A Cost/Performance Study of Modern FPGAs in Cryptanalysis

Author: Ian Howson (ian@ianhowson.com)

School of Electrical and Information Engineering
The University of Sydney

Exhaustive key search attacks will always be successful against any symmetric cipher given enough time. Many common deployments of cryptography are vulnerable to these attacks. This thesis compares the cost and performance of FPGA and software-based approaches to key search. This information is useful when assessing the security of cryptographic products.

An extremely high speed FPGA DES key search machine was implemented. An FPGA RC5 key search machine was implemented that can achieve greater search density than standard CPUs. It can be shown that a key search machine to break DES keys within a few days can be constructed very cheaply. It can be seen that regulatory issues within Australia and the United States stifle the development of cryptographic products for export.

1 Objectives

- Compare hardware and software approaches to key search using a cost/performance metric
- Investigate cipher design and how it relates to keys search
- Evaluate the security of ciphers in relation to these results

2 Technologies

CPUs can be used to conduct key search attacks with software. CPUs are very cheap, easy to obtain and have extremely high clock speeds. Most organisations already have many computers that can be used to conduct attacks.

An ASIC (Application Specific Integrated Circuits) can be used to conduct an attack. The speed will be very high, but fabrication costs are usually prohibitive. The incremental cost per device is usually quite low. Their internal design can be changed at any time.

FPGAs (Field Programmable Gate Arrays) have been used recently for key search attacks. They have many of the advantages of ASICs without the high initial cost.

3 Implementations

FPGA key search machines for the DES and RC5 ciphers were implemented. These used a Xilinx XCV1000E device operating at 100MHz on a Pilchard board. A search rate of 500Mkeys/sec was achieved for DES. This is far in excess of the search rate per device achieved by any previous implementation. RC5 achieved 3.7Mkeys/sec, slightly faster than a Pentium 4 2.5GHz.

4 Pricing

Pricing data for FPGAs and CPUs was obtained. Using this and performance estimates for each device allowed the cheapest, fastest device to be determined. Both RC5 and DES key search attacks are cheapest using Spartan IIE 200 devices. The Virtex II Pro 40 was slightly more expensive, but eight times faster per device. Using them would allow a large key search machine to be built at a lower cost and with less power, heating and space problems.

5 The EFF DES Cracker

In 1998, the Electronic Frontier Foundation constructed a DES key search machine which could break one key every 4.5 days on average. It cost USD$130,000 in materials. From the results in this thesis, an equivalent machine

could be constructed using FPGAs for USD$34,000. This is well within the resources available to most organisations and many individuals.

A further advantage of the FPGA approach is that the devices can be reprogrammed to attack any cipher or perform any operation. This opens avenues for key search machines for other ciphers or very high performance parallel computing machines at an even lower price than PC clusters.

6 Performance estimates

Two approaches to implementing ciphers on FPGAs can be used: iterative and pipelined. Iterative approaches use fewer resources but are quite slow. Pipelined approaches are very fast but expensive. Pipelined implementations are usually preferable, but the design of many ciphers makes this impossible to achieve within the available resources.

A method for determining the resource usage of a pipelined implementation is presented. This considers the operations performed by the cipher, its state size and data access patterns within the cipher.

Xilinx FPGAs contain features which allow resource usage to be dramatically decreased. Extensions to the method are described to account for this.

The RC5 cipher implementation produced was an iterative design. Estimates from this method predict that a pipelined RC5 implementation would use around 14,400 slices (the XCV1000E contains 12,288) and run at approximately 100MHz. One key can be checked per clock cycle, giving a search rate of 100Mkeys/sec. This is far higher than that achieved by any effort so far, regardless of technology.

7 Regulatory issues

Australia requires that any cryptographic exports be reviewed and approved by the Defence Signals Directorate (DSD). This is a similar procedure to that required for nuclear materials, rockets, and other “dual-use goods”. The United States generally prohibits the export of cryptography using key lengths greater than 56 bits. DES key search machines usually search a 56 bit key space, and we have seen that attacks on DES can be completed quickly at a low cost. This makes most exports of cryptography from the US nearly useless for security purposes.

8 Conclusions

From the analyses contained within the thesis, we can determine that:

- The design of a symmetric cipher greatly affects its resistance to key search attacks
- International regulations make developing cryptographic products for export difficult
- FPGAs are very suitable for conducting key search attacks
- The DES cipher should not be used for any security product or procedure
- In order to maintain security against all known threats for a period of 100 year, a key length of at least 128 bits should be used