Revista Cubana de Ciencias Informáticas
Vol. 16, No. 4, Mes Octubre-Diciembre, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 207-232

Tipo de artículo: Artículos de revisión
Temática: Tecnologías de la información y las telecomunicaciones
Recibido: 21/08/2022 | Aceptado: 01/09/2022 | Publicado: 24/10/2022

Estado del arte de los mecanismos de cambio de llaves en esquemas de cifrado en bloque

State of art of re-keying mechanisms in block cipher schemes

Daymé Almeida Echevarria 0000-0002-7573-4637*
Ramses Rodríguez Aulet 0000-0001-7653-324X
Ernesto Domínguez Fiallo 0000-0003-3831-2889

Instituto de Criptografía, Universidad de la Habana.

*Autor para correspondencia: (daymealmeidaechevarria@gmail.com)

RESUMEN

En Criptografía, la cantidad de datos permitidos a cifrar con una sola llave en un algoritmo o esquema de cifrado es conocida como tiempo de vida de la llave. Esta cantidad debe ser limitada, ya que la probabilidad de éxito durante la realización de ataques específicos aumenta con la obtención de un mayor número de datos cifrados, lo cual conlleva al cambio frecuente de las mismas. Para evitar estos cambios regulares de llaves han surgido nuevas variantes en el caso de esquemas simétricos de cifrado en bloque que extienden el tiempo de vida y que son conocidos en la literatura como mecanismos de cambio de llave externos, internos y frescos, dependiendo de donde usados, ya que trabajan a nivel de protocolos, modos de operación o en el propio algoritmo de cifrado. En este trabajo se realizó una revisión bibliográfica sobre el estado del arte de cada una de las variantes teniendo en cuenta el funcionamiento general de cada uno de ellos, sus características principales, los diseños más recientes, la seguridad que aportan al cifrado y su aporte al tiempo de vida de las llaves. Los resultados de la revisión muestran las ventajas de uso de cada uno de estos mecanismos.

Palabras clave: Mecanismos de cambio de llave; algoritmos de cifrado en bloque; cambios de llave internos; cambios de llave externos; cambios de llave frescos.

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 4, Mes Octubre-Diciembre, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 207-232

ABSTRACT

In Cryptography, the amount of data allowed to be encrypted with a single key in an algorithm or encryption scheme is known as the lifetime of the key. This amount must be limited, since the probability of success during the execution of specific attacks increases with the obtaining of a greater number of encrypted data, which leads to their frequent change. To avoid these regular key changes, new variants have emerged in the case of symmetric block cipher schemes that extend the lifetime and are known in the literature as external key change mechanisms, internal and fresh key change mechanisms, depending on where they are used, since they work at the level of protocols, modes of operation or in the encryption algorithm itself. In this work, a bibliographic review was carried out on the state of the art of each of the variants, taking into account the general operation of each one of them, their main characteristics, the most recent designs, the security they provide to encryption and their contribution to encryption key lifetime. The results of the review show the advantages of using each of these mechanisms.

Keywords: Rekeying mechanisms; Block cipher algorithms; internal re-keying; external re-keying; fresh re-keying.

Introducción

El uso de redes informáticas, el internet de las cosas y la nube se hace cada vez más extenso y necesario para la vida de las personas, sin embargo, esto trae consigo la exposición de datos personales de los ciudadanos a veces sin la protección adecuada, por ello, la Criptografía, como ciencia dedicada a la protección de la información, ha ganado un mayor espacio en los momentos actuales.

La búsqueda y diseño de protocolos y algoritmos ajustados a cada entorno con las mismas garantías de eficiencia y más seguridad, es una prioridad para los investigadores de la especialidad, sin embargo, esta garantía en el caso de los algoritmos criptográficos radica en el secreto de la llave. En la actualidad el uso creciente de ataques dirigidos a vulnerar la seguridad de estos algoritmos o esquemas de protección criptográficos deviene, en que los usuarios de las redes deban guardar o memorizar un gran número de llaves que deben ser cambiadas regularmente, de ahí que la búsqueda de mecanismos que extiendan el tiempo de vida de las mismas sea una de las lineas de investigación más importantes.

En Criptografía la información a cifrar es conocida como texto claro o mensaje y para el cifrado de estos son usados algoritmos asimétricos o simétricos en dependencia del uso de la llave. Durante el cifrado de un mensaje con un algoritmo simétrico de cifrado en bloque se recorren los valores de la permutación determinada de forma unívoca por la llave secreta, luego, si la cantidad de bloques determinada por la longitud del mensaje sobrepasa su tiempo de vida, su seguridad se ve afectada seriamente, obligándonos a realizar un cambio de llave para evitar comprometimientos, ya que, a partir de la obtención de una mayor cantidad de información cifrada con una llave, aumentan las probabilidades de éxito de disímiles ataques a los sistemas.

Dada la importancia que reviste la protección de las llaves de cifrado, así como, aumentar la vida útil de la mismas, este trabajo fue realizado con el objetivo de encontrar en la literatura, diferentes mecanismos usados para incrementar su tiempo de vida, brindar una descripción detallada de estos, su funcionamiento general, características principales, diseños más recientes, así como, la seguridad que aportan al cifrado.

Las técnicas más usadas encontradas en la literatura pública son conocidas como Mecanismos de cambios de llave o de re-keying, internos, externos y frescos (Medwed et al., 2010; Abdalla and Bellare, 2000; Akhmetzyanova et al., 2017). Los mecanismos internos de cambio de llave son utilizados para cifrar grandes cantidades de información mediante un modo de operación determinado, con la peculiaridad de que, cada cierta cantidad de bloques procesados, una nueva llave es utilizada para procesar los siguientes bloques del mensaje. Este nuevo enfoque, estudiado y popularizado en los últimos años, garantiza la seguridad del cifrado cuando el mensaje es muy largo, cambiando la llave de forma periódica.

Los mecanismos externos son utilizados a nivel de protocolos, con la peculiaridad, de que el cambio de llave se realiza una vez cifrados una cierta cantidad de mensajes, cuya longitud no sobrepasa su tiempo de vida, por lo que es una variante muy útil durante el cifrado de varios mensajes de corta longitud.

En el caso particular de los mecanismos frescos, estos surgen como una variante para evitar ataques de canal colateral en dispositivos de peso ligero, realizando el cifrado de cada mensaje con una llave diferente cada vez, por lo que afecta la estructura del cifrado de bloque usado, al generarse una permutación diferente para cada llave.

Estos mecanismos de extensión del tiempo de vida de la llaves han surgido también como alternativa para optimizar la seguridad en otros entornos como son: diseño de modos de autenticado (Khairallah, 2019; Dini and Savino, 2011), internet de las cosas (Mugal et al., 2019), redes inalámbricas de baja potencia (Dini and Savino, 2011) e inclusive, en el diseño e implementación de sistemas de almacenamiento (Qin et al., 2017).

Este trabajo estará dividido en tres sesiones, donde se explicará el funcionamiento de cada mecanismo de re-keying. Primero, comenzamos con la descripción de los mecanismos de cambio de llave frescos y el entorno donde son aplicados, para que el lector pueda comprender porque su funcionamiento general es aplicable a

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 4, Mes Octubre-Diciembre, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 207-232

tales dispositivos, por ende, se define el término: dispositivo de peso ligero. Se realiza también un análisis del estado del arte de las últimas propuestas de este mecanismo y la tendencia actual.
El segundo apartado se dedica a los mecanismos de re-keying externos y de igual manera se explica a modo general lo que se define y entiende en la literatura como protocolos criptográficos, entorno donde es aplicada esta variante, su funcionamiento general y los diseños expuestos por los investigadores de esta área. La tercera sesión está dedicada a los mecanismos internos, el estado del arte de los mismos y su aplicación en modos de operación de algoritmos de cifrado en bloque. Igualmente se explica el funcionamiento general y su ganancia de seguridad en relación al tiempo de vida de las llaves. Para finalizar, se realiza un análisis comparativo de las tres variantes en la sesión Resultados y discusión .

Mecanismos frescos

El diseño de algoritmos aplicables a dispositivos de peso ligero es una de las lineas de investigación más atractiva en la actualidad, por el amplio uso de los mismos en la vida diaria, lo que ha llevado al estudio de su protección y en particular al uso de la criptografía de peso ligero como medida para aumentar su seguridad y protección, en particular, contra ataques de canal colateral. Estos dispositivos se caracterizan por tener limitadas propiedades como: conectividad, memoria, CPU, latencia, suministro de energía y otras. Entre los más comunes se pueden encontrar etiquetas RFID (Dispositivos de Identificación de radio frecuencias), redes de sensores inalámbricos, controladores industriales y dispositivos embebidos. En otras palabras, se trata de dispositivos sencillos, baratos y poco glamurosos. Sus características esenciales es que utilizan micro controladores de 4, 8 o 16 bits, sus memorias RAM rondan sobre los 64 bytes e incluso tan solo 16 bytes. Sus conjuntos de instrucciones son muy reducidos y algunos como las etiquetas RFID no tienen batería y se alimentan de la energía electromagnética transmitida por el propio lector al acercarlo o bien sus baterías pueden remplazarse con facilidad como en el caso de los marcapazos. No todos ellos necesitan protección criptográfica, pero en algunas aplicaciones se requerirá proteger los datos en reposo o en tránsito y es aquí donde interviene la criptgrafía de peso ligero.

Esta linea de investigación trae consigo el diseño e implementación de algoritmos criptográficos que ha pesar de tener entre sus ganancias el consumo de espacio, velocidad u otras propiedades también hacen que su seguridad sea más débil, de ahí el auge de ataques de canal colateral aplicable a tales dispositivos. Muchas son las contramedidas encontradas para prevenir estos ataques como son el Análisis de potencia simple SPA o Análisis de potencia diferencial DPA y entre las más comunes podemos encontrar las técnicas de enmascaramiento

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 4, Mes Octubre-Diciembre, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 207-232

y el hiding.

El cambio de llave fresco es otra de estas contramedidas, diseñada como alternativa para proteger etiquetas de RFID y otros dispositivos de bajo costo y fue propuesto por primera vez en (Medwed et al., 2010) como una solución que provee mejores cotas de seguridad que las contramedidas descritas hasta esa fecha ante ataques de fallo y ataques de potencia simple y diferencial. Este esquema fue diseñado para protocolos de respuesta-desafío usados para autenticar tags o microcircuitos de RF baratos incluidos en los dispositivos, capaces de permitir la identificación de objetos o sujetos fuera de la línea de visión (*non-line-of-sight*) conocido como RFID.

El esquema de cambio de llave fresco contiene una función de cifrado $\mathscr{E}$ para cifrar cada desafío o bloque de mensaje X con una llave de sesión fresca o reciente. La llave de sesión K^* es obtenida con la ayuda de una función g dependiente de la llave maestra K y un *nonce* público r como entrada. Los autores en (Medwed et al., 2010) piden como principales exigencias para que este mecanismo sea seguro que la función $\mathscr{E}$ sea segura contra SPA y la función g contra ambos ataques: SPA y DPA, aunque, en el desarrollo de este mismo artículo proponen condiciones que debe cumplir la función g motivadas por la combinación de aspectos de la seguridad contra ataques de canal colateral y aspectos de implementación en hardware. El uso de llaves diferentes para cada bloque o desafío que es cifrado hace que los análisis de seguridad desde la seguridad demostrable o probabilística de estos esquemas sean complicados al generarse para cada llave una permutación diferente para el cifrado. En la figura 1 se puede ver una representación del mecanismo de cambio de llave fresco.

Desde el punto de vista criptográfico las mejores opciones para la función g son una función resumen u otro algoritmo de cifrado en bloque, sin embargo, proteger estos algoritmos sería tan costoso como proteger la misma función $\mathscr{E}$, en contraste, desde el punto de vista ingenieril, una función de suma Xor sería lo mejor, de hecho, esta función cumple con casi todos los requisitos antes expuestos, pero su difusión es muy pobre, de aquí que los autores en (Medwed et al., 2010) hayan elegido multiplicación modular y definan la función g como:

$$g : (GF(2^8)[y]/p(y))^2 \longrightarrow GF(2^8)[y]/p(y) \quad \text{tal que} \quad (k,r) \rightarrow k * r \tag{1}$$

En (Medwed et al.) proponen extender este esquema a n partes con bajo costo y muestran que todavía en este escenario permanece seguro, sin embargo, en (Dobraunig et al., 2014) se presenta un ataque genérico de texto claro escogido para recuperar la llave sobre ambos esquemas, basado en dos observaciones, la primera es que

detectar colisiones en las llaves con un mismo texto claro es fácil y la segunda es la posibilidad de obtener la llave de sesión con una simple estrategia de tiempo-memoria trade-off. A partir de las observaciones anteriores los autores proponen una nueva condición para la función de cambio de llave y es que esta sea difícil de invertir, en otras palabras, que sea difícil obtener la llave maestra de la llave de sesión y el nonce.

A partir del trabajo de Medwed otros autores se proponen buscar nuevas alternativas para la función *g*, en 2013 en (Abdalla et al., 2013) los autores proponen como variante un esquema de cifrado simétrico resistente a fugas que usa un esquema de cambio de llave resistente a fugas con una prueba de seguridad asociada, usando como algoritmo de cifrado en bloque al AES (Daemen and Rijmen, 2001, 2020) y como esquema de cambio de llave una estructura de datos tipo *Skip-list* propuesto en los años 80.

En (Belaïd et al., 2014) se realiza un análisis sobre la seguridad de los esquemas resistentes a fugas, implementados en dispositivos de peso ligero desde tres niveles diferentes, a nivel de algoritmo, en la función de cambio de llave y a nivel estructural, este último teniendo en cuenta las debilidades reales de fuga acordes al modelo de fuga basado en la Distancia de Hamming que puedan darse por la implementación. A partir de estos análisis se realizan evaluaciones sobre las componentes específicas de los cifrados de bloque, como son tamaño de las S-cajas y criterios a cumplir por las permutaciones. Como resultado de este artículo los autores proponen una nueva construcción.

A pesar de que el uso de mecanismos de re-keying frescos sea una variante prometedora para la protección de dispositivos de peso ligero muchos investigadores se han volcado a penetrar estas garantías de seguridad evidentes o a buscar mejores variantes.

En (Dobraunig et al., 2015) por ejemplo se analizan modificaciones para mitigar los ataques realizados a los esquemas de cambio de llave frescos sugeridos en (Medwed et al., 2010; Medwed et al.) y se propone como variante el uso de algoritmos de cifrados en bloque basados en tweak como alternativa más eficiente y con mayor seguridad CPA (*Chosen Plaintext Attack*). Otras variantes para evitar ataques de canal colateral donde son consideradas la inclusión de valores *tweak*, no solo en el algoritmo de cifrado en bloque, sino también en el mensaje, se pueden encontrar en los trabajos (Baksi et al., 2018; Avraham et al., 2012). En (Guo and Johansson, 2019) se presenta una nueva variante de ataque de tipo cumpleaños sobre la base de una reducción más refinada con un polinomio reducible al anillo LPN (*Learning Parity with Noise problem*) disminuyendo el tiempo de complejidad en el modelo de fuga de 128 bits. Otras variantes de esquemas propuestos y análisis de su seguridad se pueden encontrar en los trabajos (Vuppala et al., 2019; Musale and Chaudhari, 2019), donde

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 4, Mes Octubre-Diciembre, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 207-232

son combinados los mecanismos de re-keyind con otras técnicas como el enmascaramiento.

Entre los resultados más recientes presentado por Bart Mennink en (Mennink, 2020) se encuentra la propuesta de 3 soluciones generalizadas para re-keying de cifrados en bloque paralelos que superan las cotas del cumpleaños para bloques de tamaño n. La primera propuesta de solución implica, luego de la generación de la subllave, una multiplicación y llamadas al núcleo del algoritmo de cifrado en bloque, obteniéndose una seguridad de $2^{\frac{2n}{3}}$. La segunda variante hace dos llamadas al cifrado de bloque y alcanza el óptimo de seguridad de 2^n. Finalmente, la tercera solución utiliza una función de generación de subllaves un poco más grande que no requiere adaptaciones en el núcleo de cifrado y también alcanza una seguridad óptima. En el mismo trabajo se construyen además usando este esquema de cambio de llave tres modos de autenticado resistentes a ataques de canal colateral que también alcanzan las cotas del cumpleaños.

Un elemento importante en este artículo es que el autor tiene en cuenta la composición de mecanismos de cambio de llave y cifrados de bloques que usan *tweat* teniendo en cuenta la tendencia desarrollada en la literatura por el uso de estos algoritmos dada la seguridad que proveen. Ejemplo de algoritmos y modos que usan *tweat* para añadir seguridad podemos encontrarlos en (Chakraborti et al., 2021; Maram et al., 2022; Chakraborty and Kundu, 2022) ambos modos diseñados para lograr autenticación.

Mecanismos externos

El enfoque externo es realizado a nivel de protocolo y es independiente del subyacente cifrado en bloque y modo de operación. Un protocolo criptográfico es el conjunto de acciones coordinadas que realizan dos o más partes o entidades con el objeto de llevar a cabo un intercambio de datos o información usando para ello algoritmos y métodos criptográficos permitiendo dar solución a distintos problemas de la vida real, especialmente donde puede existir un grado de desconfianza entre las partes. Ejemplos clásicos de protocolos criptográficos son los conocidos Protocolo TLS usado en la mayoría de los casos en conexiones web seguras (HTTPS), protocolo Diffie-Hellman para intercambio de llave y Kerberos para establecimiento de llaves y secreto compartido.

Para el trabajo a este nivel, los mecanismos externos asumen que la llave es transformada después de cifrar un número limitado de mensajes completos y es recomendado en protocolos que tienen una forma adecuada de dividir un mensaje largo en varias partes. A partir de este enfoque el número de mensajes que pueden ser procesados de forma segura con una llave K se incrementa sustancialmente siguiendo la idea presentada en la

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 4, Mes Octubre-Diciembre, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 207-232

figura 2.

Para este tipo de mecanismo se pueden usar dos tipos de construcciones para el procesamiento de las llaves, el enfoque paralelo o en serie, en el primer caso el procesamiento de datos de las llaves es generado directamente de la llave inicial y son independientes unas de otras y en el caso seriado, las llaves dependen del estado que es actualizado después de la generación de cada llave. Otro enfoque del cambio de llave externo visto como una generalización del enfoque paralelo externo es el mecanismo basado en árboles.

Para obtener un esquema de re-keying externo se deben vincular un esquema de cifrado base, un generador y el tiempo de vida de la llave, de esta manera, dado un esquema de cifrado simétrico con sus respectivos algoritmos de generación de llaves, cifrado y descifrado $\mathscr{SE} = (\mathsf{K_e}, \mathscr{E}, \mathscr{D})$ y $\mathscr{G} = (\mathsf{K_g}, \mathscr{N})$ un generador *stateful* con tamaño de bloque k, donde k es el tamaño de la llave del esquema base y $l > 0$ el tiempo de vida de la subllave, obtenemos entonces un esquema de cifrado extendido de la forma $\overline{\mathscr{SE}}[\mathscr{SE}, \mathscr{G}, l] = (\overline{\mathsf{K}}, \overline{\mathscr{E}}, \overline{\mathscr{D}})$.

En los trabajos (Abdalla and Bellare, 2000, 2021) se propone un teorema para medir la seguridad de los mecanismos externos haciendo uso de las nociones de seguridad de Indistinguibilidad Izquierda-Derecha definida en (Bellare et al., 1997) para los esquemas de cifrado simétricos:

Teorema 1
Dado $\mathscr{SE}$ un esquema de cifrado base con tamaño de llave k, $\mathscr{G}$ un generador stateful con tamaño de bloque k y $l > 0$ el tiempo de vida de la subllave y dado $\overline{\mathscr{SE}} = \overline{\mathscr{SE}}[\mathscr{SE}, \mathscr{G}, l]$ el esquema de cifrado extendido con cambio de llave asociado, entonces

$$\mathbf{Adv}^{\mathsf{ind-cpa}}_{\overline{\mathscr{SE}}}(t, ln, m) \leq \mathbf{Adv}^{\mathsf{prg}}_{G,n}(t) + n \cdot \mathbf{Adv}^{\mathsf{ind-cpa}}_{\mathscr{SE}}(t, l, m)$$

La interpretación cualitativa de este teorema, es que si el generador y el esquema de cifrado base o subyacente son seguros, también lo será el esquema de cifrado con cambio de llave. Desde el punto de vista cuantitativo se puede interpretar que la seguridad de cifrar $l \cdot n$ mensajes con el esquema extendido, está relacionada con la pseudoaleatoriedad de n bloques de salida del generador y la seguridad de cifrar l mensajes bajo una sola llave aleatoria, de aquí, que el término de la ventaja del adversario $\mathbf{Adv}^{\mathsf{ind-cpa}}_{\overline{\mathscr{SE}}}(t, l, m)$ sea multiplicado por n y haya una ganancia clara: la seguridad del esquema de cifrado base está relacionada con el cifrado de solo l mensajes. En otras palabras se puede cuantificar la seguridad de los mecanismos externos en función de la seguridad de las primitivas que usa.

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 4, Mes Octubre-Diciembre, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 207-232

La demostración de este teorema puede encontrarse en (Abdalla and Bellare, 2021), así como, los corolarios que muestran la seguridad de los esquemas basados en generadores paralelos y en serie. Con estos análisis de seguridad se evidencia que el aumento de seguridad es posible y que se puede medir de manera general la seguridad de variados esquemas *re-keyed* eligiendo los parámetros óptimos para minimizar la ventaja de los adversarios. Ejemplos de construcciones de cambios de llave externos se pueden encontrar en (Liu, 2002; Chen et al., 2008; Prakash et al., 2016; Gueron and Lindell, 2017; Bock et al., 2019).

Uno de los últimos diseño encontrados en la literatura (Tsypyschev and Morgasov, 2022) es un artículo propuesto por Vadim Tsypyschev y Iliya Morgasov donde se propone una variante externa seriada del modo CFB llamado por los autores *Multi-key CFB*, de forma abreviada MCFB. Con este diseño se busca construir un generador de secuencia pseudoaleatorias de peso ligero, sin embargo, en su análisis de seguridad en el modelo de seguridad demostrable LOR-CPA se encuentran incongruencias relacionadas con el teorema sobre la seguridad de los mecanismos externos propuesto en (Abdalla and Bellare, 2021).

Mecanismos internos

El método de cambio de llave interno es un enfoque que incrementa el tiempo de vida de las llaves usando una transformación de los datos de la llave durante el procesamiento de cada mensaje diferente. Tal mecanismo es construido dentro de un modo de operación particular, de ahí el nombre de mecanismo interno. Cada mensaje es procesado comenzando con la misma llave (la primera llave de sección) y cada llave de sección es actualizada usando cierta técnica de actualización después de procesar una cantidad determinada de bloques del mensaje (sección), la cual es medida en bloques y se determina sin ningún protocolo específico, sino dependiendo de los requerimientos del sistema y el tiempo de vida de la llave.

Los algoritmos de cifrado en bloques se definen como transformaciones que operan sobre bloques de tamaño fijo y los modos de operación surgen como alternativa o variante al cifrado de mensajes o textos claros que su longitud superan el tamaño de dichos bloque, por lo que son los que definen como se procesan y combinan los bloques de salida del algoritmo para obtener el texto cifrado. Los modos de confidencialidad considerados como clásicos son el ECB, CBC, OFB, CFB y CTR (PUB, 1980; Knudsen, 1994; Dworkin, 2001; Rogaway, 2011) por lo que hemos encontrado en la literatura variantes de mecanismos de re-keying interno que constituyen modificaciones de los mismos.

En este enfoque tiene un papel fundamental el tamaño de la sección y este viene dado por las limitaciones del

tiempo de vida de la llave que será usada, estas limitaciones pueden estar dadas por propiedades combinatorias del modo de operación probabilísticas (Lavrikov and Shishkin, 2019) o demostrable (Bellare et al., 1997; Anand et al., 2016; Tsypyschev and Morgasov, 2022; Nemoz et al., 2022; Maram et al., 2022), ataques de canal colateral (Black and Urtubia, 2002; Liu, 2002; Perusheska et al., 2002; Suga, 2018; Banerjee et al., 2022; Lee et al., 2022; Noura et al., 2019a) o ataques conocidos al cifrado en bloque que se utiliza (Rohit and Sarkar, 2022; Bariant and Leurent, 2022; Yadav et al., 2022), etc. Tamaños de sección grandes hacen que el procesamiento de los mensajes sea más rápido, sin embargo, tamaños pequeños aumenta la cantidad de mensajes procesados de forma diferente. Es recomendable usarlo en protocolos que procesen mensajes largos, ya que la máxima ganancia en este enfoque se consigue en el incremento de la longitud del mensaje que será cifrado. La idea básica del mismo se puede apreciar en la figura 3.

La idea esencial de hacer dinámicos los modos de operación de los algoritmos de cifrado en bloques no es nueva, se puede encontrar en la bibliografía ejemplos muy antiguos de diseños de modos de operación que hacen dinámicos algunos de sus valores secretos para ganar mayor seguridad, entre estos podemos mencionar una variante de los modos OFB y CBC propuesta en (Jansen and Boekee, 1987) en el año 1988 donde los autores proponen una variante del modo de operación OFB con una función no lineal que trabaja a partir de la siguiente regla de cifrado

$$C_i = E_{k_i}(P_i) \text{donde} \quad K_i = E_k(K_{i-1}) \tag{2}$$

En (Knudsen, 1994) se realizan algunos análisis de seguridad de este modo con respecto a su distancia de unicidad, errores de propagación e implementación. En este caso el tamaño de la sección N coincide con un solo bloque y no se pudo encontrar en la literatura pruebas de su seguridad ni probabilísticas ni bajo la teoría de la seguridad demostrable.

En el artículo (Noura et al., 2019b) se proponen dos mecanismos: fresco e interno. Por lo que además de variar la llave con cada mensaje a ser cifrado, proponen una variante dinámica del modo de operación ECB en orden de evitar los asuntos asociados al orden estático de cifrado con este modo. Esto se logra seleccionando el orden de los bloques que serán cifrado de manera pseudoaleatoria y dinámica en lugar de la típica orden secuencial, ya que, la selección de los bloques está basada en una tabla de permutación dinámica que es obtenida de la llave dinámica,la cual cambia para cada mensaje de entrada. Además se lleva a cabo una mezcla pseudoaleatoria de dos bloques en lugar de uno para incrementar la aleatoriedad del texto cifrado y

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 4, Mes Octubre-Diciembre, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 207-232

hacer el criptanálisis aún más difícil. En este caso la llave cambia con cada mensaje y el orden de los bloques también dependiendo de la llave de cifrado. Este se puede ver como la integración de dos de los mecanismos de extensión de vida de las llaves.

En el año 2006 en (Popov et al., 2006) se define el modo de cifrado *Key Meshing*, para el cifrado de mensajes largos con el algoritmo GOST 28147-89, el cual transforma la llave de cifrado y el vector de inicialización una vez procesado una cierta cantidad de datos, en este caso 1024 octetos equivalentes a 256 bloques de 64 bit de texto claro. Este algoritmo afecta el estado interno del cifrado y no trabaja a nivel de protocolo, además tiene la misma desventaja que el modo OFB, ya que resulta imposible restablecer la sincronización del cifrado durante el descifre cuando los datos han sido corruptos, perdidos o desordenados. Además, es imposible re-sincronizar incluso si el vector de inicialización para cada paquete de datos es proveído explícitamente. El uso de este algoritmo en protocolos como el IPsec requiere de cuidado especial.

El procesamiento con este algoritmo de 1024 octetos empieza con el cálculo de la llave y vector de inicialización de la presente sección, a partir del descifre y cifre en el modo ECB de la llave y el vector IV de la sección anterior a partir de las siguientes fórmulas

$$K[i+1] = decryptECB(K[i], C) \tag{3}$$

$$IV0[i+1] = encryptECB(K[i+1], IVn[i]) \tag{4}$$

donde C es una constante dada fija.

En el trabajo (Popov et al., 2006) son analizadas las propiedades combinatorias y probabilísticas de este método, pero no hay análisis de su impacto sobre las propiedades criptográficas del modo de cifrado usado, de aquí que, en 2016 en (Akhmetzyanova et al., 2017) se presenten las cotas de seguridad en el modelo de seguridad estándar de la seguridad demostrable para el cifrado Magma en el modo CTR y el modo CPKM previamente usado en el cifrador GOST 28147-89. En este caso se analiza una variante del algoritmo original CPKM donde no es considerado la regla para el cambio del vector de inicialización IV y la llave es procesada con el algoritmo Kuznyechik cuando la sección es de un tamaño de 128 bits.

En la demostración de seguridad modelan un adversario usando una máquina de Turing probabilística, suponiendo que $A(t,a,b,\ldots)$ es el conjunto de adversarios cuyas fuentes computacionales (tamaño del programa y promedio de complejidad) no son mayores que t y el resto de los parámetros (ejemplo: número de preguntas

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 4, Mes Octubre-Diciembre, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 207-232

al oráculo) están limitados por los valores $a, b, \ldots$ para cada caso específico que sea analizado. Si **T** es un problema decisional donde el adversario A puede distinguir un bit b, entonces la ventaja promedio de este adversario para el problema **T** es $\mathbf{Adv}^{\mathbf{T}}(A) = Pr[A \Rightarrow 1|b = 1] - Pr[A \Rightarrow 1|b = 0]$.

Los modelos de seguridad más usados derivados del trabajo (Bellare et al., 1997) para los cifrados de bloque son los modelos PRF y PRP-CCA, en ambos casos se debe decidir entre el uso de una función aleatoria y el cifrado de bloque y el uso de una permutación pseudoaleatoria y el cifrado respectivamente. Ambos casos son consecuentes con los métodos basados de la paradoja del cumpleaños y el ataque por fuerza bruta. De aquí que se asuman las siguientes aproximaciones:

$$\mathbf{Adv}_E^{\mathsf{PRP-CCA}}(t,q) \approx \frac{t}{2^k}, \qquad \mathbf{Adv}_E^{\mathsf{PRF}}(t,q) \approx \frac{t}{2^k} + \frac{q^2}{2^n} \tag{5}$$

Así como son propuestos los modelos anteriores de seguridad para los cifrados en bloque también se define en (Bellare et al., 1997) el modelo LOR-CPA como uno de los más usuales a ser usados en las pruebas de seguridad de los modos de operación, en este caso se debe decidir entre el cifrado de dos mensajes de igual tamaño. Dentro de las relaciones encontradas entre estos modelos se debe destacar la relación entre el modelo PRP y LOR-CPA para el caso del modo de operación CTR:

$$\mathbf{Adv}_{CTR}^{\mathsf{LOR-CPA}}(t,q,m) \leqslant 2 \cdot \mathbf{Adv}_E^{\mathsf{PRF}}(t+q+nqm, qm) \tag{6}$$

En (Akhmetzyanova et al., 2017) también es usado además un problema intermedio IND-KM$_{l,m}$ para remplazar el modo CTR-CPKM$_l$ por el modo CTR-RK$_l$ donde la llave es escogida de forma aleatoria para cada nueva sección, obteniéndose para el cifrado Magma las siguientes cotas:

$$\mathbf{Adv}_{CTR}^{\mathsf{LOR-CPA}}(t,q,ml) \approx \frac{2m^2q^2l^2}{2^n} + \frac{t+q+nmql}{2^k} \approx m^2 \cdot \frac{2q^2l^2}{2^n} \tag{7}$$

$$\mathbf{Adv}_{CTR-CPKM_l}^{\mathsf{LOR-CPA}}(t,q,ml) \approx 2m\Big(2 \cdot \frac{t+qml}{2^k} + \frac{q^2l^2}{2^n} + \frac{t+qml}{2^k} + \delta\Big) \approx m \cdot \frac{2q^2l^2}{2^n} \tag{8}$$

y concluyendo que la seguridad con el modo CTR-CPKM$_l$ aumenta con respecto a la seguridad con el modo CTR clásico. Las cotas para el caso del algoritmo Kuznyechik con tamaño de sección 128 bits son similares a las obtenidas para el caso del Magma.

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 4, Mes Octubre-Diciembre, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 207-232

El método CPKM de cambio de llave interno tiene la desventaja de que pueden existir colisiones en las entradas a la permutación del cifrado en bloque en los casos de la transformación de la llave y en el procesamiento del mensaje. Debido a esta debilidad los propios autores proponen en un posterior articulo una mejora de este método al asegurar que las constantes usadas en la generación de las llaves y procesamiento del mensaje no son susceptibles a colisiones a través de la transformación usada. Pero este truco es posible solamente para modos en los que se puede predecir la entrada a la transformación de cifrado por lo que esta solución no puede ser usada en cualquier modo (por ejemplo no se puede usar en los modos CBC o CFB).

En (Ahmetzyanova et al., 2017) en 2017 los mismos autores introducen los conceptos de cambio de llave externo e interno como generalizaciones de la derivación de llaves y el método de *Key Meshing* y se discuten sus características, ventajas y desventajas. De esta misma manera proponen un nuevo mecanismo de extensión de las llaves llamado ACPKM, como una mejora del mecanismo de cambio de llave interno CPKM y se modifica el modo de autenticado GCM, así como, se aumentan las cotas de seguridad asociadas al mismo. Se realiza un análisis comparativo con respecto a la implementación en *hardware* y se concluye con que el método de cambio de llave interno no se puede ver como una alternativa diferente al cambio de llave externo sino como una extensión más fuerte o poderosa.

También afirman que la estructura de prueba obtenida (problema IKM) es útil para obtener límites de seguridad para otros modos de operación *re-keyed* que no usen valores secretos adicionales (sin llave maestra). Los análisis de seguridad de los métodos internos conducen al análisis de modos abstractos donde las llaves de sección son escogidas independientes y aleatorias. Para algunos modos de operación (CTR, OFB, CBC) la seguridad de sus correspondientes modos con llaves aleatorias puede ser fácilmente analizados, usando técnicas de argumento híbridos.

En 2017 se presenta en (Ahmetzyanova et al., 2017) el modo de cambio de llave interno de cifrado en bloque CTR - ACPKM y es asumido en el sistema de Estandarización ruso y debe pasar a través de las últimas etapas formales de normalización en el Grupo de Trabajo en Ingeniería de Internet o IETF por sus siglas en inglés (*Internet Engineering Task Force*), por lo que varios investigadores rusos han dedicado sus esfuerzos a demostrar la seguridad de estos métodos.

En 2018 en (Akhmetzyanova et al., 2018) se realiza un análisis de la seguridad de este modo de operación similar al análisis realizado para el algoritmo GCM-ACPKM con la diferencia de que en aquel caso las cotas de seguridad son analizadas con respecto a la cantidad máxima de texto claro y en el modo CTR las cotas son

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 4, Mes Octubre-Diciembre, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 207-232

dadas a partir del tamaño total del texto claro, para este análisis también se emplea el modelo de seguridad IND-CPNA propuesto anteriormente por Bellare y Rogaway en (Bellare and Rogaway, 2004). Este modelo es similar al IND-CPA pero considera un adversario con acceso al *nonce*. Este es un modelo de seguridad estándar más fuerte que permite analizar las propiedades criptográficas del modo desde el punto de vista computacional cercano al cifrado ideal *one-time-pad*. Otro análisis comparativo de este modo con respecto al algoritmo Fortuna desde un enfoque estadístico puede ser visto en (Peñate et al., 2020).

En el mecanismo de cambio de llave ACPKM el mensaje es procesado comenzando con una misma llave, la primera llave de sección y cada llave de sección es actualizada usando cierta técnica de actualización de llave después de procesar una cierta cantidad de bloques (una sección). Para el parámetro N el modo de operación de derivación de llaves interno $CTR-ACPKM_N$ trabaja de la siguiente forma:

Dado un mensaje de entrada X de m bloques de tamaño n, este será dividido en $l = \lceil \frac{m}{N} \rceil$ secciones (denotadas como $X = X^1 \| X^2 \| \ldots \| X^l$, donde $X^i \in \{0,1\}^{nN}$ para $i \in \{1,2,\ldots,l-1\}$, $X^l \in \{0,1\}^r$,$r \leqslant nN$) que serán procesadas bajo la misma llave inicial. La primera sección de cada mensaje es procesado bajo la llave de sección $K^1 = K$ usando el modo CTR. La i-ésima sección del mensaje es continuamente procesada usando el mismo modo con la llave de sección K^{i+1} , la cual fue calculada usando la transformación $ACPKM$ como sigue:

$$K^{i+1} = ACPKM(K^i) = msb_k(E_{k^i}(D_1) \| \ldots \| E_{k^i}(D_s)) \tag{9}$$

donde $s = \lceil \frac{k}{n} \rceil$ y $D_1, D_2, \ldots . D_s \in \{0,1\}^n$ son constantes arbitrarias diferentes por pares, tales que, $(\frac{n}{2}) - th$ bit (contando desde la derecha) de cada D_i es igual a 1. Note que el estado interno (contador) del modo $CTR-ACPKM_N$ no es actualizado para cada nueva sección y la condición impuesta a las constantes permite prevenir colisiones en los bloques de entrada a la permutación generada por el cifrado de bloque con la llave actual. En el análisis de seguridad descrito anteriormente los autores en Akhmetzyanova et al. (2018) proponen el siguiente resultado:

Teorema 2

Sea N el parámetro del modo $CTR-ACPKM_N$. Entonces para cualquier adversario A con un tiempo de complejidad a lo sumo t que hace preguntas, donde el tamaño máximo del mensaje es a lo sumo m ($m \leq$

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 4, Mes Octubre-Diciembre, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 207-232

$2^{n/2-1}$) bloques y un total de tamaño de mensaje de a lo sumo σ bloques, existe un adversario B tal que

$$\mathbf{Adv}^{\mathsf{ind-cpna}}_{CTR-ACPKM_N}(A) \leq l \cdot \mathbf{Adv}^{\mathsf{prp-cpa}}_{\mathscr{E}}(B) + \frac{(\sigma_1+s)^2+\ldots+(\sigma_{l-1}+s)^2+(\sigma_l)^2}{2^{n+1}} \tag{10}$$

donde $s = \lceil k/n \rceil$, $l = \lceil m/N \rceil$, σ_j es el tamaño total de bloques de datos procesados bajo una misma llave de sección K^j y $\sigma_j \leq 2^{n-1}, \sigma_1+\ldots+\sigma_l = \sigma$. El adversario B hace a los sumo σ_1+s preguntas. Además el tiempo de complejidad de B es a lo sumo $t+cn(\sigma+ls)$, donde c es una constante que depende solamente del modelo de cálculo y método de codificación.

Como otro ejemplo de diseños de mecanismos de cambio de llave interno se presenta el método propuesto en el año 2018 en (Alekseev et al., 2020) el nuevo modo de operación CTRR (Modo de cambio de llave contador con llaves relacionadas) que usa varias llaves con suma xor fija o modular, que contiene también como modo de operación base, el CTR y considera como premisa que el sudyacente cifrado de bloque, en este caso, el Kuznyechik, es seguro bajo el modelo de seguridad PRP-RKA (modelo de llaves relacionadas) introducido en (Bellare and Kohno, 2003). En este articulo se obtienen las cotas inferiores de seguridad para este modo en el modelo LOR-CPA dependiendo de la seguridad del cifrador usado en un modelo con dos llaves relacionadas.

La seguridad de un cifrado de bloque en el modelo PRP-RKA de llaves relacionas no se deriva de su seguridad estándar en el modelo PRP-CPA, las oportunidades del adversario en el modelo de llaves relacionadas son mayores que en los modelos estándar, por lo tanto, generalmente la demostración de la seguridad (en este modelo) del cifrado y su análisis requieren significativamente más esfuerzo, ya que, hay requisitos adicionales sobre el esquedule de llave. Sin embargo, el esfuerzo de desarrollar y analizar el cifrado en el modelo de llaves relacionadas está compensado por el hecho de que pueden ser desarrollados criptosistemas más eficientes sobre estos cifrados. La eficiencia se logra debido a la habilidad de trabajar no sólo con llaves independientes sino también con llaves relacionadas por una relación simple, a continuación se muestra el esquema de trabajo del algoritmo Kuznyechik en el modo CTRR:

1. $ctr_1 = IV||0^{n/2}$, $ctr_j = Inc(ctr_{j-1}), \quad j = 2,\ldots,|P|_n$
2. $K_1 = K, \quad K_j = E_{\phi(K_{j-1})}(C_1)||\ldots||E_{\phi(K_{j-1})}(C_{k/n}), \quad j = 2,\ldots,\lceil |P|/N \rceil$
3. $G_j = E_{K_i}(ctr_j),\ j = 1,\ldots,|P|_n,\ i = \lceil j \cdot n/N \rceil$;
4. Texto cifrado C es igual a $P \oplus msb_{|P|}(G_1||\ldots||G_{|P|_n})$

En este esquema el texto claro es procesado de la misma manera que en el modo estándar CTR pero la llave que es usada para generar los bloques cifrados G_j no es constante y se actualiza después de generar N/n

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 4, Mes Octubre-Diciembre, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 207-232

bloques G_j. La transformación ϕ puede ser algunas de las siguientes:
$-\phi(X) = X \oplus c$, para alguna constante $c \in V_k$, $c \neq 0^k$;
$-\phi(X) = str_k(int(X) + c \mod 2^k)$ para alguna constante $c \in \{1, \ldots, 2^k - 1\}$

Resultados y discusión

Como resultado de la revisión bibliográfica podemos decir que una de las ventaja del mecanismo externo se encuentra en el manejo de una llave inicial empleada como llave maestra que nunca es usada para el proceso de cifrado directamente, ya que de ella se derivan las llaves usadas para cada sección. El material cifrado con una llave de sección está estrictamente limitado por el tamaño de la sección sin influir las limitaciones del tiempo de vida de la llave maestra. El tiempo de vida de la llave incrementa independientemente del modo con una completa y correcta prueba de seguridad basada en la teoría de la seguridad demostrable y las fugas derivadas de una llave derivada no tienen impacto sobre el resto de las llaves derivadas.

En el caso interno las transformaciones efectuadas a la llave siempre se pueden realizar con independencia del tamaño del mensaje, siempre considerando el modo en las que son usadas sin ser necesario restaurar el proceso de cifrado en dependencia del tamaño del mensaje y las transformaciones de la llave no se ven limitadas por el tiempo de vida de la llave maestra.

Indudablemente la ventaja del caso externo es la posibilidad de usar las cotas de seguridad obtenidas para el modo de operación base para cuantificar la seguridad del modo externo correspondiente (Ahmetzyanova et al., 2017). Este enfoque es propuesto para realizarse cada vez que una cantidad de mensajes es procesado, sin embargo, el tiempo de vida de la llave depende de la longitud total de los mensajes procesados y no de su cantidad. Estos límites pueden ser acotados por las limitaciones de seguridad del tiempo de vida de la llave. Por tanto la cantidad de mensajes procesados será proporcional a su máximo tamaño y el largo del mensaje procesado requerirá una fragmentación adicional (Ahmetzyanova et al., 2017).

El enfoque interno no puede ser tratado como una alternativa del enfoque externo sino como una extensión más fuerte y permite eliminar el problema de limitación de la longitud del mensaje cuando el tiempo de vida de la llave es limitada.

El caso fresco tiene una estructura más lejana del resto y además de lograr extender el tiempo de vida de las llaves se logra evadir ataques de canal colateral, lo cual no se puede asegurar en el resto de los casos ya

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 4, Mes Octubre-Diciembre, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 207-232

que se sigue cifrando con una llave más de un bloque de texto claro, condición que se usa para implementar los ataques de canal colateral, sin embargo, al generarse una nueva permutación con el uso de cada llave de cifrado sus análisis de seguridad son más difíciles de realizar. Sin embargo, este método solo es posible o tiene sentido cuando es significativamente más fácil proteger la función de generación de llave contra los ataques diferenciales que el propio algoritmo original. A pesar de tener una ganancia evidente en su diseño se puede apreciar en los trabajos más recientes una tendencia a combinar este mecanismos con otras técnicas de enmascaramiento o a ser superada por el uso de valores *tweat* en diferentes niveles de los algoritmos de cifrado en bloque o en los modos de operación.

Conclusiones

Como resultado de la investigación realizada sobre el estado del arte se encontraron 3 mecanismos de cambio de llave y se pudo establecer los niveles donde es más óptimo su uso, concluyendo que su aplicación está determinada en primera instancia a partir de las características de los mensajes a cifrar. En el caso particular en que los mensajes puedan considerarse como pequeños o de poca longitud se recomienda el uso de mecanismos externos para garantizar el aumento del tiempo de vida de las llaves, sin embargo para el procesamiento de mensajes largos se recomienda el uso de mecanismos internos. Para los entornos de aplicación en dispositivos de peso ligero es recomendable los mecanismos frescos aunque también se recomienda el uso de valores tweat en diferentes niveles de los algoritmos de cifrado en bloque para obtener las mismas ganancias de seguridad.

En cada una de las variantes se logra un aumento del tiempo de vida de las llaves de cifrado, sin embargo, recomendamos implementar mecanismos internos cuando estemos en presencia de algoritmos de cifrado en bloque dinámicos (sus funciones o transformaciones varían en dependencia de la llave bajo ciertas relaciones o de forma aleatoria), solución que a pesar de disminuir el rendimiento aporta más seguridad al cifrado de los datos.

Se sugiere a los diseñadores trabajar en la combinación de estos mecanismos para alcanzar resultados superiores en la seguridad de los esquemas criptográficos y la protección de la información, aprovechando las ventajas de cada una de estas variantes.

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 4, Mes Octubre-Diciembre, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 207-232

Referencias

Michel Abdalla and Mihir Bellare. Increasing the lifetime of a key: a comparative analysis of the security of re-keying techniques. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 546–559. Springer, 2000.

Michel Abdalla and Mihir Bellare. Increasing the lifetime of a key: a comparative analysis of the security of re-keying techniques. *https://cseweb.ucsd.edu/ mihir/papers/rekey.pdf*, 2021.

Michel Abdalla, Sonia Belaïd, and Pierre-Alain Fouque. Leakage-resilient symmetric encryption via re-keying. In *International Conference on Cryptographic Hardware and Embedded Systems*. Springer, 2013.

Liliya R Ahmetzyanova, Evgeny Konstantinovich Alekseev, Igor Borisovich Oshkin, and Stanislav Vitalévich Smyshlyaev. Increasing the lifetime of symmetric keys for the gcm mode by internal re-keying. *IACR Cryptol. ePrint Arch.*, 2017(697), 2017.

Liliya R Akhmetzyanova, Evgeny Konstantinovich Alekseev, Igor Borisovich Oshkin, Stanislav Vitalévich Smyshlyaev, and Lolita A Sonina. On the properties of the ctr encryption mode of magma and kuznyechik block ciphers with re-keying method based on cryptopro key meshing. *Mathematical Aspects of Cryptography*, 8(2):39–50, 2017.

Liliya R Akhmetzyanova, Evgeny Konstantinovich Alekseev, and Stanislav Vitalévich Smyshlyaev. Security bound for ctr acpkm internally re-keyed encryption mode. *IACR Cryptology ePrint Archive*, 2018(950), 2018.

Evgeny K Alekseev, Kirill S Goncharenko, and Grigory B Marshalko. Provably secure counter mode with related-key-based internal re-keying. In *7 th Workshop on Current Trends in Cryptology (CTCrypt 2018)*, pages 161–180.

Evgeny K Alekseev, Kirill S Goncharenko, and Grigory B Marshalko. Provably secure counter mode with related-key-based internal re-keying. *Journal of Computer Virology and Hacking Techniques*, 16(4):285–294, 2020.

Mayuresh Vivekanand Anand, Ehsan Ebrahimi Targhi, Gelo Noel Tabia, and Dominique Unruh. Post-quantum security of the cbc, cfb, ofb, ctr, and xts modes of operation. In *Post-quantum Cryptography*, pages 44–63. Springer, 2016.

Uri Avraham, Eli Biham, and Orr Dunkelman. *ABC-A New Framewrok for Block Ciphers*. PhD thesis, Computer Science Department, Technion, 2012.

Anubhab Baksi, Shivam Bhasin, Jakub Breier, Mustafa Khairallah, and Thomas Peyrin. Protecting block ciphers against differential fault attacks without re-keying. In *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 2018.

Utsav Banerjee, Lisa Ho, and Skanda Koppula. Power-based side-channel attack for aes key extraction on the atmega328 microcontroller. *arXiv preprint arXiv: 2203.08220*, 2022.

Augustin Bariant and Gaëtan Leurent. Truncated boomerang attacks and application to aes-based ciphers. *Cryptology ePrint Archive*, 2022.

Sonia Belaïd, Fabrizio De Santis, Johann Heyszl, Stefan Mangard, Marcel Medwed, Jörn-Marc Schmidt, François-Xavier Standaert, and Stefan Tillich. Towards fresh re-keying with leakage-resilient prfs: cipher design principles and analysis. *Journal of Cryptographic Engineering*, 4(3), 2014.

Mihir Bellare and Tadayoshi Kohno. A theoretical treatment of related-key attacks: Rka-prps, rka-prfs and applications. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 491–506. Springer, 2003.

Mihir Bellare and Phillip Rogaway. Introduction to modern cryptography. chapter 4, symmetric encryption, 2004.

Mihir Bellare, Anand Desai, Eron Jokipii, and Phillip Rogaway. A concrete security treatment of symmetric encryption. In *Proceedings 38th Annual Symposium on Foundations of Computer Science*, pages 394–403. IEEE, 1997.

John Black and Hector Urtubia. {Side-Channel} attacks on symmetric encryption schemes: The case for authenticated encryption. In *11th USENIX Security Symposium (USENIX Security 02)*, 2002.

Benedikt Bock, Jan-Tobias Matysik, Konrad-Felix Krentz, and Christoph Meinel. Link layer key revocation and rekeying for the adaptive key establishment scheme. In *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*. IEEE, 2019.

Avik Chakraborti, Nilanjan Datta, Ashwin Jha, Cuauhtemoc Mancillas-López, and Mridul Nandi. Light-ocb: Parallel lightweight authenticated cipher with full security. In *International Conference on Security, Privacy, and Applied Cryptography Engineering*, pages 22–41. Springer, 2021.

Debrup Chakraborty and Samir Kundu. {\sf TrCBC} is insecure. *Cryptology ePrint Archive*, 2022.

Lily Chen et al. Recommendation for key derivation using pseudorandom functions. *NIST special publication*, 800:108, 2008.

Joan Daemen and Vincent Rijmen. Announcing the advanced encryption standard (aes). *Federal Information Processing Standards Publication*, 197, 2001.

Joan Daemen and Vincent Rijmen. *The design of Rijndael: AES the advanced encryption standard*. Springer, 2020.

Gianluca Dini and Ida M Savino. Lark: a lightweight authenticated rekeying scheme for clustered wireless sensor networks. *ACM Transactions onEmbedded Computing Systems (TECS)*, 10(4):1–35, 2011.

Christoph Dobraunig, Maria Eichlseder, Stefan Mangard, and Florian Mendel. On the security of fresh re-keying to counteract side-channel and fault attacks. In *International Conference on Smart Card Research and Advanced Applications*. Springer, 2014.

Christoph Dobraunig, François Koeune, Stefan Mangard, Florian Mendel, and François-Xavier Standaert. Towards fresh and hybrid re-keying schemes with beyond birthday security. In *International Conference on Smart Card Research and Advanced Applications*. Springer, 2015.

Morris Dworkin. Nist special publication 800-38a 2001 edition. *NIST Special Publication*, 800(3):38A, 2001.

Shay Gueron and Yehuda Lindell. Better bounds for block cipher modes of operation via nonce-based key derivation. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017.

Qian Guo and Thomas Johansson. A new birthday-type algorithm for attacking the fresh re-keying countermeasure. *Information Processing Letters*, 146, 2019.

Cees JA Jansen and Dick E Boekee. Modes of blockcipher algorithms and their protection against active eavesdropping. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 281–286. Springer, 1987.

Mustafa Khairallah. Weak keys in the rekeying paradigm: application to comet and mixfeed. *Cryptology ePrint Archive*, 2019.

Lars Ramkilde Knudsen. *Block ciphers-analysis, design and applications*. Citeseer, 1994.

IV Lavrikov and Vasily Alekseevich Shishkin. How much data may be safely processed on one key in different modes? *Mathematical Aspects of Cryptography*, 10(2):125–134, 2019.

Wai-Kong Lee, Seog Chung Seo, Hwa Jeong ang Seo, and Seong Oun Hwang. Efficient implementation of aes-ctr and aes-ecb on gpus with applications for high-speed frodokem and exhaustive key search. volume 69, pages 2962–2966, 2022.

Shengli Liu. *Information-theoretic secret key agreement*. Citeseer, 2002.

Varun Maram, Daniel Masny, Sikhar Patranabis, and Srinivasan Raghuraman. On the quantum security of ocb. *IACR Transactions on Symmetric Cryptology*, 2022.

Marcel Medwed, Christoph Petit, Francesco Regazzoni, Mathieu Renauld, and François-Xavier Standaert. Fresh re-keying ii: Security multiple parties against side-channel and fault attacks. In *International Conference on Smart Card Research and Advance Applications*, pages 115–132.

Marcel Medwed, François-Xavier Standaert, Johann Großschädl, and Francesco Regazzoni. Fresh re-keying: Security against side-channel and fault attacks for low-cost devices. In *International Conference on Cryptology in Africa*, pages 279–296. Springer, 2010.

Bart Mennink. Beyond birthday bound secure fresh rekeying: Application of authenticated encryption. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 630–661. Springer, 2020.

Muhammad arif Mugal, Peng Shi, Ata Ullah, Khalid Mahmood, Muhammad Abid, and Xiong Luo. Logical tree based secure rekeying management for smart devices groups in iot enabled wsn. *IEEE Access*, 7: 76699–76711, 2019.

Vinayak Musale and Devendra Chaudhari. Efficient and secure keying mechanism for communication in sensor networks. In *International Conference on Intelligent Data Communication Technologies and Internet of Things*. Springer, 2019.

Tristan Nemoz, Zoé Amblard, and Aurélien Dupin. Characterizing the qind-qcpa (in) security of the cbc, cfb, ofb and ctr modes of operation. *Cryptology ePrint Archive*, 2022.

Hassan Noura, Ali Chehab, and Raphael Couturier. Lightweight dynamic key-dependent and flexible cipher scheme for iot devices. In *2019 IEEE Wireless Communications and Networking conference (WCNC)*, pages 1–8. IEEE, 2019a.

Hassan N Noura, Ali Chehab, and Raphael Couturier. Efficient & secure cipher scheme with dynamic key-dependent mode of operation. *Signal processing: Image communication*, 78:448–464, 2019b.

Adrián Alfonso Peñate, Daymé Almeida Echevarria, and Laura Castro Argudín. Statistical assessment of two rekeying mechanisms applied to the generation of random numbers. *Journal of Science and Technology on Information security*, 2(12):38–44, 2020.

Milena Gjorgjievska Perusheska, Hristina Mihajloska Trpceska, and Vesna Dimitrova. Deep learning-based cryptoanalysis of different aes modes of operation. In *Future of Information and Communication Conference*, pages 675–693. Springer, 2002.

Vladimir Popov, I Kurepkin, and S Leontiev. Additional cryptographic algorithms for use with gost 28147-89, gost r 34.10-94, gost r 34.10-2001, and gost r 34.11-94 algorithms. *Retrieved January*, 2006.

A John Prakash, V Rhymend Uthariaraj, and B Lydia Elizabeth. Efficient key management protocol with predictive rekeying for dynamic networks. In *2016 2nd International Conference on Green High Performance Computing (ICGHPC)*. IEEE, 2016.

FIPS PUB. Des modes of operation, 1980.

Chuan Qin, Jingwei Li, and Patrick PC Lee. The design and implementation of a rekeying-aware encrypted deduplication storage system. *ACM Transactions on Storage (TOS)*, 13(1):1–30, 2017.

Phillip Rogaway. Evaluation of some blockcipher modes of operation. *Cryptography Research and Evaluation Committees (CRYPTREC) for the Government of Japan*, 2011.

Raghvendra Rohit and Santanu Sarkar. Cryptanalysis of reduced round speedy. *Cryptology ePrint Archive*, 2022.

Yuji Suga. Satatus survey of ssl/tls sites in 2018 after pointing out about ”search formïssues. In *2018 Sixth International Symposium on Computing and Networking Workshops (CANDARW)*, pages 483–485. IEEE, 2018.

Vadim Tsypyschev and Iliya Morgasov. Provable security of cfb mode of operation with external re-keying. *Cryptology ePrint Archive*, 2022.

Satyanarayana Vuppala, Alie El-Din Mady, and Adam Kuenzi. Rekeying-based moving target defence mechanism for side-channel attacks. In *2019 Global IoT Summit (GIoTS)*. IEEE, 2019.

Tarun Yadav, Manoj Kumar, Amit Kumar, and Saibal K Pal. A pratical-quantum differential attack on block ciphers. *Cryptology ePrint Archive*, 2022.

Conflicto de interés

Los autores no poseen conflictos de intereses y autorizan la distribución y uso de su artículo.

Contribuciones de los autores

1. Conceptualización: Daymé Almeida Echevarria
2. Curación de datos:Ramses Rodríguez Aulet
3. Análisis formal: Ernesto Dominguez Fiallo, Daymé Almeida Echevarria, Ramses Rodríguez Aulet
4. Adquisición de fondos:–
5. Investigación: Daymé Almeida Echevarria, Ernesto Dominguez Fiallo, Ramses Rodríguez Aulet
6. Metodología: Daymé Almeida Echevarria
7. Administración del proyecto: Daymé Almeida Echevarria
8. Recursos: Ernesto Dominguez Fiallo
9. Software: –
10. Supervisión: Daymé Almeida Echevarria
11. Validación: Ramses Rodríguez Aulet

12. Visualización: Ernesto Dominguez Fiallo
13. Redacción - borrador original: Daymé Almeida Echevarria
14. Redacción - revisión y edición: Ernesto Dominguez Fiallo y Ramses Rodríguez Aulet

Financiación

La investigación no requirió fuente de financiamiento.

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 4, Mes Octubre-Diciembre, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 207-232

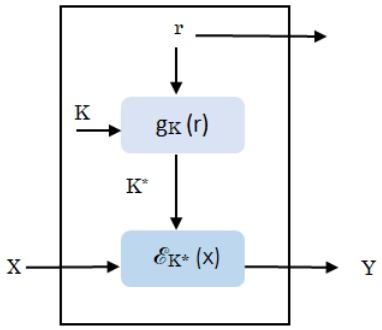

Fig. 1 - Esquema general del Mecanismo de cambio de llave fresco.

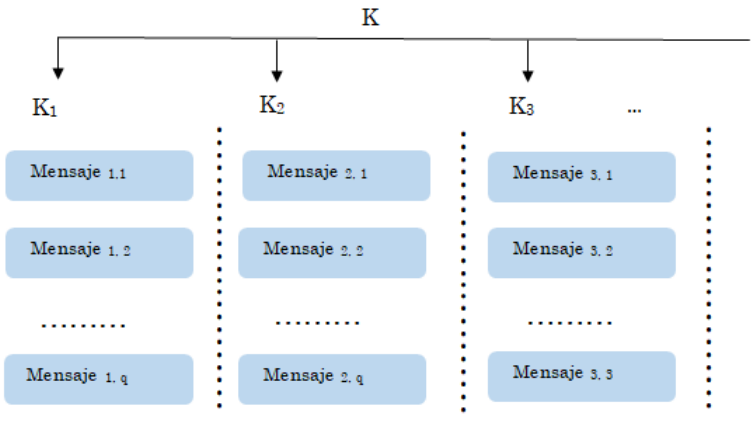

Fig. 2 - Esquema general del Mecanismo de cambio de llave externo.

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 4, Mes Octubre-Diciembre, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 207-232

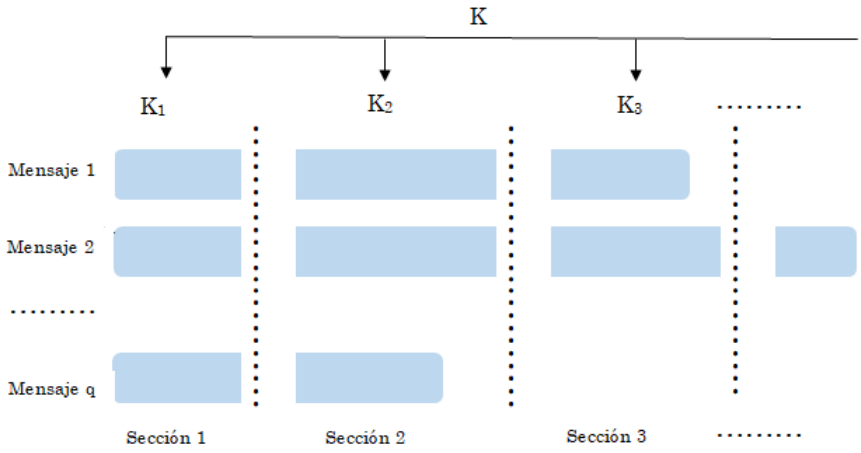

Fig. 3 - Esquema general del Mecanismo de cambio de llave interno.