A Comparative Study of Vision and AES in FHE Setting

Dilara Toprakhisar[1], Mohammad Mahzoun[1], and Tomer Ashur[1,2]

[1]Mathematics and Computer Science
Coding Theory and Cryptology
TU Eindhoven
5612 AZ Eindhoven, the Netherlands
d.toprakhisar@student.tue.nl, {m.mahzoun,t.ashur}@tue.nl

[2]imec-COSIC
KU Leuven
3001 Leuven, Belgium

The design of traditional block ciphers such as AES calls for efficient software and hardware implementations due to their domain. Optimizations to these algorithms focus on running time, gate count, and memory/power consumption [1]. 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. The arithmetic complexity of a cipher is defined by the number of non-linear arithmetic operations and such ciphers are called arithmetization-oriented ciphers.

The Marvellous design strategy defines a set of decisions to be taken when designing arithmetization-oriented ciphers. In the Marvellous design strategy, non-procedural computations, algebraic complexity, and algebraic attacks are taken into consideration whereas traditional cipher design focuses on different aspects [1].

The motivation of this work is to present an understanding of the expected behaviors 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 [1].

Vision is designed following the Marvellous design strategy to operate on binary fields with its native field $\mathbb{F}_{2^n}$. The round function consists of two steps where each step employs three layers: S-box (inversion followed by an affine polynomial), linear (multiplication with a matrix) and subkey injection [1]. Vision's state is an element of $\mathbb{F}_{2^n}^m$ which has m field elements, whereas AES state

is an element of $\mathbb{F}_{2^8}^{16}$.

In this work, we use an existing implementation of a leveled homomorphic encryption that can evaluate the AES circuit presented by Gentry et al. [3] that is 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 [1]. This implementation is built on top of the HElib library using the optimizations proposed by Gentry et al. [3]. The optimizations include a method to implement 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 [3].

For a fixed state size, we have the power to 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. We hypothesized that by decreasing the dimension of the state, the running time of inversion operations and the computation of the affine polynomial would increase, whereas the running time of matrix multiplication would decrease.

Finding and Results. We reproduced our experiments with several state sizes that are larger than 128 bits and $\mathbb{F}_{2^{64}}$ elements for Vision. The running time of AES is linear in the input size, whereas the running time of Vision is sublinear as it has a flexible state size. In these experiments, the two bottlenecks we faced are parameter selection for $\mathbb{F}_{2^{64}}$ and the running time of the affine polynomial for $\mathbb{F}_{2^{64}}$. For Vision, ring polynomial is chosen such that it factors modulo 2 into degree-d polynomials such that $64|d$ 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 with a smaller ring polynomial, therefore creating a gap between running times. The second bottleneck is that the degree of affine polynomial that is used in the first step of Vision round is linearly increasing as the size of the field elements increase. After all this effort, our implementation is still two times slower than AES.

In order to make this gap smaller, one can improve the Vision design and try to reduce the number of multiplication. 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, and Dilara Toprakhisar is a receiver of ALSP scholarship from TU Eindhoven.

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.