Cryptology ePrint Archive: Report 2011/299

On Authenticated Encryption Using Stream Ciphers Supporting an Initialisation Vector

Palash Sarkar

Abstract: We describe a systematic framework for using a stream cipher supporting an initialisation vector (IV) to perform various tasks of authentication and authenticated encryption. These include message authentication code (MAC), authenticated encryption (AE), authenticated encryption with associated data (AEAD) and deterministic authenticated encryption (DAE) with associated data. Several schemes are presented and rigourously analysed. A major component of the constructions is a keyed hash function having low collision and differential probabilities. Methods are described to efficiently extend such hash functions to take double inputs and more generally multiple inputs. In particular, double-input hash functions are required for the construction of AEAD schemes. An important practical aspect of our work is that a designer can combine off-the-shelf stream ciphers with off-the-shelf hash functions to obtain secure primitives for MAC, AE, AEAD and DAE(AD).

Category / Keywords: secret-key cryptography /

Date: received 6 Jun 2011

Contact author: palash at isical ac in