

# The use of d-truncated Gröbner bases in cryptanalysis of symmetric ciphers

Jens-Are Amundsen

Høgskolen i Gjøvik

Presentation of master's thesis 2010

Or...

How to recover the encryption key  
by solving  
huge systems of polynomial equations  
without crashing the computer!!!

# Outline of Presentation

## 1 Problem Description

- Algebraic Cryptanalysis
- Problem Description
- Research Questions

## 2 Topics

- Gröbner Bases. What? Why?
- Presentation of Two Ciphers

## 3 Results From Cryptanalysis

- Results: LILI-128
- Results: KASUMI

# Algebraic Cryptanalysis

- Express an instance of encryption/decryption as a system of polynomial equations
- Key bits are the unknown variables
- Find a simultaneous solution to the system of equations
- We use the *method of Gröbner bases*

# Problem Description

- Finding solutions to systems of polynomial equations is very hard in general
- Belongs to the class of  $\mathcal{NP}$ -complete problems
- Takes a long time to compute
- Requires huge amounts of computer memory
- We can not predict hardness in advance

# Research Questions.

- Can we implement an algorithm which uses less computer memory?
- Will it be efficient?
- What compromises must we make?

# The Method of Gröbner Bases

## Gröbner bases

- Transformation of one system of equations into another - a *Gröbner Basis* for the initial system.
- The Gröbner basis is in a triangular form.
- Triangular system is easy to solve.
- The Gröbner basis may be vary large.
- If initial system has  $N$  variables and degree  $D$ , Gröbner basis may have degree  $(N + 1)D - N$ .

## d-truncated Gröbner bases

- Degree restricted, i.e. *d-truncated* means degree  $\leq d$
- May not solve the system.

# Presentation of Two Ciphers

## LILI-128

- Stream cipher, 128 bits key
- Very simple design
- Weak output function  $\Rightarrow$  4-truncated Gröbner bases

## KASUMI

- Block cipher, 128 bits key
- 8 round Feistel network with block size 64
- Used in UMTS, GPRS and GSM
- S-box with cubic nonlinearity  $\Rightarrow$  3-truncated Gröbner bases
- Need to introduce intermediate(dummy) variables to reduce degree

# Results From Cryptanalysis

- Results: LILI-128
- Results: KASUMI

# LILI-128: System Of Equations

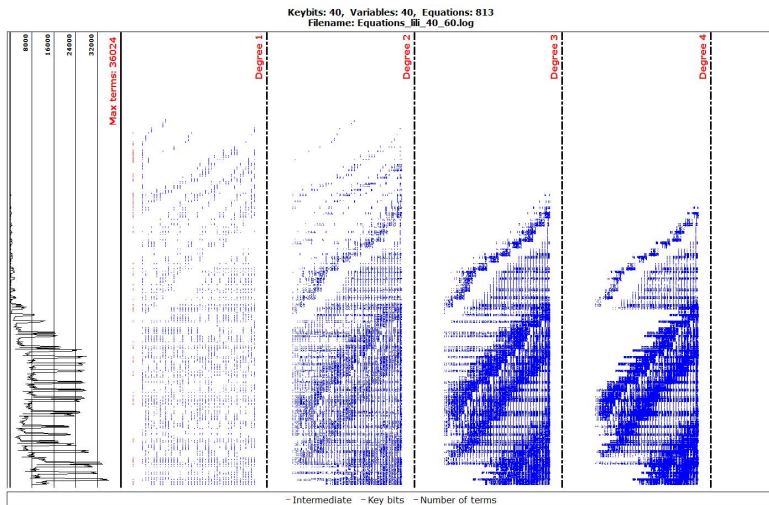


Figure: System of polynomials from 60 output bits.

# LILI-128: 4-truncated Gröbner Basis

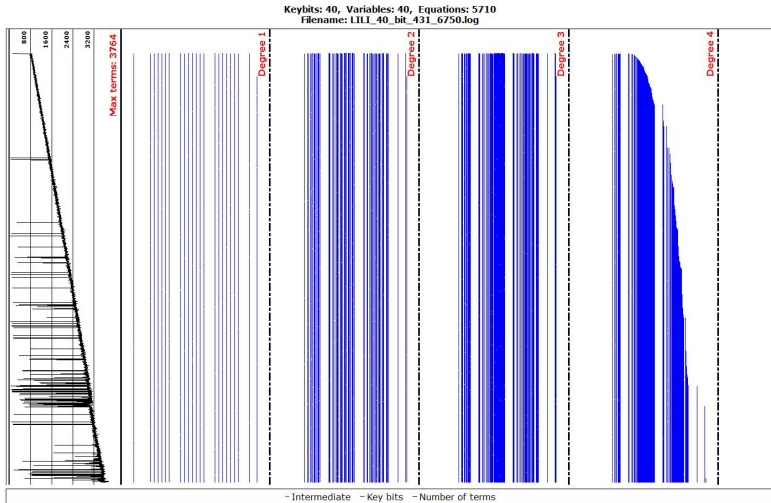
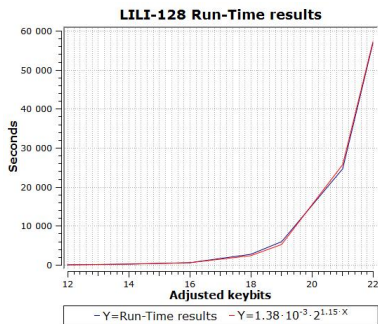
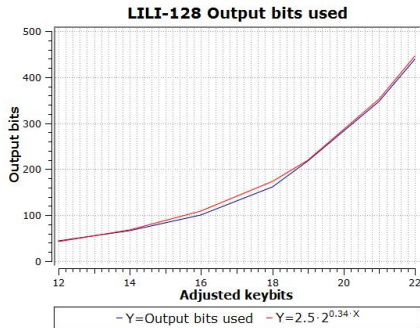


Figure: Dump of the current base after 431 output bits.

# LILI-128: Exponential Results



(a) Running time results

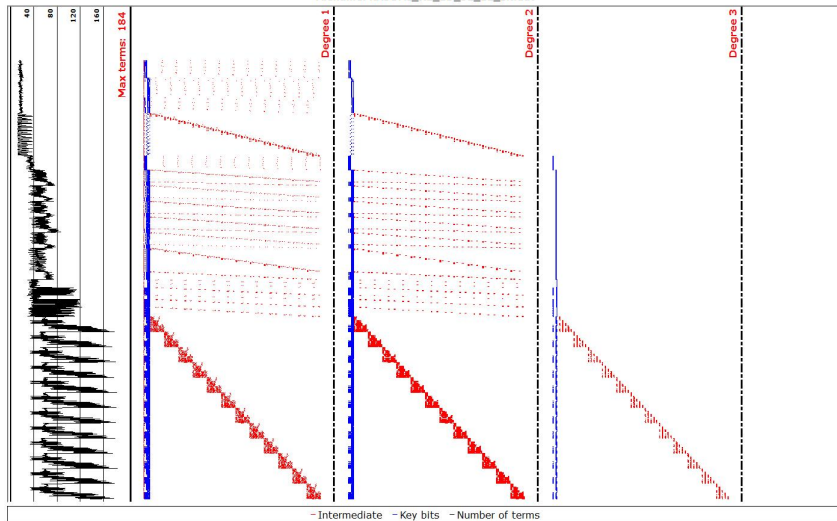


(b) Output bits used

Extrapolating, it will take 1 billion years to solve for 64 unknown keybits.

# KASUMI: System Of Equations

Keybits: 32, Variables: 992, Equations: 2689  
 Filename: KASUMI\_R2\_ED\_32\_12\_bit.dat



# KASUMI: 3-truncated Gröbner Basis

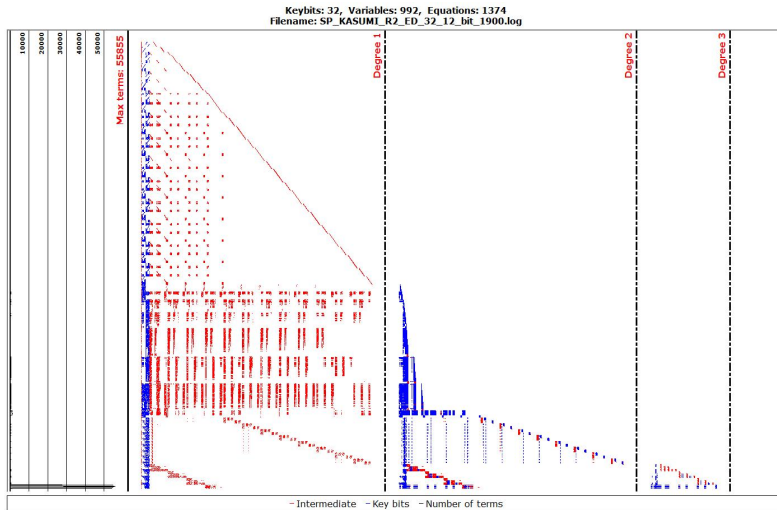
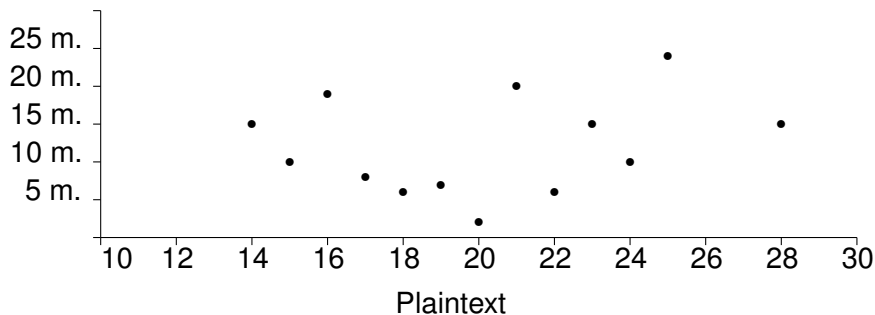


Figure: Dump of the current base after 1900 input polynomials.



# Plaintext/Ciphertext Pairs, 2 Rounds



**Figure:** Running time for two round KASUMI, 32 unknown key bits, with varying number of plaintext/ciphertext pairs

# Running Time Results for 2 Rounds

Unknown key bits	Pairs	Variables	Equations used	Time
32	20	1632	1150	1 min. 34 sec.
48	35	4528	2850	16 min. 4 sec.
64	40	5824	3700	46 min. 2 sec.
72	40	5832	3600	17 min. 13 sec.

**Table:** Systems of equations solved for two rounds. System of equations for 72 unknown keybits collapses in 17 minutes.

# Running Time Results for 3 Rounds

Unknown key bits	Pairs	Variables	Equations used	Time
<b>32</b>	<b>20</b>	<b>3552</b>	<b>2950</b>	<b>5 min. 38 sec.</b>
<b>40</b>	<b>30</b>	<b>6760</b>	<b>5500</b>	<b>1 hour 19 min.</b>
<b>48</b>	<b>40</b>	<b>9008</b>	<b>8000</b>	<b>17 hours 21 min.</b>

**Table:** Solved system of equations for three rounds

# Running Time Results for 3 Rounds

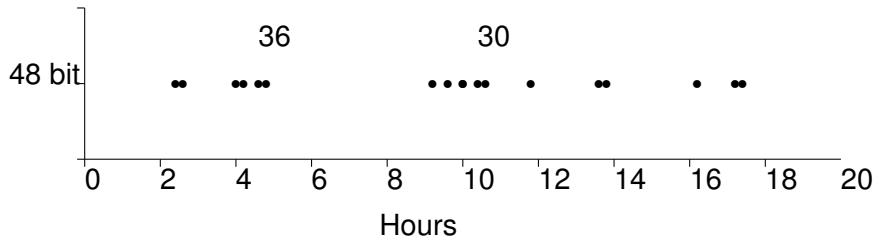


Figure: Timeline for three rounds, 48 unknown key bits

# Results, 4 rounds

- Can not solve even simple problems
- Huge number of intermediate variables
- This problem is not solvable by a 3-truncated Gröbner basis

# Summary

- Our implementation can attack large systems of polynomial equations without crashing
- We can attack some large systems of polynomial equations in a reasonable time, but the method has clear limitations
- The compromise for using 4-truncated Groebner bases for LILI-128 is an exponential number of output bits need to solve these systems.
- For KASUMI, using 3-truncated Groebner bases means we must stay below 4 rounds(!)

# The End

Thank You!  
Questions?