A Comparative Study of *Vision* and AES in FHE Setting

Dilara Toprakhisar[1], Tomer Ashur[1,2]
[1] Mathematics and Computer Science, TU Eindhoven, Eindhoven, the Netherlands
[2] imec-COSIC, KU Leuven, Leuven, Belgium

KU LEUVEN

TU/e Technische Universiteit Eindhoven University of Technology

Introduction

The design of traditional block ciphers such as AES calls for efficient software and hardware implementations due to their domain. However, the increasing number of applications that use advanced cryptographic protocols such as multi-party computation (MPC) or zero-knowledge (ZK) proofs shifts the focus of optimization to a different metric: **arithmetic complexity** [1].

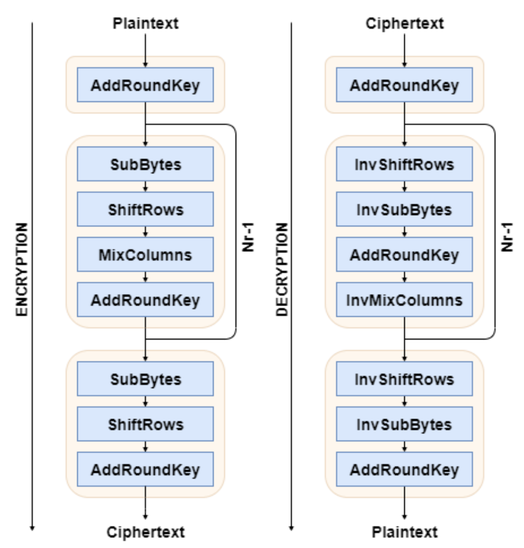


Figure 1. AES encryption and decryption flow

The *Marvellous* design strategy [1]:

- Arithmetization-oriented
- Minimizing algebraic complexity
- Non-procedural computations
- Algebraic attacks

Vision:

- Follows the *Marvellous* design strategy
- Operates over binary fields GF(2^n)
- Two steps in a round, each employs:
  - S-box
  - MDS
  - Key addition

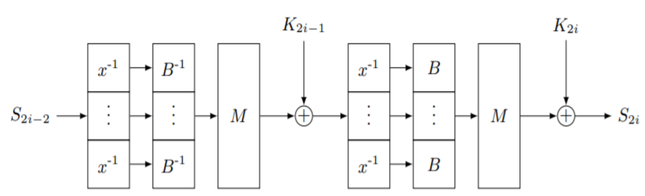
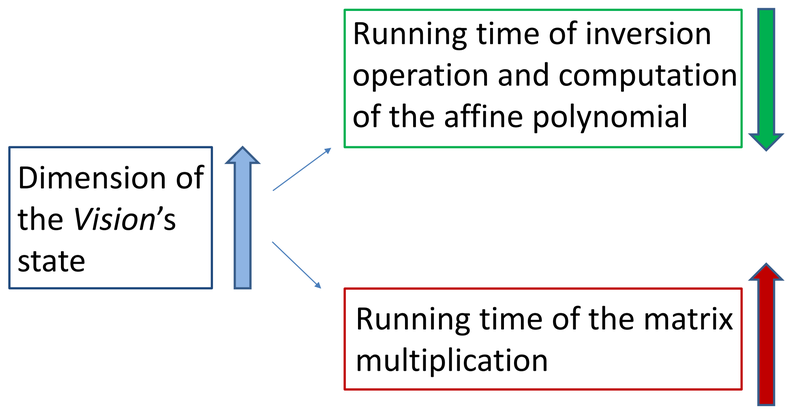


Figure 2. A single round of *Vision* [1]

Motivation: giving an overview of the expected behaviours of arithmetization-oriented ciphers in an FHE setting due to its algebraic nature.

Overview

Experiments are done using existing implementation of a levelled homomorphic encryption that can evaluate the AES circuit based on BGV cryptosystem using HElib [3]. Additionally, we describe a working implementation of a leveled homomorphic encryption that can evaluate a *Vision* circuit using HElib.



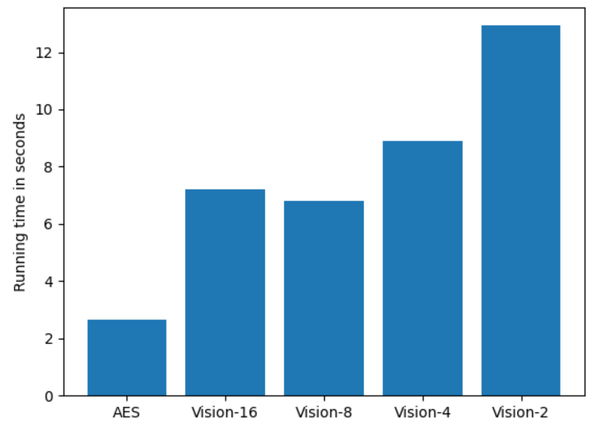


Figure 3. Running time comparison of AES and *Vision* for one round (128 bit state)

Table 1. Running times in seconds of each operation in a *Vision*'s round for variable state elements implemented with toy parameters

State	Inversion	Affine Polynomial-1	Matrix Multiplication	Key Addition	Affine Polynomial-2	One round
GF$(2^8)^{16}$	1.19	0.6006	2.008	0.003	0.19	7.2
GF$(2^{16})^8$	1.79	1.18	0.92	0.003	0.21	6.81
GF$(2^{32})^4$	2.3	3.47	0.393	0.003	0.182	8.89
GF$(2^{64})^2$	2.853	7.106	0.145	0.003	0.193	12.93

Findings and Results

Table 2. Total running times in minutes for AES and *Vision*

Algorithm	State	Parameters	Number of rounds	Total running time
AES	GF$(2^8)^{16}$	Cyclotomic polynomial: 53261 Length of the modulus chain (bits) = 820 Security level (bits) = 136.256	10	1.93
Vision	GF$(2^8)^{16}$	Cyclotomic polynomial: 163455 Length of the modulus chain (bits) = 1550 Security level (bits) = 128.529	10	26.83
Vision	GF$(2^{16})^8$	Cyclotomic polynomial: 148733 Length of the modulus chain (bits) = 2000 Security level (bits) = 158.132	10	37.07
Vision	GF$(2^{32})^4$	Cyclotomic polynomial: 164737 Length of the modulus chain (bits) = 2300 Security level (bits) = 179.373	10	63.3
Vision	GF$(2^{64})^2$	Cyclotomic polynomial: 164737 Length of the modulus chain (bits) = 3150 Security level (bits) = 126	13	76.9

Future Work

- Designing an FHE-friendly version of *Vision* following the *Marvellous* design strategy

Conclusion

- AES performs 90% faster than *Vision* in an FHE setting
- Two bottlenecks for *Vision* as the size of the field elements increase
  - Parameter selection (*i.e.* degree of the ring polynomial)
  - Running times of the inversion operation and the computation of the affine polynomial increase

Contact

Dilara Toprakhisar
Email: d.toprakhisar@student.tue.nl

References

1. Abdelrahaman Aly et al. "Design of Symmetric-Key Primitives for Advanced Cryptographic Protocols". In: *IACR Trans. Symmetric Cryptol*. 2020.3 (2020), pp. 1–45. doi: 10.13154/tosc.v2020.i3.1-45. url: https://doi.org/10.13154/tosc.v2020.i3.1-45.
2. Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. "(Leveled) fully homomorphic encryption without bootstrapping". In: *Innovations in Theoretical Computer Science 2012, Cambridge, MA, USA, January 8-10, 2012*. Ed. by Shafi Goldwasser. ACM, 2012, pp. 309–325. doi: 10.1145/2090236.2090262. url: https://doi.org/10.1145/2090236.2090262.

© Poster Template by Genigraphics® 1.800.790.4001 www.genigraphics.com