Final report on EPSRC grant "Secure Design Flow" (EP/F016786/1)

School of Electrical, Electronic and Computer Engineering, Newcastle University

Principal Investigator: Professor Alex Yakovlev

Investigators: Dr Alex Bystrov and Dr Albert Koelmans

Research Associates: Dr Frank Burns, Dr Julian Murphy, Dr Andrey Mokhov, Dr Fei Xia and Dr Delong Shang

Project length: 1st Oct 2007 – 31st March 2011

Project value: £682,897

The project has made the following contributions:

(1) Models and techniques for higher radix circuits

Two major opportunities for improving the security-applied data path synthesis using *higher radix logic* have been investigated: conversion driven approach and pre-synthesis approach.

The conversion approach produces higher radix circuits from the binary netlists previously designed using standard tools. It is based on grouping binary gates into quaternary. A number of grouping approaches have been introduced and in [1]. Bitwise gate grouping algorithm has been presented in [2]. It was superceded by more computationally efficient operandwise gate grouping algorithm [3]. However, mixed radix parts of the circuit connected using a signal conversion logic introduced certain overheads to the overall power consumption. The determined reason was a premature optimisation done in the standard binary flow preceding the conversion. Hence, in order to minimise the impact of binary artefacts, the pre-synthesis approach has been considered as a primary target of the research. The principle of the pre-synthesis approach is multi-valued logic synthesis followed by exact mapping to power-balanced components [4]. The theoretical basis of the approach has been evolved into *mixed radix* Reed-Muller expansions that use Galois arithmetic. The first results have been achieved for the binary-to-quaternary case [5]. A tool for automated synthesis has been implemented [6] and integrated with other tools to form a secure design flow, which has been applied to an example and presented in [7,15].

Finally, a generalised theory of mixed radix Reed-Muller expansions has been developed. A journal paper submission has been made [8], however the final decision is still pending.

(2) Efficient RTL higher-radix models and architectures

In [10,13] a novel way of synthesizing efficient secure circuits was presented. A new design flow using 1-of-n encoding was presented as a means to provide more efficient power-balanced circuits than can be provided by dual- rail alone. We presented a new library of optimized power-balanced cells using N-nary 1-of-n logic which represented an improvement over dual-rail. The cells were efficient, regular and easy to power-balance and covered mixed 1-of-2, 1-of-4. A novel design flow was also presented, whereby, breakdown or refinement at the subfield level to generate small regular blocks created a suitable platform for efficient mapping to the 1-of-n library. The results indicated a significant improvement in area, time and power over dual-rail.

In [9,12] our novel design-flow to generate efficient secure balanced circuits was presented based on a new library of optimized power-balanced N-nary 1-of-n logic cells. The novel, partially automatic, design flow used 1-of-n encoding to provide efficient power-balanced circuits. These circuits were subsequently evaluated in terms of area, time, power and security. A novel evaluation metric, called PBCM, was presented based on differential power analysis and correlation power analysis which enabled a security comparison of our optimized circuits against other circuits.

The metric enabled us to construct a component library with better security. The results on average suggested our circuits provided at least similar and in many cases better (43%) security than other techniques.

In [11,14] a novel efficient way of implementing the AES algorithm using an approach which included registers and lookup tables was presented. This made use of the commutative relationship between inverse and square and lookup values. The results were promising, particularly for the AES which makes use of Galois inversion. As a result, the lookup size for inversion was reduced and minimal lookup tables in terms of their gate equivalent were used.
This represented a considerable reduction over previous architectures. The regular architecture was considered an important aspect for area, time and power tradeoffs in security, which facilitates security implementation.

(3) Software development

RMMixed [6] is a mixed radix synthesis tool based on fixed polarity Reed-Muller expansions over Galois field arithmetic. Taking into account the actual values for switching energy and area for arithmetic components, the synthesis tool searches for the optimal solution with respect to the gate level characteristics. An example component library for 1-of-n encoded logic is included.

The partially automated design-flow incorporates software for generating efficient 1-of-n balanced circuits from high-level specifications including Verilog and SystemC. Input specifications are in the form of Galois encryption modules which may be refined to smaller sub-modules. Sub-modules undergo logic optimization. Davio decomposition is first applied to sub-modules to generate decision graphs which are subjected to transformations including variable ordering and reduction and more specific transformations for optimal 1-of-n alignment. Efficient conversion into 1-of-n circuit netlists is then carried out using conversion routines. A mapping algorithm uses a priority list to assign complex gates to an optimized 1-of-n library. Subsequent searches are made to assign smaller more efficient gates. This enables the generation of highly efficient output targets including 1-of-4 and mixed 1-of-4, 1-of-2.

The output from this, in the form of verilog netlists, is subsequently converted using commercial tools such as Synopsys tools to SPICE netlists. The SPICE netlists may be subsequently linked to carefully designed SPICE libraries for security evaluation.

(4) From mathematical theory to hardware development

A new and novel way to address side-channel attacks was invented and researched termed Galois Encoded Logic. This links an aspect of the mathematical theory of cryptography to alternative and "high-radix" data-representations to: preserve security down to silicon; in an endeavour to reduce power and area overhead; resist side-channel analysis; and to allow secure hardware description language driven design and cryptographic IP cores.

This has been accomplished by noticing Galois Fields can be decomposed into subfields (also known as composite or tower fields). Then the chosen lowest order field element can be represented using a suitable m-of-n code for the given field size. For example, GF(4) has four elements and could be represented in a low-power one-hot encoding (1-of-4); alternatively where bit selection is desirable it could be represented as (2-of-4). To ensure security and balanced switching an all-zeros fixed-state must be passed between operations.

To build complete secure cryptographic algorithms the basic field operations (GF addition and multiplication) are then HDL coded in m-of-n logic in for the particular field. Logical cryptographic units can then be constructed based on the algorithm's decomposition into subfields. To ensure the fixed-state a secure HDL compatible wagging register design was invented and proposed. Dynamic logic implementation was also investigated and found to be particularly efficient and low power as the higher the m-of-n code the more complex the circuitry becomes.

To investigate the technology two mainstream private key algorithms were implemented in FPGA, Camillia (Japan's national encryption algorithm) and AES (United States national encryption algorithm). The AES implementation was later implemented in an AMS 0.35um process. It was found the novelty of wagging register design caused significant confusion for the clock synthesis tools during place and route. This meant the final silicon had unnecessary switching delay on the clock tree and did not perform as fast as a timing driven place and route. This aspect was known before submission of the chip; however it functioned correctly and showed a 10x improvement in security. The results of the chip and work based on secure HDL driven design inspired work on building synthesisable clock generators for Provable Uncloneable Functions and on-demand clocking.

The chip directly led to a follow-on-fund application and award with Renesas Technologies, where the remainder of this work continued under that grant for approx 18 months; where two further chips a 64-bit floating point FPU and another AES-128 were produced. Later a license of the M14k from MIPS technologies was also secured to integrate with the test chips. The work on Galois Encoded Logic has been patented by NU technology transfer office and licensed to a spin-out company i-GXL Ltd to develop secure IP cores. A KTS from NU was secured for this work for the remainder of the grant.

(5) Patent

"Cryptographic Processing and Processors", United States Patent Application 20100208885.

(6) Spin-out Company

iGXL Ltd – investigating viability of commercialising patented technology.

(7) ASIC

AES-128 0.35um - implements a Galois Encoded Logic AES-128 IP core. The chip was fabricated as mini@asic via Europractice.

References

[1] A. Rafiev, J. Murphy, D. Sokolov, and A. Yakovlev, “Investigating gate grouping algorithms for mixed radix conversion,” Technical Report NCL-EECE-MSD-TR-2008-132, Newcastle University, May 2008.
[2] A. Rafiev, J. Murphy, D. Sokolov, and A. Yakovlev, “Bitwise gate grouping algorithm for mixed radix conversion,” in 20th UK Asynchronous Forum, 2008.
[3] A. Rafiev, J. Murphy, D. Sokolov, and A. Yakovlev, “Conversion driven design of binary to mixed radix circuits,” in Proc. International Conference on Computer Design (ICCD 2008), IEEE CS Press, pp. 410-416, October 2008.
[4] A. Rafiev, J. Murphy, and A. Yakovlev, “RTL implementations of GF(2) and GF(4) arithmetic components,” Technical Report NCL-EECE-MSD-TR-2008-139, Newcastle University, December 2008.
[5] A. Rafiev, J. P. Murphy, and A. Yakovlev, “Quaternary Reed-Muller expansions of mixed radix arguments in cryptographic circuits,” in Proc. 39th International Symposium on Multi-Valued Logic (ISMVL 2009), Okinawa, Japan, pp. 370376, IEEE CS Press, 2009.
[6] http://async.org.uk/sure/rmmixed.
[7] A. Rafiev, J. Murphy, and A. Yakovlev, “Secure design flow for asynchronous multivalued logic circuits,” in Proc. to International Symposium on Multi-Valued Logic (ISMVL 2010) Barcelona, IEEE CS Press, pp. 264-269, May 2010.
[8] A. Rafiev, A. Mokhov, F. P. Burns, J. P. Murphy, A. Koelmans, and A. Yakovlev, “Mixed radix Reed-Muller expansions,” IEEE Trans. Comp., 2011. Submitted 2nd revision.
[9] F. Burns, A. Bystrov, A. Koelmans, and A. Yakovlev. Secure Generation and Evaluation of Balanced 1-of-n Circuits. IEEE Transactions on VLSI Systems 2011. In Press (available via IEEE Xplore).
[10] F. Burns, A. Bystrov, A. Koelmans, and A. Yakovlev. Design and Security Evaluation of Balanced 1-of-n Circuits. IET Computers and Digital Techniques (Accepted for publication).
[11] F. Burns, J. Murphy, A. Koelmans and A. Yakovlev. Efficient advanced encryption standard implementation using lookup and normal basis. IET Computers and Digital Techniques 2009, 3(3), 270-280.
[12] F. Burns, A. Bystrov, A. Koelmans, and A. Yakovlev. Design and security evaluation of balanced 1-of-n circuits. NCL-EECE-MSD-TR-2010-152, Microelectronic System Design Group, School of EECE, Newcastle University, March 2010.

[13] F. Burns, A. Bystrov, A. Koelmans, and A. Yakovlev. Secure Design Flow using 1-of-n Encoding. NCL-EECE-MSD-TR-2009-146, Microelectronic System Design Group, School of EECE, Newcastle University, May 2009.
[14] F. Burns, J. Murphy, A. Koelmans, and A. Yakovlev. Efficient AES Lookup Implementation using Normal Basis. NCL-EECE-MSD-TR-2008-128, Microelectronic System Design Group, School of EECE, Newcastle University, May 2008.
[15] A. Rafiev, J. P. Murphy, A. Yakovlev. Higher Radix and Mixed Radix Logic in Secure Devices, Proc. to e-Smart Conference, Sophia Antipolis, 2009