A Comparative Study of Vision and AES in FHE Setting

Dilara Toprakhisar
Mathematics and Computer Science
Eindhoven University of Technology
5612 AZ Eindhoven, the Netherlands
d.toprakhisar@student.tue.nl

Tomer Ashur
imec-COSIC
KU Leuven
3001 Leuven, Belgium

Mathematics and Computer Science
Coding Theory and Cryptology
Eindhoven University of Technology
5612 AZ Eindhoven, the Netherlands
t.ashur@tue.nl

Abstract

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.

In this work, we present an understanding of the expected behaviors of arithmetization-oriented ciphers in an FHE setting. We compare AES as a representation of traditional block ciphers and Vision as a representation of arithmetization-oriented ciphers.

1 Introduction

Block ciphers are the building blocks of many encryption schemes and hash functions. Block ciphers such as AES and 3DES are traditionally designed to be efficient in hardware and software implementations as their design goal prioritizes efficiency in addition to security. Therefore, the design of traditional ciphers focuses on running time, gate count, or memory/power consumption [1]. As advanced cryptographic protocols such as multi-party computation (MPC) or zero-knowledge (ZK) proofs are becoming more frequently used in applications, different design constraints are becoming important. The design of block ciphers that are used in such applications is focused on arithmetic complexity. The arithmetic complexity of a cipher is defined by the number of non-linear arithmetic operations and such ciphers are called arithmetization-oriented ciphers. Arithmetization-oriented ciphers deviate from traditional ciphers in terms of relevant attacks and security analysis as the target applications are different.

Advanced cryptographic protocols such as ZK proofs, MPC, and fully homomorphic encryption operate on mathematical objects applying algebraic operations. Converting computations into a set of algebraic operations is called arithmetization.

The Marvellous design strategy defines a set of decisions to be taken when designing arithmetization-oriented ciphers. The design principles are led by security, simplicity, robustness, and efficiency. In the Marvellous design strategy, non-procedural computations, algebraic complexity, and algebraic attacks are taken into account. Minimizing the running time or energy/memory consumption are not the main optimization metrics as in traditional ciphers. In terms of efficiency, optimization metrics are defined specific to the advanced cryptographic protocol. AIR or R1CS constraints are decisive for ZK proofs, number of multiplications and number of communication rounds are decisive for MPC [1]. While statistical attacks are the main focus in the design of traditional block ciphers, arithmetization-oriented ciphers make attacks that manipulates simple polynomials possible.

The motivation of this work is to serve as a first exploration of the expected behaviours of arithmetization-oriented ciphers in an FHE setting. For that aim, this work compares AES as a representation of traditional block ciphers and Vision as a representation of the Marvellous design strategy.

Outline. This paper is organized as follows. Section 2 recalls the basics of AES and Vision. In Section 3, we describe the test environment as well as implementation specific details. In Section 4, we present our findings and results, and in Section 5, a discussion is held about our results followed by a conclusion.

2 Preliminaries

2.1 Advanced Encryption Standard (AES)

AES operates on a 128-bit plaintext as a sequence of operations. These operations form a round and are repeated a certain number of times. The number of rounds in an AES execution depends on the length of the key. In this work, AES-128 is used, which has 10 rounds.

Each round of AES consists of the following four steps:

- SubBytes: a fixed permutation is applied to each byte of the state. This permutation is chosen in such a way that small differences in the input will result in arbitrary differences in the output;
- ShiftRows: row_i is shifted to the left by i positions;
- MixColumns: a linear bijection is applied to the state. The four bytes in each column are used to generate one column of the resulting state;
- AddRoundKey: the round key is added to the state using a bit-wise XOR.

As an exception, prior to the first round, an AddRoundKey operation is applied and in the last round, the MixColumns operation is removed.

2.2 Vision

Vision is designed following the Marvellous design strategy [1] to operate over binary fields with its native field $\mathbb{F}_{2^n}$.Vision's state is an element of $\mathbb{F}_{2^n}^m$ which has m field elements, whereas AES state is an element of $\mathbb{F}_{2^8}^{4x4}$. Vision's round function consists of two steps where each step employs three layers: S-box, linear and key addition. The S-box layer applies an inversion operation to each of the state elements followed by an $\mathbb{F}_2$ linearized affine polynomial. The affine polynomial in the S-box layer of the second step is chosen such that it has a low degree and its inverse has a high degree. The inverse of this affine polynomial is used in the S-box layer of the first step. The linear layer is the multiplication of the state with an MDS matrix.

3 Experimental Setup

For our benchmarks, we use an existing implementation of a leveled homomorphic encryption that can evaluate the AES circuit presented by Gentry et al. [3] built on top of the HElib library. The implementation is based on the BGV cryptosystem [2]. Additionally, we describe a working implementation of a leveled homomorphic encryption that can evaluate a Vision circuit. This implementation is built on top of the HElib library using the same optimizations proposed by Gentry et al. The optimizations include a method for implementing the Brakerski-Gentry-Vaikuntanathan modulus switching transformation on ciphertexts using CRT representation and an alternative Brakerski-Vaikuntanathan key-switching method that does not necessarily decrease the norm of the ciphertext vector. Many of the optimizations aim to decrease the number of conversions between coefficient and evaluation representations of polynomials.

For a fixed state size, we can choose the order of the base field and the dimension of the state for Vision. A vision instance with 16 elements over $\mathbb{F}_{2^8}$ has the same state size as the state of AES. Figure 1 compares the running times of one round of AES and Vision for variable state elements implemented with toy parameters. According to our experiments, when 128 bit state is used, AES performs 60% faster than Vision.

Table 1 shows the running times of each operation of a Vision's state for different state dimensions. As the dimension of the state decreases, the running time of the inversion operation and the computation of the 1st affine polynomial increases.

4 Findings and Results

We reproduced our experiments for the full encryption with the parameters that provides more than 128 bits of security. Due to large parameter sizes, experiments are done in an environment that runs Ubuntu Server 18.04 LTS with 3 TB RAM and 4 x Intel(R) Xeon(R) Gold 6136 CPU @ 3.00GHz.

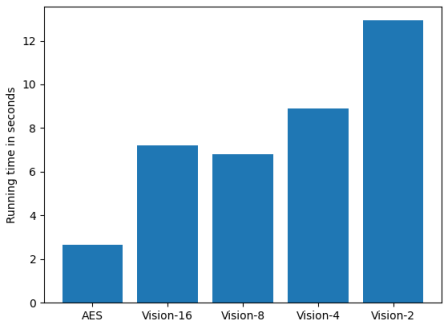

Figure 1: Running time comparison of AES and Vision for one round. Vision-X is a Vision instance with a state consisting of X field elements.

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

State	Inversion	Affine Polynomial-1	Matrix Multiplication	Key Addition	Affine Polynomial-2	Total
Vision-16/$\mathbb{F}_{2^8}^{16}$	1.19	0.6006	2.008	0.0003	0.19	7.2
Vision-8/$\mathbb{F}_{2^{16}}^{8}$	1.79	1.18	0.92	0.003	0.21	6.81
Vision-4/$\mathbb{F}_{2^{32}}^{4}$	2.3	3.47	0.393	0.003	0.182	8.89
Vision-2/$\mathbb{F}_{2^{64}}^{2}$	2.853	7.106	0.145	0.003	0.193	12.93

Table 2 shows the running times of AES and Vision variations for fixed state size of 128 bits. Due to the differences in multiplication levels and the sizes of the field elements, different ring polynomials are used to obtain given security levels.

In these experiments, the two bottlenecks we faced are parameter selection and the running time of the affine polynomial. For Vision, the ring polynomial is chosen as $\Phi_m(X)$ that factors modulo 2 into degree-d polynomials such that *degree of the field element*$|d$ which limits the parameter selection. On the other hand, ring polynomial selection is easier for AES as it factors modulo 2 into degree-d polynomials such that $8|d$. This difference makes it possible for AES to get the same security level as Vision, but with a smaller ring polynomial, therefore creating a gap between running times. The second bottleneck is that the degree of the affine polynomial that is used in the first step of Vision round is linearly increasing as the size of the field elements increase.

5 Conclusion

Our experiments show that in an FHE setting, AES performs 90% faster than Vision when more than 128 bits of security is obtained. In order to make the

Table 2: Total running times in minutes for AES and Vision for a fixed state size of 128 bits

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

gap between the running times of AES and Vision smaller, one can improve the Vision design and try to reduce the number of multiplications. It is important to make sure the improvements does not jeopardize the security of the design.

Acknowledgements Tomer Ashur is an FWO post-doctoral fellow under Grant Number 12ZH420N.

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.

[3] Craig Gentry, Shai Halevi, and Nigel P. Smart. "Homomorphic Evaluation of the AES Circuit". In: *IACR Cryptol. ePrint Arch.* 2012 (2012), p. 99. URL: http://eprint.iacr.org/2012/099.