عنوان مقاله:

JHAE: A Novel Permutation-Based Authenticated Encryption Mode Based on the Hash Mode JH

محل انتشار:

مجله محاسبات و امنیت, دوره 2, شماره 1 (سال: 1394)

تعداد صفحات اصل مقاله: 18

نویسندگان:

Javad Alizadeh - *Information Systems and Security Lab. (ISSL), Electrical Eng. Department, Sharif University of Technology, Tehran*

Mohammad Reza Aref - *Information Systems and Security Lab. (ISSL), Electrical Eng. Department, Sharif University of Technology, Tehran*

Nasour Bagheri - *Electrical Engineering Department, Shahid Rajaee Teacher Training University, Tehran, Iran*

Alireza Rahimi

خلاصه مقاله:

Authenticated encryption (AE) schemes provide both privacy and integrity ofdata. CAESAR is a competition to design and analysis of the AE schemes. AnAE scheme has two components: a mode of operation and a primitive. In thispaper JHAE, a novel authenticated encryption mode, is presented based on theJH (SHA-۳ finalist) hash mode. JHAE is an on-line and single-pass dedicatedAE mode based on permutation that supports optional associated data (AD).It is proved that this mode, based on ideal permutation, achieves privacy andintegrity up to O(۲ n/۲) queries where the length of the used permutation is ۲n.To decrypt, JHAE does not require the inverse of its underlying permutationand therefore saves area space. JHAE has been used by Artemia, one of theCAESAR's first round .candidates

کلمات کلیدی:

Authenticated Encryption, Provable Security, Privacy, Integrity, CAESAR

لینک ثابت مقاله در پایگاه سیویلیکا: