Implementation and Effectiveness Evaluation of the VeraGreg Scheme on a Low-Cost Microcontroller

Jan Říha
Department of Digital Design,Faculty of Information Technology, Czech Technical University in Prague
Thakurova 9, Praha 6

rihaja11@fit.cvut.cz

Keywords. VeraGreg, homomorphic encryption, microcontroller, Paillier cryptosystem

Abstract

Homomorphic encryption is an effective way of securing data privacy while maintaining the possibility to process the data. The VeraGreg framework, unlike other existing homomorphic cryptosystem allows for verification of computation that was done with the encrypted data.

This work deals with an implementation of the VeraGreg framework and its effectiveness comparison with a naïve scheme based on symmetric encryption. Secure microcontroller CE1302 was chosen as the implementation platform. A new library for multiprecision integer arithmetic was created as well as the first published implementation of Paillier cryptosystem using hardware RSA accelerator.

The VeraGreg framework is 200 times slower compared to the naive scheme and occupies one third more space in the program memory, so it is not a suitable alternative to symmetric cryptosystems. On the other hand, it provides privacy to the user while allowing computations with the encrypted data, and verifying that is has not been manipulated during the computation.

Acknowledgment

I would like to thank to my supervisor Jakub Klemsa, opponent Martin Novotny and grants SGS17/213/OHK3/3T/18 and SGS19/109/OHK3/2T/13