Trabajo de fin de grado

Implementación de protocolos de conocimiento cero con fines docentes

---

Autor: Pedro Ramos Suárez
Doble Grado en Ingeniería Informática y Matemáticas

Tutor: Rafael Alejandro Rodríguez Gómez
Departamento de Teoría de la Señal, Telemática y Comunicaciones

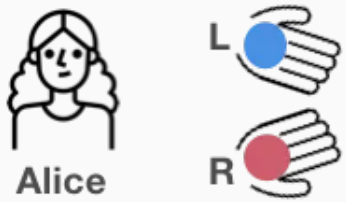
3 de julio de 2023

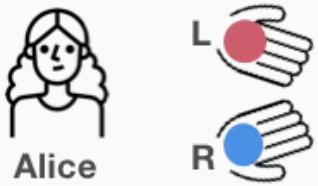
Facultad de Ciencias

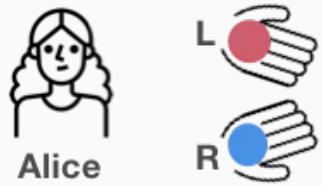
Índice

Motivación

Introducción







[6] Understanding Zero-Knowledge Proofs through Simple Examples.

Motivación

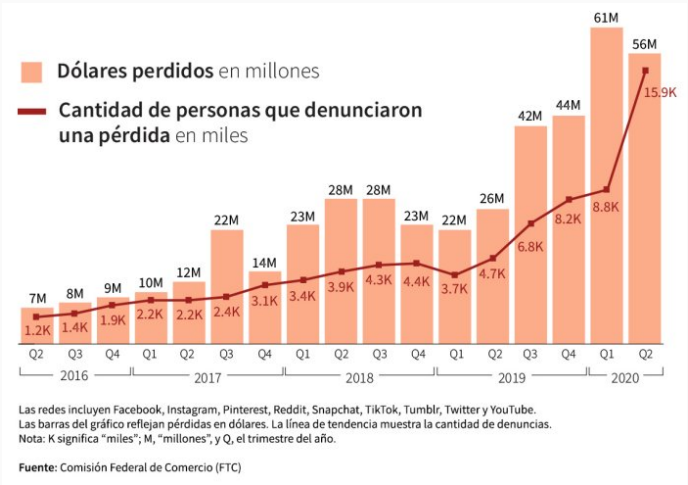


Figura 1: Fraudes [8]

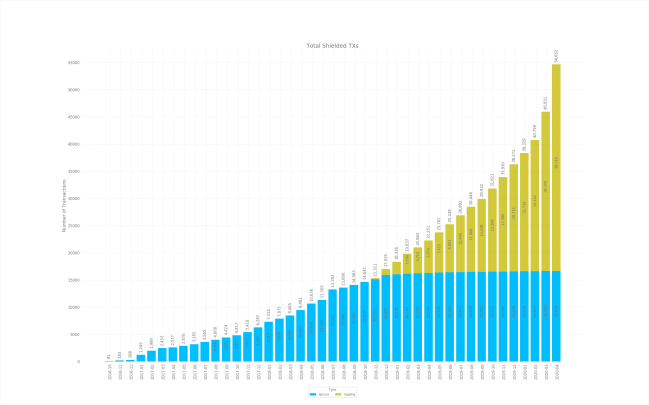


Figura 2: Zcash [9]

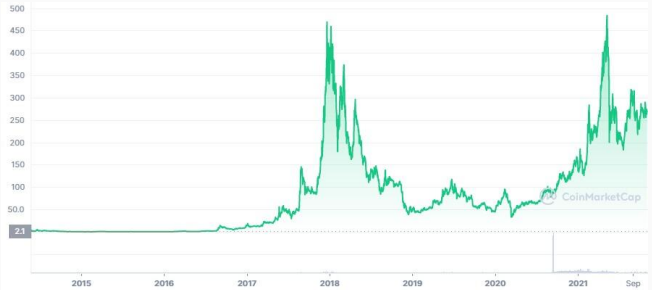


Figura 3: Monero [10]

[8] Se Disparan Los Fraudes En Instragram Por La Pandemia.

[9] Zcash Privacy Remains Strongest of Any Cryptocurrency, Even with Recent Chainalysis, Elliptic Support

[10] Monero (XMR) Price Prediction for 2023, 2024-2025 and Beyond

Aplicaciones

- Pagos anónimos.
- Autenticación.
- Más de 18 ZKRP.
- Know Your Customer (KYC).
- Evaluación del riesgo hipotecario.
- Calificación y grado de inversión.
- Voto electrónico.
- Subastas y adquisiciones electrónicas.

Protocolos de conocimiento cero en el contexto docente

Existencia de diversos artículos, pero todos centrados en su funcionamiento o en comparar diversos algoritmos:

- *Efficient Proofs that a Committed Number Lies in an Interval* [1]
- *A Survey on Zero Knowledge Range Proofs and Applications* [2]
- *Sharp: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* [3]
- *Bulletproofs: Short proofs for confidential transactions and more* [17]

Objetivos

Implementación de una herramienta que facilite el estudio de las pruebas de conocimiento cero.

Para ello, queremos:

- Conocer el funcionamiento y algunas de las posibles aplicaciones de los protocolos de conocimiento cero.
- Desarrollar una herramienta que permita al usuario experimentar con los protocolos de conocimiento cero.
- Verificar el funcionamiento correcto se espera de dichos algoritmos.

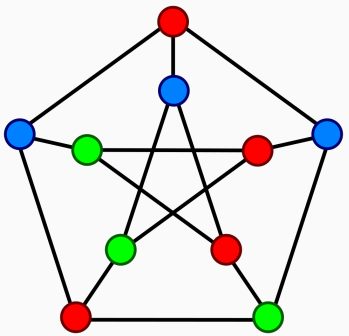
Teoría

Marco histórico

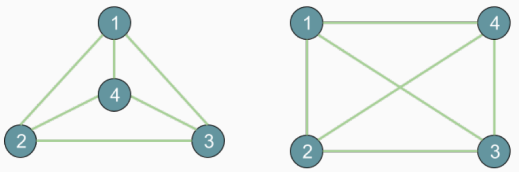
Concebidas por primera vez en 1985 por Shafi Goldwasser, Silvio Micali y Charles Rackoff en el artículo *The Knowledge Complexity of Interactive Proof-Systems* [12].

> *De particular interés es el caso donde [...] mostramos que es posible probar interactivamente que un número es cuadrático sin residuo mod m liberando 0 conocimiento adicional.*

Oded Goldreich, Silvio Micali y Avi Wigderson demostraron que se puede crear un sistema de prueba de conocimiento cero para el problema de coloreado de gráficos NP completos con tres colores.



También demostraron que el problema de no isomorfismo de gráficos, el complemento del problema de isomorfismo de gráficos, tiene una prueba de conocimiento cero.



Definición

Una prueba de conocimiento cero permite probar la verdad de una declaración sin compartir el contenido de la declaración o revelar cómo descubrió la verdad.

- **Completitud:** Si la entrada es válida, el protocolo de conocimiento cero siempre devuelve "verdadero".
- **Solidez:** Si la entrada no es válida, es teóricamente imposible engañar al protocolo de conocimiento cero para que devuelva "verdadero".
- **Conocimiento cero:** El verificador no aprende nada sobre una declaración más allá de su validez o falsedad.

Definición

Dado $x \in \mathcal{L}$, el probador es capaz de convencer a un verificador de que x pertenece a $\mathcal{L}$, es decir, existe un testigo w para x.

- **Setup:** Generación de parámetros: $params = \text{Setup}(\lambda)$.
- **Prove:** Genera la prueba de conocimiento cero: $proof = \text{Prove}(x, w)$
- **Verify:** Acepta o rechaza la prueba *proof*.

Con estos términos, una prueba de conocimiento cero cumple:

- **Completitud:**

$$Verify(Prove(x, w)) = 1$$

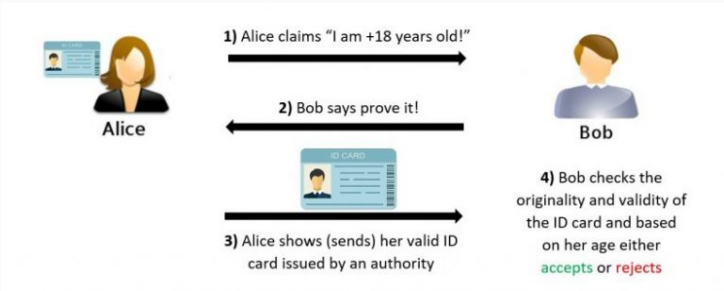
- **Solidez:**

$$P[Verify(Prove(x, w)) = 1] \text{ es suficientemente baja.}$$

- **Conocimiento cero:** El verificador no aprende nada sobre una declaración más allá de su validez o falsedad.

Pruebas interactivas y no interactivas

Pruebas interactivas



Pruebas no interactivas

Requieren sólo una ronda de comunicación entre los participantes (proveedor y verificador).

Una vez que se genera una prueba, está disponible para que cualquier otra persona (con acceso al algoritmo de verificación) la verifique.

[13] CO6GC: Introduction to Zero-Knowledge Proofs (Part 1)

ZK-SNARK y ZK-STARK

ZK-SNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge):

- **Conocimiento cero:** Un verificador puede validar la integridad de una declaración sin saber nada más sobre la declaración.
- **Sucinto:** La prueba de conocimiento cero es más pequeña que el testigo y se puede verificar rápidamente.
- **No interactivo**: La prueba es no interactiva porque el probador y el verificador solo interactúan una vez.
- **Argumento:** La prueba satisface el requisito de solidez.
- **De conocimiento:** La prueba de conocimiento cero no puede construirse sin acceso a la información secreta.

ZK-STARK (Zero-Knowledge Scalable Transparent Argument of Knowledge):

- **Escalable:** Es más rápido que ZK-SNARK en la generación y verificación de pruebas cuando el tamaño del testigo es mayor.
- **Transparente:** Se basa en la aleatoriedad verificable públicamente para generar parámetros.

Zero Knowledge Range Proof

Permiten probar que un valor entero secreto pertenece a un intervalo.

- Propuestas de representación entera:
  - **Descomposición cuadrada (Square decomposition):** Para probar que $x \in [a, b]$ es equivalente probar que $x - a \geq 0$ y que $b - x \geq 0$.
  - **Basado en firma (Signature-based)**.
- Propuestas de representación binaria:
  - **Decomposición multi-base (Multi-base decomposition):** Utiliza aritmética booleana.
  - **Compromisos homomórficos de dos niveles (Two-tiered homomorphic commitments):** Utiza *batches* de elementos de $\mathbb{Z}_p$.
  - **Bulletproofs:** El probador convence a un verificador de que conoce vectores cuyo producto interno es igual a un valor público determinado.

Descomposición cuadrada (Square Decomposition)

Sea un entero positivo x, y sea $E = g^x h^r \pmod{n}$, y supongamos que se quiere probar que $x \in [a, b]$.

Se escribe el entero positivo $x - a$ como la suma del cuadrado mayor menor que x, x_1^2, y de ρ, un número positivo. Luego se selecciona aleatoriamente $r_1, r_2 \in [0, 2^s n - 1]$ de modo que $r_1 + r_2 = r$, y se calculan:

$$E_1 = g^{x_1^2} h^{r_1} \pmod{n} \qquad \text{y} \qquad E_2 = g^{\rho} h^{r_2} \pmod{n}$$

Por lo tanto:

$$E_1 E_2 = g^{x_1^2 + \rho} h^{r_1 + r_2} \pmod{n} = g^{x-a} h^r \pmod{n} \qquad \text{y} \qquad x - a \geq 0$$

Demostrando que E_1 oculta un cuadrado y que E_2 oculta un número menor que $2^{t+\ell+1}\sqrt{b-a}$, y aplicando el mismo método para $b - x$, se prueba que:

$$x \in [a - 2^{t+\ell+1}\sqrt{b-a}, b + 2^{t+\ell+1}\sqrt{b-a}]$$

Teorema extendido de Euclides

$$mcd(a, b) = r_n$$

	a	1	0
	b	0	1
q_2	r_3	$u_3 = 1 - 0 \cdot q_2$	$v_3 = 0 - q_2 \cdot 1$
$\dots$	$\dots$	$\dots$	$\dots$
q_{i-2}	r_{i-1}	u_{i-1}	v_{i-1}
q_{i-1}	r_i	u_i	v_i
q_i	r_{i+1}	$u_{i+1} = u_{i-1} - u_i \cdot q_i$	$v_{i+1} = v_{i-1} - q_i \cdot v_i$
$\dots$	$\dots$	$\dots$	$\dots$

Tabla 1: Algoritmo extendido de Euclides

$$1 = mcd(a, n) = u \cdot a + v \cdot n \equiv u \cdot a (\text{mod } n)$$

Pruebas y verificaciones

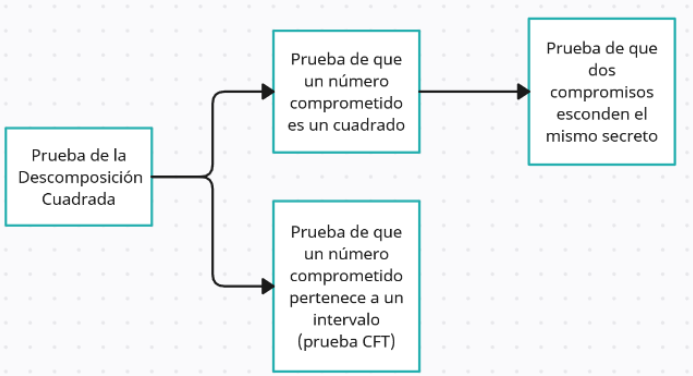


Figura 4: Esquema de pruebas

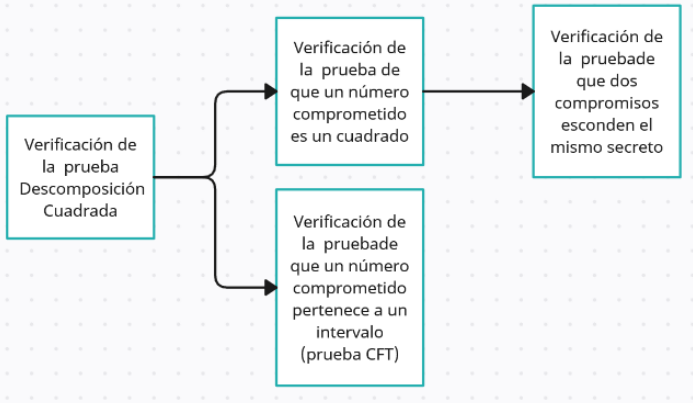
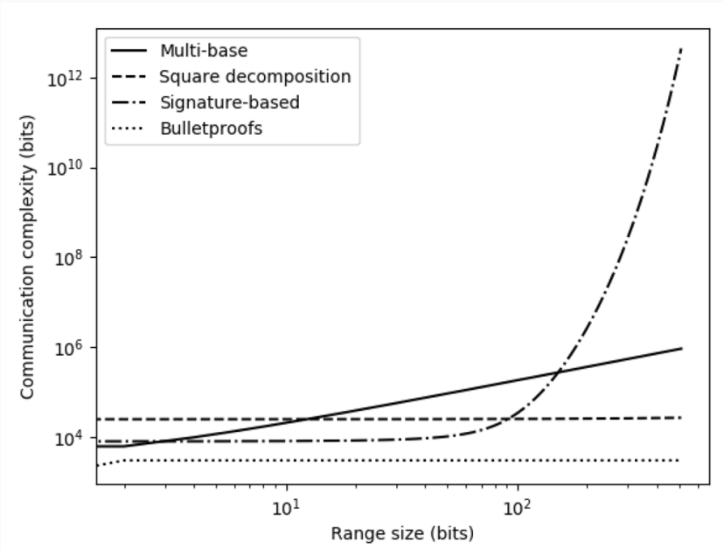
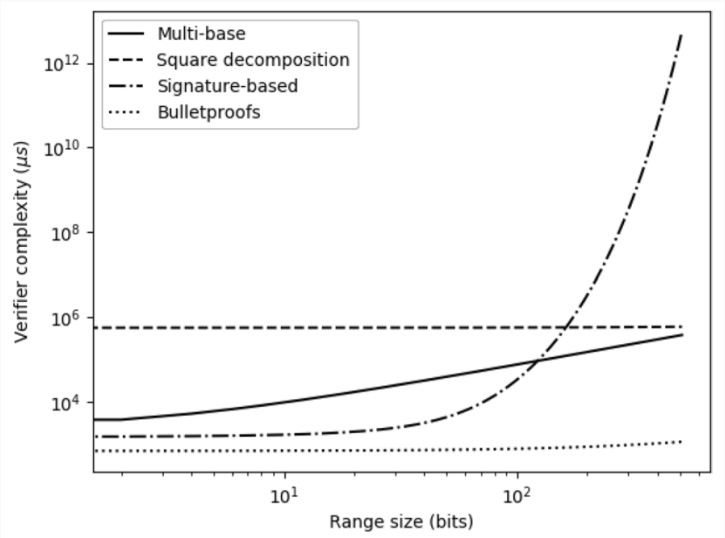
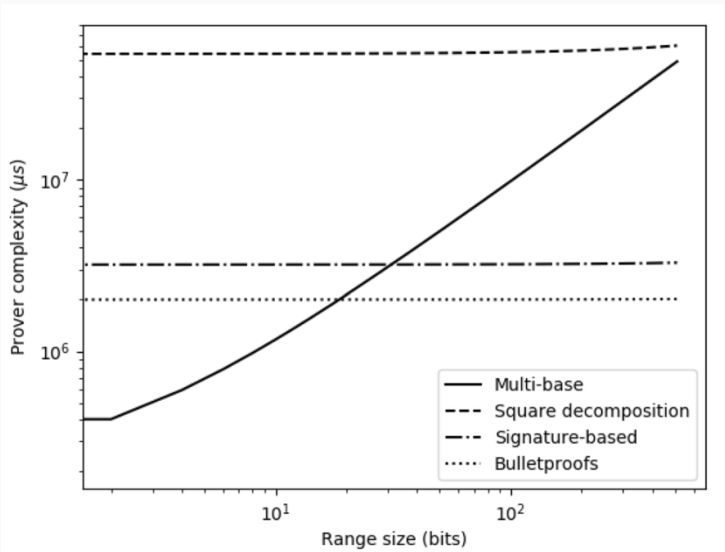


Figura 5: Esquema de verificaciones

Selección de algoritmo







[2] A Survey on Zero Knowledge Range Proofs and Applications - SN Applied Sciences.

Bulletproofs vs Sharp

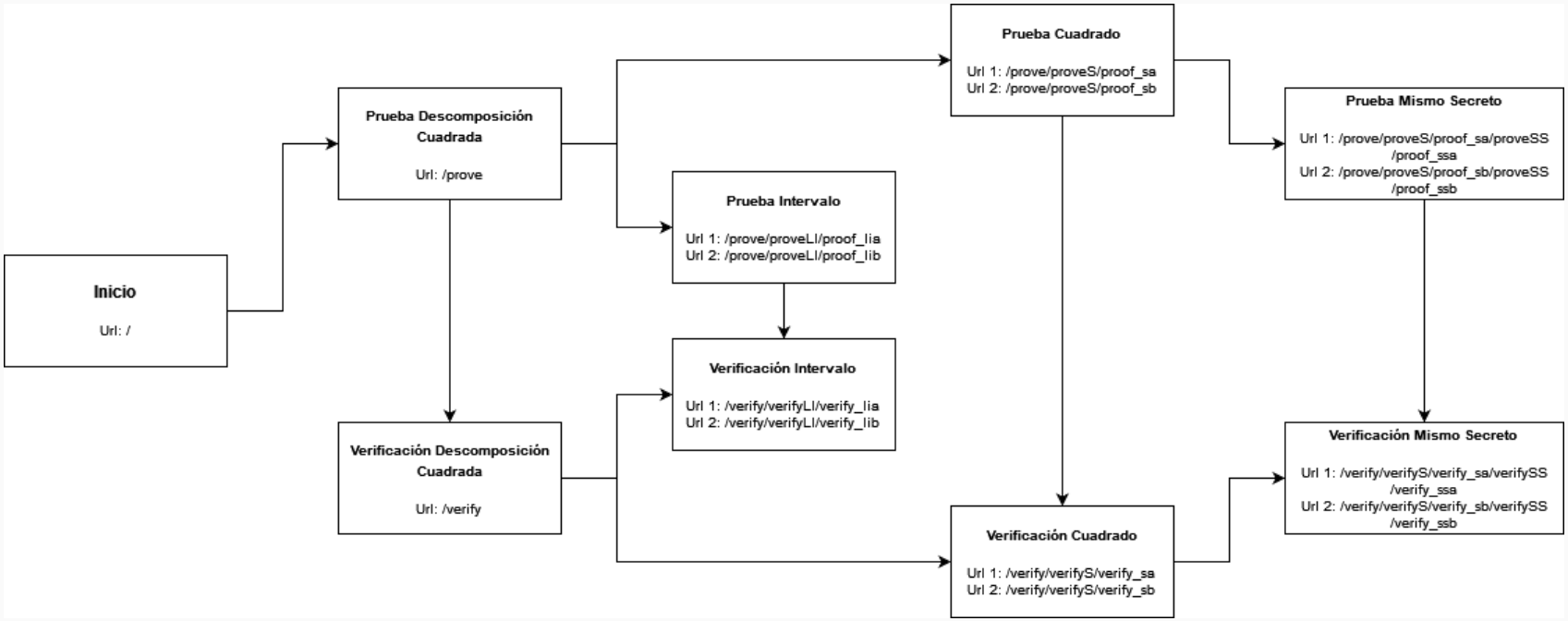
		Bulletproofs		$\text{Sharp}_{\text{SO}}^{\text{Po}}$	
$(\lambda, \log B)$	N	Prover's work	Verifier's work	Prover's work	Verifier's work
128, 64	1	20.6	2.55	1.17	0.75
	8	157	12.1	7.47	3.88
128, 32	1	10.5	1.46	0.97	0.74
	8	80.0	6.93	6.74	3.39

[3] Sharp: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security.

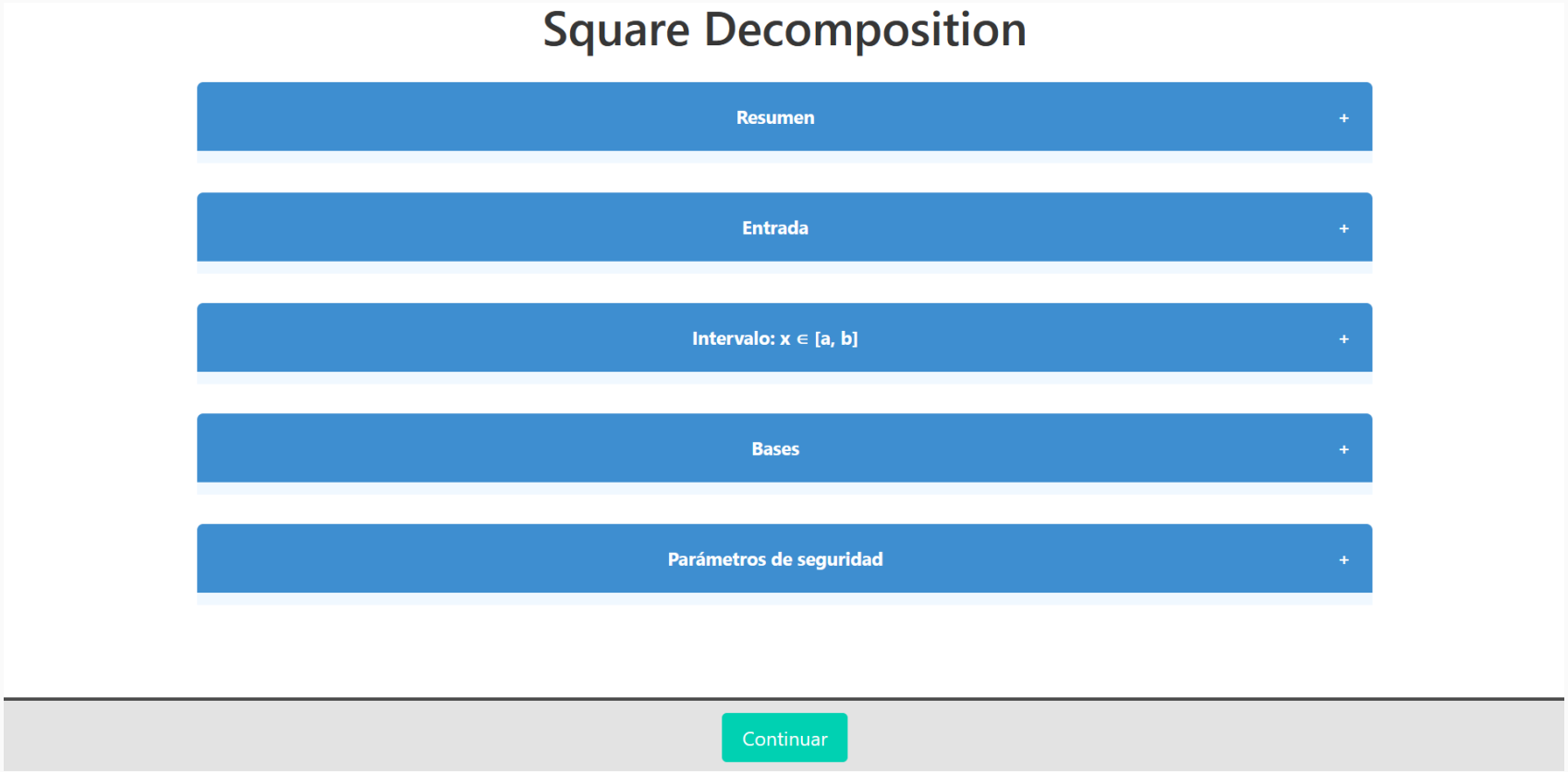
Implementación

Implementación

Esquema de la interfaz web



Interfaz web



Pruebas funcionales

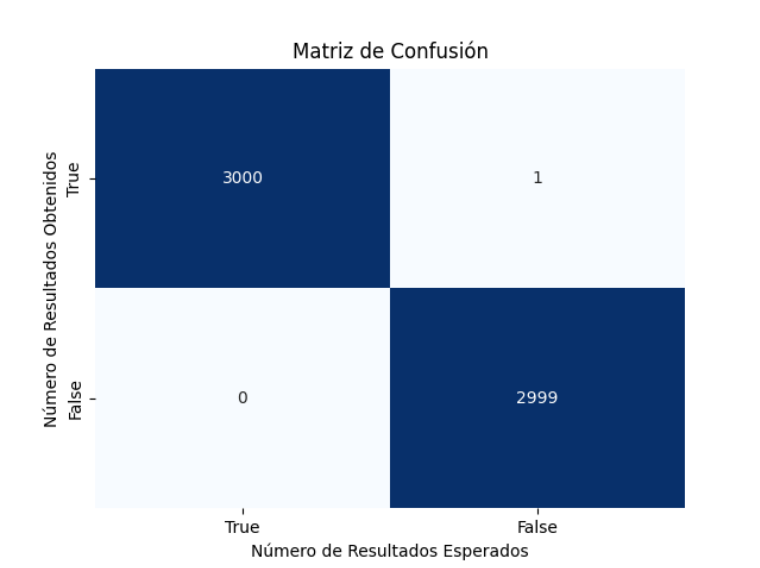


Figura 6: Resultados de una ejecución

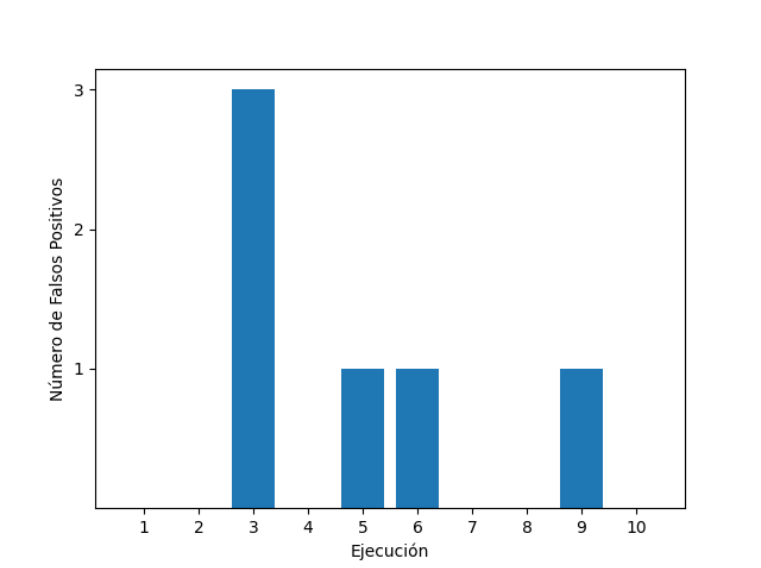
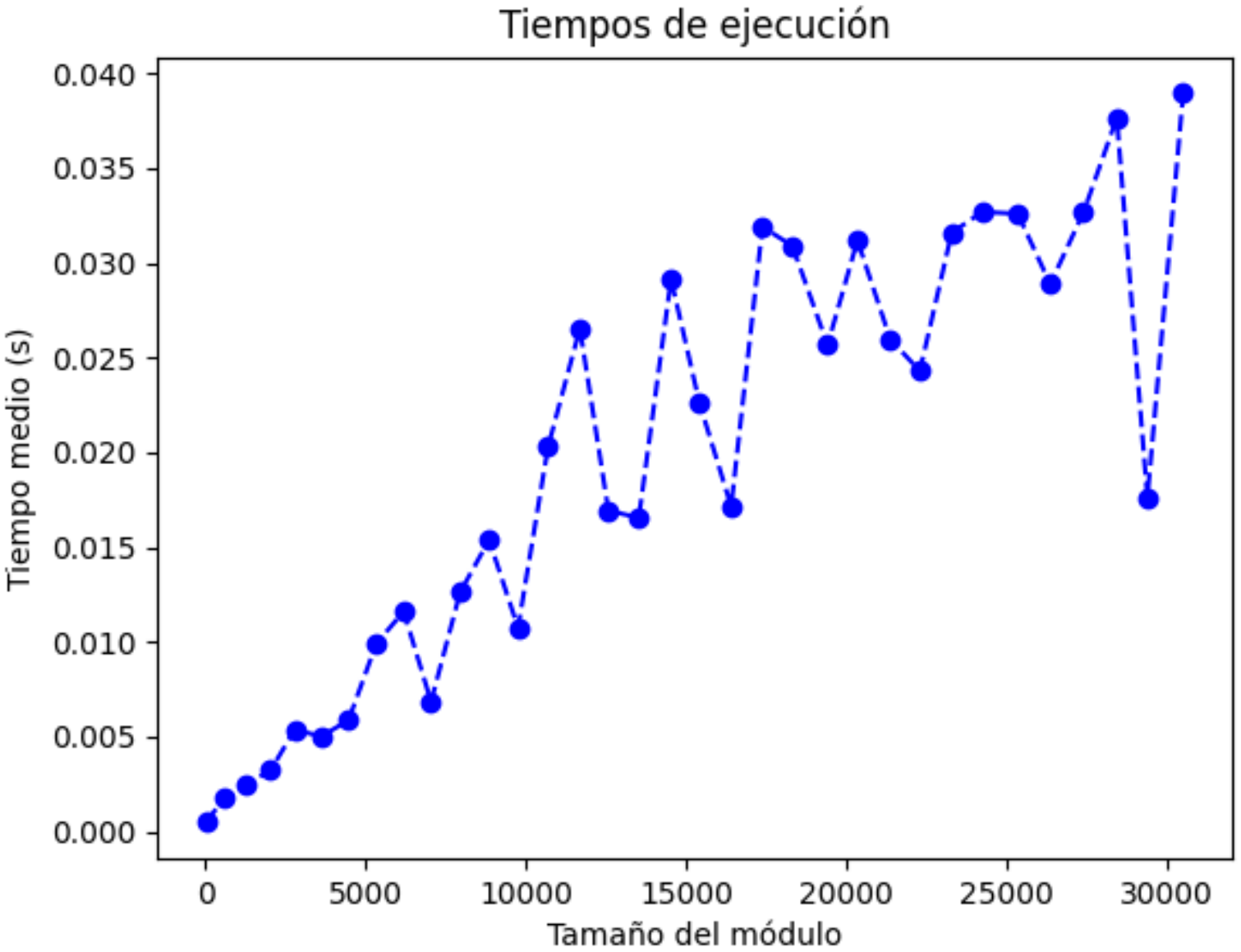
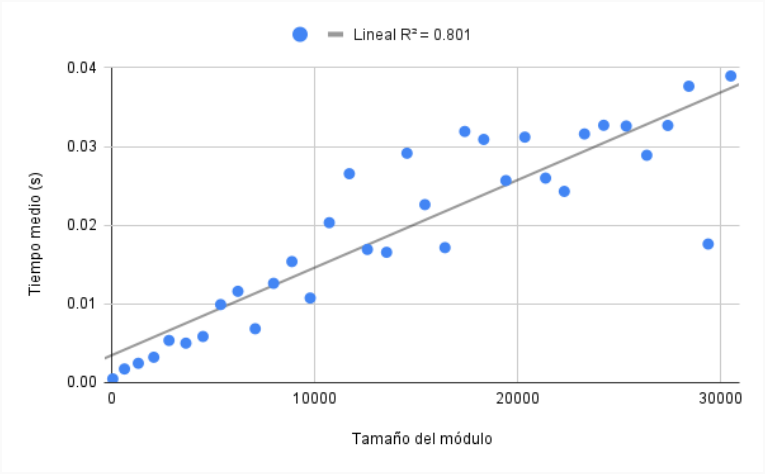


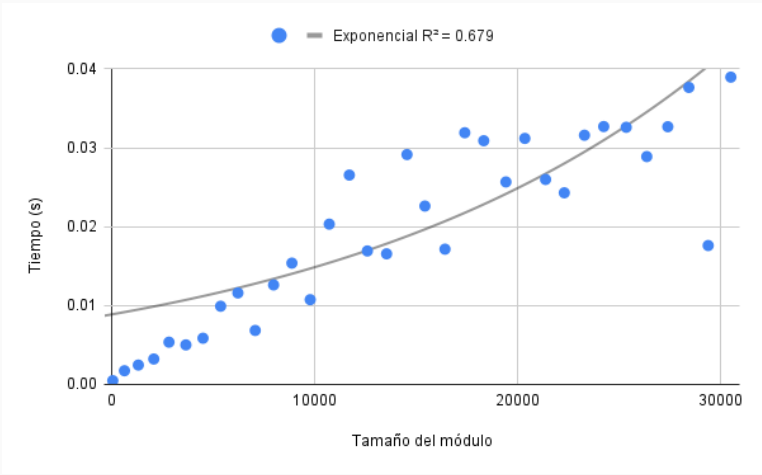
Figura 7: Resultados de 10 ejecuciones

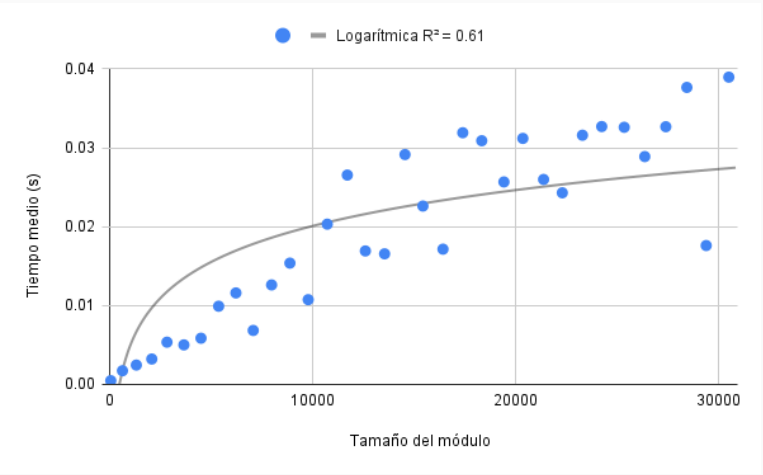
Tiempo de verificación



Regresión


Lineal R² = 0.801
Tiempo medio (s)
0.04
0.03
0.02
0.01
0.00
0
10000
20000
30000
Tamaño del módulo


Exponencial R² = 0.679
Tiempo (s)
0.04
0.03
0.02
0.01
0.00
0
10000
20000
30000
Tamaño del módulo


Logarítmica R² = 0.61
Tiempo medio (s)
0.04
0.03
0.02
0.01
0.00
0
10000
20000
30000
Tamaño del módulo

Conclusiones y Líneas de Trabajo Futuro

Conclusiones

Con este trabajo se han logrado los siguientes objetivos:

- Estudio de los protocolos de conocimiento cero.
- Comparación entre los distintos algoritmos.
- Estudio en detalle del algoritmo de la Descomposición Cuadrada.
- Implementación del algoritmo.
- Desarrollo de una herramienta docente.
- Pruebas funcionales.

Líneas de Trabajo Futuro

- Estudiar otros algoritmos ZKP.
- Solucionar las pruebas falsas clasificadas como verdaderas.
  - Errores debidos a la tolerancia.
  - Errores debidos a la aleatoriedad.

Referencias i

[1] Fabrice Boudot. "Efficient Proofs that a Committed Number Lies in an Interval", n.d. https://www.iacr.org/archive/eurocrypt2000/1807/18070437-new.pdf.

[2] Eduardo Morais, Tommy Koens, Cees van Wijk, and Aleksei Koren. "A Survey on Zero Knowledge Range Proofs and Applications - SN Applied Sciences." SpringerLink, July 31, 2019. https://link.springer.com/article/10.1007/s42452-019-0989-z.

[3] Geoffroy Couteau, Dahmun Goudarzi, Michael Klooß, and Michael Reichle. "Sharp: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security." ACM Conferences, November 1, 2022. https://dl.acm.org/doi/10.1145/3548606.3560628.

[4] Johann Engelbrecht, Salvador Llinares, and Marcelo C. Borba. "Transformation of the Mathematics Classroom with the Internet - ZDM – Mathematics Education." SpringerLink, June 26, 2020. https://link.springer.com/article/10.1007/s11858-020-01176-4.

Referencias ii

[5] Pranathi Rayavaram, Sreekriti Sista, Ashwin Jagadeesha, Justin Marwad, Nathan Percival, Sashank Narain, and Claire Seungeun Lee. "Designing a Visual Cryptography Curriculum for K-12 Education." IEEE, February 22, 2023. https://ieeexplore.ieee.org/abstract/document/10125191.

[6] 0xSage. "Understanding Zero-Knowledge Proofs through Simple Examples." Medium, May 12, 2019. https://blog.goodaudience.com/understanding-zero-knowledge-proofs-through-simple-examples-df673f796d99.

[7] Lupita. "Genuino Cloud: Correo Electrónico Corporativo." Genuino Cloud — Correo electrónico corporativo, December 6, 2020. https://genuinocloud.com/blog/3-consejos-para-proteger-tu-identidad-en-internet/.

[8] Katherine Skiba. "Se Disparan Los Fraudes En Instragram Por La Pandemia." AARP, November 4, 2020. https://www.aarp.org/espanol/dinero/estafas-y-fraudes/info-2020/se-disparan-los-enganos-en-redes-sociales-por-pandemia.html.

Referencias iii

[9] Electric Coin Company. "Zcash Privacy Remains Strongest of Any Cryptocurrency, Even with Recent Chainalysis, Elliptic Support." Electric Coin Company, September 23, 2020. https://electriccoin.co/blog/zcash-privacy-remains-strongest-of-any-cryptocurrency/.

[10] Jana Kane. "Monero (XMR) Price Prediction for 2023, 2024-2025 and Beyond." LiteFinance, January 9, 2023. https://www.litefinance.org/blog/analysts-opinions/monero-price-prediction-forecast/.

[11] Juan Fornell. "¿Qué Es Zero Knowledge Protocol (ZKP)?" Bit2Me Academy, May 4, 2023. https://academy.bit2me.com/zkp-zero-knowledge-protocol/.

[12] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. "The Knowledge Complexity of Interactive Proof-Systems", February 1989. https://people.csail.mit.edu/silvio/Selected%20Scientific

[13] Karim Baghery. "CO6GC: Introduction to Zero-Knowledge Proofs (Part 1)." COSIC, June 8, 2022. https://www.esat.kuleuven.be/cosic/blog/co6gc-introduction-to-zero-knowledge-proofs-1/.

Referencias iv

[14] Cointelegraph Research. "Pushing Bitcoin to Become More Scalable with Zero-Knowledge Proofs." Cointelegraph, August 17, 2022. https://cointelegraph.com/news/pushing-bitcoin-to-become-more-scalable-with-zero-knowledge-proofs.

[15] Paul Razvan. "ZK-SNARKs vs. ZK-Starks vs. BulletProofs? (Updated)." Ethereum Stack Exchange, March 5, 2019. https://ethereum.stackexchange.com/questions/59145/zk-snarks-vs-zk-starks-vs-bulletproofs-updated.

[16] "Zero-Knowledge Proofs." ethereum.org, n.d. https://ethereum.org/en/zero-knowledge-proofs/.

[17] Cathie Yun. "Building on Bulletproofs." Medium, July 11, 2021. https://cathieyun.medium.com/building-on-bulletproofs-2faa58af0ba8.

[18] Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. "Bulletproofs: Short proofs for confidential transactions and more", n.d. https://eprint.iacr.org/2017/1066.pdf.

Referencias v

[19] Boneh, Dan, Ben Lynn, and Hovav Shacham. "Short Signatures from the Weil Pairing." SpringerLink, November 20, 2001. https://link.springer.com/chapter/10.1007/3-540-45682-1_30.

[20] Brown, Daniel R. L. "Sec 2: Recommended elliptic curve domain parameters." January 27, 2010. https://www.secg.org/sec2-v2.pdf.

[21] "Elliptic Curve Cryptography (ECC)." Elliptic Curve Cryptography (ECC) - Practical Cryptography for Developers, n.d. https://cryptobook.nakov.com/asymmetric-key-ciphers/elliptic-curve-cryptography-ecc.

[22] Torben Pryds Pedersen. "Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing." SpringerLink, 1992. https://link.springer.com/chapter/10.1007/3-540-46766-1_9.

[23] "Zero-Knowledge Proof." Wikipedia, May 27, 2023. https://en.wikipedia.org/wiki/Zero-knowledge_proof.

Referencias vi

[24] "MD5 Hash: Generate MD5 Message Digests Online." cryptii, n.d. https://cryptii.com/pipes/md5-hash.

[25] BarD Software s.r.o. "Free Project Management Tool for Windows, Macos and Linux." GanttProject, n.d. https://www.ganttproject.biz/.

[26] "AES Animation." CrypTool Portal, n.d. https://www.cryptool.org/en/cto/aes-animation.

[27] "Free, Open Source, and Modern CSS Framework Based on Flexbox." Bulma, n.d. https://bulma.io/.