CS 290T Computational Algebra
Winter Term 2016

Homework Assignment 03:

1. Briefly explain the following terms or concepts:

   a. What information can you learn when you analyze the statistical information of the distances between the PUF responses from the same PUF instance with the same challenge?

   b. What is the method to measure the inter-distance of the responses for a PUF instance?

   c. Suppose that you have two different PUFs. One of them is based on SRAM PUF with $\mu_{\mathcal{P}}^{inter} = 49.59$ and $\sigma_{\mathcal{P}}^{inter} = 0.33$. The other one is based on Latch PUF with $\mu_{\mathcal{P}}^{inter} = 37.01$ and $\sigma_{\mathcal{P}}^{inter} = 1.23$. Which one is closer to ideal PUF by looking at the given statistical information of the inter distances and why?

   d. What is the reason of the noise in arbiter PUF?

   e. What is the way of making PUF responses uniformly random?

2. Suppose that you have a physical uncloneable function (PUF) with intra-distance ≤ 8 and inter-distance $52 \leq D_{\mathcal{P}}^{inter} \leq 73$. The PUF output length is 127-bit. You are supposed to generate a 64-bit secret key.

   a. Select N, K, and t parameters for a BCH code to remove the noise.

   b. What is the value of $m \in \mathrm{GF}(2^m)$ for this BCH code?

3. (Encoding BCH Codes) A BCH $(15, 7, 2)$ code over $\mathrm{GF}(2^4)$ is given where α is a primitive polynomial element in the field and $p(X) = X^4 + X^3 + 1$.

   a. Find the generator polynomial for the code.

   b. Compute the codeword for the message sequence $(0, 1, 1, 1, 0, 0, 0)$ where its polynomial representation is $u(X) = X^3 + X^2 + X$.

Due 5pm Wednesday March 9

Either, email an electronic copy to me (koc@cs.ucsb.edu) or bring a paper copy to the class. Electronic copy of your homework can be in Text or PDF. You could also scan/pdf your handwritten work; however, do not send (low-resolution or small) phone-camera images under any circumstances! Put your name inside the file. Also make the attached file name as your last name, followed by homework number, for example: green-hw03.pdf