NEW TECHNIQUES FOR OBSFUCATING CONJUNCTIONS

Abstract:

A conjunction over a binary alphabet is a boolean function specified by a length n pattern of 0's, 1's and wildcards. On input bit strings of length n, the function outputs 1 if the input matches the pattern at all non wildcard positions. At CRYPTO 2018, Bishop et al. proposed a simple and elegant construction to obfuscate this class of functions by embedding the pattern in the error positions of a noisy Reed-Solomon codeword, and placing the codeword in a group exponent. They prove their scheme achieves a notion of security called "distributional virtual black box" in the generic group model for random conjunctions with at most 0.774n wildcards.  

In this talk, I'll show how to abstract the Bishop et al. scheme to obtain a significantly more efficient "dual" scheme. In the generic group model, our scheme admits an intuitive proof of security and does not place any restrictions on the number of wildcards. Next, I'll describe a simple modification to the construction that avoids encoding in a group exponent and is secure under the Learning Parity with Noise (LPN) assumption. At the heart of our security proof is a reduction from standard LPN to LPN with "structured error."

No prior knowledge of the Bishop et al. paper will be assumed.