CAIRN 3: An FPGA Implementation of the Sieving Step with the Lattice Sieving (Extended Abstract) *

Tetsuya Izu, Jun Kogure and Takeshi Shimoyama

FUJITSU Limited
4-1-1 Kamikodanaka, Nakahara-ku, Kawasaki, 211-8588, Japan
{izu,kogure,shimo-shimo}@jp.fujitsu.com

Abstract. The hardness of the integer factorization problem assures the security of some public-key cryptosystems including RSA, and the number field sieve method (NFS), the most efficient algorithm for factoring large integers currently, is a threat for such cryptosystems. Recently, Izu et al. developed a dedicated sieving device "CAIRN 2" with Xilinx's FPGA which is designed to handle up to 768-bit integers. However, since CAIRN 2 uses the line sieving, it is not optimized from the viewpoint of the efficiency. In this paper, we report some results of an FPGA-based sieving hardware "CAIRN 3" with the lattice sieving. In the experimental sieving for a 768-bit integer (RSA768), CAIRN 3 is about 38 times faster than CAIRN 2. It is estimated that the full sieving for RSA768 requires about 270 years with single CAIRN 3.

Keywords. Integer factorization, the number field sieve method (NFS), the sieving step, implementation, FPGA

1 Introduction

The integer factoring problem is one of the most fundamental problem in the area of cryptology since the hardness of the problem assures the security of RSA. The number field sieve method (NFS) [LLMP90] is the most efficient algorithm for factoring large composite integers, and thus is an essential threat for RSA. Among four major steps of NFS (namely, the polynomial selection step, the sieving or the relation finding step, the linear algebra step, and the square root step), the sieving step is a dominant procedure theoretically and experimentally. In order to factor larger integers by NFS, the dedicated sieving hardware based on ASIC architectures have been discussed vitally. In 2001, Bernstein proposed an ASIC design for the linear algebra step based on a sorting algorithm [Ber01]. Then, Lenstra et al. enhanced the device by using a routing algorithm [LSTT02]. Geiselmann and Steinwandt applied these ideas to the sieving step and proposed two designs DSH and YASD [GS03,GS04]. Shamir and Tromer improved an

* A part of this research is financially supported by a contract research with the National Institute of Information and Communications Technology (NICT), Japan

optical sieving device TWINKLE [Sha99] into an ASIC-based hardware TWIRL [ST03]. Since the efficiency of TWIRL was not optimized, an improvement was proposed by Geiselmann et al. [GJK+06], and a combination of TWIRL and YASD is proposed by Geiselmann and Steinwandt recently [GS07]. On the other hand, Franke et al. proposed a sophisticated design SHARK by using a butterfly-sorting [FKP+05]. In spite of these theoretical efforts, experimental results of implementational aspects of these designs are not known.

In order to fill up the gap between theory and practice, Kim et al. developed an FPGA-based siever for the quadratic sieve method [KM00]. Recently, in CHES 2007, Izu et al. reported implementational results of a dedicated sieving device "CAIRN 2" (Circuit Aided Intelligent Relation Navigator) which is designed to handle up to 768-bit integers [IKS07]. The developed device processes the core sieving on FPGA (Xilinx's Virtex-4 XC4VLX200) and the primality test and the mini-factoring on a reconfigurable processor (IPFlex's DAPDNA-2). They actually factored a 423-bit (which was unfactored when the experiment was done) with CAIRN 2 for the sieving step (in 30 days) and usual PCs for other steps.

There are two algorithms for the sieving step: the line sieving and the lattice sieving. The line sieving is straightforward and simple, but the efficiency is inferior to that of the lattice sieving [Pol91]. In fact, in current large-scale factoring experiments such as factoring a 633-bit integer (RSA200) [BBFK05] or a 1017-bit integer (the 1039-th Mersenne number) by the special NFS [AFKLO07], the lattice sieving is widely used in the sieving step. Thus, from the viewpoint of the efficiency, CAIRN 2 is not optimized since it is based on the line sieving.

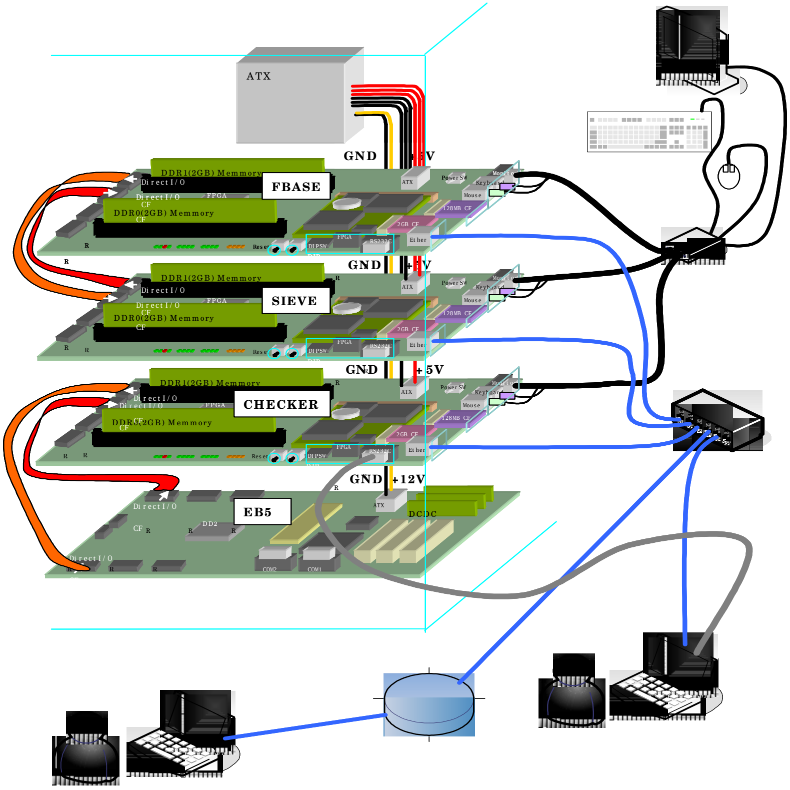
In this paper, we report experimental results of "CAIRN 3", an enhanced sieving device with the lattice sieving. Similar to CAIRN 2, CAIRN 3 processes the core sieving on FPGA (Xilinx's Virtex-4 XC4VLX200) and the others on the reconfigurable processor DAPDNA-2. In our experimentation, the sieving for a 768-bit integer (RSA768) with CAIRN 3 is about 38 times faster than that of with CAIRN 2. From this result, it is estimated that the full sieving for RSA768 requires about 270 years with single CAIRN 3. Implementational details and further experimental results 3 will be reported in the coming paper.

2 Structure of CAIRN 3

The physical structure of the developed sieving device CAIRN 3: 3 FPGA boards (Xilinx's Virtex-4 XC4VLX200 [Xilinx]) and 1 DAPDNA-EB5 board by IPFlex (which consists of the DAPDNA processor and I/O interfaces [IPFlex]) as in Figure 1 [1]. DAPDNA-2 has two processors DAP and DNA: DAP (a usual RISC processor) is a controller, while DNA is a reconfigurable hardware with 376 fixed process elements which can be connected programably. Compared to FPGA, DAPDNA-2 is suitable for complex procedures. FPGA boards are connected via 100 BaseT ethernet, while the DAPDNA-EB5 is connected to an FPGA

[1] The structural difference of CAIRN 3 from CAIRN 2 is the number of FPGA boards: 2 boards were used in CAIRN 2.

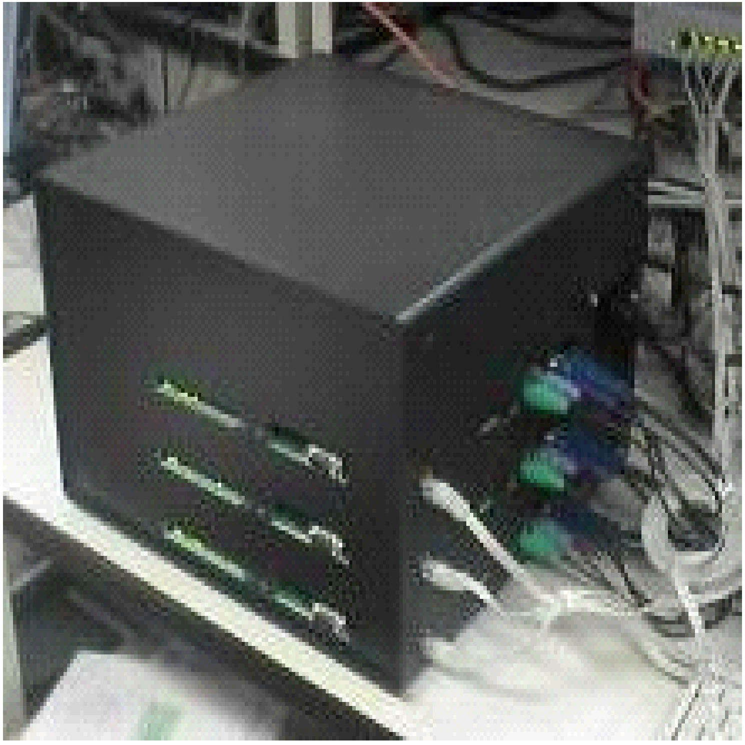
Fig. 1. Structure of CAIRN3



board via the DirectI/O. The device is connected to a control PC via 100 BaseT eithernet. Detailed specifications of CAIRN 3 are summarized in Table 1, and outlook of CAIRN 3 is in Figure 2.

Functionally, the developed device consists of 3 components FBASE, SIEVE and CHECKER. The device is designed to handle up to 768-bit integers. FBASE and SIEVE are for the lattice sieving, and CHECKER is for the relation checking. FBASE generates a lattice base from the factor base and a special-Q on the 1st FPGA board. From this lattice base, SIEVE actually sieves on the 2nd FPGA board. CHECKER executes the relation checking, namely, the trial division on the 3rd FPGA board, and the primality test and the mini-factoring on DAPDNA-EB5. In our design, a sieving device can handle several FBASEs, SIEVEs and CHECKERs, however, we only implemented 1 for each. Table 2 shows occupancies and frequencies of each component.

Fig. 2. Outlook of the developed sieving device CAIRN 3



3 Experimental Sieving for RSA768

In this section, we show experimental results of the sieving of a 768-bit integer (RSA768) with the developed device CAIRN 3. A comparison with the previous device CAIRN 2 is also described.

A target 768-bit composite was selected from the challenging problems by provided by RSA Security Inc., which is unfactored up to the moment:

$$\begin{aligned} N \ = \ & 1230186684\ 5301177551\ 3049495838\ 4962720772\ 8535695953 \\ & 3479219732\ 2452151726\ 4005072636\ 5751874520\ 2199786469 \\ & 3899564749\ 4277406384\ 5925192557\ 3263034537\ 3154826850 \\ & 7917026122\ 1429134616\ 7042921431\ 1602221240\ 4792747377 \\ & 9408066535\ 1419597459\ 8569021434\ 13. \end{aligned}$$

Used NFS parameters [LTS+03] are summarized in Table 3, where rp (ap) is the rational (algebraic) smoothness bound, rlp (alp) is the rational (algebraic) smoothness bound for large prime variation, ha, hb are the bounds for relations (a, b) and F, (G) is the rational (algebraic) polynomial.

Table 1. Specifications of the developed sieving device CAIRN 3

FPGA	Xilinx Virtex-4 XC4VLX200
	Logic Cell 200,448, Block RAM 336 × 18 Kbit, BGA 1513pin
	DDR SDRAM (1 GByte + 2 GByte) × 2 systems
Controller	CPU board: ADVANTECH's SOM-2353
	CPU: AMD Geode GX1 300 MHz (x86)
Output I/F	Direct I/O (50pin), 100 BaseTx, RS232C, VGA, KBD/Mouse
Frequency	133MHz (FPGA), 32bit/33MHz (PCI BUS), 83.4 MHz (Direct I/O)

Table 2. FPGA occupancies and frequencies

	SLICE	RAM	LUT	Register	Frequency
FBASE	99.998%	89.0%	80.1	48.8	50 MHz
SIEVE	40.9%	98.8%	32.1	19.6	100 MHz
CHECKER	78.0%	40.0%	45.0	42.0	122 MHz
Total	89099	336	178176	178176	

As summarized in Table 4, 251.9 sec. is required for 1 Special-Q in the lattice sieving. Since this procedure repeats 8192 sub-sievings over sub-areas with $2^{16} \times 8$, 30.75 msec is required for each sub-sieving. In our experiment, a Special-Q is chosen as large as *ap* (algebraic smoothness bound) and the lattice sieving finds about $\log_2 ap \approx 29$ times candidate compared to the line sieving. More precisely, the gap can be evaluated as 23.43 by using the Dickson's rho function. Since CAIRN 2 sieves a sieving area with width 2^{19} in 49.92 msec on average, CAIRN 3 establishes about 38 times speed-up for the sieving.

In our experiment with CAIRN 3, 1 relation was found in 3.920 sec on average. Since 2.17×10^9 relations are required for factoring RSA768, it is estimated that $3.920 \times 2.17 \times 10^9$ sec. $\approx$ 270 years are required with single CAIRN 3.

4 Concluding Remarks

This paper promptly reports experimental results of the dedicated sieving device CAIRN 3 based on the lattice sieving. In our experiment of the sieving for RSA768, 1 relation was found in 3.920 sec. on average. Thus, it is estimated that about 270 years are required for the full-sieving with single CAIRN 3. Implementational details of CAIRN 3 and further experimental results will be reported in the coming paper.

References

[AFKLO07] K. Aoki, J. Franke, T. Kleinjung, A. Lenstra and D. Osvik, "A Kilobit Special Number Field Sieve Factorization", Cryptology ePrint archive 2007/205, IACR, 2007.

Table 3. Parameters for RSA768[LTS+03]

$$
\begin{aligned}
rp &= 100000000 \\
ap &= 1000000000 \\
rlp &= 20000000000 \\
alp &= 30000000000 \\
ha &= 170000000000000 \\
hb &= 89000000 \\
F &= 44572350495893220x^5 \\
&\quad +1421806894351742986806319x^4 \\
&\quad -1319092270736482290377229028413x^3 \\
&\quad -4549121160536728229635596952173101064x^2 \\
&\quad +6062531470679201843447146909871507448641523x \\
&\quad -1814356642608474735992878928235210850251713945286 \\
G &= 6695805867617963760579180 67x \\
&\quad -773002852896233711606906868654206665703 7329
\end{aligned}
$$

Table 4. Performance of the sieving for RSA768

Procedure	Part	Timing	Comment
Lattice Base Computation	SIEVE FPGA	2.75 sec	per 1 Special-Q
Lattice Base Transmission	DirectIO	2.40 sec	per 1 Special-Q
Initialization	SIEVE CPU	61.49 sec	for the sieving area $2^{16} \times 2^{16}$
Lattice Sieving	SIEVE FPGA	190.43 sec	for the sieving area $2^{16} \times 2^{16}$
Candidate Transmission	Ethernet	0.044 sec	per 1 Special-Q

[BBFK05] Bahr, Boehm, Franke, Kleinjung, "RSA200", E-mail announcement, May 9, 2005. `http://www.loria.fr/~zimmerma/records/rsa200`

[Ber01] D. Bernstein. Circuits for integer factorization: a proposal. preprint, 2001.

[FKP+05] J. Franke, T. Kleinjung, C. Paar, J. Pelzl, C. Priplata and C. Stahlke, "SHARK: A Realizable Special Hardware Sieving Device for Factoring 1024-bit Integers", *CHES 2005*, LNCS 3659, pp. 119-130, Springer-Verlag, 2005.

[GJK+06] W. Geiselmann, F. Januszewski, H. Köpher, J. Pelzl and R. Steinwandt, "A Simpler Sieving Device: Combining ECM and TWIRL", *ICISC 2006*, LNCS 4296, pp.118-135, Springer-Verlag, 2006.

[GS03] W. Geiselmann and R. Steinwandt. "A Dedicated Sieving Hardware", *PKC 2003*, LNCS 2567, pp. 254-266, Springer-Verlag, 2003.

[GS04] W. Geiselmann and R. Steinwandt, "Yet Another Sieving Device", *CT-RSA 2004*, LNCS 2964, pp. 278-291, Springer-Verlag, 2004.

[GS07] W. Geiselmann and R. Steinwandt, "Non-Wafer-Scale Sieving Hardware for the NFS: Another Attempt to Cope with 1024-bit", *EUROCRYPT 2007*, LNCS 4515, pp.466-481, Springer-Verlag, 2007.

[IPFlex] IPFlex, "DAPDNA Architecture". (Available at `http://www.ipflex.com/en/E1-products/index.html`)

[IKS07] T. Izu, J. Kogure and T. Shimoyama, "CAIRN 2: An FPGA Implementation of the Sieving Step in the Number Field Sievie Method", to appear in *CHES 2007*, 2007.

[KM00] H.J. Kim and W. Mongione-Smith, "Factoring Large Numbers with Programmable Hardware", *FPGA 2000*, pp. 41-48, ACM, 2000.

[LL93] A. Lenstra and H. Lenstra (editors), "The Development of the Number Field Sieve", Vol. 1554 of Lecture Notes in Mathematics (LNM), Springer-Verlag, 1993.

[LLMP90] A. Lenstra, H. Lenstra, M. Manasse and J. Pollard, "The Number Field Sieve", *STOC 1990*, pp. 564-572, ACM, 1990.

[LS00] A. Lenstra and A. Shamir, "Analysis and Optimization of the TWINKLE Factoring Device", *EUROCRYPT 2000*, LNCS 1807, pp. 35-52, Springer-Verlag, 2000.

[LTS+03] A. Lenstra, E. Tromer, A. Shamir, W. Kortsmit, B. Dodson, J. Hughes and P. Leyland, "Factoring Estimates for a 1024-bit RSA Modulus", *ASIACRYPT 2003*, LNCS 2894, pp. 55-74, Springer-Verlag, 2003.

[LSTT02] A. Lenstra, A. Shamir, J. Tomlinson and E. Tromer, "Analysis of Bernstein's Circuit", *ASIACRYPT 2002*, LNCS 2501, pp.1-26, Springer-Verlag, 2002.

[Pol91] J. Pollard, "The Lattice Sieve", pp. 43-49, 1991, in [LL93].

[Sha99] A. Shamir, "Factoring Large Numbers with the TWINKLE Device (Extended Abstract)", *CHES 1999*, LNCS 1717, pp. 2-12, Springer-Verlag, 1999.

[ST03] A. Shamir and E. Tromer, "Factoring Large Numbers with the TWIRL Device", *CRYPTO 2003*, LNCS 2729, pp. 1-26, Springer-Verlag, 2003.

[Xilinx] Xilinx, "Vertex-4 Multi-Platform FPGA". (Available at `http://www.xilinx.com/products/silicon_solutions/fpgas/virtex/virtex4/index.htm`)