| | |
|---|---|
| **From:** | crypto-club-bounces@nist.gov on behalf of Sonmez Turan, Meltem (Assoc) |
| **To:** | CRYPTO-CLUB |
| **Subject:** | [Crypto-club] Reminder: Crypto Reading Club - November 9 |
| **Date:** | Tuesday, November 8, 2016 9:48:27 AM |
| **Attachments:** | ATT00001.txt |

---

I would like to remind you that tomorrow Ray is going to talk about *cost analysis of hash collisions*.
Hope to see you there,
Meltem

---

**From:** crypto-club-bounces@nist.gov [mailto:crypto-club-bounces@nist.gov] **On Behalf Of** Sonmez Turan, Meltem (Assoc)
**Sent:** Tuesday, November 01, 2016 11:47 AM
**To:** CRYPTO-CLUB <CRYPTO-CLUB@nist.gov>
**Subject:** [Crypto-club] Crypto Reading Club - November 9

Hi everyone,

Our next crypto reading club is scheduled on November 9. Ray Perlner is going to lead a discussion about the paper “Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete” authored by Daniel J. Bernstein.

**Abstract:** Current proposals for special-purpose factorization hardware will become obsolete if large quantum computers are built: the number-field sieve scales much more poorly than Shor's quantum algorithm for factorization. Will all special-purpose cryptanalytic hardware become obsolete in a post-quantum world?

A quantum algorithm by Brassard, Hoyer, and Tapp has frequently been claimed to reduce the cost of b-bit hash collisions from 2^{b/2} to 2^{b/3}. This paper analyzes the Brassard-Hoyer-Tapp algorithm and shows that it has fundamentally worse price-performance ratio than the classical van Oorschot-Wiener hash-collision circuits, even under optimistic assumptions regarding the speed of quantum computers.

**Date:** November 9, 2016
**Place:** 222 B341
**Time:** 10:00AM-12:00PM

Regards,
Meltem