PROGRAMMING RANDOM CHANGE OF VARIABLES FOR HOMOMORPHIC ENCRYPTION

XV International Scientific and Practical Conference Named After O.B. Makarevich. *“Modern Methods, Means and Technologies of Information Protection”*

J. P. Ramírez

September 13, 2024. Tangarog, Russia.

TABLE OF CONTENTS

INTRODUCTION

CANONICAL SET THEORY

A solution has been proposed that helps to simultaneously solve two problems in the foundations of mathematics.

- Benacerraf's Identification Problem
- Hilbert's 24-th Problem

We propose a construction of $\mathbb{N}$ and $\mathbb{R}$ that allows for simple proofs of their structures and such that $\mathbb{R}$ is a natural extension of $\mathbb{N}$.

Benacerraf's Identification Problem asks if there exists a canonical representation of natural numbers as sets and even questions whether numbers are sets at all if they cannot be canonically described as sets.

Hilbert's 24-th problem

Hilbert's 24-th Problem asks under what conditions can there exist a logical and axiomatic base for mathematics that maximizes proof simplicity. In his own words: "The 24-th problem in my Paris lecture was to be: Criteria of simplicity, or proof of the greatest simplicity of certain proofs. Develop a theory of the method of proof in mathematics in general. Under a given set of conditions there can be but one simplest proof."

PROBLEMS WITH ML

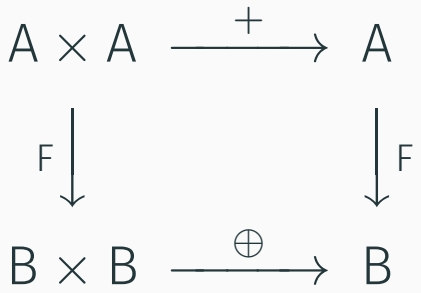
Two main issues with large scale data sharing and computing are especially related to ML and other arithmetic intensive processes.

Closing the Encryption Gap. End-to-end encryption ensures data privacy at rest and in transit. However, processing encrypted data requires for the data to be decrypted before it is processed.
We propose a Random Change of Variables to execute encrypted operations.

Von Neumann Bottleneck. The Von Neumann Architecture separates a processing unit's internal memory registers and Arithmetic Logic Unit, leading to the Von Neumann Bottleneck that is responsible for most of the energy and time consumption.
Addition and multiplication algorithms are possible whose implementation minimize circuit topology, and time, complexity [1,2].

CURRENT STANDARDIZATION OF HE

In terms of commutative diagrams a Homomorhism F is a function that commutes with two operations $+, \oplus$. That is, $F(x + y) = Fx \oplus Fy$.



We have two main approaches to finding HE schemes.

Cryptographic Way consists of starting with a well established cryptographic assumption and seeing if it is homomorhpic with a function or family of functions, or by trying to make it homomorphic.
It was first discovered that some encryption functions were homomorphic with an arithmetical operation [3].

Mathematicians Way which starts from a homomorphism and attempts to build security by introducing “noise”.

DEFICIENCIES OF CURRENT HE SCHEMES

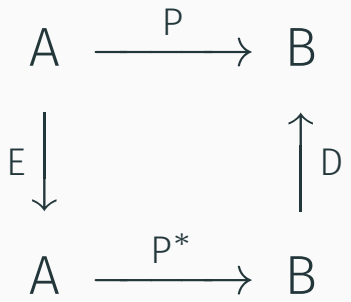
Current HE schemes are much better than 2009 when Gentry proposed the first FHE scheme. However, noise mitigation is still a central factor that accounts for the majority of time and energy consumption which makes HE in viable in many critical applications. The benchmark technique for efficiency of traditional HE schemes is usually in the form of a ‘Bootstrapping’ method to manage noise.

RANDOM CHANGE OF VARIABLES

RANDOM CHANGE OF VARIABLES

Random Change Of Variables (Uses no Homomorphisms). We choose a random change of coordinates. Instead of not knowing the key, in this case the second party does not know what change of variables has been applied to the variables, but knows what function to apply that will cancel the encryption and simultaneously process as desired.

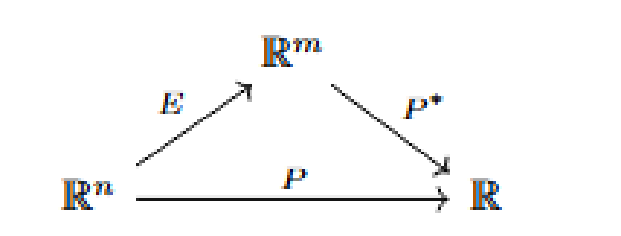
Let us start with a commutative diagram that illustrates the relation between evaluating a function P in plaintext, and evaluating an equivalent function P* in ciphertext.



(1)

RANDOM CHANGE OF VARIABLES

If we consider P* to be D∘P* as a single function, the resulting relation is $P = P' \circ E$. If, given an encryption function $E : R^n \to R^m$ we can find a computable function $P' : R^m \to R$ such that $P = P^* \circ E$, then we have an encryption scheme for process P.



A reasonably calibrated model for loan approvals based on a client's financial data (income, capital, debt, expenses, etc.) is proposed. Parameters can be modified to adapt the Credit Score model to different scenarios (different types of loans such as micro loan, business loan, loan period, interest, etc.). The proposed processing function P for this model is

$$\mathrm{P}(\mathrm{NI}, \mathrm{TE}, \mathrm{W}, \mathrm{TD}) = \frac{\mathrm{A} \cdot \mathrm{NI}}{\sqrt{\mathrm{NI}^2 + \alpha \mathrm{TE}^2}} + \frac{\mathrm{B} \cdot \mathrm{W}}{\sqrt{\mathrm{W}^2 + \beta \mathrm{TD}^2}}.$$

We generate encrypted variables

$$E\begin{bmatrix} NI & W \\ TE & TD \end{bmatrix} = \begin{bmatrix} K_1 NI + K_2 & K_4 W + K_5 \\ K_3\sqrt{NI^2 + \alpha TE^2} & K_6\sqrt{W^2 + \beta TD^2} \\ \frac{K_2}{K_3\sqrt{NI^2+\alpha TE^2}} & \frac{K_5}{K_6\sqrt{W^2+\beta TD^2}} \\ \frac{K_3}{K_1} & \frac{K_6}{K_4} \end{bmatrix}$$

where the K_i are keys of the desired bit length. *Can't solve for the keys. The function that decrypts and simultaneosuly processes the data is given by $P(NI, TE, W, TD) = 8EV_4^1\left(\frac{EV_1^1}{EV_2^1} - EV_3^1\right) + 2EV_4^2\left(\frac{EV_1^2}{EV_2^2} - EV_3^2\right)$.

CONCLUSIONS

CONCLUSIONS

Suppose we have a library of k different encryption functions $\{E_j\}_{j=1}^{k}$, of a given processing function P. If the client encrypts the variables using E_i, for some $E_i \in \{E_j\}_j$, then the encrypted variables will have to be processed with the corresponding processing function P_j^*. Furthermore, the codimension of E_j can be different from another encryption functions codimension.

It is possible to implement a randomized selection of the encryption functions that adds an extra layer of security.

FINAL REMARKS

Other applications include a Fast Derivative Approximation that can be performed with the SLFA. State-of-the-art Homomorphic Encryption can be merged together with the arithmetic architecture for designing Encrypted Processing Units. A range of challenges for HE can be solved in this model, including a version of Homomorphic Encryption that merges the Processing and the Decryption steps, into a single step. Additional description of these applications, among others in Computer Science and Mathematics, is available at my Homepage

www.binaryprojx.com
jramirez@binaryprojx.com

Thank You!