CSE 3400/CSE 5850: Assignment 3

Jonathan Degrange

October 5, 2024

Problem 1: Encryption Modes

1. Rafa's Modified ECB Scheme

Rafa's claim is false. While a random string r is added to each block, r is the same for all blocks of the message. Identical blocks will still produce identical ciphertexts, which exposes patterns in the plaintext and violates CPA security. The scheme remains vulnerable to CPA attacks.

2. Coco's Modification of OFB

Coco's modification breaks CPA security. By outputting an intermediate pad (e.g., pad_1), the encryption leaks part of the internal state. This pad could be used by an attacker to infer information about the plaintext, violating CPA security.

3. Modified CTR Mode (Two-Step Increments)

The modification impacts neither the CPA security nor the correctness of the CTR mode. The counter values are still unique for each block, ensuring that identical plaintext blocks are encrypted to distinct ciphertext blocks. The scheme remains secure and correct.

4. Ciphertext Reordering/Corruption

- (a) **Dropped block (OFB, CBC, CTR)**:
  - OFB and CTR: Dropping c_2 affects only the corresponding plaintext block, as these modes are block-independent.
  - CBC: Dropping c_2 affects both m_2 and m_3, due to block chaining.
- (b) **Reordering (OFB, CBC, CTR)**:
  - OFB and CTR: Reordering the ciphertext breaks decryption, as blocks are decrypted independently.
  - CBC: Reordering disrupts decryption, affecting all subsequent blocks due to the chaining mechanism.

- (c) **Bit flip in c_0 (OFB, CBC, CTR)**:
  - OFB and CBC: c_0 is the initialization vector (IV), so flipping bits in c_0 disrupts decryption of the entire message, since the IV influences all subsequent blocks.
  - CTR: c_0 is the initial counter value. Flipping bits in c_0 will only affect the decryption of the first block, as each block has its own counter value.
- (d) **Left half of c_3 flipped (OFB, CBC, CTR)**:
  - OFB and CTR: Only m_3 is affected by the bit flip.
  - CBC: The error propagates, affecting both m_3 and m_4 due to the chaining.

Problem 2: MAC Constructions

1. MAC with $Fk(G(m))LS2B(m)$

This is not a secure MAC. The last two bits of the message, $LS2B(m)$, are exposed in the tag, revealing information about m. This breaks the integrity of the scheme.

2. MAC with $G(y_0) \oplus G(y_1)$

This is a secure MAC. The construction relies on a secure PRF $F_k(m)$ and PRG G, ensuring that the tag is computationally indistinguishable from random, maintaining the security.

3. MAC with $Fk(m_0)Fk(m_1 \oplus m_2)$

This construction is secure. It combines outputs of a secure PRF applied to different parts of the message, providing integrity without leaking information about m.

4. Variation of CMAC

This construction is secure. The scheme applies CBC-MAC twice, ensuring that each half of the message is independently authenticated. This retains the security properties of the standard CMAC.