From: Liu, Yi-Kai (Fed)
To: (b) (6)
Subject: Fw: review a paper for PQCrypto?
Date: Sunday, December 17, 2017 10:36:08 PM

From: Alperin-Sheriff, Jacob (Fed)
Sent: Thursday, November 30, 2017 10:35 AM
To: Liu, Yi-Kai (Fed)
Subject: Re: review a paper for PQCrypto?

CT-RSA 2017 IIRC

On 11/30/17, 10:34 AM, "Liu, Yi-Kai (Fed)" <yi-kai.liu@nist.gov> wrote:

Thanks very much, that is really helpful! I will take a look... Also, do you recall where the paper was submitted last time?

Cheers,

--Yi-Kai

From: Alperin-Sheriff, Jacob (Fed)
Sent: Wednesday, November 29, 2017 3:45:44 PM
To: Liu, Yi-Kai (Fed)
Subject: Re: review a paper for PQCrypto?

(b) (5)

(b) (5)

(b) (5)

[redacted]

On 11/27/17, 11:59 AM, "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov> wrote:

Sure.

On 11/27/17, 11:51 AM, "Liu, Yi-Kai (Fed)" <yi-kai.liu@nist.gov> wrote:

Hi Jacob,

Sorry to bother you, but would you be willing to review this paper on PQCrypto? It appears to be extending some work you did with Chris Peikert on KDM security for IBE. See below for the abstract. If you can review this, let me know and I'll send you the full paper?

Thanks very much!

--Yi-Kai

= = = = =

Title: Key Dependent Message Security for Identity-Based Encryption, Revisited

Authors: Rui Zhang and Yang Tao

Affiliations: State Key Laboratory of Information Security (SKLOIS), Institute of Information Engineering (IIE), Chinese Academy of Sciences (CAS), School of Cyber Security, University of Chinese Academy of Sciences and State Key Laboratory of Information Security (SKLOIS), Institute of Information Engineering (IIE), Chinese Academy of Sciences (CAS), School of Cyber Security, University of Chinese Academy of Sciences

Countries: China and China

Abstract:

In the identity-based encryption system, private secret key ${\sf SK}_{\sf id}$ is essential to the user's information security. Careless key management, e.g. full disk encryption may leak the encryption of the private secret key, which actually causes a problem, namely, key dependent message (KDM) security. In PKC 2012,

Alperin-Sheriff and Peikert \cite{Alperin-SheriffP12} first introduced the KDM security into IBE and proposed a KDM-sID-CPA secure scheme with respect to the user's private secret key. In this paper, we revisit the KDM security in the IBE setting and consider the security in the post-quantum era. We make some optimizations on \cite{Alperin-SheriffP12} in the aspects of efficiency and security respectively. First, as for efficiency, we construct a more efficient KDM-sID-CPA secure \emph{revocable} IBE scheme in the single public/secret key pair setting based on lattices with logarithmic update complexity under the \emph{polynomial} modulus, while the existing scheme of \cite{Alperin-SheriffP12} suffers from linear update complexity and super-polynomial modulus. Second, as for security, we propose an adaptively secure KDM-ID-CPA IBE construction in the multi-key pair setting in the classical random oracle model. However, it is only secure in the single key setting in the quantum random oracle model.

= = = = =