FINAL REPORT (GR/S81421/01)

Secure Circuit Design (SCREEN)

Prof. A.Yakovlev, Dr. A. Bystrov, Dr. A.M.Koelmans, Prof. D.J.Kinniment and Prof. M.Koutny
Schools of Electrical, Electronic and Computer Engineering (EECE) and Computing Science (CS), Newcastle University,
Merz Court, Newcastle-upon-Tyne, NE1 7RU, England
http://async.org.uk/

1 Background/Context

Secure hardware is currently designed using standard CAD tools that provide no support for incorporating security measures at the circuit level. As a result, even with advanced encryption algorithms, the products remain vulnerable to attacks at the circuit level. Such attacks are based on power consumption and electromagnetic emission analysis.

The timeliness of this research project is evidenced by the fact that it has been carried out in context with several international groups working in a similar direction, namely logic design styles, dual-rail encoding, transistor-level implementations for secure hardware. A large number of papers have been published over the last three years, including those at CHES'05-07 (cf. http://www.chesworkshop.org/) and DATE while a book entitled "Power Analysis" has been written as a by product of the larger European SCARD project (http://www.scard-project.eu/). Perhaps, the most distinctive aspects of our research in contrast with that of the others were:

(a) our novel circuit design solutions were taken to the level of physical implementation of demonstrator crypto-blocks (two VLSI chips have been designed, fabricated and tested by us, and in addition our industrial partners from Atmel also fabricated and tested their demonstrator circuits derived with the help of our tools).

(b) our design approach was incorporated into the standard RTL-based synthesis flow, which facilitated its rapid exploitation by our industrial partners.

Most of the other groups' research in secure circuit design has either stopped at the level of simulation or was far from industrial design automation, i.e. required significant alterations to the accepted design practices.

It would however be unfair to state that we and only we succeeded in achieving significant improvements in resistance to side-channel attacks by using masking. Currently, this problem has not found a universal solution and remains one of the hardest grand challenges as leading hardware security researchers admit (K.Tiri's talk at DAC'07). Indeed, it is now mandatory for devices requiring security certification to prove resistance to side-channel analysis. The recognised approach, rather than four years ago of outright prevention, is now to be one of best practice: information leakage is minimised so that significantly less data dependent power consumption occurs or secret data will not be compromised within the lifetime of the secret key. Since countermeasures come at the expense of other design factors or parameters increasing, which often make a solution impractical in commercial applications, where fixed-costs, design-effort and time-to-market dictate the actual security measures implemented. For example, if the attackers work factor exceeds the maximum number of transactions the device can perform, he cannot collect enough measurements to compromise the secret information. In reality no solution is leakless and will be imperfect in the sense that they leak some information due to the physics of the implementation technology.

2 Key Advances and Supporting Methodology

SCREEN's original aim was: "To develop a set of design methods and tools for enhancing the use of industrial EDA tools in the context of developing hardware for secure systems. The enhanced design flow will incorporate certain asynchronous techniques. The timing discipline will be considered along with other aspects affecting the circuit security at the logic level, such as for example the use of value-masking codes and techniques for randomisation in the value and time domain. Therefore, depending on the requirements for the design, the new flow would not stipulate complete abandoning of global clocking or any clocking for the entire system. In this way, our approach could be characterised as the *best-effort* synthesis of secure logic."

The project managed to adhere to this goal throughout, particularly focusing on the *secure data masking approach*, and development of theoretical models, new design methods, software tools and IC prototyping and testing to support this approach.

The project on the whole followed the original objectives of this project:

(a) Investigate models and techniques for power signature analysis currently used in industrial practice. Identify the potential for improvements at the algorithmic and circuit levels, particularly focusing on the use of power-balancing codes and timing schemes.

(b) Develop the syntax and semantics of a behavioural model to capture the security measures studied under (a). It will act as an intermediate model between the specifications in behavioural HDLs and structural descriptions for control, datapath and interface logic, produced in standard, industrially acceptable, notations. This model will be supported by verification and synthesis tools.

(c) Develop RTL-architectures for different types of codes, timing and pipelining disciplines, improving power-balancing and detection of injected faults against other competing criteria (power consumption, area, speed, testability). The architectures will be supported by appropriate design templates and component libraries.

(d) Develop a case study with a demonstrator of the new design flow. The application will be a smart card chip for the industrial partner (Atmel).

Methods developed in the course of work towards objectives (a) to (c) were meant to be implemented in software tools and interfaced to the industrial CAD toolkits (Synopsys, Cadence), enhancing the existing design flow.

We believe the project has made significant advances in all these objectives. Important foundations for this project were laid in [a1,a2], where the ideas of power balancing using dual-spacer dual-rail (DSDR) protocols with negative gate optimisation and new flip-flop designs were proposed, with a blueprint of the new tool for synthesis of power-balanced logic from standard RTL netlist. The project proceeded according to its plan.

2.1 Models and techniques for power signature analysis, power-balanced coding and timing schemes (objective a) [1,3,8,9,19,24]

Most of the research (cf. Tiri et al, Kulikowski et al) on secure data masking has used a leakage model of the power signature and a Differential Power Analysis (DPA) to measure the statistical correlation between logic functions and power signatures. We also followed this approach by measuring security at different levels of abstraction, particularly concentrating on developing new protocols for hazard free (monotonic) logic operation and associated timing schemes (cf. work to objective (c) – section 2.3). Here, we developed power balancing structures for both single (either all-zero *or* all-one) and alternating (all-zero *and* all-one) spacer dual-rail logic and memory elements, a variety of control logic and protocol converters (single spacer to alternating spacer) to embed into timing schemes, with globally clocked and self-timed interfaces [1,8,19,24]. We incorporated them later (see 2.3) in the context of RTL architectures and logic synthesis with standard cells.

On the other hand, we proposed and investigated novel energy-based (rather than power readings) metrics to characterise security at the gate-level [1,24]. These characteristics are *energy imbalance* and *exposure time*. Energy imbalance is measured as the variation of energy consumed by a circuit processing different data. Exposure time is the time during which the energy imbalance is exhibited. Basically, the longer the imbalance is visible, the easier it is to measure. We demonstrated by simulation and later by measuring our chips (see 2.4) that our alternating spacer dual-rail circuits, which have the property of invariance of the switching activity from the processed data *(all logic gates switch in every clock cycle),* and hence significantly reduce the energy imbalance and give the precise bound of the exposure time to be equal to the interval spacer0-codeword-spacer1. While it is arguable whether this property of logic with alternating spacer would make significant difference in resisting the DPA type of attacks, the balanced switching activity regardless of the processed data is by itself a valuable effect that needs to be further investigated in applications such as testing and debugging. We also modelled and analysed the effect of *early propagation* (ability of a gate to fire without waiting for all its inputs) and *memory effect* (ability of a CMOS gate to store its previous state) in logic gates on security. We indicated ways of using particular classes of dual-rail gate library (e.g. NCL-D) to restrict the early propagation effect, and found new ways of adding extra transistor stacks to reduce memory effects [9,25].

We have also considered masking security for system level design flow (see section 2.2), defining a “power balancing equation” which could characterise different levels of power balancing (PB) in terms of type of PB and the ratio of power balanced area of a particular PB type to the total circuit area [3]. A range of designs (AES blocks) were then analysed for different implementation technologies such as four types of DIMS and SABL, standard cell and full custom cells, with and without memory effects and with or without early propagation. The levels were also associated with the limit level of power bias spike.

2.2 Behavioural models for secure systems, incorporation of security into HDLs and synthesis tools (objective b)

This project involved collaborative effort of researchers with complementary expertise and skills, from theoretical computing science to electronic engineers. Thus, the ideas of secrecy and security by masking have been pursued by us at different levels of abstraction and different architectural paradigms.

Abstract level modelling: Opacity [14,15,16].

The notion of secrecy in both hardware and software has been formulated in various ways in the computer security literature. However, two views of security have been developed over the years by two separate communities. The first one starts from the notion of information flow, describing the knowledge an intruder could gain in terms of properties such as non-deducibility or non-interference. The second view was initiated by Dolev and Yao's work and focussed initially on security properties. The idea here is to describe properly the capability of the intruder. Some variants of secrecy appeared, such as strong secrecy, giving more expressivity than the security property but still lacking the expressivity of information flow concepts.

Recently, *opacity* has been shown to be a promising technique for describing and unifying security properties. The essential idea is that a predicate is opaque if an observer of the system will never be able to determine the truth of that predicate.

In [14] we considered opacity as a property of the local states of the secure (or high-level) part of the system, based on the observation of the local states of a low-level part of the system as well as actions.

We proposed a Petri net modelling technique which allows one to specify different information flow properties, using suitably defined observations of system behaviour. We also discussed expressiveness of the resulting framework and the decidability of the associated verification problems.

In [15] we generalised this treatment providing a framework in which to model various situations of importance in security, for example key compromise and refresh, downgrading of secrecy labels and conditional anonymity. We also demonstrated how global changes in the abstraction mappings can be used to model how some secrecy requirements depend on the status of the observer.

A further development on the prior work was to provide a more complete treatment of silent actions. Our initial approach was formulated in terms of Petri nets [14,15]. In [16] we extended it to the more general framework of labelled transition systems. We also proved a number of (un)decidability results, and present a novel technique (based on over- and under-approximations) which may allow model checking even though the problem at hand is in general undecidable.

Hardware Design models and synthesis flow based on SystemC and Petri nets [3,24,31].

The increasing complexity of today's systems incorporating security demand more elaborate synthesis techniques to close the productivity gap. Recent work towards creating a VLSI design flow for side-channel attack resistant circuits was primarily applied at the lower level and was targeted towards power-balanced synchronous circuits. In the SCARD project (Univ. Graz) they investigated side channel attacks at the lower level and concluded the best solution to power analysis is to embed countermeasures into logic cells. The aim of our synthesis approach was to translate specifications efficiently and dynamically from higher level specifications, i.e. SystemC specifications, into robust security implementations including asynchronous circuits (single-rail and dual-rail). This entails the use of security-aware scheduling and binding in order to explore the tradeoff between security, area and time. Here the synthesized implementations include components which exhibit varying degrees of protection based on the implementation technology.

Our synthesis flow [3] extends the existing SystemC framework by adding a high level SystemC library which provides for higher level security constructs (including asynchronous) enabling the construction of behavioural security specifications which are both modular and extensible. Our synthesis flow starts out with a SystemC modular behavioural description. The SystemC specifications are first compiled using a high level security library. After compilation the synthesis flow enters the stages of partitioning, and communication synthesis. At the core of the system is a novel security-aware scheduling and binding algorithm which allows for a trade-off between security, area and time. The global scheduling approach works by scheduling to a range of components which exhibit varying security levels i.e. the algorithm schedules to components of more than one technology type. The differences in security level of components are based on the different types of technology employed. The algorithm is implemented using simulated-annealing in which security type is included as an additional cost parameter. The energy function for this is taken as a function of the delay, area and percentage security type allocation. The scheduling and binding output is subsequently translated into an intermediate Petri net format (including security-annotated datapath nets). The intermediate format is used for the mapping of the specification into power-balanced and fault-protected circuits using asynchronous direct mapping methodologies [24,31]. These are used in conjunction with a dedicated library of hardware components. The design flow was tested on cryptographic hardware such as DES and AES (cf. 2.1) [2,3].

2.3 RTL architectures for power balancing (codes and timing disciplines), design templates, component libraries, error-detection (objective c) [1,2,4,7,10,11,12,13,22,24,25,26,30]

The two main classes of the RTL architectures which we used in this project were *clocked dual-rail* and *self-timed dual-rail* architectures. For both we further developed a library of logic conversion blocks, registers, pipeline controllers, based on single and alternating spacer protocols, and developed a range of acknowledgement methods ranging from strongly indicating to early propagation logic, developed heuristics and algorithms for optimising logic using negative gate library, reduced completion detection (based on path-based and layer-based relative timing assumptions) [1,2,4]. These were incorporated into the main software tool deliverable of this project VeriMap. The VeriMap design kit converts single-rail RTL netlists into dual-rail circuits which are resistant to DPA attacks, and successfully interfaces to the Cadence CAD tools. It takes as input a structural Verilog netlist file, created by Cadence Ambit (or another logic synthesis tool), and converts it into a dual-rail netlist. The resulting netlist can then be processed by Cadence or other EDA tools. All Design For Testability (DFT) features incorporated at the logic synthesis stage are preserved. All the details of the tools (documentation, conversion libraries, source code, benchmarks) and its distribution can be found on (http://async.org.uk/screen/verimap/). The toolkit has been used, in context with Synposys and Cadence tools, in the group to design a range of crypto-circuits (Sbox, DES, AES) for simulation-based experiments and real chip designs (cf. 2.4), as well as at Atmel Smart Card ICs, where several chips were designed, fabricated and evaluated (see letter from Atmel). The tool was also integrated into the BESST design flow [19] (developed earlier in the EPSRC grant BESST (http://www.staff.ncl.ac.uk/alex.yakovlev/home.formal/besst/project-summary.html) as an automatic tool for self-timed data-path.

Novel methods for the optimisation of fully indicating dual-rail logic (under NCL-D and NCL-X architectures) have been developed [7] using the notion of partial acknowledgement, which allows optimisation for both area and power, for standard gate libraries as well as custom-level libraries. This was realised in another software tool Indie (http://async.org.uk/screen/indie/).

Cryptographic designs which suffer from power analysis attacks are also susceptible to fault attacks. A design can be secured against power analysis attacks to only leak information through test and fault detection circuitry. The common method to detect faults is to duplicate hardware or complete encryption cores, and then compare the outputs for equality or use a form of self checking circuits; this makes the circuits a direct function of data. Note, unlike power analysis, the majority of faults cannot be prevented. They can only detected and then appropriate action should be taken inside the chip, such as system reset or halting execution. If the datapath is power-balanced new checking circuitry is required which is also power-balanced, therefore we developed and simulated power-balanced self-checking checkers for secure designs in [10,11]. New on-line IDDQ testing techniques have been proposed in [30], exploiting the switching activity invariance of the dual-spacer logic. We also developed C-element-based registers with enhanced tolerance to transient faults for asynchronous dual-rail RTL architectures, which improve on the existing structures in terms of the reduced interval of sensitivity to the SEU and transient faults, at relatively minor performance cost [13].

In the context of self-timed implementation of crypto-hardware we have investigated a method of timing randomization using a combination of metastability-based random number generator and variable delay-elements [22].

2.4 Case studies and demonstrators (objective d) [2,5,6,12,25]

We realised that with lack of prior experience in physical analysis of security, it would be of paramount importance for this project to spend significant proportion of our time on designing cryptographic blocks, taping out demonstrator chips and doing measurements. Being also rather closely linked with our industrial partners, we were able to see how cryptographic hardware is used as part of a SoC for smart card applications. The work here naturally split between designing cryptographic circuits by ourselves, as well as providing our expertise and software (VeriMap) for converting experimental designs for Atmel. Additionally, under the student placement programme of J. Murphy some circuit securitisation work was done for Sharp Laboratories. While the industrial case studies are protected by NDA, in this report we can refer to our developments, which mainly focused on such key components of symmetric cryptography as Sbox and AES. Two chips, SCREEN1 and SCREEN2, have been built (through Europractice) and tested (http://async.org.uk/chip-gallery.html). Power analysis on the device from SCREEN1 resulted in a forty-fold increase in the number of measurements needed to crack the 128-bit secret key over an unmodified and architecturally identical AES processor design [6]. Area is only increased by 88% compared to 3-4x in other reported power-balancing methods.

Another chip for testing designs using one-hot codes is now being prepared for submission.

We have also designed a fully self-timed AES processor [2,5]. The design reduces leakage of internal information through balanced power consumption, which is achieved by avoidance of glitches and by data-independent switching behaviour. The design utilises a pipeline structure with built-in controllers and novel, highly balanced security latches. The performance and power consumption (measured in terms of switching activities) of the asynchronous AES are 33% and 28% better than the synchronous one, respectively, although there is a modest area penalty (18%). The main reason why the asynchronous version is so much better is that in the synchronous implementation the transition from data to spacer takes half a clock cycle. On the applications side associated with wireless sensor networking, we started investigations of tradeoffs between security and low power design criteria. We have developed an asynchronous version of MSP430 processor using the Handshake Solutions methodology and tools (HASTE) and compared it with the synchronous solution showing real benefits in terms of power consumption [12].

3 Project Plan Review

All aspects of the SCREEN work plan have been duly addressed. In terms of expected deliverables the project has been very productive. There has been 4 journal and 12 peer-reviewed international conference papers, 7 UK Asynchronous and Embedded Forums papers, a large number of Newcastle postgraduate conference presentations and papers and technical reports, three PhD theses (one awarded and two completed).

4 Research Impact and Benefits to Society

Information security is an increasingly societal issue, affecting every member of society through mobile devices, smart cards, passports etc. As discussed above in section 1, electronics must be designed with security measures embedded at all levels. This project has put emphasis on circuits design resistant to side-channel attacks, and gave a way to incorporating new circuit solutions into the industrial strength EDA tools. On the practical side, through the exploitation route with Atmel, the project has already made a strong impact on the way how secure hardware is designed. As shown below in Section 6, several academic organisations in UK and abroad have expressed interest in our software tools and downloaded VeriMap. The experience gained in SCREEN on developing tools for converting synchronous RTL to asynchronous implementation has also helped us to extablish close collaboration with a new EDA start-up Elastix Corporation, who have placed a R&D consultancy for six months at Newcastle. During Summer 2006 our PhD student J. Murphy worked at Sharp Labs of Europe (Oxford), where he was involved in hardening security of smartcard processor designs. We have also initiated discussions with the University's Technology Transfer Office (TTO), due to the strong link and application to the smartcard industry, to investigate the commercial application and economic potential of some of the methods developed in SCREEN (see section 6). On a broader scale, these results will be useful to the UK and international research in microelectronics system design, testing and dependable hardware, supported by EPSRC and EU grants.

5 Explanation of Expenditure

The expenditure plans in the original proposal have been followed without significant changes. A minor change (less than 10%) was the relocation of some of the equipment and salaries budget in order to cover the shortfall on travel and student maintenance. The latter was made possible thanks to savings made on the acquisition of a powerful oscilloscope (6GHz Infinium) from Agilent with partial help of the School’s SRIF funds and due to the replacement of a senior RA (D. Shang, who moved to another project) by a junior RA (J. Murphy) in the final year of the project. The project provided excellent opportunity for active involvement of several PG students (D. Sokolov, J.Murphy – main work on secure circuit design, Y. Zhou – main work on dual-rail area and speed optimizations, B. Halak – on online testing, E. Michalodimitrakis – who started work on security metrics, but left PhD after the first 6 months was replaced by P. Wang, now working on delay and power modelling) and even UG students (C. Hoggins, who is currently on our PhD list). With the involvement of a large number of research manpower in this project, it was inevitable that the demand for conference travel (DATE, IOLTS, ASYNC, ICCAD, PATMOS, ACiD-WG, UK Async and Embedded Forums) was higher than anticipated in the proposal.

6 Further Research or Dissemination Activities

VeriMap has already been used not only by ourselves and our industrial partners (Atmel) but a number of organisations who downloaded this toolkit and sent us various queries, amongst them Universities of Cambridge, Manchester, Southampton, Virginia Polytechnic, University of Bologna. This research has already been taken to the next stage of development for a more mature design flow for secure systems, and an EPSRC grant has been awarded (EP/F016786/1 – Project SURE, http://async.org.uk/sure/). This research will benefit our project with Self-timed Datapath Synthesis (SEDATE, EP/D053064/1) in collaboration with Universities of Manchester and Edinburgh and two companies, FTL Systems and Silistix. Our research on behavioural models of secure systems (objective (b), see 2.1) has helped us to develop long-term vision for laying a foundation for “security calculus” (this goal is currently being pursued in a FP7 project proposal, where Newcastle will act as a leading organisation).

Besides papers and conference presentations at IFIP Congress, CHES, DATE, ESSCIR, ECCTD, ASYNC, ICCAD, IOLTS, PATMOS, this research has had its impact on Adv. Tutorial on Hardware Design and Petri Nets at ATPN in Miami, June 2005, ACiD-WG Winter school in Cambridge in Jan. 2005, presentation of design tools at DATE 2005 in Munich, series of invited lectures at the Xidian University, Xi’an, China and Institute of Electronics, Chinese Academy of Sciences, Beijing in March-April 2006. The team members have also co-organised three UK Embedded Forums [28,29, http://async.org.uk/ukef07/], and hosted UK Asynchronous Forum [http://async.org.uk/ukasyncforum18/].

There have been a number of positive meetings with key people contributing to the exploitation route to date, where advice and guidance has been given; specifically on technology licensing and spin-out company formation. To this end, Newcastle TTO has appointed an external market research company, who have a dedicated smartcard market research section, to conduct a full market analysis and suggest an appropriate course of action (initial feedback has suggested the next generation contactless market may be particularly applicable). They have also sought external advice on protecting the ideas from intellectual property lawyers specialising in cryptography, who have confirmed the potential application. The next suggested step is to approach the key industry figures and initiate research and development programmes, while developing a suitable business plan. Newcastle TTO is also planning to make an application for a Follow-on Fund scheme in Feb. 2008.

Project publications

[1] D. Sokolov, J. Murphy, A. Bystrov and A.Yakovlev, "Design and Analysis of Dual-Rail Circuits for Security Applications", IEEE Transactions on Computers, Vol. 54, No.4, pp. 449-460, April 2005.

[2] D. Shang, F.Burns, A. Bystrov, A. Koelmans, D. Sokolov and A. Yakovlev. High-security asynchronous circuit implementation of AES, IEE Proceedings, Computers and Digital Techniques, vol.153, No.2, March 2006, pp. 71-77.

[3] F. Burns, J. Murphy, D. Shang, A. Koelmans and A. Yakovlev. Dynamic global security-aware synthesis using SystemC, IET Computers and Digital Techniques, July 2007, Vol. 1, Issue 4, pp 405-413.

[4] D. Shang, A. Yakovlev, A. Koelmans, D. Sokolov and A. Bystrov. Registers for Phase Difference Based Logic, IEEE Trans on VLSI Systems, vol. 15, no. 6, pp. 720-724, June 2007.

[5] D. Shang, F. Burns, A. Bystrov, A. Koelmans, D.Sokolov and A.Yakovlev. A low and balanced power implementation of the AES security mechanisms using self-timed circuits, PATMOS 2004, Santorini, LNCS 3254, pp. 471-480.

[6] J. Murphy and A. Yakovlev. An Alternating Spacer AES Crypto-Processor, Proc. of ESSCIR 2006, Montreux, Switzerland, Sept. 2006, pp. 126-129.

[7] Y.Zhou, D. Sokolov and A. Yakovlev, Cost-Aware Synthesis of Asynchronous Circuits Based on Partial Acknowledgement, Proc ICCAD'06, San Jose, November 2006,pp.158-163.

[8] D. Sokolov, J.Murphy, A.Bystrov and A. Yakovlev. Improving the security of dual-rail circuits, Proc. CHES 2004, M. Joye and J.-J. Quisquarter (Eds), Boston, August 2004, LNCS 3156, Springer, pp. 282-297.

[9] J. Murphy, A. Yakovlev, Power-balanced Asynchronous Logic, Proc. 17th European Conference on Circuit Theory and Design (ECCTD), 29 August - 2 September 2005.

[10] J. Murphy, A. Bystrov and A.Yakovlev, Self-Checking Circuits for Security Applications, 11th Annual International Mixed-Signals Testing Workshop (IMSTW'05), Cannes, France, June 2005, pp. 278-285.

[11] J. Murphy, A. Bystrov and A. Yakovlev, Power-balanced Self Checking Circuits for Cryptographic Chips, Proc. 11th International Online Testing Symposium (IOLTS'05), St. Rafael, France, July 2005, IEEE CS Press, pp. 157-162.

[12] D. Shang, C.H. Shin, P. Wang, F. Xia, A. Koelmans, M.H. Oh, S. Kim, and A. Yakovlev, Asynchronous Functional Coupling for Low Power Sensor Network Processors, PATMOS 2007, Gothenburg, Sweden, LNCS 4644, pp.53-63.

[13] K. T. Gardiner, A. Yakovlev and A. Bystrov, A C-element Latch Scheme with Increased Transient Fault Tolerance for Asynchronous Circuits, 13th IEEE International On-Line Testing Symposium (IOLTS 2007), July 2007, Heraklion, Crete, Greece, IEEE CS Press, pp. 223-230

[14] J.W.Bryans, M.Koutny and P.Y.A.Ryan, Modelling Dynamic Opacity using Petri Nets with Silent Actions. In IFIP TC1 WG1.7 Workshop on Formal Aspects in Security and Trust (FAST), World Computer Congress. IFIP International Federation for Information Processing, Volume 173 pp. 159-172 Springer Verlag 2005

[15] J.W.Bryans, M.Koutny and P.Y.A.Ryan, Modelling Opacity Using Petri Nets. Electronic Notes in Theoretical Computer Science, Volume 121, pp 101-115. Elsevier Science Publishers BV, 2004; Proc. WISP 2004.

[16] J.W.Bryans, M.Koutny, L.Mazaré and P.Y.A.Ryan, Opacity Generalised to Transition Systems. In Formal Aspects in Security and Trust: Third International Workshop, FAST 2005. LNCS 3866 pp. 81-95 Springer 2006

[17] Ping Wang, Alex Yakovlev, Refined Delay Model for Geometric Program-based Delay Optimization, 19th UK Asynchronous Forum, London, September 2007.

[18] D. Sokolov, A. Bystrov, A. Yakovlev**.** Design for low-power and high-security based on timing diversity, Proc. 2nd UK Embedded PhD Forum, Birmingham, October 2005; ISBN 0-7017-0191-9

[19] J.P. Murphy, D. Sokolov, A. Bystrov and A. Yakovlev, Resisting Side Channel Attacks Using Dual Spacer Dual Rail, 16th UK Asynchronous Forum, Manchester, Sept. 2004.

[20] Y. Zhou and A. Yakovlev. Design of an Asynchronous Sequence Generator with Dynamically Loadable Count Ratio, 16th UK Asynchronous Forum, Manchester, September 2004.

[21] A. Mokhov, D. Sokolov, A. Yakovlev, Completion Detection Optimisation based on Relative Timing, 18th UK Asynchronous Forum, Newcastle, September 2006

[22] C. Hoggins, C. D'Alessandro, D.J. Kinniment, and A. Yakovlev, Securing On-chip Operations against Timing Attacks, NCL-EECE-MSD-TR-2005-108, Microelectronic System Design Group, School of EECE, University of Newcastle upon Tyne, September 2005.

[23] D. Koppad, D. Shang, A. Bystrov, A. Yakovlev, Asynchronous Checker Designs for monitoring Handshake Interfaces, NCL-EECE-MSD-TR-2005-104, Microelectronic System Design Group, School of EECE, University of Newcastle upon Tyne, March 2005.

[24] D. Sokolov, Automated Synthesis of Asynchronous Circuits Using Direct Mapping for Control and Data Paths, PhD Thesis, Newcastle University, NCL-EECE-MSD-TR-2006-111, January 2006.

[25] J. Murphy, Standard Cell and Full Custom Power-Balanced Logic: ASIC Implementation, PhD Thesis, submitted September 2007, viva due 3 Dec. 2007.

[26] Yu. Zhou, Automatic Synthesis and Optimisation of Asynchronous Data Paths Using Partial Acknowledgement, PhD Thesis, submitted November 2007, viva due 8 January 2008.

[27] E. Michalodimitrakis, Asynchronous Secure Hardware Design, Postgraduate Conference (PGC'05), School of EECE, Newcastle University, January 2005.

[28] A. Koelmans, A. Bystrov, M. Pont (Eds). Proc. First UK Embedded Forum, NEC, Birmingham, October 2004. Newcastle University, ISBN 0-7017-0180-3 (http://www.staff.ncl.ac.uk/albert.koelmans/books/firstukembforum.pdf).

[29] A. Koelmans, A. Bystrov, M. Pont, R. Ong, A. Brown (Eds). 2nd UK Embedded Forum,NEC, Birmingham, Oct.2005, Newcastle Univ., ISBN 0-7017-0191-9 (http://www.staff.ncl.ac.uk/albert.koelmans/books/secondukembforum.pdf).

[30] J. Murphy and A.Bystrov. On-line IDDQ testing of security circuits, Second UK Embedded Forum, Proceedings, NEC, Birmingham, October 2005, University of Newcastle upon Tyne, ISBN 0-7017-0191-9

Additional references

[a1] A. Bystrov, D. Sokolov, A. Yakovlev and A. Koelmans, Balancing power signature in secure systems, Fourteenth UK Asynchronous Forum, Newcastle, June 2003

[a2] A. Yakovlev, A. Bystrov, D. Sokolov, J. Murphy, V. Varshavsky and V. Marakhovsky, Phase-difference based logic: principle and applications, Workshop of ACiD-WG Working Group, Turku, Finland, June 2004.

7 Reports from Project Partners

A letter from Atmel is attached as a separate document.