2025 암호분석경진대회

3번 문제

화이트박스 암호 (White-box cryptography)는 공격자가 소프트웨어의 내부를 완전히 분석할 수 있는 화이트박스 모델 공격자 환경에서 암호 알고리즘 키를 포함한 내부 정보를 보호하면서 암호 연산을 수행할 수 있도록 설계한 암호입니다.

주어진 소스파일(wbcaes128.c)은 Chow et al.의 White-box cryptography and an AES implementation 논문 방식으로 AES-128 암호화를 외부 인코딩 없이 구현한 버전입니다. 즉, 일반 AES-128 암호화와 동일하게 동작합니다. 이를 분석하여128비트 마스터키를 찾아내고, 그 분석 논리 및 과정을 상세히 문서화하시오.

■ 참고

[1] Chow, Stanley, et al. "White-box cryptography and an AES implementation." International Workshop on Selected Areas in Cryptography. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002. https://doi.org/10.1007/3-540-36492-7_17

[2] Muir, James A. "A tutorial on white-box AES." Advances in network analysis and its applications (2012): 209-229. https://doi.org/10.1007/978-3-642-30904-5_9

[3] Bos, Joppe W., et al. "Differential computation analysis: Hiding your white-box designs is not enough." Cryptographic Hardware and Embedded Systems-CHES 2016: 18th International Conference, Santa Barbara, CA, USA, August 17-19, 2016, Proceedings 18. Springer Berlin Heidelberg, 2016. https://doi.org/10.1007/978-3-662-53140-2_11