Métodos de autenticación basados en criptografía de conocimiento cero

Zero-knowledge proof-based cryptographic authentication methods

Ing. Adiane Cueto Portuondo[*], Ing. Angel Alejandro Guerra Vilches[2], Ing. Leanny Laura Duardo Polo[3]

Recibido: 11/2025 | Aceptado: 11/2025 | Publicado:12/2025

Resumen

El presente artículo examina la evolución de los métodos de autenticación en un contexto donde la seguridad y la privacidad son cada vez más cruciales. Se destaca la necesidad de sistemas que garanticen la confidencialidad y la integridad de la información, sobre todo en un medio digital vulnerable. El estudio se centra en explorar las distintas categorías de autenticación desde métodos tradicionales, como contraseñas y tókenes físicos, hasta enfoques más avanzados, como la autenticación multifactorial (MFA, *Multi-Factor Autentication*) y el uso de certificados digitales. Sin embargo, el enfoque principal radica en el análisis de las Pruebas de Conocimiento Cero (ZKP, *Zero Knowledge Proof*) como una solución innovadora para mitigar las vulnerabilidades inherentes a los métodos tradicionales. La metodología utilizada incluye una revisión exhaustiva de la literatura y un análisis

[*] Departamento de Ciberseguridad, Facultad Ciberseguridad, Universidad de las Ciencias Informáticas. adianecp855@gmail.com

[2] Departamento de Infraestructuras Tecnológicas, Facultad de Ciberseguridad, Universidad de las Ciencias Informáticas. angelagv@uci.cu

[3] Departamento de Infraestructuras Tecnológicas, Facultad de Ciberseguridad, Universidad de las Ciencias Informáticas. leannyldp@uci.cu

detallado de los protocolos de ZKP aplicados a la autenticación, con especial énfasis en su implementación en entornos de computación en la nube. Los resultados subrayan la eficacia de las ZKP para verificar la identidad de los usuarios sin comprometer la información sensible y presentan ventajas significativas en comparación con otros métodos.

Palabras clave: autenticación, criptografía de conocimiento cero, computación en la nube, seguridad, privacidad

Abstract

The article "Authentication Methods Based on Zero-Knowledge Cryptography" examines the evolution of authentication methods in a context where security and privacy are increasingly crucial. It highlights the need for systems that ensure the confidentiality and integrity of information, especially in an increasingly vulnerable digital environment. The estudy focuses on exploring various categories of authentication, from traditional methods such as passwords and physical tokens to more advanced approaches like Multi-Factor Authentication (MFA) and the use of digital certificates. However, the main focus is on the analysis of Zero-Knowledge Proofs (ZKP) as an innovative solution to mitigate the inherent vulnerabilities of traditional methods. The methodology used includes an exhaustive literature review and a detailed analysis of ZKP protocols applied to authentication, with particular emphasis on their implementation in cloud computing environments. The results underscore the effectiveness of ZKPs in verifying user identities without compromising sensitive information, presenting significant advantages over other methods.

Keywords: *authentication, zero-knowledge cryptography, cloud computing, security, privacy*

Introducción

Un ciudadano promedio utiliza las tecnologías para acceder a todo tipo de servicios (correo, cuentas bancarias, redes sociales, dispositivos móviles, servicios de comunicaciones, entre otros). Estos servicios deben proporcionar seguridad y confiabilidad, para lo cual se requiere

algún tipo de información que identifique de forma única al usuario (Rodríguez Valdés et al., 2018).

La autenticación es un proceso que verifica la identidad de un usuario que intenta acceder a una información específica. Los sistemas de autenticación se utilizan de forma habitual para proteger datos sensibles e impedir el acceso no autorizado a sistemas y redes (Marmolejo-Corona et al., 2023). Este proceso es fundamental para garantizar la confidencialidad, integridad y disponibilidad de los recursos en un entorno digital, pues la autenticación efectiva minimiza el riesgo de accesos no autorizados y protege la información contra robos, alteraciones o usos indebidos. Con el aumento de la ciberdelincuencia y de la exposición de información personal, la necesidad de métodos de autenticación robustos y seguros ha cobrado una importancia crucial. Las técnicas de autenticación han evolucionado desde las contraseñas tradicionales hasta las Pruebas de Conocimiento Cero (ZKP) para enfrentar los desafíos de seguridad en un mundo cada vez más digitalizado.

Este trabajo explora diversos métodos de autenticación, desde los más tradicionales hasta los más innovadores, con un enfoque especial en la criptografía de conocimiento cero. El problema central que aborda la investigación es la vulnerabilidad de los métodos de autenticación tradicionales (como las contraseñas y los tókenes físicos) frente a ataques sofisticados y la exposición de información sensible. El artículo se divide en varias secciones. En primer lugar, se realiza una revisión exhaustiva de la literatura sobre métodos de autenticación, en la que se destacan las limitaciones y vulnerabilidades de los enfoques tradicionales. En segundo lugar, se profundiza en las ZKP, mediante la explicación sus fundamentos teóricos y su aplicación en la autenticación. Se analizan diferentes protocolos de ZKP (como el de Schnorr, Feige-Fiat- Shamir, y Guillou-Quisquater), y se discute su seguridad y eficiencia.

El objetivo final es proporcionar una comprensión profunda de cómo las ZKP pueden utilizarse para asegurar la identidad de los usuarios sin comprometer la privacidad ni la seguridad de la información. Este enfoque innovador no solo mitiga las vulnerabilidades

de los métodos tradicionales, sino que también abre nuevas posibilidades para la autenticación segura en un entorno digital cada vez más complejo y expuesto a amenazas.

Materiales y métodos

Para la elaboración de este estudio se realizó una búsqueda exhaustiva en diversas bases de datos académicas reconocidas como Google Scholar, Scopus, IEEE Xplore y ACM Digital Library.

Con el objetivo de garantizar la inclusión de estudios relevantes y de alta calidad se establecieron criterios de inclusión específicos.

- Publicaciones en revistas revisadas por pares o conferencias de alto impacto: se priorizaron estudios publicados en revistas científicas con un riguroso proceso de revisión por pares, así como en conferencias internacionalmente reconocidas en los campos de la criptografía, la seguridad en la nube y la privacidad de datos.
- Enfoque en métodos de autenticación basados en ZPK: se seleccionaron estudios que abordaran el desarrollo, la implementación y la evaluación de técnicas de autenticación que emplean ZPK.
- Aplicaciones en seguridad en la nube y *blockchain*: se priorizaron trabajos que investigaran la aplicación de ZPK en el contexto de la seguridad en la nube y en tecnologías de *blockchain*; se destacan casos de uso como la autenticación en sistemas distribuidos, la protección de la privacidad en transacciones y la integridad de los datos.

La metodología empleada en esta investigación se dividió en dos enfoques complementarios. En primer lugar, se realizó una revisión bibliográfica, en la que se exploró la literatura existente sobre métodos de autenticación basados en ZKP en el contexto de la seguridad en la nube y *blockchain*. Esta revisión proporcionó una visión general del estado actual de la investigación en este campo y permitió señalar posibles áreas de mejora o innovación.

En segundo lugar, se aplicó un enfoque analítico-sintético que implicó el análisis detallado de los principios teóricos subyacentes a las ZPK y de su aplicación en autenticación criptográfica. A través de una revisión bibliográfica, se profundizó en conceptos clave y se sintetizó

el conocimiento adquirido para identificar posibles áreas de mejora o nuevas direcciones de investigación. Este enfoque combinó la comprensión teórica con la identificación de aplicaciones prácticas, lo que proporcionó una base sólida para avanzar en el campo de la autenticación basada en criptografía de conocimiento cero.

Existen diversos métodos para autenticar a los usuarios que varían en seguridad y complejidad. Estos se pueden agrupar en tres grandes categorías:

1. Autenticación basada en conocimiento

Contraseñas alfanuméricas

Entre los métodos más tradicionales y ampliamente utilizados dentro de la autenticación basada en conocimiento se encuentran las contraseñas alfanuméricas. Son una combinación de caracteres que utilizan el código ASCII para generar una clave secreta de dimensión variable. Son fáciles de implementar y muy comunes en todos los tipos de sistemas. Una contraseña alfanumérica fuerte debe ser aleatoria y larga, por tanto, difícil de recordar. Por la naturaleza de los procesos mnemotécnicos cuando los usuarios tienen que establecer o recordar muchas contraseñas, que utilizan en sistemas distintos, suelen emplear claves parecidas o con frases sencillas de recordar (Rodríguez Valdés et al., 2018). Este método, aunque es el más común, es en extremo vulnerable a varios tipos de ataques, entre ellos:

- *Phishing*: donde los atacantes engañan a los usuarios para que revelen sus contraseñas mediante sitios web falsificados o correos electrónicos maliciosos.
- Ataques de diccionario: que utilizan listas predefinidas de palabras comunes y combinaciones alfanuméricas para intentar adivinar la contraseña.
- Ataques de fuerza bruta: que implican probar todas las combinaciones posibles hasta encontrar la contraseña correcta.

One-Time Password (OTP)

En contraste con las contraseñas estáticas, otro método común dentro del mismo grupo de autenticación basada en conocimiento es el *One-Time Password* (OTP). Dicho sistema asegura el uso de

contraseñas con un sistema OTP, es decir, el usuario posee una contraseña por un tiempo determinado y para un uso específico. Esta solución es usada en general para el proceso de autenticación de inicio para los accesos externos, los cuales se realizan mediante VPN (Red Privada Virtual) (Mendoza Arteaga et al., 2020). Aunque los sistemas OTP ofrecen una capa adicional de seguridad al generar contraseñas temporales, que caducan después de un solo uso, también presentan vulnerabilidades que los atacantes pueden explotar. Por ejemplo, si un atacante logra interceptar el canal de comunicación (como mensajes SMS o correos electrónicos), a través del cual se envía el OTP, podría utilizar el código antes de que expire y acceder a la cuenta o sistema objetivo. Además, los dispositivos móviles utilizados para recibir OTP pueden ser comprometidos por *malware*, lo que permitiría a los atacantes capturar los códigos en tiempo real.

Otra vulnerabilidad significativa es el *phishing* dirigido, donde un atacante engaña al usuario para que revele su OTP en un sitio web falso o por medio de una aplicación maliciosa. De esta forma el atacante puede autenticarse como si fuera el usuario legítimo. Estos riesgos resaltan la necesidad de implementar medidas de seguridad adicionales.

Autenticación Gráfica

Los Sistemas de Autenticación Gráfica son usados tanto para la autenticación de usuarios en un sistema como para la generación de claves para el uso en algoritmos criptográficos (Shendage, S. et al., 2014). Las contraseñas gráficas pueden estar formadas por la combinación de fotos, imágenes o iconografías. Las características de la imagen producen un espacio de claves mucho mayor. La eficiencia de estos sistemas se basan en la gran capacidad de los seres humanos de recordar patrones en imágenes, en vez de memorizar conjuntos de caracteres de gran longitud y complejidad (Rodríguez Valdés et al., 2018).

En general, estos sistemas poseen ventajas demostradas sobre los métodos tradicionales de introducción de texto y conservan espacios de claves considerables. Sin embargo, la autenticación gráfica también presenta algunas desventajas significativas. Uno de sus principales inconvenientes es que su implementación puede ser más compleja y costosa

que los métodos tradicionales, ya que requieren interfaces gráficas más avanzadas y sistemas de almacenamiento y recuperación de imágenes eficientes. Además, dependen de dispositivos con capacidades gráficas modernas, lo que puede limitar su uso en dispositivos más antiguos o con recursos limitados. El empleo de imágenes personales o identificables puede plantear problemas de privacidad y, aunque los espacios de claves son mayores, los ataques de fuerza bruta siguen siendo una amenaza. La interfaz de usuario puede ser menos intuitiva para algunos usuarios, y la compatibilidad entre diferentes sistemas y plataformas puede ser un problema.

2. Autenticación basada en posesión

Tókenes físicos

Además de lo que el usuario conoce, la autenticación basada en posesión se apoya en lo que el usuario posee, como es el caso de los tókenes físicos. Un token es un dispositivo de almacenamiento que contiene una clave secreta que se utiliza en el proceso de autenticación (Mendoza Arteaga et al., 2020). Los tókenes son emitidos y certificados por una entidad de confianza, como una autoridad de certificación, que valida la autenticidad y la integridad de la información contenida en el token, lo que le añade una capa adicional de seguridad.

De manera general, estos tókenes se presentan como tarjetas inteligentes o magnéticas, pero pueden verse en muchas otras como dispositivos digitales o memorias USB. Estas tarjetas contienen un microchip capaz de almacenar información y realizar funciones criptográficas, lo que permite su uso en una amplia gama de aplicaciones, desde el comercio electrónico hasta el control de acceso físico y lógico (Mendoza Arteaga et al., 2020). En muchos países, las tarjetas inteligentes se han convertido en una parte integral de los documentos de identidad, lo que facilita no solo la identificación personal sino también la autenticación segura en servicios en línea y presenciales.

Además de los riesgos de pérdida o robo, los tókenes (como cualquier dispositivo físico) pueden deteriorarse con el tiempo debido al uso continuo. Este deterioro afecta la funcionalidad del token lo que lo vuelve menos fiable, incluso, en algunos casos, inutilizable.

3. Autenticación basada en inherencia

Biometría

Dentro de los métodos de autenticación, la biometría representa un enfoque basado en lo que el usuario es. Este método consiste en la autenticación de un individuo mediante sus características físicas: forma de su rostro, huellas dactilares, estructura y forma de su voz, patrón de iris y otras características únicas de cada ser vivo. El reconocimiento biométrico consiste en almacenar, medir y comparar los rasgos característicos de un individuo (Mendoza Arteaga et al., 2020).

Los esquemas de autenticación basados en información biométrica son alternativas a las contraseñas alfanuméricas. Para su implementación es necesario, en todos los casos, utilizar elementos de *hardware* especializado. Este requisito eleva los costos y la complejidad de los sistemas, lo que puede ser una barrera para su empleo en entornos donde los recursos son limitados. Además, la precisión y confiabilidad de estos dispositivos pueden verse afectadas por factores externos, como la calidad del *hardware*, las condiciones ambientales o el estado físico del usuario. La biometría puede ser conceptualmente difícil de falsificar, pero fácil de suplantar. Esto no significa que puedan ser copiados o duplicados con la misma facilidad que una contraseña, pero la recolección de datos biométricos (como huellas dactilares o imágenes faciales) puede realizarse sin el conocimiento del usuario en situaciones de alta tecnología. El rendimiento de estos sistemas también puede verse comprometido por circunstancias como la salud del usuario, estrés y otros factores que pueden hacer el proceso extenso e incómodo (Rodríguez Valdés et al., 2028).

Autenticación Multifactor (MFA)

Un solo factor de autenticación no es seguro, por lo que en la actualidad la autenticación multifactor (MFA) es la tendencia para verificar que los usuarios sean legítimos (Mendoza Arteaga et al., 2020). Este proceso de seguridad permite que el usuario corrobore su identidad mediante la confirmación de dos factores de autenticación diferentes (clave estática y clave dinámica) (Espinoza Tinoco et al., 2022). Por ejemplo, un sistema puede requerir una contraseña (algo que el usuario sabe) y un código enviado a su teléfono (algo que el usuario tiene).

La MFA aumenta de forma significativa la seguridad al requerir varios niveles de autenticación.

Este tipo de autenticación presenta vulnerabilidades relacionadas con la forma en que se implementa. Si un sitio web utiliza un método de autenticación de dos factores basado en SMS, los atacantes pueden clonar la tarjeta SIM del usuario y redirigir los mensajes de texto a su propio dispositivo. Además, si se utiliza una aplicación de autenticación, el dispositivo del usuario puede verse comprometido por *malware* o virus, lo que permite a los atacantes acceder a los códigos de seguridad generados por la aplicación (Marmolejo-Corona et al., 2023).

La implementación de MFA puede crear un conflicto entre la comodidad y la seguridad. Para muchos usuarios, la necesidad de completar pasos adicionales para autenticarse puede ser percibida como incómoda y engorrosa. Lo anterior puede llevar a una resistencia a su utilización, o incluso a la desactivación de estas medidas si se les da la opción. Además, no todos los servicios en línea son compatibles con MFA, lo que obliga a los usuarios a elegir entre seguridad y conveniencia. Esta incompatibilidad también puede generar dificultades técnicas para configurar o utilizar MFA, especialmente en dispositivos y aplicaciones obsoletos.

Otro desafío significativo de la MFA es la dependencia de proveedores externos para la entrega de códigos de autenticación o para la validación de datos biométricos. Esta subordinación introduce un punto de fallo adicional en el proceso de autenticación. Si el servicio externo es comprometido, la autenticación del usuario también puede estar en riesgo, esto expone al sistema a posibles brechas de seguridad.

Certificados digitales

Entre otros métodos más recientes se encuentra el certificado digital. Este consiste en un documento electrónico que verifica la identidad de una persona u organización en Internet y utiliza tecnología criptográfica para proteger la privacidad y la seguridad de las comunicaciones en línea. Es emitido por una autoridad de certificación responsable

de verificar la identidad del registrante del certificado y garantizar la autenticidad de la clave pública asociada con el certificado. Permite cifrar y descifrar datos, firmar documentos de forma digital y autenticar a usuarios en transacciones y servicios en línea (Marmolejo-Corona et al., 2023).

Aunque son esenciales para la seguridad en línea, los certificados digitales pueden ser vulnerables si se compromete la clave privada asociada. En tal caso, un atacante puede suplantar la identidad del usuario, lo que conlleva graves riesgos de seguridad. Además, tienen una fecha de caducidad y si no se renuevan a tiempo puede interrumpir servicios críticos. La confianza en las autoridades de certificación (CA, por sus siglas en inglés) es esencial, no obstante, si una CA es vulnerada todo el sistema de certificación resulta afectado. Por último, cumplir con normativas y estándares regulatorios implica una gestión constante y puede ser costoso para las organizaciones.

Autenticación mediante el uso de pruebas de ZKP

A pesar de los avances en métodos de autenticación (como la multifactorial y el uso de certificados digitales), persisten desafíos relacionados con la seguridad y la privacidad. Los métodos tradicionales, aunque eficaces en muchos casos, siguen siendo vulnerables a ataques sofisticados y a la exposición de información sensible. Es aquí donde las Pruebas de Conocimiento Cero emergen como una solución innovadora que aborda estos problemas de manera única.

Las ZKP permiten a una parte (*prover*) demostrar a otra (*verifier*) que posee cierto conocimiento o ha realizado una operación sin revelar ninguna información adicional sobre ese conocimiento o el proceso en sí. Este enfoque resuelve una de las limitaciones clave de los métodos de autenticación tradicionales: la necesidad de compartir información sensible para validar la identidad del usuario.

La autenticación mediante ZKP se encuadra, sobre todo, en los métodos basados en conocimiento, ya que el usuario demuestra conocer cierta información sin revelar cuál es esa información. En este contexto, el conocimiento es lo que permite la autenticación, pero a diferencia de los métodos tradicionales (como las contraseñas), el

protocolo de ZKP garantiza que el conocimiento no sea compartido con el sistema de autenticación, lo que añade una capa de seguridad crucial (Fenzi, 2019).

Autenticación en la nube

La computación en la nube ofrece acceso rápido y económico a recursos informáticos como almacenamiento y aplicaciones, lo que la hace atractiva para pequeñas y medianas empresas. Sin embargo, este modelo presenta graves desafíos de seguridad como problemas de privacidad, falta de transparencia, filtraciones de datos, y robos de identidad. La naturaleza conectada y dinámica de la nube aumenta la vulnerabilidad a ataques, ya que las defensas tradicionales no son suficientes para proteger este entorno.

Los servicios en la nube requieren que los usuarios almacenen información sensible, esto expone los datos a posibles accesos no autorizados, sobre todo cuando se utilizan métodos de autenticación débiles. Además, las múltiples copias de datos y servicios en la nube generan un entorno complejo que puede resultar en problemas de gestión y seguridad, y aumenta el riesgo de ataques como el secuestro de sesiones, que consiste en obtener credenciales durante el inicio de sesión (Bermúdez, M. et al., 2020).

Dado este panorama, se requiere un enfoque robusto de seguridad en la nube que trascienda las prácticas tradicionales. Aquí es donde las ZKP se presentan como una solución eficaz. En este contexto, las ZKP permiten verificar la identidad de los usuarios sin revelar información sensible, lo que mitiga los riesgos asociados a la exposición de datos. Su implementación proporciona una capa adicional de seguridad al evitar que los atacantes puedan acceder a información crítica, aun cuando logren interceptar las comunicaciones. Esto no solo protege la integridad y confidencialidad de los datos, sino que también aborda de manera efectiva las principales preocupaciones de seguridad asociadas con la computación en la nube.

Pruebas de conocimiento cero (ZKP)

El protocolo criptográfico ZKP permite compartir y verificar información sin exponer datos sensibles. En esencia, dicho protocolo

diseña un procedimiento en el que un agente (denominado probador) afirma que algo es cierto, mientras que otro agente (el verificador)comprueba que efectivamente lo es, sin necesidad de conocer toda la información. Por tanto, es un sistema para demostrar el conocimiento de algo que ha sucedido sin que la prueba exija revelar todos los datos (Guillou & Quisquater, 1988).

Lo anterior se logra mediante la generación de una prueba por parte del probador que cumple con un conjunto específico de criterios, los cuales el verificador puede utilizar para confirmar la afirmación sin aprender nada más sobre la declaración. En consecuencia, los ZKP permiten minimizar y limitar el acceso a los datos en contextos distribuidos, como los servicios de Internet en general o la computación en la nube (Vilchez Moya et al., 2023).

La criptografía de conocimiento cero se basa en el concepto de «un engañador convincente», donde una entidad, llamada el verificador, puede estar convencida de que otra entidad, llamada el probador, posee cierta información sin aprender nada más sobre ella. Esto se logra mediante la interacción entre el verificador y el probador, en la que se realiza una serie de desafíos y respuestas que permiten verificar la validez de la afirmación sin revelar detalles adicionales (Hernández, D. et al., 2020).

A continuación, se presenta un ejemplo: Alice y Bob se enfrentan a un desafío particular, Bob es daltónico y no puede diferenciar los colores rojo y verde. Sin embargo, Alice tiene en sus manos dos círculos idénticos que difieren solo en el color: uno es rojo y el otro es verde. El objetivo de Alice es demostrarle a Bob que los círculos son diferentes, sin revelar más información. El probador es Alice y el verificador es Bob.

1. Alice muestra los dos círculos a Bob y le explica que son diferentes, pero Bob no puede diferenciarlos.
2. Para comenzar la demostración, Alice le pide a Bob que se ponga ambos círculos a la espalda y le indica que muestre uno de los círculos y luego lo vuelva a esconder.

3. A continuación, Alice le dice a Bob que tiene la opción de volver a mostrar el mismo círculo que mostró inicialmente o cambiarlo por el otro círculo.
4. Cada vez que Bob muestra un nuevo círculo, Alice le indica si cambió el círculo o no.
5. Alice adivina correctamente si Bob cambió o no el círculo en cada turno sucesivo.
6. A medida que Alice adivina de manera correcta, se vuelve cada vez más probable que los círculos sean diferentes.
7. A través de esta interacción y los aciertos consecutivos de Alice, Bob se convence de que los círculos son diferentes sin que Alice tenga que revelar explícitamente por qué.

Una prueba de conocimiento cero debe satisfacer tres propiedades:

- Completitud: si la declaración es válida, entonces el verificador honesto (Bob) estará convencido de este hecho por un probador honesto. En consecuencia, Bob aceptará la identificación de Alice con probabilidad uno.
- Solidez: si la declaración es inválida, ningún probador tramposo puede convencer al verificador honesto de que es verdadera. En consecuencia, el verificador (Bob) rechazará la prueba con una probabilidad de al menos la mitad.
- Conocimiento cero: si la declaración es verdadera, ningún verificador tramposo puede descubrir nada nuevo aparte de esta información (Ezziri & Khadir, 2020).

Existen diferentes protocolos de conocimiento cero que comparten el principio de demostrar que se conoce algo sin tener que decir con exactitud qué es lo que se sabe. En el protocolo de conocimiento cero interactivo, el verificador y el demostrador interactúan entre sí múltiples veces antes de que el verificador pueda estar seguro de que el demostrador conoce la información requerida. El protocolo se fundamenta sobre la base de considerar que, si el usuario realmente conoce la información, entonces debería ser capaz de responder ciertas preguntas o realizar ciertas operaciones con éxito, mientras que un impostor no sería capaz de hacerlo. En consecuencia, las ZPK interactivas tienen aplicaciones en diversas áreas, como la autenticación, la

verificación de identidad, la protección de la privacidad y la seguridad en sistemas distribuidos (Henry, R., 2014).

En cambio, en el Protocolo de Conocimiento Cero No Interactivo (NIZK) el demostrador envía una sola prueba al verificador, sin que sea necesaria ninguna interacción adicional. En este tipo de protocolos (como la prueba de Schnorr), la parte que conoce el secreto interactúa con otra parte (el verificador) para demostrar que conoce el secreto sin revelarlo y sin necesidad de interactuar entre ellos. Algunos casos de sistemas basados en NIZK son las criptomonedas como Zcash y Monero, y las soluciones de autenticación de dos factores basadas en criptografía de clave pública como la autenticación de dos factores universal (U2F).

Otro tipo de protocolo de conocimiento cero aplica la teoría de grafos para demostrar el conocimiento de ciertas relaciones entre los elementos de un grafo. Este protocolo se basa en un desafío-respuesta entre las dos partes. En la primera fase, la parte que quiere demostrar que posee la información (proponente) construye un grafo a partir de dicha información y lo envía a la otra parte (verificador). En la segunda fase, el verificador elige un nodo del grafo y envía una pregunta al proponente pidiéndole que proporcione la información relacionada con ese nodo. En la tercera fase, el proponente responde a la pregunta sin revelar información adicional sobre el grafo. El proceso se repite varias veces sobre diferentes nodos del grafo en cada iteración. Al final, si el proponente puede responder correctamente todas las preguntas del verificador, se considera que ha demostrado que conoce la información sin revelarla.

Por último, cabe mencionar el Protocolo de Conocimiento Cero Basado en Criptografía de Curva Elíptica, un sistema de cifrado muy seguro que utiliza matemáticas complejas para proteger y descifrar información. En este sistema, también se diferencia entre el emisor, el verificador y la prueba. Esta última es el proceso que permite verificar la autenticidad de la información sin revelarla y para realizarla, el emisor y el verificador seleccionan una curva elíptica y un punto de partida en esa curva. El emisor luego realiza una serie de cálculos matemáticos utilizando la información que desea verificar y envía los

resultados de estos cálculos al verificador, quien utiliza estos resultados para determinar si la información es auténtica o no. Este protocolo es muy rápido y eficiente, lo que lo hace ideal para su uso en sistemas en línea y otros entornos de alta velocidad (Wanden-Berghe, C.A., 2013).

Protocolos utilizados en la autenticación

Protocolo de Schnorr

El esquema de autenticación y firma de Schnorr obtiene su seguridad de la dificultad de calcular logaritmos discretos. Para generar un par de claves, primero se eligen dos números primos (p y q), de modo que q sea un factor primo de $p-1$. Luego, se elige una que no sea igual a 1, tal que $a^q \equiv 1 \bmod p$. Todos estos números pueden ser comunes a un grupo de usuarios y pueden ser publicados libremente. Para generar un par de claves específicas (clave pública/clave privada) se elige un número aleatorio menor que q. Esta es la clave privada s. Luego, se calcula $v \equiv a^{-s} \bmod p$. Esta es la clave pública (Schneier, 1996). Protocolo de Autenticación de Schnorr (Véase Figura 1):

1. Alice elige un número aleatorio r menor que q y calcula $x = a^r \bmod p$. Esta es la etapa de preprocesamiento y se puede realizar mucho antes de que Bob esté presente.
2. Alice envía x a Bob.
3. Bob envía a Alice un número aleatorio e entre 0 y $2^t - 1$.
4. Alice calcula $y = (r + s \cdot e) \bmod q$ y envía a Bob.
5. Bob verifica que $x = a^y \cdot v^e \bmod p$.

Esto es porque $x = a^{r+s \cdot e} \cdot (a^{-s})^e = a^r \bmod p$.

La seguridad se basa en el parámetro t. La dificultad para romper el algoritmo es de aproximadamente 2^t. Schnorr recomendó que p tenga alrededor de 512 bits, q alrededor de 140 bits, y t sea 72 bits.

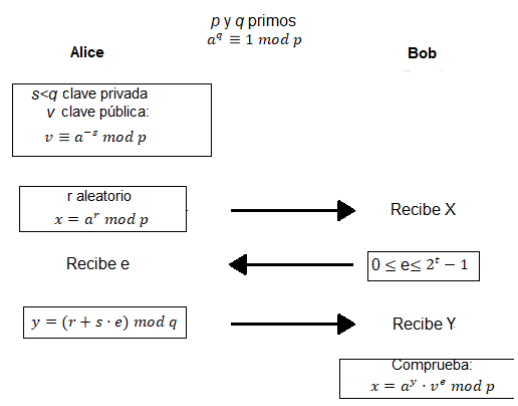

Figura 1. Ronda Protocolo de Schnorr

Dado que el cálculo del logaritmo discreto *s*, a partir de $v \equiv a^{-s} \, mod \, p$ es computacionalmente difícil, el protocolo asegura que un atacante no puede derivar la clave privada a partir de la clave pública.

Protocolo de Identificación Fiege-Fiat-Shamir

El protocolo creado por Uriel Fiege, Amos Fiat y Adi Shamir en 1988 es una de las implementaciones más comunes de una ZPK. El protocolo Fiat-Shamir se basa en la dificultad de la raíz cuadrada. El reclamante demuestra su conocimiento de una raíz cuadrada módulo un gran número *n* (Hasan, J., 2019).

El Esquema de Identificación Feige-Fiat-Shamir incluye dos entidades (el probador y el verificador), de acuerdo con el principio de todas las ZKP. El probador tiene un token secreto y busca autenticación, por lo que debe demostrar a otra entidad (el verificador) que lo autentique en función del token secreto del probador a través de una secuencia de problemas, sin que el verificador conozca el token secreto del probador.

Configuración única

Un centro de confianza publica un módulo $N = p \cdot q$ que es el producto de dos números primos. Cada posible reclamante (proponente) selecciona un secreto *s* que sea coprimo con N y publica $v = s^2 \, mod \, N$ como su clave pública (Figura 2).

1. Público: el módulo N y $v = s^2 \, mod \, N$.
2. Alice selecciona r y envía a Bob $x = r^2 \, mod \, N$.
3. Bob elige e ∈ {0,1}.
4. Alice envía $y = r \cdot s^e \, mod \, N$.
5. Bob debe verificar: $y^2 = x \cdot v^e \, mod \, N$.

Esto es porque $y^2 = r^2 \cdot s^{2e} = r^2 \cdot (s^2)^e = \; x \cdot v^e \, mod \, N$.

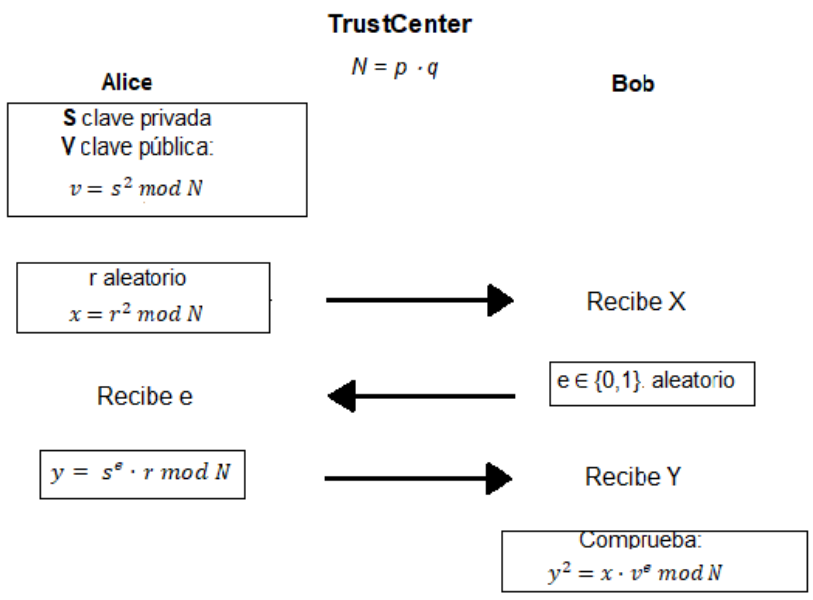

Figura 2. Ronda Fiege-Fiat-Shamir

Por ejemplo, si elegimos $e = 1$, entonces:

1. Público: el módulo N y $v = s^2 \ mod \ N$.
2. Alice selecciona r y envía a Bob $x = r^2 \ mod \ N$.
3. Bob elige $e = 1$.
4. Alice envía $y = r \cdot s \ mod \ N$.
5. Si $y^2 = x \cdot v \ mod \ N$, entonces Bob lo acepta, lo que significa que Alice pasa esta iteración del protocolo.

Por lo tanto, Alice debe conocer s en este caso.

El protocolo se basa en la dificultad de calcular raíces cuadradas modulares sin conocer s. Esto se garantiza por las propiedades derivadas del Teorema de Euler que aseguran la dificultad de invertir las operaciones modulares y la dispersión adecuada de los resultados. Al repetir este proceso varias veces, Bob puede estar seguro de que Alice conoce el secreto s, aunque nunca lo revele de forma directa. Cada iteración refuerza la confianza de Bob en que Alice realmente conoce el secreto.

Protocolo Guillou-Quisquater

Feige-Fiat-Shamir fue el primer protocolo práctico basado en identidad. Por su parte, el protocolo de Guillou-Quisquater se diseñó para disminuir el número de iteraciones y acreditaciones por iteración empleado en el primero al aumentar el trabajo computacional. Para algunas implementaciones, como las tarjetas inteligentes, un gran número de iteraciones es menos que ideal. Los intercambios con el mundo exterior consumen tiempo y el almacenamiento requerido para cada acreditación puede sobrecargar los recursos limitados de la tarjeta.

Louis Guillou y Jean-Jacques Quisquater desarrollaron un algoritmo de identificación de conocimiento cero más adecuado para aplicaciones como estas. Los intercambios entre Alice y Bob, y las acreditaciones paralelas en cada intercambio se mantienen al mínimo absoluto: solo hay un intercambio de una acreditación por cada prueba. Para el mismo nivel de seguridad, la computación requerida por Guillou-Quisquater es mayor que la de Feige-Fiat-Shamir por un factor de tres. Y al igual que Feige-Fiat-Shamir, este algoritmo de

identificación puede convertirse en un algoritmo de firma digital (Schneier, B., 1996).

El protocolo de identificación Guillou-Quisquater es un esquema de ZPK diseñado para optimizar la autenticación en dispositivos de seguridad (como microprocesadores o tarjetas inteligentes), lo que minimiza tanto la transmisión como los requisitos de memoria, a cambio de un aumento en el trabajo computacional.

Una vez más, sea n el producto de dos números primos p y q. Sea v coprimo con $\varphi(n) = (p - 1)(q - 1)$.

Sea J la clave pública de Alice, entonces, se define su clave privada B tal que $J \cdot B^v \equiv 1 \ mod \ n$.

Alice envía a Bob sus credenciales, J. Ahora, quiere probarle a Bob que esas credenciales son suyas. Para hacerlo, debe convencer a Bob de que conoce B. En la Figura 3 se presenta el protocolo:

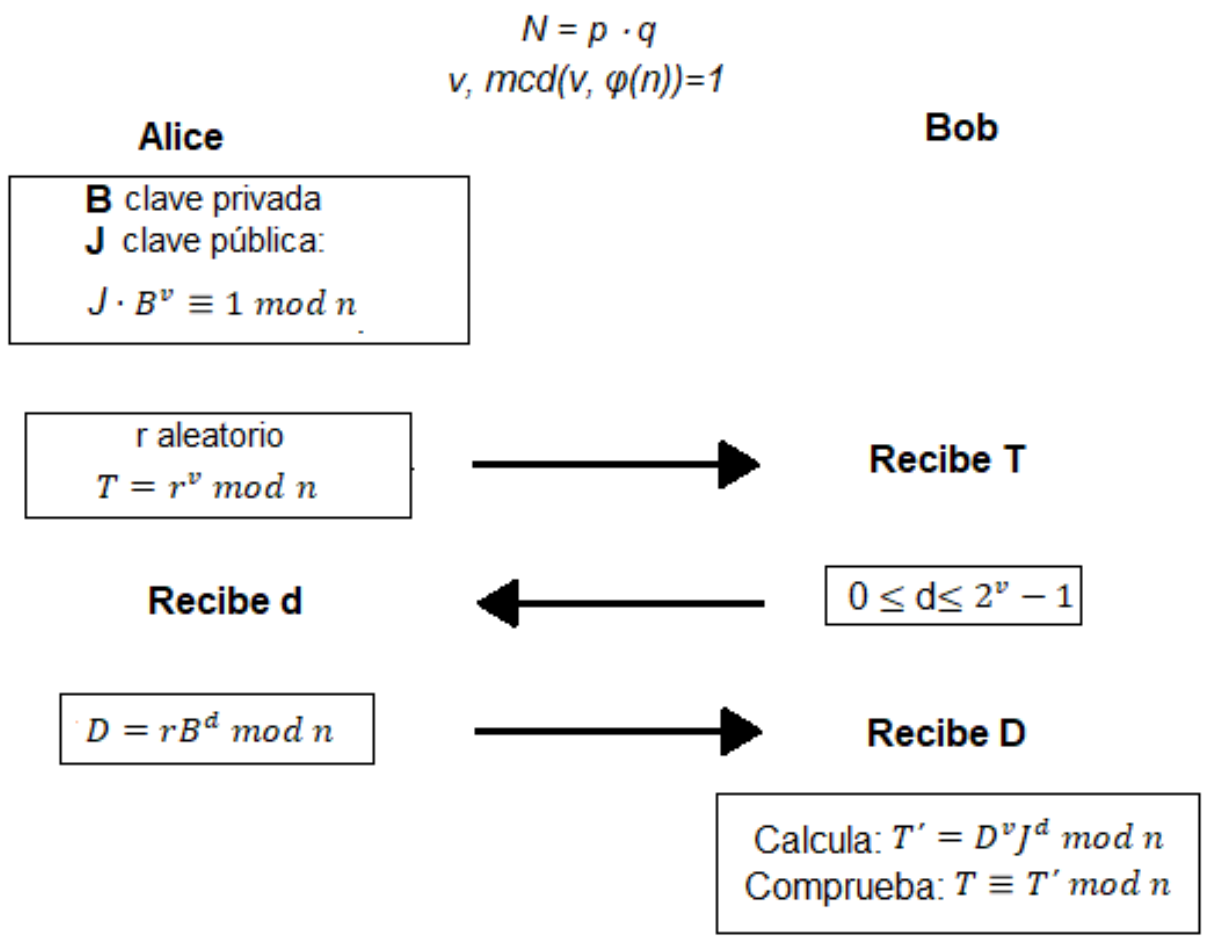

Figura 3. Ronda Guillou-Quisquater

1. Alice elige un número entero aleatorio r, tal que r esté entre 1 y $n-1$. Calcula $T = r^v \ mod \ n$ y lo envía a Bob.

2. Bob elige un número entero aleatorio, e, tal que e esté entre cero y $v-1$. Envía e a Alice.

3. Alice calcula $D = rB^d \ mod \ n$ y lo envía a Bob.

4. Bob calcula $T' = D^v J^d \ mod \ n$. Si $T \equiv T' \ mod \ n$, entonces la autenticación tiene éxito.

Las matemáticas no son tan complejas:

$$T' = D^v J^d = (rB^d)^v J^d = r^v D^{dv} J^d = r^v (J \cdot B^v)^d = r^v \equiv T \bmod n.$$

Dado que B fue construida para satisfacer $J \cdot B^v \equiv 1 \bmod n$ (Schneier, 1996) y (Guillou & Quisquater, 1988).

La seguridad de este protocolo reside en el parámetro *v*, ya que define el rango de valores entre los cuales Bob puede elegir su desafío *d* y, en consecuencia, la probabilidad de que un impostor pueda adivinarlo. Si Eve lograra adivinar el valor de *d*, podría hacerse pasar por Alice incluso sin conocer su clave privada *s*. Podría elegir un valor y aleatorio de antemano que sería el que envíe en el tercer paso y definir $x = y^v J^d$. En el primer paso en consecuencia; de esta manera, la verificación de Bob en el paso final sería trivialmente cierta. Recordar que, aunque Eve no conoce la clave privada de Alice, tiene acceso a su clave pública (Vilchez Moya et al., 2023).

Seguridad en estos protocolos

Uno de los ataques más comunes en los métodos de autenticación es el de *replay*, que consiste en reutilizar una comunicación exitosa anterior entre dos partes para suplantar la identidad de una de ellas mediante el reenvío de mensajes intercambiados. Aunque muchos protocolos de autenticación, como Kerberos, son vulnerables a este ataque, los protocolos de ZKP son resistentes debido a que cada ejecución es única gracias a la aleatorización utilizada. En el caso de los ZKP interactivos, también son negables a terceros que no participaron en la prueba, una propiedad que no se mantiene en los ZKP no interactivos.

Gracias a su naturaleza de conocimiento cero, la seguridad en los protocolos de autenticación basados en ZKP no se deteriora con el tiempo y es resistente a la interceptación de comunicaciones (*eavesdropping*) y al ataque de *chosen-text*. Este último ataque, común en esquemas de autenticación de tipo *challenge-response*, busca extraer información del secreto del probador seleccionando desafíos específicos. Sin embargo, los ZKP evitan que un verificador deshonesto obtenga información porque las respuestas del probador siempre contienen aleatoriedad. Además, los ZKP previenen

efectos no deseados, como la firma digital involuntaria de un archivo, que pueden ocurrir cuando se reutiliza la misma clave RSA para autenticación y firma digital.

El ataque *man-in-the-middle*, donde un atacante intercepta y modifica mensajes entre dos partes, es ineficaz contra los protocolos ZKP ya que el secreto nunca se transmite por el canal de comunicación. Además, ZKP protege contra la suplantación de identidad (un riesgo en esquemas de autenticación débiles basados en contraseñas), pues nunca revela el secreto ni información relacionada al verificador. En cuanto al *phishing*, ZKP ofrece una defensa sólida, y evita que los usuarios revelen sus credenciales a través de técnicas engañosas como correos fraudulentos o sitios web clonados. Dos protocolos ZKP propuestos proporcionan autenticación sin necesidad de compartir contraseñas, superando otros esquemas actuales.

En resumen, los protocolos de autenticación ZKP se destacan como una de las opciones más seguras frente a esquemas tradicionales como la autenticación débil con contraseñas y la autenticación fuerte de *challenge-response*, gracias a su resistencia a numerosos ataques conocidos. Las debilidades de los protocolos ZKP suelen surgir de deficiencias en su implementación, dado que sus fundamentos teóricos son sólidos y robustos (Bukovits, 2023).

Conclusiones

El presente estudio destacó la relevancia y el impacto de las Pruebas de Conocimiento Cero (ZKP) en el ámbito de la autenticación criptográfica, en especial en contextos como la seguridad en la nube. La revisión exhaustiva de los principales protocolos y métodos de ZKP ha revelado que estas técnicas juegan un papel crucial en la mejora de la privacidad y la seguridad en sistemas distribuidos, lo que ofrece garantías robustas sin comprometer la confidencialidad de la información.

La implementación de ZKP representa un avance significativo en la autenticación segura y permite verificar la validez de una transacción o identidad sin necesidad de revelar información sensible. La flexibilidad y adaptabilidad de estos métodos son valiosas en un

entorno donde la protección de datos y la privacidad son de suma importancia. Las diversas aplicaciones de ZKP demuestran el potencial de estas técnicas para fortalecer la seguridad en diversos contextos.

Por último, la protección de la privacidad y el desarrollo de marcos éticos para el uso de tecnologías de autenticación basadas en ZKP son aspectos fundamentales que deben ser considerados. A medida que estas técnicas se integran en aplicaciones más amplias, es esencial explorar enfoques para garantizar la privacidad de los datos y establecer directrices éticas para su implementación en entornos sensibles. Estas áreas representan importantes direcciones para futuras investigaciones y desarrollo en el campo de la autenticación criptográfica.

Referencias bibliográficas

Bermúdez León, M. J. (2020). *Métodos de seguridad, computación en la nube*. Repositorio USAM. http://repositorio.usam.ac.cr/xmlui/handle/11506/2202

Bukovits, N. A. (2023). *Zero Knowledge proofs y sus aplicaciones prácticas* [Tesis de grado, Universidad de Buenos Aires]. https://www.sidalc.net/search/Record/tpos:1502-2432_BukovitsNA/Description

Espinoza Tinoco, L., Barriga Rivera, B., Izurieta Navarrete, J., & Morales Alarcón, C. H. (2022). Seguridad informática aplicando la Autentificación por Doble factor para la plataforma HomeOfi. *Ciencias Técnicas y Aplicadas*, *8*(3). https://dialnet.unirioja.es/servlet/articulo?codigo=8637935

Ezziri, S., & Khadir, O. (2020). A Zero-Knowledge Identification Scheme Based on the Discrete Logarithm Problem and Elliptic Curves. En F. Saeed, T. Al-Hadhrami, E. Mohammed, & A. Al-Sarem (Eds.), *Advances on Smart and Soft Computing* (Vol. 1188, pp. 13-23). Springer. https://doi.org/10.1007/978-981-15-6048-4_3

Fenzi, G. (2019). *Zero Knowledge Proofs Theory and Applications* [Tesis de maestría, University of St. Andrews]. https://info.cs.st-andrews.ac.uk/student-handbook/files/project-library/cs4796/2020/gf45-Final_Report.pdf

Guillou, L. C., & Quisquater, J.-J. (1988). A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory. En C. G. Günther (Ed.), *Advances in Cryptology — EUROCRYPT '88* (Vol. 330, pp. 123-128). Springer. https://link.springer.com/chapter/10.1007/3-540-45961-8_11

Hasan, J. (2019). Overview and Applications of Zero Knowledge Proof (ZKP). *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *8*(5). https://www.academia.edu/download/63348598/Overview-and-Applications-of-Zero-Knowledge-Proof-ZKP20200518-20172-1ev7qkn.pdf

Henry, R. (2014). *Efficient Zero-Knowledge Proofs and Applications* [Tesis doctoral, University of Waterloo]. UWspace. https://uwspace.uwaterloo.ca/handle/10012/8621

Hernández Fernández, D. (2020). *Pruebas de conocimiento cero* [Tesis de grado, Universidad de Salamanca]. GREDOS. https://gredos.usal.es/handle/10366/152749

Marmolejo-Corona, I. V., Bautista-Aguilar, F. A., Santiago-González, Y. F., & Serrano-Manzano, G. A. (2023). Seguridad en Sistemas de Autenticación: Análisis de Vulnerabilidades y Estrategias de Mitigación. *Xikua Boletín Científico de la Escuela Superior de Ciudad Sahagún*, 11(22). https://repository.uaeh.edu.mx/revistas/index.php/xikua/article/view/10802

Mendoza Arteaga, A., Bolaños Burgos, F., Cedeño Sarmiento, C., & Saltos Rivas, W. R. (2020). La importancia de la autenticación multifactor para el usuario final en un entorno financiero. Informática y Sistemas: *Revista de Tecnologías de la Informática y las Comunicaciones*, *4*(1). https://revistas.utm.edu.ec/index.php/Informaticaysistemas/article/download/2347/2560

Quisquater, J.-J., Guillou, L. C., Berson, T. A., Blåken, G., Guillot, P., Loret, E., Loyer, B., Lussis, P., M'Raihi, D., Noro, M., Poupard, C., Pralile, O., Riguidel, M., Tardy-Corfdir, A., & Vallee, B. (1989). How to Explain Zero-Knowledge Protocols to Your Children. En G. Brassard (Ed.), *Advances in Cryptology — CRYPTO' 89 Proceedings* (Vol. 435, pp. 628-631). Springer. https://link.springer.com/chapter/10.1007/0-387-34805-0_60

Rodríguez Valdés, O., Legón, C. M., & Socorro Llanes, R. (2018). Seguridad y usabilidad de los esquemas y técnicas de autenticación gráfica. *Revista Cubana de Ciencias Informáticas, 12*(2). http://scielo.sld.cu/scielo.php?pid=S2227-18992018000500002&script=sci_arttext&tlng=pt

Schneier, B. (1996). *Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C*. John Wiley & Sons. https://onlinelibrary.wiley.com/doi/book/10.1002/9781119183471

Shendage, S. S., Dhainje, P., & Yevale, R. S. (2014). Cued Click Points: Graphical Password Authentication Technique for Security. *International Journal of Computer Science and Information Technologies,* 5(2). https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=ec7ee0b0434b9ac467afe5c2a1ce0df35a802b63

Vilchez Moya, C., Bermejo Higuera, J. R., Bermejo Higuera, J., & Sicilia Montalvo, J. A. (2023). Implementation and Security Test of Zero-Knowledge Protocols on SSI Blockchain. *Applied Sciences, 13*(9), 5717. https://doi.org/10.3390/app13095717

Wanden-Berghe Fajardo, C. A. (2023). *Blockchain e inteligencia artificial en el sistema de información contable: la disrupción de la partida triple* [Tesis doctoral, Universidad de Alicante]. RUA. https://rua.ua.es/dspace/handle/10045/135180