
An Algebraic Attack on the Bluetooth Key Stream Generator

Frederik Armknecht

`armknecht@th.informatik.uni-mannheim.de`

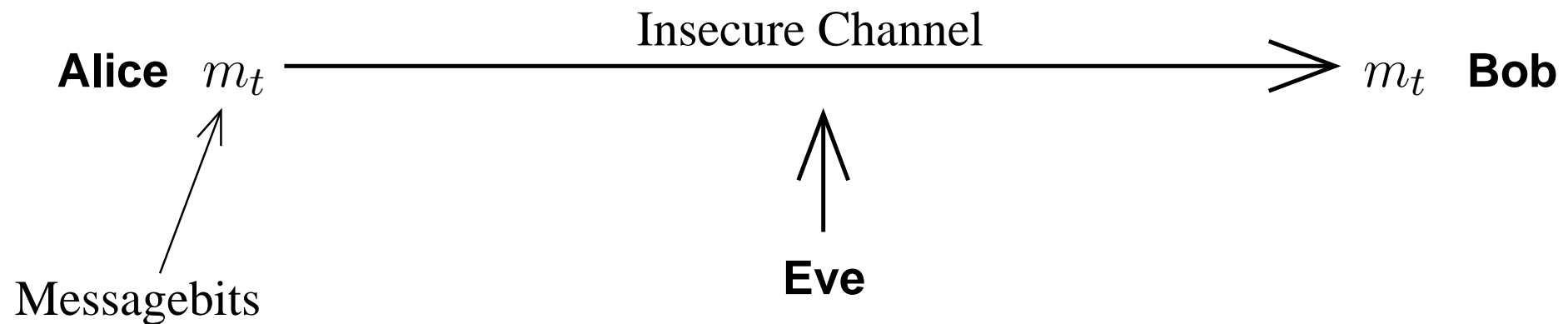
University of Mannheim
(Germany)

Bluetooth is a standard for wireless communication between different devices (e.g. mobile phones, desktop computers, . . .), making pervasive computing possible.

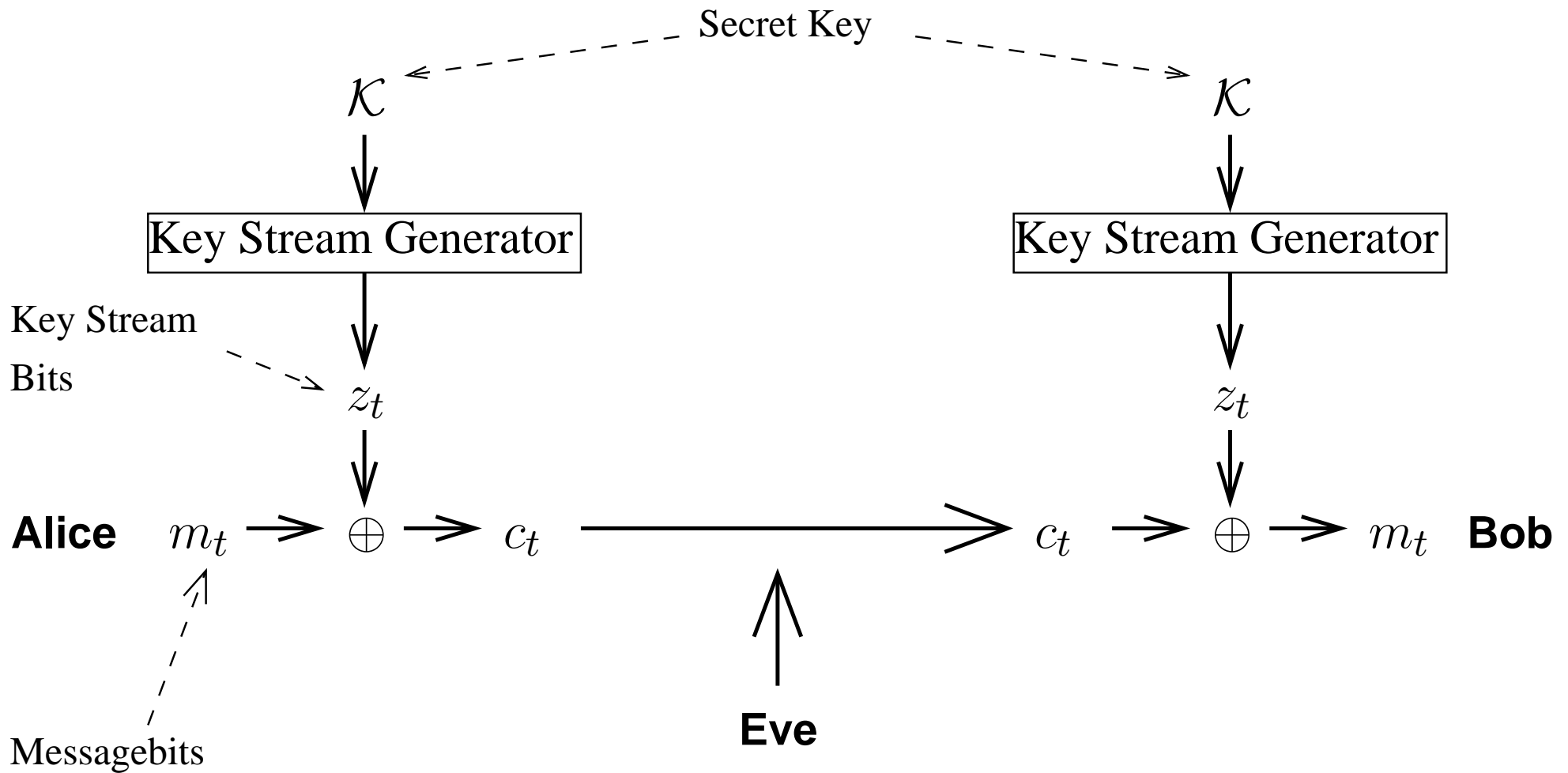
How secure is the Bluetooth encryption?

Situation

Alice wants to send a message $m = (m_1, m_2, \dots)$ to Bob without being eavesdropped.



Using Key Stream Generators



The Eavesdropper Eve

It is assumed that Eve knows:

- The key stream generator
- Some of the key stream bits z_t

Eve knows not:

- The secret key \mathcal{K}

Eve tries to recover the secret key \mathcal{K} .

Algebraic Attacks

Algebraic attacks came up in the last years. There exist algebraic attacks against

- Block ciphers
 - ◆ AES, Serpent (Courtois, Pieprzyk; 2002)
- Stream ciphers
 - ◆ Toyocrypt, LILI-128 (Courtois, Meier; 2003)
 - ◆ Bluetooth key stream generator (Armknecht; 2002)

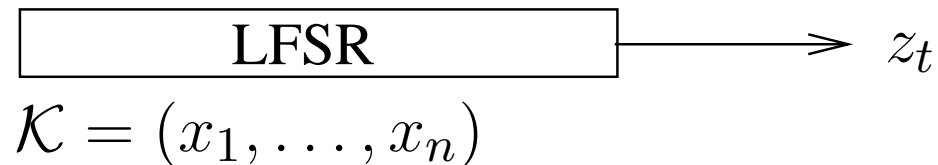
Algebraic Attacks

Simply spoken, an algebraic attack consists of two steps:

1. Set up a system of equations, the unknowns being the bits of the secret key \mathcal{K} .
2. Solve it.

Key Stream Generator I

Linear feedback shift register (LFSR) of length n :



Advantages:

- Very fast
- z_t seem to be randomly chosen

Disadvantage:

- For each clock t , there exists a known linear function F_t with $z_t = F_t(x_1, \dots, x_n)$

Algebraic Attack on LFSRs

Algebraic attack on LFSRs:

1. Set up system of linear equations

$$z_1 = F_1(x_1, \dots, x_n)$$

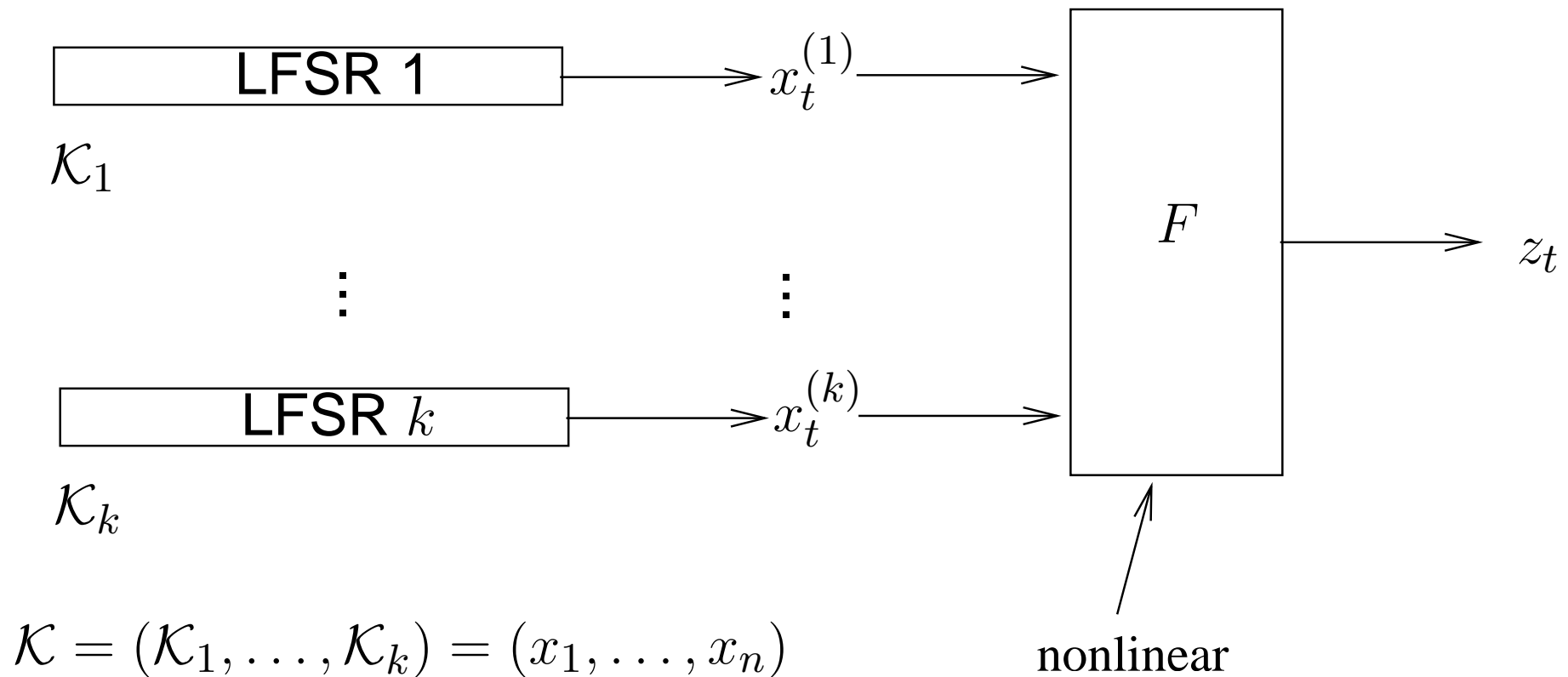
$$z_2 = F_2(x_1, \dots, x_n)$$

⋮

2. Solve this system of equations (easy, as it is linear)

Key Stream Generator II

A combiner with k LFSRs:



Algebraic Attack on k -combiners

Algebraic attack on k -combiners:

1. Set up system of nonlinear equations

$$z_1 = F(x_1^{(1)}, \dots, x_1^{(k)}) = F_1(x_1, \dots, x_n)$$

$$z_2 = F(x_2^{(1)}, \dots, x_2^{(k)}) = F_2(x_1, \dots, x_n)$$

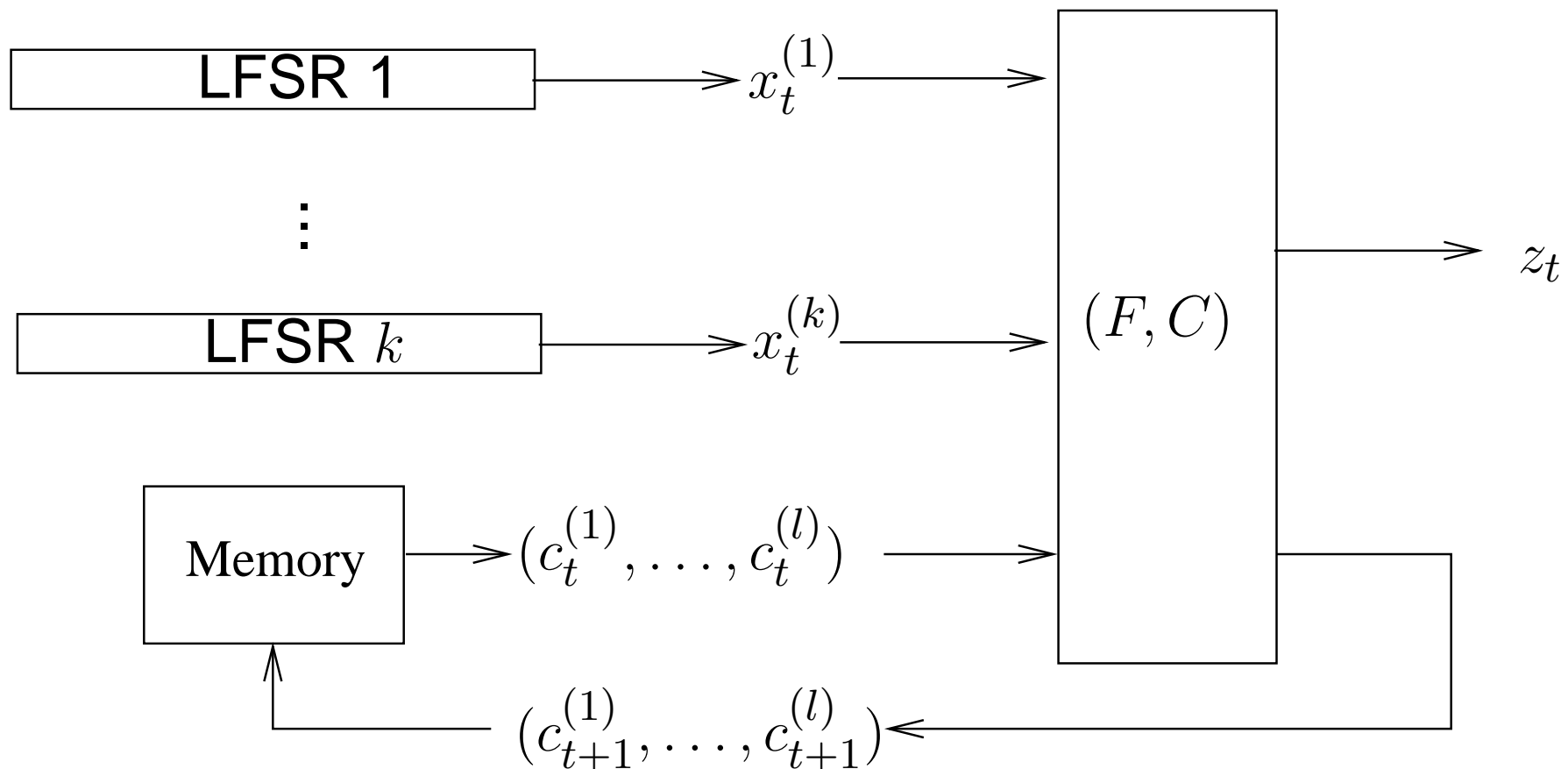
⋮

Each F_t has the same degree d .

2. Replace each monomial of degree > 1 by a new variable (Linearization) \Rightarrow a system of linear equations in $\approx \binom{n}{d}$ unknowns.
3. Solve this system of linear equations.

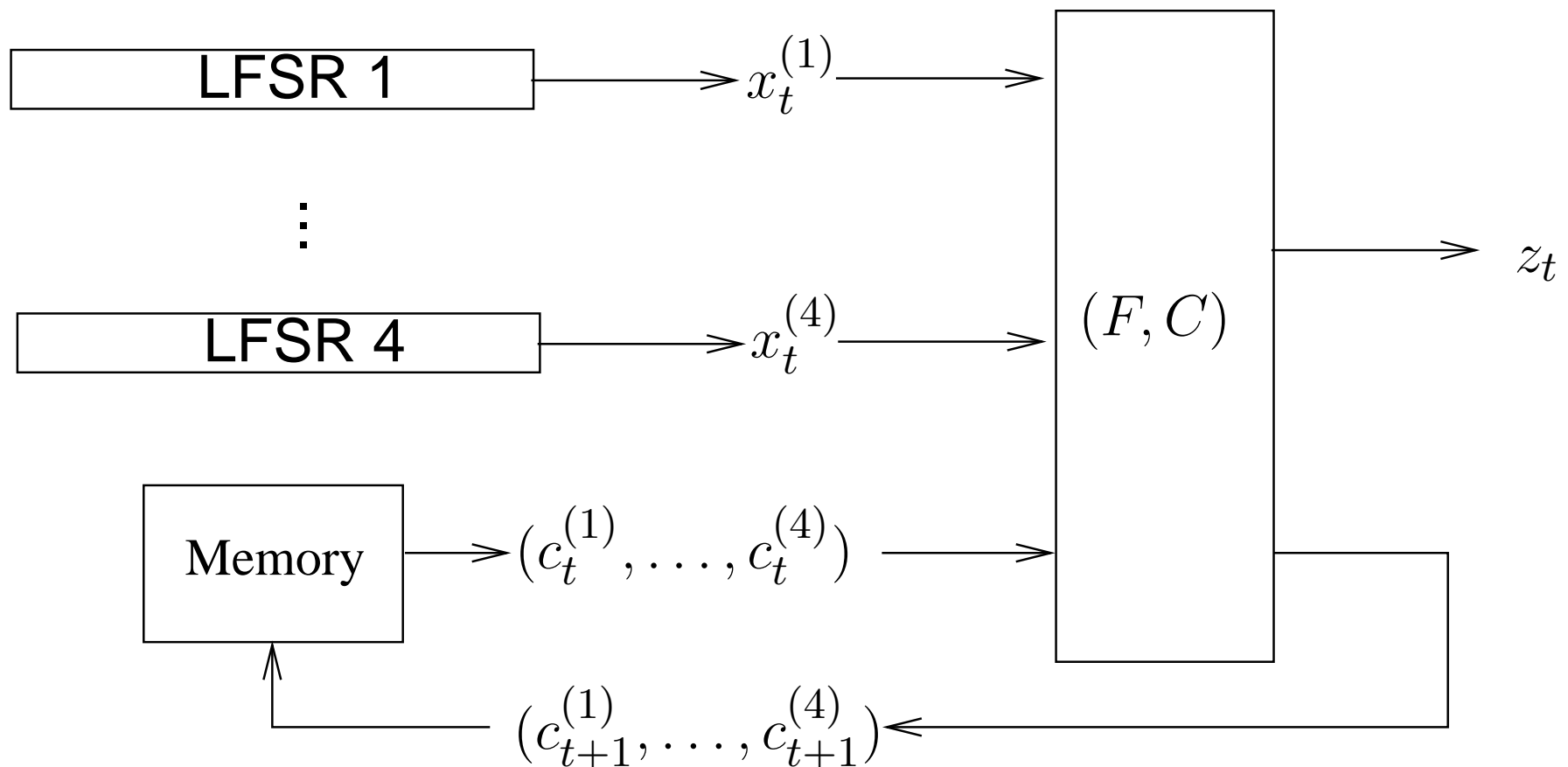
Key Stream Generator III

A combiner with k LFSRs and l memory bits:



Bluetooth Key Stream Generator

The Bluetooth key stream generator:



Algebraic Attack on Bluetooth?

1. System of equations:

$$\begin{aligned} & \vdots \\ z_t &= F(x_t^{(1)}, \dots, x_t^{(4)}, c_t^{(1)}, \dots, c_t^{(4)}) \\ &= F(x_t^{(1)}, \dots, x_t^{(4)}, C_t(x_1^{(1)}, \dots, x_{t-1}^{(4)}, c_1^{(1)}, \dots, c_1^{(4)})) \\ &= F_t(x_1, \dots, x_n, c_1^{(1)}, \dots, c_1^{(4)}) \\ & \vdots \end{aligned}$$

In general, the functions F_t have a high degree.

2. Solving ???

A relation without memorybits

Surprisingly, there exists a relation \tilde{F} of degree 4 with

$$0 = \tilde{F}(X_t, X_{t+1}, X_{t+2}, X_{t+3}, z_t, z_{t+1}, z_{t+2}, z_{t+3})$$

where

- $X_t = (x_t^{(1)}, x_t^{(2)}, x_t^{(3)}, x_t^{(4)})$ is the output of the 4 LFSRs at clock t
- $z_t, z_{t+1}, z_{t+2}, z_{t+3}$ are four successive bits of the known keystream

This relation depends NOT on the memory bits!

Algebraic Attack on Bluetooth!

1. Set up the following system of equations

$$\begin{aligned} & \vdots \\ 0 &= \tilde{F}(X_t, X_{t+1}, X_{t+2}, X_{t+3}, z_t, z_{t+1}, z_{t+2}, z_{t+3}) \\ &= \tilde{F}_t(x_1, \dots, x_n, z_t, z_{t+1}, z_{t+2}, z_{t+3}) \\ & \vdots \end{aligned}$$

2. Linearization \Rightarrow system of linear equations with $\approx 2^{23.07}$ unknowns.

3. Solve it. Work effort $\approx 2^{67.58}$ operations.

Alg. attacks on comb. with memory

Theorem (Krause, Armknecht; 2003)

For each combiner C with k LFSRs and l memory bits, a nontrivial relation \tilde{F}_C of degree $\lceil k(l+1)/2 \rceil$ with

$$0 = \tilde{F}_C(X_t, \dots, X_{t+l}, z_t, \dots, z_{t+l})$$

can be constructed.

\Rightarrow Algebraic attacks are always possible on combiners with memory!