Algoritmo criptográfico Mickey

Alejo Perrone – Aldo Silvestre – Emiliano Ciganotto – Nicolas Tosco
Asignatura Criptografía – Docentes: Mg. Jorge Eterovic – Esp. Marcelo Cipriano
Universidad Tecnológica Nacional – Facultad Regional Buenos Aires

lejaperrone@gmail.com - aldosilvestre89@gmail.com - emilianociganotto@hotmail.com - tosconicolas@gmail.com

Keywords Criptografía (Stream Cipher, eSTREAM, Mickey)

Abstract.

En la búsqueda del resguardo de la información, nos encontramos en el gran dilema de qué métodos debemos implementar para conservar la misma confidencial y solo permitir que las personas que deseamos la visualicen. En este documento nos concentraremos en una herramienta que hace hincapié en aquellos dispositivos con hardware limitado.

/

I. Introducción

La criptografía moderna busca garantizar la confidencialidad de la información y prevenir que personas no autorizadas tengan acceso a ella. Estos principios se pueden aplicar en dispositivos portátiles que requieren proteger la información almacenada y procesada. Este tipo de aplicaciones requieren ciertos compromisos de diseño, que se logran usando hardware de alto desempeño. El algoritmo criptográfico Mickey está dirigido a plataformas con recursos limitados de hardware. Está pensado para tener una baja complejidad en hardware y a la vez un alto nivel de seguridad, garantizando que este sea considerado en un algoritmo que hace hincapié en la velocidad , seguridad y simplicidad , en comparación con otros algoritmos más conocidos como el AES cipher.

Este informe presenta la historia, el esquema, fortalezas y debilidades a fin de permitir al lector conocer los datos más relevantes, y de alto nivel, del algoritmo.

II. HISTORIA

Mickey (Mutual Irregular Clocking KEYstream generator) es un algoritmo de tipo stream cipher desarrollado por Steve Babbage y Matthew Dodd. Está diseñado para ser utilizado en plataformas de limitados recursos. Fue uno de los tres ciphers aceptados en Profile 2 de eSTREAM portfolio, no está patentado y su utilización es gratuita para cualquier uso.

III. ESQUEMA

Mickey recibe dos parámetros de entrada, una clave secreta K de 80 bits etiquetados $k_0 \ldots k_{79}$ y un vector de inicialización IV($iv_0 \ldots iv_{l-1}$) que puede ir de 0 a 80 bits donde iv_{l-1} es su longitud . Los key streams de salida son etiquetados como z_0, $z_1 \ldots$, el texto cifrado se produce a partir de texto sin formato operando bit a bit con XOR, como en la mayoría de los cifrados de flujo. Aplicando las operaciones del algoritmo resultará en un texto cifrado al que se denominará C1.

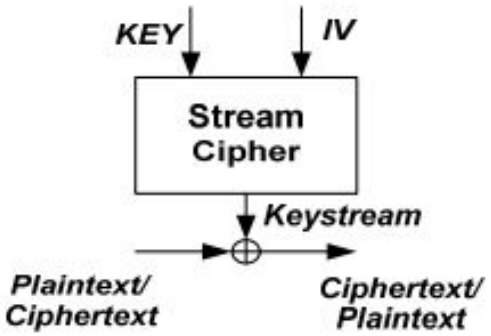

Fig. 2. Proceso inicial del algoritmo

La máxima longitud de streams de salida es 2^{40} bits.

El algoritmo funciona alrededor de dos registros R y S, cada uno de los cuales tiene dos modos de clocking seleccionado por un bit de control. La linealidad de R aseguraría buenas propiedades estadísticas y garantías sobre el período, mientras que la no linealidad de S protegería contra los ataques que podrían montarse contra un sistema lineal.

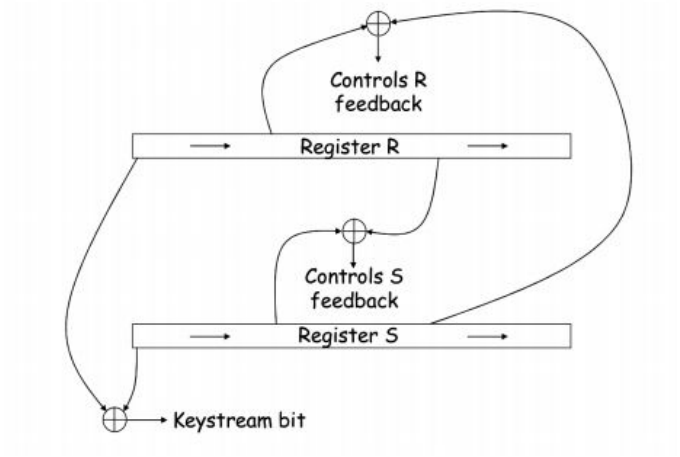

Fig. 2. Estructura del algoritmo Mickey

IV. FORTALEZAS

Los cifrados de flujo que hacen uso de reloj variable a menudo se prestan a ataques estadísticos, en los que el atacante adivina cuántas veces se ha sincronizado el registro en un momento determinado. Hay una serie de

características de un diseño de cifrado que pueden hacer posibles tales ataques.

Los principios detrás del diseño de MICKEY para repeler dichos ataques son los siguientes:

- selección de bits de control aleatorios
- función de retroalimentación del registro R (ataques basados en modelo lineal probabilístico)
- inmunidad a ataques algebraicos
- sincronización en el generador global, no reduce la entropía del sistema
- función de salida simple (confianza en sus clocks irregulares)

V. DEBILIDADES

Debido a que la inicialización de la familia MICKEY de cifrados de flujo proporciona buenas propiedades de difusión, asumimos que la inicialización de estos cifrados de flujo es perfecta, es decir, después de la ejecución, los estados internos se distribuyen de manera uniforme e independientes. Pero según su fórmula, existe un par (K ′, IV ′) con probabilidad 0,5 que genera un flujo de claves de 1 bit desplazado. Con esta debilidad, aplicando ataques de resincronización de diapositivas y ataques de clave relacionados, podemos dar con ataques de recuperación de claves eficientes en la familia de cifrados de flujo MICKEY.

VI. CONCLUSIONES

En conclusión, se puede decir que, aunque la versión 1 de MICKEY ha sufrido muchas amenazas, estas han sido solucionadas en la versión 2.0 y no existe ninguna amenaza significativa contra esta version hasta el momento. Entonces, mientras se considera una implementación en hardware, MICKEY 2.0 podría ser una muy buena opción.

REFERENCIAS

[1] P. KITSOS, "On the Hardware Implementation of the MICKEY-128 Stream Cipher ", may 2005, https://eprint.iacr.org/2005/301.pdf

[2] ENCRYPT - European Network of Excellence in Cryptology, "Call for Stream Cipher Primitives", Scandinavian Congress Center, Aarhus, Denmark, 26-27 May 2005, http://www.ecrypt.eu.org/stream/

Perrone, Alejo
Silvestre, Aldo
Ciganotto, Emiliano
Tosco, Nicolás