CRIPTOGRAFÍA DE CURVA ELÍPTICA: IMPORTANCIA, APLICACIONES Y COMPARATIVA FRENTE AL ALGORITMO RSA

ELLIPTIC CURVE CRYPTOGRAPHY: IMPORTANCE, APPLICATIONS AND COMPARISON WITH RSA ALGORITHM

José Enrique Iglesias
Universidad San Francisco Xavier
iglesias.enrique@usfx.bo
https://orcid.org/0009-0009-2390-8453
Bolivia

Recibido: 19 Mayo 2026 / Revisado: 29 Junio 2026 / Aceptado: 12 Julio 2026 / Publicado: 4 Agosto 2026

Resumen

La seguridad de las comunicaciones en redes públicas se ha vuelto un pilar fundamental del contexto digital actual, donde la criptografía asimétrica desempeña un rol central. La criptografía de Curva Elíptica (ECC), propuesta de manera independiente por Neal Koblitz y Victor Miller en 1985, constituye una alternativa relevante a los esquemas clásicos basados en la factorización de números enteros, como el algoritmo RSA. Su seguridad se fundamenta en el Problema del Logaritmo Discreto sobre Curvas Elípticas (ECDLP), que permite alcanzar niveles equivalentes de seguridad con tamaños de clave significativamente menores.

El presente artículo analiza, mediante una revisión sistemática de literatura reciente, la importancia, aplicaciones y rendimiento comparativo de la ECC frente al algoritmo RSA. La metodología consistió en una búsqueda cualitativa en Scopus, IEEE Xplore, ScienceDirect, MDPI y SpringerLink, limitada a publicaciones de los últimos cinco años. Los resultados evidencian que la ECC se ha consolidado como esquema asimétrico preferente en escenarios con recursos restringidos, particularmente en IoT, TLS, blockchain y firma digital, donde sus variantes principales (P-256, secp256k1, Curve25519 y Ed25519) presentan ventajas demostradas en eficiencia computacional, consumo de memoria y tamaño de claves. Se concluye que la ECC redefine las condiciones de viabilidad de la criptografía asimétrica contemporánea.

Palabras clave: *Criptografía de curva elíptica, ECC, ECDSA, Seguridad informática, Criptografía asimétrica*

Abstract

The security of communications in public networks has become a fundamental pillar of the current digital context, where asymmetric cryptography plays a central role. Elliptic Curve Cryptography (ECC), independently proposed by Neal Koblitz and Victor Miller in 1985, constitutes a relevant alternative to classical schemes based on the factorization of integers, such as the RSA algorithm. Its security relies on the Elliptic Curve Discrete Logarithm Problem (ECDLP), which enables equivalent security levels with significantly smaller key sizes.

This article analyzes, through a systematic review of recent literature, the importance, applications, and comparative performance of ECC against the RSA algorithm. The methodology consisted of a qualitative search in Scopus, IEEE Xplore, ScienceDirect, MDPI, and SpringerLink, limited to publications from the last five years. The results show that ECC has consolidated as the preferred asymmetric scheme in resource-constrained scenarios, particularly in IoT, TLS, blockchain, and digital signatures, where its main variants (P-256, secp256k1, Curve25519, and Ed25519) present demonstrated advantages in computational efficiency, memory consumption, and key size. It is concluded that ECC redefines the conditions of viability of contemporary asymmetric cryptography.

Keywords: *Elliptic curve cryptography, ECC, ECDSA, Information security, Asymmetric cryptography.*

Introducción

En la actualidad, la seguridad de las comunicaciones y la protección de la información se han convertido en pilares fundamentales para garantizar la integridad, confidencialidad y autenticidad de los datos que se transmiten a través de redes públicas, las cuales se caracterizan por ser inseguras. La criptografía asimétrica o de clave pública desempeña un papel importante en este contexto, ya que permite cifrar la información sin necesidad de compartir previamente una clave secreta entre el emisor y el receptor. Durante décadas, el algoritmo RSA (Rivest, Shamir y Adleman) ha sido el referente en este tipo de criptografía, el cual es ampliamente utilizado en certificados digitales, intercambio de claves y firma electrónica.

Bajo este contexto, el crecimiento exponencial del Internet de las Cosas (IoT), los dispositivos móviles y las tecnologías blockchain ha planteado nuevos desafíos de seguridad que requieren soluciones criptográficas con altos niveles de seguridad y bajos requerimientos computacionales y de procesamiento. La criptografía de Curva Elíptica (ECC), propuesta de manera independiente por Neal Koblitz y Victor Miller en 1985, permite responder a estas necesidades y se constituye en una alternativa a los sistemas de criptografía basados en la factorización de números enteros. La ECC se fundamenta en la dificultad del Problema del Logaritmo Discreto sobre Curvas Elípticas (ECDLP), un problema matemático que permite alcanzar niveles equivalentes de seguridad al algoritmo RSA, pero con tamaños de clave significativamente menores.

De acuerdo con Adeniyi et al. (2024), la ECC se ha consolidado como algoritmo criptográfico en sistemas IoT, debido a su eficiencia y rendimiento. Asimismo, Shah et al. (2025) sostienen que el tamaño reducido de las claves y el alto nivel de seguridad han posicionado a la ECC como uno de los algoritmos asimétricos más relevantes en la

actualidad. Esta tendencia se observa en la adopción de variantes como secp256k1 en Bitcoin y Ethereum, Curve25519 en protocolos de mensajería segura y los estándares NIST P-256 y P-384 en certificados y firmas digitales.

El presente artículo tiene como objetivo principal analizar la importancia, aplicaciones y rendimiento comparativo de la criptografía de curva elíptica frente a otros esquemas asimétricos clásicos. A partir de este objetivo general, se realiza un estudio de los fundamentos matemáticos esenciales de la ECC, la comparación de tamaños de clave, eficiencia y aplicabilidad frente a RSA, la identificación de sus principales aplicaciones en TLS, blockchain, IoT y firma digital.

Metodología de búsqueda

Al tratarse de un artículo de revisión, se adoptó un enfoque cualitativo enmarcado en la identificación y análisis sistemático de literatura científica relacionada con la ECC, considerando tanto sus fundamentos teóricos como sus aplicaciones prácticas. La búsqueda de información se realizó en bases de datos científicas ampliamente reconocidas por su rigor académico y su cobertura en áreas como ciencias de la computación, seguridad de la información y criptografía, entre las que se incluyen Scopus, IEEE Xplore, ScienceDirect, MDPI y SpringerLink.

Las estrategias de búsqueda se construyeron empleando términos clave en inglés, esto debido a la escasa literatura que existe en español, los mismos fueron articulados mediante los operadores booleanos AND y OR, con el objeto de combinar los aspectos teóricos en relación con los contextos aplicativos. Las cinco cadenas utilizadas fueron: "Elliptic Curve Cryptography" AND ("RSA comparison" OR "key size"); "ECC" AND IoT security"; "ECDSA" OR "Ed25519" AND "digital signature"; "secp256k1" AND "blockchain"; "Elliptic Curve Diffie-Hellman" AND "TLS". La búsqueda se restringió a publicaciones comprendidas entre 2021 y 2025, este aspecto es fundamental ya que la ciberseguridad es un campo de rápida evolución.

En cuanto a la pertinencia y calidad de los estudios revisados, se definieron los siguientes criterios de inclusión: (a) artículos publicados en revistas científicas indexadas, (b) estudios que aborden aspectos teóricos, comparativos o aplicados de la ECC, y (c) publicaciones disponibles en texto completo. Como criterios de exclusión se establecieron los siguientes: (a) registros duplicados entre bases de datos, (b) publicaciones sin revisión por pares y actas de congresos sin arbitraje riguroso, y (c) trabajos enmarcados en aspectos puramente matemáticos sin vinculación criptográfica.

En relación al proceso de selección, el mismo se llevó a cabo en tres etapas. En la primera etapa, tras aplicar las cadenas de búsqueda, se identificaron 38 registros iniciales que abordaban la temática de la ECC en sus distintas dimensiones. En la segunda etapa, se eliminaron 9 registros duplicados entre bases de datos y 18 registros que no cumplían los criterios de inclusión tras la revisión de títulos y resúmenes, quedando 11 documentos preseleccionados. Finalmente, en la tercera etapa, tras la lectura de los documentos y la evaluación de pertinencia temática y calidad metodológica, se incluyeron 7 estudios que constituyen la base bibliográfica sobre la cual se estructura el presente análisis.

Finalmente, los ejes temáticos que se utilizaron para la construcción de las cadenas de búsqueda fueron los siguientes: Criptografía de Curva Elíptica, Criptografía Asimétrica, algoritmo ECDSA, curvas

estandarizadas, seguridad en IoT, aplicaciones en TLS y Blockchain. Esta cobertura permitió abordar de manera integral los fundamentos, las variantes actuales y los principales escenarios de aplicación de la ECC en el contexto actual.

Desarrollo y discusión

Fundamentos matemáticos de la criptografía de curva elíptica

Una curva elíptica se define de forma simplificada como $y^2 = x^3 + ax + b$, donde los coeficientes a y b satisfacen la condición de no singularidad $4a^3 + 27b^2 \neq 0$. Esta condición garantiza que la curva no presente puntos singulares como intersecciones consigo misma o discontinuidades, lo cual es necesario para que su estructura matemática sea válida en criptografía.

La seguridad de la ECC se basa en la dificultad del Problema del Logaritmo Discreto sobre Curvas Elípticas (ECDLP), el cual consiste en: dados dos puntos P y Q pertenecientes a la curva tales que $Q=kP$, determinar el valor escalar k que satisface dicha relación. En la actualidad, no se conocen algoritmos eficientes para resolver el ECDLP, lo que permite alcanzar niveles equivalentes de seguridad al algoritmo RSA con tamaños de clave significativamente menores (Abhishek y Raj, 2021).

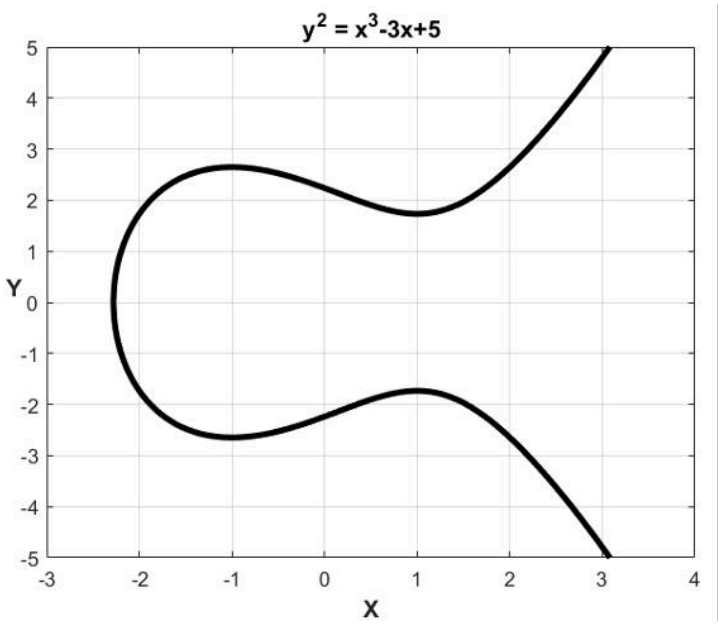

Figura 1. *Representación gráfica de una curva elíptica - Condición de no singularidad*

Geométricamente, sobre el conjunto de puntos de una curva elíptica se define una operación de suma entre dos puntos P y Q, esta suma se realiza trazando la recta que pasa por ambos puntos, la cual intersecta nuevamente la curva elíptica en un tercer punto (R'). Luego, este punto se refleja respecto al eje horizontal para obtener el resultado final de la operación. Cuando los puntos coinciden ($P = Q$), la suma se calcula utilizando la recta tangente a la curva en ese punto, siguiendo el mismo procedimiento de intersección y reflexión. Este mecanismo de suma es la base de las operaciones utilizadas en la criptografía de curva elíptica (Tanksale, 2024).

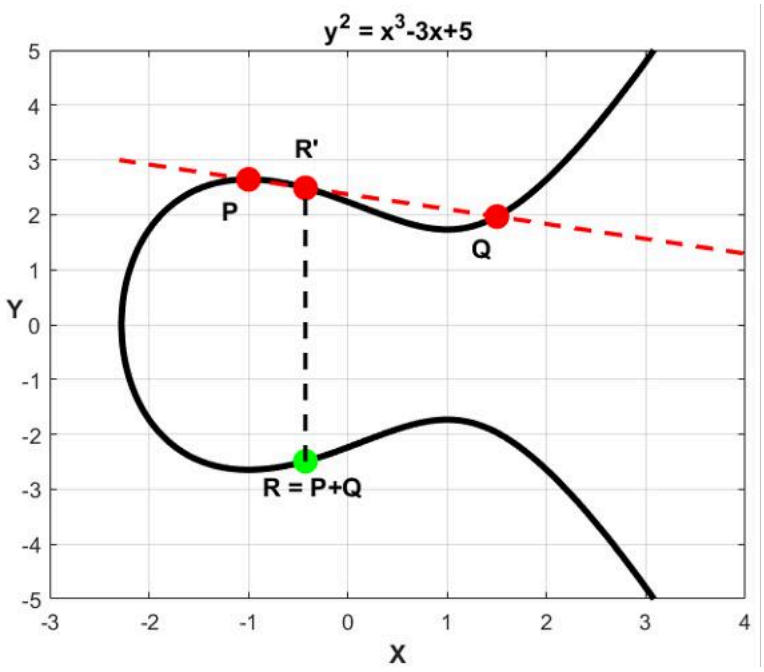

Figura 2. *Suma de puntos P + Q = R sobre una curva elíptica*

A partir de la operación de suma de puntos se define la operación central de la criptografía de curva elíptica que es la multiplicación escalar, expresada como kP, que consiste en sumar el punto P consigo mismo k veces. Esta operación posee una propiedad fundamental centrada en que calcular $Q = kP$ a partir de k y P es computacionalmente eficiente, pero recuperar k a partir de P y Q corresponde al Problema del Logaritmo Discreto sobre Curvas Elípticas, problema que no posee soluciones eficientes conocidas. Esta asimetría es la que sustenta el funcionamiento de la ECC, donde el escalar k actúa como clave privada y el punto $Q = kP$ como clave pública, de manera que esta última puede compartirse abiertamente sin comprometer a la primera. Sobre este principio se construyen aplicaciones como el intercambio de claves Diffie-Hellman sobre curva elíptica (ECDH) y los esquemas de firma digital ECDSA y EdDSA.

Comparativa entre ECC y el algoritmo RSA

Una de las principales razones por las que la ECC ha tomado ventaja sobre el algoritmo de criptografía RSA es su eficiencia para alcanzar niveles equivalentes de seguridad, mientras que RSA requiere tamaños de clave de 2048 a 3072 bits para garantizar entre 112 y 128 bits de seguridad, la ECC alcanza el mismo nivel con claves de apenas 224 a 256 bits (Ntayagabiri et al., 2024). Esta diferencia se traduce en ventajas importantes a nivel operativo, ya que el uso de claves más pequeñas permite reducir el costo computacional manteniendo niveles de seguridad equivalentes, además de acelerar ciertos procesos tales como la generación de claves y las firmas digitales.

Tabla 1. *Equivalencia de niveles de seguridad entre ECC y RSA*

Nivel de seguridad (bits)	Tamaño clave RSA (bits)	Tamaño clave ECC (bits)	Ejemplo de curva ECC
80	1024	160	secp160r1
112	2048	224	secp224r1
128	3072	256	P-256, secp256k1
192	7680	384	P-384
256	15360	521	P-521

Nota. Elaborada a partir de Ntayagabiri et al. (2024) y Shah et al. (2025)

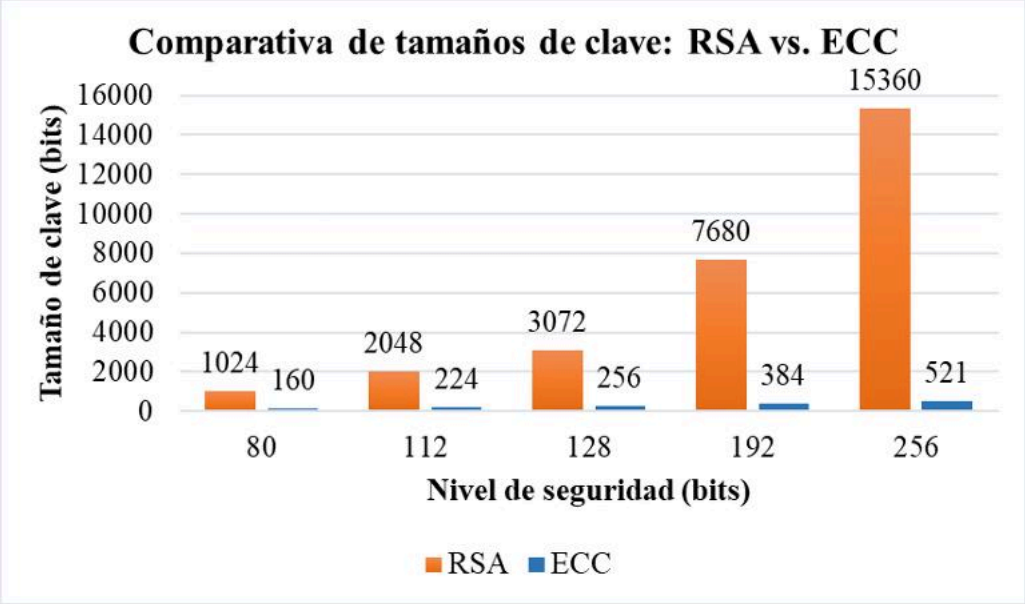

Figura 3. *Tamaños de clave entre RSA y ECC para distintos niveles de seguridad*

Lo expuesto anteriormente muestra la diferencia entre el algoritmo RSA y la Criptografía de Curva Elíptica. Mientras que RSA requiere un aumento considerable del tamaño de clave para mantener niveles equivalentes de seguridad desde 1024 hasta 15360 bits, ECC logra los mismos niveles utilizando claves mucho más pequeñas, entre 160 y 521 bits. Esta diferencia muestra la eficiencia de ECC en términos de costos computacionales y consumo de memoria. Asimismo, se presentan algunas curvas representativas para criptografía de curva elíptica, entre las que se incluyen secp160r1, NIST P-256 y secp256k1, las cuales se aplican en protocolos de comunicación segura (TLS), firmas digitales, blockchain, sistemas de Internet de las Cosas (IoT) y protocolos de intercambio de claves.

Aplicaciones de la Criptografía de Curva Elíptica

La consolidación de la ECC en aplicaciones reales ha favorecido el desarrollo de distintos ámbitos, tales como las comunicaciones seguras en Internet, las tecnologías blockchain y criptomonedas, el Internet de las Cosas (IoT) y la firma digital.

En el ámbito de las comunicaciones seguras, TLS 1.3, la versión más reciente de este protocolo, ha adoptado masivamente el uso de las Curvas Elípticas como mecanismo predeterminado de intercambio de claves.

Existen variantes como Curve25519 que se destaca por ofrecer velocidades de handshake superiores y resistencia a vulnerabilidades de implementación frente a esquemas tradicionales. La inclusión de X25519 y X448 en el estándar TLS 1.3 para el intercambio de claves entre dos partes a través de un canal inseguro representa un punto de inflexión en la adopción de la criptografía elíptica moderna.

En el ámbito de blockchain y criptomonedas, la curva secp256k1 sustenta el esquema de firmas digitales ECDSA utilizado en Bitcoin, Ethereum y en gran parte de las criptomonedas derivadas.

En este contexto, Balasubramanian (2024) señala que su adopción se debe, por un lado, a la eficiencia computacional que ofrece, por otro lado, a la transparencia de sus parámetros, es decir, a que los valores que definen la curva fueron generados de manera pública y verificable, sin procedimientos ocultos o dependientes de entidades centralizadas. En consecuencia, la seguridad de las direcciones de Bitcoin y la integridad de las transacciones se fundamentan directamente en la dificultad del Problema del Logaritmo Discreto sobre Curvas Elípticas (ECDLP) asociado a esta curva.

En el contexto del Internet de las Cosas, la criptografía de curva elíptica se ha posicionado como una alternativa adecuada para dispositivos que tienen restricciones de procesamiento, memoria y energía.

Adeniyi et al. (2024) concluyen que la ECC ha recibido mayor atención y es más frecuentemente empleada en sistemas IoT que otros métodos criptográficos. Bajo este contexto, Zhao et al. (2022) propusieron un protocolo de autenticación de tres factores basado en ECC para el Internet Industrial de las Cosas (IIoT), demostrando su viabilidad práctica con propiedades formales de seguridad verificadas mediante la herramienta Scyther, la cual sirve para analizar y verificar la seguridad de protocolos de comunicación.

En el ámbito de la firma digital, los esquemas ECDSA y EdDSA se consolidan como los más utilizados para garantizar autenticación, integridad y no repudio. En particular, EdDSA se construye sobre las curvas conocidas como Curve25519 y Curve448, las cuales se caracterizan por generar firmas de manera determinista, es decir, sin depender de valores aleatorios en cada operación, esta propiedad reduce significativamente el riesgo de fallos de seguridad asociados a una mala generación de números aleatorios, una debilidad conocida en implementaciones incorrectas de ECDSA.

Adicionalmente, estos esquemas han sido incorporados formalmente en el estándar FIPS 186-5 publicado por el NIST en 2023, donde se definen los métodos aprobados para la generación y verificación de firmas digitales.

A continuación, se presentan las principales Curvas Elípticas utilizadas en criptografía y sus aplicaciones.

Tabla 2. *Principales Curvas Elípticas estandarizadas y sus aplicaciones*

Curva	Tamaño	Estándar / Origen	Aplicaciones principales
secp256r1 (P-256)	256 bits	NIST FIPS 186	TLS, certificados X.509, S/MIME
secp256k1	256 bits	SECG	Bitcoin, Ethereum, criptomonedas
Curve25519 (X25519)	256 bits	RFC 7748	Intercambio de claves TLS, Signal, WhatsApp
Ed25519	256 bits	RFC 8032; FIPS 186-5	SSH, firma digital, autenticación
Curve448 / Ed448	448 bits	RFC 7748 / RFC 8032	TLS 1.3, escenarios de mayor nivel de seguridad

Nota. Elaborada a partir de Shah et al. (2025) y Tanksale (2024).

Conclusiones

La revisión realizada permite concluir que la pertinencia de la criptografía de curva elíptica no reside únicamente en su capacidad de igualar la seguridad ofrecida por el algoritmo RSA, sino en redefinir las condiciones bajo las cuales la criptografía asimétrica resulta viable. Mientras que RSA fue diseñado para entornos con recursos abundantes, la ECC abre la posibilidad de implementar mecanismos de clave pública en escenarios donde antes resultaba inviable, particularmente en dispositivos con limitaciones de hardware, energéticas o de procesamiento.

Asimismo, se observa que la elección de una curva elíptica debe responder a criterios de transparencia y propósito de aplicación. Por ejemplo, la adopción de secp256k1 en sistemas blockchain por su origen abierto, las curvas NIST P-256 y P-384 en entornos de certificados digitales, o Curve25519 y Ed25519 en aplicaciones de mensajería por sus propiedades de seguridad, evidencia que la ECC ha tenido avances considerables al punto de ofrecer alternativas diferenciadas según el contexto de uso.

Finalmente, fruto del proceso de revisión se pudo identificar dos vacíos importantes que deben ser considerados en futuras investigaciones. En primer lugar, la producción académica en español sobre criptografía de curva elíptica sigue siendo limitada en comparación con la amplia literatura anglosajona, lo que restringe su difusión y apropiación en el contexto regional, es así que se abre una oportunidad para fortalecer el desarrollo científico en el ámbito latinoamericano. En segundo lugar, se evidencia la necesidad de contar con más estudios comparativos de carácter experimental en entornos específicos, como el Internet de las Cosas industrial y los sistemas embebidos, de tal manera que permitan contrastar los fundamentos teóricos de la ECC con resultados prácticos y verificables en escenarios reales.

Referencias Bibliográficas

Abhishek, K., y Raj, E. G. (2021). Evaluation of computational approaches of short Weierstrass elliptic curves for cryptography. Cybernetics and Information Technologies, 21(4), 70-88. https://doi.org/10.2478/cait-2021-0045

Adeniyi, A. E., Jimoh, R. G., y Awotunde, J. B. (2024). A systematic review on elliptic curve cryptography algorithm for internet of things: Categorization, application areas, and security. Computers and Electrical Engineering, 118. https://doi.org/10.1016/j.compeleceng.2024.109330

Balasubramanian, K. (2024). Security of the Secp256k1 elliptic curve used in the Bitcoin blockchain. Indian Journal of Cryptography and Network Security, 4(1), 9-15. https://doi.org/10.54105/ijcns.A1426.04010524

Ntayagabiri, J. P., Ndikumagenge, J., Bentaleb, Y., y El Makhtoum, H. (2024). Comparative analysis of elliptic curve-based cryptographic approaches for Internet of Things security. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10(6), 568-583. https://doi.org/10.32628/CSEIT2410457

Shah, N. H., Ismail, S. A., Azizan, A., Anoop, A., Khan, D. T., y Ahamed, S. (2025). Lightweight Authentication Protocols in Internet of Things - A Review. International Journal of Engineering Trends and Technology, 73(3). https://doi.org/10.14445/22315381/IJETT-V73I3P108

Tanksale, V. (2024). Efficient elliptic curve Diffie–Hellman key exchange for resource-constrained IoT devices. Electronics, 13(18). https://doi.org/10.3390/electronics13183631

Zhao, X., Li, D., y Li, H. (2022). Practical Three-Factor Authentication Protocol Based on Elliptic Curve Cryptography for Industrial Internet of Things. Sensors, 22(19). https://doi.org/10.3390/s22197510