From: Moody, Dustin
To: Sonmez Turan, Meltem
Subject: crypto-club talk
Date: Wednesday, January 20, 2016 9:27:00 AM

Meltem,

Let's go with:

Title: 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.

Speakers: Yi-Kai Liu, Ray Perlner, Rene Peralta, Stephen Jordan, Dustin Moody, and possibly Daniel Smith-Tone