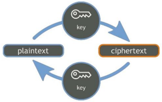
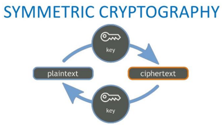
Attacks against Filter Generators Exploiting Monomial Mappings

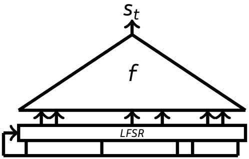
Yann Rotella
Joint work with Anne Canteaut, FSE 2016

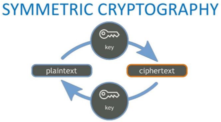
July 12, 2019
SIAM Bern 2019

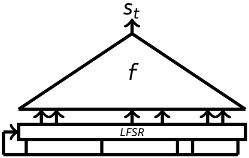
SYMMETRIC CRYPTOGRAPHY




SYMMETRIC CRYPTOGRAPHY
key
plaintext
ciphertext
key


s_t
f
LFSR


SYMMETRIC CRYPTOGRAPHY
key
plaintext
ciphertext
key


s_t
f
LFSR

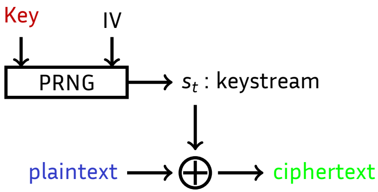
$$\mathbb{F}_{2^n}$$

Structure of this Talk

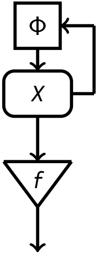
Plan of this Section

Stream ciphers

- Symmetric cryptography, $\neq$ block ciphers
- Based on Vernam cipher (one-time pad)
- PRNG

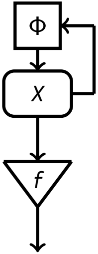


Generic attacks



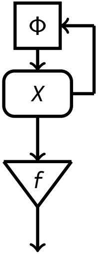
- Key recovering

Generic attacks



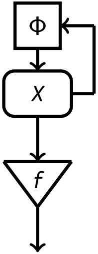
- Key recovering
- Initial state recovering

Generic attacks



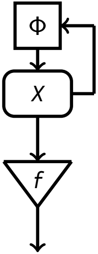
- Key recovering
- Initial state recovering
- Next-bit prediction

Generic attacks



- Key recovering
- Initial state recovering
- Next-bit prediction
- distinguishing s_t from a random sequence

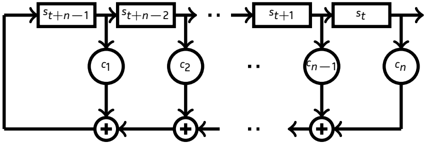
Generic attacks



- Key recovering
- Initial state recovering
- Next-bit prediction
- distinguishing s_t from a random sequence

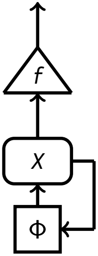
Always take an internal state twice bigger as the security level (i.e. key size)

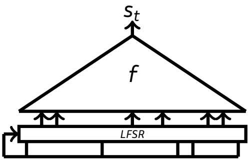
Linear feedback shift Register (LFSR)



- Nice statistical properties
- Linear
- $s_{t+L} = \sum_{i=1}^{n} c_i s_{t+n-i}, \forall t \leq 0$
- $P(X) = 1 - \sum_{i=1}^{n} c_i X^i$
- $P^*(X) = X^n P(1/X)$
- We wil take P primitive

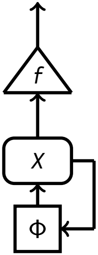
Filtered LFSR

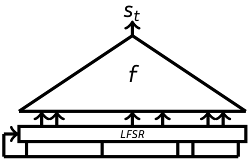




$$s_t = f(u_{t+\gamma_1}, \dots, u_{t+\gamma_n})$$

Filtered LFSR





$$s_t = f(u_{t+\gamma_1}, \ldots, u_{t+\gamma_n})$$

Algebraic Normal Form

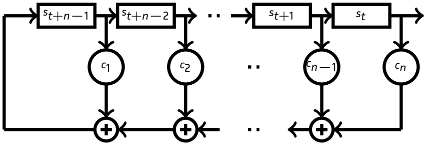
$$f(x_1, x_2, \ldots, x_n) = \sum_{u \in \mathbb{F}_2^n} a_u \prod_{i=1}^{n} x_i^{u_i}$$

$$= a_0 + a_1x_1 + a_2x_2 + \cdots + a_3x_1x_2 + \cdots + a_{2^n-1}x_1 \cdots x_n$$

Plan of this Section

LFSR over a Finite Field

- α : root of the primitive characteristic polynomial in $\mathbb{F}_{2^n}$
- Identify the n-bit words with elements of $\mathbb{F}_{2^n}$ with the dual basis of $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$

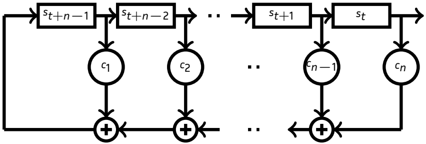


Proposition

The state of the LFSR at time $(t+1)$ is the state of the LFSR at time t multiplied by α.

LFSR over a Finite Field

- α : root of the primitive characteristic polynomial in $\mathbb{F}_{2^n}$
- Identify the n-bit words with elements of $\mathbb{F}_{2^n}$ with the dual basis of $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$



Proposition

The state of the LFSR at time $(t+1)$ is the state of the LFSR at time t multiplied by α.

For all t, $X_t = X_0\alpha^t$

Boolean functions

Proposition (Univariate representation)

$$F(X) = \sum_{i=0}^{2^n-1} A_i X^i$$

with $A_i \in \mathbb{F}_{2^n}$

Boolean functions

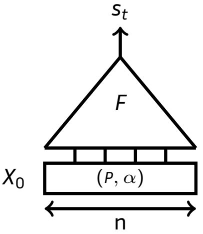
Proposition (Univariate representation)

$$F(X) = \sum_{i=0}^{2^n-1} A_i X^i$$

with $A_i \in \mathbb{F}_{2^n}$

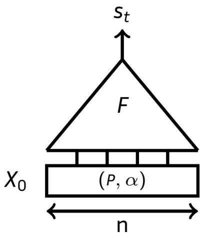
For all t, $s_t = F(X_0 \alpha^t)$

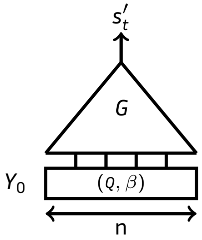
Monomial equivalence [Rønjom - Cid 2010]



For all t, $s_t = F(X_0 \alpha^t)$

Monomial equivalence [Rønjom - Cid 2010]

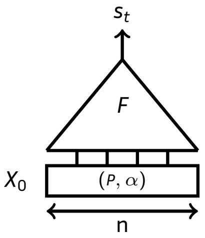


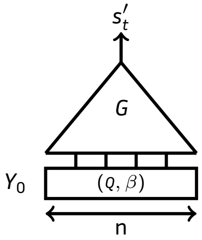


For all t, $s_t = F(X_0\alpha^t)$

$\beta = \alpha^k$ with $\gcd(k, 2^n - 1) = 1$

Monomial equivalence [Rønjom - Cid 2010]



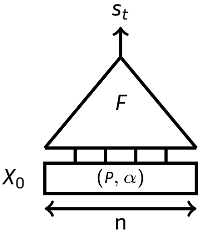


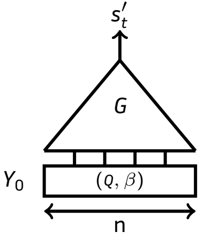
For all t, $s_t = F(X_0\alpha^t)$

$\beta = \alpha^k$ with $\gcd(k, 2^n - 1) = 1$

Let $r = k^{-1} \mod (2^n - 1)$.

Monomial equivalence [Rønjom - Cid 2010]



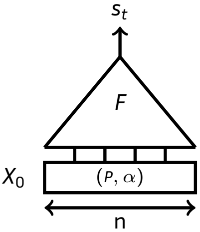


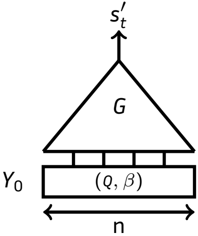
For all t, $s_t = F(X_0\alpha^t)$

$\beta = \alpha^k$ with $\gcd(k, 2^n - 1) = 1$

Let $r = k^{-1} \mod (2^n - 1)$.
If $G(X) = F(X^r)$ and $Y_0 = X_0^k$.

Monomial equivalence [Rønjom - Cid 2010]





For all t, $s_t = F(X_0\alpha^t)$

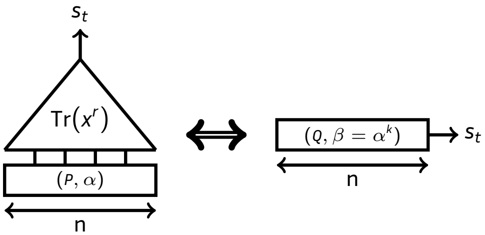
$\beta = \alpha^k$ with $\gcd(k, 2^n - 1) = 1$

Let $r = k^{-1} \mod (2^n - 1)$.
If $G(X) = F(X^r)$ and $Y_0 = X_0^k$.
Then $s'_t = G(Y_0\beta^t) = G(Y_0\alpha^{kt}) = F(Y_0^r\alpha^{rkt}) = F(X_0\alpha^t) = s_t$

For all t, $s'_t = s_t$ if $Y_0 = X_0^k$

Example

$F(x) = \mathrm{Tr}(x^r)$, with $\gcd(r, 2^n - 1) = 1$:
Let k be such that $rk \equiv 1 \mod (2^n - 1)$.



$\Longrightarrow$ The initial generator is equivalent to a plain LFSR of the same size.

Consequence

The security level of a filtered LFSR is the minimal security level for a generator of its equivalence class.

Consequence

The security level of a filtered LFSR is the minimal security level for a generator of its equivalence class.

- Algebraic attacks
- Correlation attacks

Algebraic attacks

Λ : Linear complexity

Proposition (Massey-Serconek 94)

Let an LFSR of size n filtered by a Boolean function F:

$$F(X) = \sum_{i=0}^{2^n-1} A_i X^i$$

Then

$$\Lambda = \#\{0 \leq i \leq 2^n - 2 : A_i \neq 0\}$$

Algebraic attacks

Λ : Linear complexity

Proposition (Massey-Serconek 94)

Let an LFSR of size n filtered by a Boolean function F:

$$F(X) = \sum_{i=0}^{2^n-1} A_i X^i$$

Then

$$\Lambda = \#\{0 \leq i \leq 2^n - 2 : A_i \neq 0\}$$

The monomial equivalence does not affect the complexity of algebraic attacks: see [Guang Gong, Sondre Røonjom, Tor Helleseth and Honggang Hu, IEEE-IT 2011, Discrete Fourier Spectra Attacks]

Plan of this Section

Results

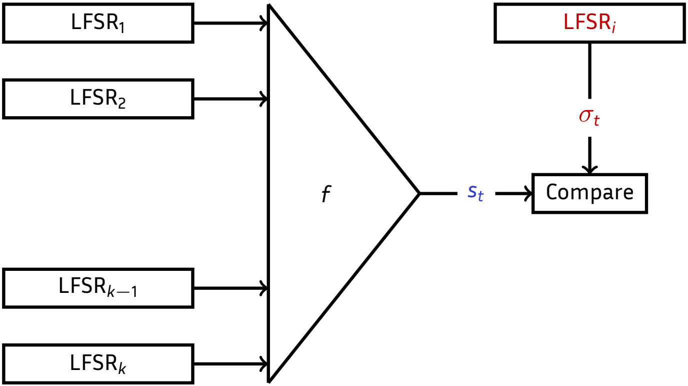
Proposition

The relevant criterion for correlation attacks is the generalized non-linearity and not the non-linearity.

Proposition

When $2^n - 1$ is not a prime number, we recover the initial state using a divide and conquer technique.

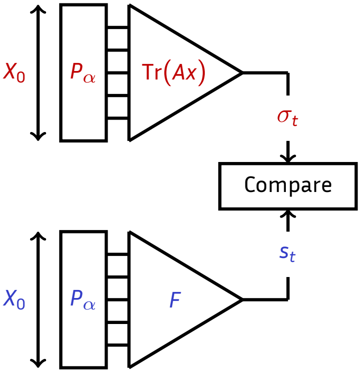
Correlation attack [Siegenthaler 85]



Criterion

The criterion behind the correlation attack is the **resiliency** of f.

Fast correlation attack [Meier - Staffelbach 88]

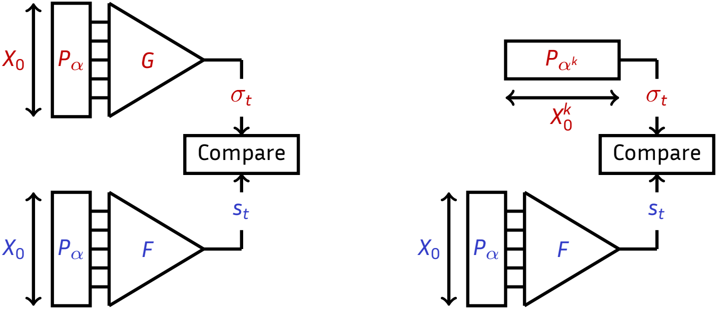


Criterion

The criterion behind the fast correlation attack is the **non-linearity** of F.

Generalized fast correlation attacks

$G(x) = \mathrm{Tr}(Ax^k)$



Generalized non-linearity [Gong & Youssef 01]

Non-linearity :

Not anymore !

Relevant security criterion:

Generalized non-linearity

$$\mathsf{GNL}(f) = d(f, \{\mathrm{Tr}(\lambda x^k, \lambda \in \mathbb{F}_{2^n}, \gcd(k, 2^n - 1) = 1\})$$

Generalized non-linearity [Gong & Youssef 01]

Non-linearity :

Not anymore !

Relevant security criterion:

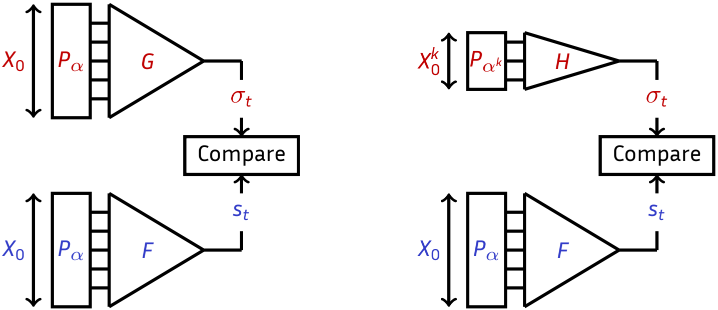
Generalized non-linearity

$$\mathrm{GNL}(f) = d(f, \{\mathrm{Tr}(\lambda x^k, \lambda \in \mathbb{F}_{2^n}, \gcd(k, 2^n - 1) = 1\})$$

And if k is not coprime to $2^n - 1$?

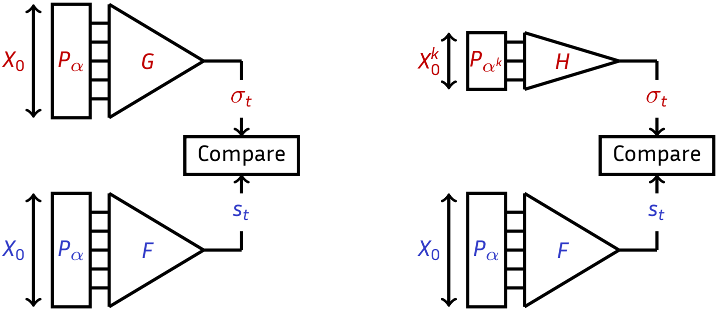
A more efficient correlation attack

When $\gcd(k, 2^n - 1) > 1$ and F correlated to $G(X) = H(X^k)$.



A more efficient correlation attack

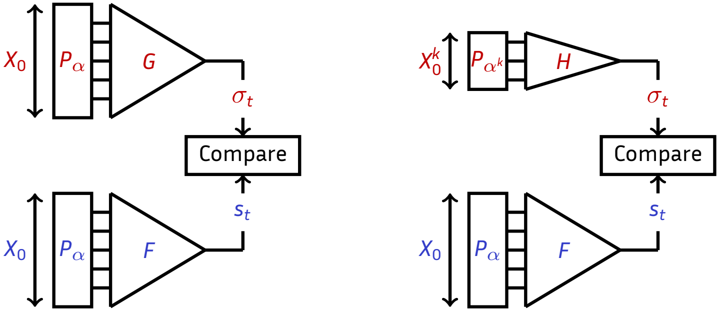
When $\gcd(k, 2^n - 1) > 1$ and F correlated to $G(X) = H(X^k)$.



- Number of states of the small generator: $\tau_k = \text{ord}(\alpha^k)$.

A more efficient correlation attack

When $\gcd(k, 2^n - 1) > 1$ and F correlated to $G(X) = H(X^k)$.



- Number of states of the small generator: $\tau_k = \mathrm{ord}(\alpha^k)$.
- Exhaustive search on X_0^k: Time $= \frac{\tau_k \log(\tau_k)}{\varepsilon^2}$

Recovering the remaining bits of the initial state

Property

We get $\log_2(\tau_k)$ bits of information on X_0 where $\tau_k = \text{ord}(\alpha^k)$:

Recovering the remaining bits of the initial state

Property

We get $\log_2(\tau_k)$ bits of information on X_0 where $\tau_k = \text{ord}(\alpha^k)$:

If we perform two distinct correlation attacks with k_1 et k_2, then we get $\log_2(\text{lcm}(\tau_{k_1}, \tau_{k_2}))$ bits of information.

Plan of this Section

Some open questions

- Need for new criterion?
- As $\mathcal{T}_k$ is always odd, we have $\varepsilon \geq \frac{\mathcal{T}_k}{2^n}$, but can we have a joint bound for different k ?
- Function F takes a small number of inputs...
- Find an efficient algorithm that computes H that approximates F ?
- How this criterion is linked to the classical ones ?

Cryptanalysis of an Equivalent Model of Stream Cipher Espresso

ZHANG Jia-Min, QI Wen-Feng

Information Engineering University, Zhengzhou 450002, China

摘要 | 图/表 | 参考文献(9) | 相关文章 (5)

全文: PDF (309 KB) HTML (1 KB)
输出: BibTeX | EndNote (RIS)

摘要 Espresso算法是由E. Dubrova和M. Hell两人设计的面向5G通信需求的序列密码算法, 算法采用256级的非线性反馈移位寄存器(NFSR)作为驱动部件, 密钥长度为128比特, 初始化向量为96比特, 过滤输出函数为6次布尔函数. 由于驱动部件为NFSR, 因此Espresso算法可以较好地抵抗标准代数攻击以及相关攻击等分析方法. 然而本文将证明无论参数如何选择, 只要是利用E. Dubrova和M. Hell所提方法构造出来的NFSR, 其任意寄存器上的输出序列均可由同级数的线性反馈移位寄存器(LFSR)通过选取适当的过滤函数生成, 即等于某个LFSR的前馈序列. 特别的, 这些LFSR是相同且过滤函数可显式地表达出来. 利用这一结果, 我们证明了Espresso算法的输出序列为某个256级LFSR的前馈过滤, 对应的过滤函数为12次布尔函数. 针对该等价模型, 我们可以成功地实施代数攻击, 其时间复杂度为O(266.86). 我们指出, 要想抵抗等价模型下的代数攻击, Espresso算法中的输出函数至少应为8次布尔函数. 最后我们还讨论了等价模型下输出函数的其他漏洞.

关键词： 非线性反馈移位寄存器, 代数攻击, Espresso, 等价模型

Abstract: Espresso is a stream cipher, designed by E. Dubrova and M. Hell to meet the requirement of 5G communications, which uses 128-bit key, 96-bit IV (Initial Vector) and an 6-degree Boolean function as its output function. It adopts a 256-bit Nonlinear Feedback Shift Registers (NFSR) in a special class as its driving part, which makes it invulnerable to the classical algebraic attack and correlation attack. In this paper, we prove that as long as an NFSR is generated by the method proposed by E. Dubrova and M. Hell, the output sequences of any register of the NFSR can also be generated by some Linear Feedback Shift Registers with a proper filter function. Especially, these LFSRs are the same and the filter functions can be represented explicitly. Based on this result, we prove that the output sequences of Espresso are just sequences generated by some 256-bit LFSR with a 12-degree filter function. We successfully mount an algebraic attack to the equivalent model of Espresso with time complexity being O(266.86). We point out that to defend the algebraic attack in such equivalent model, the degree of Espresso's output function should be 8 at least. Finally, some other flaws of the original output function of Espresso are also discussed.

Key words: NFSR algebraic attack Espresso equivalent model

服务
- 把本文推荐给朋友
- 加入我的书架
- 加入引用管理器
- E-mail Alert
- RSS

作者相关文章
- 章佳敏
- 戚文峰

基金资助:国家自然科学基金项目(61272042, 61100202, 61100200, 61170235, 61309017, 61402524, 61521003); 国家863计划(2015AA01A708)

通讯作者: 章佳敏, E-mail: jiamin.zhang.edu@gmail.com

引用本文:

章佳敏, 戚文峰. Espresso算法等价模型的密码分析[J]. 密码学报, 2016, 3(1): 91-100.
ZHANG J M, QI W F. Cryptanalysis of an Equivalent Model of Stream Cipher Espresso. Journal of Cryptologic Research, 2016, 3(1): 91-100.

链接本文:

http://www.jcr.cacrnet.org.cn:8080/mmxb/CN/10.13868/j.cnki.jcr.000112 或 http://www.jcr.cacrnet.org.cn:8080/mmxb/CN/Y2016/V3/I1/91

PDF Preview

密码学报 ISSN 2095-7025 CN 10-1195/TN E-mail: jcr@cacrnet.org.cn

Thank You for your attention !

Questions ?