

# The use of $k$ -best paths algorithms in clock control sequence reconstruction

Turid Herland

June 8, 2006

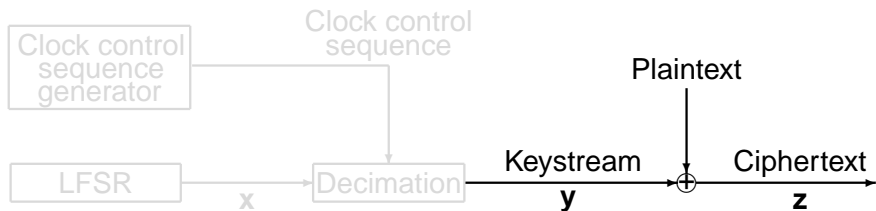
# Outline

- 1 Introduction
- 2 Contribution
  - Finding initial state of the LFSR
  - Clock control sequence reconstruction
- 3 Experiments
  - Purpose
  - Results
- 4 Conclusions

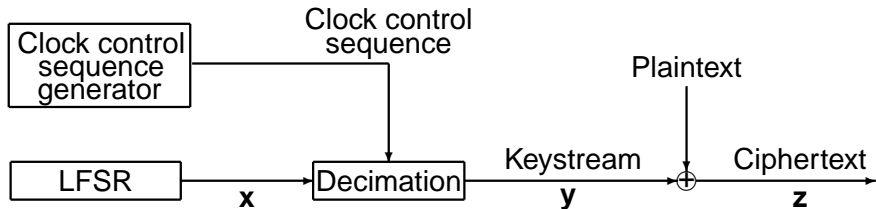
# Outline

- 1 Introduction
- 2 Contribution
  - Finding initial state of the LFSR
  - Clock control sequence reconstruction
- 3 Experiments
  - Purpose
  - Results
- 4 Conclusions

# Stream Cipher with Clock Controlled Keystream Generator



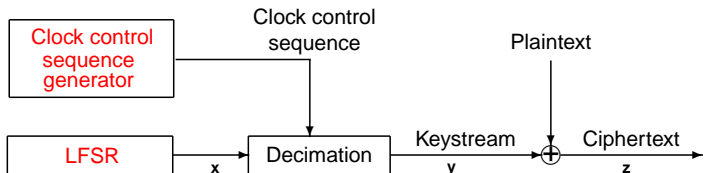
# Stream Cipher with Clock Controlled Keystream Generator



# Goal: Cryptanalysis

**Cryptanalysis:** To decrypt the ciphertext without knowledge of the secret key.

**Secret key:** Initial states of LFSR and clock control sequence generator.

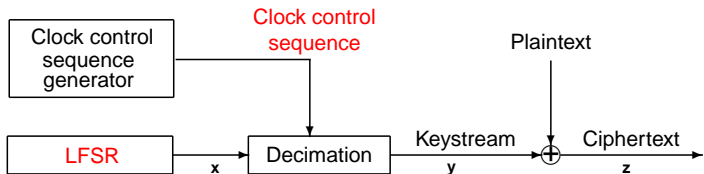


# Outline

- 1 Introduction
- 2 **Contribution**
  - Finding initial state of the LFSR
  - Clock control sequence reconstruction
- 3 Experiments
  - Purpose
  - Results
- 4 Conclusions

# Main contribution: Proposed attack

- Main contribution: New attack
- Attack has two phases:
  - 1 Find initial state of the LFSR
  - 2 Clock control sequence reconstruction



# Outline

- 1 Introduction
- 2 **Contribution**
  - Finding initial state of the LFSR
  - Clock control sequence reconstruction
- 3 Experiments
  - Purpose
  - Results
- 4 Conclusions

# Finding initial state of the LFSR

- Use existing method based on edit distances

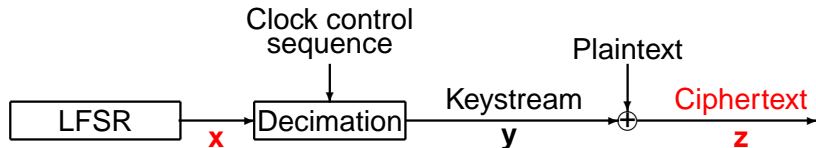
**Edit distance:** Number of deletions and substitutions needed to convert sequence  $x$  to ciphertext sequence  $z$ .



# Finding initial state of the LFSR

- Use existing method based on edit distances

**Edit distance:** Number of deletions and substitutions needed to convert sequence  $\mathbf{x}$  to ciphertext sequence  $\mathbf{z}$ .



# Outline

- 1 Introduction
- 2 **Contribution**
  - Finding initial state of the LFSR
  - **Clock control sequence reconstruction**
- 3 Experiments
  - Purpose
  - Results
- 4 Conclusions

# Edit distance matrix

$\mathbf{x} = 1010110111$ ,  $\mathbf{z} = 1101011$

| $e \backslash s$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|------------------|---|---|---|---|---|---|---|---|
| 0                | 0 | 0 | 1 | 2 | 3 | 4 | 4 | 5 |
| 1                | * | 2 | 1 | 1 | 1 | 2 | 3 | 3 |
| 2                | * | * | 4 | 3 | 2 | 2 | 2 | 2 |
| 3                | * | * | * | 6 | 5 | 4 | 3 | 3 |

# Example path in edit distance matrix

$\mathbf{x} = 1010110111$ ,  $\mathbf{z} = 1101011$

| $e \backslash s$ | 0     | 1 | 2         | 3 | 4 | 5 | 6     | 7 |
|------------------|-------|---|-----------|---|---|---|-------|---|
| 0                | 0 ← 0 | 1 | 2         | 3 | 4 | 4 | 5     |   |
| 1                | *     | 2 | 1 ← 1 ← 1 | 2 | 3 | 3 |       |   |
| 2                | *     | * | 4         | 3 | 2 | 2 | 2     | 2 |
| 3                | *     | * | *         | 6 | 5 | 4 | 3 ← 3 |   |

*k*-best paths problem: To find the *k* shortest paths between two given nodes in a graph.

# Example path in edit distance matrix

$x = 1010110111$ ,  $z = 1101011$

| $e \backslash s$ | 0     | 1 | 2         | 3 | 4 | 5 | 6     | 7 |
|------------------|-------|---|-----------|---|---|---|-------|---|
| 0                | 0 ← 0 | 1 | 2         | 3 | 4 | 4 | 5     |   |
| 1                | *     | 2 | 1 ← 1 ← 1 | 2 | 3 | 3 |       |   |
| 2                | *     | * | 4         | 3 | 2 | 2 | 2     | 2 |
| 3                | *     | * | *         | 6 | 5 | 4 | 3 ← 3 |   |

**$k$ -best paths problem:** To find the  $k$  shortest paths between two given nodes in a graph.

# Outline

- 1 Introduction
- 2 Contribution
  - Finding initial state of the LFSR
  - Clock control sequence reconstruction
- 3 Experiments**
  - Purpose
  - Results
- 4 Conclusions

# Outline

- 1 Introduction
- 2 Contribution
  - Finding initial state of the LFSR
  - Clock control sequence reconstruction
- 3 Experiments**
  - Purpose**
  - Results
- 4 Conclusions

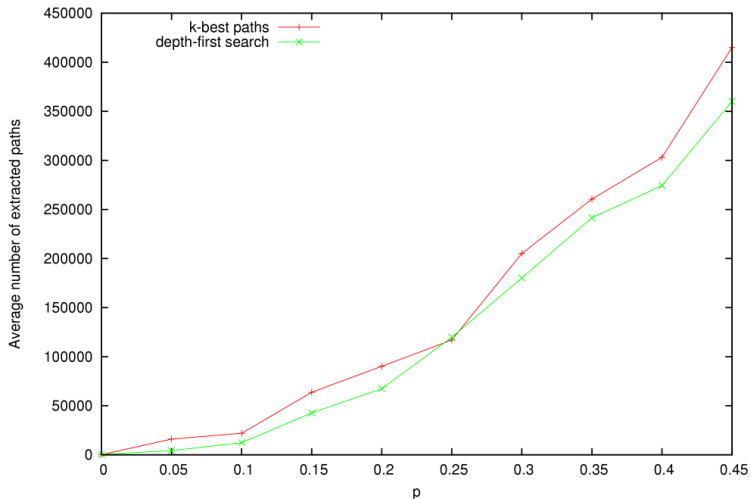
# Purpose of thesis/experiments

- Check whether the  $k$ -best paths attack finds the solution.
- Compare the performance of this attack to attack that uses depth-first search.

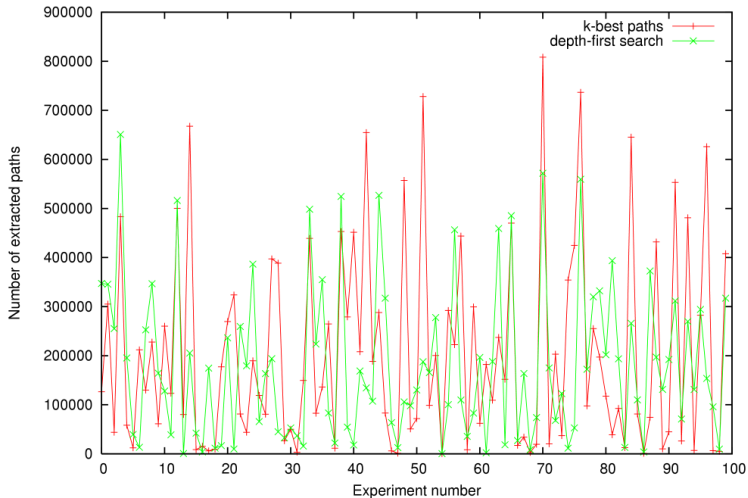
# Outline

- 1 Introduction
- 2 Contribution
  - Finding initial state of the LFSR
  - Clock control sequence reconstruction
- 3 Experiments
  - Purpose
  - **Results**
- 4 Conclusions

# Average number of extracted paths



# Number of extracted paths for individual experiments



# Outline

- 1 Introduction
- 2 Contribution
  - Finding initial state of the LFSR
  - Clock control sequence reconstruction
- 3 Experiments
  - Purpose
  - Results
- 4 Conclusions

# Conclusions

- It is possible to use  $k$ -best paths algorithms for clock control sequence reconstruction.
- The proposed attack performs similar to, but slightly worse than existing attack, on average.
- Outlook
  - Run several attacks in parallel.

# Conclusions

- It is possible to use  $k$ -best paths algorithms for clock control sequence reconstruction.
- The proposed attack performs similar to, but slightly worse than existing attack, on average.
- Outlook
  - Run several attacks in parallel.

# Thankyou

- I would like to thank professor Slobodan Petrović for suggesting the topic, and for all the help I have received during the work on the thesis.