HW5

Jessica Sines

March 24, 2021

For this homework I chose to recreate the experiments in the provided paper. I managed to implement the Baby-AES cryptosystem, find biases for the S-Box, and verify some equations from page 10. I ran out of time before part (d), generating P-C pairs with a predetermined key and verifying I could find the key using these equations, but I am confident that if I spent further time I would be able to produce results. I did not attempt a differential attack.

For part (a), I implemented the functions bAES_Encrypt and bAES_Decrypt. Both use the key scheduler bAES_keySchedule, an s-box bAES_SBox or its inverse bAES_SBox_Inv, and some finite field algebra (ffAdd, ffMultiply, ffInverse). All these implementations use copious amounts of bit manipulation, much of it poorly written and not extendable to larger block sizes, but it was quite fun to write. I checked programmatically with a wide range of inputs and did not find any plaintext/key combination where the encryption and decryption did not reproduce the plaintext.

For part (b), I found the biases of the s-box using the code from your slides. Nothing particularly exciting, I got the same results.

For part (c), I recreated the same one-round version that the paper describes (bbAES_Encrypt) and created a function checkEQ to verify some of the equations it describes. The function checkEQ generates a random key, then checks it with random plaintexts and their encryptions with that key to check if the equations hold. I included the first 4 equations on page 10 of the paper, as well as one garbage equation with every bit from plaintext, ciphertext, and key to show a probability of .5

I regret not making it through part (d) and if I have free time this weekend I'll be taking a swing at it. I considered doing the other homework option as well to make up for the fact that I didn't finish, but the questions are all things I computed by hand numerous times while implementing them in code to check that my outputs were correct, so I assume you won't mind. Overall this project was very fulfilling and I learned a great deal.

My code is attached (babyaes.py) and the results can be found in the main function starting on line 252. All code besides the high_bias function is my own work.