Embedded Tutorial

Applications of Reversible Logic in Cryptography and Coding Theory

Kamalika Datta, Bengal Engineering and Science University, Shibpur, India
Indranil Sengupta, Indian Institute of Technology, Kharagpur, India

Abstract

With the increasing emphasis on low-power design and quantum computation, research activities in the area of reversible logic synthesis and testing have gained momentum over the last couple of decades. It is expected that reversible logic will provide us with a viable alternative to building ultra-low power circuits and systems in not too distant future. In the classical works for synthesis of reversible circuits, gate libraries comprising of standard reversible gates like NOT, CNOT, TOFFOLI, FREDKIN, etc. are considered. To evaluate the goodness of a synthesized netlist, various metrics such as gate count, quantum cost, and equivalent transistor cost have been considered by various researchers. The synthesis approaches that have been reported can be broadly categorized into three groups: (a) exact synthesis approaches which try to obtain optimal reversible gate netlists, but can be used for small circuits only, (b) heuristic based approaches which try to utilize some domain knowledge intelligently to reduce the complexity of search, and can be used for somewhat larger circuits, and (c) synthesis approaches that rely on higher level functional representations like binary decision diagram (BDD) or exclusive sum-of-products (ESOP). The last approach is scalable to larger circuits (with 200 inputs or more), however, the synthesized netlist is not optimal and various rule-based heuristic approaches have been proposed to minimize the cost. There have been works also that report techniques for implementing sequential circuits with reversible properties, which will be useful for building complex systems containing finite-state machines.

There are various transformations that are carried out as part of cryptographic algorithms that are inherently reversible in nature. For instance, any block cipher that uses a key K to transform a plaintext P into a ciphertext C during encryption must be reversible, because decryption will be doing just the reverse (C to P). Also, in standard symmetric block ciphers like DES or AES, there is a combinational block called substitution box or S-box which is also reversible in nature. In AES, the S-box has 8 inputs and 8 outputs, and implements a one-to-one onto mapping. The same reversibility requirements hold for stream ciphers and public-key ciphers like RSA. Although not much work has been carried out in the area of reversible implementations of cryptographic algorithms, this can be a very good area for future research. Similar considerations hold for various coding and decoding techniques used in communication, which are also inherently reversible in nature. Some examples of such coding/decoding are Manchester, Differential Manchester, Bipolar AMI, 4B/5B, 8B/10B, Hamming error correcting code, etc. All these techniques can potentially be implemented using reversible logic circuits. Specific case studies of some of the areas as mentioned will be reported, with synthesis results.

Speaker Biographies

Kamalika Datta is presently pursuing her PhD degree from the Bengal Engineering and Science University, Shibpur, in the area of synthesis of reversible logic circuits. Previously she completed MS (by research) from the Indian Institute of Technology, Kharagpur, in the year 2010. She worked as an Assistant Professor in the KIIT University, Bhubaneswar, for one year prior to joining the PhD programme in June 2011. Her research interests include reversible logic circuits, network security and audio watermarking.

Indranil Sengupta has obtained his B.Tech., M.Tech. and Ph.D. degrees in Computer Science and Engineering from the University of Calcutta in the years 1983, 1985 and 1990, respectively. He joined the Indian Institute of Technology, Kharagpur, as a faculty member in 1988, in the Department of Computer Science and Engineering. He had been the former Heads of the Department of Computer Science and Engineering and also the School of Information Technology of the Institute. A Centre of Excellence in Information Assurance has been set up at IIT Kharagpur under his leadership, where leading edge research and development activities in cryptography and network security are being pursued. He has over 25 years of teaching and research experience. He has guided 13 PhD students, and has more than 100 publications to his credit in international journals and conferences. His research interests include cryptography and network security, VLSI design and testing, and mobile computing. He had been the General Chairs of Asian Test Symposium (ATS-2005), International Conference on Cryptology in India (INDOCRYPT-2008), International Symposium on VLSI Design and Test (VDAT-2012), and International Symposium on Electronic System Design (ISED-2012). His research interests include VLSI design and testing, and network security.