République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

École Normale Supérieure

Kouba, Alger

Mémoire présenté pour obtenir le grade de magister

Par : Manel BOUHNIK

Spécialité : Mathématiques

Option : Algèbre et théorie des nombres

Cryptanalyse du générateur Q-SIFR

Soutenu le 16/12/2015 **à** 13 : 30

Devant le jury :

Mr. Abdelhafid MOKRANE	Professeur, ENS KOUBA	Président
Mr. Abdallah DERBAL	Professeur, ENS KOUBA	Examinateur
Mr. Djilali BENAYAT	Professeur, ENS KOUBA	Examinateur
Mr. Abdellah MOKRANE	Professeur, PARIS 8	Co-Directeur de mémoire
Mr. Abdelaziz CHOUTRI	M.C.A, ENS KOUBA	Directeur de mémoire

Table des matières

ملخص

اخترع Goresky و Klapper مولد الشفرات غير الخطي $FCSR$ في 1993 ، كبديل لمولد الشفرات الخطي $LFSR$. لكن حتى $FCSR$ لا يمكن استعماله لوحده كمولد للمفاتيح. لهذا السبب، اقترح Arnault و Berger استعمال $FCSR$ فلتر في 2005. الضعف المتعلق ببنية هذا الاخير ادّى Hell و Johansson الى تطوير هجوم فعّال ضده في 2008.

في هذه المذكرة، قمنا اوّلا بتفصيل المقال:

Design of a Novel Pseudo-Random Generator Based on Vectorial FCSRs

لـ بوفلجة عليلو، عبد العزيز مرجان و عبد الله مقران الذي تم نشره بـ .s.hyfT Y. Chung et M. Yung(Eds.) في 2010. وضع الكتّاب مفهوم شعاعي لمولد الشفرات غير الخطية الذى سمي $VFCSR$. أخيرا، قمنا بترجمة كل هذه المولدات ($LFSR, FCSR,$ و $VFCSR$) فى شكليها Fibonacci و Galois بـ Fortran 95.

Résumé

Les registres à décalage et à rétroaction linéaire avec retenue (FCSRs) sont introduits par Goresky et Klapper en 1993, comme un alternatif des registres à décalages et à rétroaction linéaire (LFSRs). Mais aussi un FCSR ne peut pas être utilisé seul comme un générateur de clé. Pour résoudre ce problème, Arnault et Berger ont proposé d'utiliser le FCSR Filtré en 2005. Une faiblesse liée à la structure de représentation permet une attaque efficace, développée par Hell et Johansson en 2008.

Dans ce mémoire, on a détaillé d'abord l'article Design of a Novel Pseudo-Random Generator Based on Vectorial FCSRs de Boufeldja Allailou, Abdelaziz Morjane et Abdellah Mokrane publié dans le journal Y. Chung et M. Yung(Eds.) en 2010. Les auteurs ont introduit une conception vectorielle des registres à décalage à rétroaction linéaire avec retenue qu'ils l'ont dénommé VFCSR. Enfin, on a programmé tous ces générateur (LFSR, FCSR et VFCSR) en mode Fibonacci et Galois en Fortran 95.

Abstract

In 1993, Goresky and Klapper have introduced for the first time the feedback with carry shift registers (FCSRs) as alternative to linear feedback shift registers (LFSRs). The problem was the impossibility to use the FCSR as a generator of key. To solve that, Arnault and Berger proposed to use Filtred FCSR in 2005. Weakness related to the representation structure allowded an efficient attack developed by Hell and Johansson in 2008.

In this paper, we first detailed the article Design of a Novel Pseudo-Random Generator Based on Vectorial FCSRs of Boufeldja Allailou, Abdelaziz Morjane, and Abdellah Mokrane published in the newspaper Y. Chung et M. Yung(Eds.) in 2010. The authors introduced a vector design of Feedback with Carry Shift Registers, they have called VFCSR. Finally, we programmed all these generator (LFSR, FCSR, and VFCSR) in Fibonacci and Galois representation by Fortran 95.