OCB2 summary

donderdag 19 januari 2023 22:02

Block cipher modes

- Electronic Code Book (ECB): permutes all blocks in the same way. Does not remove structure/patterns in data.
- Counter (CTR): the permutation applied to a block depends on its 'number'. This is vulnerable to manipulation of the contained message (since blocks are treated independent of each other).
- Tweakable block cipher: accepts an additional 'tweak' and is indistinguishable from a random permutation per tweak and per key.
- Offset Codebook Mode 2 (OCB2): a block cipher mode which had a security proof and was broken anyway. The proof placed unrealistic restrictions on the attacker.

AEAD

AE(AD) stands for *Authenticated Encryption (with Associated Data)*. It implies the following:

- Ciphertext does not reveal information about plaintext (except length)
- It is impossible to create a valid ciphertext without knowledge of the key

Both properties hold even when the adversary has access to encryption/decryption oracles and is able to choose nonces.

OCB2 forgery

A forgery for OCB2 can be constructed from an encryption oracle query for (N, A, M), with $M = len(0^n)||m_2$, where $|m_2| = n$, $A = \epsilon$ and N is arbitrary.
Some modifications allow for extending this attack to longer messages. Some more work allows for constructing universal forgeries and recovering plaintexts.