عنوان مقاله:

A Comprehensive Survey on Evaluation of Lightweight Symmetric Ciphers: Hardware and Software Implementation

محل انتشار:

کنفرانس بین المللی مهندسی کامپیوتر و فناوری اطلاعات (سال: 1395)

تعداد صفحات اصل مقاله: 12

نویسندگان:

Jaber Hosseinzadeh - *Data and Communication Security Laboratory (DCSL), Faculty of Engineering, Ferdowsi University of Mashhad, Mashhad, Iran*

Jaber Hosseinzadeh - *Faculty Of Engineering,Azad University Of Urmia,Urmia,Iran*

خلاصه مقاله:

Low-resource devices like wireless sensor networks have some limitations on memory, power and energy. Using common encryption algorithms are not appropriate for these devices due to their hard limitations and leads to a waste of energy and power. Here, lightweight symmetric ciphers have been evaluated in hardware and software implementations. Comprehensive Evaluation of lightweight ciphers in this work is performed based on cost, speed, efficiency and balance criterion. In each of the criteria, evaluation is done based on a specific measure and the best ciphers have been introduced in each. Evaluation in terms of hardware and software implementation indicates the superiority of SPECK and SIMON ciphers. Evaluation in terms of speed in hardware implementation indicates the superiority of Trivium and Grain, and it shows the superiority of MASHA and SPECK in software implementation. Results of the Evaluation in terms of efficiency express the superiority of SIMON and SPECK. The results of these evaluations helps finding ciphers appropriate to the user based on requirements and restrictions. The user sets his desired system and then obtains the system needs; at the final step, based on the type of requirements, the results of .our work help the system to select the appropriate cipher

کلمات کلیدی:

Cost criterion, efficiency criterion, speed criterion, hardware implementation, software implementation

لینک ثابت مقاله در پایگاه سیویلیکا:

https://civilica.com/doc/494039