# UNIVERSIDAD POLITÉCNICA SALESIANA
# SEDE QUITO

**CARRERA:**
**INGENIERÍA ELÉCTRICA**

**Trabajo de titulación previo a la obtención del título de**
**INGENIERO ELÉCTRICO**

**TEMA:**
**SEGURIDAD EN EL SISTEMA DE GESTIÓN DE DATOS MEDIDOS DE ENERGÍA ELÉCTRICA APLICANDO CIFRADO HOMOMÓRFICO**

**AUTOR:**
**BYRONE DARIO RUGEL CAMPOVERDE**

**TUTOR:**
**ESTUARDO JOSAFAT CORREA ZAPATA**

**Quito, febrero 2019**

Datos de Catalogación Bibliográfica

Byrone Dario Rugel Campoverde

**SEGURIDAD EN EL SISTEMA DE GESTIÓN DE DATOS MEDIDOS DE ENERGÍA ELÉCTRICA APLICANDO CIFRADO HOMOMÓRFICO**

Universidad Politécnica Salesiana, Quito – Ecuador 2019
Ingeniería Eléctrica

Breve reseña historia e información de contacto:

**Byrone Dario Rugel Campoverde** (Y'1991-M'05). Realizó sus estudios secundarios en el "Liceo Naval", se graduó de Físico Matemático. Egresado de la Facultad de Ingeniería Eléctrica en la Universidad Politécnica Salesiana. Su trabajo se basa en Seguridad en el sistema de gestión de datos medidos de energía eléctrica aplicando cifrado homomórfico.
byronedario@gmail.com

Dirigido por:

**Estuardo Josafat Correa Zapata** (Y'1963 – M'09). Se graduó de Ingeniero de Sistemas en 1997 en la Escuela Politécnica Nacional de Quito – Ecuador, recibió su grado de Magister en Educación Universitaria en 2010 en la Universidad Tecnológica Indoamérica de Quito, Ecuador. Sus trabajos de investigación están relacionados con técnicas de modelado y simulación matemática para la planificación de redes de distribución eléctrica en redes inteligentes.
ecorrea@ups.edu.ec

## DECLARATORIA DE COAUTORÍA DEL DOCENTE TUTOR/A

Yo, Estuardo Josafat Correa Zapata declaro que bajo mi dirección y asesoría fue desarrollado el trabajo de titulación *Seguridad en el sistema de gestión de datos medidos de energía eléctrica aplicando cifrado homomórfico* realizado por Byrone Dario Rugel Campoverde, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana para ser considerados como trabajo final de titulación.

Quito, febrero 2019

Estuardo Josafat Correa Zapata
Cédula de identidad: 170818330-4

## CESIÓN DE DERECHOS DE AUTOR

Yo, Byrone Dario Rugel Campoverde, con documento de identificación N° 172079891-5, manifiesto mi voluntad y cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor/es del trabajo de grado/titulación intitulado: "SEGURIDAD EN EL SISTEMA DE GESTIÓN DE DATOS MEDIDOS DE ENERGÍA ELÉCTRICA APLICANDO CIFRADO HOMOMÓRFICO", mismo que ha sido desarrollado para optar por el título de: Ingeniero Eléctrico, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia, suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

Firma

.....

Nombre: Byrone Dario Rugel Campoverde

Cédula: 172079891-5

Fecha: Quito, febrero 2019

## 1. ÍNDICE GENERAL

## 2. ÍNDICE DE FIGURAS



## 3. ÍNDICE DE TABLAS

# SEGURIDAD EN EL SISTEMA DE GESTIÓN DE DATOS MEDIDOS DE ENERGÍA ELÉCTRICA APLICANDO CIFRADO HOMOMÓRFICO


## Resumen

El sector eléctrico ecuatoriano está pasando por un gran desarrollo debido al crecimiento poblacional y la implementación de nuevas tecnologías tanto en el campo de la generación como en el de la distribución, lo que ha provocado un aumento en el consumo energético, esto se traduce en un aumento de flujo de información por medio de la red eléctrica ecuatoriana, por otro lado, la información es un recurso valioso y privado que las compañías eléctricas tienen que proteger, para ello los nuevos dispositivos de medición de energía inteligentes podrían adaptarse a un sistema de encriptación homomórfico de información, con el objetivo de salvaguardar los datos de los usuarios. En este trabajo se estudia y analiza la seguridad de los archivos generados en el sistema de gestión de datos de energía eléctrica y se implementa el cifrado totalmente homomórfico para encriptar y desencriptar archivos de tal forma que la información solo sea accesible mediante el uso de una clave o llave, utilizando herramientas de desarrollo actuales y acordes al tema. Además, se realizó una comparativa entre el cifrado propuesto y otros tipos de cifrado logrando determinar que el cifrado homomórfico puede utilizar numero reales a diferencia de otros que solo usan números enteros positivos.



***Palabras Clave:*** homomórfico, información, medición, redes, seguridad.



## Abstract

The Ecuadorian electric sector is going through a great development due to the population growth and the implementation of new technologies, such in the generation field as in the distribution field. This has caused a raise of energetic consumption, and given place to an increase in the information flow through the Ecuadorian electricity network. On the other hand, information is a valuable and private resource that the electronic companies have to protect. For this, the new smart energy measurement devices could adapt to an homomorphic information encryption system, with the aim of safeguarding the users data.

In this work the security of the files generated in the electric power data management system is studied and analyzed, and the fully homomorphic encryption is implemented to encrypt and decrypt files, so that the information is only accessible through a password or key, using tools of current development and relating to the theme.

In addition, a comparison was made between the proposed encryption and other types of encryption, determining that the homomorphic cipher can use real numbers, unlike others that only use positive integers.



***Keywords:*** homomorphic, information, measurement, networks, security.

# 1. Introducción

En la actualidad el sector eléctrico está pasando por grandes cambios como la utilización de energías renovables, matriz energética, biocombustibles, y el uso eficiente de energía. La eficiencia energética está jugando un rol determinante en este crecimiento, que juntamente con el uso de redes inteligentes, reflejan sus resultados en el menor consumo de energía y por ende menor gasto económico en los usuarios como lo afirma Michael Wagner en [1]. Las redes inteligentes (Smart Grids) son vistas por numerosas y diversas partes interesadas como el enfoque de próxima generación con el objetivo de proporcionar electricidad a millones de hogares en todo el mundo, estas redes han introducido capacidades de computación y comunicación en las redes eléctricas tradicionales para actualmente hacerlas "inteligentes" y "conectadas" [1]. La comunicación se realiza mediante chips encargados del procesamiento y con unidades de almacenamiento incorporadas en los medidores de electricidad tradicionales, de modo que son capaces de realizar funciones "inteligentes". Luego, los medidores inteligentes se comunican con los electrodomésticos en el hogar, así como también con las instalaciones de generación y administración de las compañías eléctricas, proporcionando redes inteligentes con una gran conectividad [2]. El aumento de electricidad consumida por los diferentes usuarios en la red eléctrica unido al desconocimiento de la cantidad de corriente que consumen los diferentes equipos electrodomésticos ha hecho que hoy en día sea cotidiano escuchar acerca de las redes inteligentes, que a menudo se relacionan con el concepto de medición inteligente ya que tienen la capacidad de ofrecer a los usuarios un detalle de la cantidad de energía consumida de manera periódica y asegurar el consumo eficiente de la misma[3]. Los medidores inteligentes por el contrario de los medidores convencionales que solo muestran la potencia eléctrica consumida por hora son capaces de mostrar el consumo diario y así poder crear perfiles de carga, permiten facturar en tiempo real, y le dan la posibilidad de visualizar el historial de la energía consumida, por lo que no solo otorga beneficios al consumidor sino también la empresa distribuidora [4].

Como la demanda eléctrica en Ecuador está en aumento, se están incorporando a la red nuevos y mejores medidores electromecánicos, que tienen ventajas sobre sus predecesores, por ejemplo: la variedad de datos medidos, mejor detalle en la información, facilidad de lectura a distancia, y la notificación en caso de manipulación del medidor. Estas optimizaciones de recursos operativos se ven reflejados en la menor necesidad de intervención de recursos humanos [5].

Una de las mejoras de los sistemas de medición nuevos es una mejor interfaz, que incluye al usuario en sus gastos y no lo hace un consumidor pasivo sino uno que se ajusta a sus necesidades. Estos nuevos equipos medidores abren un nuevo campo de redes eléctricas inteligentes.

El tema “redes inteligentes” ha abierto un campo interesante en cuanto a la protección de la información manejada por cada usuario. La información es un recurso invaluable en una empresa, por lo que cifrar esta información es fundamental [6]. Cifrar o encriptar datos es alterarlos de alguna forma, usualmente mediante una clave o llave, con el objetivo de que no sean legibles para quien no posea la misma. Con la llave, los poseedores van a ser capaces de descifrar los datos y poder leer la información antes encriptada. Cifrar y descifrar datos son procesos que toman un determinado tiempo, que en múltiples ocasiones es muy extenso, por

tanto, es crucial preguntarse si es o no necesario cifrar la información, una posible respuesta es que para cualquier empresa resulta devastador perder la información de sus usuarios, debido a que estas pérdidas pueden ocasionar el cierre total de sus actividades.

Los beneficios de cifrar la información de una empresa son muchos, por ejemplo, se protege la información privada que, de caer en manos equivocadas, lo que puede provocar perjuicios económicos, pérdidas de ventaja en el mercado o incluso el cierre de la empresa como lo afirma Beth-Anne Schuelke-Leech en [7]. El robo de información respectiva a los clientes puede dañar la imagen de la empresa, lo que puede causar daños irreparables. El cifrado se usa principalmente en la trasmisión de información porque esta viaja a través de medios externos por lo que es susceptible a ser interceptada.

El uso de información cifrada es fundamental para la protección tanto de los clientes como de la empresa que provee el servicio. Existen diferentes tipos de cifrados utilizados para encriptar la información, pero se hará énfasis en un tipo específico de cifrado de información, el cual es el cifrado homomórfico, que actualmente podría ser aplicado a los medidores inteligentes del sistema eléctrico ecuatoriano. Se describirá matemáticamente su funcionamiento con el objetivo de entenderlos y así ayudar a la correcta evolución de las redes inteligentes del sistema eléctrico ecuatoriano, con vistas a mejorar la eficiencia del consumo energético [1],[8].

En la sección 2 de este documento se pueden ver algunos antecedentes de protocolos de seguridad comúnmente usados por los medidores inteligentes, así como los protocolos de cifrado propuestos. En la sección 3 se propone los tipos de cifrado aptos para nuestro propósito y se evalúa su viabilidad para realizar este proceso. En la sección 4 se presenta el cifrado homomórfico y su aplicación directa en los sistemas de redes eléctricas. En la sección 5 se desarrolla el código de programación homomórfica, la sección 6 se evalúa el desempeño del programa de encriptación y también se presenta la comparación del modelo empleado con respecto a otros modelos propuestos. La Sección 7 contiene las conclusiones y recomendaciones realizadas en base a la teoría de encriptación homomórfica y sus resultados simulados. Finalmente, en la Sección 8 se concluye el desarrollo de este documento presentando las citas bibliográficas de apoyo.

## 2. Trabajos relacionados

La investigación sobre las redes inteligentes abarca un amplio espectro: comenzando por la tecnología mencionada en los trabajos de K. Moslehi en [9] y de A. Bose en [10], luego en la economía, el marketing, las políticas y cuestiones legales mencionadas por R. E. Schuler en [11]; llegando su investigación por la generación de potencia, transmisión, distribución según Zu Wei en [12], la gestión de carga, diagnóstico y recuperación de fallos según B. Saint en [13], y B. D. Russell y C. L. Benner en [14]; para finalizar con la implementación y comunicaciones de los medidores inteligentes en [15], [16] y [17] mencionado por E. Inga, A. Rubio y Milton Ruiz respectivamente.

Entre estos temas, se tiene un particular interés en la seguridad y la privacidad de las redes inteligentes. Dentro de la investigación realizada por B. Schuelke-Leech, B. Barry, M. Muratori, y B. Yurkovich en [7], identifica varias vulnerabilidades, amenazas de seguridad e invaciones de privacidad en redes inteligentes, lo que llama la atención y los esfuerzos del gobierno, del mundo académico y de la industria en [18] H. Khurana revisa los desafíos de seguridad en redes inteligentes, con

un enfoque especial en la confianza, la autenticación y el cifrado en [19] y [20], McDaniel-MacLaughlin y Metke-Ekl, respectivamente, han articulado los requisitos de seguridad para redes inteligentes, y señalaron diferentes tecnologías de seguridad para cumplir con dichos requisitos. En particular, han elaborado la infraestructura de clave pública (PKI) y la informática confiable, y la posible adopción de redes inteligentes [21]. Como comparación, nos centramos en un problema particular, que es la encriptación de información en bases de datos de redes inteligentes.

Se han propuesto diversos enfoques de cifrado de datos dentro de la medición de energía como menciona F. García y B. Jacobs en [22] como el cifrado parcialmente Homomórfico respecto o a la suma o a la multiplicación. En los sistemas de red inteligente, aunque la potencia de los medidores generalmente no es una preocupación, el ancho de banda de comunicación puede ser aún insuficiente para el envío de cantidades grandes de información como se describe en [17], por lo que un encriptado que genere datos de mucha mayor extensión que el inicial no es eficiente, una posible solución a esta problemática se detalla en el trabajo de Milton Ruiz en [23]. En redes inteligentes, el uso de energía se considera privacidad del propietario y no debe revelarse a otros medidores [24]. Por lo tanto, la información se encriptaría de manera consecutiva a la medición con la posibilidad de aplicar el cifrado en la base de datos de la empresa distribuidora de energía. En este documento se emplea el cifrado homomórfico para el encriptado dentro de la red manteniendo los datos generados de forma segura para cada medidor.

# 3. Preliminares

Entre los cifrados más aptos podemos citar los que menciona K. Zotos en [25] según los problemas citados en [19], mismos que se caracterizan dentro de dos grupos, la criptografía simétrica y asimétrica. A continuación, se definirá e ilustrará el método de proceso de estos grupos.

## 3.1 Criptografía simétrica

La criptografía simétrica define que el proceso de cifrado y descifrado hace uso de una única clave. Este tipo de cifrado es vulnerable al tener que compartir esta clave entre el emisor y el receptor. A pesar de contar con una llave robusta, actualmente con el desarrollo tecnológico es totalmente viable obtener una llave privada en poco tiempo, según Sourabh Chandra [26].

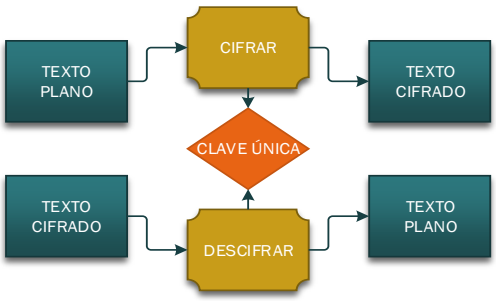


**Figura 1.** Ilustración del proceso general para algoritmos de criptografía simétrica (Fuente: autor)

### DES

El algoritmo DES (Data Encryption Standard) de cifrado, fue implementado en base a la necesidad de un método de protección en las comunicaciones empresariales, tiene la peculiaridad de cifrar por bloques, estos tienen longitud finita en bits que son sometidos a operaciones básicas dando como resultado otro bloque de la misma longitud de cifrado [27].

### AES

Este algoritmo, AES (Advanced Encryption Standard) también se lo conoce como Rijndael, puede realizar operaciones básicas a una matriz de 4x4

bits reordenándoles para encriptarlos, usando una llave única y un campo finito determinado en la mayoría de sus procesos de cálculo. [28].

**One-Time Pad**
Es un tipo de cifrado que permite un solo uso de una clave aleatoria de la misma longitud del texto en combinación durante el proceso de cifrado. Se ha demostrado que este tipo de cifrado mientras la clave sea totalmente aleatoria es irrompible [29].

**ECB**
El algoritmo ECB (Electronic Code Book) es un tipo de cifrado en bloque. Este sistema funciona cifrando partes de los datos con una clave común, es decir se dividen los datos y se cifran usando diferentes claves [30].

### 3.2 Criptografía asimétrica
Este tipo de criptografía usa dos claves una de uso público y otra de uso privado que es la que permite descifrar el texto. Así se consigue que solo el que posea la clave privada será capaz de leer la información [31]. Este tipo de clave asimétrica elimina el problema que tiene la criptografía simétrica al existir la posibilidad de fuga por dos lados. Aunque elimina este problema, este tipo de cifrado implica más tiempo de cómputo para cifrar y descifrar y además aumenta el tamaño del texto [26].

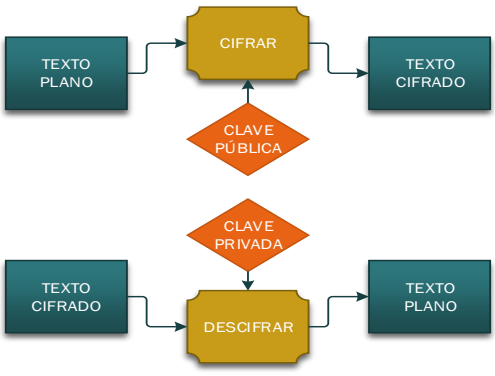


**Figura 2.** Proceso de criptografía asimétrica (Fuente: autor)

**RSA**
(Rivest, Shamir y Adleman), algoritmo asimétrico que funciona usando dos números primos obtenidos al azar. La ventaja de este tipo de algoritmo radica en la facilidad de factorizar números grandes y se considera un algoritmo seguro [27].

**Pailler**
Este método es un algoritmo asimétrico probabilístico, que se basa en un criptosistema homomórfico aditivo dado que a partir del cifrado de m1 y m2 es posible el cálculo de m1 + m2 como lo detalla Michael O'Keeffe The [32].

## 4. Cifrado homomórfico
A lo largo de la historia se han usado diferentes tipos de algoritmos para encriptar información, cada uno con sus diferencias particulares, pero todos con un propósito común de dar seguridad a la información. En este trabajo haremos énfasis en la criptografía usando el cifrado homomórfico [29].

### 4.1 Bases del cifrado homomórfico
La criptografía homomórfica mantiene el orden de los datos cifrados, debido a que si se ordena la base datos por un campo, el orden de los registros será el mismo tanto si dicho campo está cifrado o no, esto se comprueba con la investigación realizada por Klaus Kursawe en [33].
Un texto cifrado homomórficamente tiene la propiedad de poder hacer operaciones sobre este sin tener que descifrarlo.
Un ejemplo de cifrado es el cifrado Cesar, el cual es parcialmente homomórfico y consiste en cambiar cada letra por otra que se encuentre un número fijo delante de esta, y así lo mismo para todas, este cifrado es muy inseguro debido a que puede cifrar dos fragmentos en serie, se puede decir que es homomórfico respecto a la

concatenación. Por ejemplo, si cifráramos la palara Hello y World, por otras que se encuentren 13 letras adelante, la clave seria 13 podría descifrar el texto, y no importa que las palabras se unan formándose helloworld una vez cifradas, como este cifrado es homomórfico a la concatenación esta operación es permitida y no influye en el cifrado[25],[34].

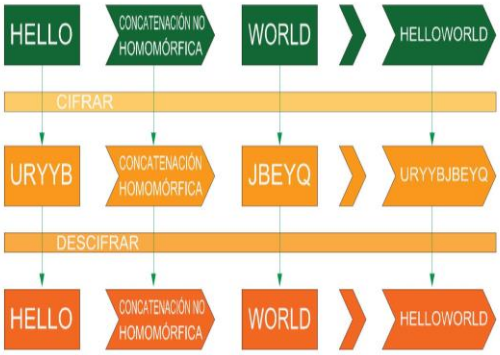


**Figura 3.** Ilustración de cifrado homomórfico (Fuente: autor)

Si bien el cifrado César es "inseguro", se puede llegar a comparar con otros tipos de cifrados, como es el RSA, el cual es caracterizado como "puro y sin relleno" debido a su aplicación directa de la multiplicación para cifrar y descifrar [26], [35].
Para el desarrollo de este trabajo se utilizará el modelo de encriptación RSA, basado en el uso de algoritmos asimétricos que permitan la multiplicación de datos sobre cifrado, esto conlleva a que también tendrá sus desventajas como son las claves de gran longitud como lo explica Sourabh Chandra y Sarika Y. Bonde en [26] y [36] respectivamente.
A continuación, se detallan las ecuaciones usadas como funciones criptográficas en el proceso de cifrado:

$$Enc(m) = m^e \equiv c \, mód \, n \quad (1)$$

$$Dec(c) = c^d \equiv m \, mód \, n \quad (2)$$

Donde, Enc y Dec son las funciones cifrar y descifrar, respectivamente.
Luego se tiene:

$$n = p * q \quad (3)$$

Donde p y q dos primos de tamaño considerable:

Los exponentes de cifrado y descifrado conciernen a e y d, de tal manera que:

$$e * d \equiv 1 \, mód \, (p - 1) * (q - 1) \quad (4)$$

Resultando dos textos cifrados c1 y c2, que se relacionan respectivamente con m1 y m2, se puede deducir que:

$$c1 * c2 \equiv {m_1}^e * {m_2}^e \equiv (m_1 * m_2)^e \; mód \; n \quad (5)$$

Esto hace admisible que se puedan multiplicar directamente los dos textos cifrados y esto no influya al descifrar el texto, obteniéndose el mismo valor esperado [22].
Una vez descubierto el homomorfismo multiplicativo, se preguntaron si existiría algún tipo de cifrado completamente homomórfico, que permitiera hacer cualquier tipo de operaciones en el texto. En el 2009 se determinó una respuesta teórica del primer esquema de cifrado homomórfico propuesto por el investigador de IBM Craig Gentry, pero este requería de un poder de computo que no era el de su época, y predijo que se necesitarían de cómo mínimo una década para poder hacer de este un algoritmo utilizable pero las consecuencias de este se piensan incalculables.
Aunque el cifrado completamente homomórfico sea difícil de crear, los cifrados parcialmente homomórficos

respecto a una operación o incluso a dos, sirven al propósito de cifrar un dato para permitir que por ejemplo la operación de concatenación sea permitida, para así poder juntar las partes de texto que se quiera y una vez descifradas poder leerlas [36].

## 4.2 Definición del cifrado homomórfico

El esquema de cifrado homomórfico cuenta con los siguientes elementos:

- Enc()
  Explicación: indica un esquema de encriptación probabilístico ($\oplus$, $\otimes$).
- Dec()
  Explicación: indica un esquema de descifrado.
- M
  Explicación: resultante de la operación y sus definiciones.
- C
  Explicación: resultante de la operación $\otimes$ y sus definiciones.

Donde:

$$c_1 = Enc_{k1}(m1) \quad (6)$$
$$c_2 = Enc_{k2}(m2) \quad (7)$$

Existe una clave k tal que:

$$c_1 \otimes c_2 = Enc_k(m1 \oplus m2) \quad (8)$$

En consecuencia, el descifrado de una operación $\otimes$ a los valores cifrados es el resultado de aplicar la función $\oplus$ a valores no cifrados [37] [32].

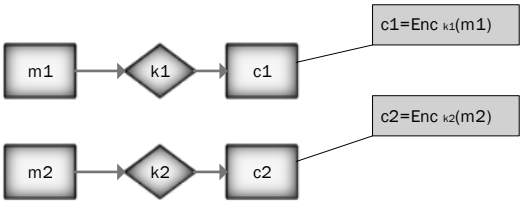


**Figura 4.** Cifrado de texto (Fuente: autor)

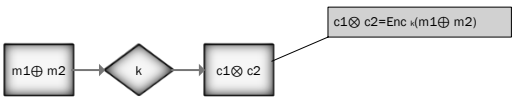


**Figura 5.** Cifrado Homomórfico (Fuente: autor)

## 4.3 Cifrado Homomórfico Aditivo

Este esquema de cifrado se describe a continuación:
La llave o clave está constituida de la manera que se observa en la ecuación (9).

$$k = (p, q) \quad (9)$$

Donde p y q son números primos elegidos por el usuario, bajo la característica que deben ser números privados, para mantener la seguridad del cifrado.
Luego se calcula:

$$n = p * q \quad (10)$$

Este valor calculado será conocido únicamente por el servidor.
La seguridad según describen los autores se basa en la dificultad del problema de factorización[21]. Bajo esta característica, el cifrado es realizado bajo la siguiente primitiva:

$$Enc_k(a) = (a \bmod p, a \bmod q) \quad (11)$$

Donde a $\in \mathbb{Z}_n$
Ahora, bien la primitiva de descifrado es:

$$Dec_k(d_1, d_2) = d_1 * q * q^{-1} + d_2 * p * p^{-1} \ (mód\ n) \quad (12)$$

Donde el inverso multiplicativo de q es tal que:

$$q * q^{-1} = 1 \ (mód\ p) \quad (13)$$

y el inverso multiplicativo de p es tal que

$$p * p^{-1} = 1 \ (mód\ q) \quad (14)$$

### 4.4 Ejemplo

Sea p = 5 y q = 7

$$n = p * q = 5 * 7 = 35 \quad (15)$$

La llave es k = (5,7). Si el usuario quiere sumar las siguientes cantidades: $a_1 = 5$ y $a_2 = 6$.

Entonces el cifrado de ambos números es:

$$E(a_1) = (0,5) \quad (16)$$
$$E(a_2) = (1,6) \quad (17)$$

Mismos que se acumulan en la base de datos. El servidor es capaz de realizar la suma sin tener que descifrar los datos, lo cual es equivalente a la aplicación de la ecuación siguiente:

$$E(a_1) + E(a_2) = (0 + 1, 5 + 6) = (1,11) \quad (18)$$

El resultado (1,11) es enviado al usuario, y éste puede descifrar utilizando la primitiva:

$$d_1 * q * q^{-1} + d_2 * p * p^{-1}(mód\ n) = (1 * 7 * 3 + 11 * 5 * 3(mód\ 35) = 11 \quad (19)$$

Donde 11 es la suma de 5 y 6 [21], [32],[34].

## 5. Desarrollo del programa

En esta sección, se describe el esquema del programa realizado para el cifrado homomórfico con sus variables de entrada, salida, funciones y su pseudocódigo.

Dados los textos cifrados bin_1, …, bin_t que cifra m_1, ..., m_t con nuestro esquema bajo alguna clave (llave), y dado una función f computable de manera eficiente, cualquiera puede calcular eficientemente un texto cifrado (o conjunto de textos cifrados) que encripta f(m_1, …, m_t) bajo esa llave. Esto permite cálculos generales en datos cifrados. Al no existir información sobre m_1, ..., m_t o sobre el valor de f(m_1,…,m_t) que se filtró, significa que el esquema de cifrado es consistente con la privacidad [32], [38].

Si se requiere que el esquema calcule alguna función f de los datos (encriptados) (m_1,…,m_t) se envía una descripción de f al esquema que usa la maleabilidad para calcular una encriptación de f(m_1,…,m_t) que se descifrará.

Un esquema de cifrado homomórfico tiene tres algoritmos: keygen, encrypt y decrypt, todos los cuales deben ser eficientes, es decir, se ejecutan en tiempo polinomial con parámetro λ, que puede abreviarse como: poli (λ), donde λ especifica la longitud de bits de las claves.

En un esquema de cifrado simétrico o de clave secreta, keygen utiliza λ para generar una única clave que se usa tanto en encrypt como en decrypt primero para asignar un mensaje a un texto cifrado, y luego para asignar el texto cifrado de nuevo al mensaje original [39].

En el camino hacia el cifrado completamente homomórfico se empieza construyendo un esquema que puede manejar una clase limitada de funciones permitidas, ya probadas para la adición y el producto [29].

Para una mejor comprensión de la encriptación y su implicación con cifrar y descifrar mediante la aplicación de una llave [26], [40], se puede ilustrar este proceso mediante el gráfico de la figura 6.

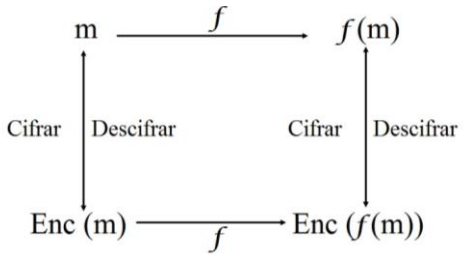


**Figura 6.** Idea general de la encriptación homomórfica (Fuente: autor)

Donde se observa que la llave o clave para cifrar o descifrar es “f”.
A continuación, se presenta a detalle el esquema del sistema de encriptación homomórfica que se aplicará en el desarrollo del programa.

## 5.1 Variables de entrada

Datos de entrada, números en el rango de los reales que deseamos cifrar:
m1, m2, … mn.

## 5.2 Variables de salida

bin1 y bin2 son los números correspondientes a las transformaciones binarias de m1 y m2.
bin1Encrypt, bin2Encrypt código encriptado de las variables bin1, bin2 respectivamente.
sumEncrypt, mulEnctypt suma y multiplicación encriptada de las variables bin1Encrypt, bin2Encrypt.
resSuma, resMult código descifrado (en binario) de las variables sumEncrypt, mulEnctypt respectivamente.
strSuma, strMult transforma a cadena las variables resSuma, resMult respectivamente.

## 5.3 Funciones

Función DivEnt: Retorna la parte entera de una división:
Entradas: num1, num2.
Proceso:
Entero= Parte entera de división de num1 para num2.
Salidas: Entero.

Función Mod:
Entradas: z, p.3
Proceso:
Residuo= Residuo de la división de “z” para “p”.
Salidas: Residuo

Función Llave: Retorna una llave con la cual se puede encriptar y desencriptar los números ingresados.
Entradas: Ninguna.
Proceso:
LAMBDA = 4.
N = LAMBDA.
P = LAMBDA elevado a 2.
Q = LAMBDA elevado a 3.
llave = entero largo aleatorio de “P” bits.
Mientras llave sea divisible entre 2, desde 0:
llave = entero largo aleatorio de “P” bits.
Fin Mientras.
Salidas: llave.

Función de encriptación: Retorna la encriptación de los números ingresados.
Entradas: llave, bin1.
Proceso:
q = entero largo, aleatorio, de “Q” bits.
binRandom = 2 * [entero largo aleatorio de (N - 1) bits].
bin1Encrypt = llave * q + binRandom + bin1.
Salidas: bin1Encrypt.

Función de desencriptación: Retorna la desencriptación de los números ingresados.
Entradas: llave, bin1Encrypt.
Proceso:
binResul = Mod(bin1Encrypt, llave) divisible entre 2.
Salida: binResul.

Función binaria: Convierte en números binarios los números enteros ingresados.
Entradas: binResul, binResul2.
Proceso:
Si, binResul mayor a 0:
Mientras binResul mayor que 0.
Si, binResul divisible entre 2, desde 0:
Añade “0” al final de listan binResul2 ="0" + binResul2.
Caso contrario:
Añade “0” al final de listaN.
binResul2 ="0"+ binResul2.
binResul = Maximo entero menor o igual a (binResul /2).

Fin Si.
Fin Mientras.
Caso contrario:
Si, binResul igual a 0:
Añade “0” al final de listaN
Caso contrario:
Error
Fin Si
Fin Si
Para, Reverso de listan desde i:
Añade “i” al final de listaRn.
Fin Para.
Salidas: listaRn.

Los datos al ser encriptados serán cargados desde un archivo plano que contiene bases de datos reales de la Empresa Eléctrica Quito S.A. con los cuales se trabajará, de igual manera para realizar la desencriptación, el código cifrado se cargará desde el archivo plano generado por el proceso de encriptación.

Función suma: Operación suma sobre los números cifrados
Entradas:bin1Encrypt, in2Encrypt.
Proceso:
sumEncrypt = Suma de bin1Encrypt + bin2Encrypt.
Salidas: sumEncrypt.

Función: Desencriptación de la operación suma.
Entradas: sumEncrypt.
Proceso:
resSuma = Desencriptación de sumEncrypt.
Salidas: resSuma.

Función multiplicación: Operación multiplicación sobre los números cifrados.
Entradas: bin1Encrypt,bin2Encrypt.
Proceso:
multEncrypt = Multiplicación de listas (bin1Encrypt, bin2Encrypt)
Salidas: multEncrypt.

Función: Desencriptación de la operación multiplicación.
Entradas: multEncrypt.
Proceso:
resMult = Desencriptación de multEncrypt
Salidas: resMult.

## 5.4 Funcionalidad del programa

Los datos cargados previamente desde un archivo plano se pasan como parámetros a las variables m1 y m2 y así mismo pasan a la función binario la cual realiza la transformación en binario de los números ingresados bin1 y bin2 respectivamente, para cada número binario se realiza una llave mediante la función llave que nos ayuda a encriptar los números, sumarlos o multiplicarlos, y luego proceder a descifrar la operación realizada [25], [41], [42].

Estos números binarios se encriptan mediante la función de encriptación, una vez que se tiene los números cifrados, se realiza la suma de los mismos mediante la función suma la cual nos devuelve la suma encriptada de los dos números cifrados, para poder verificar que los resultados sean correctos el programa llama a la función desencriptación, que retorna en números binarios el resultado de la suma encriptada, luego se realiza la conversión de estos números binarios a números enteros mediante la función binaria y así se obtiene el resultado de la suma de los números ingresados.

Para realizar la multiplicación de los números ingresados el programa llama a la función multiplicación y se pasa como parámetros los números cifrados (bin1Encrypt, bin2Encrypt) obtenidos anteriormente, luego se procede a realizar la desencriptación mediante la función desencriptación que retorna en números binarios el resultado de la multiplicación encriptada, luego se realiza la conversión de estos números binarios a números enteros mediante la función binaria y así se obtiene el resultado de la multiplicación de los números ingresados. Los datos de la

encriptación y desencriptación serán almacenados en un archivo plano respectivamente para su mejor manejo [43], [32].

## 6. Desempeño del programa

Se quiere que el programa completamente homomórfico sea eficiente, para ello es importante tomar en cuenta que la complejidad y extensión del encriptado dependerá del parámetro de seguridad λ, dependiendo a su vez de la función que se evalúe [25]. La medida que se usará para evaluar la eficiencia del programa estará en función del tiempo de ejecución, a continuación, en la Tabla 1 se detalla el tiempo de encriptado y desencriptado según el número de cifras del dato ingresado:

**Tabla 1.** Medición de tiempos de ejecución

| Nº | Número de cifras de ingreso | Tiempo de encriptación (segundos) | Tiempo de desencriptación (segundos) |
|---|---|---|---|
| 1 | 1 | 0.0040 | 0.0040 |
| 2 | 10 | 0.0120 | 0.0150 |
| 3 | 100 | 0.0270 | 0.0260 |
| 4 | 1000 | 0.0290 | 0.0350 |
| 5 | 10000 | 0.0470 | 0.0500 |
| 6 | 100000 | 0.0540 | 0.0600 |
| 7 | 1000000 | 0.0580 | 0.0720 |
| 8 | 10000000 | 0.0610 | 0.0850 |
| 9 | 100000000 | 0.0780 | 0.0990 |

Se puede evidenciar que los tiempos de ejecución son directamente proporcionales al número de cifras de los datos que se ingresan, por lo tanto, si se tiene un número de menos cifras para la entrada, el tiempo va a ser menor, pero si ingresamos un número muy grande, el tiempo de ejecución va a aumentar[43].

En relación con el tamaño de los archivos encriptados vs el tiempo de encriptación se ha realizado el siguiente esquema:

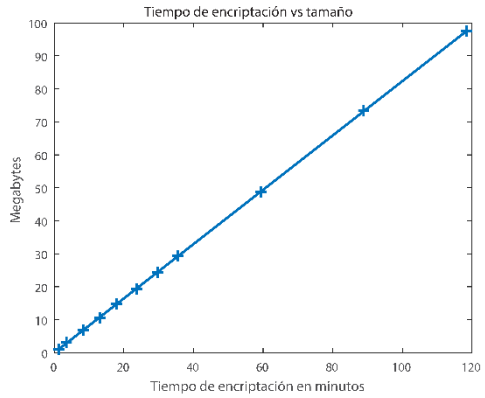


**Figura 7.** Tiempos de encriptación vs. tamaño de archivo (Fuente: autor)

Se puede apreciar en la figura 8 al igual que en la tabla de medición de tiempos en ejecución del programa, que el tiempo es lineal con respecto al tamaño del archivo encriptado obteniendo una media de 0.823 Megabytes por minuto, por lo que se puede prever de manera sencilla los tiempos de encriptación de archivos de mayor tamaño.

Estos resultados contrastan con lo obtenido por Sujoy Sinha Roy en [42] cuyos resultado fueron casi cuadráticos.

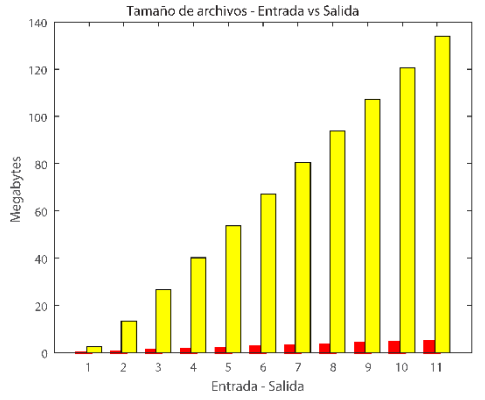


**Figura 8.** Comparación de archivos de entrada y salida (Fuente: autor)

Debido a la complejidad del código y la longitud de la llave aplicada en el programa, el tamaño de los archivos resultantes de la encriptación es aproximadamente un 2747% mayor al archivo inicial en todos los casos, como se detalla en la figura 9, dato que es acorde a lo que mencionó Sourabh

Chandra y Sarika Y. Bonde en [26] y [36] respectivamente.
Haciendo referencia al proceso de desencriptación se ha validado el tamaño del archivo encriptado en función del tiempo de desencriptación.

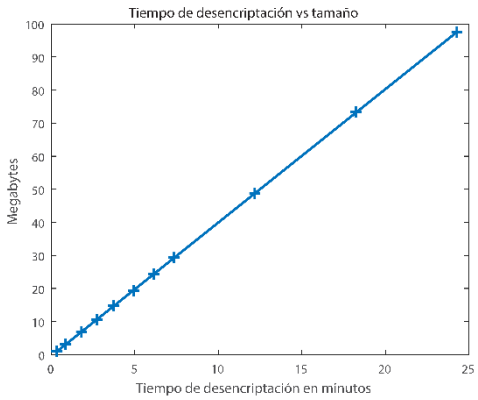


**Figura 9.** Tiempos de desencriptación vs. el tamaño del archivo (Fuente: autor)

Al igual que con los tiempos de encriptación, el proceso de desencriptación se mantiene lineal según el tamaño del archivo, con la particularidad de demorarse alrededor de un 20.49% del tiempo que toma encriptar el mismo tamaño de archivo, esto refleja la complejidad del proceso de encriptación dada la cantidad de procesos que requiere.

## 7. Resultados y discusión

Los datos utilizados en este documento provienen de mediciones reales de la Empresa Eléctrica Quito.
Dado el desempeño del programa es fácil ver que a diferencia del cifrado propuesto por Flavio D. Garcia en [22] y Michael O'Keeffe en [32] los datos de entrada no se restringen al grupo de los enteros sino que se puede trabajar con todos los números reales. Una ventaja con respecto a los cifrados propuesto por C. A. Melchor y Michael O'Keeffe en [44] y [32] es que el cifrado que se propone en este trabajo es totalmente homomórfico lo cual abre las puertas a muchas aplicaciones en el ámbito eléctrico.
La desventaja que presenta el modelo de encriptación detallado en este trabajo con respecto a los otros propuestos por Flavio D. Garcia en [22], Michael O'Keeffe en [32] y C. A. Melchor en [44] es que el tamaño del archivo resultante de la encriptación es mayor al del archivo inicial, por lo que se podría aplicar soluciones al tráfico de información como los protocolos de enrutamiento dinámico propuestos por Milton Ruiz en [23],

## 8. Conclusiones

Se puede concluir que el cifrado propuesto mejora la seguridad en los sistemas de medición inteligente de manera que se preserva la identidad e información confidencial de los usuarios en todo momento, ya que de presentarse la necesidad de operar los datos no es necesaria la desencriptación para su manipulación. Se podría decir que la opción adecuada para mejorar la seguridad en sistemas de medición inteligente es el cifrado propuesto, se considera conveniente abarcar un enfoque más general aplicándolo a nivel nacional, aplicando su uso a un modelo de emisor – receptor, los medidores inteligentes como emisores y la empresa distribuidora como receptora.
Se constató que el cifrado homomórfico posee una estructura sólida y robusta. Sólida puesto que mantiene los datos encriptados de manera confiable y robusto ya que trabaja con archivos planos que son la base de otros tipos de archivos (en este caso se trabajó con archivos .txt y .xlsx). Además, el cifrado homomórfico puede realizar operaciones sobre cifrado lo que produce un resultado muy complejo, difícil de desencriptar por otros métodos. Hay recalcar que el número de operaciones sobre cifrado es limitado dado que luego de cada operación va en aumento el tamaño del dato encriptado junto con mayores posibilidades de error al desencriptar por lo que es

recomendable no realizar más de dos repeticiones de una misma operación.

Se pudo determinar que el cifrado homomórfico plantea una rigidez más elevada a la hora de generar claves ya que si se quiere generar una llave muy pequeña (menor a tres cifras), esto provocaba resultados erróneos de cifrado y descifrado por lo que se recomienda utilizar una llave de cuatro dígitos puesto que un número mayor produciría un tamaño de archivo no manejable ni óptimo.

La información proveniente de los medidores inteligentes entra en los parámetros de eficiencia del cifrado homomórfico propuesto en este documento sin embargo cabe recalcar que no se considera apto para su utilización en Big Data dada la problemática que se presentaría al cifrar bases de datos del orden de los Terabytes, esto incurriría en gastos extra de almacenamiento que en algún momento serían insustentables.

En función del desempeño del programa se concluye que los tiempos de encriptación y desencriptación son lineales con respecto al tamaño del archivo, así como también permanece constante la relación del tamaño del archivo inicial y final, demostrando así su efectiva funcionalidad con la utilización de equipo de gama doméstica, por lo que se recomienda el uso de procesadores especializados para una mayor eficiencia.

# 9. Referencias


[1] M. Wagner, M. Kuba, and A. Oeder, "Smart Grid Cyber Security : A German Perspective," *2012 Int. Conf. Smart Grid Technol. Econ. Policies*, pp. 1–4.

[2] W. Wang, Y. Xu, and M. Khanna, "A survey on the communication architectures in smart grid," *Comput. Networks*, vol. 55, no. 15, pp. 3604–3629, 2011.

[3] W. Aslam, M. Soban, F. Akhtar, and N. A. Zaffar, "Smart meters for industrial energy conservation and efficiency optimization in Pakistan: Scope, technology and applications," *Renew. Sustain. Energy Rev.*, vol. 44, pp. 933–943, 2015.

[4] Q. Sun, H. Li, Z. Ma, C. Wang, J. Campillo, and Q. Zhang, "A Comprehensive Review of Smart Energy Meters in Intelligent Energy Networks," *IEEE Internet Things J.*, vol. 3, no. 4, pp. 464–479, 2016.

[5] W. Zhu, Q. Guo, and A. Overall, "Data Security and Encryption Technology Research on Smart Grid Communication System," *2016 Eighth Int. Conf. Meas. Technol. Mechatronics Autom.*, pp. 175–178, 2016.

[6] R. Jiang, R. Lu, and K. K. R. Choo, "Achieving high performance and privacy-preserving query over encrypted multidimensional big metering data," *Futur. Gener. Comput. Syst.*, 2016.

[7] B.-A. Schuelke-Leech, B. Barry, M. Muratori, and B. J. Yurkovich, "Big Data issues and opportunities for electric utilities," *Renew. Sustain. Energy Rev.*, vol. 52, pp. 937–947, 2015.

[8] F. Borges, S. Member, and M. Mühlhäuser, "EPPP4SMS : Efficient Privacy-Preserving Protocol for Smart Metering Systems and Its Simulation Using Real-World Data," vol. 5, no. 6, pp. 2701–2708, 2014.

[9] K. Moslehi and R. Kumar, "Smart Grid - a reliability perspective," in *2010 Innovative Smart Grid Technologies (ISGT)*, 2010, pp. 1–8.

[10] A. Bose, "Smart Transmission Grid Applications and Their

Supporting Infrastructure," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 11–19, Jun. 2010.

[11] R. E. Schuler, "Electricity Markets, Reliability and the Environment: Smartening-Up the Grid," in *2010 43rd Hawaii International Conference on System Sciences*, 2010, pp. 1–7.

[12] Xu Wei, Zhou Yu-hui, and Zhu Jie-lin, "Energy-efficient distribution in smart grid," in *2009 International Conference on Sustainable Power Generation and Supply*, 2009, pp. 1–6.

[13] B. Saint, "Rural distribution system planning using Smart Grid Technologies," in *2009 IEEE Rural Electric Power Conference*, 2009, pp. B3-B3-8.

[14] B. D. Russell and C. L. Benner, "Intelligent Systems for Improved Reliability and Failure Diagnosis in Distribution Systems," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 48–56, Jun. 2010.

[15] E. Inga Ortega, D. Arias Cazco, V. Orejuela Luna, and J. Inga Ortega, "Comunicaciones celulares para medición inteligente de energía eléctrica en sistemas de distribución," *Ingenius*, 2013.

[16] A. C. Rubio Juan E. and J. Lopez, "Recommender system for privacy-preserving solutions in smart metering," *Pervasive Mob. Comput.*, vol. In Press, 2017.

[17] M. Ruiz, P. Masache, and E. Inga, "Optimal Communications for Smart Measurement of Electric Energy Reusing Cellular Networks," *2018 Int. Conf. Inf. Syst. Comput. Sci.*, pp. 198–204, 2018.

[18] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Secur. Priv.*, 2010.

[19] P. McDaniel and S. McLaughlin, "Security and Privacy Challenges in the Smart Grid," *IEEE Secur. Priv. Mag.*, vol. 7, no. 3, pp. 75–77, May 2009.

[20] A. R. Metke and R. L. Ekl, "Security Technology for Smart Grid Networks," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 99–107, Jun. 2010.

[21] H. Liao, P. Lee, Y. Chao, and C. Chen, "A Location-Dependent Data Encryption Approach for Enhancing Mobile Information System Security," pp. 625–628, 2007.

[22] F. D. Garcia and B. Jacobs, "Privacy-friendly Engery-metering via Homomorphic Encryption," *STM 2010 Secur. Trust Manag.*, pp. 226–238, 2010.

[23] M. Ruiz, P. Masache, and J. Dominguez, "High Availability Network for Critical Communications on Smart Grids," no. Ssn, pp. 1–5, 2018.

[24] C. Efthymiou and G. Kalogridis, "Smart Grid Privacy via Anonymization of Smart Metering Data," *2010 First IEEE Int. Conf. Smart Grid Commun.*, no. September, pp. 238–243, 2010.

[25] K. Zotos and A. Litke, "Cryptography and Encryption," p. 5, 2005.

[26] S. Chandra, "A comparative survey of symmetric and asymmetric key cryptography," *2014 Int. Conf. Electron. Commun. Comput. Eng.*, pp. 83–93, 2014.

[27] A. Cabrera Aldaya, A. José, and C. Sarmiento, "Diseño e integración de algoritmos criptográficos en sistemas empotrados sobre FPGA," *RIELAC*, vol. 3, pp. 41–51, 2013.

[28] Y. Yuan, Y. Yang, L. Wu, and X. Zhang, “A High Performance Encryption System Based on AES Algorithm with Novel Hardware Implementation,” *2018 IEEE Int. Conf. Electron Devices Solid State Circuits*, pp. 1–2.

[29] C. Gentry, “A FULLY HOMOMORPHIC ENCRYPTION SCHEME,” 2009.

[30] I. F. Elashry, O. S. F. Allah, and A. M. Abbas, “A New Diffusion Mechanism for Data Encryption in The ECB Mode,” *2009 Int. Conf. Comput. Eng. Syst.*, pp. 288–293, 2009.

[31] J. Chaudhry, U. A. Qidwai, R. G. Rittenhouse, and M. Lee, “Vulnerabilities and Verification of Cryptographic Protocols and Their Future in Wireless Body Area Networks,” *2012 Int. Conf. Emerg. Technol.*, pp. 1–5, 2012.

[32] M. O’keeffe, “The Paillier Cryptosystem A Look Into The Cryptosystem And Its Potential Application,” 2008.

[33] K. Kursawe, G. Danezis, and M. Kohlweiss, “Privacy-friendly Aggregation for the Smart-grid.”

[34] O. O. Obi, F. H. Ali, and E. Stipidis, “Explicit expression for decryption in a generalisation of the Paillier scheme,” pp. 1–4.

[35] L. C. Han and N. M. Mahyuddin, “An Implementation of Caesar Cipher and XOR Encryption Technique in a Secure Wireless Communication,” *2014 2nd Int. Conf. Electron. Des.*, pp. 111–116.

[36] S. Y. Bonde, “Analysis of Encryption Algorithms ( RSA , SRNN and 2 key pair ) for Information Security,” *2017 Int. Conf. Comput. Commun. Control Autom.*, pp. 1–5, 2017.

[37] J. H. Cheon and J. Kim, “A Hybrid Scheme of Public-Key Encryption and Somewhat Homomorphic Encryption,” *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 5, pp. 1052–1063, 2015.

[38] C. Cheng and T. Jiang, “A Novel Homomorphic MAC Scheme for Authentication in Network Coding,” *IEEE Commun. Lett.*, vol. 15, no. 11, pp. 1228–1230, 2011.

[39] Y. Ma, L. Wu, X. Gu, J. He, and Z. Yang, “A Secure Face-Verification Scheme Based on Homomorphic Encryption and Deep Neural Networks,” vol. 5, no. 1, 2017.

[40] J. L. Raisaro *et al.*, “Protecting Privacy and Security of Genomic Data in i2b2 with Homomorphic Encryption and Differential Privacy,” *IEEE/ACM Trans. Comput. Biol. Bioinforma.*, vol. 15, no. 5, pp. 1413–1426, 2018.

[41] B. Wang, Y. Zhan, and Z. Zhang, “Cryptanalysis of a Symmetric Fully Homomorphic Encryption Scheme,” *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 6, pp. 1460–1467, 2018.

[42] S. S. Roy, F. Vercauteren, J. Vliegen, and I. Verbauwhede, “Hardware Assisted Fully Homomorphic Function Evaluation and Encrypted Search,” vol. 66, no. 9, pp. 1562–1572, 2017.

[43] W. Wang, Y. Hu, L. Chen, X. Huang, S. Member, and B. Sunar, “Exploring the Feasibility of Fully Homomorphic Encryption,” *IEEE Trans. Comput.*, vol. 64, no. 3, pp. 698–706, 2015.

[44] C. A. Melchor, P. Gaborit, and J. Herranz, “Additively Homomorphic Encryption with t-Operand Multiplications Additively Homomorphic

Encryption with d -Operand Multiplications," no. January, 2008.

# 10. Estado del arte

**Tabla 2.** Matriz del estado del arte

| | DATOS | | | TEMÁTICA | | | | | | FORMULACIÓN DEL PROBLEMA FUNCIONES OBJETIVO | | | | | RESTRICCIONES DEL PROBLEMA | | | | | PROPUESTAS PARA RESOLVER EL PROBLEMA | | | | | SOLUCIÓN PROPUESTA | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ITEM | AÑO | TÍTULO DEL ARTÍCULO | CITAS | BIG DATA EN SYSTEMAS ELECTRICOS | ENCRIPTACIÓN DE DATOS | PROTOCOLOS DE PRIVACIDAD Y PRESERVACIÓN DE DATOS | DATA AGGREGATION | MEDICION INTELIGENTE | SEGURIDAD DE DATOS EN EL SISTEMA ELÉCTRICO | MEDICIÓN DE GRAN CANTIDAD DE DATOS | IMPLEMENTACIÓN DE MÉTODOS DE ENCRIPTACIÓN | MINIMIZACIÓN DE RIESGOS DE DATOS | MINIMIZACIÓN DE COSTOS | MAXIMIZACIÓN DE PRIVACIDAD | COSTO | INFRAESTRUCTURA | TAMAÑO DE DATOS ENCRIPTADOS | TIEMPOS DE CIFRADO DE DATOS | LIMITACIONE DE EQUIPOS | SISTEMA DE ENCRIPTACIÓN | UTILIZACION DE ALGORITMOS DE CIFRADO | REDUCCION DE TIEMPOS DE CIGRADO | MEJORAR TRÁFICO DE INFORMACIÓN | IMPLEMENTACIÓN DE AMI PARA MEDICION DE DATOS | ENCRIPTACIÓN HOMOMÓRFICA | ALGORITMOS CONVENCIONALES DE CIFRADO | PROTOCOLOS PARA TRÁFICO DE INFORMACIÓN | INCORPORACIÓN DE CIFRADOS A AMI BASADA EN IEEE 802 | REDUCCIÓN DE DATOS DENTRO DEL ANCHO DE BANDA |
| 1 | 2012 | Smart Grid Cyber Security: A German Perspective | 8 | | | ☒ | | ☒ | | | | ☒ | | | ☒ | ☒ | | | | | | | | | | ☒ | | | |
| 2 | 2011 | A survey on the communication architectures in smart grid | 638 | ☒ | ☒ | | | | ☒ | ☒ | ☒ | ☒ | | ☒ | | | ☒ | | | | ☒ | | ☒ | | | ☒ | | ☒ | |
| 3 | 2015 | Smart meters for industrial energy conservation and efficiency optimization in Pakistan | 20 | ☒ | ☒ | ☒ | | ☒ | | ☒ | | ☒ | ☒ | ☒ | | | ☒ | ☒ | | ☒ | ☒ | | | | ☒ | ☒ | | ☒ | |
| 4 | 2016 | A Comprehensive Review of Smart Energy Meters in Intelligent Energy Networks | 67 | ☒ | ☒ | | | ☒ | | ☒ | | ☒ | ☒ | ☒ | ☒ | ☒ | ☒ | ☒ | ☒ | | ☒ | | | | ☒ | ☒ | | ☒ | ☒ |
| 5 | 2016 | Data Security and Encryption Technology Research on Smart Grid Communication System | 4 | ☒ | ☒ | ☒ | | | ☒ | | ☒ | ☒ | ☒ | | | ☒ | ☒ | ☒ | ☒ | ☒ | | ☒ | | ☒ | | | | | |
| 6 | 2018 | Achieving high performance and privacy-preserving query over encrypted multidimensional big metering data | 24 | ☒ | ☒ | | ☒ | | ☒ | ☒ | | | | | | | | | | | | | | ☒ | | | ☒ | | |
| 7 | 2015 | Big Data issues and opportunities for electric utilities | 23 | ☒ | | | | ☒ | | | | ☒ | ☒ | | ☒ | | | | | ☒ | | | | ☒ | | ☒ | | ☒ | |
| 8 | 2014 | EPPP4SMS: Efficient Privacy-Preserving Protocol for Smart Metering Systems and Its Simulation Using Real-World Data | 35 | ☒ | ☒ | | ☒ | | | ☒ | ☒ | ☒ | | | | | ☒ | ☒ | | | | ☒ | ☒ | | | ☒ | | | |
| 9 | 2010 | Smart Grid - a reliability perspective | 425 | | | | | ☒ | | ☒ | | | ☒ | | | | | | | | | | ☒ | | | ☒ | | | |
| 10 | 2010 | Smart Transmission Grid Applications and Their Supporting Infrastructure | 429 | | | | | ☒ | | ☒ | | | | | ☒ | ☒ | | | | ☒ | | | | | | | ☒ | | |
| 11 | 2010 | Electricity Markets, Reliability and the Environment: Smartening-Up the Grid | 10 | ☒ | | | ☒ | ☒ | | ☒ | | ☒ | | | ☒ | | | | | ☒ | | | | | | | | ☒ | |
| 12 | 2009 | Energy-efficient distribution in smart grid | 39 | ☒ | | | ☒ | ☒ | | | ☒ | | ☒ | ☒ | | ☒ | | ☒ | | | | | | ☒ | ☒ | ☒ | | | ☒ |

| | DATOS | | | TEMÁTICA | | | | | | FORMULACIÓN DEL PROBLEMA FUNCIONES OBJETIVO | | | | | RESTRICCIONES DEL PROBLEMA | | | | | PROPUESTAS PARA RESOLVER EL PROBLEMA | | | | | SOLUCIÓN PROPUESTA | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ITEM | AÑO | TÍTULO DEL ARTÍCULO | CITAS | BIG DATA EN SYSTEMAS ELECTRICOS | ENCRIPTACIÓN DE DATOS | PROTOCOLOS DE PRIVACIDAD Y PRESERVACIÓN DE DATOS | DATA AGGREGATION | MEDICION INTELIGENTE | SEGURIDAD DE DATOS EN EL SISTEMA ELÉCTRICO | MEDICIÓN DE GRAN CANTIDAD DE DATOS | IMPLEMENTACIÓN DE MÉTODOS DE ENCRIPTACIÓN | MINIMIZACIÓN DE RIESGOS DE DATOS | MINIMIZACIÓN DE COSTOS | MAXIMIZACIÓN DE PRIVACIDAD | COSTO | INFRAESTRUCTURA | TAMAÑO DE DATOS ENCRIPTADOS | TIEMPOS DE CIFRADO DE DATOS | LIMITACIONE DE EQUIPOS | SISTEMA DE ENCRIPTACIÓN | UTILIZACION DE ALGORITMOS DE CIFRADO | REDUCCION DE TIEMPOS DE CIGRADO | MEJORAR TRÁFICO DE INFORMACIÓN | IMPLEMENTACIÓN DE AMI PARA MEDICION DE DATOS | ENCRIPTACIÓN HOMOMÓRFICA | ALGORITMOS CONVENCIONALES DE CIFRADO | PROTOCOLOS PARA TRÁFICO DE INFORMACIÓN | INCORPORACIÓN DE CIFRADOS A AMI BASADA EN IEEE 802 | REDUCCIÓN DE DATOS DENTRO DEL ANCHO DE BANDA |
| 13 | 2009 | Rural distribution system planning using Smart Grid Technologies | 59 | ☒ | ☒ | | | ☒ | ☒ | | | ☒ | ☒ | | | ☒ | | | ☒ | | | | | ☒ | | | | ☒ | |
| 14 | 2010 | Intelligent Systems for Improved Reliability and Failure Diagnosis in Distribution Systems | 102 | ☒ | | ☒ | ☒ | | | | | | ☒ | | ☒ | | | | ☒ | | | | | ☒ | | | | ☒ | |
| 15 | 2013 | Comunicaciones celulares para medición inteligente de energía eléctrica en sistemas de distribución | 10 | ☒ | | ☒ | ☒ | ☒ | ☒ | ☒ | | | ☒ | | | ☒ | | | ☒ | | | | | ☒ | ☒ | | | ☒ | |
| 16 | 2017 | Recommender system for privacy-preserving solutions in smart metering | 8 | ☒ | ☒ | ☒ | | | ☒ | | ☒ | ☒ | | ☒ | | ☒ | ☒ | | ☒ | ☒ | ☒ | | | | ☒ | ☒ | ☒ | | |
| 17 | 2018 | Optimal Communications for Smart Measurement of Electric Energy Reusing Cellular Networks | 0 | | | ☒ | ☒ | ☒ | ☒ | ☒ | | | ☒ | | | ☒ | ☒ | | ☒ | | | | ☒ | ☒ | | | ☒ | |
| 18 | 2010 | Smart-grid security issues | 526 | | ☒ | ☒ | | | ☒ | | ☒ | ☒ | | ☒ | ☒ | ☒ | | | | | ☒ | ☒ | | ☒ | | ☒ | | | |
| 19 | 2009 | Security and Privacy Challenges in the Smart Grid | 968 | ☒ | | ☒ | | ☒ | ☒ | ☒ | | | ☒ | | ☒ | | | | | | ☒ | | | | | | ☒ | | |
| 20 | 2010 | Security Technology for Smart Grid Networks | 550 | | | ☒ | ☒ | ☒ | | ☒ | | | ☒ | | ☒ | | | | | ☒ | | | | | ☒ | | | ☒ | |
| 21 | 2007 | A Location-Dependent Data Encryption Approach for Enhancing Mobile Information System Security | 23 | ☒ | ☒ | ☒ | | | | | ☒ | ☒ | | ☒ | | ☒ | | ☒ | | ☒ | ☒ | ☒ | | | | ☒ | | | |
| 22 | 2010 | Privacy-friendly Engery-metering via Homomorphic Encryption | 329 | | ☒ | ☒ | | ☒ | ☒ | | ☒ | ☒ | | ☒ | ☒ | | ☒ | ☒ | ☒ | | | ☒ | | | | ☒ | ☒ | | | |
| 23 | 2018 | High Availability Network for Critical Communications on Smart Grids | 3 | ☒ | | | ☒ | | ☒ | | | | ☒ | | | ☒ | | | ☒ | | | | | ☒ | | | | ☒ | |
| 24 | 2010 | Smart Grid Privacy via Anonymization of Smart Metering Data | 568 | | ☒ | ☒ | | ☒ | ☒ | ☒ | ☒ | | | ☒ | | | ☒ | ☒ | | ☒ | ☒ | | | ☒ | ☒ | | | | |
| 25 | 2005 | Cryptography and Encryption | 5 | | ☒ | ☒ | | | | | ☒ | ☒ | | | | | | | | ☒ | ☒ | | | | ☒ | | | | |
| 26 | 2014 | A comparative survey of symmetric and asymmetric key cryptography | 36 | | ☒ | ☒ | | | | | ☒ | ☒ | | | | | ☒ | ☒ | | ☒ | ☒ | ☒ | | | ☒ | | | | |
| 27 | 2013 | Diseño e integración de algoritmos criptográficos en sistemas empotrados sobre FPGA | 2 | ☒ | ☒ | ☒ | | | | | ☒ | | | | | | | ☒ | | | ☒ | | | | ☒ | | | | |

| | DATOS | | | TEMÁTICA | | | | | | FORMULACIÓN DEL PROBLEMA FUNCIONES OBJETIVO | | | | | RESTRICCIONES DEL PROBLEMA | | | | | PROPUESTAS PARA RESOLVER EL PROBLEMA | | | | | SOLUCIÓN PROPUESTA | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ITEM | AÑO | TÍTULO DEL ARTÍCULO | CITAS | BIG DATA EN SYSTEMAS ELECTRICOS | ENCRIPTACIÓN DE DATOS | PROTOCOLOS DE PRIVACIDAD Y PRESERVACIÓN DE DATOS | DATA AGGREGATION | MEDICION INTELIGENTE | SEGURIDAD DE DATOS EN EL SISTEMA ELÉCTRICO | MEDICIÓN DE GRAN CANTIDAD DE DATOS | IMPLEMENTACIÓN DE MÉTODOS DE ENCRIPTACIÓN | MINIMIZACIÓN DE RIESGOS DE DATOS | MINIMIZACIÓN DE COSTOS | MAXIMIZACIÓN DE PRIVACIDAD | COSTO | INFRAESTRUCTURA | TAMAÑO DE DATOS ENCRIPTADOS | TIEMPOS DE CIFRADO DE DATOS | LIMITACIONE DE EQUIPOS | SISTEMA DE ENCRIPTACIÓN | UTILIZACION DE ALGORITMOS DE CIFRADO | REDUCCION DE TIEMPOS DE CIGRADO | MEJORAR TRÁFICO DE INFORMACIÓN | IMPLEMENTACIÓN DE AMI PARA MEDICION DE DATOS | ENCRIPTACIÓN HOMOMÓRFICA | ALGORITMOS CONVENCIONALES DE CIFRADO | PROTOCOLOS PARA TRÁFICO DE INFORMACIÓN | INCORPORACIÓN DE CIFRADOS A AMI BASADA EN IEEE 802 | REDUCCIÓN DE DATOS DENTRO DEL ANCHO DE BANDA |
| 28 | 2018 | A High Performance Encryption System Based on AES Algorithm with Novel Hardware Implementation | 0 | | | ☒ | | | | | ☒ | ☒ | | ☒ | ☒ | ☒ | | | | ☒ | | | | | | | ☒ | | | |
| 29 | 2009 | A FULLY HOMOMORPHIC ENCRYPTION SCHEME | 1857 | | ☒ | ☒ | | | | | ☒ | | | | | | | ☒ | | | ☒ | | | | | ☒ | | | |
| 30 | 2009 | A New Diffusion Mechanism for Data Encryption in The ECB Mode | 5 | ☒ | ☒ | | | | | | ☒ | | | | | | | ☒ | | | ☒ | | | | | | ☒ | | |
| 31 | 2012 | Vulnerabilities and Verification of Cryptographic Protocols and Their Future in Wireless Body Area Networks | 7 | ☒ | ☒ | ☒ | | | | | ☒ | ☒ | | ☒ | ☒ | | | | ☒ | ☒ | | | | | | ☒ | | | |
| 32 | 2008 | The Paillier Cryptosystem A Look Into The Cryptosystem And Its Potential Application | 7 | ☒ | ☒ | ☒ | | | | | ☒ | ☒ | | | | | ☒ | ☒ | | ☒ | | ☒ | | | ☒ | | | | |
| 33 | 2011 | Privacy-friendly Aggregation for the Smart-grid | 317 | ☒ | | | ☒ | | ☒ | | ☒ | ☒ | | ☒ | | ☒ | | | ☒ | | ☒ | | | | ☒ | | ☒ | | |
| 34 | 2007 | Explicit expression for decryption in a generalisation of the Paillier scheme | 2 | | ☒ | | | | | | ☒ | | | | | | ☒ | | | | ☒ | | | | ☒ | | | | |
| 35 | 2014 | An Implementation of Caesar Cipher and XOR Encryption Technique in a Secure Wireless Communication | 8 | ☒ | | ☒ | | | | | ☒ | | | | | | | ☒ | | | ☒ | | | | | ☒ | | | |
| 36 | 2017 | Analysis of Encryption Algorithms ( RSA , SRNN and 2 key pair ) for Information Security | 1 | | | ☒ | | | | | ☒ | | | | | | | | | | ☒ | ☒ | | | | ☒ | | | |
| 37 | 2015 | A Hybrid Scheme of Public-Key Encryption and Somewhat Homomorphic Encryption | 18 | | ☒ | | | | | | ☒ | | | | | | ☒ | ☒ | | ☒ | | | | | ☒ | | | | |
| 38 | 2011 | A Novel Homomorphic MAC Scheme for Authentication in Network Coding | 14 | ☒ | ☒ | ☒ | | | | | ☒ | ☒ | | ☒ | | | ☒ | | | ☒ | | ☒ | | | ☒ | | | ☒ | |
| 39 | 2017 | A Secure Face-Verification Scheme Based on Homomorphic Encryption and Deep Neural Networks | 3 | ☒ | | ☒ | | | | | ☒ | ☒ | | ☒ | | | ☒ | ☒ | ☒ | | ☒ | ☒ | | | ☒ | | | | |
| 40 | 2018 | Protecting Privacy and Security of Genomic Data in i2b2 with Homomorphic Encryption and Differential Privacy | 2 | ☒ | ☒ | | | | | | ☒ | | | | | | ☒ | ☒ | | | ☒ | ☒ | | | ☒ | | | | |

| | DATOS | | | TEMÁTICA | | | | | | FORMULACIÓN DEL PROBLEMA FUNCIONES OBJETIVO | | | | | RESTRICCIONES DEL PROBLEMA | | | | | PROPUESTAS PARA RESOLVER EL PROBLEMA | | | | | SOLUCIÓN PROPUESTA | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ITEM | AÑO | TÍTULO DEL ARTÍCULO | CITAS | BIG DATA EN SYSTEMAS ELECTRICOS | ENCRIPTACIÓN DE DATOS | PROTOCOLOS DE PRIVACIDAD Y PRESERVACIÓN DE DATOS | DATA AGGREGATION | MEDICION INTELIGENTE | SEGURIDAD DE DATOS EN EL SISTEMA ELÉCTRICO | MEDICIÓN DE GRAN CANTIDAD DE DATOS | IMPLEMENTACIÓN DE MÉTODOS DE ENCRIPTACIÓN | MINIMIZACIÓN DE RIESGOS DE DATOS | MINIMIZACIÓN DE COSTOS | MAXIMIZACIÓN DE PRIVACIDAD | COSTO | INFRAESTRUCTURA | TAMAÑO DE DATOS ENCRIPTADOS | TIEMPOS DE CIFRADO DE DATOS | LIMITACIONE DE EQUIPOS | SISTEMA DE ENCRIPTACIÓN | UTILIZACION DE ALGORITMOS DE CIFRADO | REDUCCION DE TIEMPOS DE CIGRADO | MEJORAR TRÁFICO DE INFORMACIÓN | IMPLEMENTACIÓN DE AMI PARA MEDICION DE DATOS | ENCRIPTACIÓN HOMOMÓRFICA | ALGORITMOS CONVENCIONALES DE CIFRADO | PROTOCOLOS PARA TRÁFICO DE INFORMACIÓN | INCORPORACIÓN DE CIFRADOS A AMI BASADA EN IEEE 802 | REDUCCIÓN DE DATOS DENTRO DEL ANCHO DE BANDA |
| 41 | 2018 | Cryptanalysis of a Symmetric Fully Homomorphic Encryption Scheme | 4 | | ☒ | | | | | | ☒ | | | | | ☒ | ☒ | ☒ | | | ☒ | | | | ☒ | | | | |
| 42 | 2017 | Hardware Assisted Fully Homomorphic Function Evaluation and Encrypted Search | 7 | | ☒ | | | | | | ☒ | | | | | | ☒ | ☒ | | ☒ | | ☒ | | | ☒ | | | | |
| 43 | 2015 | Exploring the Feasibility of Fully Homomorphic Encryption | 62 | | ☒ | ☒ | | | | | ☒ | ☒ | | | | | ☒ | | | ☒ | | | | | ☒ | | | | |
| 44 | 2010 | Additively Homomorphic Encryption with t-Operand Multiplications | 112 | | ☒ | | | | | | ☒ | | | | | | ☒ | ☒ | | | ☒ | | | | ☒ | | | | |
| | | | CANTIDAD: | 25 | 27 | 25 | 10 | 15 | 13 | 13 | 29 | 22 | 13 | 14 | 12 | 15 | 20 | 21 | 10 | 19 | 21 | 9 | 10 | 12 | 23 | 12 | 5 | 10 | 2 |

**Tabla 3.** Resumen e indicadores del estado del arte