RW778: Implementation and Application of Automata, 2006
Week 6 Lecture 1

L. van Zijl

Department of Computer Science
University of Stellenbosch

2006

Cryptology with $\oplus$-NFAs

References:

1. Chaudhuri, Design of CA-based Cipher System, Chapter 7 (and earlier chapters for terminology clarification)
2. Cryptanalysis, Chapter 42.
3. Van Zijl, $\oplus$-NFAs as Block Cipher Systems. Course notes.

Cryptology with $\oplus$-NFAs

- What is cryptology?
  - Plain text, encoding text, decoding text, key
- How good is a cipher? Cryptanalysis: study of breaking ciphers (read up on Turing's Enigma work).
- Stream-based vs block-based cipher systems.
- Relationship between unary $\oplus$-NFA and null-boundary XNOR CA

Cryptology with $\oplus$-NFAs

- Definition of $\oplus$-NFAs: $\delta(A, b) = \oplus_{q \in A} \delta(q, b)$

Cryptology with $\oplus$-NFAs

- Definition of $\oplus$-NFAs: $\delta(A, b) = \oplus_{q \in A} \delta(q, b)$
- Example:

δ	a
0	$\{0\}$
1	$\{0, 1\}$
2	$\{1, 2\}$
3	$\{2, 3\}$

Cryptology with $\oplus$-NFAs

- Definition of $\oplus$-NFAs: $\delta(A, b) = \oplus_{q \in A} \delta(q, b)$
- Example:

δ	a
0	$\{0\}$
1	$\{0,1\}$
2	$\{1,2\}$
3	$\{2,3\}$

- $$\begin{aligned} & 0 \to \overline{0} = 123 \to \overline{\{03\}} = 12 \to \overline{\{02\}} = 13 \\ & \to \overline{\{0123\}} = \emptyset \to \overline{\emptyset} = 0123 \\ & \to \overline{\{3\}} = 012 \to \overline{\{2\}} = 013 \to \overline{\{123\}} = 0 \end{aligned}$$

Cryptology with $\oplus$-NFAs

- Good rules:

Cryptology with $\oplus$-NFAs

- Good rules:
  - $\delta(q_i, a) = \overline{\{q_i\}}$, for $0 \leq i \leq n-1$.

Cryptology with $\oplus$-NFAs

- Good rules:
  - $\delta(q_i, a) = \overline{\{q_i\}}$, for $0 \leq i \leq n-1$.
  - $\delta(q_i, a) = \overline{\{q_i, q_{i+1}\}}$, for $0 \leq i \leq n-2$ and $\delta(q_{n-1}, a) = \overline{\{q_{n-1}\}}$.

Cryptology with $\oplus$-NFAs

- Good rules:
  - $\delta(q_i, a) = \overline{\{q_i\}}$, for $0 \leq i \leq n-1$.
  - $\delta(q_i, a) = \overline{\{q_i, q_{i+1}\}}$, for $0 \leq i \leq n-2$ and $\delta(q_{n-1}, a) = \overline{\{q_{n-1}\}}$.
  - $\delta(q_i, a) = \overline{\{q_{i-1}, q_i\}}$, for $1 \leq i \leq n-2$ and $\delta(q_0, a) = \overline{\{q_0\}}$.

Cryptology with $\oplus$-NFAs

- Good rules:
  - $\delta(q_i, a) = \overline{\{q_i\}}$, for $0 \leq i \leq n-1$.
  - $\delta(q_i, a) = \overline{\{q_i, q_{i+1}\}}$, for $0 \leq i \leq n-2$ and $\delta(q_{n-1}, a) = \overline{\{q_{n-1}\}}$.
  - $\delta(q_i, a) = \overline{\{q_{i-1}, q_i\}}$, for $1 \leq i \leq n-2$ and $\delta(q_0, a) = \overline{\{q_0\}}$.
- All cycles same and even length (permutation groups).

Cryptology with $\oplus$-NFAs

- Good rules:
  - $\delta(q_i, a) = \overline{\{q_i\}}$, for $0 \leq i \leq n-1$.
  - $\delta(q_i, a) = \overline{\{q_i, q_{i+1}\}}$, for $0 \leq i \leq n-2$ and $\delta(q_{n-1}, a) = \overline{\{q_{n-1}\}}$.
  - $\delta(q_i, a) = \overline{\{q_{i-1}, q_i\}}$, for $1 \leq i \leq n-2$ and $\delta(q_0, a) = \overline{\{q_0\}}$.
- All cycles same and even length (permutation groups).
- Each cycle forms permutation π of length $2r$.

Cryptology with $\oplus$-NFAs

- Good rules:
  - $\delta(q_i, a) = \overline{\{q_i\}}$, for $0 \leq i \leq n-1$.
  - $\delta(q_i, a) = \overline{\{q_i, q_{i+1}\}}$, for $0 \leq i \leq n-2$ and $\delta(q_{n-1}, a) = \overline{\{q_{n-1}\}}$.
  - $\delta(q_i, a) = \overline{\{q_{i-1}, q_i\}}$, for $1 \leq i \leq n-2$ and $\delta(q_0, a) = \overline{\{q_0\}}$.
- All cycles same and even length (permutation groups).
- Each cycle forms permutation π of length $2r$.
- Therefore, π^r gives mapping.

Cryptology with $\oplus$-NFAs: Algorithm
Algorithm

- Take k $\oplus$-NFAs M_i with 'good' rules, and such that all cycles same and even length.

Cryptology with $\oplus$-NFAs: Algorithm
Algorithm

- Take k $\oplus$-NFAs M_i with 'good' rules, and such that all cycles same and even length.
- Use M_i to construct permutations $p_1, p_2, \ldots, p_k$.

Cryptology with $\oplus$-NFAs: Algorithm
Algorithm

- Take k $\oplus$-NFAs M_i with 'good' rules, and such that all cycles same and even length.
- Use M_i to construct permutations $p_1, p_2, \ldots, p_k$.
- For all permutations p_i, calculate $p_i^{r_i}$.

Cryptology with $\oplus$-NFAs: Algorithm
Algorithm

- Take k $\oplus$-NFAs M_i with ‘good’ rules, and such that all cycles same and even length.
- Use M_i to construct permutations $p_1, p_2, \ldots, p_k$.
- For all permutations p_i, calculate $p_i^{r_i}$.
- Divide plaintext into blocks B_j.

Cryptology with $\oplus$-NFAs: Algorithm
Algorithm

- Take k $\oplus$-NFAs M_i with 'good' rules, and such that all cycles same and even length.
- Use M_i to construct permutations $p_1, p_2, \ldots, p_k$.
- For all permutations p_i, calculate $p_i^{r_i}$.
- Divide plaintext into blocks B_j.
- Apply function $p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}$ to each message block.

Cryptology with $\oplus$-NFAs: Algorithm
Algorithm

- Take k $\oplus$-NFAs M_i with 'good' rules, and such that all cycles same and even length.
- Use M_i to construct permutations $p_1, p_2, \ldots, p_k$.
- For all permutations p_i, calculate $p_i^{r_i}$.
- Divide plaintext into blocks B_j.
- Apply function $p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}$ to each message block.
- To decode, calculate $(p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k})^{-1}$ for each message block.

Cryptology with $\oplus$-NFAs
Example continued

- Let $k = 1$, and let the message blocks be 1111, 1010 and 0011.

Cryptology with $\oplus$-NFAs
Example continued

- Let $k = 1$, and let the message blocks be 1111, 1010 and 0011.
- Then the encoded message is 1110, 0001 and 1010.

Cryptology with $\oplus$-NFAs
Homework

Homework: Implement a system to encode and decode text using a block cipher based on $\oplus$-NFAs.