셀룰러 오토마타를 이용한 LSB곱셈기 설계

하경주*, 구교민**

*경산대학교, **대구교육대학교

Design of a LSB Multiplier using Cellular Automata

Kyeoung-Ju Ha*, Kyo-Min Ku**

Dept. of Information processing, Kyungsan Univ. **Daegu Nationl Univ. of Education

요 약

GF(2m)상에서 모듈러 곱셈은 공개키 암호 시스템과 같은 응용에서의 기본 연산으로 사용된다. 본 논문에서는 이와 같은 모듈러 곱셈 연산을 셀룰러 오토마타를 이용하여, GF(2m)상에서 m 클럭 사이클만에 처리할 수 있는 연산기를 설계하였다. 이 곱셈기는 LSB 우선방식으로 설계되었으며, 지수연산을 위한 하드웨어 설계에 효율적으로 이용될 수 있을 것이다.