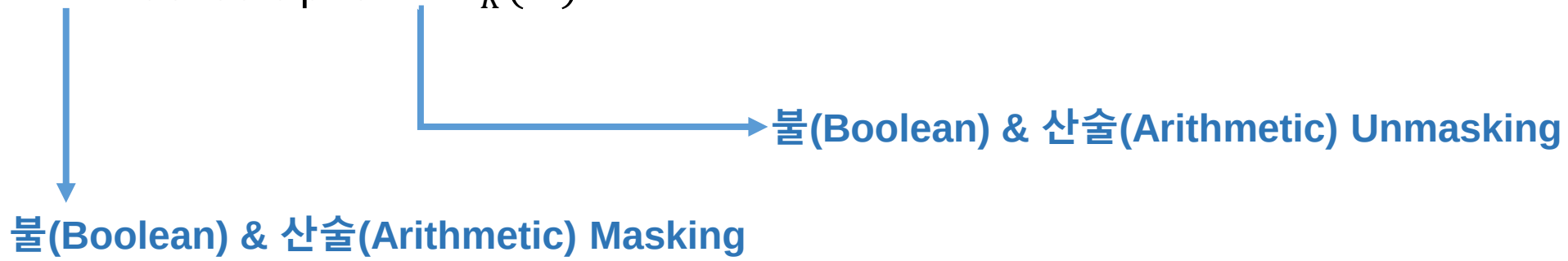
Masked AES

https://youtu.be/2M-8cWiRRJs

마스킹 기법

- 암호 연산 내부의 중간 값을 마스크 난수로 덧씌워 공격자가 획득한 부가 정보가 암호 알고리즘의 중간 중보와 연관을 갖지 않도록 하는 대응 기술
  - m → Original cipher → $E_K(m)$
  - m → Masked cipher → $E_K(m)$



마스킹 기법

- 불(Boolean)-masking : $x' = x \oplus r$
- 산술(Arithmetic)-masking : $A = x - r \bmod 2^k$

x : 마스킹이 적용될 원래 값

r: : 난수

x', A : 난수 r로 마스킹이 적용된 값

k : 처리되는 데이터의 크기

마스킹 기법

- 암호 알고리즘에 사용되는 연산
  부울(Boolean) 연산과 산술(Arithmetic)연산을 번갈아 사용하는 경우 많음

- 산술-부울 & 부울-산술 변환 알고리즘을 통해 중간 값들의 마스킹 변환 필요

- 마스킹 변환 과정에서 원래 데이터 값인 x가 노출 X

x-r → (x-r) + (r xor r) → x xor r

111 – 100 = 3 / (111 – 100) + (100 xor 100) = 3 + 0 / 111 xor 100 = 3

박은수, 오수현, 하재철 (2017). 부채널 공격에 대응하는 마스킹 기반의 블록 암호LEA. 정보보호학회논문지, 27(5),1023-1032

마스킹 기법

- Goubin의 부울-산술 마스킹 변환 기법
  - 부울 마스킹 된 중간 값을 산술 연산을 위해 산술 마스킹 된 중간값으로 변환하는 기법
  - **연산량이 매우 적고** 효율적이기 때문에 많은 알고리즘에서 사용
    - ✓ 5번의 XOR
    - ✓ 2번의 뺄셈
    - ✓ **총 7번 기본 연산**(XOR, AND, OR, 뺄셈, 덧셈, shift 등)

Input : x', r_x	
Output : A	
1. $\Gamma = \gamma$	5. $\Gamma = \Gamma \oplus r_x$
2. $T = x' \oplus \Gamma$	6. $A = x' \oplus \Gamma$
3. $T = T - \Gamma$	7. $A = A - \Gamma$
4. $T = T \oplus x'$	8. $A = A \oplus T$

김창균, 박제훈, 한대완, 이동훈 (2016). LEA에 대한 마스킹 기반 부채널분석 대응기법에 관한 분석. 정보보호학회논문지, 26(6), 1431-1441

마스킹 기법

- Goubin의 산술-불 마스킹 변환 기법
  - 산술 마스킹 된 중간값을 부울 연산을 위해 부울 마스킹 된 중간값으로 변환하는 기법
  - **m비트 연산을 처리 하는 경우**
    - ✓ (2m+4)번의 XOR연산
    - ✓ (2m+1)번의 AND연산
    - ✓ m번의 shift 연산

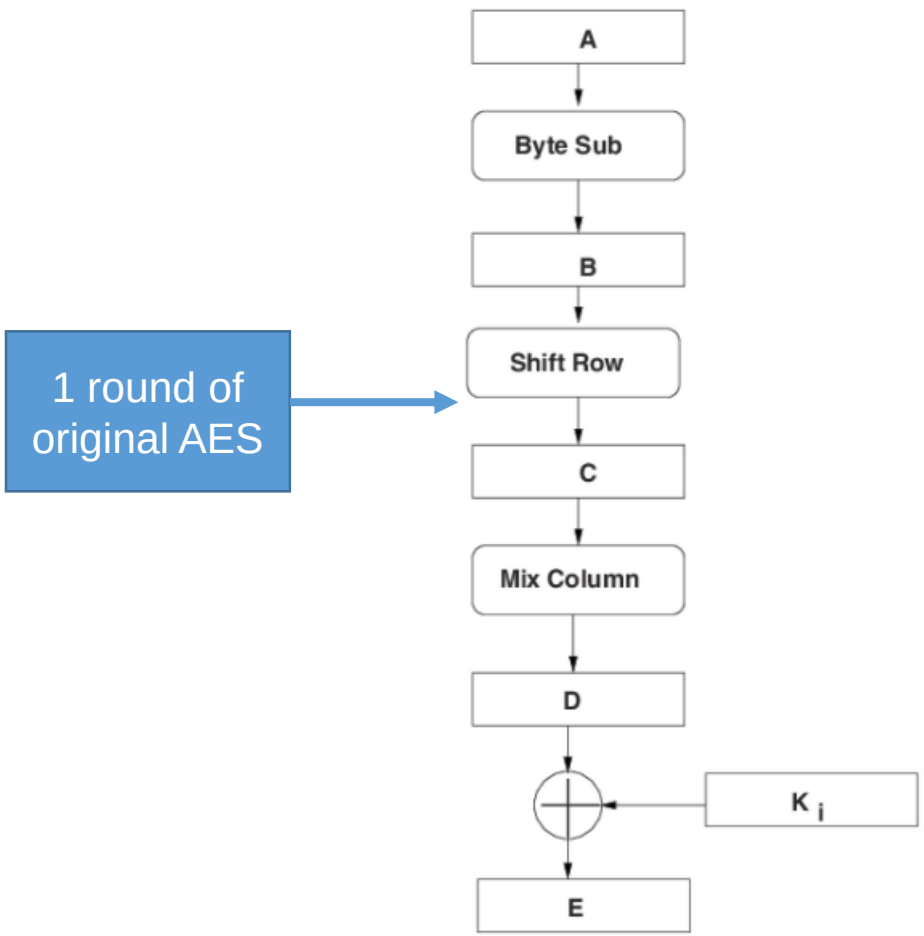
    총 (5m+5)번의 기본 연산 소요

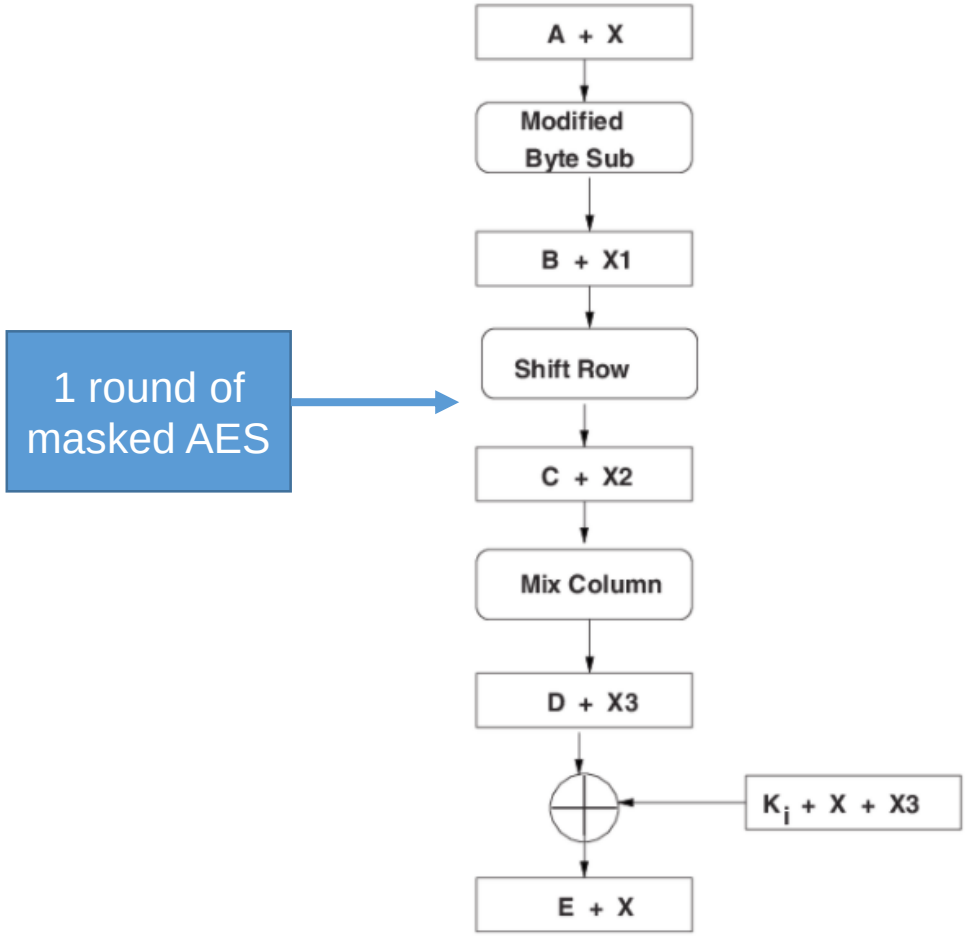
Input : A, r_x
Output : x'

1. $\Gamma = \gamma$	6. $\Gamma = \Gamma \oplus x'$
2. $T = 2\Gamma$	7. $\Gamma = \Gamma \wedge r_x$
3. $x' = \Gamma \oplus r_x$	8. $\Omega = \Omega \oplus \Gamma$
4. $\Omega = \Gamma \wedge x'$	9. $\Gamma = T \wedge A$
5. $x' = T \oplus A$	10. $\Omega = \Omega \oplus \Gamma$
11. for $i = 1$ to $k-1$ do	
11.1 $\Gamma = T \wedge r_x$	11.4 $\Gamma = \Gamma \oplus T$
11.2 $\Gamma = \Gamma \oplus \Omega$	11.5 $T = 2\Gamma$
11.3 $T = T \wedge A$	
12. $x' = x' \oplus T$	

AES의 마스킹 기법

- C. Herbst, E. Oswald, and S. Mangard, “An AES Smart Card Implementation Resistant to Power Analysis Attacks”(2006)





+ → ⊕ 를 의미

AES의 마스킹 기법

- Generate 6 random bytes : $(m, m', m_1, m_2, m_3, m_4)$
- Compute(m_1', m_2', m_3', m_4') = mixcolumn(m_1, m_2, m_3, m_4)
- Modified ByteSub : generation of Masking S-box(ms) using m , m'

<마스킹 s-box 생성 방법>
For x from 0 to 0xff
ms(x xor m) = S(x) xor m'

x → Original cipher → S(x)

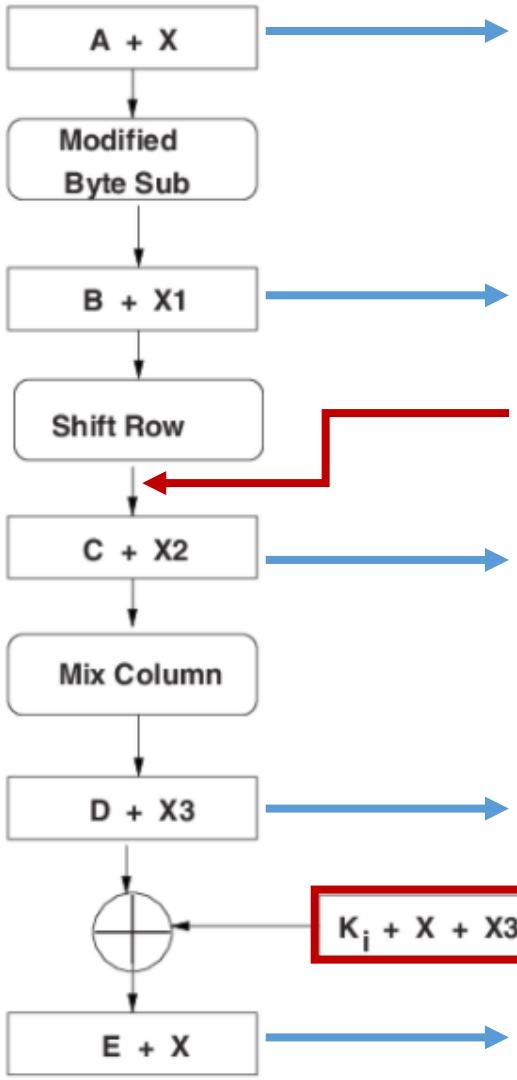
x xor m→ Masked cipher → S(x) xor m'

Algorithm 1. First-order masked AES

Input : 16 바이트의 평문 x ($(x_0x_1...x_{15})_{2^8}$), 마스터키 K, 라운드 수 Nr
Output : 16 바이트의 암호문 y ($(y_0y_1...y_{15})_{2^8}$)

1. 여섯 개의 난수 m, m', m_1, m_2, m_3, m_4 생성
2. 마스킹 S-box 테이블 생성
   For i=0 to 255 do $MS(i \oplus m) = S(i) \oplus m'$;
3. (m_1', m_2', m_3', m_4') ← Mixcolumns(m_1, m_2, m_3, m_4);
4. 마스터키 K와 함께 마스킹된 AES 키 스케줄링을 수행 (각 16 바이트의 라운드키 k_i' $(0 \le i \le Nr)$은 16 바이트의 $(m_1' \oplus m' \| m_2' \oplus m' \| m_3' \oplus m' \| m_4' \oplus m')^4$로 마스킹 됨 [4])
5. $s(=s_0s_1...s_{15})$ ← $(x \oplus (m_1' \| m_2' \| m_3' \| m_4')^4) \oplus k_0'$
6. For j=1 to $Nr-1$
   For i=0 to 15 do $s_i = MS(s_i)$;
   s=Shiftrow(s); s=Mixcolumns(s);
   $s \leftarrow s \oplus k_j'$;
7. For i=0 to 15 do $s_i = MS(s_i)$;
8. s=Shiftrow(s);
   $s \leftarrow s \oplus k_{Nr}'$; $s \leftarrow s \oplus (m_1' \| m_2' \| m_3' \| m_4')^4$;
9. Return $y \leftarrow s$

AES의 마스킹 기법



(a) x= $m \,||\, m \,||\, \ldots. \,||\, m$

+ → ⊕ 를 의미

(b) X1 = $m' \,||m' \,||\, \ldots. \,||\, m'$

(c) X1 xor $((m_1||m_2||m_3||m_4||m_1||\ldots..||\, m_4)$ xor X1)

(d) X2 = $m_1||m_2||m_3||m_4||m_1||\ldots..||\, m_4$

(e) X3 = $m_1'||m_2'||m_3'||\, m_4'||m_1', ||m_4'$

(f) x= $m \,||\, m \,||\, \ldots. \,||\, m$

김희석, 홍석희 박학수,전력 분석에 안전한 AES에 대한 새로운 종류의 충돌쌍 공격, 정보처리학회 논문지, , 2013, vol.2, no.9, 통권 012호 pp. 393-398 (6 pages)

AES 마스킹 기법 취약점

- Masked AES의 1라운드 Masked s-box연산
  - 마스킹 s-box를 하나만 만들었기 때문에 매 라운드에 동일한 x’(난수)값을 사용
  - N차 전력분석(N개의 시점을 조합하여 전력분석 하는 것)에 취약

Q & A