Criptografía aplicada en entornos industriales: un mapeo sistemático de la literatura

José Federico Castro Tramontina[1], Carlos Neil[1], Jorge Kamlofsky[1], Pedro Hecht[2]

[1] Universidad Abierta Interamericana – Facultad de Tecnología Informática
Centro de Altos Estudios en Tecnología Informática – Buenos Aires, Argentina
JoseFederico.CastroTramontina@alumnos.uai.edu.ar
{Carlos.Neil, Jorge.Kamlofsky}@uai.edu.ar
[2] Universidad de Buenos Aires – Facultad de Ciencias Económicas
Escuela de Negocios y Administración Pública – Buenos Aires, Argentina
phecht@dc.uba.ar

Resumen

Contexto: los sistemas de control industrial se encuentran conectados a redes específicas que permiten su administración tanto en planta como en forma remota. Esta interconexión requiere de mecanismos específicos de protección que aseguren la integridad de los equipos y del personal de planta, siendo la criptografía un mecanismo básico para la protección de la información procesada, almacenada y transmitida.
Objetivos: presentar los antecedentes del cifrado de comunicaciones entre autómatas industriales. Esto permitirá, a futuro, añadir una capa extra de seguridad sobre estos dispositivos presentes en las Infraestructuras Críticas del Sistema de Defensa Nacional.
Métodos: se detalla la creación y ejecución de un protocolo que establece un conjunto de preguntas y un procedimiento de búsqueda. Posteriormente se aplican filtros para la selección de artículos. Finalmente, se procede al análisis para poder responder las preguntas planteadas.
Resultados: la aplicación de los pasos detallados ha demostrado que existen desarrollos tecnológicos que abordan este problema, los cuales son explicados en este trabajo.
Conclusiones: ya se ha implementado criptografía en entornos industriales, siendo necesario definir un enfoque innovador que responda a las características diferenciadoras de los entornos operacionales, para facilitar su adopción.

Palabras clave: autómatas industriales, ciberseguridad industrial, criptografía, infraestructuras críticas

1. Antecedentes

La automatización de procesos industriales se realiza actualmente mediante los llamados ICS (Industrial Control Systems), sistemas de alta disponibilidad para asegurar la integridad física del personal y de los activos empleados en entornos industriales, a fin de mantener la continuidad de la producción. Sin embargo, su seguridad siempre estuvo basada en el aislamiento físico y en la separación entre las Tecnologías de la Operación (OT) de las Tecnologías de la Información (IT), generando una falsa sensación de seguridad . Esta división hoy se encuentra desdibujada debido a la interconexión de estas redes, brindando mayor flexibilidad y eficiencia, a costa de su exposición a nuevas vulnerabilidades y amenazas cibernéticas ([1] y [2]).

Los autómatas industriales son aquellos dispositivos que recogen información de campo remoto para la adquisición, control y monitoreo de los procesos que se ejecutan en entornos operacionales. La ausencia de un estándar para proteger la transmisión de esta información entre dispositivos PLC (Programmable Logic Controller) y SCADA (Supervisory Control and Data Acquisition), aumenta la vulnerabilidad de los sistemas ciberfísicos industriales [3].

2. Preguntas de investigación

Se determinaron seis preguntas de investigación que condujeron el desarrollo del presente mapeo sistemático de la literatura:

Tabla 1. Preguntas de investigación y motivación

Pregunta de investigación	Motivación
PI1: ¿Qué trabajos abordaron el cifrado de comunicaciones entre autómatas industriales?	Determinar los antecedentes de la aplicación de criptografía para la protección de ICS
PI2: ¿Qué trabajos abordaron la aplicación de protección criptográfica en entornos similares como IoT, IIoT, WSN y en niveles superiores de la Arquitectura de Purdue?	Determinar enfoques actuales aplicados en entornos y dispositivos similares, e implementaciones de criptografía en capas superiores al nivel de control
PI3: ¿Se ha aplicado criptografía sobre ICS (Industrial Control Systems) para su protección?	Identificar las últimas tendencias en cuanto a cifrado de comunicaciones entre autómatas industriales
PI4: ¿Las protecciones criptográficas fueron implementadas sobre el dispositivo o sobre el protocolo de red?	Determinar la capa, zona o sector de la red industrial donde se aplica la protección criptográfica (dispositivo, medio guiado, protocolo de red, etc.)
PI5: ¿Los algoritmos criptográficos implementados son ligeros/livianos o compatibles con dispositivos de poder de cómputo limitado?	Entender las capacidades y limitaciones de los dispositivos de pequeño porte (ej.: PLC) que realizarán el cifrado de la información
PI6: ¿Cuáles son los algoritmos criptográficos, protocolos de red y estándares implementados sobre ICS y similares?	Determinar los protocolos de red, de intercambio de claves, cifradores simétricos y estándares empleados sobre ICS en la actualidad

3. Métodos de revisión

En esta sección se explica el método empleado para el desarrollo del mapeo sistemático. El mismo es el propuesto en [4] y consta de tres pasos básicos: selección de bases de datos, definición de una cadena de búsqueda y selección de criterios de inclusión y exclusión.

3.1. Fuentes

En primer lugar se definieron los motores de búsqueda específicos para realizar las búsquedas. Fueron incluidos: IEEE Xplore, ACM Digital Library, ScienceDirect y SEDICI, complementando los mismos con el buscador "Google Scholar" y "ResearchGate" para maximizar los resultados.

3.2. Definición de términos

Con respecto a la cadena de búsqueda, en primer lugar se identificaron tres grupos de palabras clave:

Tabla 2. Términos empleados para la búsqueda

Términos principales	Términos alternativos
cybersecurity	industrial cybersecurity ciberseguridad ciberseguridad industrial
industrial control systems	programmable logic controller cyber-physical systems industrial automation control systems
cryptography lightweight cryptography	encryption criptografía criptografía ligera criptografía liviana

Posteriormente, se concatenaron los términos anteriores en una cadena de búsqueda para la primera iteración en los buscadores ya mencionados, uniendo términos de 1. o 2., con términos de 3. (ver Tabla 3).

La primera iteración en el buscador IEEE Xplore devolvió pocos resultados relevantes. Por ello, se refinó y modificó la cadena incluyendo los términos referentes a "Internet of Things", "Industrial Internet of Things", y sus correspondientes abreviaturas.

La segunda iteración en IEEE Xplore devolvió nuevamente pocos artículos relacionados, razón por la cual se modificó nuevamente la cadena, esta vez incluyendo términos alternativos referentes a los dispositivos empleados para control automático en el sector industrial, el protocolo de uso más extendedido en redes

industriales y la abreviatura para “Industrial Automation Control System” (PLC, SCADA, Modbus e IACS).

La iteración 3 resultó en la cadena de búsqueda más favorable para la identificación de artículos primarios en todos los buscadores excepto para ScienceDirect, buscador que presenta una limitación de empleo de hasta ocho operadores booleanos, por lo cual se realizó una reformulación.

Tabla 3. Cadenas de búsqueda

Iteración	Cadena de búsqueda
1	(("ciberseguridad") OR (“ciberseguridad industrial”) AND ("criptografía" OR "cifrado" OR "encriptación") OR ("industrial cybersecurity" OR "programmable logic controller" OR “cyber-physical systems”) AND ("cryptography" OR "encryption")
2	(("lightweight cryptography" OR "cryptography" OR "encryption") AND ("industrial" OR "cyber-physical" OR "cyber-physics" OR "iot" OR "internet of things" OR "industrial internet of things"))
3	(("lightweight cryptography" OR "cryptography" OR "encryption" OR "criptografía ligera" OR "criptografía") AND ("iacs" OR "ics" OR "plc" OR "scada" OR "modbus" OR "industrial"))
4 (ScienceDirect)	(("cryptography" OR "encryption" OR "criptografía ligera" OR "criptografía") AND ("ics" OR "plc" OR "scada" OR "modbus" OR "industrial"))

Una vez definida la cadena, se estableció como período de búsqueda el lapso comprendido entre el 2017 y el 2022 para los artículos de investigación primarios.

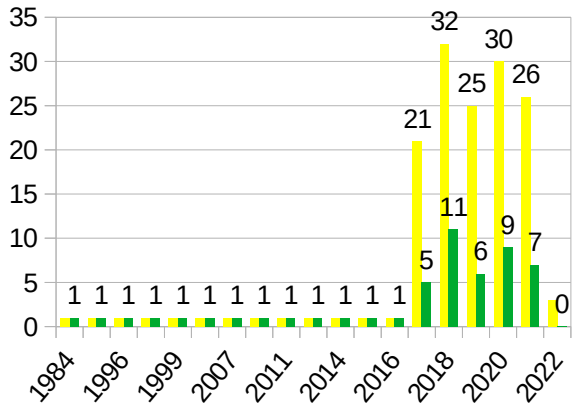

Figura 1. Número de artículos por año de publicación

3.3. Criterios de inclusión y exclusión

Por otra parte, los criterios de inclusión y exclusión definidos para el presente trabajo fueron los siguientes:

Tabla 4. Criterios de inclusión y exclusión

Nº	Criterio de inclusión
1	Artículos comprendidos en el período 2017-2022
2	Artículos redactados en inglés y español
3	Artículos que abordan la problemática propuesta desde el punto de vista de la ciberseguridad industrial
4	Artículos que implementan criptografía para su solución
5	Artículos que responden a las preguntas de investigación
Nº	**Criterio de exclusión**
1	Artículos no accesibles
2	Artículos redactados en otros idiomas
3	Artículos que implementan algoritmos criptográficos que no reunen propiedades post-cuánticas
4	Artículos que no abordan la problemática desde el punto de vista de la ciberseguridad industrial (en planta)
5	Artículos que no implementan criptografía para su solución
6	Artículos que proponen la adición de hardware para el cifrado de la información

Cabe destacar que existen artículos de investigación que se encuentran fuera del rango especificado, siendo estos las publicaciones originales de los algoritmos, estándares y protocolos implementados en los artículos primarios analizados.

4. Búsqueda de trabajos

Para la obtención de los artículos se siguió un procedimiento que consta de tres pasos, según la siguiente figura:

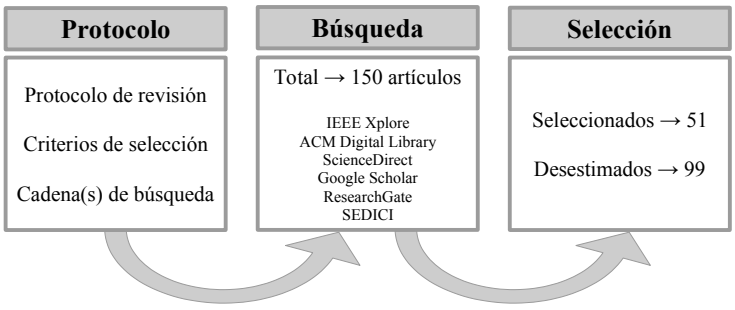

Figura 2. Pasos del proceso de mapeo sistemático de la literatura

El paso inicial consistió en el establecimiento del protocolo de revisión. Posteriormente se realizó la búsqueda de trabajos, obteniendo un total de 150 artículos, de los cuales resultaron excluidos 99 trabajos y aceptados 51 artículos.

De los seleccionados, se comprobó el cumplimiento de los criterios de inclusión, se determinó si respondían las PI y se extrajo el texto que respondía a cada una de ellas. Finalmente, se reunió toda la información extraída en el presente documento.

5. Síntesis de información obtenida durante el estudio

PI1: ¿Qué trabajos abordaron el cifrado de comunicaciones entre autómatas industriales?

En [5] se presentó un protocolo autenticado de establecimiento de clave para dispositivos IIoT (Industrial Internet of Things). El mismo fue basado en técnicas de hashing, compuertas XOR, PUF (Physically Unclonable Functions, funciones de una vía cuyo output depende de su única microestructura) y nonce (número aleatorio empleado por única vez para autenticación).

En [6] se empleó criptografía de curvas elípticas para desarrollar un criptosistema híbrido. El mismo está enfocado a sistemas de distribución de energía eléctrica inteligentes. Los autores aseguran que su propuesta resiste ataques de inyección, del tipo "replay", inyección de código, entre otros. Sin embargo, el algoritmo simétrico para cifrado de la información que se emplea es AES-128 [7], el cual no reúne condiciones de ligero/liviano y post-cuántico.

SDN_IIOT_EN [8] es un nuevo algoritmo criptográfico ligero para redes definidas por software para dispositivos IIoT. El mismo posee una longitud de clave de 128 bits, que cifra en bloques de 64 bits. Los autores dejan claro que el algoritmo posee ciertos aspectos a mejorar, como la cantidad de rondas a realizar por el mismo para encontrar un balance entre el tiempo de cifrado y su efecto.

Una simulación numérica [9] se llevó a cabo sobre un esquema novedoso de transmisión segura de datos para IIoT basado en el paradigma de "Fog Computing". La transmisión segura (y por consecuencia el cifrado de la información) se realiza en los nodos Fog, antes de ser subida a la nube. Por ende, en caso de existir un atacante que haya logrado el ingreso a la red industrial donde el protocolo de comunicaciones empleado sea Modbus TCP o similar, este tendrá acceso a los paquetes en claro.

En [10] se propuso MX-SORTS, algoritmo de configuración adaptativa para el cifrado y firma de tráfico de redes de subestaciones parte de smart grids. Si bien este enfoque no propone la adición de hardware específico o módulos de cifrado, las operaciones criptográficas se realizan en dispositivos Raspberry Pi, realizando el cifrado de la información fuera del dispositivo de control industrial que la produjo.

La factibilidad de implementación de un "encrypted controller" es analizada en [11], consistente en un módulo de cifrado homomórfico. Si bien se propone adición de hardware, en el mismo se implementa un "testbed" que puede ser tomado de ejemplo para la implementación de un Laboratorio de Ciberseguridad Industrial.

MACSec (Media Access Control Security, IEEE 802.1AE) es un estándar definido por el Institute of Electrical and Electronics Engineers para enlaces Ethernet punto a punto seguros. En [12] se propone una modificación a este protocolo para ser empleado en redes industriales donde los dispositivos "legacy" son la norma. Se implementó la suite criptográfica "ChaCha20-Poly1305" [13], la cual presenta propiedades post-cuánticas y de criptografía ligera.

En [14] se propuso un KMS (Key Management System) específico para ICS. En el documento se establecen los requerimientos puntuales para el protocolo, se proponen

las operaciones que realiza el mismo, pero no se realizan pruebas de concepto para demostrar su factibilidad. Más aún, los autores reconocen que su propuesta posee inconvenientes en términos de costo computacional, por lo cual siguen trabajando en mejoras a este problema.

Modbus TCP [15] es el protocolo de uso más extendido en las redes industriales actuales. Lamentablemente, al encapsularse sus mensajes dentro de la pila TCP/IP, la carga útil se transmite en claro. En [16] se propuso una implementación de este protocolo y se la aseguró mediante la adición de TLS (Transport Layer Security), consiguiendo tiempos de solicitud/respuesta por debajo de los 16,67 ms en infraestructuras de control de redes eléctricas.

En [17] se propuso un esquema de pre-distribución de claves basado en cálculos matriciales, donde las claves no son transmitidas por la red sino calculadas independientemente por los dispositivos desplegados en la misma.

El estudio realizado en [18] es de especial interés para el proyecto ya que trabaja directamente sobre ICS y su arquitectura particular. En este trabajo se aborda el estándar IEC 61499 de desarrollo de aplicaciones industriales, que emplea los denominados FB (Function Blocks). Los autores proponen una capa adicional denominada CL4FB (Confidentiality Layer for Function Blocks) para encriptar datos mediante el algoritmo AES, previo intercambio de claves mediante Diffie-Hellman.

La librería PLCrypto [19] es sin duda el trabajo más cercano a uno de los objetivos que persigue el proyecto de investigación. Se realizó una prueba de concepto sobre un PLC Allen-Bradley ControlLogix 5571, y el código fuente se encuentra disponible en la cuenta de GitHub de uno de los autores para facilitar su testeo y migración a otros vendors. El cifrado es realizado en la capa lógica de control, esto se traduce a algoritmos criptográficos codificados en ST (Structured Text) [20]. Dicho lenguaje es muy limitado ya que no soporta punteros y operaciones del tipo bit-wise shifting/rotation (cambio y rotación de bits). Se presenta una exhaustiva explicación de las limitaciones computacionales del PLC y distintos “benchmarks” como pruebas de rendimiento para cada uno de los algoritmos criptográficos aplicados. Sin embargo, su estudio debe enfocarse solamente en entender el funcionamiento de un PLC para ejecutar soluciones criptográficas en forma nativa. Por acertada recomendación del director del proyecto, no se aconseja la aplicación directa de PLCrypto sobre entornos reales, ambientes no virtualizados y/o aislados por técnicas de sandboxing debido a la aparente intención estatal del país de procedencia de este trabajo de investigación, de realizar inteligencia sobre ICS foráneos, siendo esta una vía ideal para infiltrar malware, a fin de satisfacer dichos requerimientos. En [21] se presenta el Plan 2025 para su desarrollo industrial, liberado durante el 2015. En [22] se detalla cómo un oficial de inteligencia de igual procedencia aguarda su sentencia por espionaje industrial sobre compañías extranjeras de la industria metalúrgica, de energía solar, de producción de chips para computadoras y laboratorios de investigación sobre COVID-19, entre otras. En forma más explicita aún, en [23] se detallan las tácticas de dicho estado para obtener en forma indiscriminada información sobre tecnología de punta para sus futuros desarrollos.

Finalizando con esta PI, en [24] se presentó un sistema generador de claves simétricas de cuatro etapas.

PI2: ¿Qué trabajos abordaron la aplicación de protección criptográfica en entornos similares como IoT, IIoT, WSN y en niveles superiores de la Arquitectura de Purdue?

En [25] y [26] se aplicó protección criptográfica sobre el medio guiado, en este caso consistente en fibra óptica. Los resultados demostraron que no se introduce "overhead" significante al cifrar las tramas Ethernet que se transmiten, alcanzando de esta manera un throughput cercano al máximo para el estándar 1000Base-X (1 Gbps).

En [27] se aplicó el algoritmo PRESENT-80 [28] sobre transistores experimentales TFET (tunnel field-effect transistor). El cifrador de bloque implementado (también empleado en PLCrypto) presenta propiedades criptográficas ligeras.

En [29] y [30] se propusieron criptosistemas basados en un protocolo Diffie-Hellman modificado. Mediante este, es posible comparar textos cifrados en servidores cloud para entornos IIoT.

Las tecnologías del tipo Blockchain también están teniendo un gran auge en los entornos IIoT. Se ha presentado en [31] un tokenizer portátil basado en esta tecnología, IBT (Industrial Blockchain Tokenizer) basado en la red Ethereum.

En [32] se aborda la problemática de distribución y gestión de claves a largo plazo para sistemas SCADA.

Un esquema criptográfico para sistemas ciberfísicos basado en la Matriz Q de Fibonacci fue desarrollado en [33]. Los beneficios de trabajar con ella se materializan en la baja complejidad computacional del esquema, que es de orden logarítmico.

Una infraestructura de gestión de claves para IACS (Industrial Automation Control Systems) fue presentada en [34].

En [35] se aplicó el stream cipher Trivium [36] sobre FPGA.

En [37], [38], [39] y [40] se estudian distintos esquemas de cifrado de clave pública específicos para IIoT que responden al paradigma de "Keyword-Based Encryption".

Los autores de [41] presentaron una propuesta de criptografía simétrica para dispositivos IoT. Aseguran haber encontrado dificultades al realizar los cálculos matriciales debido a la longitud de clave utilizada.

En [42] se aplicó criptografía de curvas elípticas sobre el protocolo LoRaWAN (Long Range Wide Area Network) para dispositivos IoT. Si bien se emplea el protocolo AES-128.

En [43] se presentó PERMS, criptosistema híbrido y ligero basado en PRESENT para procesadores ARM.

El trabajo realizado en [44] también es de especial interés para el proyecto de investigación, ya que propuso una modificación del software OpenPLC para lograr cifrado simétrico mediante el algoritmo AES-256.

En [45] se abordó un enfoque para elevar el nivel de seguridad en sistemas SCADA mediante la adición de una capa entre la física y la de enlace, basada en el principio de Shannon de un sistema incondicionalmente seguro.

En [46] se aplicó criptografía de curvas elípticas en redes WSN (Wireless Sensor Networks) para evitar un tipo de ataque muy particular: réplica de nodos.

Un enfoque basado en intercambio cuántico de claves es desarrollado en [47]. Se emplea el protocolo BB84 [48] sobre fibra óptica para el intercambio de claves, donde cada una de ellas es empleada una única vez para el cifrado de mensajes.

En [49] se propuso la técnica "Network Coding", que si bien no es un criptosistema completo, implica bajo costo computacional para corrección de errores y protección de mensajes de una red basada en protocolo Modbus.

En [50] se aplica tecnología Blockchain combinada con un protocolo denominado SSB (Secure Scuttlebutt Protocol) para aplicaciones descentralizadas de intercambio de mensajes, para la protección de la información en sistemas SCADA.

PI3: ¿Se ha aplicado criptografía sobre ICS (Industrial Control Systems) para su protección?

Por lo anteriormente expresado, se ha determinado que sí se ha aplicado criptografía sobre ICS. En mayor o menor medida, y en distintas capas, se ha protegido la información de redes industriales mediante técnicas criptográficas.

Se diferencias dos grandes grupos: cifrar o proteger la información una vez que esta se encuentra próxima a subirse a la nube o una vez en ella ([31], [29] y [10]), y encriptar o asegurar la información en el interior de la red industrial, para asegurar las mismas frente a atacantes que mediante escalada de privilegios logren acceder a la misma ([14], [16], [51], [5], [44], [6], [52], [11], [17], [42], [18], [19] y [32]).

PI4: ¿Las protecciones criptográficas fueron implementadas sobre el dispositivo o sobre el protocolo de red?

Con respecto a esta PI, se han diferenciado tres grupos: estudios en los cuales se aplicó criptografía directamente en el dispositivo ([5], [18], [27], [14], [11], [19] y [6]), trabajos donde se implementó protección criptográfica sobre el o los protocolos de red ([31], [12], [42], [29], [52], [25], [51], [40], [16] y [10]), y artículos en los cuales las modificaciones fueron probadas mediante software de simulación ([44] y [24]).

PI5: ¿Los algoritmos criptográficos implementados son ligeros/livianos o compatibles con dispositivos de poder de cómputo limitado?

Dado que la intención es cifrar la información desde los más bajos niveles, los algoritmos a implementar deben ser ligeros para posibilitar su procesamiento en dispositivos de pequeño porte.

Se han diferenciado diferentes grupos al responder esta PI: trabajos donde se aplica criptografía de curvas elípticas con características ligeras ([42], [46] y [6]), desarrollos en los que se aplicó cifradores de bloque (block ciphers) ligeros ([19], [27], [43] y [8]), implementaciones de cifradores de flujo (stream ciphers) ligeros ([35]) y artículos donde se implementó la propuesta en entornos reales o simulados para comprobar que el retardo añadido era mínimo ([45], [10], [24], [5], [33] y [8]).

PI6: ¿Cuáles son los algoritmos criptográficos, protocolos de red y estándares implementados sobre ICS y similares?

Es necesario conocer ciertos estándares de la electrónica industrial para lograr las competencias específicas que el desarrollo de nuevas soluciones para estos dispositivos requieren. El estándar IEC 61131-3 describe los lenguajes de programación específicos para dispositivos PLC y similares [20].

Sobre los protocolos de red, si bien existen varias alternativas, Modbus TCP [15] es el de uso más extendido actualmente en la industria.

Por otro lado, se resumen en la siguiente tabla los algoritmos criptográficos implementados en los artículos de investigación primarios presentados en este mapeo:

Tabla 5. Algoritmos implementados en artículos de investigación primarios

Propuesta	Algoritmo / Protocolo	Longitud de bloque	Longitud de clave / hash	Tipo
PLCrypto [19]	Chaskey [57]	-------	128 bits	MAC
	PRESENT [28]	64 bits	80 bits	Block cipher
	SIMON [58]	32 bits	64 bits	Block cipher
		48 bits	72 bits / 96 bits	
		64 bits	96 bits / 128 bits	
		96 bits	96 bits / 144 bits	
		128 bits	128 bits / 192 bits / 256 bits	
	SPECK [58]	32 bits	64 bits	Block cipher
		48 bits	72 bits / 96 bits	
		64 bits	96 bits / 128 bits	
		96 bits	96 bits / 144 bits	
		128 bits	128 bits / 192 bits / 256 bits	
	SPONGENT [53]	-------	88 bits / 128 bits / 224 bits / 256 bits	Hash function
	PHOTON [54]	-------	80 bits / 128 bits / 160 bits / 224 bits / 256 bits	Hash function
	Subset-sum based OWF [55]	256 bits / 384 bits / 512 bits	-------	Primitiva criptográfica alternativa
	UOWHF [56]	32 bits	64 bits	Primitiva criptográfica alternativa
		64 bits	128 bits	
		128 bits	128 bits	
		128 bits	256 bits	
Hybrid encryption scheme [6]	AES [7]	128 bits	128 bits / 192 bits / 256 bits	Block cipher
Security in IEC 61499 Systems [18]				
Rejoin Mechanism for LoRaWAN Using ECC [42]				
Securing SCADA using OpenPLC [44]				

Propuesta	Algoritmo / Protocolo	Longitud de bloque	Longitud de clave / hash	Tipo
MACsec for ICS [12]	ChaCha20-Poly1305 [13]	128 bits	256 bits (clave) / 96 bits (nonce)	Stream cipher + MAC
Lightweight encryption using stream ciphers [35]	TRIVIUM [36]	-------	80 bits	Stream cipher
Communication based on quantum encryption [47]	BB84 [48]	-------	Según acuerdo entre emisor y receptor	Protocolo cuántico

6. Conclusiones

Se ha determinado que la aplicación de criptografía sobre entornos industriales ya ha sido abordada. Por ello, desde el proyecto "Ciberseguridad en Sistemas Operacionales" ([59], [60], [61] y [62]) se está trabajando para realizar una contribución novedosa, perdurable en el tiempo, de implementación sencilla, económica y basada en criptografía post-cuántica. Se desestima la adición de hardware, ya que esto elevaría costos y tiempos de implementación, dificultando la transferencia tecnológica hacia la industria.

Se detectan ciertas dificultades, tales como los limitados recursos que presentan los autómatas industriales, sumado a la especificidad de los estándares y lenguajes de programación vigentes en el campo de la electrónica industrial. Se recomienda trabajar en lenguaje ST (Structured Text), ya que el mismo permite manejo de variables y ejecución de ciertas operaciones matemáticas. Es importante también, observar las últimas tendencias sobre "Criptografía Ligera", para eventualmente aplicar algoritmos criptográficos que cumplan con dicha característica.

Referencias

[1] G. Assenza, L. Faramondi, G. Oliva, and R. Setola, "Cyber threats for operational technologies," *International Journal of System of Systems Engineering*, vol. 10, no. 2, pp. 128–142, 2020, doi: 10.1504/IJSSE.2020.109127.

[2] L. L. Dhirani, E. Armstrong, and T. Newe, "Industrial IoT, cyber threats, and standards landscape: Evaluation and roadmap," *Sensors*, vol. 21, no. 11, Jun. 2021, doi: 10.3390/S21113901.

[3] M. Herrero Collantes and A. López Padilla, "Protocolos y seguridad de red en infraestructuras de SCI," España, 2015. Accessed: Jan. 08, 2022. [Online]. Available: https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/incibe_protocolos_seguridad_red_sci.pdf

[4] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering - A systematic literature review," *Information and Software Technology*, vol. 51, no. 1. Elsevier, pp. 7–15, Jan. 01, 2009. doi: 10.1016/j.infsof.2008.09.009.

[5] M. Masud, M. Alazab, K. Choudhary, and G. S. Gaba, "3P-SAKE: Privacy-preserving and physically secured authenticated key establishment protocol for wireless industrial networks," *Computer Communications*, vol. 175, pp. 82–90, Jul. 2021, doi: 10.1016/J.COMCOM.2021.04.021).

[6] S. Khasawneh and M. Kadoch, "A hybrid encryption scheme for advanced metering infrastructure networks," in *The proceedings of the 1st EAI international conference on smart grid assisted internet of things, Sault Ste. Marie*, Aug. 2017, pp. 1–11. doi: 10.4108/EAI.7-8-2017.152990.

[7] J. Daemen and V. Rijmen, "AES Proposal: Rijndael," *First Advanced Encryption Standard (AES) Conference*, vol. 1, 1998.

[8] D. Ma and Y. Shi, "A Lightweight Encryption Algorithm for Edge Networks in Software-Defined Industrial Internet of Things," in *2019 IEEE 5th International Conference on Computer and Communications, ICCC 2019*, Dec. 2019, pp. 1489–1493. doi: 10.1109/ICCC47050.2019.9064352.

[9] H. Hui, C. Zhou, S. Xu, and F. Lin, "A novel secure data transmission scheme in industrial internet of things," *China Communications*, vol. 17, no. 1, pp. 73–88, Jan. 2020, doi: 10.23919/JCC.2020.01.006.

[10] H. Zhang, B. Qin, T. Tu, Z. Guo, F. Gao, and Q. Wen, "An adaptive encryption-as-a-service architecture based on fog computing for real-time substation communications," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 1, pp. 658–668, Jan. 2019, doi: 10.1109/TII.2019.2948113.

[11] X. Li, M. Liu, R. Zhang, P. Cheng, and J. Chen, "Demo Abstract: An Industrial Control System Testbed for the Encrypted Controller," in *Proceedings - 9th ACM/IEEE International Conference on Cyber-Physical Systems, ICCPS 2018*, Aug. 2018, pp. 343–344. doi: 10.1109/ICCPS.2018.00045.

[12] T. Lackorzynski, G. Garten, J. S. Huster, S. Kopsell, and H. Hartig, "Enabling and Optimizing MACsec for Industrial Environments," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7599–7606, Nov. 2021, doi: 10.1109/TII.2020.3040966.

[13] A. Langley, W. Chang, N. Mavrogiannopoulos, J. Strombergson, and S. Josefsson, "Chacha20-Poly1305 cipher suites for Transport Layer Security (TLS)," no. July, pp. 1–23, 2016, Accessed: Jan. 03, 2022. [Online]. Available: https://www.hjp.at/doc/rfc/rfc7905.html

[14] Z. Drias, A. Serhrouchni, and O. Vogel, "Identity-based cryptography (IBC) based key management system (KMS) for industrial control systems (ICS)," *2017 1st Cyber Security in Networking Conference, CSNet 2017*, vol. 2017-Janua, pp. 1–10, Dec. 2017, doi: 10.1109/CSNET.2017.8242008.

[15] A. Swales, "Open Modbus/TCP specification," 1999. Accessed: Dec. 27, 2022. [Online]. Available: http://www.dankohn.info/projects/Fieldpoint_module/Open_ModbusTCP_Standard.pdf

[16] M. K. Ferst, H. F. M. De Figueiredo, G. Denardin, and J. Lopes, "Implementation of secure communication with modbus and transport layer security protocols," in *2018 13th IEEE International Conference on Industry*

Applications, INDUSCON 2018 - Proceedings, Jan. 2019, pp. 155–162. doi: 10.1109/INDUSCON.2018.8627306.

[17] P. T. C. *et al.*, "Key pre-distribution scheme with join leave support for SCADA systems," *International Journal of Critical Infrastructure Protection*, vol. 24, pp. 111–125, Mar. 2019, doi: 10.1016/J.IJCIP.2018.10.011.

[18] A. Tanveer, R. Sinha, and S. G. Macdonell, "On Design-time Security in IEC 61499 Systems: Conceptualisation, Implementation, and Feasibility," in *Proceedings - IEEE 16th International Conference on Industrial Informatics, INDIN 2018*, Sep. 2018, pp. 778–785. doi: 10.1109/INDIN.2018.8472093.

[19] Z. Yang, Z. Bao, C. Jin, Z. Liu, and J. Zhou, "PLCrypto: A symmetric cryptographic library for programmable logic controllers," *IACR Transactions on Symmetric Cryptology*, vol. 2021, no. 3, pp. 170–217, 2021, doi: 10.46586/tosc.v2021.i3.170-217.

[20] K.-H. John and M. Tiegelkamp, *IEC 61131-3: Programming Industrial Automation Systems*. 2001. doi: 10.1007/978-3-662-07847-1.

[21] "Made in China 2025," China, 2015. [Online]. Available: http://www.cittadellascienza.it/cina/wp-content/uploads/2017/02/IoT-ONE-Made-in-China-2025.pdf

[22] S. Ben-Achour, "China's state-backed cyberattacks are part of a larger plan - Marketplace," *Marketplace*, 2021. https://www.marketplace.org/2021/12/09/chinas-state-sponsored-industrial-espionage-is-part-of-a-larger-system/ (accessed Jan. 10, 2023).

[23] D. A. Levine, "Made in China 2025," *Source: Journal of Strategic Security*, vol. 13, no. 3, pp. 1–16, 2020, doi: 10.2307/26936543.

[24] E. H. Riyadi, T. K. Priyambodo, and A. E. Putra, "The Dynamic Symmetric Four-Key-Generators System for Securing Data Transmission in the Industrial Control System," *International Journal of Intelligent Engineering and Systems*, vol. 14, no. 1, pp. 376–386, 2021, doi: 10.22266/IJIES2021.0228.35.

[25] A. Pérez-Resa, M. Garcia-Bosque, C. Sánchez-Azqueta, and S. Celma, "Physical Layer Encryption for Industrial Ethernet in Gigabit Optical Links," *IEEE Transactions on Industrial Electronics*, vol. 66, no. 4, pp. 3287–3295, Apr. 2019, doi: 10.1109/TIE.2018.2847670.

[26] A. Pérez-Resa, M. Garcia-Bosque, C. Sánchez-Azqueta, and S. Celma, "Chaotic Encryption Applied to Optical Ethernet in Industrial Control Systems," *IEEE Transactions on Instrumentation and Measurement*, vol. 68, no. 12, pp. 4876–4886, Dec. 2019, doi: 10.1109/TIM.2019.2896550.

[27] H. Thapliyal, T. S. S. Varun, and S. Dinesh Kumar, "Low-power and secure lightweight cryptography via tfet-based energy recovery circuits," in *2017 IEEE International Conference on Rebooting Computing, ICRC 2017 - Proceedings*, Nov. 2017, pp. 1–4. doi: 10.1109/ICRC.2017.8123640.

[28] A. Bogdanov *et al.*, "PRESENT: An ultra-lightweight block cipher," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2007, vol. 4727 LNCS, pp. 450–466. doi: 10.1007/978-3-540-74735-2_31.

[29] A. Hassan, R. Elhabob, U. Ibrahim, and Y. Wang, "Efficient Public Key Cryptography Scheme with Equality Test for Heterogeneous Systems in IIoT," in *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*, 2020, vol. 12383 LNCS, pp. 108–121. doi: 10.1007/978-3-030-68884-4_9.

[30] R. Elhabob, Y. Zhao, I. Sella, and H. Xiong, "An efficient certificateless public key cryptography with authorized equality test in IIoT," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 3, pp. 1065–1083, Mar. 2020, doi: 10.1007/S12652-019-01365-4.

[31] D. Mazzei *et al.*, "A Blockchain Tokenizer for Industrial IOT trustless applications," *Future Generation Computer Systems*, vol. 105, pp. 432–445, Apr. 2020, doi: 10.1016/J.FUTURE.2019.12.020.

[32] H. Saputra and Z. Zhao, "Long term key management architecture for SCADA systems," *IEEE World Forum on Internet of Things*, pp. 314–319, May 2018, doi: 10.1109/WF-IoT.2018.8355183.

[33] T. Zhou, J. Shen, X. Li, C. Wang, and H. Tan, "Logarithmic encryption scheme for cyber–physical systems employing Fibonacci Q-matrix," *Future Generation Computer Systems*, vol. 108, pp. 1307–1313, Jul. 2020, doi: 10.1016/j.future.2018.04.008.

[34] T. C. Pramod and N. R. Sunitha, "Key management infrastructure design and novel techniques to establish secure communications in critical infrastructures," in *International Journal of Critical Computer-Based Systems*, 2017, vol. 7, no. 2, pp. 171–189. doi: 10.1504/IJCCBS.2017.084930.

[35] T. Hiscock, O. Savry, and L. Goubin, "Lightweight instruction-level encryption for embedded processors using stream ciphers," *Microprocessors and Microsystems*, vol. 64, pp. 43–52, Feb. 2019, doi: 10.1016/j.micpro.2018.10.001.

[36] C. De Cannière and B. Preneel, "Trivium," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 4986 LNCS, pp. 244–266, 2008, doi: 10.1007/978-3-540-68351-3_18.

[37] M. Ma, D. He, N. Kumar, K.-K. R. K. R. Choo, and J. Chen, "Certificateless searchable public key encryption scheme for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 2, pp. 759–767, Feb. 2017, doi: 10.1109/TII.2017.2703922.

[38] D. He, M. Ma, S. Zeadally, N. Kumar, and K. Liang, "Certificateless public key authenticated encryption with keyword search for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3618–3627, Aug. 2017, doi: 10.1109/TII.2017.2771382.

[39] P. Liu, K. Liu, T. Fu, Y. Zhang, and J. Hu, "A privacy-preserving resource trading scheme for Cloud Manufacturing with edge-PLCs in IIoT," *Journal of Systems Architecture*, vol. 117, p. 102104, Aug. 2021, doi: 10.1016/J.SYSARC.2021.102104.

[40] N. Pakniat, D. Shiraly, and Z. Eslami, "Certificateless authenticated encryption with keyword search: Enhanced security model and a concrete

construction for industrial IoT," *Journal of Information Security and Applications*, vol. 53, p. 102525, Aug. 2020, doi: 10.1016/j.jisa.2020.102525.

[41] G. Manikandan and R. Perumal, "Symmetric cryptography for secure communication in IoT," *Materials Today: Proceedings*, Nov. 2020, doi: 10.1016/j.matpr.2020.09.737.

[42] S. Milani and I. Chatzigiannakis, "Design, Analysis, and Experimental Evaluation of a New Secure Rejoin Mechanism for LoRaWAN Using Elliptic-Curve Cryptography," *Journal of Sensor and Actuator Networks*, vol. 10, no. 2, p. 36, Jun. 2021, doi: 10.3390/JSAN10020036.

[43] C. G. Thorat and V. S. Inamdar, "Implementation of new hybrid lightweight cryptosystem," *Applied Computing and Informatics*, vol. 16, no. 1–2, pp. 195–206, 2018, doi: 10.1016/j.aci.2018.05.001.

[44] T. Alves, T. Morris, and S.-M. M. Yoo, "Securing SCADA applications using OpenPLC with end-to-end encryption," in *Proceedings of the 3rd Annual Industrial Control System Security Workshop*, Dec. 2017, pp. 1–6. doi: 10.1145/3174776.3174777.

[45] T. Cherifi and L. Hamami, "A practical implementation of unconditional security for the IEC 60780-5-101 SCADA protocol," *International Journal of Critical Infrastructure Protection*, vol. 20, pp. 68–84, Mar. 2018, doi: 10.1016/J.IJCIP.2017.12.001.

[46] L. Sujihelen and C. Jayakumar, "Inclusive elliptical curve cryptography (IECC) for wireless sensor network efficient operations," *Wireless Personal Communications*, vol. 99, no. 2, pp. 893–914, Mar. 2018, doi: 10.1007/S11277-017-5157-4.

[47] W. Yang, Y. Peisong, and Z. Qianchuan, "Industry trusted network communication based on quantum encryption," in *Chinese Control Conference, CCC*, Jul. 2019, pp. 7016–7022. doi: 10.23919/ChiCC.2019.8865710.

[48] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, no. P1, pp. 7–11, Mar. 1984, doi: 10.1016/j.tcs.2014.05.025.

[49] S. Nazir and M. Kaleem, "Random Network Coding for Secure Packet Transmission in SCADA Networks," in *2018 3rd International Conference on Emerging Trends in Engineering, Sciences and Technology, ICEEST 2018*, Feb. 2019, pp. 1–4. doi: 10.1109/ICEEST.2018.8643329.

[50] R. Brandão, "A blockchain-based protocol for message exchange in a ICS network: student research abstract," in *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, Mar. 2020, pp. 357–360. doi: 10.1145/3341105.3374231.

[51] T. Alves, R. Das, and T. Morris, "Embedding Encryption and Machine Learning Intrusion Prevention Systems on Programmable Logic Controllers," *IEEE Embedded Systems Letters*, vol. 10, no. 3, pp. 99–102, Sep. 2018, doi: 10.1109/LES.2018.2823906.

[52] X. Zhang, X. Cai, C. Wang, K. Han, and S. Zhang, "A dynamic security control architecture for industrial cyber-physical system," *Proceedings - IEEE*

International Conference on Industrial Internet Cloud, ICII 2019, pp. 148–151, Nov. 2019, doi: 10.1109/ICII.2019.00038.

[53] A. Bogdanov, M. Knežević, G. Leander, D. Toz, K. Varici, and I. Verbauwhede, "SPONGENT: The design space of lightweight cryptographic hashing," *IEEE Transactions on Computers*, vol. 62, no. 10, pp. 2041–2053, 2013, doi: 10.1109/TC.2012.196.

[54] J. Guo, T. Peyrin, and A. Poschmann, "The PHOTON family of lightweight hash functions," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 6841 LNCS, pp. 222–239, 2011, doi: 10.1007/978-3-642-22792-9_13.

[55] R. Impagliazzo and M. Naor, "Efficient cryptographic schemes provably as secure as subset sum," *Journal of Cryptology*, vol. 9, no. 4, pp. 199–216, Sep. 1996, doi: 10.1007/BF00189260.

[56] M. Naor and M. Yung, "Universal one-way hash functions and their cryptographic applications," in *Proceedings of the twenty-first annual ACM symposium on Theory of computing*, 1989, pp. 33–43. doi: 10.1145/73007.73011.

[57] N. Mouha, B. Mennink, A. Van Herrewege, D. Watanabe, B. Preneel, and I. Verbauwhede, "Chaskey: An efficient MAC algorithm for 32-bit microcontrollers," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2014, vol. 8781, pp. 306–323. doi: 10.1007/978-3-319-13051-4_19.

[58] R. Beaulieu, S. Treatman-Clark, D. Shors, B. Weeks, J. Smith, and L. Wingers, "The SIMON and SPECK lightweight block ciphers," in *Proceedings - Design Automation Conference*, 2015, vol. 2015-July. doi: 10.1145/2744769.2747946.

[59] J. Kamlofsky, S. Abdel Masih, H. Colombo, C. Milio, and P. Hecht, "Ciberseguridad en los sistemas de control industrial: clave para la ciberdefensa de las infraestructuras críticas," in *XXI Workshop de Investigadores en Ciencias de la Computación*, 2019, pp. 971–974. Accessed: May 01, 2021. [Online]. Available: http://sedici.unlp.edu.ar/handle/10915/77258

[60] J. Kamlofsky *et al.*, "Seguridad en las redes industriales: clave para la ciberdefensa de las infraestructuras críticas," *XIX Workshop de Investigadores en Ciencias de la Computación*, vol. 9, pp. 1089–1094, 2017, Accessed: May 17, 2021. [Online]. Available: http://sedici.unlp.edu.ar/handle/10915/62725

[61] J. Kamlofsky, H. Colombo, M. Sliafertas, and J. Pedernera, "Un Enfoque para Disminuir los Efectos de los Ciber-ataques a las Infraestructuras Críticas," *III Congreso Nacional de Ingeniería Informática Sistemas de Información (CONAIISI)*, vol. 3, pp. 2346–9927, 2015, [Online]. Available: https://www.f-secure.com/v-descs/korgo.shtml

[62] J. Kamlofsky, S. A. Masih, H. Colombo, and D. Veiga, "Ciberdefensa de Infraestructuras Industriales," *XVII Workshop de Investigadores en Ciencias de la Computación*, vol. 17, 2015, Accessed: May 20, 2021. [Online]. Available: http://sedici.unlp.edu.ar/handle/10915/46259