COLLABORATION PROPOSAL

FOR THE IMPLEMENTATION OF A FULLY HOMOMORPHIC ENCRYPTION SCHEME

Join us as we take part in the revolution of cloud computing, unlocking untapped mathematical potential that will redefine standards of computing performance and data privacy across multiple sectors including smart cities and grids, Machine Learning such as in specific cases of AI and Neural Network training utilizing sensitive data, operating vectors of encrypted databases, and energy management, amongst other activities that directly depend on a difficult balance between data security and efficient computing. Together, we can develop the next generation of arithmetic-compatible encryption to set new standards of security, performance and efficiency.

My mathematical research provides an optimal representation of mathematical objects and structures [1,2,3] with direct applications in computer science [4,5,6], and the mathematical foundations of computer science. Leveraging this new mathematical description, we seek to create value by offering efficient technological solutions to a range of industries. Among these, is a general method [4] for time and energy efficient Fully Homomorphic Encryption [7,8]. The search for efficient algorithms that can process encrypted data (without decrypting it first) is still ongoing and it is a problem at the forefront of Machine Learning and other emerging technologies [9-13] and has recently been referred to as the 'Holy Grail' of Cryptography by industry giants.

This document is a proposal for the continued development of Language-Level solutions to Fully Homomorphic Encryption (FHE) based on a "random change of variables" method I have published and presented by the author at international conferences. Through strategic partnering and collaboration, we are poised to drive innovation and create a competitive edge in the rapidly evolving technological landscape, advancing private and secure cloud-computing performance and throughput. A separate proposal discusses a Compute-In-Memory architecture based on a patent-pending Simple and Linear Fast Adder [5,6] filed by the author.

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

This initiative is based on a "random change of variables" method that allows fast and low-powered calculation of mathematical operations on encrypted vectors [4]. Mathematics is the invisible framework supporting scientific progress and technological innovation. Not only does it advance our understanding of abstract concepts, but it also provides practical solutions to real-world challenges because it is the universal language behind all sciences. The coding language that computers understand is built on mathematics. Consequently, by refining the underlying principles of mathematics, we essentially upgrade the 'language' that enables our technology to communicate and perform tasks more efficiently.

In a world pushing the boundaries of innovation, we are reaching the limits of current technological frameworks. Using a novel conceptualization of the foundations of mathematics with immediate applications in a number of key technologies we can facilitate seamless data representation and computational throughput, from high-level software languages down to the System-on-Chip hardware level, and introduce efficiency in ways previously unexplored.

Problem:

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 desirable 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. The message written in this secret language is called *cyphertext.* Applications of these ideas are quite apparent and have been around a long time before computers.

Traditional encryption seeks to encrypt data at rest or in transit (end-to-end encryption). However, cloud computing, Machine Learning, smart grids, and other recent developments call for more sophisticated methods of encryption that are compatible with mathematical and logical operations. Suppose you wish to solicit a bank loan. The bank requires financial information from you, in order to approve or deny the credit. That information is fed into a mathematical equation and the numeric result will determine if the loan is approved or not. You can send your information securely to the bank and the bank will be able to safely store the information, using standard end-to-end encryption. However, the bank will need to make use of your data, and in doing so it will have to decrypt it first. Once the data is decrypted, it will most likely be stored somewhere in decrypted form. This means your data can ultimately be used for unintended purposes either by the bank or a third party that compromises the bank's security. It is common for banks to pay out significant amounts in penalties derived from accidental data breaches and broken confidentiality agreements stemming from the liability of storing clients' sensitive information within the potential reach of employees, executives, third-parties, contractors, and others.

In other words, current encryption standards are very secure for data at rest and in transit (end-to-end encryption). However, when the information has to be processed, a problem arises because the information has to be decrypted first.

Solution:

Homomorphic Encryption gives us the ability to eliminate the confidence factor completely to ensure data integrity, even when the data is being processed. In our example of a loan approval, both the client and the bank can benefit. The bank is able to make complex decisions without the liability of handling and storing sensitive data, while the client's privacy and digital identity is uncompromised. In essence HE *processes data without reading the data*. The numbers are encrypted during the whole data path including storage, transmission *and processing*. The main difference between processing information using traditional encryption and HE is that the order of processing and decrypting the information is inverted. With traditional encryption we first decrypt the ciphertext, and then process the plaintext inputs. With HE we first process the ciphertext, then the output is decrypted. This is the main benefit of HE. The order of the decryption and the processing is reversed. The result of this inversion of steps is that the original inputs are not shared with the second party. Paradoxically, the data is processed without being read.

To cite more relevant examples, suppose a client wishes to train an AI, off-site. Or perhaps a Smart Grid is possible for a certain system, but a Neural Network must be trained with sensitive data that cannot be shared with the service provider. Solutions to these problems exist but they come with very big efficiency trade-offs. Currently, there is a growing interest in finding more efficient and reliant techniques for Homomorphic Encryption given there are persisting problems including noise, and time and energy consumption.

Enhancing trust in cloud computing by providing a secure environment for data-driven decision-making opens the door to otherwise impossible solutions. Homomorphic Encryption makes centralized processing possible without compromising data privacy, and is set to revolutionize cloud computing facilitating accurate and comprehensive data processing and analysis while ensuring efficiency, security and privacy. The possibilities for a safe and efficient cloud computing environment are limitless in the ever-evolving integration of data security and processing throughput. However, standard HE techniques operate in complicated mathematical spaces that lead to significant time delays and energy consumption that renders implementation in many critical applications inviable.

HE by Random Change of Variables:

We propose a HE scheme [4] for applications that require processing heavy loads of private data such as ML and AI training, banking, aviation, traffic planning, online commerce and security, cloud computing, communications, and biometric technology, among others, without the huge trade-offs related to most HE schemes.

The "change of variables" method [4] helps reduce some problems associated with standard HE techniques such as noise, bit-precision, and time and energy constraints. Additionally, it is flexible and can be adapted for managing different number of parties, permission settings, security levels, efficiency requirements, etc. Our work goes beyond conventional protection of sensitive data. We're pioneering a new level of security and throughput for computing encrypted data.

The proposed solution solves a range of challenges for HE and introduces a blind suite of solutions. Information will no longer have to be stored or accessed in plaintext form in order to be used; it stays encrypted during processing. Our secure homomorphic computing scheme allows accurate and complex decision-making while maintaining data integrity, and without significant time and energy tradeoffs. Furthermore, the encrypted data can only be used for the intended purposes. This method ensures that any unintended operation performed on the data results in a meaningless string.

Why This HE Scheme?

Replacement of traditional HE schemes, with the proposed method, will:

- Significantly Improve Time and Energy Efficiency
- Allow Fully Homomorphic Encryption
- Eliminate Noise Restrictions
- Arbitrary Precision is Achieved without Huge Tradeoffs
- Encrypted Data can Only be Used for Intended Purposes
- Flexibility for Different Requirements and Applications

What's Next?

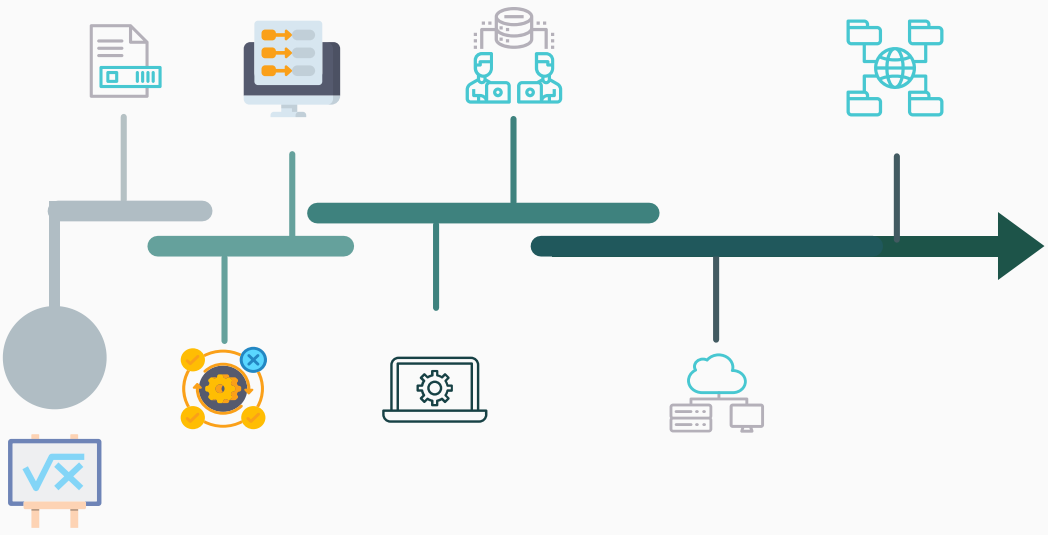
1. Developing libraries and software for current FHE applications and standards.
2. Research and Development from Low and High-Level-Languages to hardware level such as the patent-pending Compute-In-Memory architecture for a Simple and Linear Fast Adder (SLFA) [5,6].
3. Encryption Units for fast and secure cloud computing.

PROGRESS STAGES

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

Progress:

We have successfully completed stage 0. Progress on stage 1 has commenced with a Minimum Viable Product in the form of an Encrypted Database that can return results of arithmetic operations on encrypted vectors of the DB.



STAGE (0): MATHEMATICAL MODEL AND CONCEPT PRODUCT

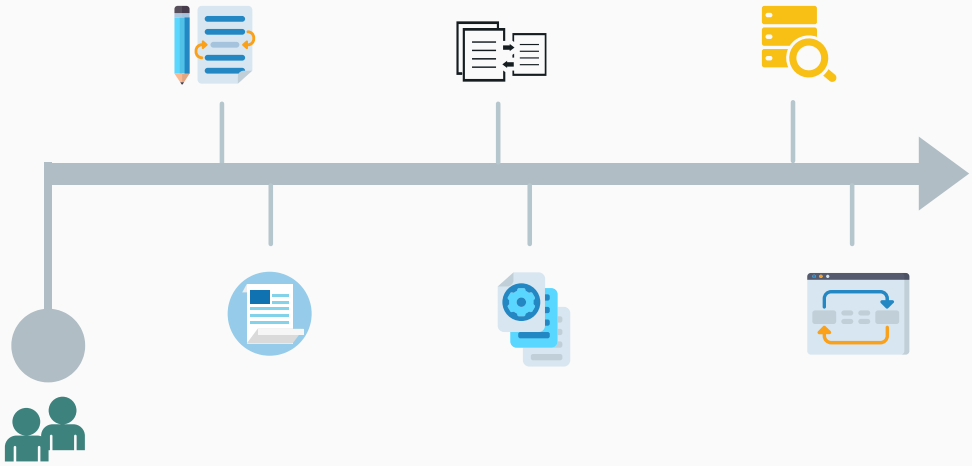
Summary

Traditionally, encryption schemes are designed to be decrypted by a second party. However, recent applications require the second party to process and manipulate the data without decrypting it. This scheme benefits a wide range of industries including AI and neural network training, Universal Digital Identification, banking, aviation, traffic planning and transportation systems, online commerce, cloud storage and data verification, communications, genomics and biometric technology, etc.

I have developed a Proof of Concept, with the "random change of variables" method for HE, which allows encrypted evaluation of a loan application [4]. Users send their personal data to a banking institution and the data will be evaluated to determine whether the loan is granted or denied. The clinet sends their data to the bank in encrypted form and the bank processes it without decrypting it. The bank processes the client's data but cannot know the original inputs. The bank only has access to 1) encrypted input data, and 2) output data.

OBJECTIVES FOR STAGE (0)

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



THE TEAM

A team of specialists in Cryptography, Low to 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 product has been developed with a team of two Jr. software Engs.

Mathematics

Mathematical expertise covering the basic areas of cryptography, number theory, mathematical analysis, matrix analysis, computational geometry, Probability Theory, Finite Mathematics and Combinatorics, Algebra and Logic, and Machine Learning is needed to choose the best research topics for later stages.

STAGE (1): IDENTIFYING PROTOCOLS FOR IMMEDIATE IMPLEMENTATION

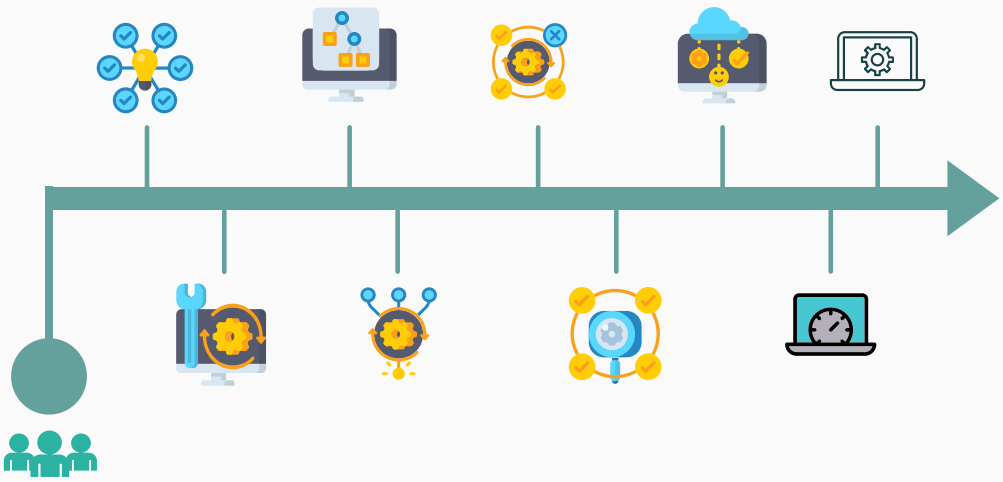
Summary

The market and demand for Homomorphic Encryption schemes is already existent and growing. It is important to carefully compare schemes in order to identify the best candidates for immediate implementation. Candidates will be chosen on the basis of cost-benefit ratio, simplicity of implementation, applicability and strategic goals, among other criteria. The most immediate and important applications being Machine Learning and Cloud Computing across many industries.

This change of variable method for HE is flexible and suits a range of applications. After having successfully completed the desired POC, we are developing a Minimum Viable Product that will allow the User to send a request to an encrypted data base to perform an operation on an encrypted vector of that data base. The user will know the result of the operation but is unable to decrypt the vector. A number of industries will benefit directly from this protocol.

OBJECTIVES FOR STAGE (1)

- Consolidate and Expand the Team
- Identify Critical Intellectual Property from the Theoretical Framework
- Prioritize Implementations Based on Speed and Simplicity
- Identify Key Industries and Clients for Immediate Implementation
- Development and Evaluation



STAGE (2): DEVELOPMENT

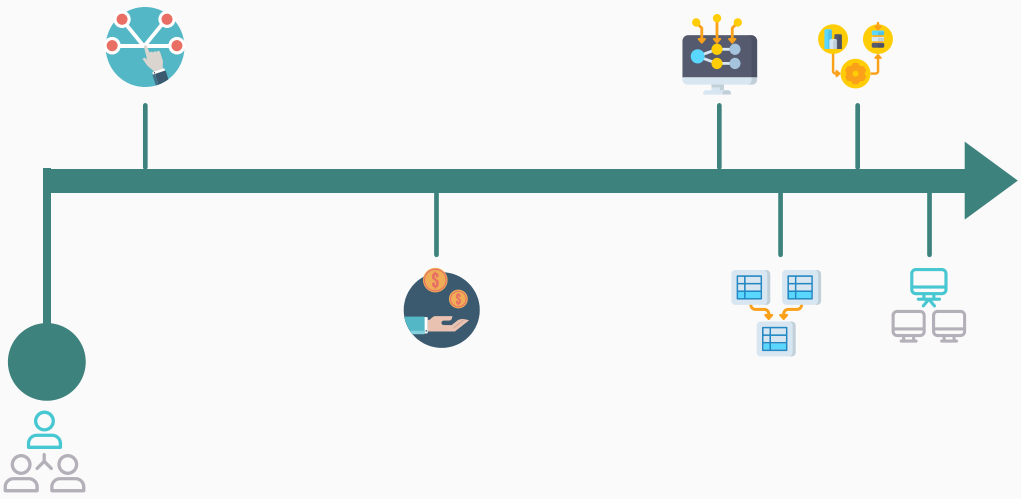
Summary

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

We seek collaboration with participants in the data processing and cloud computing industry to replace existing FHE schemes where it is most convenient. The first applications may include ML and AI, finance, aviation and transportation, and Digital Signal Processing. During this stage we look to collaborate, with partners from key industries.

OBJECTIVES FOR STAGE (2)

- 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

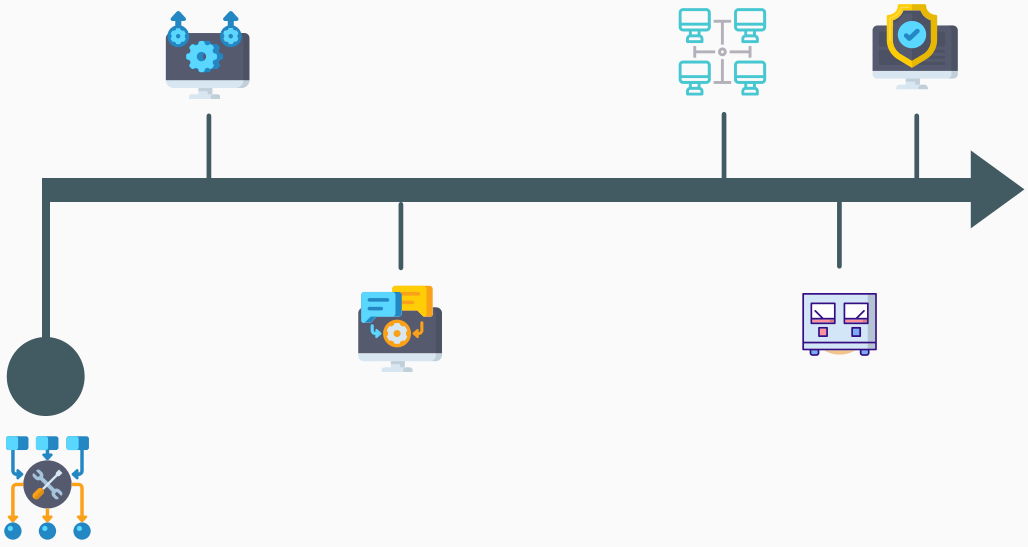
Summary

In the previous stage, we work together with our partners' teams to tailor design software-based encryption schemes for their specific needs. In this stage we ensure that our future clients can successfully implement FHE to their processes.

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

OBJECTIVES OF STAGE (3)

- Testing and Troubleshooting
- Validation of Schemes



STAGE (4): PRODUCT IMPLEMENTATION

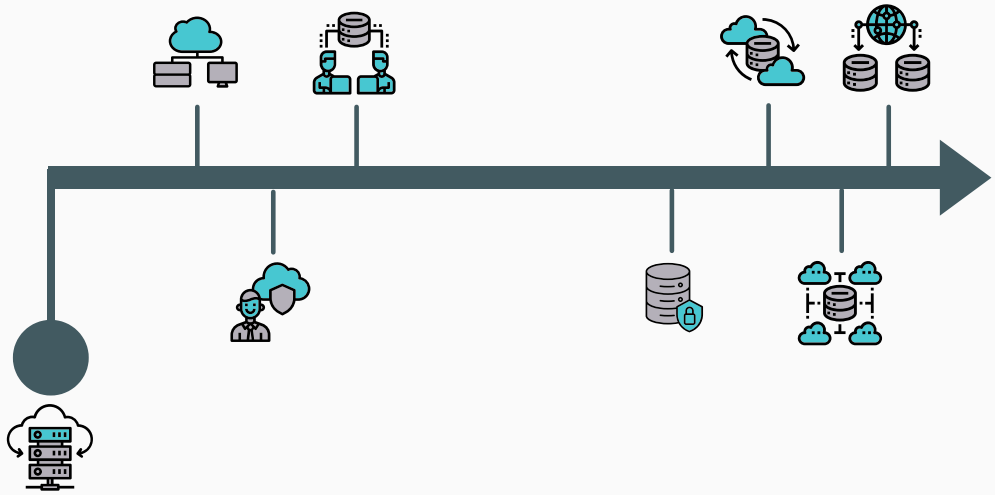
Summary

There is a growing complexity to the problems that computing has to 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 that could make real-time decisions to maximize flow. Setting aside the technical difficulties that may arise, the first downside of such an implementation would be the surrender of huge amounts of private and sensitive information regarding each individual's destination and travel patterns to a centralized data base. That is to say, even if we can solve certain problems at a technical level, they are often not viable for full-scale implementation because of privacy and legal issues. 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 horizontal and vertical 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



LET'S PARTNER

Applications of the HE method we propose can be adapted and scaled to other industries and applications from those mentioned above, creating more revenue sources in the long-term as well. By developing a strategic plan for commercialization and growth, we can achieve a lasting projection of high ROI for our investors.

To secure the necessary resources for research and development, we seek strategic collaborations and partnership with academic, and research experts, as well as industry leading institutions. Together, we can advance this unique focus into the world of cryptography, computational throughput and other critical technologies, acquiring a strategic advantage in the changing technological landscape.

As we stand at the forefront of current innovations, we invite you to push the boundaries of mathematical theory with us. Tangible solutions to today's social and technical challenges, of increasing complexity and breadth, are possible through a long-term vision of a horizontal and vertical integration of mathematically optimal computational standards across all devices and systems. While our work may appear theoretical, its impact is far-reaching in the technology-driven world we live in and seeks to lay foundation for more efficient and secure computing at every level.

Join us in this exciting journey. 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

- [x] Generate world class research in applied mathematics and computer sciences.
- [x] Participation in key international conferences and symposiums.
- [x] Validate new FHE schemes
- [ ] Benchmark the results to existing standards.
- [ ] Early marketing strategies for connecting to general and targeted public.
- [ ] Collaboration and strategic alliances with clients and partners.

MISSION

Maintaining our clients at the forefront of fundamental
processes in digital technologies
through high-value global solutions 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] Ramirez, J. 2023. "Canonical Set Theory with Applications from Matrix Operations and Data Structures to Homomorphic Encryption."
Monograph Exclusively on Author's personal home page: www.binaryprojx.com

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

[3] Ramirez, J. 2015. Systems and Categories. arXiv:1509.03649v5 [math.CT]

[4] Ramirez, J. 2024. "Programming Random Change of Variables for Homomorphic Encryption." White Paper Exclusively on Author's personal homepage: www.binaryprojx.com

[5] J. P. Ramírez, "Simple and Linear Fast Adder of Multiple Inputs and Its Implementation in a Compute-In-Memory Architecture," 2024 International Conference on Artificial Intelligence, Computer, Data Sciences and Applications (ACDSA), Victoria, Seychelles, 2024, pp. 1-11,
doi: 10.1109/ACDSA59508.2024.10467957.

[6] Ramirez, J. “SIMPLE AND LINEAR FAST ADDER,” WIPO, Patentscope.
Publication Number: WO/2023/220537.
Publication Date: 16/11/2023.
Applicant’s and Inventor’s name: Juan Pablo Ramirez

[7] Ronald L. Rivest, Len Adleman, and Michael L. Detouzos. On data banks and privacy homomorphisms. In Foundations of Secure Computation, pages 165–179. Academic Press, 1978. Available at https://people.csail.mit.edu/rivest/pubs.html#RAD78.

[8] C. Gentry, (2009). “A Fully Homomorphic Encryption Scheme,” Doctoral Dissertation, Symposium on the Theory of Computing, NY, New York, USA, 2009.

[9] Nathan Dowlin, Ran Gilad-Bachrach, Kim Laine, Kristin Lauter, Michael Naehrig, and John Wernsing. CryptoNets: “Applying Neural Networks to Encrypted Data with High Throughput and Accuracy.” In 33rd International Conference on Machine Learning (ICML 2016), volume 48 of Proceedings of Machine Learning Research, pages 201–210. PMLR, 2016.
URL: http://proceedings.mlr.press/v48/ gilad-bachrach16.html.

[10] Florian Bourse, Michele Minelli, Matthias Minihold, and Pascal Paillier. “Fast Homomorphic Evaluation of Deep Discretized Neural Networks.” In Advances in Cryptology – CRYPTO 2018, Part III, volume 10993 of Lecture Notes in Computer Science, pages 483–512. Springer, 2018.
doi:10.1007/978-3-319-96878-0 17.

BIBLIOGRAPHY

11] Christina Boura, Nicolas Gama, Mariya Georgieva, and Dimitar Jetchev. “Simulating Homomorphic Evaluation of Deep Learning Predictions.” In Cyber Security Cryptography and Machine Learning (CSCML 2019), volume 11527 of Lecture Notes in Computer Science, pages 212–230. Springer, 2019. doi:10.1007/ 978-3-030-20951-3 20

[12] Marcelo Blatt, Alexander Gusev, Yuriy Polyakov, and Shafi Goldwasser. “Secure Large-Scale Genome-Wide Association Studies Using Homomorphic Encryption.” Cryptology ePrint Archive, Report 2020/563, 2020. https://ia.cr/2020/563.

[13] iDASH secure genome analysis competition.
http://www.humangenomeprivacy.org

JUAN PABLO RAMÍREZ

PHONE NUMBERS:

+1 (708) 945 - 4477

EMAIL AND PERSONAL PAGE:

jramirez@binaryprojx.com
www.binaryprojx.com

ADDRESS:

Guadalajara, Jalisco, México

EDUCATION

UNIVERSIDAD DE GUADALAJARA

2008 - 2011, Guadalajara, México

1. Teaching experience
2. Served in panels for designing new academic programs in Natural Sciences and Engineering
3. Speaker at International Conferences and Symposiums
4. Participation and Leadership in academic and industrial research and application programs
5. 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
6. Applied Mathematics with Dr. Alexander Yakhnov, from the Dept. of Mathematics
7. Project managing and Director of events such as workshops and "Art and Science Week"
8. Experience in software development and managing high-level to low-level language projects

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

2011 - 2013, Cd. Guanajuato, México

1. Research presented at area-specific conferences and seminars
2. Activities divulging mathematical sciences

LANGUAGES

English
Spanish
C++
Python
MySql
Java
JavaScript

RESEARCH AREAS

Mathematics

Physics

Computer Sciences

RESEARCH TOPICS

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

PARTICIPATIONS

- "Recursive Solutions for Constant Coefficient Differential Equations". Physical-Mathematical Sciences Week, Universidad de Guadalajara, 2010.
- "Axiomatic Basis for Probability". Second School on Logic and Sets, UNAM campus Morelia, 2013.
- "General Theory of Systems and Algebraic Structures". Physical-Mathematical Sciences Week, Universidad de Guadalajara, 2017.
- "A Natural Construction of Real Numbers". Physical-Mathematical Sciences Week, Universidad de Guadalajara, 2017.
- Workshop on "Mathematics and Paint". Physical-Mathematical Sciences Week, Universidad de Guadalajara, 2018.
- "Topologies of N in the Construction of R". Physical-Mathematical Sciences Week, Universidad de Guadalajara, 2018.
- Organization and Direction of "Art and Sciences Week", including workshops, conferences, roundtables and creation of Smart Mural (Universidad de Guadalajara, 2018, 2022, 2024).
- 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, 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.
- Smart Mural. Inauguration of 55 Mexican Congress of Mathematics, 2022.
- “Canonical Block Form for Finite Groups”. Algebra Special Session, 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 Special Session, 55 Mexican Congress of Mathematics, Guadalajara, Jalisco, 2022.
- “Simple Representation of Natural and Real Numbers”. Logic and Foundations Special Sessions, 55 Mexican Congress of Mathematics, Guadalajara, Jalisco, 2022.
- "A Pseudo Measure on the Space of Finite Functions and Permutations”. Algebra Special Sessions, 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 Science Special Sessions, 56 Mexican Congress of Mathematics, San Luis Potosí, 2023.
- "Simple and Linear Fast Adder of Multiple Inputs and It's Implementation for a Compute-In-Memory Architecture". International Conference on Artificial Intelligence, Computer, Data Sciences and Applications, 1-2 February 2024, Victoria-Seychelles.
- "Programming Random Change of Variables for Homomorphic Encryption". Modern Methods, Means and Technologies of Information Protection (timed to coincide with the 90th anniversary of its founder, Professor Oleg Borisovich Makarevich, on September 11-15th), Taganrog, Russia.

PUBLICATIONS

- Ramirez, J. 2024. "Programming Random Change of Variables for Homomorphic Encryption". Report on my participation in "Modern Methods, Means and Technologies of Information Protection" 2024 international conference soon available.
- Ramirez, J. 2024. "Programming Random Change of Variables for Homomorphic Encryption". Full White Paper Exclusively on Author's personal page: www.binaryprojx.com
- J. P. Ramírez, "Simple and Linear Fast Adder of Multiple Inputs and Its Implementation in a Compute-In-Memory Architecture," 2024 International Conference on Artificial Intelligence, Computer, Data Sciences and Applications (ACDSA), Victoria, Seychelles, 2024, pp. 1-11, doi: 10.1109/ACDSA59508.2024.10467957.
- Ramirez, J. “SIMPLE AND LINEAR FAST ADDER,” WIPO, Patentscope. Publication Number: WO/2023/220537. Publication Date: 16/11/2023. Applicant’s and Inventor’s name: Juan Pablo Ramirez
- Ramirez, J. 2023. "Canonical Set Theory with Applications from Matrix Operations and Data Structures to Homomorphic Encryption" Monograph Exclusively on Author's personal home page: www.binaryprojx.com
- J. P. Ramírez. "A New Set Theory for Analysis," Axioms. 2019. 8, no. 1: 31. https://doi.org/10.3390/axioms8010031. Cited by Lovyagin (2021) on the topic of Finite Arithmetic and Non-Standard Analysis for Hyperrationals with Applications to AI.
- 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
- Ramirez, J. 2015. Systems and Categories. arXiv:1509.03649v5 [math.CT]

CURRENT PROJECTS

Currently, I am seeking to develop some critical applications, of the mathematical framework I propose, in computer sciences at a software and hardware level ranging from significant optimizations in the representations of numbers and operations, to the algorithms that process and share confidential data.

I am founder of a Research and Development startup, "OPERACIONES DIGITALES Y PROCESAMIENTO INTEGRAL DE DATOS ENCRIPTADOS, SAS" incorporated in Mexico, that studies and integrates mathematical efficiency from a new standpoint that is proving to yield numerous advantages across applications in natural sciences, mathematics and computer sciences.

My current main goals are to establish collaboration and partnering for continuing development on industry level applications, which include a patent for a Simple and Linear Fast Adder that has a scalable design with constant topological complexity and linear growth with respect to the number of input bits. Another direct application of my research includes an encryption scheme that allows encrypted data to be processed, without decrypting it first, which has numerous applications including AI training with sensitive data.