
**AlaRI Master Projects
2003-2004**

Security

1. Design Space Exploration for the FOX Encryption Algorithm

Abstract: Among the whole class of cryptographic algorithms, symmetric key block ciphers are often used to provide good security with low complexity, especially considering dedicated hardware implementations. FOX is a novel block cipher family, which has many interesting features and is specifically targeted to multimedia streaming encryption. Different choices can be made for the parameters of the cipher architecture in order to scale the security and the performance of the cipher. The goal of this project is to implement the FOX algorithm in custom silicon, using the technology libraries installed at ALaRI; different optimizations will be applied on the hardware architecture, in order to satisfy different constraints in terms of latency, area occupation, security and possibly power consumption. A thorough discussion of the trade offs between the various implementations will also be carried out, highlighting the similarities and the main differences from the AES algorithm.

2. Developing Concurrency for a Crypto-Accelerator

Abstract: So far the concurrency have not been considered for the crypto-accelerator. If this may not be a problem for some usage scenarios, it is for others. Concurrency needs to be studied not to degrade performance of the system. QoS should also be taken into account for developing this topic. In this context, concurrency means usage of a single accelerator by more than one concurrent processes. Goal of the project is to develop concurrency for the ST accelerator and possibly to modify the accelerator's driver (if provided).

3. Exploration and hardware Implementation of Exponentiation for Cryptographic Applications

Abstract: The search for new public-key schemes, improvements to existing cryptographic mechanisms and proofs of security is continuing at a rapid pace. Various standards and infrastructures involving cryptography are rapidly increasing. Security products are getting more importance as the security need of the information intensive society is increasing.

Arithmetic of finite fields is used in various applications such as Diffie-Hellman and pseudo random bit generators. It is also learned that exponentiation is most time consuming and complex arithmetic operation for Key exchange, digital signatures and authentication. So exponentiation becomes a critical operation to be given high intensity of attention. In fact one can device an efficient algorithm since a fixed number is many different powers in exponentiation.

This project will start with focusing on architecture for exponentiation on $GF(2^n)$. Then various techniques for efficient exponentiation will be studied and implemented. Also various experiments on changing the base operator P of $GF(p^n)$ are expected to take place in final steps.

4. Study of the new Linux IPSec implementation

Abstract: Aim of this project is to provide a detailed study of the new IPSec implementation provided in the 2.6 series of the Linux kernel. Particular focus has to be put on the use of the cryptographic API, to discover differences with the implementation provided with FreeS/WAN, the 2.4 kernel series IPSec implementation.

5. Study and Optimization of an IPSec Accelerator Usage Based On Dimension Of IP Datagrams

Abstract: IPSec accelerator performance may heavily depend on packets dimension. In many cases the time needed to transfer data and to set up the accelerator is higher than the time to process the packet (e.g. to encrypt) in software. Main goal of this project is to develop an algorithm for co-processor usage optimization. Simulations need to be performed both to demonstrate the algorithm and to tune its parameters.

6. IPSec in a Mobile IPv6 Environment

Abstract: IPSec is an important part of the Mobile IPv6 protocol that can be used to provide security services for the IP datagrams being sent over the network. The security characteristics of IPSec can be used in Mobile IPv6 networks to establish secure communication links. This project aims to develop a testbed platform in an IPv6 mobility environment which provides an experimental basis for definition of set of guidelines for IPSec configuration and studying possible optimizations of the protocol in a Mobile IPv6 environment.

Pervasive Computing

7. Implementation and Power Optimization of a Bluetooth Universal Remote Controller

Abstract: This project consists of building a universal remote controller which can be used to control any kind of device capable of communicating its user interface. The remote will be based on a Bluetooth-enabled StrongARM board running the Bluetooth stack plus a remote control application. The final goals of this project are: to define a Bluetooth remote controller profile, along with a formal way to define a device's interface, and to optimize the power consumption of the device in a typical usage scenario.

Hardware and Software for Advanced Applications

8. Analysis and Extensions of Power Modelling for Boolean functions

Abstract: Currently, there exist ways to model the power consumption of general behavioral hardware blocks (represented with a vectorial Boolean function) using some parameters of the function. This is useful at a higher lever for making decisions about the implementation of a circuit and to choose the lowest power consuming architecture in a very fast way. The goal of this project is to analyze the existing models for power consumption and possibly to extend them, enhancing their precision. This study is useful to better understand how good the sources of power consumption can be identified and to possibly extend the current synthesis methodologies for small functions.

9. Arm 9 Instruction-Set Emulator

Abstract: Microprocessor modelling is a critical part of the development of both hardware and software in the design cycle of new processors. With the growth of application specific processors, there is a strong need for modeling environments based on precise semantics that can be used for rapid generation of detailed processor simulators. In this work is proposed the development of an arm 9 instruction set simulator (ISS) as case of study, using the proprietary Chorizo technology that allows a quick modelling phase and that automatically generates the C-code for the fundamental modules of the emulator.

10. Routing Scheme in the Spidergon Network-on-Chip

Abstract: Market, application and technology trends lead to new challenges for the on-chip communication moving from the actual shared-bus used in current System on Chip to Network on Chip (NoC) solutions. A low cost, high performance NoC called Spidergon has been proposed by AST (STMicroelectronics). In this thesis a model of the Spidergon is implemented using the OMNeT++ Discrete Event Simulation System in order to evaluate the routing algorithm and virtual channel performances of the NoC.

11. Area Estimation of Configurable STBus Interconnects

Abstract: Stbus is a versatile, high performances interconnect IP, which allows to specify a communication infrastructure in terms of protocols, interfaces and components. It comes with an automated environment (Stbus generation kit) which supports the whole design flow, from network functional high level specifications down to the mapped design and global floor planning.

Beside these capabilities a fast estimation support is required, to evaluate since the beginning of the design process both power and area performances of the interconnect system. This would imply a faster design space exploration and the possibility to support optimisers. Of course the problem of high level estimation is the lack of accuracy, since in the early stages of design flow only high level parameters are known. On the other side a gate level estimation would lead to unsustainable synthesis and simulation time.

An innovative methodology for automatic generation of energy model for STBus IP has already been presented, together with experimental results and will be integrated in STBus Generation Kit.

The goal of this project is the development and integration of an high level area estimator in the Stbus Generation Kit. The aim is providing the designer with a fast and sufficiently accurate area estimate of the interconnect system, once high level parameters have been set.

12. Controlling Embedded Systems with GSM Phone on a Personal Network

Abstract: Challenges to be addressed as a frame of reference Requirements from embedded systems and their design are growing rapidly due to both increase of mission criticality and development of products designed and built with multi-disciplinary technologies. Merging heterogeneous subsystems to a dependable device is severe, mostly when personal health and safety is involved. Skills from different engineering disciplines must be merged, entering specifications that support user-dependent operation without ambiguity. Development of optimal system has to be tuned to a structural implementation that shares the user- environment with adequate dependability (life, power, security, flexibility). Operation of the embedded system within the environment must properly consider both exchange of information and privacy. The previous three facets identify three research fields for personal use of embedded systems: user dependence, implementation structure, internal and external system hierarchies. While the whole field could support and demonstrate a number of cooperative projects, the project targeted for this experiment aims at providing a global feeling of how the challenge could be answered. Further investigation in the related market could bring to a wider collaboration with companies operating in the field. The master thesis work consists of exploring the feasibility of defining a comprehensive solution to the problem. Concerning user dependence, the development is targeted to apply to "body network", i.e. to the set of personal applications that can be borne by a person for his necessities. These could be personal health monitors, sport training assistants, "home" or "work" connections, sense enablers like vision or hearing aids, or others. A common feature is that the system must be non invasive to operate without trouble, and semantically tunable to become also mentally non disturbing. Its operation must be so power conscious to foresee taking power from the environment in the near future. Its connection and its language must be adaptable to user preference to enable hacker-free dependability. Thus we will study the achievability of such features assuming field programmability of hardware to support both minimum consumption and personal language by means of a tunable controller. Concerning the implementation structure, the configurability of the interface to the robot shall be evaluated, proposing a tentative protocol to interleave payload messages and configuration information. The protocol shall be modeled in UML to be reusable in other designs with different peripheral systems, merging interdisciplinary contribution, and interfaced with an UML model of the robot. For the purpose of the master work, configuration shall be studied as software only. The demonstration of the work shall be able to show evidence of the technique. We will interface a toy-robot developing a tunable interface to a set of digital or voice commands. The toy robot shall be programmed by simple instructions in its own proprietary language. The demonstration will use a commercial modem interface, implement the dialogue between the robot and a gsm phone via Bluetooth stream, and will evaluate the power figure for a possible integrated system in case of diverse choices of primitive software semantic objects of the robot.

13. Embedded Fingerprint Recognition System

Abstract: The goal of this project is to implement, in an embedded system, a complete fingerprint recognition system. The project will be done in collaboration with the University of Applied sciences of Berne (HTI – Biel) and the microelectronics laboratory (MicroLab), under the supervision of Dr. Marcel Jacomet and Dr. Lorenz Müller. The fingerprint recognition project will be based on a thesis written by Hans Walter Kramer, at the Berner Fachhochschule ("Improvement of fingerprint verification algorithms")¹. The problem of the fingerprint recognition can be divided in the following points: 1.PRE-PROCESSING: Consists essentially on the scan of the finger to capture the fingerprint image, with any kind of sensor, and the binarization (from gray level to black and white) of the image. 2.EXTRACTION OF FINGERPRINT FEATURES: This process locates features in the ridges and furrows of the skin, called minutae. Minutae points are located where ridge endings or bifurcations are found. This process requires the biggest part of the calculation power. Different open source algorithms on this topic can be found, but they require a big amount of calculation power. 3. MATCHING PROCESS: This step matches the features (minutae) of the query and the template. The minutae may be subjected to: translation, rotation and distortion. The system will be developed for a ARM7TDMI platform, in order to integrate it into a larger project (Cod-It / Axsionics) at MicroLab

14. Performance Comparison of Automatic Instruction-set-Extension Methodologies

Abstract: Performance Comparison of Automatic Instruction-set Extension Methodologies Extending generic processors with specialized units is now a possibility offered by many commercial processors. A key aspect is to generate the instruction set extensions (ISEs) directly from the high-level language description in a fully automated manner. Ad-hoc functional units (AFUs) represent the hardware realizations of the critical sections of an application. The report shows comparisons of different small program fragments which have been assembled with extended instruction-sets based on MIPS architecture. Different methodologies are used to show the performance, limits and difficulties of a state-of-the-art automatic ISEs generator.

15. GENI: a Framework for GENERating Compiler Ir

Abstract: The development and improvement of processors requires new instructions and new hardware features to be easily tested and refined, before they become part of the final design.

An efficient way to support new ISAs in retargetable compilers is to allow the possibility to extend the machine model for which we compile and, also, the customization of the IR languages supported by the compiler.

Describing an IR language for a retargetable production compiler is a tedious work and requires compiler and high-level C++ knowledge. In order for the computer and hardware architects to tackle this complexity, a metalanguage has been designed that allows describing a compiler's IR independently of the given compiler. In addition, we implement a set of tools to easily describe in a unified view, through a graphical user interface, the compiler's IR. The tools that we implement are written in Java, in order to be portable on different platforms.

16. Hyperprocessor Design

Abstract: The aim of this project is to evaluate Hyperprocessor Functional Model (HFM). The HFM is a 'pure' functional simulator of the Hyperprocessor architecture, based on ARM functional simulator. Main goal of this project is to evaluate the accuracy of the HFM and to tune it to more accurate models, such cycle-accurate (CA) ARM simulators. The main contribution of the project should be to gain further understanding about limits of the existing hyperprocessor tools. Creation of a simplified cycle accurate model based on the principle of hyperprocessing is also a challenge of this project in order to better understand basic principle in multiprocessor communication and to test the accuracy of the current functional model.

17. Noise Reduction in Return Path of DOCSIS Cable Network

Abstract: The project concerns a software-hardware implementation for digital processing of a DOCSIS CaTV network return path QPSK signal. Numerical simulation, DWT/FFT implementation on a FPGA platform, area and throughput optimization, noise removal algorithms are included in the project.

18. System-Level Design of the Security Concept of a Wireless Meter Reader

Abstract: Starting from a UML System-Level Design of a Wireless Meter Reading (WMR) System, the designer should develop a security concept/model/protocol (e.g. based on IPSec) taking care of low-power constraints. A possible implementation could be based e.g. on lwIP (light weight protocol). The security concept/model/protocol will be described using UML and one of the goals of the present project will be checking on efficiency of use of UML against "traditional" approaches.

19. System-Level Design using UML and a HW/SW Codesign Environment

Abstract: The project involves the development and test of a methodology for the design of embedded systems starting from UML specifications. The designer has the possibility to provide the functional and structural specification of a system as a set of communicating modules (classes) in the UML specification. HW/SW partitioning information provided by the user on a module-by-module basis are then used in order to export the system specification to a specific Codesign environment able to synthesize hardware, software and the interfaces between hardware and software. Cost

and performance estimates provided by the codesign tool should be back-annotated into the original UML specification in order to drive hardware/software partitioning iterations until the optimal architecture has been identified.

20. Migrating from VxWorks to Linux: a Feasibility Study

Abstract: The goal of this project is to port an existing application from VxWorks, a real-time operating system by WindRiver, to an Embedded Linux platform. The application to migrate controls medical instruments and it has been developed by TXT and coded in C. A crucial aspect of migration is the re-utilization of the existing code in the new operating system: this allows using the same program without having to change the code. This important goal, can be achieved by means of some interfacing libraries and/or some automatic/semiautomatic migration tools. Besides the migration, the existing software will be extended to support new communication channel, such as USB.

21. A Study on Open Source Adequacy for Embedded System Designs

Abstract: Free/Libre Open Source Software (FLOSS) is frequently used to lower software costs and shorten development time. In this study we analyze the problems, benefits and opportunities derived from using FLOSS in new embedded designs. A set of criteria is proposed to help embedded system developers decide whether their project can benefit from FLOSS. Two projects based on open source are evaluated against the proposed criteria: the uIP TCP/IP stack and the MIPL Mobile IPv6 protocol for Linux. Finally the cost, features and performance of the projects studied are compared to their commercial counterparts to determine the advantages of each option.

Master research projects to be completed:

22. Power Optimization of a Bluetooth Ad-Hoc Network

Abstract: This aim of this project is to investigate the usage of different implementations of the Bluetooth module in some ad-hoc networking and sensor network scenarios. The work will include the power modeling, through experimental measurements, of the Bluetooth modules and a following study to determine the best way to make use of the protocol in some ad-hoc power-critical scenarios. This study will also include the optimal deployment, routing and power control strategies in the presented cases.

23. Implementation of a Universal Hashing Block for IPSec Accelerators

Abstract: Hash functions are a very important ingredient in any cryptographic infrastructure; they are mainly used to produce message digests that can be signed or message authentication codes that directly authenticate the message. In 2002, NIST finalized the new hashing standard, the SHA-2 family of algorithms; other hashing functions include SHA-1 and MD5. The goal of this project is to continue the research already made at ALaRI in this topic and implement a fast ASIC hardware unit that is ideally capable to run the aforementioned algorithms. This unit could be used to accelerate many security protocols, including IPSec, and so speed up secure Internet connections by potentially a wide margin.