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

FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

VeraGreg I

- privacy X data mining,
- smart home, IoT.
- **VER**ifiable **A**g**GREG**ate,
- additively homomorphic scheme,
- allows verification of operations → first-ever additively homomorphic scheme that allows *verification* of operations.

VeraGreg II

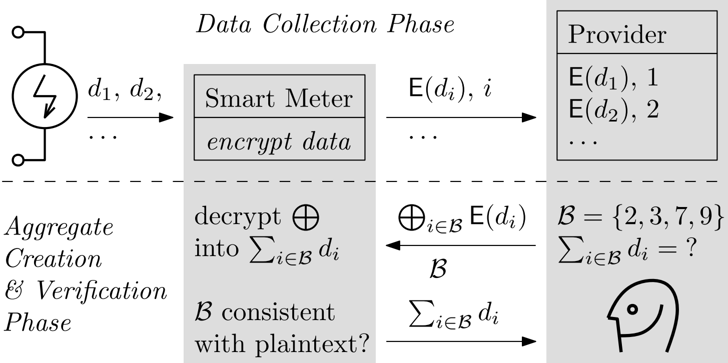


Figure: Example usage of the VeraGreg framework[1]

[1]Klemsa, J.; Kencl, L.; et al. VeraGreg: A Framework for Verifiable Privacy-Preserving Data Aggregation. In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Commu- nications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2018, ISSN 2324-9013, pp. 1820– 1825

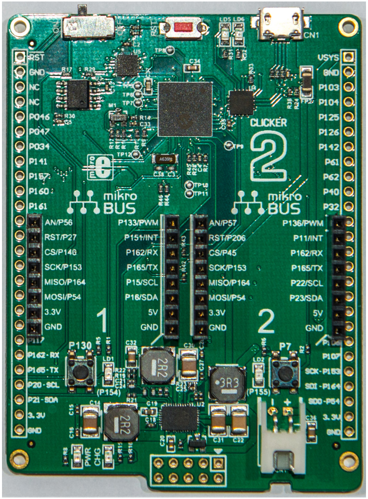
Platform

- Datasheets under NDA,
- inaccessible development tools (boards, compilers).

	HW acc.			Price		NDA
Name	RSA	AES	NVM	Chip	Board	
CEC1302	✓	✓	×	1.93 $	39 $	×
CEC1702	✓	✓	×	1.93 $	39 $	×
MAX32510	✓	✓	✓	NA	561 $	✓

Selected Platform

- Microchip CEC1302,
- based on ARM-M4 core,
- AES,
- RSA,
- TRNG,
- secure boot.
- MikroElektronika Clicker for CEC1302



Instance of the VeraGreg Framework

- Init : creates keys,
- Grant : grants unique ID to each encrypted value,
- E : $c = AHE((\mathrm{SE}(b) \cdot m_1 + d) \cdot m_2)$,
- Add : $a = \bigoplus_{i=1}^{n} n_i \cdot \mathrm{AHE}(p_i)$,
- D:
  1. $\tilde{p} = AHE^{-1}(c)$,
  2. $\tilde{p} \bmod m_2 \neq 0 \implies \bot$,
  3. $\tilde{b}_{\mathrm{SE}} = \tilde{p}/(m_1 m_2)$,
  4. $\tilde{b}_{\mathrm{SE}} \neq \sum_{i=1}^{n} n_i \cdot \mathrm{SE}(b_i) \implies \bot$,
  5. $d = (\tilde{p} \div m_2) \mod m_1$.

AHE–Additively Homomorphic Encryption
SE–Symmetric encryption
$\bot$–Aggregate check failed
$\bigoplus$–Addition in AHE cryptosystem

Cryptographic Primitives

AHE—Paillier Cryptosystem

- Additively homomorphic,
- used in real world (electronic voting systems),
- based on RSA problem.

Encryption

$$c = (1 + m \cdot n)r^n \bmod n^2. \tag{1}$$

where m is a message and r is a random integer such that $0 < r < n$.
Decryption

$$m = \frac{(c^d \bmod n^2) - 1}{n} \cdot d^{-1} \bmod n. \tag{2}$$

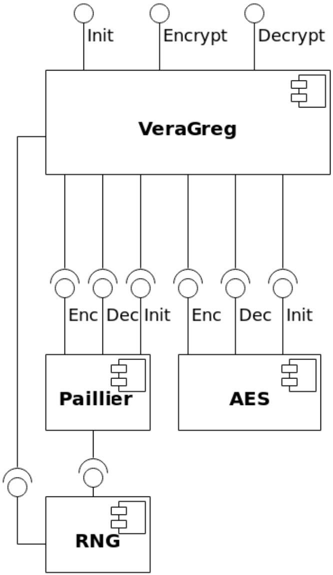
(decryption needs *integer division*)

SE—AES

- Can be accelerated on the selected platform,
- widespread.

System Design

- Modular,
- multiplatform,
- maximal usage of the security features of the selected platform.



Side Channel Attacks Countermeasures

- Hiding in power,
  - MCU peripherals,
- randomly swapped operations during encryption
  - $AHE((\mathrm{SE}(b) \times m_1 + d) \times m_2) = AHE(\mathrm{SE}(b) \times m_1 \times m_2 + d \times m_2)$.

Multiprecision Arithmetic—Problems

- Crypto libraries do not implement certain necessary operations (e.g. *integer division*),
- general libraries are not suitable for crypto,
- constrains defined by the selected platform and tools.

Library *bigi*

- Novel multiprecision ANSI C library,
- implements also "exotic operations" (integer division),
- tailored for microcontrollers

Implemented operations:

- standard arithmetic
  - addition, subtraction, multiplication, *integer division*, exponentiation,
- modular arithmetic
  - multiplication, Montgomery multiplication, (Barett) reduction, inversion (EEA), exponentiation,
- other
  - GCD.

Open source

```
https://github.com/takyrajdr/bigi
```

J. Říha, J. Klemsa, M. Novotný, "Multiprecision ANSI C Library for Implementation of Cryptographic Algorithms on Microcontrollers", 2019 8th Mediterranean Conference on Embedded Computing (MECO)

Paillier Cryptosystem on RSA Hardware

- 1st published implementation of Pailliers cryptosystem using RSA hardware[2],
- due to HW limitations not NIST SP 800-57 compliant.

Variant	Enc	Dec
SW module	2162 ms	1503 ms
HW module	711 ms	1241 ms

$$Enc : c = (1 + m \cdot n) r^n \bmod n^2.$$

$$Dec : m = \frac{(c^d \bmod n^2) - 1}{n} \cdot d^{-1} \bmod n.$$

[2] Říha, Jan. Implementation and Effectiveness Evaluation of the VeraGreg Scheme on a Low-Cost Microcontroller. Master's thesis. Czech Technical University in Prague, Faculty of Information Technology, 2019.

Comparison with AES

Variant	Enc	Dec
AES	5 ms	5 ms
VeraGreg	1032 ms	1504 ms

Variant	Code size	RAM
AES	8032 B	760 B
VeraGreg	15055 B	19553 B

Future Work

- Evaluation of side channel analysis:
  - VeraGreg,
  - Paillier cryptosystem,
- Using microcontroller with 4096 bit RSA accelerator.