COPACOBANA
A Cost-Optimized Special-Purpose Hardware for Code-Breaking

Sandeep Kumar[1], Christof Paar[1], Jan Pelzl[1], Gerd Pfeiffer[2], Manfred Schimmler[2]
[1] Horst Görtz Institute for IT Security, Ruhr University Bochum, Germany
{kumar,cpaar,pelzl}@crypto.rub.de
[2] Department of Computer Science, Faculty of Engineering,
Christian-Albrechts-University Kiel, Germany
{gp,masch}@informatik.uni-kiel.de

Abstract

Cryptanalysis of symmetric and asymmetric ciphers is computationally extremely demanding. Since the security parameters of almost all practical crypto algorithms are chosen such that attacks with conventional computers are computationally infeasible, the only promising way to tackle existing ciphers (assuming no mathematical breakthrough) is to build special-purpose hardware. This contribution presents a special-purpose hardware labeled COPACOBANA (Cost-Optimized Parallel Code Breaker), which is optimized for running cryptanalytical algorithms with low communication overhead. The price-performance ratio as primary and a cost margin of less than US$ 10,000 as secondary design goal led to a reconfigurable computer built as cluster of programmable logic devices.

1. Introduction

Cryptanalysis of modern cryptographic algorithms requires massive computational effort, often between 2^{56} to 2^{80} operations. A characteristic of many (but not all) cryptanalytical algorithms is that they can run in a highly parallel fashion with very little interprocess communication. Such applications map naturally to a hardware based design, requiring repetitive mapping of the basic block. However, it should be stressed that the mere availability of computational resources is not the core problem, but providing massive computational resources *at affordable costs* is.

With the recent advent of low-cost FPGA families with much logic resources, field programmable gate arrays (FPGA) provide a very interesting alternative tool for the massive computational effort required for cryptanalytic applications. In addition, to the cost-performance advantage over PC-based machines, such a machine has the advantage over ASIC-based designs that it can be used to attack various different cryptosystems without the need to rebuilt a new machine each time.

In the next Section, the architecture of such an FPGA based hardware is explained. This new machine is labeled COPACOBANA (Cost-Optimized Parallel Code Breaker) because it is only twice as expensive as the low-cost FPGAs that it contains.

2. Architecture

The metric to decide whether an architecture is "good" or not is a function of performance, flexibility, and monetary cost. An established performance metric for hardware implementations is the area-time (AT) complexity. Whenever we can minimize the AT-complexity, the design can be called efficient. ASIC implementations can be AT-minimal and are the best choice for high-volume applications. FPGAs in contrast are reprogrammable and, thus, are flexible. Moreover, if only a relatively small number of chips ($< 10\,000$) is required, FPGAs are preferable since the production of ASICs is profitable only when targeting high volumes.

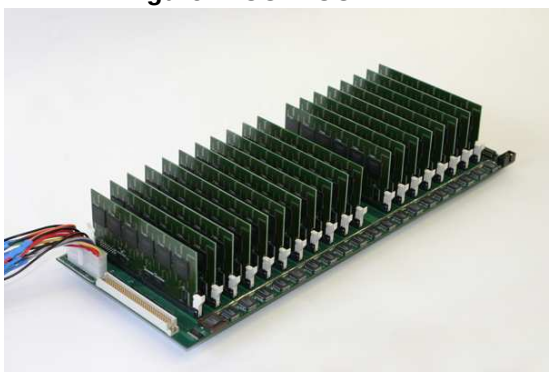
Many algorithms tackling the most important problems in cryptanalysis can be implemented on FPGAs. However, code breaking involves more effort than programming just a single FPGA with a particular algorithm. What is needed is a powerful massively parallel machine, tweaked to the needs of the targeted algorithms. In our case, not much communication overhead is required. Conventional parallel computing architectures, such as provided by Cray, can in theory also be used for cryptanalytical applications. However, the cost-performance ratio is not optimized with this approach, resulting in prohibitively expensive attack machines. Simi-

larly, many features of current high-end computers are not required for the targeted cryptanalytical problems. For instance, high-speed communication between CPUs, fast floating point operations, memory etc., is not necessary in our context. All of these features usually increase the cost of such a device, which is in particular annoying when they are superfluous. For the same reason a simple grid of conventional PCs is not efficient, as can be seen from implementations of DES: An implementation on a single FPGA can be more than 100 times faster than an implementation on a conventional PC, while the FPGA is much cheaper than the PC [3]. Therefore, a custom design is inevitable in order to obtain a low-cost architecture with the required performance.

The COPACOBANA machine depicted in Figure 1 was built to fit those requirements and consists of 120 independent low-cost FPGAs (XC3S1000), connected to a host-PC via a standard interface. The initialization of FPGAs, the control, and the accumulation of results is done by the host. All time-critical computations are done by the FPGAs, which realize the actual cryptanalytical architectures. Several different design options have been considered. A cost-performance optimized design became only feasible by strictly restricting all functionality to those directly necessary for code breaking.

A step towards an extendable and simple architecture has been accomplished by the design of a small pluggable FPGA module as custom made 4-layer printed circuit board in DIMM format, comprising 6 FPGAs. These FPGAs are directly connected to a common 64-bit data bus on board of the FPGA module which is interfaced to the backplane data bus via 3-state transceivers. Closely connected the backplane hosts 20 FPGA-modules and the controller card. All modules are connected by a 64-bit data bus and a 16-bit address bus. This single master bus is easy to control because no arbiter is required. Interrupt handling is totally avoided in order to keep the design as simple as possible. If the communication scheduling of an application is unknown in advance, the bus master will need to poll the FPGAs.

Figure 1. COPACOBANA



Data transfer from and to the FPGAs and to the host-PC is accomplished by the control interface. The controller hardware has to handle the adaptation of different clock rates: The USB interface uses a clock rate of 24 MHz, the backplane is clocked with 33 MHz, and the controller itself is running at an internal clock of 133 MHz. Programming can be done for all FPGAs simultaneously, for a set of such, or for a particular one. Details of the implementation of the control logic can be found in [2]. The top level entity of COPACOBANA is a host-PC which is used to program and control all FPGA implementations. For this purpose, a software library has been written to issue commands to the USB connected [2] controller card of COPACOBANA.

3. Conclusion and Future Work

The work at hand presents a machine of a cost-efficient design hosting 120 low-cost FPGAs. The hardware can be adopted to any suitable task, not necessarily restricted to code breaking. Recapulating, COPACOBANA is the first and currently the only available cost-efficient design to solve cryptanalytical challenges. For example, the Data Encryption Standard (DES) can be broken within 9 days with this hardware for less than US$ 10,000 [3]. Almost certainly there will exist more interesting problems apart from cryptology, which can be solved efficiently with the design at hand. In an ongoing project, we plan to apply the Smith-Waterman algorithm for scanning sequences of DNA or RNA against databases.

At least we like to thank the Xilinx Inc. for the generous donation of Spartan-3 FPGAs which formed the basis of our design.

References

[1] Electronic Frontier Foundation, “Cracking DES: Secrets of Encryption Research,” *Wiretap Polotics & Chip Design*, O’Reilly & Associates Inc., July 1998.

[2] C. Schleiffer, J. Pelzl, “Design of a Host Interface for COBRA,” *Technical Report*, Bochum, Germany: January 2006.

[3] S. Kumar, C. Paar, J. Pelzl, G. Pfeiffer, A. Rupp, M. Schimmler, “How to Break DES for € 8,980 in 9 Days,” *Proc. of the 2nd International Workshop on Special-Purpose Hardware for Cryptanalytic Applications (SHARCS’06)*, Cologne, Germany: April 2006.