Numerical Solvers in Cryptanalysis

M. Lamberger, T. Nad, V. Rijmen

Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology
Inffeldgasse 16a, A-8010 Graz, Austria

Tomislav.Nad@iaik.tugraz.at
1 Motivation

2 Trivium (Bivium A)

3 Conversion Methods

4 Numerical Methods
Motivation

- Linear and differential cryptanalysis
  - Successful techniques to break many existing ciphers
  - New ciphers try to resist
  - New techniques needed

- Numerical solvers
  - Well researched
  - Fast and efficient
  - Working on real numbers
Basic Approach

$GF(2)$ equations

solution

$GF(2)$
Basic Approach

\[ \text{GF}(2) \]

equations

linear/differential cryptanalysis

solution

\[ \text{GF}(2) \]
Basic Approach

\[ GF(2) \]

conversion

\[ \mathbb{R} \]

equations

solution

\[ GF(2) \]
Basic Approach

$GF(2)$

equations

conversion

$R$

equations

numerical methods

$R$

solution

$GF(2)$

solution

M. Lamberger, T. Nad, V. Rijmen

WMC 2008

Numerical Solvers in Cryptanalysis
**Basic Approach**

- GF(2) equations
- Conversion
- R equations
- Numerical methods
- Solution
- Inverse conversion
- GF(2) solution
Motivation

Trivium (Bivium A)

Conversion Methods

Numerical Methods
Trivium and Bivium A

- Designed by Christophe De Cannière [1]
- Synchronous stream cipher
- eStream finalist
Trivium and Bivium A

- Designed by Christophe De Cannière [1]
- Synchronous stream cipher
- eStream finalist
- 288 bit internal state
Trivium and Bivium A

- Designed by Christophe De Cannière [1]
- Synchronous stream cipher
- eStream finalist
- 288 bit internal state
- Reduced variant by Raddum [4]
  - Bivium A
Trivium and Bivium A

- Designed by Christophe De Cannière [1]
- Synchronous stream cipher
- eStream finalist
- 288 bit internal state
- Reduced variant by Raddum [4]
  - Bivium A
- Attack
  - Known plaintext attack
  - Goal: state recovery
Keystream generation

For $i=1$ to $N$ do

\[ T_1 \leftarrow S_{66} + S_{93} \]
\[ T_2 \leftarrow S_{162} + S_{177} \]
\[ T_3 \leftarrow S_{243} + S_{288} \]
\[ Z_i \leftarrow T_1 + T_2 + T_3 \]

\[ T_1 \leftarrow T_1 + S_{91} \cdot S_{92} + S_{171} \]
\[ T_2 \leftarrow T_2 + S_{175} \cdot S_{176} + S_{264} \]
\[ T_3 \leftarrow T_3 + S_{286} \cdot S_{287} + S_{69} \]

\[ (S_1, S_2, \ldots, S_{93}) \leftarrow (T_3, S_1, S_2, \ldots, S_{92}) \]
\[ (S_{94}, S_{95}, \ldots, S_{177}) \leftarrow (T_1, S_{94}, S_{95}, \ldots, S_{176}) \]
\[ (S_{178}, S_{179}, \ldots, S_{288}) \leftarrow (T_2, S_{178}, S_{179}, \ldots, S_{287}) \]

end for
Keystream generation: Bivium A

For \( i = 1 \) to \( N \) do

\[
\begin{align*}
T_1 & \leftarrow S_{66} + S_{93} \\
T_2 & \leftarrow S_{162} + S_{177} \\
T_3 & \leftarrow S_{243} + S_{288} \\
Z_i & \leftarrow T_1 + T_2 + T_3 \\
T_1 & \leftarrow T_1 + S_{91} \cdot S_{92} + S_{171} \\
T_2 & \leftarrow T_2 + S_{175} \cdot S_{176} + S_{264} \\
T_3 & \leftarrow T_3 + S_{286} \cdot S_{287} + S_{69} \\
(S_{1}, S_{2}, \ldots, S_{93}) & \leftarrow (T_3, S_{1}, S_{2}, \ldots, S_{92}) \\
(S_{94}, S_{95}, \ldots, S_{177}) & \leftarrow (T_1, S_{94}, S_{95}, \ldots, S_{176}) \\
(S_{178}, S_{179}, S_{288}) & \leftarrow (T_2, S_{178}, S_{179}, S_{287})
\end{align*}
\]

end for
Keystream generation: Bivium A

For i=1 to N do

\[
T_1 \leftarrow S_{66} + S_{93}
\]

\[
T_2 \leftarrow S_{162} + S_{177}
\]

\[
T_3 \leftarrow S_{243} + S_{268}
\]

\[
Z_i \leftarrow T_1 + T_2 + T_3
\]

\[
T_1 \leftarrow T_1 + S_{91} \cdot S_{92} + S_{171}
\]

\[
T_2 \leftarrow T_2 + S_{175} \cdot S_{176} + S_{264}
\]

\[
T_3 \leftarrow T_3 + S_{286} \cdot S_{287} + S_{69}
\]

\[
(S_1, S_2, \ldots, S_{93}) \leftarrow (T_3, S_1, S_2, \ldots, S_{92})
\]

\[
(S_{94}, S_{95}, \ldots, S_{177}) \leftarrow (T_1, S_{94}, S_{95}, \ldots, S_{176})
\]

\[
(S_{178}, S_{179}, S_{288}) \leftarrow (T_2, S_{178}, S_{179}, S_{287})
\]

end for
Keystream generation: Bivium A

For \( i = 1 \) to \( N \) do

\[
T_1 \leftarrow S_{66} + S_{93}
\]
\[
T_2 \leftarrow S_{162} + S_{177}
\]
\[
Z_i \leftarrow T_2
\]
\[
T_1 \leftarrow T_1 + S_{91} \cdot S_{92} + S_{171}
\]
\[
T_2 \leftarrow T_2 + S_{175} \cdot S_{176} + S_{69}
\]

\[
(S_1, S_2, \cdots, S_{93}) \leftarrow (T_2, S_1, S_2, \cdots, S_{92})
\]
\[
(S_{94}, S_{95}, \cdots, S_{177}) \leftarrow (T_1, S_{94}, S_{95}, \cdots, S_{176})
\]

end for
Keystream generation: Bivium A

For i=1 to N do

\[
\begin{align*}
T_1 & \leftarrow S_{66} + S_{93} \\
T_2 & \leftarrow S_{162} + S_{177} \\
Z_i & \leftarrow T_2 \\
T_1 & \leftarrow T_1 + S_{91} \cdot S_{92} + S_{171} \\
T_2 & \leftarrow T_2 + S_{175} \cdot S_{176} + S_{69}
\end{align*}
\]

\[
(S_1, S_2, \cdots, S_{93}) \leftarrow (T_2, S_1, S_2, \cdots, S_{92})
\]

\[
(S_{94}, S_{95}, \cdots, S_{177}) \leftarrow (T_1, S_{94}, S_{95}, \cdots, S_{176})
\]

end for
Keystream generation: Bivium A

For $i=1$ to $N$ do

$T_1 \leftarrow S_{66} + S_{93}$

$T_2 \leftarrow S_{162} + S_{177}$

$Z_i \leftarrow T_2$

$T_1 \leftarrow T_1 + S_{91} \cdot S_{92} + S_{171}$

$T_2 \leftarrow T_2 + S_{175} \cdot S_{176} + S_{69}$

$(S_1, S_2, \ldots, S_{93}) \leftarrow (T_2, S_1, S_2, \ldots, S_{92})$

$(S_{94}, S_{95}, \ldots, S_{177}) \leftarrow (T_1, S_{94}, S_{95}, \ldots, S_{176})$

end for
System of Equations

- First round

\[
\begin{align*}
S_{162} + S_{177} + Z_1 &= 0 \\
S_{162} + S_{177} + S_{175} \cdot S_{176} + S_{69} + S_{178} &= 0 \\
S_{66} + S_{93} + S_{91} \cdot S_{92} + S_{171} + S_{179} &= 0
\end{align*}
\]

- 177 keystream bits \( Z_i \) needed for a fully determined system
- 327 equations and variables
  - 177 linear equations
  - 150 nonlinear equations
1 Motivation

2 Trivium (Bivium A)

3 Conversion Methods

4 Numerical Methods
Conversion: Requirements

- Convert from a normal form
  - Algebraic Normal Form
- A solution for the Boolean system should be a solution for the real system
- A solution for the real system should be a solution for the Boolean system
- Low degrees
- Simple as possible
Conversion Methods

- Standard Conversion

\[
GF(2) = \{0, 1\} \rightarrow \{0, 1\} \subset \mathbb{R} \\
X_1 \cdot X_2 \Rightarrow x_1 \cdot x_2 \\
X_1 + X_2 \Rightarrow x_1 + x_2 - 2 \cdot x_1 \cdot x_2
\]

- Multiplication in \( GF(2) \) becomes mult. in \( \mathbb{R} \)
- Increasing amount of monomials
- Increasing degree
- Multilinearity
Conversion Methods (cont’d)

- Fourier Conversion

\[ GF(2) = \{0, 1\} \rightarrow \{1, -1\} \subset \mathbb{R} \]
\[ X_1 \cdot X_2 \implies \frac{1}{2}(1 + x_1 + x_2 - x_1 \cdot x_2) \]
\[ X_1 + X_2 \implies x_1 \cdot x_2 \]

- Addition in \( GF(2) \) becomes mult. in \( \mathbb{R} \)
- Variables can cancel out \( (x^2 = 1) \)
- Increasing amount of monomials
- Increasing degree
Adapted Standard Conversion (ASC)

\[
\begin{align*}
S_{162} + S_{177} + Z_1 &= 0 & \text{Type I} \\
S_{162} + S_{177} + S_{175} \cdot S_{176} + S_{69} + S_{178} &= 0 & \text{Type II} \\
S_{66} + S_{93} + S_{91} \cdot S_{92} + S_{171} + S_{179} &= 0 & \text{Type II}
\end{align*}
\]

- Convert each type of equation separately
- Do not change the structure of the equations
- Keep the degree low
- Evaluate over \( GF(2) \) and over the reals
- Introduce new variables for each possible real value
ASC (cont’d)

\[ S_{162} + S_{177} = Z_i \rightarrow \begin{cases} 
S_{162} - S_{177} = 0 & \text{if } Z_i = 0 \\
S_{162} + S_{177} - 1 = 0 & \text{if } Z_i = 1 
\end{cases} \]
ASC (cont’d)

\[ S_{162} + S_{177} = Z_i \rightarrow \begin{cases} 
S_{162} - S_{177} = 0 \text{ if } Z_i = 0 \\
S_{162} + S_{177} - 1 = 0 \text{ if } Z_i = 1 
\end{cases} \]

\[ S_{66} + S_{93} + S_{91} \cdot S_{92} + S_{171} + S_{179} = 0 \]

\[ S_{328} \cdot (S_{66} + S_{93} + S_{91} \cdot S_{92} + S_{171} + S_{179}) = 0 \]

\[ S_{330} \cdot (S_{66} + S_{93} + S_{91} \cdot S_{92} + S_{171} + S_{179} - 2) = 0 \]

\[ S_{329} \cdot (S_{66} + S_{93} + S_{91} \cdot S_{92} + S_{171} + S_{179} - 4) = 0 \]

\[ S_{328} + S_{329} + S_{330} = 1 \]
ASC (cont’d)

\[ S_{162} + S_{177} = Z_i \rightarrow \begin{cases} 
S_{162} - S_{177} = 0 \text{ if } Z_i = 0 \\
S_{162} + S_{177} - 1 = 0 \text{ if } Z_i = 1 
\end{cases} \]

\[ S_{66} + S_{93} + S_{91} \cdot S_{92} + S_{171} + S_{179} = 0 \]

\[ s_{328} \cdot (s_{66} + s_{93} + s_{91} \cdot s_{92} + s_{171} + s_{179}) = 0 \]
\[ s_{330} \cdot (s_{66} + s_{93} + s_{91} \cdot s_{92} + s_{171} + s_{179} - 2) = 0 \]
\[ s_{329} \cdot (s_{66} + s_{93} + s_{91} \cdot s_{92} + s_{171} + s_{179} - 4) = 0 \]
\[ s_{328} + s_{329} + s_{330} = 1 \]

- 777 equations and variables
- Fewer monomials
- More equations and variables
- Maximum degree is 3
- New type of equations are linear
Other Conversion Tricks

- Convert each side separately

\[ S_{66} + S_{93} + S_{171} + S_{179} = S_{91} \cdot S_{92} \]
Other Conversion Tricks

- Convert each side separately
  \[ S_{66} + S_{93} + S_{171} + S_{179} = S_{91} \cdot S_{92} \]

- Split equations and Standard Conversion
  \[
  \begin{align*}
  S_{91} \cdot S_{92} & = R_1 \\
  S_{66} + S_{93} & = R_1 + R_2 \\
  S_{171} + S_{179} & = R_2
  \end{align*}
  \]
Other Conversion Tricks

- Convert each side separately

\[ S_{66} + S_{93} + S_{171} + S_{179} = S_{91} \cdot S_{92} \]

- Split equations and Standard Conversion

\[
\begin{align*}
S_{91} \cdot S_{92} &= R_1 \\
S_{66} + S_{93} &= R_1 + R_2 \\
S_{171} + S_{179} &= R_2 \\
S_{91}S_{92} - r_1 &= 0 \\
S_{66} + S_{93} - S_{66}S_{93} - r_1 - r_2 + 2r_1r_2 &= 0 \\
S_{171} + S_{179} - 2S_{171}S_{179} - r_2 &= 0
\end{align*}
\]
Conversion Methods: Comparison

\[ S_{66} + S_{93} + S_{171} + S_{179} + S_{91} \cdot S_{92} = 0 \]

Standard Conversion

\[
\begin{align*}
S_{171} + S_{179} - 2S_{171}S_{179} + S_{66} - 2S_{171}S_{66} - 2S_{179}S_{66} + \\
4S_{171}S_{179}S_{66} + S_{91}S_{92} - 2S_{171}S_{91}S_{92} - 2S_{179}S_{91}S_{92} + \\
4S_{171}S_{179}S_{91}S_{92} - 2S_{66}S_{91}S_{92} + 4S_{171}S_{66}S_{91}S_{92} + \\
4S_{179}S_{66}S_{91}S_{92} - 8S_{171}S_{179}S_{66}S_{91}S_{92} + S_{93} - 2S_{171}S_{93} - \\
2S_{179}S_{93} + 4S_{171}S_{179}S_{93} - 2S_{66}S_{93} + 4S_{171}S_{66}S_{93} + \\
4S_{179}S_{66}S_{93} - 8S_{171}S_{179}S_{66}S_{93} - 2S_{91}S_{92}S_{93} + \\
4S_{171}S_{91}S_{92}S_{93} + 4S_{179}S_{91}S_{92}S_{93} - 8S_{171}S_{179}S_{91}S_{92}S_{93} + \\
4S_{66}S_{91}S_{92}S_{93} - 8S_{171}S_{66}S_{91}S_{92}S_{93} - 8S_{179}S_{66}S_{91}S_{92}S_{93} + \\
16S_{171}S_{179}S_{66}S_{91}S_{92}S_{93} = 0
\end{align*}
\]
Conversion Methods: Comparison

\[ S_{66} + S_{93} + S_{171} + S_{179} + S_{91} \cdot S_{92} = 0 \]

Fourier Conversion

\[ \frac{1}{2} \left( S_{171} S_{179} S_{66} S_{93} + S_{171} S_{179} S_{66} S_{91} S_{93} + S_{171} S_{179} S_{66} S_{92} S_{93} - S_{171} S_{179} S_{66} S_{91} S_{92} S_{93} \right) = 1 \]
Conversion Methods: Comparison

\[ S_{66} + S_{93} + S_{171} + S_{179} + S_{91} \cdot S_{92} = 0 \]

Adapted Standard Conversion

\[ S_{328} \cdot (S_{66} + S_{93} + S_{91} \cdot S_{92} + S_{171} + S_{179}) = 0 \]
\[ S_{330} \cdot (S_{66} + S_{93} + S_{91} \cdot S_{92} + S_{171} + S_{179} - 2) = 0 \]
\[ S_{329} \cdot (S_{66} + S_{93} + S_{91} \cdot S_{92} + S_{171} + S_{179} - 4) = 0 \]
\[ S_{328} + S_{329} + S_{330} = 1 \]
Conversion Methods: Comparison

\[ S_{66} + S_{93} + S_{171} + S_{179} + S_{91} \cdot S_{92} = 0 \]

Splitting

\[ S_{91} S_{92} - r_1 = 0 \]

\[ S_{66} + S_{93} - S_{66} S_{93} - r_1 - r_2 + 2 r_1 r_2 = 0 \]

\[ S_{171} + S_{179} - 2 S_{171} S_{179} - r_1 = 0 \]
Summary for Bivium A

Standard Conversion
- 327 equations and variables
- Degree is 6
- High amount of monomials with high degree

Fourier Conversion
- 327 equations and variables
- Degree is 6
- Less monomials
- No variables cancel out

Adaptive Standard Conversion
- 777 equations and variables
- Degree is 3
- Low amount of monomials

Splitting
- 627 variables and equations
- Degree is 2
- Low amount of monomials
1 Motivation

2 Trivium (Bivium A)

3 Conversion Methods

4 Numerical Methods
Converted System: Facts

- Large systems of polynomials
  - Highly nonlinear, degrees between 2 and 6
  - Multilinear
  - Coefficients are 1
  - Sparse
  - Fully determined
  - Possible over-determined
  - Solution exists
    - $\in \{0, 1\}^n$ or $\in \{-1, 1\}^n$ respectively
  - Precomputed solution available
  - Continuously differentiable
    - Regular Jacobian in the solution
    - Ill-conditioned Jacobian
      - A lot of singular points
Converted System: Facts

- Large systems of polynomials
  - Highly nonlinear, degrees between 2 and 6
  - Multilinear
  - Coefficients are 1
  - Sparse
  - Fully determined
  - Possible over-determined

- Solution exists
- Solution is $\in \{0, 1\}^n$ or $\in \{-1, 1\}^n$ respectively
- Precomputed solution available
- Continuously differentiable
- Regular Jacobian in the solution
- Ill-conditioned Jacobian
- A lot of singular points
Optimization Problem

\[ \min \| F(s) \|^2 \]

Box-bounded optimization problem

\[ s, l, u \in \mathbb{R}^n \]

\( F: \mathbb{R}^n \rightarrow \mathbb{R}^n \)

Iterative algorithms

Starting point needed

Global and local convergence

Global and local optimum
Optimization Problem

\[
\min \| F(s) \|_2^2 \\
l_i \leq s_i \leq u_i \quad (i = 1, \ldots, n)
\]

- Box-bounded optimization problem
- \( s, l, u \in \mathbb{R}^n \)
- \( F : \mathbb{R}^n \rightarrow \mathbb{R}^n \)
- Iterative algorithms
- Starting point needed
- Global and local convergence
- Global and local optimum
Interior Reflective Newton Method [2]

- Box constrained problem
- Iterates are between upper and lower bounds
- Good global convergence
- Scales well with the system size
DIRECT Algorithm [3]

- Box constrained problem
- Global optimization, global search
- Good results on random systems
- Good results on systems with more than one global optimum
Experiments

- Bivium A
  - Standard
  - Fourier
  - ASC
  - Splitting

- Starting point
  - Random walk on the cube
  - Random in \((0, 1)\) or \((-1, 1)\) respectively
  - Guessing bits (variables)
## Results

<table>
<thead>
<tr>
<th>System</th>
<th>Starting point</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bivium A (F)</td>
<td>a,b</td>
<td>local optimum</td>
</tr>
<tr>
<td></td>
<td>c (250)</td>
<td>solution found</td>
</tr>
<tr>
<td>Bivium A (S)</td>
<td>a,b</td>
<td>local optimum</td>
</tr>
<tr>
<td></td>
<td>c (250)</td>
<td>solution found</td>
</tr>
<tr>
<td>Bivium A (ASC)</td>
<td>a,b</td>
<td>real-valued solution</td>
</tr>
<tr>
<td></td>
<td>c (580)</td>
<td>solution found</td>
</tr>
<tr>
<td>Bivium A (Splitting)</td>
<td>a,b</td>
<td>local optimum</td>
</tr>
<tr>
<td></td>
<td>c (470)</td>
<td>solution found</td>
</tr>
</tbody>
</table>

a Random in \( \{0, 1\}^n \) or \( \{-1, 1\}^n \) respectively

b Random in \( (0, 1)^n \) or \( (-1, 1)^n \) respectively

c Guessing bits (variables)
Conclusions

- Hard problem
- Converted systems are difficult
  - Large and highly nonlinear
- High influence on the system over the reals
- Many possibilities to model the problem over the reals
  - Mixed Integer Linear Problem
  - Mixed Integer Nonlinear Problem
  - Adding constraints to the problem
- High amount of different solvers/algorithms/strategies
- Does a real-valued solution contain useful information?
- Does a local optimum contain useful information?
Thank you for your attention!
References

Trivium: A stream cipher construction inspired by block cipher design principles.

On the convergence of interior-reflective newton methods for nonlinear minimization subject to bounds.

Lipschitzian optimization without the lipschitz constant.

Cryptanalytic Result on Trivium.
eSTREAM project. 2006.