CIS4212 Trustworthy Infrastructures
Undergrad Group 17
Henrique Gamonal De Castro & Carlos Pineda
2/15/2026

Homework 3 Extra Credit

Symmetric Authenticated Encryption (AE)

Imagine you are sending a secret package to a friend. Standard encryption is like putting your message in a strong locked box so nobody can read it. However a clever attacker might still be able to smash the box, replace the contents and send it along. Authenticated encryption solves this by not only locking the box but also putting a unique tamper evident wax seal on it. It provides both confidentiality to hide the data and integrity to prove it has not been messed with. Doing these two steps together in one unified mode is much safer and more efficient than trying to do them separately.

One of the most widely used modes is Galois Counter Mode or GCM . GCM works by splitting the task into two parts. First it uses a standard counter mode to lock the data. It assigns a unique number to each block of your message, encrypts that number with your secret key and then combines it with your message. Next it builds the wax seal. It takes the locked data and uses a special type of math called a universal hash function over a binary Galois field to generate a unique fingerprint known as the authentication tag.

Here is the algorithmic description for GCM for a message with n blocks. First we define our inputs which are the Secret Key K the Initialization Vector IV and our Plaintext message blocks P1 through Pn. Step one is to create our counters. We set T1 equal to our IV plus a starting number and then for each following block Ti equals the previous counter Ti minus 1 plus 1. Step two is the encryption. For each message block you encrypt the counter value Ti with your key K and combine it with your plaintext block Pi using an XOR operation to get your ciphertext Ci. We write this as Ci equals E of K and Ti XORed with Pi for i equals 1 to n. Step three is the authentication. You take all those resulting ciphertext blocks and run them through a special Galois Field hash function called GHASH alongside any extra unencrypted data you want to authenticate. The final authentication tag is created by taking the output of that GHASH function and XORing it with the encryption of your very first starting counter.

Fault-Attacks on AES

To understand Differential Fault Analysis you first need to know that the internal structure of AES includes SubBytes, Shift Rows, MixColumns and AddRoundKey. If an attacker manages to inject a tiny physical error into the chip right before the final rounds of this process the MixColumns step takes that single mistake and spreads it out in a very predictable way. By comparing the correct scrambled output with the faulty output researchers can use math to work backward and figure out the secret key which enables efficient Differential Fault Analysis under realistic physical fault injection models like laser voltage or electromagnetic fault injection. The SubBytes step is one of the most critical targets for practical fault attacks because it is the only part of the process that does not follow simple straight line math. This non linear nature makes it the perfect puzzle piece for attackers to exploit when solving for the key.

Acoustic fault injection is a fascinating physical attack. Think of a singer hitting the exact right high note to shatter a crystal glass. Every physical object has a natural vibrating frequency. By blasting a computer chip with highly specific sound waves attackers rely on the underlying physical principles of resonance and mechanical stress. This vibration can influence cryptographic hardware by tricking the system into reading a zero instead of a one. While acoustic attacks are interesting we must consider their feasibility compared to other physical fault injection techniques. It is quite difficult to focus sound waves perfectly enough to cause a specific error without just crashing the whole device.

Power based and electromagnetic fault attacks are much more common. A power attack is like flickering the lights in a room really fast. By briefly dropping the electricity going to the microchip, power glitches and EM pulses can induce transient or permanent faults in cryptographic devices. When we compare these attacks in terms of precision cost accessibility and effectiveness against AES implementations in embedded systems we see clear differences. Power glitches are extremely cheap and accessible making them a very popular choice for attackers. Electromagnetic attacks cost a bit more to set up but they offer higher precision because you can target a microscopic corner of the chip. Both methods are highly effective against basic embedded systems that do not have physical shields or software checks built in to catch the errors.