Research Proposal

Waajacu: Santiago Restrepo Ruiz.

June 15, 2023

Conflicto armado, paz negociada y posconflicto.

1 Prefacio

Se necesita conocer los siguientes dos conceptos ténicos centrales:

(**ZKP**) Pruebas de Conocimiento Cero (Zero-Knowledge Proofs).

(**COOPERACION HOMOMÓRFICA**) Computación Homomórfica.

2 Sinopsis

Se define una estrategia de cooperación entre *entidades* interactivas en conflicto. Que trabajan en pro de un objetivo común: de naturaleza sensible, privada y/o de levantamiento armado con raices irresolubles.

La extrategia a desarrollar utiliza Pruebas de Conocimiento Cero para permitir a las *entidads* observar a sus contrapartes sin que aquellas o estas se vean obligadas a revelar sus ventajas competitivas.

De manera simultánea, se define la Cooperación Homomórfica.

La Mátemática de lo que es necesario ya está resuelta, compete a la ciencia politica lo siguiente. **waajacu.com** se compromete a liberar con licencia libre los algoritmos necesarios, y a fabricar versiones utilizables en lenguaje de Ensamblador.

Esta investigación es importante porque busca la reducción del conflicto. Instar a las partes malintencionadas a comportarse de manera justa (ZKP) y cooperar en pro de un objetivo común (Homomorfismos).

3 Pregunta de investigacion

”¿Cómo se puede diseñar e implementar una estrategia basada en Pruebas de Conocimiento Cero y Computación Homomórfica para permitir la cooperación entre entidades en conflicto, salvaguardando la privacidad y ventajas competitivas de cada una, y promoviendo un objetivo común?”

4 Planteamiento del problema

El constante conflicto entre entidades, ya sea en el ámbito político, económico, social o militar, ha creado una necesidad crítica de estrategias de cooperación que permitan trabajar hacia un objetivo común sin comprometer la seguridad, la privacidad y las ventajas competitivas de cada parte. Sin embargo, existe un desafío significativo en la implementación de tales estrategias, principalmente en la capacidad para cooperar y verificar la cooperación de cada entidad sin revelar información.

5 Objetivos

Objetivo General:

- Desarrollar una estrategia basada en Pruebas de Conocimiento Cero (ZKP) y Computación Homomórfica para permitir la cooperación entre entidades en conflicto sin comprometer su privacidad ni sus ventajas competitivas, y promover la consecución de un objetivo común.

Objetivos Específicos:

- Diseñar un marco teórico para una estrategia que integre el uso de ZKP y Computación Homomórfica para la cooperación en contextos conflictivos.
- Traducir este marco teórico en algoritmos utilizables y liberarlos con licencia libre.
- Implementar estos algoritmos en lenguaje de Ensamblador y validar su funcionamiento en situaciones de prueba.

6 Lineamientos

Lineamientos Teóricos:

- Pruebas de Conocimiento Cero (ZKP): Estudiaremos las teorías y aplicaciones de las ZKP, en particular cómo se pueden utilizar para verificar la información sin revelar los detalles subyacentes. Se explorará tanto la teoría matemática como las aplicaciones prácticas.

- Computación Homomórfica: Se investigará la teoría y práctica de la computación homomórfica, centrándose en cómo permite las operaciones en datos cifrados, y su relevancia para la cooperación entre entidades que desean mantener la privacidad de su información.

- Cooperación y Conflicto: Se revisarán las teorías y modelos de conflicto y cooperación, con un enfoque especial en el papel de la privacidad y las ventajas competitivas en la interacción entre entidades. También se explorará la literatura existente sobre estrategias de cooperación en situaciones de conflicto.

Lineamientos Metodológicos:

- Análisis Teórico: Realizaremos un análisis detallado de las teorías y principios subyacentes a las ZKP, la computación homomórfica y la cooperación en conflictos. Esto involucrará la revisión de literatura académica y técnica relevante.

- Diseño de Algoritmos: Basándonos en nuestro análisis teórico, diseñaremos algoritmos que implementen nuestra estrategia de cooperación. Estos algoritmos serán desarrollados de manera que puedan ser liberados con licencia libre.

- Implementación en Ensamblador: Implementaremos los algoritmos diseñados en lenguaje de ensamblador. Esta implementación será realizada teniendo en cuenta la optimización y eficiencia del código.

- Análisis de Impacto: Examinaremos el potencial impacto de la estrategia en la cooperación entre entidades en conflicto, analizando

la literatura existente y utilizando métodos cualitativos y cuantitativos según sea apropiado.

7 Bibliografía

References

[1] Goldwasser, Shafi, Silvio Micali, and Charles Rackoff, *The Knowledge Complexity of Interactive Proof Systems*. SIAM Journal on Computing, vol. 18, no. 1, pp. 186-208, 1989.

[2] Gentry, Craig, *A Fully Homomorphic Encryption Scheme*. PhD thesis, Stanford University, 2009.

[3] Hyde, Randall, *The Art of Assembly Language*. No Starch Press, 2nd edition, 2010.