

**Framework of a Novel Technique for
Algebraic and Fast Correlation Attacks
Based on the Dedicated Sample Decimation**

Miodrag Mihaljevic and Hideki Imai

SASC 2004

Brugge, Belgium, October 14, 2004

Roadmap of the presentation

- Introduction
- Underlying Ideas for Novel Approach
- The Dedicated Sample Based Approach
- Preliminary Discussion of Algebraic and Fast Correlation Attacks Based on Dedicated Sampling

1. Introduction

Fast Correlation and Algebraic Attacks,
Motivation for the work,
Model under consideration,
Abstract of the talk

Fast Correlation and Algebraic Attacks - Underlying Problems

Fast Correlation Attack:

- solve an overdefined system of **highly noisy linear** equations

Fast Algebraic Attack:

- solve an overdefined system of **error-free (or low noisy) nonlinear** equations

Fast Correlation and Algebraic Attacks – The Most Powerful Reported Approaches

Fast Correlation Attack:

- in order to generate more equations for probabilistic decoding employ appropriate **linear combinations** of the initial parity-checks

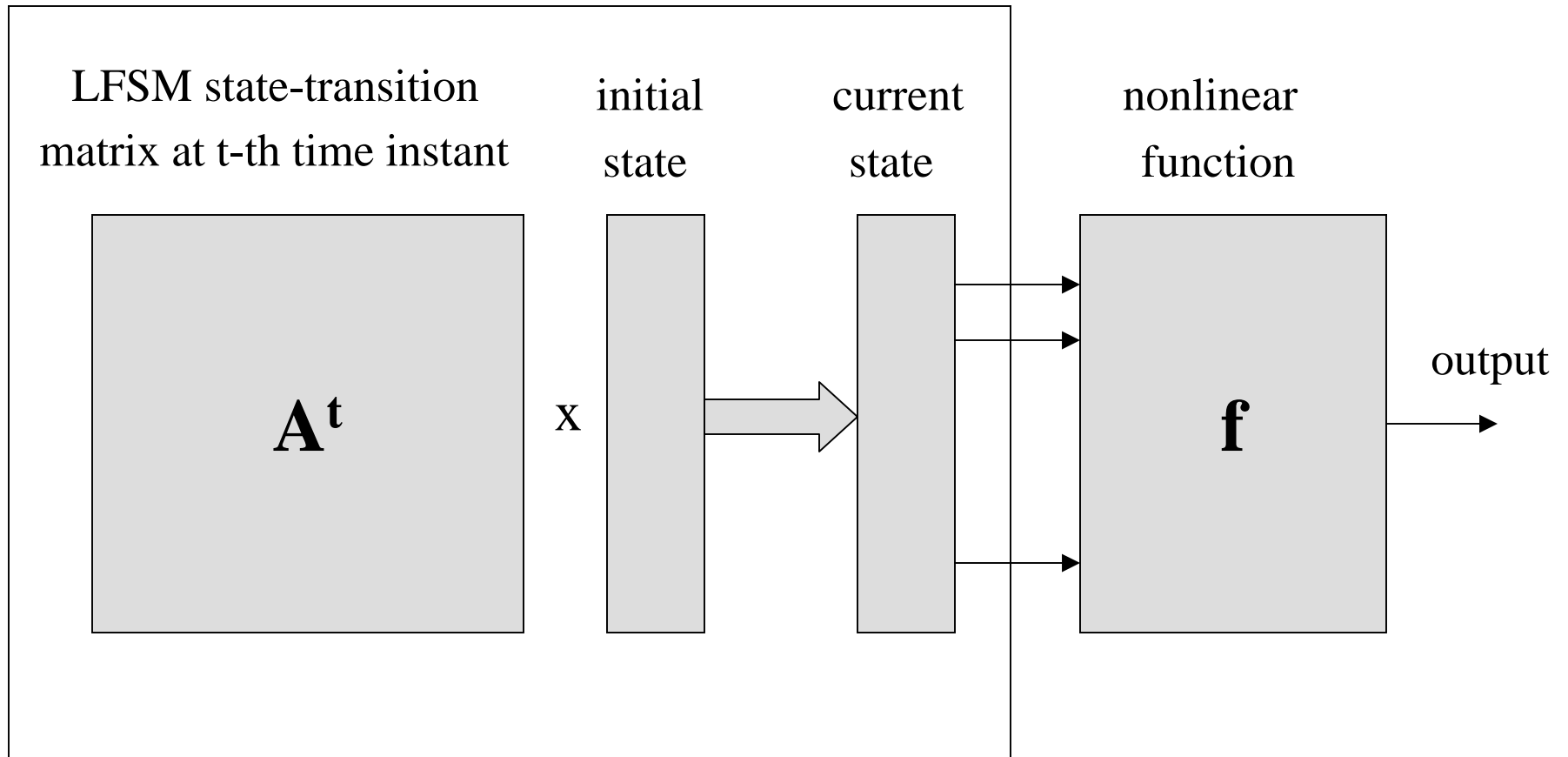
Fast Algebraic Attack:

- in order to reduce **nonlinearity** of the initial equations employ appropriate **linear combinations** of the initial equations

Motivation for the Work

- **extension** of the results from
- M.Mihaljevic and H. Imai, “The Decimated Sample Based Improved Algebraic Attacks on Nonlinear Filters”, SCN 2004
- into a **complementary direction**

Linear Finite State Machine (LFSM)



Abstract of the Talk

- This paper proposes improved approaches for cryptanalysis of keystream generators based on a composition of a linear finite state machines (LFSM) and nonlinear mapping.
- The main feature of the proposed approach is that it is based on **identification and selection for further processing certain suitable positions in the given sample so that only the decimated sample elements are relevant for the attacking.**
- The proposed approaches employ search over a set of the hypothesis and the sampling dedicated to the underlying hypothesis.

2. Underlying Ideas for the Novel Approach

involve into the game more particular
information

Algebraic Attacks

- The **performance** of most reported algebraic attacks strongly **depend on the nonlinear part**, and if this part does not have certain characteristics appropriate for cryptanalysis the attacks could become very complex and not feasible.
- We address the following issue: Find a way to **involve into the algebraic attack certain characteristics of the linear part in order to obtain more powerful attacks** in the cases when the nonlinear part is heavily resistant against the reported algebraic attacks

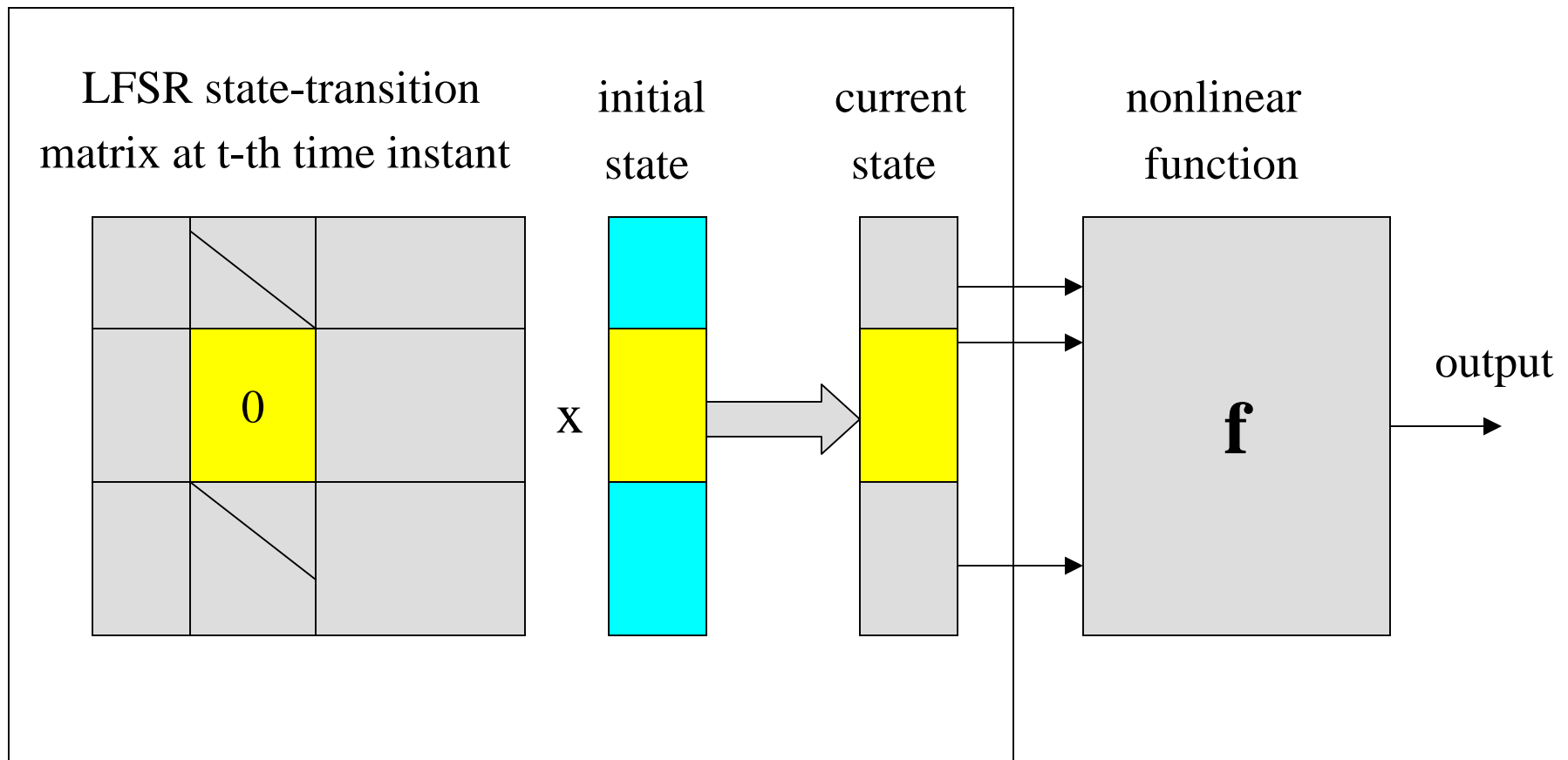
Fast Correlation Attacks


- The **noise** involved in the system of equations is a **consequence of linearization** of a nonlinear system of equations which describes the considered stream cipher.
- So, **this noise** is not an usual random one and accordingly **could be an objective of the adjustment attempts**.
- Accordingly, the motivations for this work were consideration of the techniques for **specification the systems of equations with a noise lower than the one obtained by a simple straightforward linearization** of the initial system of nonlinear equations related to the nonlinear filter.

Main Idea

- **suppose certain B bits of the LFSM initial state and**
- **search for the powers of the state transition matrix which provide that certain input argument (arguments) of the nonlinear function are equal to zero**
- **implying reduced nonlinearity of the underlying system of equations regarding to algebraic attacks,**
- **or reduced the correlation noise regarding to fast correlation attacks.**

Linear Feedback Shift Register (LFSR)



 assumed bits of the initial state

Toy Example (1)

- $\mathbf{f}(\cdot) = \mathbf{x}_1(\mathbf{t}) + \mathbf{x}_2(\mathbf{t}) \mathbf{x}_3(\mathbf{t}) + \mathbf{x}_3(\mathbf{t}) \mathbf{x}_4(\mathbf{t}) + \mathbf{x}_5(\mathbf{t}) \mathbf{x}_6(\mathbf{t}) \mathbf{x}_7(\mathbf{t}) \mathbf{x}_8(\mathbf{t}) \mathbf{x}_9(\mathbf{t}) \mathbf{x}_{10}(\mathbf{t})$
- algebraic attacks: $\mathbf{x}_5(\mathbf{t}) = \mathbf{0}$ implies reduction of the nonlinearity **from 6 to 2**

Toy Example (2)

- $\mathbf{f}(\cdot) = \mathbf{x}_1(\mathbf{t}) + \mathbf{x}_2(\mathbf{t}) \mathbf{x}_3(\mathbf{t}) + \mathbf{x}_3(\mathbf{t}) \mathbf{x}_4(\mathbf{t}) + \mathbf{x}_5(\mathbf{t}) \mathbf{x}_6(\mathbf{t}) \mathbf{x}_7(\mathbf{t}) \mathbf{x}_8(\mathbf{t}) \mathbf{x}_9(\mathbf{t}) \mathbf{x}_{10}(\mathbf{t})$
- correlation attacks: $\mathbf{x}_3(\mathbf{t}) = \mathbf{0}$ implies reduction of the correlation nose from **0.38** to **0.0156**.

Simple: $\mathbf{f}(\cdot) = \mathbf{x}_1(\mathbf{t}) + \mathbf{e}(\mathbf{t})$ $\Pr(\mathbf{E}(\mathbf{t})=1)=0.38$

Novel: $\mathbf{f}(\cdot) = \mathbf{x}_1(\mathbf{t}^*) + \mathbf{e}(\mathbf{t}^*)$ $\Pr(\mathbf{E}^*(\mathbf{t})=1)=0.0156$

A Trade-Off Goal

- Assuming **B bits**,
- In the case of algebraic attacks, achieve a way to reduce the nonlinearity **d** of the filter function, providing that

$$L^{wd} \gg 2^B L^{wd*}$$

- In the case of correlation attacks find a way to reduce the correlation noise.

3. Framework of the Dedicated Decimation Based Cryptanalysis

General Framework (1)

- Suppose certain B bits of the LFSM initial state and search for the powers of the state transition matrix which provide that **certain input argument (arguments) of the nonlinear function are equal to zero** implying
- **reduced nonlinearity** of the underlying system of equations regarding to algebraic attacks, or
- **reduced the correlation noise** regarding to fast correlation attacks.

General Framework (2)

- **Decimate the sample** corresponding to the above identified powers and for further processing take into account only the decimated sample elements.
- Note that the **sample decimation depends on the assumed B bits**, i.e. for each of the assumptions a dedicated sampling should be specified.

General Framework (3)

- Employ suitable algebraic or fast correlation attack **over the decimated sample** and recover a candidate for the secret key.
- Run over all **2^B possibilities** and check the validity of each candidate.

4. Preliminary Discussion

Some Hints

Preliminary discussion (1)

- Implementation of the framework includes the preprocessing phase which is independent of a particular sample, and the processing phase which recovers the secret key based on the given sample.
- The preprocessing phase includes construction of $2^{\mathbf{B}} \times \mathbf{N}$ dimensional table.
- Each row of the table contains \mathbf{N} indices of the sampling positions dedicated to the assumed \mathbf{B} bits.

A Preprocessing Output – the **Table**

1	$S(t_1^{(1)})$	$S(t_2^{(1)})$		$S(t_N^{(1)})$
2	$S(t_1^{(2)})$	$S(t_2^{(2)})$		$S(t_N^{(2)})$
2^B				

Preliminary discussion (2)

- Assuming a nonlinear function suitable for the proposed attack, the **gain** in the processing phase is a consequence of the following:
- a highly **reduced nonlinearity** of the related system of equations in the case of algebraic attacks;
- a highly **reduced correlation noise** in the case of fast correlation attacks.

Preliminary discussion (3)

- The proposed attacking framework can imply **a design criteria** for the nonlinear function employed in a nonlinear filter keystream generator.

Thank You Very Much for the
Attention,

and

QUESTIONS Please!