Revista Cubana de Ciencias Informáticas
Vol. 17, No. 1, Mes Enero-Marzo, 2023
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 31-44

Tipo de artículo: Artículo originales
Temática: Matemática computacional
Recibido: 06/11/2022 | Aceptado: 18/12/2022 | Publicado: 29/01/2023

Criptoanálisis algebraico a los cifrados en bloques ligeros SIMON y SIMECK

Algebraic cryptanalysis of the lightweight block ciphers SIMON and SIMECK

Roberto Labrada Claro 0000-0002-5225-784X[1]
Miguel Angel Borges Trenard 0000-0001-7154-7730[2]
Mijail Borges Quintana 0000-0002-5656-0037[3*]

[1]Departamento de Matemática, Facultad de Ciencias Naturales y Exactas, Universidad de Oriente, Av. Patricio Lumumba s/n, Santiago de Cuba 90500, Cuba, evilrobertolc@gmail.com.
[2]Doctorate in Mathematics Education, Universidad Antonio Nariño, Bogotá 111321, Colombia, borgestrenard2014@gmail.com.
[3]Departamento de Matemática, Facultad de Ciencias Naturales y Exactas, Universidad de Oriente, Av. Patricio Lumumba s/n, Santiago de Cuba 90500, Cuba, mijail@uo.edu.cu.

*Autor para correspondencia: (mijail@uo.edu.cu)

RESUMEN

El campo de la Criptografía Ligera es relativamente nuevo, su esencia consiste en la necesidad de encontrar compromisos entre ligereza y seguridad. En este trabajo se realizó un estudio de SIMON y SIMECK, los cuales son cifrados en bloques ligeros. Se halló la modelación algebraica de estas importantes operaciones de cifrado y fueron programados y aplicados ataques algebraico sobre estos cifrados. Se comparan los resultados con los obtenidos por otros autores; llegando a conclusiones concernientes a las bases de Gröbner y los sistemas "SAT-solvers".

Palabras clave: criptografía ligera; criptoanálisis algebraico; sistemas "SAT-solvers".

Revista Cubana de Ciencias Informáticas
Vol. 17, No. 1, Mes Enero-Marzo, 2023
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 31-44

ABSTRACT

The field of Lightweight Cryptography is relatively new, its essence is the need to find compromises between lightness and security. In this work, a study of SIMON and SIMECK was carried out, which are lightweight blocks ciphers. The algebraic modeling of these important encryption operations was found and algebraic attacks on these encryptions were programmed and applied. The results are compared with those obtained by other authors; reaching conclusions concerning the Gröbner bases and "SAT-solvers" systems.

Keywords: lightweight cryptography; algebraic cryptanalysis; "SAT-solvers" systems.

Introducción

La Criptografía Ligera (Nayancy et al., 2022) es relativamente nueva, la misma se centra en buscar un compromiso entre ligereza y seguridad. Una interrogante que guía esta tendencia pudiese ser: ¿cómo se puede llegar a altos niveles de seguridad utilizando pequeñas potencias de cálculo? En años recientes han recibido considerable atención los denominados Cifrados en Bloques Ligeros (**CBL**) (Sehrawat and Gill, 2018). En comparación con los cifrados tradicionales, los **CBL** tienen dos propiedades principales:

1) Las aplicaciones sobre dispositivos restringidos no requieren como regla el cifrado de grandes masas de datos, por ello los **CBL** no necesitan tener gran capacidad para el procesamiento.

2) Los **CBL** son usualmente implementados a nivel de hardware, en particular en plataformas tales como microcontroladores de 8 bits.

Los diseñadores de cifrados ligeros tienen que atender la relación costo-seguridad-desempeño (Hatzivasilis et al., 2018). Para los cifrados en bloques ligeros la longitud de la clave del cifrado es la que genera la relación costo-seguridad, la cantidad de rondas del cifrado provee de la relación seguridad-desempeño y la arquitectura de hardware provee la relación costo-desempeño. Usualmente, dos de esas tres relaciones pudiesen ser optimizadas, siendo muy complejo optimizar las tres al mismo tiempo.
Siguiendo la anterior idea, la presentación pública en 2015 del trabajo de especialistas de la Agencia de Seguridad Nacional de los Estados Unidos (Beaulieu et al., 2015), sobre las Familias de Cifrados en Bloques Ligeros SIMON y SPECK, tuvo impacto en la comunidad científica criptográfica, por las características muy

buenas de los cifrados y también por el lugar y forma de procedencia de los mismos.

Aunque los cifrados en bloques ligeros se implementan sobre dispositivos restringidos (Kumar et al., 2021), no sucede lo mismo con los criptoanálisis que a ellos se les realizan. Diversos estudios se han realizado sobre criptoanálisis a cifrados en bloques ligeros, ver por ejemplo: (M.A. Borges-Trenard, 2017), en que se realiza un ataque algebraico a cinco rondas del cifrador en bloques SIMON, (AlKhzaimi and Lauridsen, 2013), donde se muestra que la versión más pequeña de SIMON exhibe un marcado efecto diferencial. En la mayoría de los casos, las observaciones presentadas no llevan abiertamente a un ataque, sino que proveen de bases para futuros análisis a las variantes de cifrados especificadas.

Como un muestra de que el estudio de éstos cifrados y en particular de las métodos de criptoanálisis continúa siendo un problema de interés, en (Abed et al., 2019) se realizan investigaciones para implementar y optimizar el cifrado SIMON en equipos de bajas prestaciones, en Yeo et al. (2021) se realiza un análisis mediante criptoanálisis algebraico a los cifrados SIMON y PRESENT, utilizando la idea de fijar algunos bits de la clave, en Dehnavi (2018) se muestra que con las investigaciones realizadas podría acelerarse el proceso de búsqueda de características lineales y diferenciales de las familias de cifrados de bloque SIMON y SPECK, y reducirse la complejidad de los ataques lineales y diferenciales contra estos cifrados. Por otra parte, en Leurent et al. (2021) los autores continúan profundizando en el fuerte efecto de agrupamiento para el criptoanálisis diferencial y lineal, debido a la existencia de muchos caminos con las mismas entradas y salidas.

Se hace entonces necesario la programación, comprensión y conocimientos sobre vulnerabilidades de este tipo de cifrados ante los ataques más conocidos, tanto de forma computacional, como en sus fundamentos matemáticos. En esa dirección se encuentra el propósito del presente trabajo, el cual resume una parte de la tesis de maestría (Claro, 2018).

Métodos o Metodología Computacional

Familia de Cifrados en Bloques Ligeros

Comprender el funcionamiento interno de los cifrados es el primer paso para encontrar debilidades o fortalezas en ellos, requisito indispensable al momento de ofrecer un criterio de seguridad y decidir qué cifrado usar y bajo cuáles condiciones. Por lo anterior, a continuación se describen las funciones de cifrado y descifrado de los algoritmos escogidos y algunas de sus propiedades, así como se discute sobre paquetes de cálculos para la ejecución de estos cifrados.

Revista Cubana de Ciencias Informáticas
Vol. 17, No. 1, Mes Enero-Marzo, 2023
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 31-44

Familia SIMON

SIMON (Beaulieu et al., 2015) es un cifrado liviano, diseñado por la Agencia de Seguridad Nacional de los Estados Unidos, publicado en el verano del 2013, puede ser implementado tanto en software como en hardware y posee un alto desempeño en una variedad de dispositivos. Para ser tan flexible como posible, sus diseñadores presentaron a la familia SIMON de 10 algoritmos, la cual consiste en una combinación de diferentes tamaños de bloques y claves.

Función de Ronda

SIMON pertenece a la familia de cifrados en bloques del tipo Feistel (Liu et al., 2021). El cifrado y descifrado se basan en las operaciones XOR, AND y la rotación circular $\lll j$ (rotar j bits a la izquierda). Para cada ronda (r_i), el esquema de Feistel opera con dos listas de n-bits, una izquierda (L_{i-1}) y otra derecha (R_{i-1}), creando el estado de ronda de $2n$-bits. La mitad izquierda pasa a través de una función en cada ronda:

$$f(L_{i-1}) = (L_{i-1} \lll 1)\&(L_{i-1} \lll 8) \oplus (L_{i-1} \lll 2),$$

donde & denota la operación AND y $\oplus$ denota a XOR. Luego, $f(L_{i-1})$ se suma a la otra mitad R_{i-1} y a la clave de ronda K_i

$$L_i = f(L_{i-1}) \oplus R_{i-1} \oplus K_i,$$

para crear la nueva parte izquierda L_i y definir la nueva mitad derecha como $R_i = L_{i-1}$.

Generación de las claves de ronda

La función de generación de las claves de ronda es similar a la función de ronda; utiliza las operaciones XOR y la rotación circular, solo que ahora es hacia la derecha, $\ggg j$ (rotar j veces a la derecha). Para evitar propiedades lineales y simetrías en las rotaciones circulares, se agrega a la generación de las claves una sucesión de constantes de rondas z_j. Una constante c también se suma junto con z_j, donde $c = (2n-4)$. Dependiendo del número $m = 2,3,4$, escogido para la entrada, la generación de las claves será: $k_{i+m} =$

$$\begin{aligned} c \oplus (z_j)_i \oplus k_i (I \oplus (\ggg 1))(\ggg 3) k_{i+1}, \text{ si } m = 2, \\ c \oplus (z_j)_i \oplus k_i (I \oplus (\ggg 1))(\ggg 3) k_{i+2}, \text{ si } m = 3, \\ c \oplus (z_j)_i \oplus k_i (I \oplus (\ggg 1))(\ggg 3) k_{i+3} \oplus k_{i+1}, \text{ si } m = 4. \end{aligned} \quad (1)$$

Revista Cubana de Ciencias Informáticas
Vol. 17, No. 1, Mes Enero-Marzo, 2023
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 31-44

para $0 \leq i < T - m$, donde T es el número de rondas.

La creación de la clave para $m = 4$ se representa en la Figura 1.

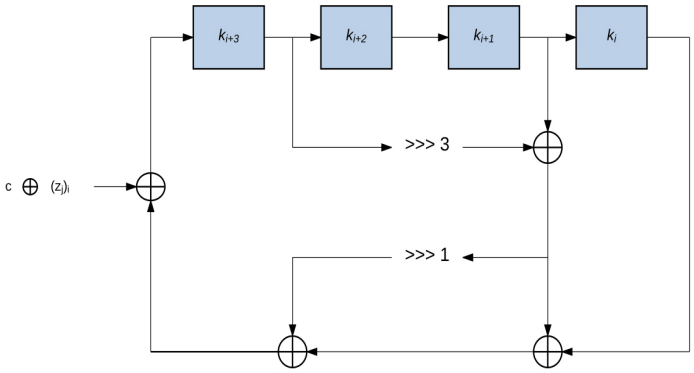

Fig. 1 - Creación de las claves del cifrado SIMON para $m = 4$.

Familia SIMECK

En (Yang et al., 2015) se presenta una nueva Familia de cifrados en bloques ligeros llamada SIMECK; los autores argumentan que la nueva familia se constituye de cifrados ligeros que combinan los buenos componentes de diseño de SIMON y SPECK y da lugar a cifrados en bloques más compactos, eficientes y resistentes; aun tras diferentes tipos de ataque, tal como se puede apreciar en (Sadeghi and Bagheri, 2019) y (Li et al., 2019).

SIMECK (Yang et al., 2015) está diseñado para dejar huellas extremadamente pequeñas en su implementación en hardware y para ser compacto en su implementación en software. La función de ronda y el algoritmo generador de la clave siguen una estructura de Red de Feistel.

La familia SIMECK se compone de tres cifrados que se denotan por SIMECK$2n/mn$, donde $2n$ es la longitud de bloque y mn es la longitud de la clave; n toma valores de 16, 24 ó 32. El objetivo de tener tres opciones para las longitudes es satisfacer los requisitos de diferentes sistemas.

Función de Ronda

Revista Cubana de Ciencias Informáticas
Vol. 17, No. 1, Mes Enero-Marzo, 2023
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 31-44

Para cifrar un bloque de $2n$ bits, primero se divide éste en dos partes de n bits, l_0 y r_0, donde l_0 contiene los primeros n bits más significativos y r_0 contiene los restantes n bits. Estas dos mitades son procesadas por la función de ronda del SIMECK para ciertos números de rondas T, entonces finalmente se concatenan las salidas l_T y r_T y así se logra el texto cifrado. El número de rondas T para SIMECK32/64, SIMECK48/96 y SIMECK64/128 es 32, 36, y 44, respectivamente.

La función de ronda para la i-ésima ronda queda definida de la siguiente forma:

$$R_{k_i}(l_i, r_i) = (r_i \oplus f(l_i) \oplus k_i, l_i),$$

donde l_i y r_i son las dos mitades del estado, k_i es la clave de ronda y la función f se define como

$$f(x) = (x \,\&\, (x \lll 5)) \oplus (x \lll 1),$$

donde & denota la operación AND y $x \lll i$ es la rotación circular de x hacia la izquierda i veces.

Generación de las claves de ronda

Para generar la clave de ronda k_i partiendo de la clave principal de entrada K, ésta se segmenta en 4 partes de igual longitud y se declaran como los estados iniciales de la clave (t_2, t_1, t_0, k_0), los mismos se dan como entrada al registro de desplazamiento con retroalimentación mostrado en la Figura 2.

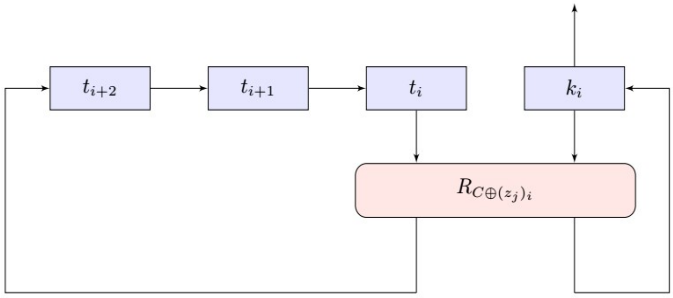

Fig. 2 - Generación de las claves de ronda del cifrador en bloques SIMECK.

Los n bits menos significativos de K son colocados en el estado inicial k_0, mientras que los n más significativos

Revista Cubana de Ciencias Informáticas
Vol. 17, No. 1, Mes Enero-Marzo, 2023
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 31-44

en t_2. Para actualizar el registro y generar las claves de ronda se utiliza nuevamente la función de ronda, se le agrega además una constante de ronda $C \oplus (z_j)_i$. La operación de actualización puede ser expresada como:

$$\begin{cases} k_{i+1} = t_i, \\ t_{i+3} = k_i \oplus f(t_i) \oplus C \oplus (z_j)_i, \end{cases} \tag{2}$$

donde $0 \leq i \leq T-1$. El valor de la constante C está definido por $C = 2^n - 4$ y $(z_j)_i$ denota el i-ésimo bit de la sucesión z_j. Entonces k_i es usado como la clave de ronda de la i-ésima ronda.

Resultados y discusión

Modelación algebraica de 5 rondas del SIMON

En (Astrid, 2016) se obtiene una representación de las transformaciones del cifrado, como un sistema de ecuaciones polinómicas en varias variables, reducido a 5 rondas del SIMON32. Interpretando el algoritmo y reordenando las ecuaciones de forma tal que las variables desconocidas se encuentren en el miembro izquierdo y sustituyendo la variable desconocida x_3 por el valor conocido C_R, el sistema de ecuaciones quedaría expresado como sigue:

$$x_0 \oplus k_1 = f(P_L) \oplus P_R, \tag{3}$$
$$x_1 \oplus f(x_0) \oplus k_2 = P_L, \tag{4}$$
$$x_2 \oplus f(x_1) \oplus x_0 \oplus k_3 = 0, \tag{5}$$
$$f(x_2) \oplus x_1 \oplus k_4 = C_R, \tag{6}$$
$$x_2 \oplus k_5 = f(C_R) \oplus C_L, \tag{7}$$
$$k_5 \oplus k_1 \oplus k_2 \oplus (k_4 \ggg 3) \oplus (k_2 \ggg 1) \oplus (k_4 \ggg 4) = D. \tag{8}$$

donde (P_L, P_R) y (C_L, C_R) son los lados izquierdo y derecho de los textos claros y cifrado respectivamente, k_i es la i-ésima clave de ronda, x_{i-1} es la parte izquierda de la salida después de la ronda $i-1$, y D es una constante conocida, que es la que permite generar cada clave k_{i+m} a partir de las siguientes, según las ecuaciones (1).

Revista Cubana de Ciencias Informáticas
Vol. 17, No. 1, Mes Enero-Marzo, 2023
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 31-44

Para un par o dos pares de texto claro y cifrado, la cantidad de incógnitas supera a la cantidad de ecuaciones, a partir de 3 pares, se observa una tendencia a que el número de ecuaciones es superior al de incógnitas, que es justo lo que se recomienda, tanto para la unicidad de la solución, como para la posibilidad de resolverlo. El siguiente paso es transformar las 5 ecuaciones vectoriales a sus respectivas representaciones por componentes.

Ataque

Para calcular la solución de los sistemas, se utilizó el paquete de bases de Gröbner que posee el sistema de cálculo simbólico MAPLE (Versión 18). Todos los cálculos realizados se llevaron a cabo en un computador con un procesador Intel Core i7-4790, a 3.6 GHz, con 16 GB de RAM. Para realizar los experimentos se tomó en cada intento una clave y los respectivos textos claros de forma aleatoria, realizándose 100 intentos por cada experimento, el tiempo resultante mostrado en las Tablas denota el promedio de tiempo de los ataques. Las opciones en la columna de resultados son S (cuando se obtuvo éxito, es decir, se obtuvo la clave) y N cuando no se pudo obtener, que los recursos del computador no fueron suficientes para realizar los cálculos.

Para cada par en cuestión, se obtuvieron las ecuaciones de ronda correspondientes. Luego de alcanzado el sistema polinómico, se creó el álgebra de polinomios junto con las ecuaciones del campo, para garantizar que las soluciones se mantuviesen en el campo de trabajo y no en alguna extensión del mismo. Los resultados se listan a continuación (ver página siguiente).

Tabla 1 - Resultados del criptoanálisis algebraico al SIMON32/64.

Rondas	Pares	Tiempo(s)	Resultado
5	1	32752.425	N
5	2	1059.797	S
5	3	2.687	S
6	3	13.000	S
7	3	27290.922	N
7	4	24350.594	N
7	5	31623.891	N
7	6	$1{,}94481172 * 10^5$	N

Revista Cubana de Ciencias Informáticas
Vol. 17, No. 1, Mes Enero-Marzo, 2023
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 31-44

Modelación algebraica de 5 rondas del SIMECK

Teniendo en cuenta la similitud entre el proceder del cifrado SIMECK y la de SIMON y la similitud entre las primitivas de ambos cifrados; surge entonces de forma natural la interrogante siguiente: dada las pocas diferencias de los algoritmos y teniendo en cuenta el ataque algebraico ya realizado sobre el SIMON, ¿el cifrado SIMECK ofrece mayor o menor resistencia que el cifrado SIMON?

Con el objetivo de responder tal interrogante, para hacerle un ataque al cifrado SIMECK y poder realizar comparaciones, se decidió proceder de la misma forma para realizar el criptoanálisis algebraico. Utilizando el mismo método, se logró obtener una representación de las transformaciones del cifrado como un sistema de ecuaciones polinómicas en varias variables.

Ataque

Para cada par en cuestión, se obtuvieron las ecuaciones de ronda correspondientes, luego de alcanzado el sistema polinómico, se creó el álgebra de polinomios junto con las ecuaciones del campo, para garantizar que las soluciones se mantuviesen en el campo de trabajo y no en alguna extensión del mismo. Los resultados se listan en la Tabla 2.

Tabla 2 - Resultados del criptoanálisis algebraico al SIMECK32/64.

Rondas	Pares	Tiempo(s)	Resultado
5	1	23949.844	N
5	2	1606.359	S
5	3	2.903	S
6	3	17651.625	S
6	4	408.266	S
7	3	11697.141	N
7	4	15716.469	N
7	5	19288.454	N
7	6	33762.937	N

Revista Cubana de Ciencias Informáticas
Vol. 17, No. 1, Mes Enero-Marzo, 2023
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 31-44

Resumen y contraste de los ataques

SIMON

Desde la vista a luz pública del cifrado SIMON, varios artículos han intentado atacarlo, véase por ejemplo (Zhang et al., 2022), (Rohit and Gong, 2018) o (Astrid, 2016); donde se realiza un ataque algebraico a texto claro conocido de una versión reducida del SIMON, utilizando un software del tipo "SAT-solver" (Gomes et al., 2008). El ataque al SIMON en (Astrid, 2016) se realizó en un computador con procesador Intel Core i7 2.70 GHz, con 16 GB de RAM, y fue implementado con el SAT-solver CryptoMiniSat2. Ellos atacaron 5 y 6 rondas del cifrado logrando:

- 5 rondas del SIMON32/64, con tres pares de texto claro y sus respectivos textos cifrados, el tiempo de ejecución fue de un promedio de 3.75s, logrando obtener la clave.
- 6 rondas del SIMON32/64, con tres pares de texto claro y sus respectivos textos cifrados, el tiempo de ejecución fue de un promedio de 290.7s, logrando obtener la clave.
- Para dos pares, según afirman los autores, se obtenían sistemas que no tenían solución única.

Otro objetivo que llevó a experimentar con el SIMON vino directamente de lo comentado en el párrafo anterior, ya que surgió la siguiente interrogante: entre el empleo de SAT-solver o el cálculo mediante Bases de Gröbner (Bečejac and Stefanov, 2020), ¿con cual método de solución de sistemas de ecuaciones polinómicas se obtiene mejor resultado? En tal sentido, se pudo apreciar que se mejoró el tiempo de búsqueda de la clave logrado en (Astrid, 2016), lográndose incluso calcular la clave con sólo 2 pares, lo cual no se obtuvo en (Astrid, 2016); en general, el resultado con las bases de Gröbner en MAPLE fue mejor que con los sistemas SAT-solvers utilizados en (Astrid, 2016).

SIMECK

El cifrado SIMECK es un derivado de los cifrados SIMON y SPECK (Beaulieu et al., 2015), el cual según los autores, "ha tomado de cada uno lo mejor para constituir un cifrado más seguro y más eficiente". Resultó entonces interesante ver cómo se comportaban ambos cifrados bajo el mismo ataque. La conclusión que

se obtuvo fue que, para cada experimento, el tiempo que demoró calcular la clave del cifrado SIMECK se mantuvo siempre por encima del tiempo que demoró hallar la clave del SIMON, que era lo esperado.

Conclusiones

Los resultados descritos en este trabajo muestran un estudio de los cifrados pertenecientes a la Familia de Cifrados en Bloques Ligeros y una valoración sobre su resistencia al criptoanálisis algebraico. Se estudió con detalle el modo de operar de las funciones de cifrado y descifrado de los algoritmos escogidos, así como algunas propiedades que poseen. También se programaron paquetes de cálculo para el cifrado y descifrado de los principales miembros de estas familias.

Se halló la modelación algebraica de importantes operaciones de cifrado y fueron programadas algunas técnicas para el criptoanálisis algebraico. Estas técnicas se aplicaron a los cifrados SIMON y SIMECK.

Como resultado directo de las experimentaciones, se llegó a la conclusión que en general, el resultado con las bases de Gröbner en MAPLE fue mejor que con los sistemas "SAT-solvers", utilizados en (Astrid, 2016), lo que constituye una alternativa al ataque antes mencionado.

Referencias

Sa'ed Abed, Reem Jaffal, Bassam Jamil Mohd, and Mohammad Alshayeji. Fpga modeling and optimization of a simon lightweight block cipher. *Sensors*, 19(4):913, 2019.

Hoda AlKhzaimi and Martin M Lauridsen. Cryptanalysis of the simon family of block ciphers. *IACR Cryptology ePrint Archive*, 2013:543, 2013.

Berghult Astrid. A practical comparison between algebraic and statistical attacks on the lightweight cipher simon, 2016.

Ray Beaulieu, Stefan Treatman-Clark, Douglas Shors, Bryan Weeks, Jason Smith, and Louis Wingers. The simon and speck lightweight block ciphers. In *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, pages 1–6. IEEE, 2015.

Vladimir Bečejac and Predrag Stefanov. Groebner bases algorithm for optimal pmu placement. *International Journal of Electrical Power & Energy Systems*, 115:105427, 2020.

R. Labrada Claro. Criptoanálisis algebraico a cifrados en bloques ligeros. Tesis en opción al título de Máster en Matemática. Universidad de La Habana, Cuba, 2018.

Seyed Mojtaba Dehnavi. Further observations on simon and speck block cipher families. *Cryptography*, 3(1): 1, 2018.

Carla P Gomes, Henry Kautz, Ashish Sabharwal, and Bart Selman. Satisfiability solvers. *Foundations of Artificial Intelligence*, 3:89–134, 2008.

George Hatzivasilis, Konstantinos Fysarakis, Ioannis Papaefstathiou, and Charalampos Manifavas. A review of lightweight block ciphers. *Journal of cryptographic Engineering*, 8(2):141–184, 2018.

K Kranthi Kumar, B Srikanth, Y Kasiviswanadham, Ch DV Subbarao, DNVSLS Indira, and NL Pratap. The importance of light-weight encryption cipher in restricted iot systems to make intelligent technology safer for devices. *Applied Nanoscience*, pages 1–11, 2021.

Gaëtan Leurent, Clara Pernot, and André Schrottenloher. Clustering effect in simon and simeck. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 272–302. Springer, 2021.

Hang Li, Jiongjiong Ren, and Shaozhen Chen. Improved integral attack on reduced-round simeck. *IEEE Access*, 7:118806–118814, 2019.

Jiajie Liu, Bing Sun, and Chao Li. New approach towards generalizing feistel networks and its provable security. *Security and Communication Networks*, 2021, 2021.

R. Labrada-Claro M.A. Borges-Trenard. Ataque algebraico a cinco rondas del cifrado en bloques simon. Congreso Internacional Compumat. La Habana, Cuba, 2017.

Nayancy, Sandip Dutta, and Soubhik Chakraborty. A survey on implementation of lightweight block ciphers for resource constraints devices. *Journal of Discrete Mathematical Sciences and Cryptography*, 25(5): 1377–1398, 2022.

Raghvendra Rohit and Guang Gong. Correlated sequence attack on reduced-round simon-32/64 and simeck-32/64. *Cryptology ePrint Archive*, 2018.

Sadegh Sadeghi and Nasour Bagheri. Security analysis of simeck block cipher against related-key impossible differential. *Information Processing Letters*, 147:14–21, 2019.

Deepti Sehrawat and Nasib Singh Gill. Lightweight block ciphers for iot based applications: a review. *International Journal of Applied Engineering Research*, 13(5):2258–2270, 2018.

Gangqiang Yang, Bo Zhu, Valentin Suder, Mark D Aagaard, and Guang Gong. The simeck family of lightweight block ciphers. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 307–329. Springer, 2015.

Sze Ling Yeo, Duc-Phong Le, and Khoongming Khoo. Improved algebraic attacks on lightweight block ciphers. *Journal of Cryptographic Engineering*, 11(1):1–19, 2021.

Jinbao Zhang, Jiehua Wang, Ge Bin, and Jianhua Li. An efficient differential fault attack against simon key schedule. *Journal of Information Security and Applications*, 66:103155, 2022.

Conflicto de interés

Los autores autorizan la distribución y uso de su artículo.

Contribuciones de los autores

1. Conceptualización: Miguel Angel Borges Trenard, Roberto Labrada Claro, Mijail Borges Quintana
2. Curación de datos: Roberto Labrada Claro, Miguel Angel Borges Trenard
3. Análisis formal: Miguel Angel Borges Trenard, Mijail Borges Quintana
4. Adquisición de fondos:
5. Investigación: Miguel Angel Borges Trenard, Roberto Labrada Claro, Mijail Borges Quintana
6. Metodología: Miguel Angel Borges Trenard, Mijail Borges Quintana
7. Administración del proyecto: Mijail Borges Quintana

8. Recursos:
9. Software: Roberto Labrada Claro, Miguel Angel Borges Trenard
10. Supervisión: Mijail Borges Quintana, Miguel Angel Borges Trenard
11. Validación: Miguel Angel Borges Trenard, Mijail Borges Quintana
12. Visualización: Roberto Labrada Claro, Miguel Angel Borges Trenard, Mijail Borges Quintana
13. Redacción - borrador original: Roberto Labrada Claro, Miguel Angel Borges Trenard
14. Redacción - revisión y edición: Mijail Borges Quintana, Miguel Angel Borges Trenard

Financiación

La investigación que da origen a los resultados presentados en la presente publicación recibió fondos de la Oficina de Gestión de Fondos y Proyectos Internacionales bajo el código PN223LH006-015; así como de la Red CYTED “NUEVAS HERRAMIENTAS CRIPTOGRÁFICAS PARA LA E-COMUNIDAD”.