AN IRREGULAR CLOCK-CONTROLLED BINARY STREAM CIPHER WITH NONLINEAR FEEDBACK SHIFT REGISTERS
'THE SAFE STREAM CIPHER'

by

Serhat Eren Arslan

B.S., Electrical and Electronics Engineering, Istanbul University, 2003

Submitted to the Institute for Graduate Studies in
Science and Engineering in partial fulfilment of
the requirements for the degree of
Master of Science

Graduate Program in Electrical and Electronics Engineering

Boğaziçi University

2006

ABSTRACT

AN IRREGULAR CLOCK-CONTROLLED BINARY STREAM CIPHER WITH NONLINEAR FEEDBACK SHIFT REGISTERS 'THE SAFE STREAM CIPHER'

Stream ciphers are one of the most important classes of encryption algorithms used to ensure security in digital communication. The design of many stream ciphers is based on use of Linear Feedback Shift Registers (LFSRs), due to their simplicity, speed of implementation in hardware and providing sequences with good statistical properties. However, this efficient component is not sufficient when we consider security. The designer should use many nonlinear functions and mechanisms to make the system more resistant against cryptanalysis. A stream cipher should have high period, high linear complexity, good statistical properties and be resistant against most recent successful attacks such as algebraic attacks, correlation attacks, time/memory trade-off attacks, and divide and conquer attacks.

In this thesis, a new stream cipher design is proposed. SAFE is designed to be resistant against algebraic and correlation attacks. In the design phase, the objective was to design a stream cipher with good randomness, high period and linear complexity and resistance against many attacks. The innovation in this thesis is the proposal of nonlinear feedback shift registers instead of linear feedback shift registers to provide resistance against correlation and algebraic attacks. In addition, another innovation is the use of a new irregular decimation algorithm, $EBSG_{variant}$, for increasing the security of the cipher. Keystream properties of the cipher and its resistance with respect to some well known cryptographic attacks are investigated. From the mathematical expressions and simulation results, it is shown that the cipher produces keystream sequences with satisfying basic security requirements and provides high resistance against well known attack types. Finally, we can say that SAFE can be appropriate for both software and hardware applications due to its simple design.

ÖZET

DOĞRUSAL OLMAYAN GERİ BESLEMELİ KAYAN SAKLAÇLI DÜZENSİZ SAAT KONTROLLÜ İKİLİ DİZİ TİP ŞİFRELEYİCİ 'SAFE DİZİ TİP ŞİFRELEYİCİ'

Dizi tip şifreleme algoritmaları güvenli sayısal haberleşme uygulamalarında kullanılan en yaygın şifreleme metotlarındandır. Bu tip şifreleme algoritmaların çoğunluğu basitliğinden, donanımdaki hızından ve iyi istatistiksel özelliklere sahip olduğundan Doğrusal Geri Beslemeli Kayan Saklaçları (LFSRs) tasarımlarında kullanmaktadır. Fakat bu randımanlı bileşenler güvenliği dikkate aldığımızda yeterli olmamaktadır. Tasarımcı, sistemi kriptanalize karsı daha güçlü yapmak için birçok doğrusal olmayan fonksiyonlar ve mekanizmalar kullanmalıdır. Bir dizi tip şifreleyici yüksek periyoda, yüksek doğrusal karmaşıklığa, iyi istatistiksel özelliklere ve cebirsel saldırılar, ilinti saldırıları, zaman bellek ödünleşimi saldırıları, böl ve fethet saldırıları gibi birçok başarılı güncel saldırıya karsı dayanıklı olmalıdır.

Bu tezde yeni bir dizi tip şifreleyici tasarımı önerilmektedir. SAFE cebirsel ve ilinti saldırılarına karsı güçlü olması için tasarlandı. Tasarım evresinde hedef, iyi rasgeleliğe, yüksek periyoda ve doğrusal karmaşıklığa sahip ve saldırılara karsı dayanıklı bir dizi tip şifreleyici tasarlamaktı. Bu tezde yapılan yeniliklerde birisi, ilinti ve cebirsel saldırılara karşı dayanıklılığı artırmak için doğrusal geri beslemeli kayan saklaçların yerine doğrusal olmayan geri beslemeli kayan saklaçların önerilmesidir. Buna ek olarak, başka bir yenilik ise yeni bir seyreltme algoritmasının, $EBSG_{variant}$, şifreleyicinin güvenliğini artırmak amacıyla kullanılmasıdır. Ayrıca bu algoritmaların ürettikleri çıktı dizilerinin özellikleri ve algoritmaların bilinen bazı saldırılara karsı dirençleri çalışmada verilmektedir. Matematiksel açılımlar ve benzetim sonuçları ışığında şifreleyicinin istenen minimum çıktı özelliklerinin gereksinimleri yerine getirdiği ve bilinen bazı saldırı tiplerine karşı yüksek dirence sahip olduğu gösterilmektedir. Sonuç olarak, SAFE basit tasarımı sayesinde donanım ve yazılım uygulamaları için uygundur diyebiliriz.