Análisis y estudio del período de recursión de los algoritmos Trivium y Trivium Toy.

Ing. Antonio Castro Lechtaler[1,2] Msc.
Esp. Marcelo Cipriano[1], Lic. Edith García[1],Lic. Julio Liporace[1]
Lic. Ariel Maiorano[1], Eduardo Malvacio[1]

[1]Laboratorio de Investigación en Técnicas Criptográficas y Seguridad Teleinformática.
Escuela Superior Técnica, Facultad de Ingeniería. Instituto Universitario del Ejército.
[2] F.C.E. Universidad de Buenos Aires.

acastro@iese.edu.ar
marcelocipriano@iese.edu.ar
edumalvacio@gmail.com

1. Resumen.

Esta línea de investigación persigue el análisis y estudio del período de recursión de los algoritmos Trivium [1,2] y Trivium Toy[3]- ambos pertenecientes a los Registros No lineales de Desplazamiento (NLSFR)- para lograr la completa fundamentación matemática de su robustez criptológica como generadores de secuencias seudoaleatorias.

.

El uso del correo electrónico, home banking, redes sociales, la amplia difusión de la telefonía móvil y el acceso a redes de computadoras de manera inalámbrica han aumentado los requerimientos de confidencialidad de la información dado que la transmisión se realiza por canales inseguros.

Algunos esquemas de cifrado/descifrado, aunque provean la seguridad requerida para dotar de confidencialidad a la información que protegerán no consiguen satisfacer la demanda de velocidad que les es requerida. La gran potencia de procesamiento y el tiempo que se requiere para tal fin los hace perdedores en esta carrera contra el tiempo.

Los esquemas de encripción por flujo o cadena de bits son más adecuados para ser montados en plataformas "livianas" como celulares y tablets. Inclusive su sencilla implementación en hardware los convierte en grandes soluciones para satisfacer las demandas de seguridad y velocidad de nuestra sociedad.

El Trivium se ha dado a conocer al resultar finalista en el e-Stream en el año 2005 [4]. No se conocen ataques efectivos contra él, inclusive al ser sometido a diferentes técnicas de criptoanálisis [5, 6, 7].

Sin embargo aún hay problemas abiertos, por ejemplo no se conoce la forma de determinar el período de recursión de las secuencias seudoalea-torias que genera.

Por ello nos hemos planteamos realizar estos estudios desde la teoría de los campos finitos y los registros de desplazamientos lineales (LFSR) y no lineales (NLSFR) [8].

2. Palabras Claves.

Secuencias seudoaleatorias. Cifrado de flujo. Stream Ciphers. Trivium.

3. 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.

Resultados parciales de esta investigación han sido presentados en CACIC 2013, y tal presentación fue premiada 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 Vol. 14 (No. 1, Abril 2014).

Además hemos podido, recientemente, 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 cadenas cifrantes de la familia del trivium.

Como tal tiene posibilidades de ser inscripta en la reciente ampliación de la convocatoria del Ministerio de Ciencia, Técnica e Innovación Productiva, para proyectos de investigación, como consecuencia de la creación del Instituto Universitario del Ejército.

4. Introducción.

4.1. Generalidades

Hoy en día es ampliamente conocido el uso de Linear Feedback Shift Register (LFSR) para generar secuencias pseudo-aleatorias con período y complejidad lineal controladas. El estudio de los LFSRs comenzó alrededor de los años `60 [9] y continuó durante mucho tiempo. En la actualidad se cuenta con una importante cantidad de resultados y aplicaciones [10]: para el diseño de algoritmos criptológicos, para el análisis de la complejidad de una secuencia binaria, para códigos correctores de errores, para generación de claves, etc.

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 (NLFS), una generalización de los anteriores, resultaron estar por mucho tiempo postergados. Mientras que la teoría detrás de los LFSRs es sólida y

bien entendida, muchos problemas fundamentales relacionados con los NLFSRs son problemas abiertos, uno de ellos por ejemplo, es determinar el período (o una cota del período) de la secuencia de salida de un NLFSR.

En los últimos años ha comenzado a aparecer literatura en torno a estos registros no lineales y también sistemas de cifrado en cadena (stream ciphers) que utilizan de alguna manera NLFSRs, tal es el caso de la familia TRIVIUM (De Cannière-Preneel), BIVIUM, CUADRI-VIUM.

El Trivium Toy es 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,

5. Resultados y Objetivos.

5.1. Resultados intermedios de la línea de Investigación.

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

Hemos 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”.

Hemos hecho además un análisis de velocidad de los dos algoritmos: les hemos solicitado a ambos la misma cantidad de bits de una secuencia seudoaleatoria. El Toy es signifi-cativamente más veloz que el Trivium original, para ser más precisos, aproximadamente tres veces más veloz que el trivium original.

5.2. Etapa actual

Estamos llevando adelante el análisis matemático de los polinomios asociados al Trivium y al Trivium Toy. Hemos factorizado ambos polinomios y estamos computando la cantidad de secuencias que cada algoritmo permite generar y la longitud de las mismas secuencias.

Además estamos estudiando otras propiedades de los polinomios de manera que nos permitan observar otras características de los generadores, por ejemplo la posibilidad de personalización o no de los mismos.

Los alumnos que se han sumado al laboratorio están llevando a hardware el Trivium Toy para poder evaluar su performance en un sistema genérico de compuertas programables. De esta manera comenzar a indagar la posibilidad de montar este generador en diversos dispositivos móviles con requerimientos de comunicaciones cifradas, tanto para uso militar como civil.

5.3. Etapa final.

Si se pueden alcanzar los resultados descritos en 5.2 cabe la posibilidad de poder responder algunos de los problemas abiertos que el Trivium.

Obtenidos estos resultados podremos extender los mismos al resto de la familia de Stream Ciphers que comparten la misma estructura.

Además poder calcular la cantidad de claves débiles que generan secuencias de período corto, para alertar sobre ellas e impedir su uso, si se las puede hallar.

Publicaremos estos resultados en los próximos meses. Es nuestra intención poder hacerlo en el CACIC 2014.

6. Formación de Recursos Humanos.

Además de los investigadores que forman parte de nuestro laboratorio, se han sumado Eduardo Malvacio, Santiago Storni y José Ignacio Ariznabarreta, los tres alumnos del último año de la carrera de Ingeniería de nuestra universidad. Como así también el Ing. Néstor Tapia, egresado de nuestra universidad y estudiante de posgrado de Criptografía y Seguridad Teleinformática, también en nuestra casa de estudios.

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

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