Analysis of Rabin-p and HIME(R) encryption scheme on IoT platform

ABSTRACT

This paper focuses on the implementation and analysis of the

performance of the Rabin-p encryption scheme on the microprocessor platform. Rabin-p is an asymmetric cryptosystem that comes with simpler cryptographic properties than the Rabin cryptosystem. Rabin-p encryptionhas yet been tested on any IoT platform. The study tries to analyze the Rabin-p behavior instead of the algorithm optimization itself on the IoT platform. The algorithm of Rabin-p tested by utilizing the C-programming and implemented on a microprocessor system namely Raspberry Pi 3 model B. The Raspberry Pi 3 can be a multi-sensor in an IoT environment. The Rabin-p runtime taken to encrypt and decrypt as well as the power consumption is then compared with the performance of another Rabin variant, the HIME(R) encryption scheme. The result shows Rabin-p encryption scheme runtime is faster at 50% and current withdraw less at 1.3% compared to HIME(R).

Keyword: HIME(R); Encryption; IoT; Rabin-p; Rabin; Public key