Call for Papers

Special Issue of Integration, the VLSI Journal: Hardware Architectures for Algebra, Cryptology and Number Theory

Guest Editors: Kris Gaj and Rainer Steinwandt

Submission Deadline: July 25, 2009

During the last years, the interaction of research in computer engineering with research in algebra and number theory has intensified. This interaction is especially visible in cryptography and cryptanalysis, but covers also other areas, such as coding theory, and signal and image processing.

Within cryptology, prominent examples include new hardware architectures for analyzing, attacking and implementing public key cryptosystems, such as RSA, Elliptic and Hyperelliptic Curve Cryptosystems and Pairing-based Schemes. Recent developments include theoretical and practical designs for implementing factoring and discrete logarithm algorithms, such as the Number Field Sieve, in hardware, efficient hardware architectures for primality testing and counting of points on elliptic and hyperelliptic curves, efficient algorithms for pairing computations over various fields and curve types, spectral modular multiplication methods for fast modular exponentiation, and many more.

Within coding theory, multiple error detection and correction codes, used in storage devices, mobile phones, broadband modems, satellite, deep space and military communication devices, etc., are based on algebraic principles. Prominent examples include linear block codes and convolutional codes, which are often implemented most efficiently in VLSI circuits.

Within digital image processing, numerous image processing and computer vision algorithms are based on algebraic techniques and require hardware acceleration for efficient processing. Numerous other examples of interactions between computer engineering and algebra can be found in the areas of artificial intelligence, bioinformatics, lossless and lossy compression, steganography, and many others. For this special issue, topics of particular interest include

- Algebraic attacks against block ciphers, stream ciphers, and hash functions
- Algebraic techniques countering fault attacks
- Algebraic techniques countering side channel attacks
- Efficient implementations of algebraic algorithms for compression in hardware
- Efficient implementations of error detection and error correction codes based on algebra and number theory
- Efficient implementations of image processing and computer vision algorithms based on algebraic methods
- Fast finite field arithmetic in hardware
- Fast modular arithmetic for very long integers
- Fast number field arithmetic in hardware
- Fast pairing arithmetic in hardware
- Hardware architectures for computing discrete logarithms
- Hardware architectures for elliptic and hyperelliptic curve cryptography
- Hardware architectures for factoring integers
- Hardware architectures for point counting on elliptic and hyperelliptic curves
- Hardware architectures for primality testing
- Hardware support in computational algebra and number theory
- Non-standard applications of computer algebra and their implementations in hardware

Submissions

Submitted manuscripts do not have to be anonymous, and each submission will be reviewed by at least three independent referees. All manuscripts should be submitted through the Elsevier Editorial Submission system (EES) at `http://ees.elsevier.com/vlsi/`, using the article type *SI: Hardware Architectures*. Submissions must contain original work and must not be in parallel under submission at a different journal or conference/workshop with proceedings. Extended versions of conference papers must add substantial novelty to the conference version. In particular, authors should ensure that there are no copyright problems with earlier publications.

For questions on this special issue, please feel free to contact one of the guest editors:

Kris Gaj: George Mason University, 4400 University Drive, Fairfax, VA 22030, `kgaj@gmu.edu`

Rainer Steinwandt: Florida Atlantic University, 777 Glades Road, Boca Raton, FL 33431, `rsteinwa@fau.edu`

Deadline

Submissions must be received by July 25, 2009.