Integrate Your Work with LaTeX

Gavin Xiaoxu Yao

PhD Student
Dept. of Electronic Engineering
City University of Hong Kong

香港城市大學
City University
of Hong Kong

Department of
Electronic Engineering

PhD's Documents

- Articles
  - Conference/Journal Paper, Report, Proposal, Thesis
- Slides
- Poster
- Webpage
- Curriculum Vitae
- Data
- Chart

Available Tools

WYSIWYG: what you see is what you get

Makeup language: LaTeX

Capability of LaTeX

- Articles ✓*Of Course!*
  - Conference/Journal Paper, Report, Proposal, Thesis
- Slides ✓
- Poster ✓
- Webpage ✓
- Curriculum Vitae ✓
- Data
- Chart

As capable as Word and PowerPoint.
Available at: https://www.dropbox.com/sh/jyv2gz71x6onbuj/45p4V1NA25

Slides: Beamer

Introduction:

http://en.wikibooks.org/wiki/LaTeX/Presentations

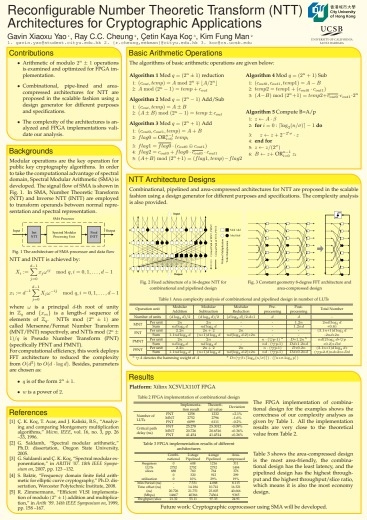
Tutorial:

http://www.uncg.edu/cmp/reu/presentations/CharlesBatts-BeamerTutorial.pdf

Poster

Available at:

http://www.brian-amberg.de/uni/poster/



Reconfigurable Number Theoretic Transform (NTT) Architectures for Cryptographic Applications

Gavin Xiaoxu Yao [1], Ray C.C. Cheung [2], Çetin Kaya Koç [3], Kim Fung Man [2]
1. gavin.yao@student.cityu.edu.hk 2. {r.cheung,eekman}@cityu.edu.hk 3. koc@cs.ucsb.edu

Contributions

- Arithmetic of modulo $2^n \pm 1$ operations is examined and optimized for FPGA implementation.
- Combinational, pipe-lined and area-compressed architectures for NTT are proposed in the scalable fashion using a design generator for different purposes and specifications.
- The complexity of the architectures is analyzed and FPGA implementations validate our analysis.

Backgrounds

Modular operations are the key operation for public key cryptography algorithms. In order to take the computational advantage of spectral domain, Spectral Modular Arithmetic (SMA) is developed. The signal flow of SMA is shown in Fig. 1. In SMA, Number Theoretic Transform (NTT) and Inverse NTT (INTT) are employed to transform operands between normal representation and spectral representation.

Fig. 1 The architecture of SMA processor and data flow

NTT and INTT is achieved by:

$$X_i := \sum_{j=0}^{d-1} x_j \omega^{ij} \mod q, i = 0, 1, \ldots, d-1$$

$$x_i := d^{-1} \sum_{j=0}^{d-1} X_j \omega^{-ij} \mod q, i = 0, 1, \ldots, d-1$$

where ω is a principal d-th root of unity in $\mathbb{Z}_q$ and $\{x_m\}$ is a length-d sequence of elements of $\mathbb{Z}_q$. NTTs mod $(2^n \pm 1)$ are called Mersenne/Fermat Number Transform (MNT/FNT) respectively, and NTTs mod $(2^n \pm 1)/q$ is Pseudo Number Transform (PNT) (specifically PFNT and PMNT).
For computational efficiency, this work deploys FFT architecture to reduced the complexity from $O(d^2)$ to $O(d \cdot \log d)$. Besides, parameters are chosen as:

- q is of the form $2^n \pm 1$.
- w is a power of 2.

Basic Arithmetic Operations

The algorithms of basic arithmetic operations are given below:

```
Algorithm 1 Mod $q = (2^n \pm 1)$ reduction
1: $(c_{out}, temp) = A \bmod 2^n \mp \lfloor A/2^n \rfloor$
2: $A \bmod (2^n - 1) = temp + c_{out}$

Algorithm 2 Mod $q = (2^n - 1)$ Add/Sub
1: $(c_{out}, temp) = A \pm B$
2: $(A \pm B) \bmod (2^n - 1) = temp \pm c_{out}$

Algorithm 3 Mod $q = (2^n + 1)$ Add
1: $(c_{out0}, c_{out1}, temp) = A + B$
2: $flag0 = \mathrm{OR}_{i=0}^{n-1}\ temp_i$
3: $flag1 = \overline{flag0} \cdot (c_{out0} \oplus c_{out1})$
4: $flag2 = c_{out0} + flag0 \cdot \overline{c_{out0}} \cdot c_{out1}$
5: $(A+B) \bmod (2^n+1) = (flag1, temp) - flag2$

Algorithm 4 Mod $q = (2^n + 1)$ Sub
1: $(c_{out0}, c_{out1}, temp1) = A - B$
2: $temp2 = temp1 + (c_{out0} \cdot c_{out1})$
3: $(A-B) \bmod (2^n+1) = temp2 + \overline{c_{out0}} \cdot c_{out1} \cdot 2^n$

Algorithm 5 Compute B=A/p
1: $z \leftarrow A \cdot \beta$
2: for $i = 0 : \lceil \log_2(n/\sigma) \rceil - 1$ do
3:     $z \leftarrow z + 2^{-2^i \sigma} \cdot z$
4: end for
5: $z \leftarrow z/(2^\sigma)$
6: $B \leftarrow z + \mathrm{OR}_{i=0}^{n-1}\ z_i$
```

NTT Architecture Designs

Combinational, pipelined and area-compressed architectures for NTT are proposed in the scalable fashion using a design generator for different purposes and specifications. The complexity analysis is also provided.

Fig. 2 Fixed achitecture of a 16-degree NTT for combinational and pipelined design

Fig. 3 Constant geometry 8-degree FFT architecture and area-compressed design

Table 1 Area complexity analysis of combinational and pipelined design in number of LUTs

Operation unit		Modular Addition	Modular Subtraction	Modular Reduction	Pre-processing	Post-processing	Total Number
Number of units		$(d\log_2 d)/2$	$(d\log_2 d)/2$	$(d\log_2 d)/2$-d+1	d	d	-
MNT	Per unit	$2n$	$2n$	-	-	$1.2n$	$2nd(\log_2 d$ $+0.6)$
	Sum	$nd\log_2 d$	$nd\log_2 d$	-	-	$1.2nd$	
FNT	Per unit	$2.2n$	$2n+2$	$2n$	-	-	$(3.1n+1)d\log_2 d$ $-2nd+2n$
	Sum	$1.1nd\log_2 d$	$(n+1)d\log_2 d$	$nd(\log_2 d$-2$)+2n$	-	-	
PMNT	Per unit	$2n$	$2n$	-	$n \cdot (\nabla p$-1$)$ [a]	$D+1.2n$ [b]	$nd(2\log_2 d+\nabla p$ $+0.2)+Dd$
	Sum	$nd\log_2 d$	$nd\log_2 d$	-	$nd \cdot (\nabla p$-1$)$	$Dd+1.2nd$	
PFNT	Per unit	$2.2n$	$2n+2$	$2n$	$n \cdot (\nabla p$-1$)$	$D+0.2n$	$(3.1n+1)d\log_2 d+$ $(\nabla p$-2.8$)nd+2n+Dd$
	Sum	$1.1nd\log_2 d$	$(n+1)d\log_2 d$	$nd(\log_2 d$-2$)+2n$	$nd \cdot (\nabla p$-1$)$	$Dd+0.2nd$	

[a] ∇A denotes the hamming weight of A
[b] D=$(\nabla\beta+\lceil\log_2(n/\sigma)\rceil) \cdot (\lceil n+\sigma$-$\log_2 p\rceil)$

Results

Platform: Xilinx XC5VLX110T FPGA

Table 2 FPGA implementation of combinational design

		Implementation result	Theoretical value	Deviation
Number of LUTs	FNT	1258	1232	+2.1%
	MNT	2752	2796	-1.6%
	PNT	6099	6111	-0.2%
Critical path delay (ns)	FNT	25.278	25.3012	-0.09%
	MNT	20.726	20.6516	+0.36%
	PNT	41.454	41.4514	+0.26%

The FPGA implementation of combinational design for the examples shows the correctness of our complexity analyses as given by Table 1. All the implementation results are very close to the theoretical value from Table 2.

Table 3 FPGA implementation results of different architectures

	Combinational	2-stage Pipelined	4-stage Pipelined	Area-compressed
#registers	0	608	1216	311
LUTs	2752	2752	2752	1494
slices	688	760	764	376
	0	320	912	299
utilization	0	10%	29%	19%
Min Period (ns)	-	7.531	4.088	8.115
Time offset (ns)	-	14.184	10.741	16.321
(ns)	20.726	21.751	23.005	40.666
(Mbps)	14667	40366	74364	9365
Thr.ghput/slice	21.32	53.11	97.33	24.91

Table 3 shows the area-compressed design is the most area-friendly, the combinational design has the least latency, and the pipelined design has the highest throughput and the highest throughput/slice ratio, which means it is also the most economy design.

Future work: Cryptographic coprocessor using SMA will be developed.

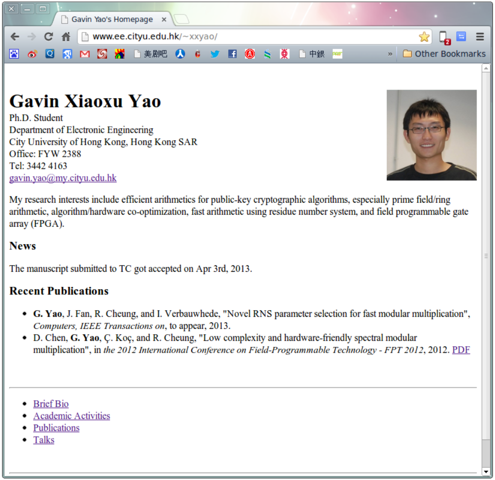
References

[1] Ç. K. Koç, T. Acar, and J. Kaliski, B.S., "Analyzing and comparing Montgomery multiplication algorithms," *Micro, IEEE*, vol. 16, no. 3, pp. 26 –33, 1996.
[2] G. Saldamh, "Spectral modular arithmetic," Ph.D. dissertation, Oregon State University, 2005.
[3] G. Saldamli and Ç. K. Koç, "Spectral modular exponentiation," in *ARITH '07. 18th IEEE Symposium on*, 2007, pp. 123 –132.
[4] S. Baktir, "Frequency domain finite field arithmetic for elliptic curve cryptography," Ph.D. dissertation, Worcester Polytechnic Institute, 2008.
[5] R. Zimmermann, "Efficient VLSI implementation of modulo $(2^n \pm 1)$ addition and multiplication," in *Arith '99. 14th IEEE Symposium on*, 1999, pp. 158 –167.

Webpage

LaTeX2`html`

`http://www.latex2html.org/`



Gavin Xiaoxu Yao

Ph.D. Student
Department of Electronic Engineering
City University of Hong Kong, Hong Kong SAR
Office: FYW 2388
Tel: 3442 4163
gavin.yao@my.cityu.edu.hk

My research interests include efficient arithmetics for public-key cryptographic algorithms, especially prime field/ring arithmetic, algorithm/hardware co-optimization, fast arithmetic using residue number system, and field programmable gate array (FPGA).

News

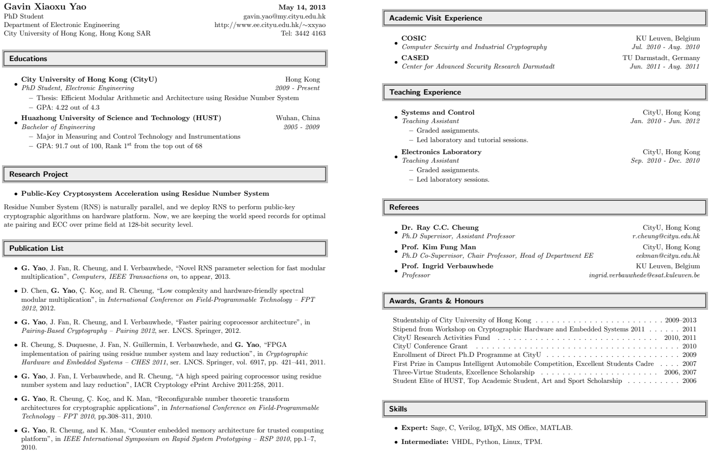
The manuscript submitted to TC got accepted on Apr 3rd, 2013.

Recent Publications

- **G. Yao**, J. Fan, R. Cheung, and I. Verbauwhede, "Novel RNS parameter selection for fast modular multiplication", *Computers, IEEE Transactions on*, to appear, 2013.
- D. Chen, **G. Yao**, Ç. Koç, and R. Cheung, "Low complexity and hardware-friendly spectral modular multiplication", in *the 2012 International Conference on Field-Programmable Technology - FPT 2012*, 2012. PDF

- Brief Bio
- Academic Activities
- Publications
- Talks

CV



Gavin Xiaoxu Yao — **May 14, 2013**
PhD Student — gavin.yao@my.cityu.edu.hk
Department of Electronic Engineering — http://www.ee.cityu.edu.hk/~xxyao
City University of Hong Kong, Hong Kong SAR — Tel: 3442 4163

Educations

- **City University of Hong Kong (CityU)** — Hong Kong
  PhD Student, Electronic Engineering — *2009 - Present*
  - Thesis: Efficient Modular Arithmetic and Architecture using Residue Number System
  - GPA: 4.22 out of 4.3
- **Huazhong University of Science and Technology (HUST)** — Wuhan, China
  Bachelor of Engineering — *2005 - 2009*
  - Major in Measuring and Control Technology and Instrumentations
  - GPA: 91.7 out of 100, Rank 1st from the top out of 68

Research Project

- **Public-Key Cryptosystem Acceleration using Residue Number System**

Residue Number System (RNS) is naturally parallel, and we deploy RNS to perform public-key cryptographic algorithms on hardware platform. Now, we are keeping the world speed records for optimal ate pairing and ECC over prime field at 128-bit security level.

Publication List

- **G. Yao**, J. Fan, R. Cheung, and I. Verbauwhede, "Novel RNS parameter selection for fast modular multiplication", *Computers, IEEE Transactions on*, to appear, 2013.
- D. Chen, **G. Yao**, Ç. Koç, and R. Cheung, "Low complexity and hardware-friendly spectral modular multiplication", in *International Conference on Field-Programmable Technology – FPT 2012*, 2012.
- **G. Yao**, J. Fan, R. Cheung, and I. Verbauwhede, "Faster pairing coprocessor architecture", in *Pairing-Based Cryptography – Pairing 2012*, ser. LNCS. Springer, 2012.
- R. Cheung, S. Duquesne, J. Fan, N. Guillermin, I. Verbauwhede, and **G. Yao**, "FPGA implementation of pairing using residue number system and lazy reduction", in *Cryptographic Hardware and Embedded Systems – CHES 2011*, ser. LNCS. Springer, vol. 6917, pp. 421–441, 2011.
- **G. Yao**, J. Fan, I. Verbauwhede, and R. Cheung, "A high speed pairing coprocessor using residue number system and lazy reduction", IACR Cryptology ePrint Archive 2011:258, 2011.
- **G. Yao**, R. Cheung, Ç. Koç, and K. Man, "Reconfigurable number theoretic transform architectures for cryptographic applications", in *International Conference on Field-Programmable Technology – FPT 2010*, pp.308–311, 2010.
- **G. Yao**, R. Cheung, and K. Man, "Counter embedded memory architecture for trusted computing platform", in *IEEE International Symposium on Rapid System Prototyping – RSP 2010*, pp.1–7, 2010.

Academic Visit Experience

- **COSIC** — KU Leuven, Belgium
  Computer Secuirty and Industrial Cryptography — *Jul. 2010 - Aug. 2010*
- **CASED** — TU Darmstadt, Germany
  Center for Advanced Security Research Darmstadt — *Jun. 2011 - Aug. 2011*

Teaching Experience

- **Systems and Control** — CityU, Hong Kong
  Teaching Assistant — *Jan. 2010 - Jun. 2012*
  - Graded assignments.
  - Led laboratory and tutorial sessions.
- **Electronics Laboratory** — CityU, Hong Kong
  Teaching Assistant — *Sep. 2010 - Dec. 2010*
  - Graded assignments.
  - Led laboratory sessions.

Referees

- **Dr. Ray C.C. Cheung** — CityU, Hong Kong
  Ph.D Supervisor, Assistant Professor — *r.cheung@cityu.edu.hk*
- **Prof. Kim Fung Man** — CityU, Hong Kong
  Ph.D Co-Supervisor, Chair Professor, Head of Department EE — *eekman@cityu.edu.hk*
- **Prof. Ingrid Verbauwhede** — KU Leuven, Belgium
  Professor — *ingrid.verbauwhede@esat.kuleuven.be*

Awards, Grants & Honours

Studentship of City University of Hong Kong	2009–2013
Stipend from Workshop on Cryptographic Hardware and Embedded Systems 2011	2011
CityU Research Activities Fund	2010, 2011
CityU Conference Grant	2010
Enrollment of Direct Ph.D Programme at CityU	2009
First Prize in Campus Intelligent Automobile Competition, Excellent Students Cadre	2007
Three-Virtue Students, Excellence Scholarship	2006, 2007
Student Elite of HUST, Top Academic Student, Art and Sport Scholarship	2006

Skills

- **Expert:** Sage, C, Verilog, LaTeX, MS Office, MATLAB.
- **Intermediate:** VHDL, Python, Linux, TPM.

My Setting

- OS: Ubuntu
  - http://www.ubuntu.com/
- LaTeX: texlive
  - bash: sudo apt-get install texlive-full
- Editor: gvim + vim-latex-suite
  - Vim: http://www.vim.org/
  - Vim-latex-suite: http://vim-latex.sourceforge.net/

Frame

Basic Frame

```
\begin{frame}[<alignment>]
  \frametitle{Frame Title Goes Here}
  Frame body text and/or LaTeXcode
\end{frame}
```

Useful [<alignment>]: [plain]

Lists

Itemize

```
\begin{itemize}
  \item The first item
  \item The second item
\end{itemize}
```

- The first item
- The second item

Enumerate

```
\begin{enumerate}
  \item The first item
  \item The second item
\end{enumerate}
```

1. The first item
2. The second item

Another one is description: \item[1st] The first item

Text

Font Size

\Huge

\huge

\Large

\large

\normalsize

\small

\footnotesize

\scriptsize

\tiny

Fonts

\textbf{**Sample**}

\textit{*Sample*}

\textsf{Sample}

\textsl{*Sample*}

\textrm{Sample}

\emph{*Sample*}

\alert{Sample}

\textcolor{yourcolor}{Sample}

Space

Space

\vspace{0.5cm}

\hspace{.1\textwidth}

Alignment

\centering

\raggedleft

\raggedright

Block and Columns

Block

```
\begin{block}{Block title}
  Content here
\end{block}
```

Columns

```
\begin{columns}
  \column{.5\textwidth}
    Column 1 content
  \column{.5\textwidth}
    Column 2 content
\end{columns}
```

Table and Figure

Block

```
\begin{tabular}{<alignment>}
   Sth. & Sth. & Sth. \\
   Sth. & Sth. & Sth. \\
   Sth. & Sth. & Sth.
\end{tabular}
```

Figure

```
\includegraphics[width=.5\textwidth]{figure/cityu_logo.JPG}
```

Animation

Animation

```
\pause

\visible<number>{visible text}
\invisible<number>{invisible text}

\textcolor<2>{blue}{change color later}

\begin{itemize}[<+->]
  \item<1-> The first item
  \item<2> The second item
\end{itemize}

\usepackage{xmpmulti}
\multiinclude[format=pdf,graphics={scale=0.06},position={0,0}]
      {figure/dualmodemul}
```

Title Page

Preamble

```
\title[short title]{long title}
\subtitle[short subtitle]{long subtitle}
\author[short author]{long author}
\date[short date]{long date}
\institution[short name]{long name}
```

Title Frame

```
\begin{frame}
  \titlepage
\end{frame}
```

Section

Section

```
\section{Section Name}
  \subsection{SubSection Name}
  \subsection*{SubSection Name}
```

Table of Contents

```
\begin{frame}<beamer>
  \frametitle{Agenda}
  \tableofcontents
\end{frame}
```

```
\begin{frame}<beamer>
  \frametitle{Agenda}
  \tableofcontents[currentsection,currentsubsection]
\end{frame}
```

Themes

Usage

```
\usetheme{Warsaw}
```

Themes

Antibes Bergen Berkeley Berlin
Boadilla Copenhagen Darmstadt Dresden
Frankfurt Goettingen Hannover Ilmenau
Juanlespins Madrid Malmoe Marburg
Montpellier Paloalto Pittsburgh Rochester
Singapore Warsaw

Remarks

I am not sales.

- LaTeX is not better than other tools.
- I use it because I am lazy.
- Changing habit is not comfortable.

One tip on Presentation: Keep it Simple

- Simple language to be heard
- Simple structure to be absorbed
- Simple example for easy learning
- Simple layout to focus

Finally,

- One cannot make a silk purse out of a sow’s ear.
  巧妇难为无米之炊.