

a conditional proof of security

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-05/5435.html>

From: Bartosz Zoltak (X_at_vmpcffunction.com;))

Date: 05/29/04

Date: Sat, 29 May 2004 18:46:26 +0200

At

<http://www.vmpcffunction.com/public.htm>

I put links to a paper "One-Way IND-CNA Key Setup – a Step Towards Provably Secure Symmetric Encryption". I don't really know how novel, if any at all, the described ideas are, but I enjoyed writing them and I hope some of the people here might like to look and say what they think.

Abstract:

We analyse the consequences of the specific properties of the key-setup phase in symmetric encryption schemes for their security. We find that key-setup routines satisfying IND-CNA and one-wayness allow to construct schemes which are provably secure against key-recovery attacks. We propose a specific cryptosystem for which we show that the key-setup routine ensures a significant increase in the security of the scheme regardless of the possible attacks against the underlying cipher. The paper presents a proof, based on a set of assumptions, that the scheme remains secure even if a successful key-recovery attack against the underlying cipher is found.

Have a nice look/read

(The paper is also available at ePrint.)

Bartosz

--

Bartosz Zoltak

<http://www.vmpcffunction.com>

X@vmpcffunction.com; X=bzoltak