COLLABORATION PROPOSAL

FOR THE IMPLEMENTATION OF A SIMPLE AND FULLY HOMOMORPHIC ENCRYPTION SCHEME

Join us in a revolution of the field of computer microprocessors and cloud computing, unlocking untapped mathematical potential that will redefine computing performance across multiple sectors such as Machine Learning, AI and neural network training, Digital Signal Processing, and cryptography, among others. Together, we will be able to develop the next generation of software and hardware-based mathematical encryption schemes to set new standards of privacy, reliability and efficiency in cloud computing.

My mathematical research provides an optimal representation of all mathematical objects and structures [1,2], with the potential to revolutionize computer science and applied mathematics. By leveraging this new mathematical description and developing practical applications, we seek to create value by offering efficient technological solutions to a range of industries. Applications include a general method for time and energy efficient Fully-Homomorphic Encryption (often referred to as the Holy Grail of Cryptography), as well as a new processor architecture with unique capabilities and characteristics that can replace the existing Von-Neumann Architecture with a Computing-In-Memory scheme, which is key in achieving time and energy efficient AI and Neural Network training. Through strategic partnerships and collaborations, we are poised to drive innovation and create a competitive edge in the rapidly evolving technological landscape, countering diminishing returns in computing performance [3,4]. This proposal focuses on Low-Level-Languages and SW based solutions to cryptography. A separate proposal discusses a Computing-In-Memory architecture based on a patent-pending Simple and Linear Fast Adder (SLFA).

REPORT AUTHOR

Juan P. Ramírez

ALLIANCES
Partners / Clients

We look to work with experts, institutions and businesses

DEVELOPMENT

By working with our clients, we are able to provide custom designed and tailor-fitted encryption and computation schemes.

Collaborations

Applications and Integration

TEAM

Sr. Engineers

Research
Math - Physics - CS

INDUSTRY

We are positioned to be a driving froce that will impact almost any sector of science and technology.

Revision of mathematical foundations with efficient operations and other applications.

LEADERSHIP

RESEARCH

Through strategic partnerships and collaborations, we will create a competitive edge.

Middle and Final Customer Satisfaction.

INNOVATION

VALUE

PRODUCTS AND SERVICES

First we focus on a new generation of simple yet powerful HE methods with important applications in cloud computing.

A proposal of new mathematical methods yields results in applied physics, numerical methods, cryptography, data mining, high-performance computing among others.

Globally competitive patents for digital and analog systems.

Mathematically optimized architectures for data science, cryptography, analog and digital devices.

Effective Campaigns

MARKETING AND CUSTOMER EXPERIENCE

THEORETICAL FRAMEWORK

Through a fundamental solution to the problem of numerical representations and their computational complexity, we seek to transform the computing industry. This initiative is based on a major revision of mathematical foundations that allows fast and low-powered homomorphic encryption of mathematical operations. The mathematical framework is given in the paper shown below [1]. This article and other supporting papers are cited in the bibliography, at the end of this proposal.

Canonical Set Theory with Applications from Parallel Matrix Operations and Data Structures to Homomorphic Encryption

Juan Ramírez

July 7, 2023

Jalisco, México
www.binaryprojx.com
jramirez@binaryprojx.com

Abstract

Few questions have resounded through the mind of the mathematician, as much as the simple question of describing the nature of a number. The longstanding consensus is that it does not matter which set theory is used to describe numbers. What matters is that it can be done. It is widely believed that the particular choice of a construction for natural and real numbers is irrelevant for the rest of mathematics. Here, a set theory is proposed as a canonical theory that yields transparent proofs in fundamental areas of mathematics including group theory, discrete mathematics, analysis, data types, and new results tying these areas and addressing Hilbert's 24-th (twenty-fourth) Problem and Benacerraf's Identification Problem. Applications to computer science include a model for Homomorphic Encryption, and a linearly-scaleable circuit that serves for parallel addition and multiplication of scalars, vectors and matrices, with wide implications for Area-Specific Integrated Circuits (ASICs) used in CGI, Neural Networks and AI training, Dimensionality Reduction for Machine Learning at Software and Hardware Level, Digital Signal Processing, among other applications that depend on fast and low-powered vector operations. This low-power In-Situ (In-Memory) computing architecture, based on a patent-pending Simple and Linear Fast Adder (SLFA), is a direct consequence of the proposed set theory. Algebraic invariants are also described with results bringing together set theory, discrete mathematics, number theory and algebraic structures. A canonical block form is defined for the Cayley table of finite groups, in terms of the numeric representation of groups. Automorphisms, and the minimal independent system of equations that define the group are given by the block form, among other information regarding groups' internal and external structure. The proposed construction of natural numbers is generalized to provide a simple and transparent construction of the continuum of real numbers, with a fast approximation for the numeric derivative that can be implemented with the SLFA. Infinite data structures are defined in the most efficient way with the smallest possible data type. A countable sequence of real numbers is coded in a single real number, and an infinite $\infty \times \infty$ real-valued matrix is also coded with a single real number. A real function is coded in a set of real numbers, and a countable sequence of real functions is also coded in a set of real numbers. These codings are meaningful and computable. Mathematical objects of all types are well assigned to tree structures in a proposed hierarchy of types.

Keywords: Structuralism; Set Theory; Fast Adder; Arithmetic Logic Unit; Finite Group; Real Number; Fast Derivative; Data Types; Tree; Complexity; Matrix Multiplication; Fully-Homomorphic Encryption

The science of Cryptography was born to solve the problem of secure communications. For example, two parties wish to communicate a message that could be intercepted by a third party. It is desireable to communicate the message in a Language that can be read by the intended parties but cannot be read by unintended parties even if the message is intercepted. This secret language is called *cypher text* and the applications of these ideas are quite apparent and have been around for a long time.

Problem:

In recent years new cryptographic problems have come up, requiring a new type of encryption that goes beyond this simple application. For example, you walk into a bank to solicit a loan. The bank will request sensitive financial information, such as income, existing loans, expenses, liabilities, investments, capital, assets, etc. The bank will then input this information into a mathematical formula to calculate whether or not your loan is approved. The main problem with this is that the bank will have to see your financial data in order to make this decision; to compute the result they will have to know the inputs. Would it be possible for the bank to make this decision without having to see your information? This concept is Homomorphic Encryption, and it is the science of *Computing Without Knowing*. The possibilities for creating a safe and efficient Cloud Computing environment are limitless and will enable the safe sharing of information in the ever-evolving integration of data and processes.

Currently there are various ways of implementing HE, but these are not energy efficient, and time performance is not feasible for many applications.

Solution:

The basic idea behind the scheme proposed is that operations can be displaced to different parts of the number line. For example, the expression 8+10=18 can be displaced. If we multiply this expression by 2 the result is 16+20=36. Multiplying this expression by 2 again gives 32+40=72. Notice that all three expressions are true. You can ask someone to perform an addition for you without telling them which addition you want them to do, because you can ask them to add an equivalent pair of numbers anywhere on the number line. When you have the result you simply transport the result back to the origin, which only you know. Perhaps the addition you wanted to know was 4+5=9, or perhaps it was 80+100=180. These are all equivalent operations.

Why This HE Scheme?

Replacement of traditional HE schemes with the proposed encryption will:

-Significantly Improve Time and Energy Efficiency

-Allow Fully Homomorphic Encryption

-Eliminate Noise Restrictions

What's Next?

1. Developing libraries and software for current FHE applications and standards.

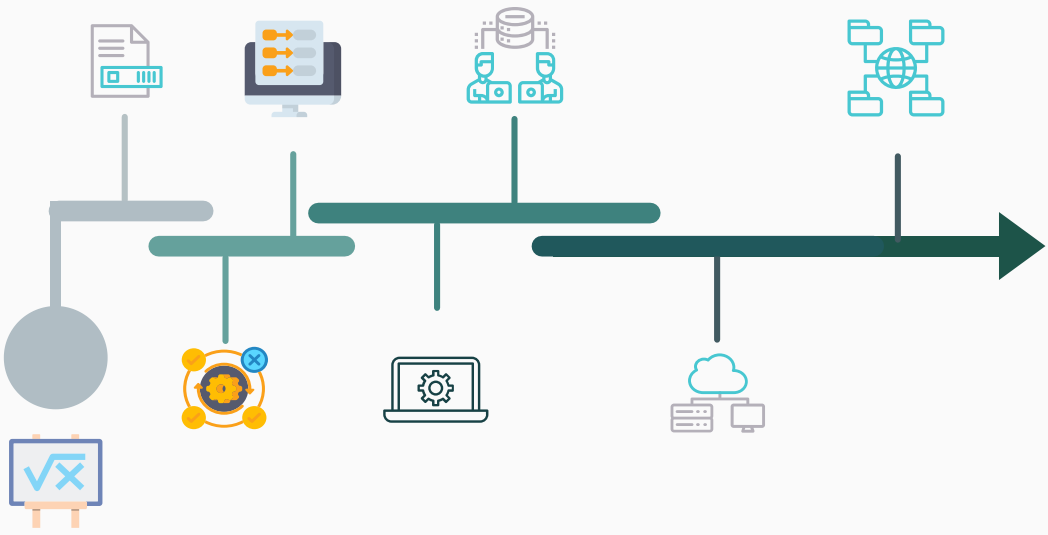
2. Research and Development of Low-Level-Languages connecting with advancements in the hardware level such as the In-Memory Simple and Linear Fast Adder (SLFA) presented in the adjoint presentation.

3. Designing and Production of Encryption Units for fast and secure cloud computing.

PROGRESS STAGES

0. Mathematical Model and Concept Product
1. Identifying Protocols for Immediate Implementation
2. Development
3. Auditing
4. Product Implementation

Progress:
We have succesfully started progress on stage 0 with a well-defined Fully Homomorphic Encryption (FHE) Scheme.



STAGE (0): MATHEMATICAL MODEL AND CONCEPT PRODUCT

Summary

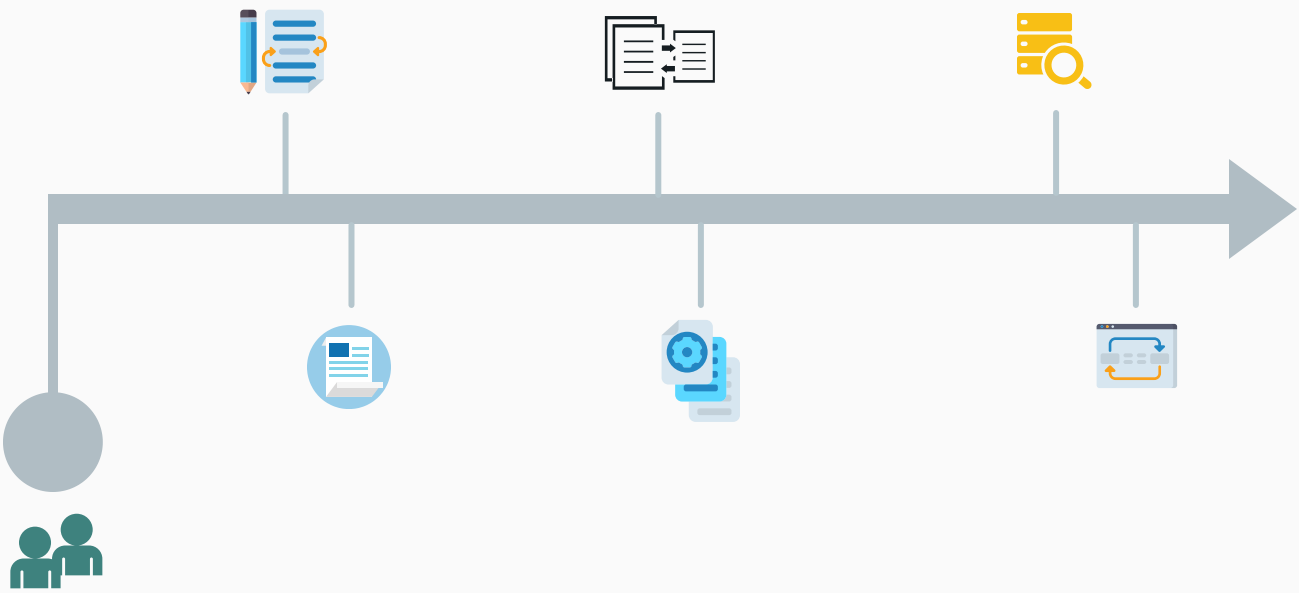
Traditionally, encryption schemes are meant to be deciphered by a second party. However, recent applications have required encrypting a message that the second party can access and manipulate without deciphering it. The message can then be sent elsewhere for verification or further processing. These scenarios can be applied to a wide range of industries such as AI and neural network training, Universal Digital Identity, banking, aviation, traffic planning, on-line commerce, cloud storage and data verification, communications, genomics and biometric technology, etc.

A general mathematical method for HE schemes is being developed; these concepts are available in [1]. Initially, a HE scheme should be chosen that will allow for the simple implementation of the mathematical model, that can showcase some of the advantages and differences with other HE implementations.

The concept product will allow users to send an encrypted numeric data base, to which only they will have the key, along with a prompt for operating on the database. The operated data base will be sent back to the user for deciphering. When the user deciphers the operated data base, the result will be the same as if the operation was done on the original database, i.e., the desired result is obtained. In other words, the user is able to release the data to a second party to perform operations on the data, but only the user knows the initial inputs and final result. The second party will only have access to 1) encrypted inputs, and 2) encrypted output. The user will be the holder of a private key, which will allow him to encrypt the inputs and decrypt the output.

OBJECTIVES FOR STAGE (0)

- Build a Core R&D Team
- Mathematical Model
- Concept Product
- Conclusions and Planning for Next Stages



THE TEAM

A team of specialists in Cryptography, Medium-Level Languages, and Mathematics will lay the groundwork for specialized, state-of-the-art, Homomorphic Encryption schemes, among other applications to Cloud Computing and Information Theory.

Software

The initial concept products will have to be developed with a team of SW Engs.

Mathematics

A team of mathematicians covering the basic areas of cryptography, number theory, mathematical analysis, matrix analysis, computational geometry, AI, Probability Theory, Finite Mathematics and Combinatorics, Algebra and Logic, will help to choose the best research topics for later stages.

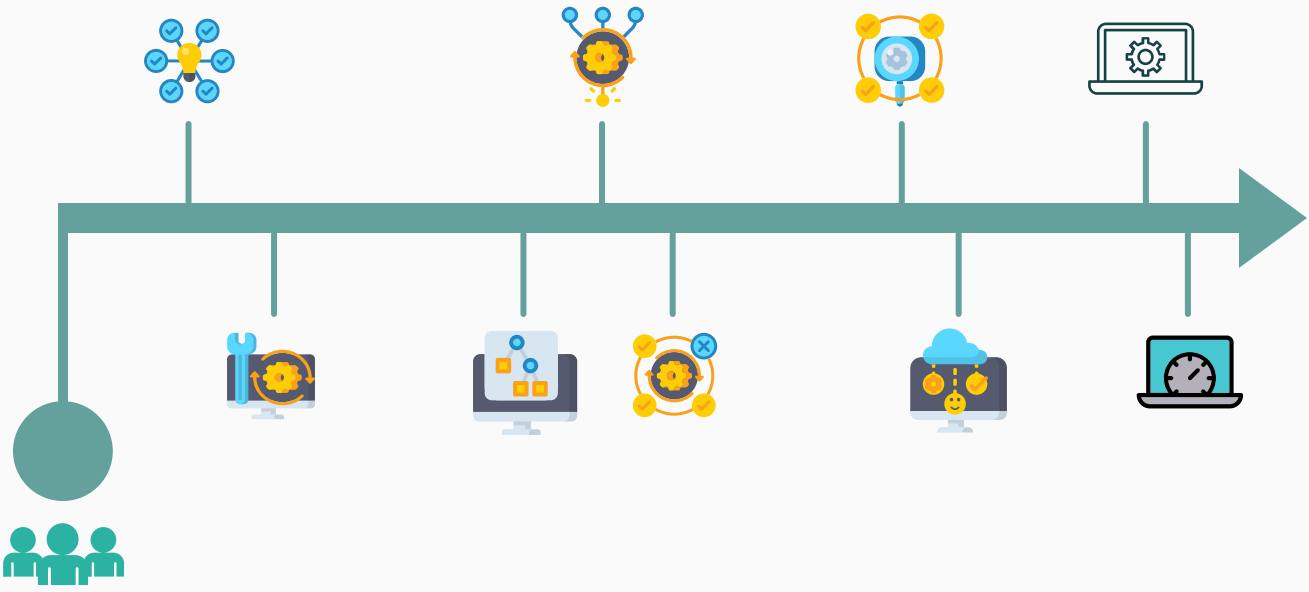
STAGE (1): IDENTIFYING PROTOCOLS FOR IMMEDIATE IMPLEMENTATION

Summary

The market and demand for Homomorphic Encryption schemes is already existent and growing in depth and breadth. It is important to carefully compare schemes in order to identify the best candidates for immediate implementation using the mathematical model developed in the last stage. Candidate schemes will be chosen on the basis of time, simplicity and applicability, as well as strategic goals.

OBJECTIVES FOR STAGE (1)

- Consolidate and Expand the Team
- Identify Critical Patents from the Theoretical Framework
- Reduce Candidate Implementations Prioritizing Quickness and Simplicity
- Identifying Industries and Clients for Immediate Implementation
- Development and Evaluation



STAGE (2): DEVELOPMENT

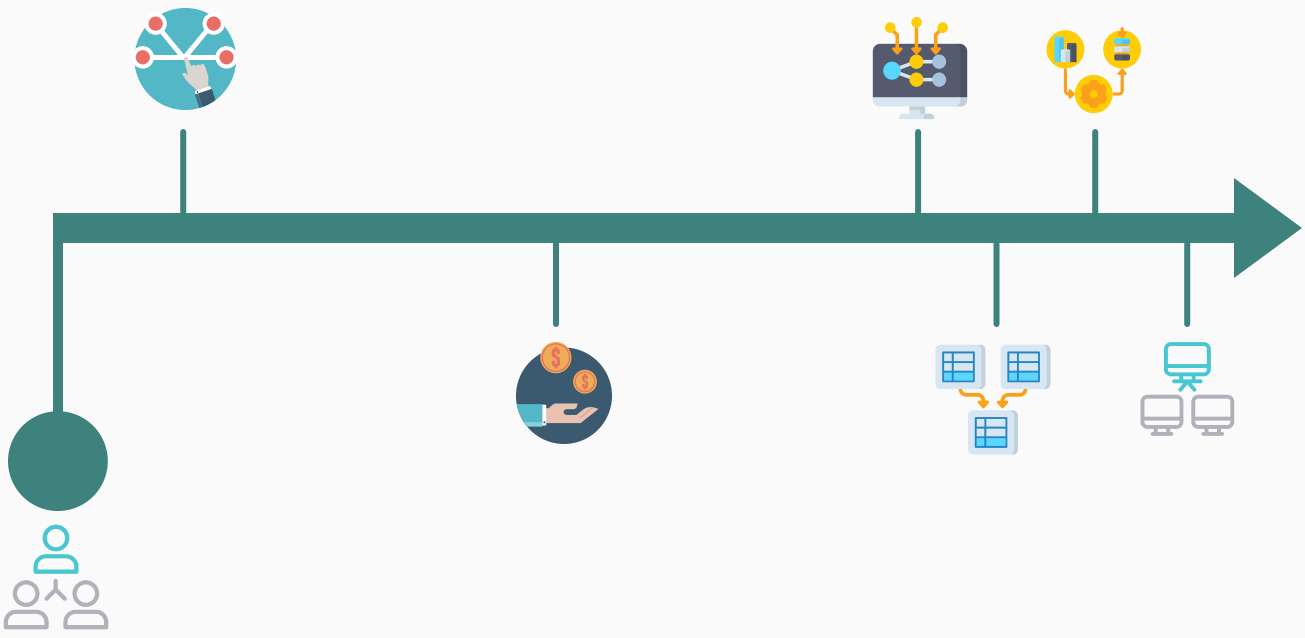
Summary

Once the immediate implementation industries are recognized and prioritized by simplicity and speed of integration, along with their preliminary technical aspects, we proceed to integrate our FHE scheme to current standards and problems of those industries.

We seek collaboration with participants in the data processing and cloud computing industry to replace existing FHE schemes where it is convenient. The first applications will be in the banking and finance, aviation and transportation, telecommunications and Cloud Computing. During this stage we look to collaborate, by contract, with clients from key industries that will benefit from our initial schemes.

OBJECTIVES FOR STAGE (2)

- Find Sr. Engs. and Team Leadership
- Establish Collaboration with Industry Clients
- Secure Development Contracts with Key Industries
- Integrate Our Schemes to Client Standards



STAGE (3): AUDITING

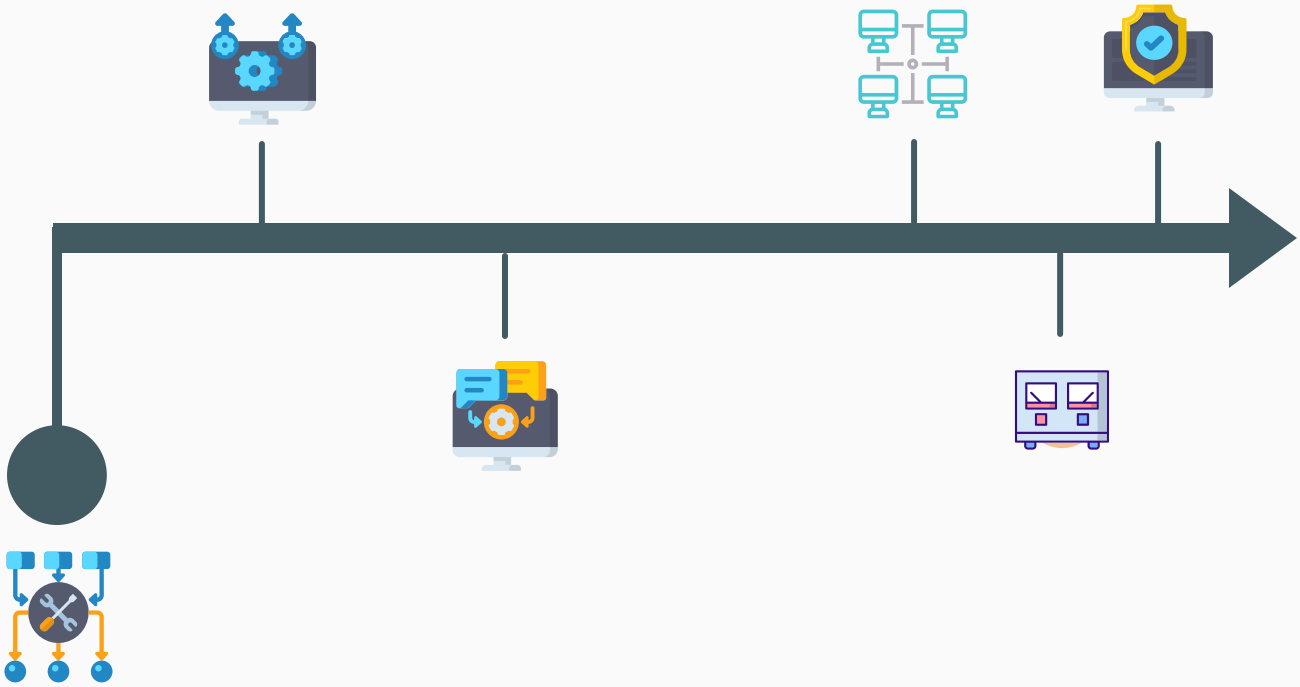
Summary

In the previous stage, we work together with our clients' teams to tailor design SW based encryption schemes for their specific needs. In this stage we ensure that our clients conclude successful implementation of FHE to their processes.

First, a serious of security and performance audits will be conducted on our FHE schemes. We maintain cooperation with our clients for additional testing, troubleshooting, quality monitoring, etc.

OBJECTIVES OF STAGE (3)

- Testing and Troubleshooting
- Validation of Schemes



STAGE (4): PRODUCT IMPLEMENTATION

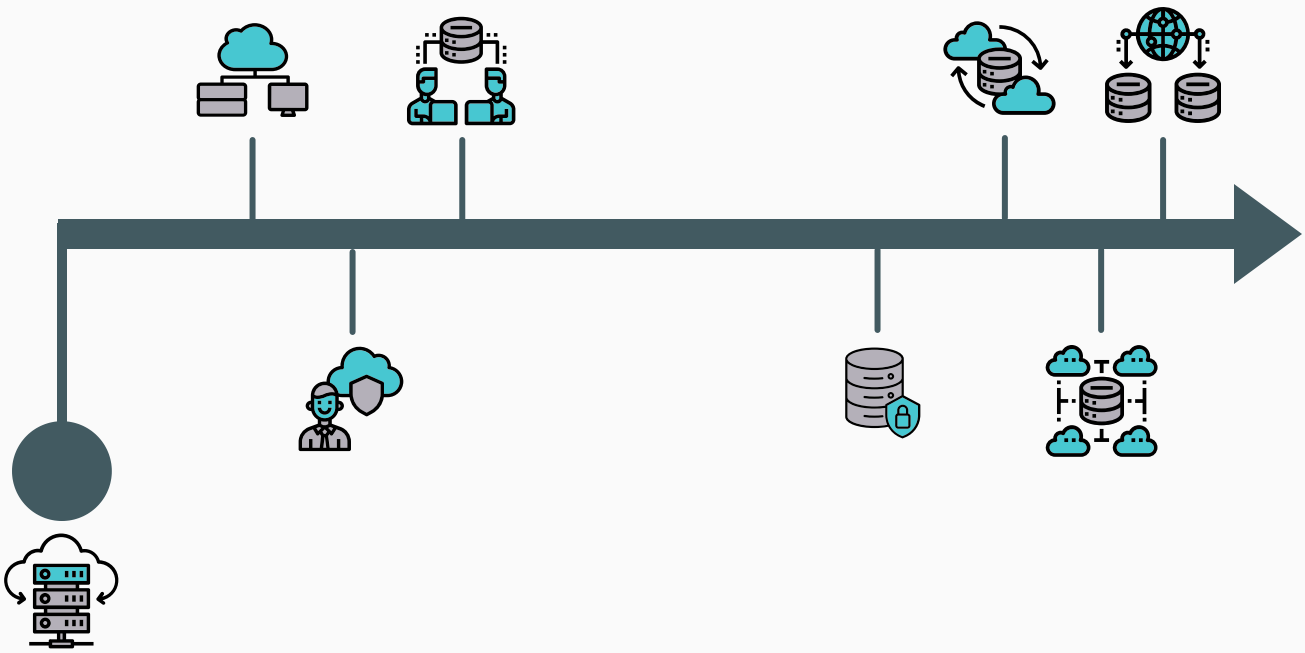
Summary

There is a growing complexity to the problems that computing must solve. Some of these problems could have easier solutions if data could be freely shared in an efficient and safe manner. For example, traffic light synchronization can be better planned if the travel paths of most vehicles were processed into a central data base. The first downside of such an implementation would be the surrender of huge amounts of private and sensitive information to a centralized data base. Because of this, FHE is central to the solution of many socially important problems.

The implementation of Fully Homomorphic Encryption will consist of several stages to complete. Modern cloud computing will require a vertical and horizontal integration of FHE that allows fast, efficient and secure computing across all devices and systems, at every level.

OBJECTIVES OF STAGE (4)

- First Product Applications
- Additional Schemes
- Elaborate Large-Scale Schemes



To secure the necessary resources for research and development, we seek strategic collaborations and partnership with a wide range of industries, as well as building a strong brand and reputation of innovation and quality. As our ally, you will be greatly benefited by this unique focus into microprocessors and other critical technologies and acquire a strategic advantage in the changing technological landscape.

Join us in this exciting journey and let's make history together. Thank you!

Juan P. Ramírez
Project Leader

STRATEGIES

Leadership

- R+D on fast and secure Homomorphic Encryption.
- Collaboration in R+D, with partners of relevant industries and institutions.
- Exploring new research areas with applications to Information Theory.

Innovation

- New approach to state-of-the-art encryption.
- Innovate industrial and academic research by reformulating applicable mathematical foundations.

Services and Products

- Offering a safe, private and secure environment for businesses and users to share and process data as needed.
- Providing privacy and security in large-scale integration of digital solutions while maintaining computational throughput.

Marketing and Customer Experience

- Web Development, and online testing/auditing.
- A general Fully Homomorphic Encryption method that adapts to different scenarios.
- Personalized encryption for every application, increasing performance and security.

EARLY TACTICS

- Validate new FHE schemes and compare the results to existing standards.
- Generate world class Research in Applied Mathematics and Computer Sciences.
- Participation in key international conferences and symposiums.
- Collaboration and strategic alliances with clients and partners.
- Early marketing strategies for connecting to general and targeted public.

MISSION

Maintaining our clients at the forefront of fundamental
processes in digital technologies
through global high-value patents and world-class R+D.

As well as the responsible integration of technological solutions
and the exploration of state-of-the-art applications that enrich experiences for
general public, scientists and artists.

VISION

Modern anthropological sciences and technological development from AI
to Social Organization, are product of interactions between
humanities and natural sciences.

The greatest challenges that science must solve are related to human realities and
are growing in complexity and breadth.

Recognizing that the nature of our most critical problems is socio-technical,
a better comprehension of solutions and implementations will be possible.

BIBLIOGRAPHY

[1] Ramírez, Juan Pablo. 2023. "Canonical Set Theory with Application from Parallel Matrix Operations and Data Structures to Homomorphic Encryption". *Exclusively on Author's personal page: www.binaryprojx.com*

[2] Ramírez, Juan Pablo. 2019. "A New Set Theory for Analysis" ***Axioms*** **8, no. 1: 31. https://doi.org/10.3390/axioms8010031.**

[3] Par Persson Mattson. Why Haven't CPU Clock Speeds Increased in the Last Few Years? Why Haven't CPU Clock Speeds Increased in the Last Few Years? | COMSOL Blog

[4] Infographics: Operation Costs in CPU Clock Cycles - IT Hare on Soft.ware
translated by Sergey Ignatchenko.

[5] Hennessy, J.L. and Patterson, D.A. (1990) Computer Architecture: A Quantitative Approach. Morgan Kaufmann, Waltham.

[6] Andrew Reilly. Multi-Core Processors are the Key to Unlocking Aviation's Future. ***AeroSpaceTechReview.com*** **(Nov. 10, 2020).**

[7] Yiqiu Sun, Haichao Yang, et. al. ASIC Design for Bitcoin Mining. ***University of Michigan*****.**

[8] Miguel Albert Orenga, Gerard Enrique Manonellas. Estructura de Computadores, Módulo 7: La Arquitectura CISCA. ***Universitat Oberta Catalunya.***

[9] M.S. Schmalz. Organization of Computer Systems, Section 3: Computer Arithmetic. ***University of Florida.***

[10] Abrar, M., Elahi, H., Ahmad, B.A. ***et al.*** **An area-optimized** ***N*****-bit multiplication technique using** ***N*****/2-bit multiplication algorithm.** ***SN Appl. Sci.*** **1, 1348 (2019). https://doi.org/10.1007/s42452-019-1367-6**

[11] Niall Emmart and Charles C. Weems. High Precision Integer Multiplication with a GPU Using Strassen's Algorithm with Multiple FFT Sizes. ***Parallel Processing Letters, Vol.21, No. 03, pp. 359-375 (2011).*** **https://doi.org/10.1142/S0129626411000266**

[12] Arithmetic Logic Units (ALU) Information: Specs.
Globalspec.com

[13] Muhammad Ikmal Mohd Taib, Muhammad Najmi Zikry Nazri, et. al (2020). Design of Multiplication and Division Operation for 16 Bit Arithmetic Logic Unit (ALU). ***JOURNAL OF ELECTRONIC VOLTAGE AND APPLICATION VOL. 1 NO. 2 (2020) 46-54***
DOI: https://doi.org/10.30880/jeva.2020.01.02.006

BIBLIOGRAPHY

[11] Hennessy, J.L. and Patterson, D.A. (1990) Computer Architecture: A Quantitative Approach. Morgan Kaufmann, Waltham.

[12] Andrew Reilly. Multi-Core Processors are the Key to Unlocking Aviation's Future. *AeroSpaceTechReview.com* (Nov. 10, 2020).

[13] Yiqiu Sun, Haichao Yang, et. al. ASIC Design for Bitcoin Mining. *University of Michigan*.

[14] Chenyu Wang, Ge Shi, Fei Qiao, Rubin Lin, Shien Wu and Zenan Hu. Research Progress in Architecture and Application of RRAM with Computing-In-Memory. Nanoscale Adv., 2023, 5, 1559-1573.

[15] R. Uma, Vidya Vijayan, et. al. Area, Delay, and Power Comparison of Adder Topologies. *International Journal of VLSI design & Communication Systems (VLSICS) Vol.3, No.1, February 2012*.

[16] Singh, Kumar and Singh. Performance Analysis of Fast Adders Using VHDL. *2009 International Conference on Advances in Recent Technologies in Communication and Computing*.

[16] Xie, Jingya, Niu, Xinxiang, Hu, Xiaoyong, Wang, Feifan, Chai, Zhen, Yang, Hong and Gong, Qihuang. "Ultracompact all-optical full-adder and half-adder based on nonlinear plasmonic nanocavities" *Nanophotonics 6, no. 5 (2017): 1161-1173*. https://doi.org/10.1515/nanoph-2017-0035

JUAN PABLO RAMÍREZ

PHONE NUMBERS:

+1 (708) 945 - 447
+52 (33) 2343 - 1317

EMAIL AND PERSONAL PAGE:

jramirez@binaryprojx.com
www.binaryprojx.com

ADDRESS:

Guadalajara, Jalisco, México

EDUCATION

UNIVERSIDAD DE GUADALAJARA

2008 - 2011, Guadalajara, México

- Teaching experience
- Served in panels for designing new academic programs in Natural Sciences and Engineering
- Participation in research and industrial application programs
- Speaker at Conferences and Seminars
- Developing and solving mathematical models for Theoretical Physics, with Dr. Georgi Pogosyan of the International Center for Advanced Studies and the Joint Institute for Nuclear Research
- Applied Mathematics with Dr. Alexander Yakhnov, from the Dpt. of Mathematics
- Director of extra-curricular academic events such as workshops and the "Art and Science Week"

UNIVERSIDAD DE GUANAJUATO Y CENTRO DE INVESTIGACIÓN EN MATEMÁTICAS (CIMAT)

2011 - 2013, Cd. Guanajuato, México

- Research presented at area-specific conferences and seminars
- Experience in mid-level and low-level programming languages
- Activities divulging mathematical sciences

LANGUAGES

English
Spanish
C++
Python

RESEARCH AREAS

Mathematics

Physics

Computer Sciences

RESEARCH TOPICS

- General Theory of Systems
- Mathematical Analysis
- Axiomatic Basis and Mathematical Foundations
- Numeric Solutions
- Recursivity
- ALU Architecture
- Computability and Complexity
- Category Theory
- Logical Systems
- Formal Systems and Languages
- Cryptography and Homomorphic Encryption
- among other related topics.

PARTICIPATIONS

- Conference on Recursive Solutions for Constant Coefficient Differential Equations (U. de G. 2010)
- Conference on Axiomatic Basis for Probability (Second School on Logic and Sets, UNAM campus Morelia, 2013)
- Conference on General Theory of Systems and Algebraic Structures (Physical-Mathematical Sciences Week, Universidad de Guadalajara, 2017)
- Conference on A Natural Construction of Real Numbers (Physical-Mathematical Sciences Week, Universidad de Guadalajara)
- Workshop on Mathematics and Paint (Physical-Mathematical Sciences Week, Universidad de Guadalajara, 2018)
- Conference on Topologies of N, in the Construction of R (Physical-Mathematical Sciences Week, Universidad de Guadalajara, 2018)
- Organization and Direction of Art and Science Week at Universidad de Guadalajara, including workshops, conferences, roundtables and creation of Mural Inteligente (2018).
- Workshop on Mathematics and Paint (Physical-Mathematical Sciences Week, Universidad de Guadalajara, 2018)
- Workshop on Higher Order Derivatives for Solving Partial Fractions and their Applications (XIII Encuentro de Especialistas del Norte de Jalisco y Sur de Zacatecas, 2018).
- "The Nature of Numbers" (Logic and Foundations Special Session available online, 52 Mexican Congress of Mathematics, Monterrey, Nuevo León, 2019)
- "The Nature of Numbers" (Universidad de Guanajuato/CIMAT, 2019)
- Chicago Quantum Summit (University of Chicago, 2020)
- Mural Inteligente (Inauguration of 55 Mexican Congress of Mathematics, 2022)
- "Simple Representation of Natural and Real Numbers" (Logic and Foundations Sessions, 55 Mexican Congress of Mathematics, Guadalajara, Jalisco, 2022)
- "Simple and Linear Fast Adder based on a Simple Representation of Natural and Real Numbers" (Computer Science Sessions, 55 Mexican Congress of Mathematics, Guadalajara, Jalisco, 2022)
- "Canonical Block Form for Finite Groups" (Algebra, 55 Mexican Congress of Mathematics, Guadalajara, Jalisco, 2022)
- "A Pseudo Measure on the Space of Finite Functions and Permutations" (Algebra, 56 Mexican Congress of Mathematics, San Luis Potosí, 2023)
- "An Algorithm for Fast Multiplication and Addition of Multiple Inputs and it's Implementation for In-Memory-Computing" (Computer Sciences, 56 Mexican Congress of Mathematics, San Luis Potosí, 2023)

PUBLICATIONS

- Ramirez, J. 2023. "Canonical Set Theory with Applications from Matrix Operations and Data Structures to Homomorphic Encryption" *Exclusively on Author's personal home page: www.binaryprojx.com*
- Ramírez, J. "Logarithmic-Time Addition for BIT-Predicate With Applications for a Simple and Linear Fast Adder And Data Structures" *Preprints.org* 2020, 2020070415. https://doi.org/10.20944/preprints202007.0415.v4
- Ramírez, J. "A New Set Theory for Analysis" *Axioms* 8, no. 1: 31. https://doi.org/10.3390/axioms8010031. Cited by Lovyagin (2021) on Finite Arithmetic and Non-Standard Analysis for Hyperrationals with Applications to AI.
- Ramirez, J. 2015. Systems and Categories. arXiv:1509.03649v5 [math.CT]
- Ramírez, J., Londoño W., et. al. "Closed Solution for Partial Fractions" Boletín Redipe, ISSN-e 2256-1536, Vol. 7, Nº. 11, 2018 (Special issue dedicated to: Pedagogical value of the media), págs. 172-178