Cryptology ePrint Archive: Report 2013/151

Some Fixes To SSH

Xu ZiJie

Abstract: To against some known attacks to Secure Shell (SSH), I propose some fixes to SSH. The fixes include add a key producer function and revise the MAC.

Category / Keywords: Authenticated Encryption, SSH, CBC

Date: received 13 Mar 2013, last revised 24 Mar 2013

Contact author: xuzijiewz at gmail com