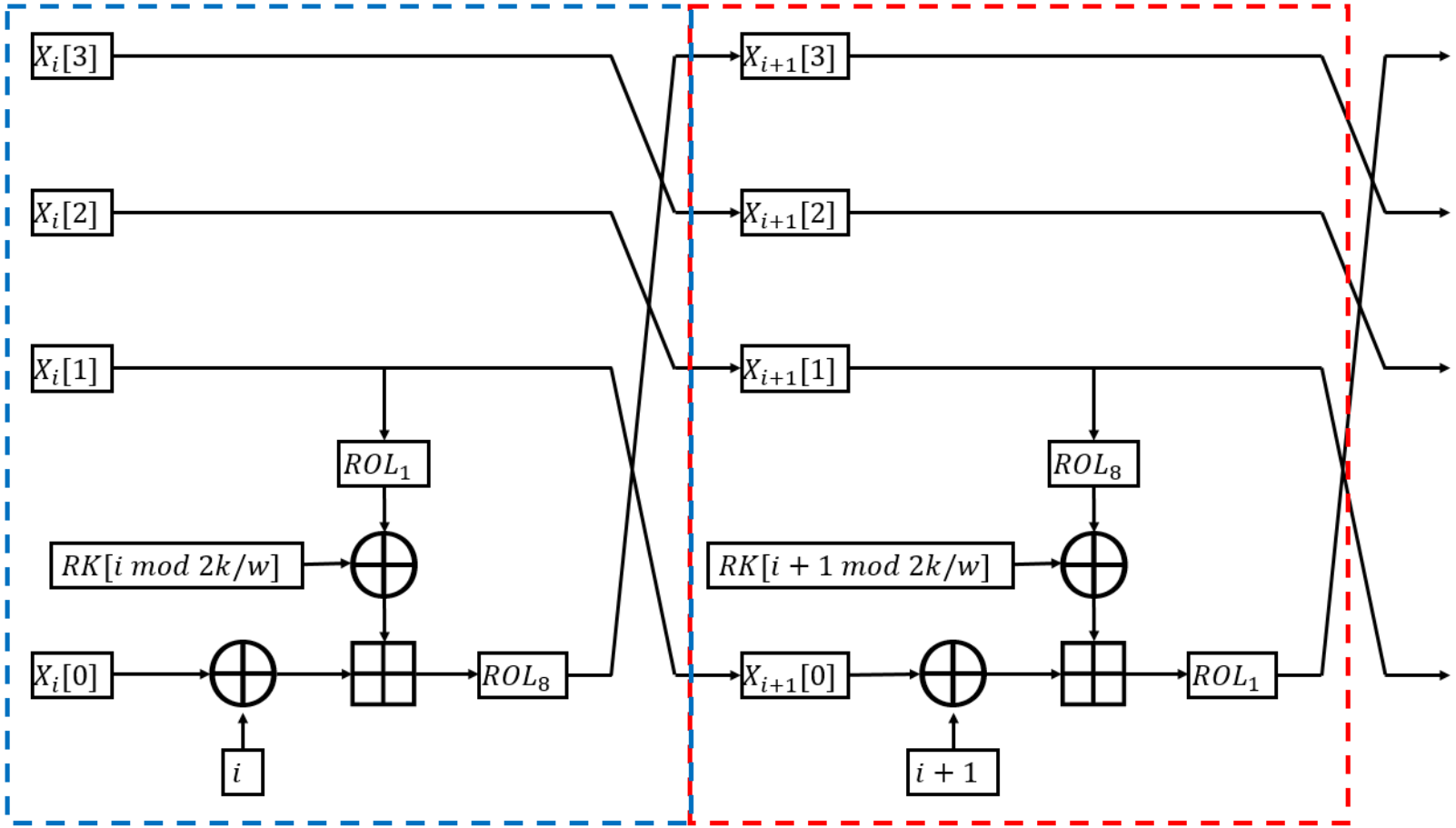
Round key 발생 구조



CryptoCraft LAB

1 CHAM 구동 방식

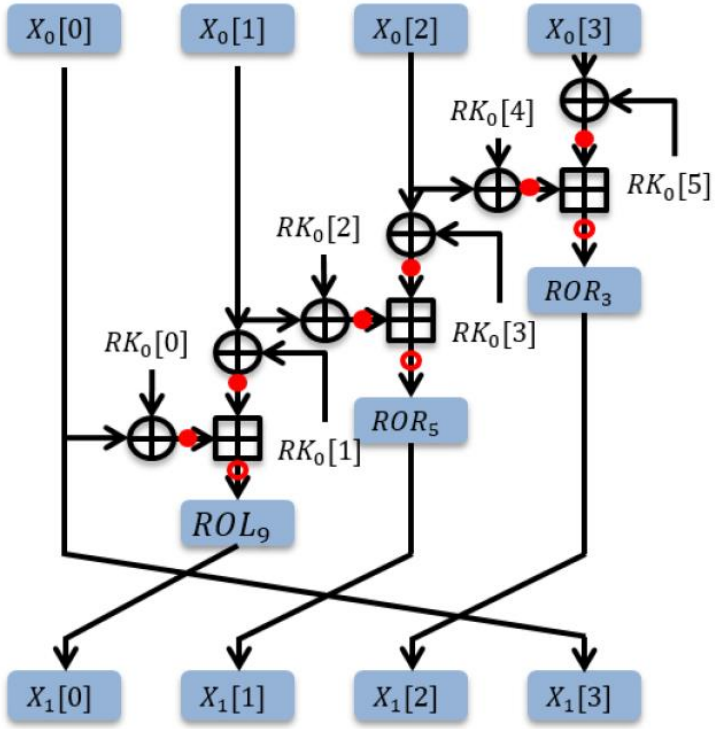
CHAM 라운드 별 동작 방식

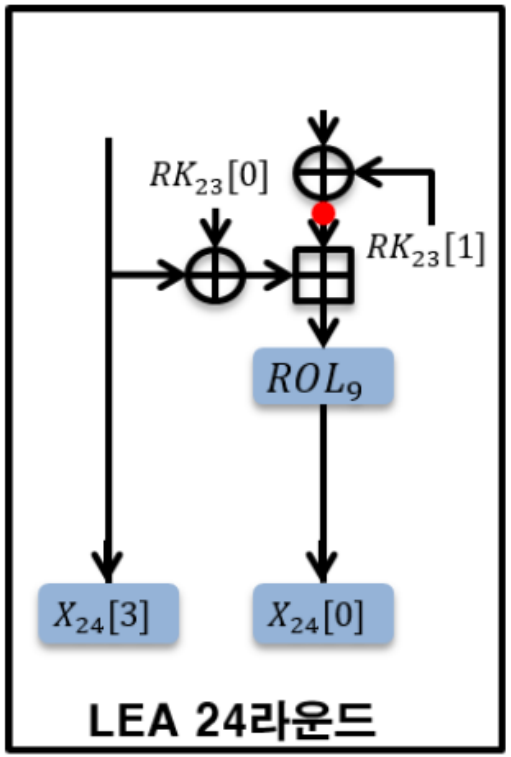


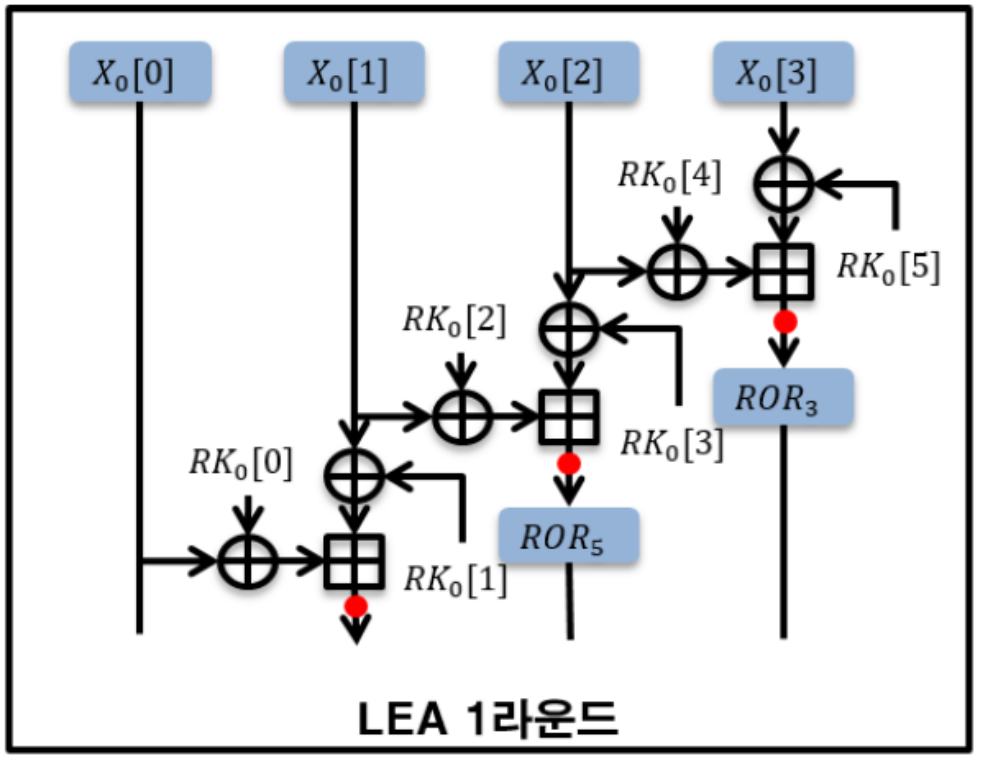
CryptoCraft LAB

2 LEA 공격 방법(평문 + 암호문)

※참조 논문에서 그림 발췌





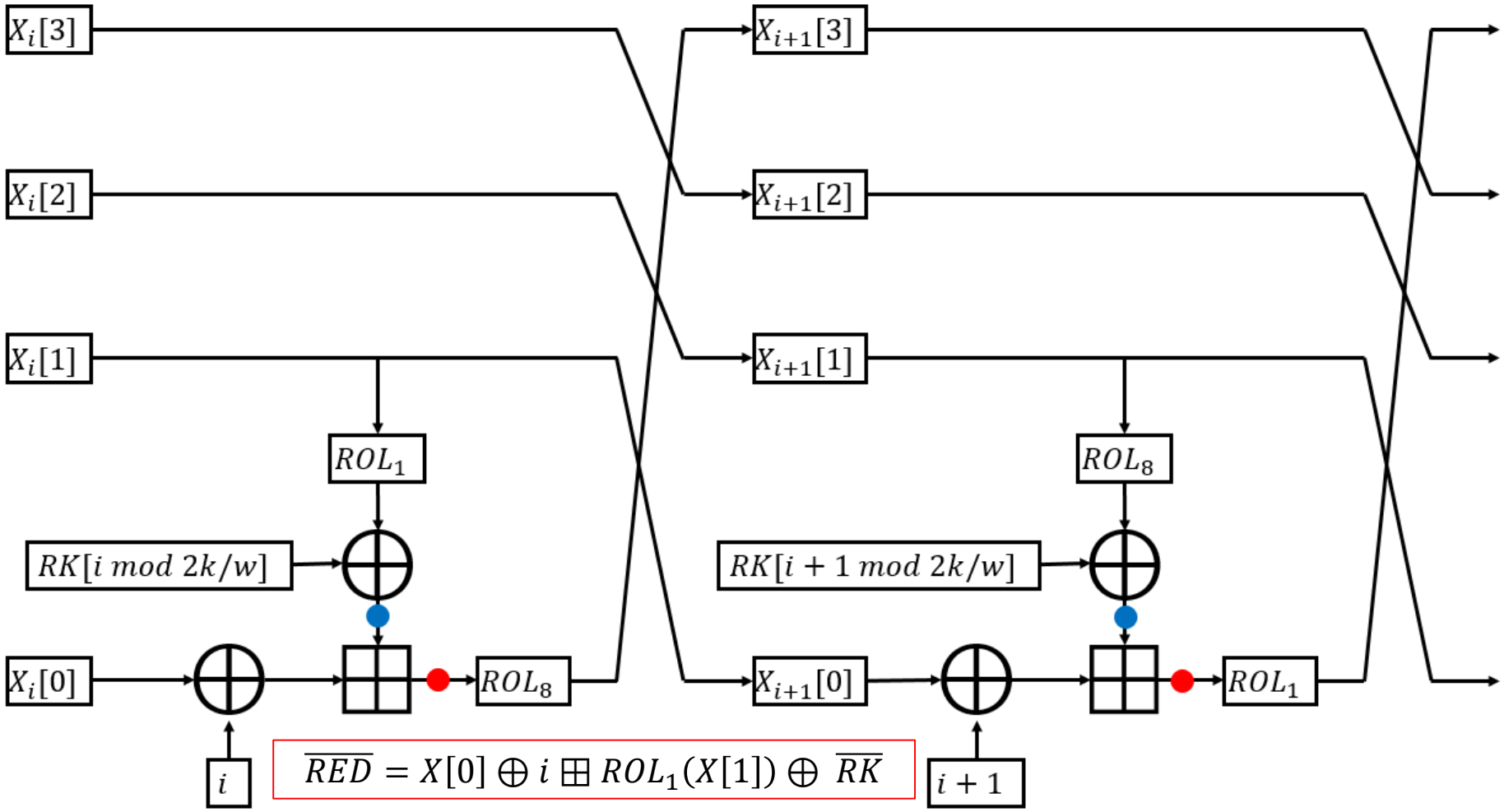


$$ROR(X_{24}[0])_9 = \overline{RED} - X_{24}[3] \oplus R_{23}[0]$$

박진학, 김태종, 안현진, 원유승, 한동국 LEA에 대한 부채널 분석 및 대응방법, 정보보호학회논문지 25(2), 2015.4, 449-456(8 pages)

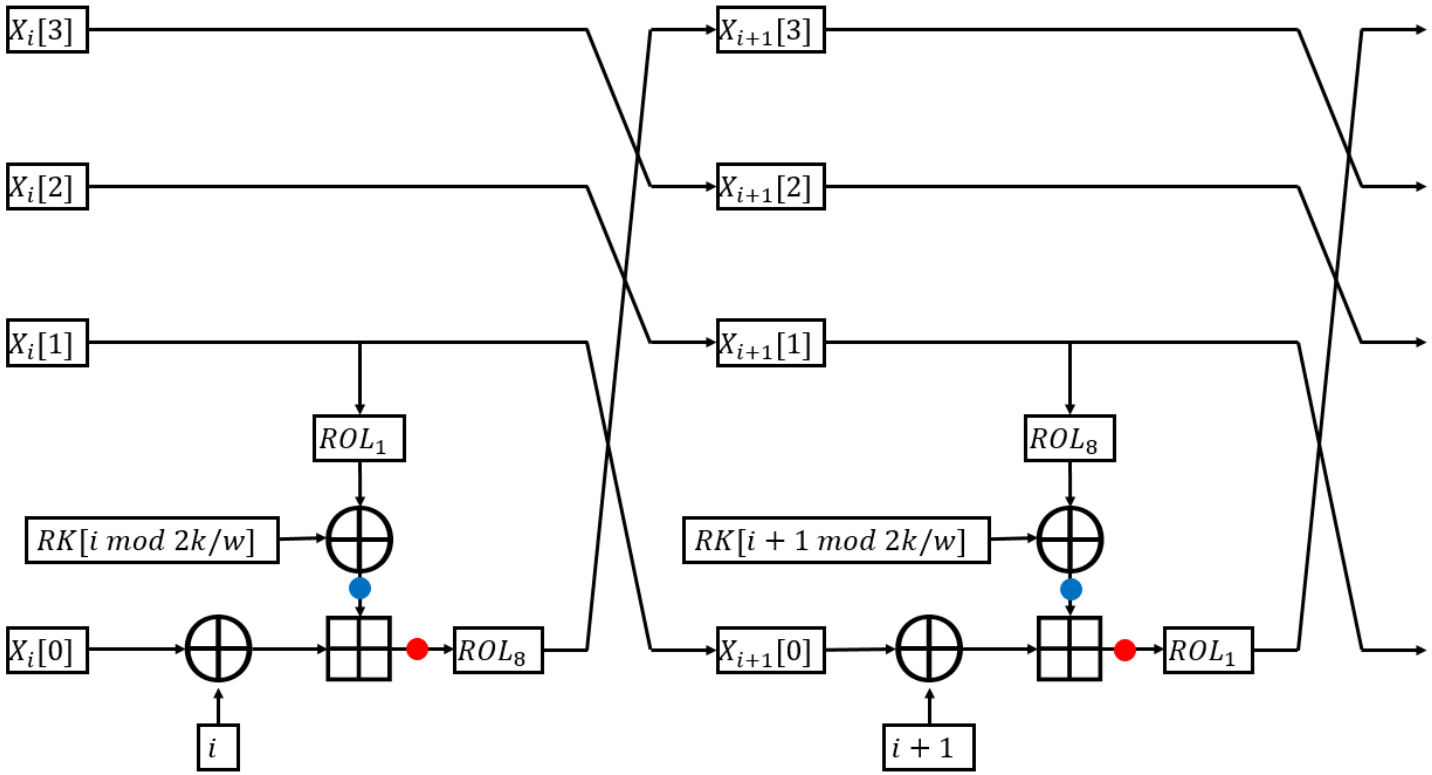
CryptoCraft LAB

3 CHAM 공격 방법(평문)



CryptoCraft LAB

3 CHAM 공격 방법(주의할 점)



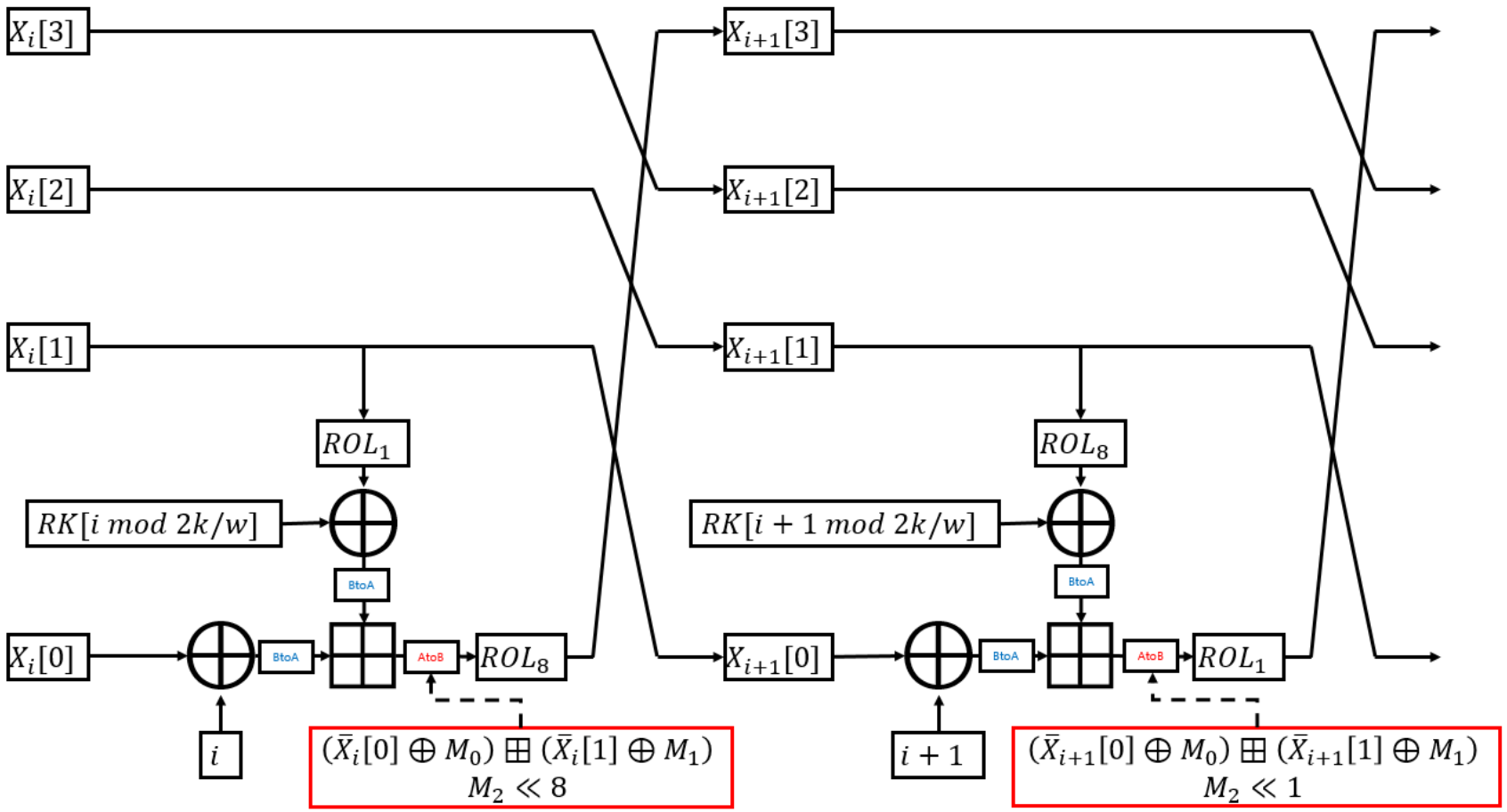
n: 평문 블록의 비트 길이, k: 키의 비트 길이
r: 라운드 횟수, k/w: 분할 된 키 워드의 수

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

CryptoCraft LAB

4 마스킹 기법 적용 방안

BtoA: '⊕' → '⊟'
AtoB: '⊞' → '⊕'



CryptoCraft LAB

Thank You