From: Chen, Lily
To: Sonmez Turan, Meltem
Cc: Dworkin, Morris J.
Subject: FW: The title and abstract of your talk
Date: Monday, January 11, 2016 1:45:52 PM

Hi, Meltem:

Here is the title and abstract of Jacob’s talk. 222/A318 is the room Sara reserved for us. Somehow I did not ask him for a bio. I will ask him now. You can go ahead to send the announcement for crypto-club. We may later send one to the whole ITL.

Thanks,

Lily

From: Jacob Alperin-Sheriff [mailto:jacobmas@gmail.com]
Sent: Monday, January 11, 2016 1:35 PM
To: Chen, Lily
Subject: Re: The title and abstract of your talk

Title: Public-Key Cryptography from Worst-Case Lattice Problems

Lattice-based cryptography, in particular the Learning With Errors (LWE) problem and its variants, is perhaps the most promising form of post-quantum cryptography. In addition to being resistant against quantum attacks, it enjoys several other useful properties: it can be based on the worst-case hardness of variants of the shortest vector problem, as well as an equivalence of the search and decision versions of the problem. In this talk we survey the reductions in the literature from worst-case lattice problems to LWE, and discuss potential paths for improvement.

On Mon, Jan 11, 2016 at 9:47 AM, Chen, Lily <lily.chen@nist.gov> wrote:
Hi, Jacob:

We have been waiting the title and abstract of your talk to give the announcement. If they are ready, please send to me today.

Thanks,

Lily

--
-Jacob Alperin-Sheriff