An Analysis of the AAβ Asymmetric Encryption Scheme on Embedded Devices for IoT Environment

Syed Farid bin Syed Adnan
Universiti Teknologi MARA Shah Alam

Abstract:

AA-Beta (AA_β) asymmetric cryptographic scheme whose algorithm consists of only basic arithmetic operations of addition and subtraction for the encryption processes offers energy-efficient capabilities on low powered devices such as those commonly found in the Internet of Things (IoT).These features resulted in faster runtime compared to the more established RSA asymmetric encryption scheme, making AA_β a potential alternative for IoT security. At the time of this project, AA_β algorithm still exists as a mathematical concept and proven in a mathematical based software. In addition, this research found no known practical implementation of the AA_β algorithm to prove or to validate its efficiency on a real-world computing platform. It is also not known how the algorithm would perform against the widely used RSA on resource-constrained platforms. This research seeks to study the AA_β design philosophy and the specifications of the AA_β asymmetric encryption scheme, develop the AA_β encryption scheme and evaluate the computational speed, power consumption and feasibility of AA_β encryption scheme on an embedded system in the practical domain. The results from the study are being compared to the mathematical simulation, and experimentally, to the RSA. This investigation takes the form of an IoT environment, beginning with an in-depth examination of the AA_β encryption scheme design, and continuing into the development and real-world application of AA_β from its mathematical origin. The experimental analysis focused on the AA_β algorithm's performance on embedded platforms, namely, the Raspberry Pi microcomputer and microcontroller (ARM Cortex-M7) platforms. A feasibility assessment for an AA_β cryptosystem for sensor nodes including a client to server testbed with wireless communications was carried out in the final stage. In this research work, the performance analysis of the AA_β scheme produced remarkable timing improvements for the encryption and decryption of messages when compared to previous trials on a numeric computing environment. The research goes on to compare the energy consumptions for encryption and decryption using the AA_β scheme with similar processes using the Textbook RSA scheme on the aforesaid embedded platforms. The AA_β encryption process demonstrates a significantly lower energy consumption compared to RSA, where as much as three times less energy was used by AA_β when encrypting messages while considerable energy savings were also seen during AA_β message decryption on the Raspberry Pi 2 and ARM Cortex-M7 device.