From: crypto-club@nist.gov on behalf of Sonmez Turan, Meltem
To: CRYPTO-CLUB
Subject: Crypto Reading Club - February 3, 2016
Date: Thursday, January 21, 2016 10:59:03 AM

Hi everyone,

The next crypto reading club meeting is scheduled on February 3, 2016. Our post-quantum cryptography group (Yi-Kai Liu, Ray Perlner, Rene Peralta, Stephen Jordan, Dustin Moody, and possibly Daniel Smith-Tone) is going to present the talk titled "Post-Quantum Cryptography: NIST's plan for the future".

Abstract: In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will be able to break the existing infrastructure of public-key cryptography. The focus of *post-quantum cryptography* is to identify candidate quantum-resistant cryptographic systems that are secure against both quantum and classical computers, as well as the impact that such post-quantum algorithms will have on current protocols and security infrastructures. In this talk, we will explain our current understanding about the status of quantum computing and post-quantum cryptography. We will also talk about NIST's plans to move forward in this space.

Date: Feb. 3, 2016
Time: 10AM-12PM
Place: 222 B341

Regards,
Meltem