Período y Longitud de Recursión de los algoritmos Trivium y Trivium Toy.

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

1. Resumen.

Esta línea de investigación busca la resolución de problemas abiertos que el algoritmo Trivium aún posee. En particular, la longitud de recursión (complejidad lineal) y período de las secuencias binarias generadas por los algoritmos Trivium [1, 2] y Trivium Toy[3], incluídos éstos dentro de la teoría de Registros Desplazables No Lineales (NLSFRs).

El objetivo es lograr un estudio completo de los fundamentos matemáticos involucrados, para de ésta manera poder medir su robustez criptológica como generadores de secuencias seudoaleatorias.

El algoritmo Trivium ha resultado ser finalista en el concurso europeo e-Stream del año 2005 [4]. Al día de hoy, al aplicarle diferentes técnicas de criptoanálisis no se conocen ataques efectivos contra este generador [5, 6, 7].

En el año 2012 la International Organization for Standardization (ISO) y la International Electrotechnical Commission (IEC) han publicado la norma *ISO*/IEC *29192-3*:2012. En ella se especifican dos algoritmos de cifrado de flujo para ser utilizados en criptografía liviana: el Enocoro y el Trivium.

En el caso del Trivium quedan por resolver aún algunos problemas abiertos: no se conoce la forma de determinar la longitud de recursión de las secuencias seudoaleatorias que genera tampoco su período, se desconoce la existencia de ciclos cortos y cuáles son los estados iniciales que los generan (claves débiles).

Por ello, nos hemos planteamos realizar estos estudios desde la teoría de los campos finitos y los registros de Desplazamientos Lineales (LFSRs) y No Lineales (NLSFRs) [8].

Palabras Claves:

Randon Sequences. Stream Ciphers. Trivium. Trivium Toy. LFRS. NLFSR.

2. Contexto.

El Laboratorio de Investigación en Técnicas Criptográficas y Seguridad Teleinformática (CRIPTOLAB) pertenece a la Escuela Superior Técnica “Gral. Div. Manuel N. Savio” (EST), Facultad de Ingeniería, del Instituto Universitario del Ejército Argentino (IUE) en el área del Posgrado en Criptografía y Seguridad Informática que se dicta en esta institución, junto a otros posgrados y carreras de grado en ingeniería.

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 presentaciones 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.

Hoy en día es ampliamente conocido el uso de Linear Feedback Shift Register (LFSR) para generar secuencias pseudoaleatorias con período y complejidad lineal controladas. Aunque el estudio de los LFSRs comenzó alrededor de los años `60 [11, 12] y continuó durante mucho tiempo.

Sin embargo, debido a su naturaleza lineal, los LFSRs resultan ser por sí sólo inseguros: es sabido que cuando 2n bits (consecutivos) de la secuencia de salida de un LFSR es conocida, toda la sucesión resulta ser totalmente predecible. Asimismo, diseños de sistemas basados en LFSRs intentan agregar no linealidad combinando entre otras cosas sus salidas a través de una función no lineal, sin embargo esto tampoco ofrece la seguridad deseada.

Los Nonlinear Feedback Shift Register (NLFSs), una generalización de los anteriores, resultaron estar por mucho tiempo postergados. Sin embargo se revitalizó su estudio con el advenimiento de la llamada "Criptografía Liviana": la criptografía que puede ser montada sobre plataformas de poco poder de cálculo como una tablet o un teléfono inteligente. Pero también en una cantidad de otros dispositivos tales como marcapasos, procesadores centrales montados en autos de alta gama, grúas, tractores y cosechadoras de alto desempeño, entre otros.

En los últimos años ha comenzado a aparecer literatura en torno a estos registros no lineales. Tal es el caso de la familia TRIVIUM (De Cannière-Preneel), BIVIUM, CUADRIVIUM.

Nuestro modelo propuesto Trivium Toy consiste en un Registro de Desplazamiento Retroalimentado no Linealmente (NLFSR). Consta de tres registros desplazables no lineales de longitudes 31, 28 y 37, es decir un total de 96 bits, con una clave de 31 bits y un vector de inicialización de al menos 28 bits, obteniendo una cantidad de claves y vectores para su uso de 2^{59} bits. Creado en nuestro laboratorio a los efectos de poder reducir el campo de trabajo para hallar la longitud de recursión, período y poder también generalizar los resultados de dicha investigación a la familia del algoritmo Trivium.

4. Líneas de Investigación, Desarrollo e Innovación

Se busca resolver los problemas abiertos que el Trivium aún posee. Por ejemplo:

- su longitud de recursión.

- su período.

- la existencia o no de estados iniciales que generen secuencias seudoaleatorias cortas, inseguros para usos criptológicos.

- la posibilidad de extender de los resultados anteriores al resto de la familia de algoritmos que comparten la misma filosofía de construcción (univim, bivium, trívium, cuatrivium, etc.)

- la existencia de propiedades matemáticas que permitan la personalización de este algoritmo, sin disminución por ello de la seguridad criptológica.

5. Resultados y Objetivos.

Se ha podido reducir la estructura del Trivium obteniendo el llamado Trivium Toy, respetando la filosofía de contrucción y sin disminuir sensiblemente la fortaleza del mismo.

Se ha comprobado empíricamente que las secuencias seudoaleatorias que genera el Trivium Toy pasa los test de seudoleatoriedad aceptados por la comunidad científica: los test del NIST, la batería de test "Die Hard" y "Die Hardest".

Se ha llevado adelante una comparación del rendimiento de los algoritmos a través del estudio de la velocidad en el proceso de generación de secuencias cifrantes. Para ello cada algoritmo generó una secuencia seudoaleatoria de igual longitud. El Toy resultó significativamente más veloz que el Trivium original. Precisamente alrededor de tres veces más veloz.

Considerando el modelo lineal de los algoritmos, se han factorizado ambos polinomios asociados. Se han computado la cantidad de secuencias con ciclo corto que cada algoritmo genera y la longitud de recursión de las mismas.

También se ha comprobado que, en los modelos lineales que le dan sustento a los no lineales, el proceso de *interleave* involucrado no aporta mayor seguridad al algoritmo al no aumenta significativamente la complejidad lineal de la secuencias obtenidas[13].

Se lleva adelante el análisis matemático de los polinomios asociados al Trivium y al Trivium Toy.

También se están estudiando otras propiedades de los polinomios de manera que se puedan observar otras carácterísticas de los mismos que permitan por ejemplo, la posibilidad de personalizar o no estos criptosistemas.

Se han montado estos algoritmos en hardware, lo que permitirá evaluar su performance en un sistema genérico de compuertas programables. Así se podrán montar estos generadores en diversos dispositivos móviles con requerimientos de comunicaciones cifradas.

6. Formación de Recursos Humanos.

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

Asimismo 2 estudiantes de grado de la carrera de Ingeniería en Informática realizaron la Práctica Profesional Supervisada el Proyecto Final de Carrera (tesina de grado) alineados también con estos temas.

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.