# Secuencias Seudoaleatorias para Criptología

Antonio Castro Lechtaler[1,2]; Marcelo Cipriano[1]; Edith García[1]; Julio Liporace[1]
Ariel Maiorano[1], Eduardo Malvacio[1], Néstor Tapia[1], Dulio, Nicolás[1]; Pérez, Pablo[1]

[1]Laboratorio de Investigación en Técnicas Criptográficas y Seguridad Teleinformática.
Escuela Superior Técnica, Facultad de Ingeniería. Instituto Universitario del Ejército.
[2] UNdeC Universidad Nacional de Chilecito.

acastro@est.iue.edu.ar; marcelocipriano@est.iue.edu.ar, editxgarcía@gmail.com,
maiorano@gmail.com, edumalvacio@gmail.com, tapianestor87@gmail.com
nico_n44@hotmail.com; pablo_1711_pap@hotmail.com

## 1. Resumen.

Esta línea de investigación busca la resolución de problemas abiertos acerca de la complejidad lineal y período de las secuencias binarias seudoaleatorias.

Las mismas pueden ser generadas, por ejemplo, por Registros de Desplazamientos Realimentados No Linealmente (NLFSR: Non-Linear Feedback Shift Registers). En particular los algoritmos Trivium [1, 2] y Trivium Toy[3].

El algoritmo Trivium ha conformado el portfolio final del concurso europeo e-Stream del año 2005 [4].

A la fecha, no se conocen ataques efectivos contra este generador [5, 6, 7].

El estudio de las propiedades de las secuencias seudoaleatorias en general puede extenderse a cualquier algoritmo, por ejemplo la familia A5 -empleados en telefonía celular-, los Generadores Controlados por Reloj (Clock-Controlled Generators) u otros.

El objetivo es lograr un estudio completo de los fundamentos matemáticos involucrados. Así poder medir la robustez criptológica de los generadores de secuencias seudoaleatorias.

La teoría de los campos finitos y los registros de Desplazamientos Lineales (LFSRs) y No Lineales (NLSFR) [8] ofrecen las herramientas matemáticas para abordar las problemáticas involucradas.

**Palabras Claves:**

Randon Sequences. Stream Ciphers. LFRS. NLFSR.

## 2. Contexto.

El CRIPTOLAB (Laboratorio de Investigación en Técnicas Criptográficas y Seguridad Teleinformática) pertenece a la Escuela Superior Técnica "Gral. Div. Manuel N. Savio" (EST), Facultad del Ejército, Universidad Nacional de la Defensa (UNDEF) en el área de la carrera de grado de Ingeniería en Informática y el posgrado en Criptografía y Seguridad Informática que se dictan en esta institución.

El desarrollo científico y tecnológico es relevante a nivel estratégico y es por ello que tanto las Fuerzas Armadas en general como el Ejército en particular destina recursos de investigación para cumplir con tal fin.

Resultados parciales de esta investigación han sido presentados en CACIC 2013 [3] y CACIC 2014[9], siendo ambas presen-

taciones premiadas como “mejor exposición” del Workshop de Seguridad Informática.

Asimismo dicho trabajo ha sido seleccionado entre los mejores del mencionado congreso y hemos sido invitados a incluirlo en el número regular del Journal of Computer Science and Technology [10].

Además hemos podido dar entidad propia a esta línea de investigación al poder incluirla dentro de los proyectos de la EST – IUE bajo el nombre de Stream Cipher: Estudio de las propiedades y vulnerabilidades de generadores seudoaleatorios de la familia Trivium.

## 3. Introducción.

Los generadores lineales del tipo Linear Feedback Shift Register (LFSR) generan secuencias pseudo-aleatorias con período y complejidad lineal controladas. Su estudio comenzó alrededor de los años `60 [11, 12].

Dada su naturaleza lineal, los LFSRs resultan ser inseguros: cuando 2n bits consecutivos (siendo n la longitud del registro) de la secuencia de salida de un LFSR son conocidos, toda la sucesión resulta ser predecible. Sistemas basados en LFSRs intentan agregar complejidad linealidad combinando, entre otras cosas, sus salidas a través de una función no lineal. Esto tampoco ofrece la seguridad deseada.

Los NLFSRs (una generalización de los LFSRs) estuvieron por mucho tiempo postergados en la comunidad criptológica. Su estudio se revitalizó con el advenimiento de la llamada “Criptografía Liviana”. La misma puede ejecutarse sobre plataformas de poco poder de cálculo. Incluso una cantidad de nuevos dispositivos tales como marcapasos, procesadores centrales montados en autos, grúas, tractores y cosechadoras de alto desempeño, entre otros.

La revitalización del estudio de los NLFSRs ha comenzado a aparecer literatura. Tal es el caso de la familia TRIVIUM (De Cannière-Preneel), BIVIUM, CUADRIVIUM, entre otros.

## 4. Líneas de Investigación, Desarrollo e Innovación

Inicialmente el estudio del algoritmo Trivium y el Trivium Toy [13] llevó los investigadores a desarrollar herramientas propias e implementar otras reconocidas por la comunidad científica, desde los fundacionales test de Golomb hasta las baterías de test del NIST, “DieHard”[1] y “DieHarder”[2].

Estas herramientas permiten abordar los problemas de la complejidad lineal, la búsqueda del período y demás propiedades criptológicas que se desean conocer de una determinada secuencia seudoaleatoria.

El CriptoLab podría analizar las propiedades criptológicas de secuencias de números generado por un modelo basado en álgebras no conmutativas. En particular el esquema que utiliza como elementos de la estructura algebraica a los Cuaterniones de Hamilton [14].

## 5. Resultados y Objetivos.

Se espera poder analizar y evaluar las características y propiedades criptológicas de enormes secuencias de números.

## 6. Formación de Recursos Humanos.

Además de los investigadores que forman parte del staff fijo del laboratorio, el

[1] http://stat.fsu.edu/pub/diehard/

[2] http://www.phy.duke.edu/~rgb/General/dieharder.php

equipo de investigación cuenta con la participación de 2 estudiantes del posgrado en Criptografía y Seguridad Teleinformática. Los mismos están realizando sus Trabajos Finales de Integración (tesina de posgrado) en temas afines a esta línea de investigación, en la cual colaboran.

Durante el año 2015 se han sumado al proyecto dos alumnos de 4to año de la carrera de Ingeniería Informática. Uno de ellos es Pablo Pérez como alumno ayudante y Nicolás Dulio que ha recibido la beca Estímulo a las Vocaciones Científicas, perteneciente al Programa Estratégico de Investigación y Desarrollo, Plan de Fortalecimiento (Componente de Formación de Recursos Humanos) del Consejo Interuniversitario Nacional.

## 7.Referencias y Bibliografía


[1] De Canniére, C. and Preneel, B. "TRIVIUM A Stream Cipher Construction Inspired by Block Cipher Design Principles". In Workshop on Stream Ciphers Revisited (SASC2006), 2006.

[2] De Canniére, C. and Preneel, B. "TRIVIUM Specifications". eSTREAM, ECRYPT Stream Cipher Project, Report. 2008.

[3] Castro Lechtaler, A.; Cipriano, M.; García, E.; Liporace, J.; Maiorano, A.; Malvacio, E. "Model Design for a Reduced Variant of a Trivium Type Stream Cipher". XIX Congreso Argentino de Ciencias de la Computación, Mar del Plata, Buenos Aires. 2013.

[4] eSTREAM: eSTREAM – The ECRYPT Stream Cipher Project: http://www.ecrypt.eu.org/stream/

[5] McDonald, C. and Pieprzyk, C. "Attacking Bivium with MiniSat", Cryptology ePrint Archive, Report 2007/040, 2007.

[6] Raddum, H."Cryptanalytic Results on Trivium", eSTREAM, ECRYPT Stream Cipher Project, Report 2006/039, 2006.

[7] Maximov, A. and Biryukov, A. "Two Trivial Attacks on Trivium", Selected Areas in Cryptography, Lecture Notes in Computer Science, Vol.4876, Springer, 2007.

[8] Dubrova, E. "A List of Maximum-Period NLFSRs", Cryptology ePrint Archive, Report 2012/166, March 2012, http://eprint.iacr.org/2012/166

[9] Castro Lechtaler, A.; Cipriano, M.; García, E.; Liporace, J.; Maiorano, A.; Malvacio, E., Tapia, N., "Trivium Vs. Trivium Toy". XX Congreso Argentino de Ciencias de la Computación, Octubre 2014. Universidad Nacional de La Matanza, San Justo, Buenos Aires.

[10] Castro Lechtaler, Antonio; Cipriano, Marcelo; García, Edith; Liporace, Julio; Maiorano, Ariel; Malvacio, Eduardo. "Model design for a reduced variant of a Trivium Type Stream Cipher." Journal of Computer Science and Technology Vol. 14, No. 1, Abril 2014.

[11] Golomb. "Shift Register Sequences". Aegean Park Press, 1982.

[12] Massey, J.L. "Shift-register synthesis and BCH decoding". IEEE Transactions on Information Theory 15, 1969.

[13] Castro Lechtaler, A.; Cipriano, M.; García, E.; Liporace, J.; Maiorano, A.; Malvacio, E., Tapia, N., "On the Interleaving Process Applied to the Trivium Algorithm". II Congreso Nacional de Ingenieria Informática/Ingeniería de Sistemas (CoNaIISI), Noviembre 2014. Universidad Nacional de San Luis, San Luis.

[14] Kamlofsky, J; Hecht, J; Hidalgo Izzi, O; Abdel Masih, S. "A Diffie-Hellman Compact Model Over Non-Commutative Rings Using Quaternions", VIII CIBSI-TIBETS, Ecuador, 2015.