EMBEDDING QUANTUM CRYPTOGRAPHY ON DSP-BOARDS

Roland Lieger, Thomas Lorünser, Gerhard Humer and Florian Schupfer

ARC Seibersdorf Research GmbH, Donau-City Straße 1/4, A-1220 Vienna, Austria (Europe)
phone: +43 50550 4154, fax: +43 50550 4150
email: {thomas.loruenser, gerhard.humer, roland.lieger, florian.schupfer}@arcs.ac.at
web: www.arcs.ac.at/IT/ITS, www.quantenkryptographie.at/

ABSTRACT

Quantum cryptography is the only system for key generation that can provably not be tampered by an eavesdropper without being noticed. While its theoretical basis is already reasonably well understood, commercial application is hampered by the lack of ready-to-use embedded encryption systems. In this paper we will describe our hardware solution, developed for setting up an application oriented quantum cryptography embedded-system.

1. QUANTUM CRYPTOGRAPHY

Quantum cryptography was born in the late 60's and its intense theoretical treatment began in the 80's and lasts until now. Since then – particularly in the last decade - a huge number of papers dedicated to all aspects of quantum cryptography have been published. A good overview of quantum cryptography can be found in [1].

The first experimental realisation was reported in 1989 by C.H. Bennet et al from IBM Research. A detailed description of the first experiments can be found in [2]. This success motivated many experimentalists to enter the field of quantum cryptography and even though this field is still of interest for basic research a huge basis of know-how has been accumulated.

1.1 Motivation (Why Quantum Cryptography?)

In spite of the intense interest of researchers around the globe and especially scientists in the USA and Europe, quantum cryptography did not seem to make any essential progress with respect to commercialisation. Different causes can be identified for explanation of this fact, but the main reason was the lack of a pronounced market need.

The situation has changed in the last few years. The emerging requirements for technologies stronger than public key cryptography are related to the ever-increasing availability of computing power and the expected advent of quantum computers in the next decade. Quantum computers in particular will render the public key infrastructure paradigm vulnerable, because they will be capable to decrypt in real-time secrets encoded with asymmetric cryptography.

Another aspect, which also calls for stronger encryption techniques, is the presence of the global surveillance network ECHELON, maintained by the USA and its allies. (See the EC parliament report [3] for details.) It is proven, that ECHELON was not only used for politically driven espionage, but also for economic one and it has in several occasions caused drastic damages to the European economy. The quoted EC parliament report [3] recommends in this relation migration to stronger encryption technologies in general and to quantum cryptography in particular. ARC Seibersdorf research leads a European consortium dedicated to bringing quantum cryptography to real life within an EC sponsored project, which is about to start (Integrated Project SECOQC - Proj.Nr. 506813, Call FP6/2003/IST/1). Important initial results have been already obtained in the FIT/IT project PRODEQUAC (Nr. 806015 – Austrian Ministry of Transportation and Innovation), which is currently carried out by ARC Seibersdorf research, the Institute of Experimental Physics at the University of Vienna (IfE) and Siemens AG. Some of these results are reported in the current paper.

1.2 Principles of Quantum Key Distribution

Quantum cryptography uses quantum mechanical effects for simultaneous generation of identical and absolutely random bit sequences at two distinct locations. These sequences are principally not accessible to a third party trying to tamper the procedure and, therefore, they can be used as keys for subsequent encryption. That's why this technology is also often referred to as Quantum Key Distribution (QKD).

To operate QKD, on the one hand, a direct optical link between the two peers generating the key is required. This link can be either established through a dedicated optical fiber or through a free space line-of-sight connection. On the other hand a channel for public communication is needed, which can be a traditional network connection.

The maximum distance, which can be bridged by a practical QKD system is currently limited to 20-100 km due to the unavoidable absorption and noise on the quantum channel. The maximum distance also depends on the method employed, the level of security desired and the expected performance in bits per second.

1.3 State of the Art in Quantum Cryptography

A wide variety of quantum key distribution systems has been implemented [1] since the first laboratory proof-of-principle tests. These systems employ different signal

sources, e.g. single photon sources, weak coherent pulses, entangled pairs of photons or strong overlapping light pulses. Moreover, many detection schemes, including single photon counting techniques and coherent detection methods have been used.

Besides experimental prototypes Id Quantique from Switzerland first launched a commercially available QKD system in 2002 [4]. This system is capable of generating keys over 67 km and makes them available on an USB interface. It is a standalone QKD device not integrated into any system or infrastructure of any form.

In the last months another enterprise, MagiQ Technologies [5], entered the scene of quantum cryptography with Navajo, an out-of-the-box security gateway using quantum cryptography, which is much more application oriented than the device by Id-Quatique.

1.4 Our Approach

Our concept aims at providing a scalable security solution embedding quantum cryptography as security enhancing core technology on standalone devices. Therefore, we are developing a dedicated signal processing device which, on the one hand, embeds all necessary tasks for QKD and on the other hand fully manages secure networking. Moreover, it should fulfil the requirements given in applications from highest to middle security levels. The developments will yield in a highly secure embedded-system connecting different secured infrastructures at different locations through public networks on a point-to-point basis. Additionally, the hardware components developed so far will allow setting up a modular and software configurable system capable of supporting different optical layers and different application scenarios.

2. SYSTEM AND REQUIREMENTS

Embedding quantum cryptography requires an integrated hardware/software solution managing all the different tasks arising on the discussed standalone system.

2.1 Optical Setup

The quantum optical test bed, which will be used for setting up the prototype, is developed in parallel at the IfE. The setup implements the BB84 protocol [1] and its structure is depicted in Figure 1. It consists of a source for entangled photons and the detection units each containing four single photon detectors. The expected performance of our first prototype will be about few tens of key bits per second at a distance of 10 km.

2.2 Requirements

Due to the interfaces given by the optical segment the hardware has to be capable of sampling four detector signals at nanosecond level. To correlate the photon measurement results at both parties the photon counting logic has to be synchronised with a high stability and with a precision better than the sampling period.

To distil a key with a reasonable bit error rate out of the raw measurements taken, an intense communication over a public

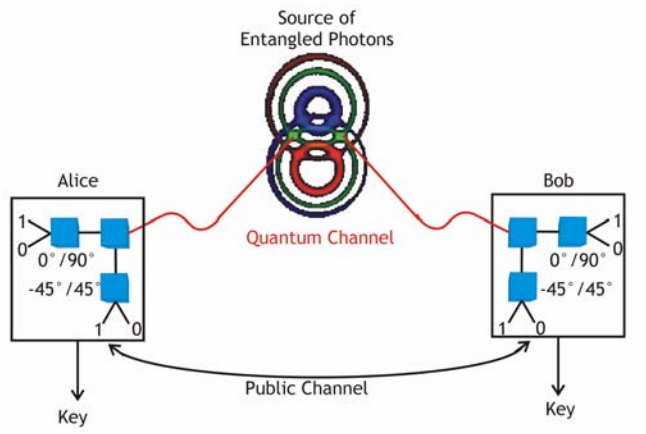

Figure 1: Quantum Key Distribution System

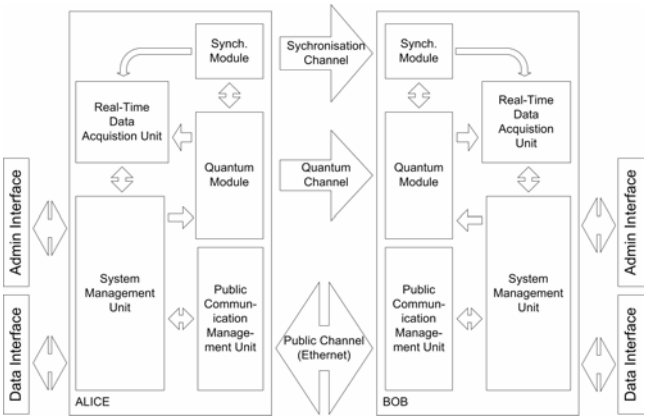

Figure 2: Tasks necessary for QKD

channel is necessary. This public channel could be any traditional communication channel, but for practical usage it should be realised as Ethernet interface, because of the easy connection to public networks available from Internet Service Providers.

Additionally the hardware has to provide computing power for real-time packet encryption with symmetrical algorithms like AES. Ideally it allows for hardware implementation of special cryptography tasks in configurable devices such as FPGA's (Field Programmable Gate Array) to improve performance.

To securely handle sensitive data to be encrypted on the embedded-system the latter has to provide an additional interface, which must be completely inaccessible from the public channel. This interface, being encapsulated from public networks, can also be used for administration, but ideally the hardware supports more administration interfaces (e.g. web and console).
Besides the key generation through optic measurements and the use of this key for subsequent encryption, the optical segment must also be monitored and controlled. Therefore, the embedded hardware must be able to communicate with a

manifold of different sensors and actuators to guarantee stability and performance of the optical setup.

An overview of all tasks mentioned above and their relations is sketched in Figure 2.

3. HARDWARE ARCHITECTURE OF THE DSP-BOARD

To accommodate the requirements of quantum cryptography a DSP-board has been designed that uses three main computational components: A Xilinx Virtex2 XC2V2000 FPGA, a Texas Instruments TMS320C6416 DSP (Digital Signal Processor) and a Motorola Coldfire MCF5272 Microcontroller. We are currently using two identical boards on each side of the communication channel, making it easy to maintain a strict separation of encrypted and plain text data. The boards' block diagram is sketched on Figure 3.

The FPGA serves several purposes; First of all it provides the interface to the optical equipment. For every single photon received a short (20ns) signal is generated by the photon detector. Moreover, the information carried by this signal lies in the leading edge and its timing is important for correlating the measured events. Since single photon detectors exhibit a high error rate, in parallel to every information carrying photon (belonging to an entangled photon pair) an equally short but intensive optical pulse is sent for synchronization along a separate dedicated optical fiber, which we call synchronization channel. It is the task of the FPGA to detect valid photon counting events and corresponding synchronization pulses using an extremely high timing resolution of 1.25ns This requires the sampling circuitry to run at 800 MHz.
In addition to this fast timing logic, the FPGA also implements a dual ported RAM (DPRAM) that serves the central data exchange between all computing elements of a board. While the DPRAM is physically implemented on the FPGA to reduce the chip count, it can logically be thought of as an independent device, accessible to FPGA, DSP and Coldfire. Contrary to ordinary DPRAM however some memory areas are protected against access from a specific device, making it possible to exchange data between two computing elements (e.g. FPGA and DSP) without running the risk, that the third computing element (e.g. Coldfire) eavesdrops on the communication.
Finally the FPGA provides the high speed LVDS interface to the other RTS-DSP-board.

The DSP is the main resource for 'real' computing. Clocked at 600 MHz it is capable of up to 4800 MIPS and fast enough to run symmetric encryption algorithms. In addition to its computing logic, the DSP also contains 1 MByte of internal RAM. This makes it possible to create and store extremely sensitive data (such as encryption keys) directly on the chip, without ever sending them over an external bus. An external (slower) RAM of 32 MByte (expandable to 512

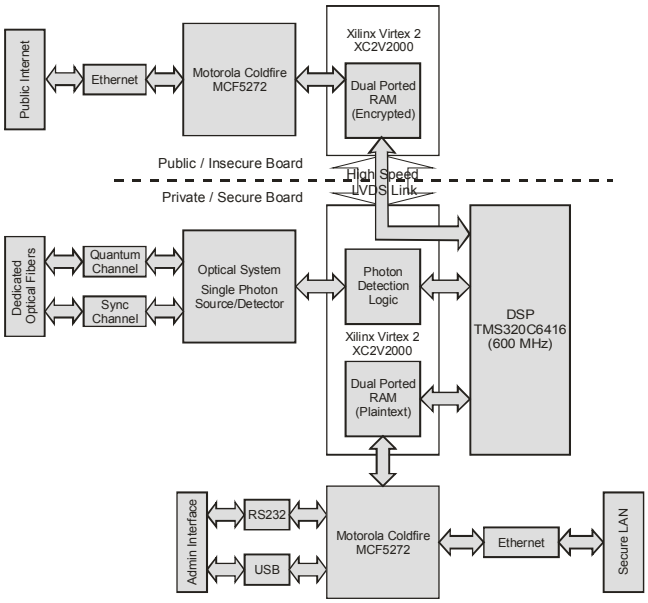

Figure 3: Block diagram of board configuration

MByte using a standard SO-DIMM) is available, if the internal RAM should prove insufficient for large tables. 4 MByte of Flash-ROM are used to store the DSP's own applications and the configuration files of the FPGA (which the DSP configures at boot time).

In addition to the two chips dedicated to signal and data processing the RTS-DSP board features a Motorola XCF5272VF66 ('Coldfire' – a member of Motorola's successful 68000 family of microprocessors) CPU. Clocked at only 66 MHz it is too slow to be used for high-speed data processing itself, but it is more than sufficient to serve as a communication subsystem providing support for Fast Ethernet, USB 1.1 and RS232. Thus it is easily possible to exchange data with the sending/receiving PC without burdening the computation components with the overhead and complexity of external interfaces. The Coldfire is equipped with 2 MByte of Flash-ROM and 16 MByte of RAM, and is running µClinux, a special edition of Linux trimmed down for embedded systems.

Both the DSP and the Coldfire have their own Flash- and RAM-Memory. It is not possible for the Coldfire to directly access the DSPs memory or vice-versa. Communication between the components takes place by means of the dual-ported RAM only. Since DSP and Coldfire use different physical busses to access the DPRAM it is not possible for the Coldfire to tamper with the communication between DSP and FPGA, nor can the Coldfire use the DPRAM to obtain information about the internal state of the FPGA. Since the DSP's RAM is connected using yet another, completely separate physical bus, the Coldfire (or the FPGA) can not eavesdrop on that bus either. This guaranties that the Coldfire can not (even if it has been subverted by an attacker and is running malicious code) corrupt the DSP's internal state. Since the FPGAs configuration is controlled solely by

the DSP, this also guaranties the integrity of the FPGA's configuration.
Considering the above facts it is easy to see that the DPRAM is the only interface of the DSP to the outside world. Obviously this encapsulation makes the DSP an excellent choice when running security-critical applications.

4. SOFTWARE ARCHITECTURE

Since there are three computing elements on the DSP-board, it is possible to distribute the algorithms to get optimal performance and security from every chip.

While the FPGA performs tricky timing measurements it simultaneously computes the statistics of event occurrences in the optical photon detectors that have to be done extremely fast during quantum key distribution. It also provides the DPRAM and the interface to the other RTS-DSP-board, but runs hardly any computational algorithm.

The excellent security encapsulation and its high computational power make the DSP the logical choice for secure storage of the generated key and implementation of the actual encryption/decryption algorithms. Note that the actual encryption key is generated and used in the DSP only. It is stored in the on-chip RAM and never transmitted to the external environment (not even to the external RAM or the trusted Coldfire, who might send it to other systems over the private network).
While the DSP has been optimized for fast array processing, it can also quickly compute many complex algorithms, such as AES or DES.

Since the DSP (and the FPGA) run only application specific algorithms and no operating system, there are also no operating system bugs and security holes. The Coldfire on the other hand runs a copy of µClinux, a slim edition of Linux that has been trimmed down to fit the needs of embedded devices (low memory footprint, low processing capacity, no Memory Management Unit (MMU)). Even though the entire µClinux is just a few hundred KByte in size, it still retains its communication subsystem, so writing TCP/IP based applications for data exchange with external systems is very convenient. Since µClinux's TCP/IP stack includes powerful packet filter code (iptables) unwelcome IP packets are eliminated before any internal processing takes place.

To build a complete embedded encryption system two Coldfires are needed, one providing the Ethernet interface towards the public network (handling only encrypted data) and one for the secure local network (handling plaintext data). These two interfaces must be kept as separate as possible. It is not acceptable to have decrypted data stored in a memory connected to CPU that also has a network interface to the internet, since a hacker who manages to subvert this system would otherwise obtain direct access to plain-text data.
This separation is currently implemented by using two DSP-boards, one for the public and one for the private side Ethernet. On the public side board, only the communication subsystem implemented in the Coldfire is really needed; The FPGA just provides connectivity to the other DSP-board and the DSP is idle. All the actual encryption/decryption process takes place on the private DSP-board. We are aware that the resources of the public board are not used efficiently, and will add the second Coldfire at the next redesign of our board.
Thus each of the three processing elements provides its own specialized features: A FPGA for high speed I/O and simple algorithms, A DSP for complex algorithms like encryption/decryption and controlling the FPGA and the Coldfire(s) as communication subsystem. Each chip executes those computations that it is best suited for. The joint application of all three elements yields an integrated, high performance, provably secure encryption system.

5. CONCLUSIONS

The hardware presented here is a novel solution for embedding quantum cryptography. It allows the flexible distribution of all the different tasks required for a standalone quantum cryptography device, on different hardware components all situated on two printed circuits. The board enables straightforward and portable implementation of networking support and at the same time its design guarantees encapsulation of critical data from unwanted access, hence, it provides a very high level of security.

REFERENCES

[1] N. Gisin, G. Riordy, W. Tittel and H. Zbinden, "Quantum cryptography" *Rev. of Modern Phys*. vol 74, pp. 145-195, 2002.

[2] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, , "Experimental Quantum Cryptography", *J. Cryptology* vol 5, pp. 3–28, 1992.

[3]"Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))", Temporary Committee on the ECHELON interception system.

[4] D. Stucki, N. Gisin, O.Guinnard, G. Ribordy and H. Zbinden, "Quantum key distribution over 67 km with a plug&play system", *New J. of Physics* vol 4, pp. 41.1-41.8, 2002.

[5] http://www.magiqtech.com, MagiQ Technologies, New York, USA.