Journal of Scientific and Practical Computing
Vol.3, No.2 (2009) 3–22

On Weakly Invertible Semi-input-memory Finite Automata with Delay 2

Renji Tao

Institute of Software
Chinese Academy of Sciences
Beijing 100080, China
trj@ios.ac.cn

Abstract: Semi-input-memory finite automata are a generalization of input-memory finite automata by appending an autonomous finite automaton component. This paper gives a decision criterion of weakly invertible semi-input-memory finite automata with delay 2 of which the minimal output weight of length 2 and the sizes of input and output alphabets are identical. The results are used to generate a kind of weakly invertible semi-input-memory finite automata with delay 2 and to give other proofs of results in binary case. In addition, a frame of binary ciphers with delay 2 and bounded propagation is presented.

Keywords finite automata, semi-input-memory, invertibility

1. Introduction

Finite automata are regarded as a natural mathematical model of cryptographic systems. This stimulates the investigation of invertibility of finite automata, which has been received extensive attentions since 1950s (see the references of [5]). Among others, in [3] we introduce the concept of semi-input-memory finite automata for characterizing the boundness of the error propagation in decoding. Such a finite automaton is called a feedforward inverse if it is a weak inverse. (cf. [5 page 13 and §1.5]) Due to the equivalence between boundness of the error propagation in decoding and feedforward invertibility [3], the simplicity of semi-input-memory finite automata relative to general finite automata causes investigating the structure of feedforward inverses for the investigation of the error propagation. But the problem of the structure of feedforward inverses is not trivial. There are systematic results on this topic only in the case of small delay.

In [4], a decision criterion of feedforward inverse finite automata is presented which is used to characterize the structure of feedforward inverse finite automata with delay 0 and 1 in [4, 1, 2, 10] and binary ones with delay 2 in [11].

In [6], a result on mutual invertibility is given: for any stronger connected finite automaton with the same sizes of the input and output alphabets, it is a feedforward inverse if and only if it is weakly invertible. (cf. [5 page 56, Theorem 2.2.2]) Based on mutual invertibility, [7, 8] give another characterization of the structure of automata mentioned in previous paragraph, and [9] studies the structure of binary feedforward