부채널 분석에서의 마스킹 기법 활용 및 방향

김금태, 노종선
서울대학교

kkt1513@snu.ac.kr, jsno@snu.ac.kr

요 약

본 논문은 부채널 분석에 대응 방식 중 하나인 마스킹 기법에 대한 분석과 그 향후 방향에 대해 논한다. 마스킹 기법은 민감한 데이터를 두 개 이상의 조각들로 쪼개, 어느 하나가 노출이 되거나 정보가 새어나가더라도 전체 안전성에 영향을 미치지 않도록 하는 대응기법이다.

Ⅰ. 서 론

암호화 알고리즘이 수학적으로 안전성이 증명되고, 작동상 문제가 없다고 하더라도 실제 세상에서 적용될 경우 부채널 분석에 취약 할 수 있다. 부채널 분석(Side Channel Attack)이란 알고리즘이 동작하는 장비의 전력 소비량, 수행 시간, 전자기파 등의 물리적인 구현 정보를 가지고 비밀키 혹은 민감한 정보를 찾아내는 공격법을 말한다. 부채널 분석은 1996 년 Kocher[1]에 의해 처음 제시된 이후, 많은 발전을 거듭해왔다. 장비로부터 나오는 물리적 정보로부터 민감한 데이터를 알아내는 비침습적 방법 외에도 결함주입 등의 침습적 방법이 있다.

이러한 부채널 분석 방법에 대한 대응기법 중 대표적인 것으로 마스킹(masking) 기법이 있다. 마스킹 기법이란 민감한 데이터를 여러 개의 조각들로 나누어 처리하는 것으로, 중간값이 노출 되더라도 다른 조각들에 대한 정보를 알 수 없도록 만들어 보호하는 방식이다. 마스킹 기법중에는 크게 Arithmetic masking 과 Boolean masking 두 개가 있다.

Boolean masking 은 각 조각들이 민감한 데이터에 random 한 bitstring 을 XOR 하여 만들어진다. 반면, Arithmetic masking 은 random 한 integer 를 더하고, modular reduction 을 취하여 이루어진다. 이 둘은 각각 효율적인 연산에 활용될 수 있다. 예를 들어, Booelan masking 은 symmetric 연산, PRNG 등에서 효율적이고, Arithmetic masking 은 polynomial multiplication, comparison 등에서 효율적이다. 따라서, 전체적인 알고리즘 효율성을 위해서는 이 둘 사이를 바꾸는 방식이 중요한데, A2B(Arithmetic to Boolean)과 B2A(Boolean to Arithmetic) conversion 이 있다. 본 논문에서는 A2B 변환을 중심으로 다룰 예정이다.

Ⅱ. 본론

Arithmetic masking 에서 민감한 데이터 $x = A + R$은 A2B conversion 을 거쳐 $x = B \oplus R$ 로 변환 되는데, 원래 mask 인 A 를 $B = (A + R) \oplus R$ 을 계산함으로써 교체한다. 여기서 문제가 되는 것이 중간값 $A + R$ 이 x 의 값이므로 그대로 노출된다는 것인데, 사전에 table 을 만들어 놓음으로써 그 노출을 방지할 수 있다. 그 table 은 G 로 표시하고 $G[A] = (A + r) \oplus r$ 을 미리 계산하여 사용한다. 그러나 모든 input A 에 대하여 table 을 만들어 놓는 것은 storage 측면에서 효율적이지 않다. 따라서 적당한 k bit 짜리 A_l 을 만들어 $G[A_l] = (A_l + r) \oplus r$ 을 사용하여 효율적인 size 의 table 을 만든다.

먼저, masked 된 input (A, R)을 k bit 단위로 잘라서 (A_l, R_l)을 만든다. 이를 정해진 mask 값 r 에 대하여 (A_l, r)의 mask 로 바꾸고, A2B conversion 을 진행해서 (B_l, r)로 바꾼 뒤, 다시 원래 값 (B_l, R_l)로 remask 하면 conversion 이 진행된다. 효율적인 연산을 위해서 k bit 단위로 잘랐지만 carry 에 대해서 잘 처리해주어야한다. Carry 를 저장하는 table C 는 $C[A_l] = c_{out}(A_l + r) + \gamma$ 로 계산된다. 마찬가지로 중간값 $(A_l + r)$ 을 노출시키지 않기위해 mask γ를 추가하여 계산한다. (A_l, R_l)이 carry 를 넘겨주는 다음 chunk 를 (A_h, R_h)라 하면, 다음 두 step 을 통해 안전하게 다음 A_h를 계산 할 수 있다.

$$A_h \leftarrow A_h + C[A_l]$$
$$A_h \leftarrow A_h - \gamma$$

Ⅲ. 결론

Masking 은 부채널 분석에 대한 대응기법으로

앞으로 발전 방향이 많다. 본 논문에서는 두 개의 share 로만 이루어진 first-order masking 을 설명했지만, 그보다 많은 여러 개의 share 들로 이루어지는 higher-order masking 기법[2]에 대해서도 많은 논문이 나오고 있다.

NIST PQC 표준화 작업[3]에 PKE/KEM track 에 최종 선정된 Crystals-Kyber 에 대한 masking 기법[4]이 주된 연구 방향이 될 것이고, 나아가 더 많은 암호 알고리즘에도 적용이 될 것이다.

또한, Arithmetic 과 Boolean 두 masking 을 변환하는 A2B, B2A conversion 알고리즘에 대한 효율성 개선 및 최적화여부도 좋은 연구 방향이 될 것이다.

ACKNOWLEDGMENT

이 논문은 2021 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2021-0-00400, 저사양 디바이스 대상 고효율 PQC 안전성 및 성능 검증 기술 개발)

참 고 문 헌

[1] Kocher, Paul C. "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems." *Annual International Cryptology Conference*. Springer, Berlin, Heidelberg, 1996.

[2] Ngo, Kalle, et al. "Side-Channel Attacks on Lattice-Based KEMs Are Not Prevented by Higher-Order Masking." *Cryptology ePrint Archive* (2022).

[3] https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022

[4]Bos, Joppe W., et al. "Masking kyber: First-and higher-order implementations." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2021): 173-214.