Indian Statistical Institute

Applied Statistics Unit

SEMINAR NOTICE

(Pre-Submission Seminar)

Speaker: Anik Raychaudhuri
Title: Indifferentiability and Other Related Security Notions
Date: 05 July, 2023
Time: 16:00 PM
Venue: ASU Seminar Room
Online Platform: Google Meet (meet.google.com/mzv-bwpx-hky)

Abstract: Random oracles are cryptographers' conception of what an 'ideal' hash function should be. Put succinctly, a random oracle is a perfectly random function that you can evaluate quickly. Random functions are beautiful not just because the output is random-looking (of course), but also because they're automatically collision-resistant and pre-image resistant. The problem with random functions is that you just can't evaluate them quickly: you need exponential storage space to keep them, and exponential time to evaluate one. Moreover, we know of nothing in the 'real' world that can approximate them. When cryptographers try to analyze their schemes with random functions, they have to go off into an imaginary fantasy world that we call the 'random oracle model'. In 2004, Maurer, Renner and Holenstein gave us a powerful tool for answering this question. What they showed is that it's always possible to replace functionality A (e.g., a random oracle) with another functionality B (e.g., an ideal compression function) provided that the following rules are satisfied: There exists a way to 'construct' something 'like' A out of B. There exists a way to 'simulate' something 'like' B using A. An attacker who interacts with {constructed A-like thing, B} cannot tell the difference (i.e., can't differentiate it) from {A, simulated B-like thing}. In this thesis We look at indifferentiability and some other related security notions in detail. We look back at the definitions and then look at some constructions which achieve the desired security goals. Specifically:

1. We look at the 3-round tweakable random permutation based cipher introduced by Coron et al. in TCC 2010, and improve their security results by almost two times.
2. We also look at the security of EM-based Key-alternating ciphers in the public permutation model. In this model rather than simulating the adversary has direct access to the underlying primitives also in the ideal world. This model is generally used to analyze keyed-constructions as opposed to unkeyed constructions in indifferentiability. We show that 5-round EM-based key alternating ciphers achieve beyond birthday security (2n/3-bits).
3. Finally, we dive deeper into the notion of crooked-indifferentiability introduced by Russel et al. in CRYPTO 2018. Crooked-indifferentiability is a novel concept which can be used to build secure constructions from subverted primitives. Russel et al. showed that the enveloped xor construction is crooked indifferentiable from a random oracle. We found some mistakes in their proofs and then corrected them. We also develop a new technique to analyze crooked indifferentiability and then use them to to show security of the sponge and the Merkle-Damgard constructions, both of which are easier to implement and less costly in memory uses than the enveloped xor construction.

All are invited to attend.