Efficient implementation of multivariate quadratic polynomial on Graphics Processing Units

Kouichi SAKURAI
Kyushu Univ. JAPAN

NSC-JST Joint workshop on “ICT”
27th-28th Nov 2012

My Personal/Academic with 台湾

- First visit 台湾（台北, 台南or 高雄?）2000??
- 2003
  - 37th IEEE International Carnahan Conference on Security Technology (ICCST '03), Oct 台北
  - 9th Asiacrypt'2003, Dec 台北 (by Chi Sung Laih)
- 2007: MOU between ISIT and TWISC & NTUST
  - Institute of Systems and Information Technology (福岡市)
  - Taiwan Information Security Center (by D.T.Lee)
  - NTUST：School of management, National Taiwan University of Science and Technology (by T.C. Wu)

My Personal/Academic 台湾　(II)

- 2008: **Japan-Taiwan Joint Research on Cryptography and Information Security towards next IT-society**
- 福岡　FUKUOKA SRP Center Building, Fukuoka, Japan, October
-
- Hosted by Institute of Systems, Information Technologies and Nanotechnologies(ISIT) and Interchange Association, Japan (IAJ　交流協会).
- Sponsored by National Science Council and Taipei Economic & Cultural Representative Office in Japan.

- The research of Cryptography and Information Security has many topics, from theory to application including policy, and it is international. This joint-seminar would enhance the researchers both of Japan and Taiwan to collaboration with understanding each major research areas, and complement the difference of their original research topics towards the next step of explicit joint-research with individual researchers.

2nd Japan-Taiwan Joint Research Symposium on Cryptography and Information Technology toward Next IT-society 2010 NOV. 15th-16th

漢来大飯店 (15F, Chatter Room) 高雄市

- 李徳財（Dr. Der-Tsai Lee, Academician）中央研究院（Academia Sinica）
  呉宋成（Prof. Tzong-Chen Wu, Ph.D.） 中華民国資通安全学会 理事長
- 官大智（国立中山大学), 楊中皇（国立高雄師範大学), 莊文勝(国立高雄第一科技大学)
- 羅乃維（国立台湾科技大学） ，陳Chia Mei（国立中山大学)
- 簡宏宇(（National Chi Nan Univ.), 范俊逸 (国立中山大学)
- 鄭振牟（国立台湾大学), 楊柏因（中央研究院)
- 王智弘（国立嘉義大学), 郭文中（国立虎尾科技大学)

岡本栄司（Eiji Okamoto, Ph.D.） 筑波大学 (University of Tsukuba)
満保雅浩（Masahiro Mambo, Ph.D.） 筑波大学 (University of Tsukuba)
金岡晃 （Akira Kanaoka, Ph.D.） 筑波大学 (University of Tsukuba)
櫻井幸一（Sakurai Kouichi, Ph.D.）九州大学 (Kyushu University) / *1
佐久間淳（Jun Sakuma, Ph.D.） 筑波大学 (University of Tsukuba)
安藤類央（Ruo Ando, Ph.D. 情報通信研究機構（NICT)）
崎山一男（Kazuo Sakiyama, Ph.D.） 電気通信大学 (The University of Electro-Communications）
松浦幹太（Kanta Matsuura, Ph.D.） 東京大学 (The University of Tokyo）
西出隆志（九州大学） 江藤文治（九州先端科学技術研究所）
et.al.

Some of my Supervised 台湾留学生

- En-Jung Farn (2010)
  - **Ph.D Student of Dept of Computer Science National Tsing Hua University**
  - **父 Prof. Dr. FARN**
  - **En-Jung Farn** and Chaur-Chin Chen,
    "Jigsaw puzzle images for steganography,"
    Optical Engineering, 48(7): 077006 (July 2009) **(SCIE)**
- **周士博**
  - **Ms student (Now working with NIFTY日本)**
  - **"Detecting Primary User Emulation Attack with Two Users Cooperative Scheme in cognitive radio networks"**
  - **母：Prof. Wuu Lih-Chau (国立雲林科技大學)**

Brief History of Multivariate Quadratic Crypto

- Matsumoto-Imai Eurocrypt 1988
    - RSA (1978) Elliptic Curve Crypto (1985)
- Based on multivariate quadratic polynomials.
    - Note that Solving systems of multivariate polynomial equations is proved to be NP-complete
- Attacked by Pataran (Crypto'95)
- Modified by Pataran et al (EuroCrypt'96~)
    - Oil and Vinegar (Attacked and Revised .....)

Post-Quantum Cryptography (after Shor 1994)

- Shor FOCS'9 4
  - “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer”
- No more RSA nor ECC if Quantum Computer
- Cryptostems from NP-complete problme
  - ReInvente Matsumoto-Imai ! E.g Rainbow (2005)
- 4th PQ-crypto workshop, 2011 台北
  - Program Chair: Bo-Yin Yang (Academia Sinica)
  - General chair: Chen-Mou Cheng (NTU)

Two Aspects of Fast computation on Cryptography

- Efficent implementation of crypto-algorithms
  - Today's talk on GPU faster on Stream cipher
- Cryptanalysis via Fast Processors
  - **ECC2K-130 on NVIDIA GPUs [IndoCrypt2010]**
  - D. J. Bernstein and H-C Chen and C-M Cheng and T. Lange and R. Niederhagen and P. Schwabe and B-Y Yang (欧米台)
  - Certicom ECC2K-130 challenge is to compute an elliptic-curve discrete logarithm on a Koblitz curve over F_2^131, of which cost of the computation to approximately 2^77 bit operations in 2^61 iterations.
  - Rresulting GPU software performs more than 63 million iterations per second, including 320 million F_2^131 multiplications per second, on a $500 NVIDIA GTX 295 graphics card.

Histroy of Today’ Research Introduction with 台湾

- 2011Oct. “Fast Implementation and Experimentation of Multivariate Polynomial Cryptosystems on GPU,” 6th Joint Workshop on Information Security (JWIS2011), 高雄/台湾 by S.Tanaka, T.Nishide & K. SAKURAI

- 2011 Nov. : Send Mr.Tanaka(1st PhD) to Prof. ChengM.Cheng &Dr. BI Yang

- 2012a “Efficient Implementation of Evaluating Multivariate Quadratic System with GPUs,” 6th International Workshop on Advances in Information Security(WAIS 2012), by S.Tanaka, T.Nishide & K. SAKURAI
- 2012b "Efficient Parallel Evaluation of Multivariate Quadratic Polynomials on GPUs,” 13th International Workshop on Information Security Applications(WISA 2012) by S. Tanaka, T. Chou, Bo-Yin Yang, Chen-Mou Cheng,& Kouichi Sakurai

Efficient Parallel Evaluation of Multivariate Quadratic Polynomials on GPUs

Satoshi Tanaka[†], Tung Chou[‡],
Bo-Yin Yang,[‡] Chen-Mou Cheng,[*]
Kouichi Sakurai[†]

[†] Kyushu University, Japan
[‡] Academia Sinika, Taipei, Taiwan
[*] National Taiwan University, Taipei, Taiwan

This work is partially supported by JST,
Strategic Japanese-Indian Cooperative Program on Multidisciplinary Research Field,
which combines Information and Communications Technology with Other Fields

Introduction

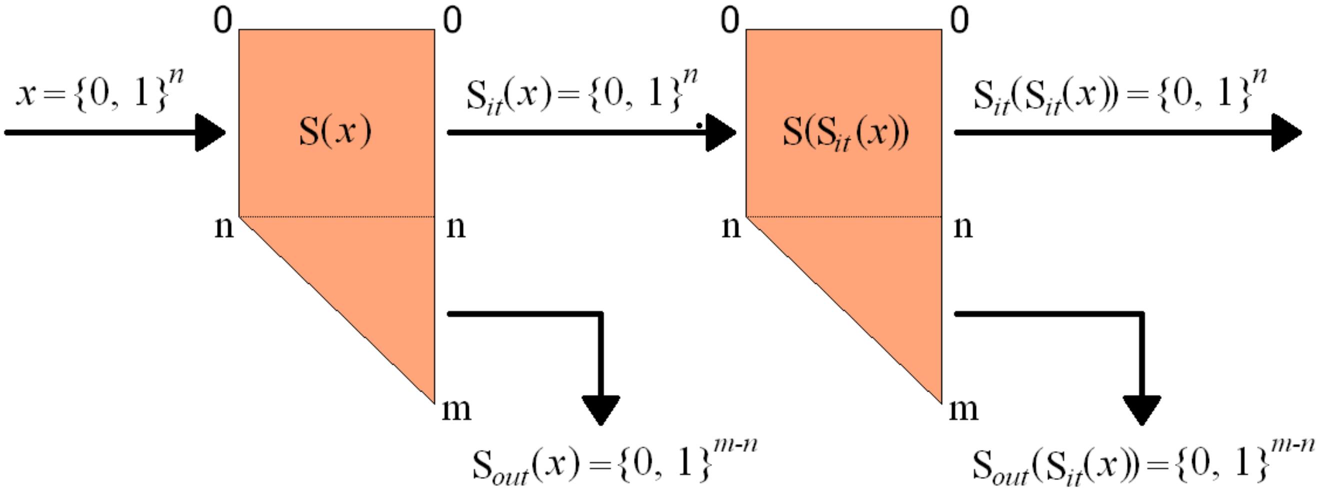
- Multivariate cryptography
  - Public key: multivariate polynomial system
    - e.g. n unknowns and m polynomials system

$$\begin{cases} f_1(x_1, \dots, x_n) = \alpha_1 + \sum_{i=1}^{n} \beta_{1,i} x_i + \sum_{i=1}^{n} \sum_{j=i}^{n} \gamma_{1,i,j} x_i x_j + \cdots \\ \vdots \\ f_m(x_1, \dots, x_n) = \alpha_m + \sum_{i=1}^{n} \beta_{m,i} x_i + \sum_{i=1}^{n} \sum_{j=i}^{n} \gamma_{m,i,j} x_i x_j + \cdots \end{cases}$$

  - Security: hardness of solving systems

QUAD Stream Cipher[EuroCrypt2009]

- It uses a multivariate quadratic polynomial system as a pseudorandom keystream generator
  - QUAD(q, n, r)
    - n unknowns and $m(= n + r)$ polynomials system over $\mathbb{GF}(q)$


0
0
0
0
$x = \{0, 1\}^n$
$S(x)$
$S_{it}(x) = \{0, 1\}^n$
$S(S_{it}(x))$
$S_{it}(S_{it}(x)) = \{0, 1\}^n$
n
n
n
n
m
m
$S_{out}(x) = \{0, 1\}^{m\text{-}n}$
$S_{out}(S_{it}(x)) = \{0, 1\}^{m\text{-}n}$

QUAD Stream Cipher

- Security
  - It depends on the hardness of the multivariate quadratic (MQ) problem
  - It has a provable security

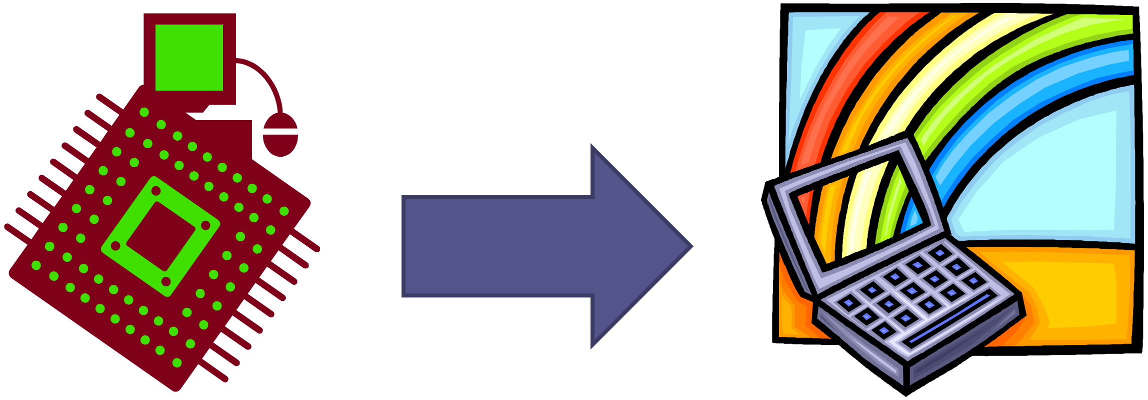
- Speed
  - It is slow compared with other symmetric ciphers
    - It requires $\frac{m(n+1)(n+2)}{2}$ multiplications and additions

GPGPU

- It is a technique for performing general-purpose computation with Graphical Processing Units (GPUs)
    - GPU has a large amount of power of computation
- GPUs have a SIMD architecture
    - It is better to handle several simple tasks

GPGPU for NVIDIA Architecures

- CUDA API
  - Develop environment for GPU based on C language



host
(computer)

device
(GPU)

Related Works

- Efficient implementations of Berbain et al. [BBG]
    - ▫ They showed some strategies of efficient implementations for multivariate cryptography
    - ▫ They implemented several multivariate cryptosystems
        - The throughput of QUAD(2,160,160) is 8.45 Mbps

[BBG]Berbain C., Billet, O., and Gilbert, H.,
“Efficient Implementations of Multivariate Quadratic Systems.” In Computer Science 2007.

Implementation Strategy

- Reduce computational cost
  - Use strategies of Berbain et al.[BBG]
    - Variables are treated as vectors
    - Precompute each quadratic term $x_i x_j$
    - Compute only non-zero terms in $\mathbb{GF}(q)$
- Parallelize computation of multivariate quadratic polynomial systems

[BBG]Berbain C., Billet, O., and Gilbert, H.,
"Efficient Implementations of Multivariate Quadratic Systems." In Computer Science 2007.

Basic Strategy of Parallelization

- Assume that $\alpha_{i,j} = 0 \ (i > j)$, $t_{i,j} = \alpha_{i,j} x_i x_j$

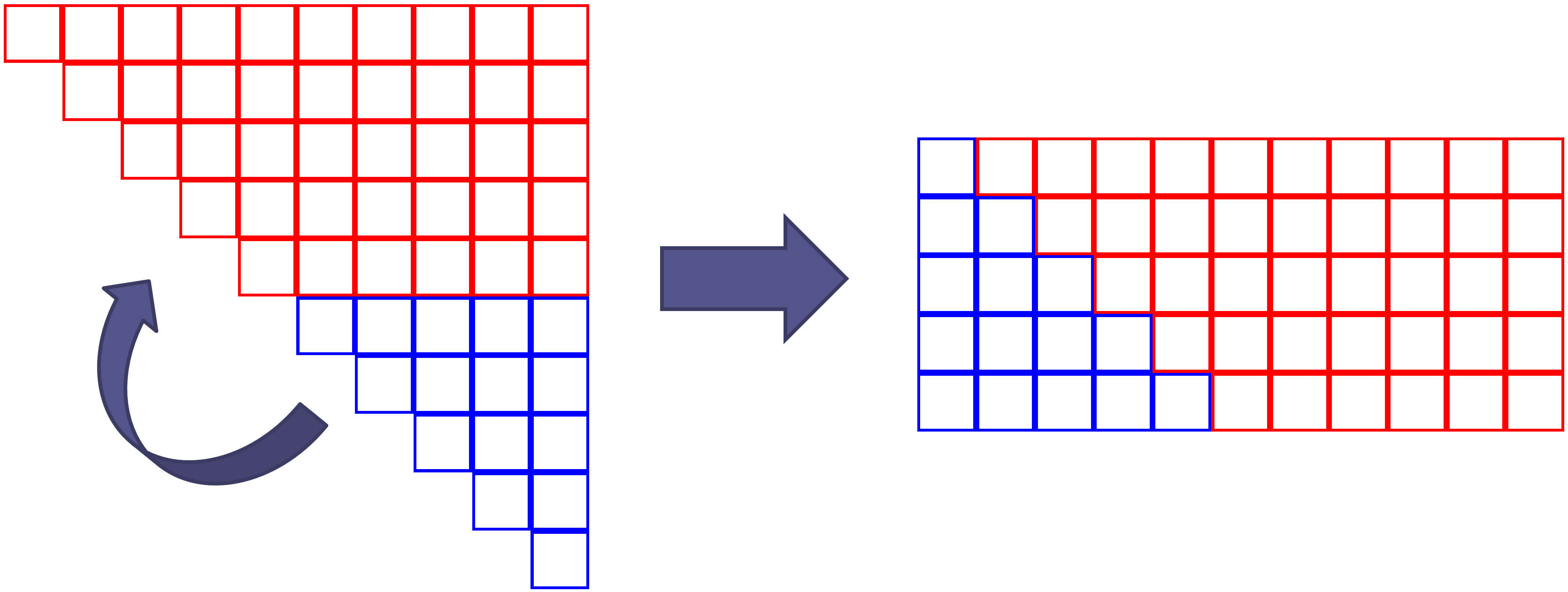
$$\sum_{1 \le i \le j \le n} \alpha_{i,j} x_i x_j = \sum_{1 \le i \le n} \sum_{1 \le j \le n} t_{i,j}$$

- Compute a matrix
  1. Compute $S_k(x) = \sum_{i=1}^{n} t_{i,j}$
  2. Compute $\sum_{k=1}^{n} S_k(x)$

	1	2		n-1	n
1	$t_{1,1}$	$t_{1,2}$	$\cdots$	$t_{1,n\text{-}1}$	$t_{1,n}$
2	0	$t_{2,2}$	$\cdots$	$t_{2,n\text{-}1}$	$t_{2,n}$
	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
n-1	0	0	$\cdots$	$t_{n\text{-}1,n\text{-}1}$	$t_{n\text{-}1,n}$
n	0	0	$\cdots$	0	$t_{n,n}$

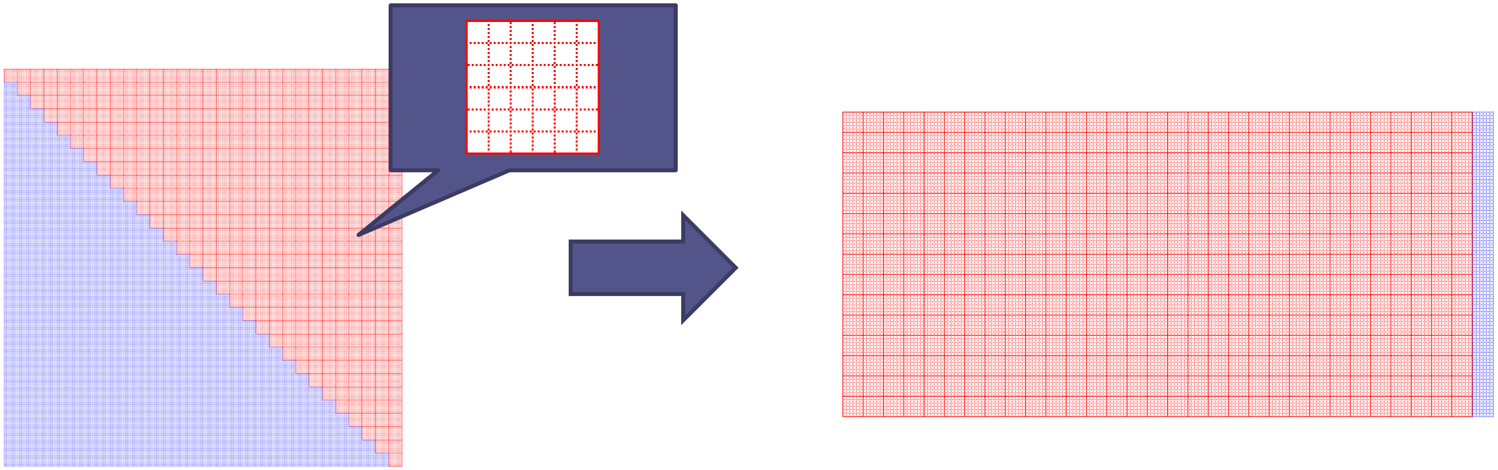
Parallelization Method 1

- Reshape triangular to rectangle matrix



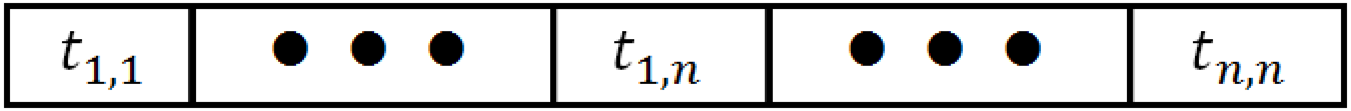
Parallelization Method 1

- Optimization on NVIDIA GeForce GTX 580
  - Setting non-zero variables to groups every 31 non-zero variables as k-set.
  - Assuming a 31k-degree triangular matrix
    - Reshape to a 16k×31k (as 15k×32k) rectangle matrix

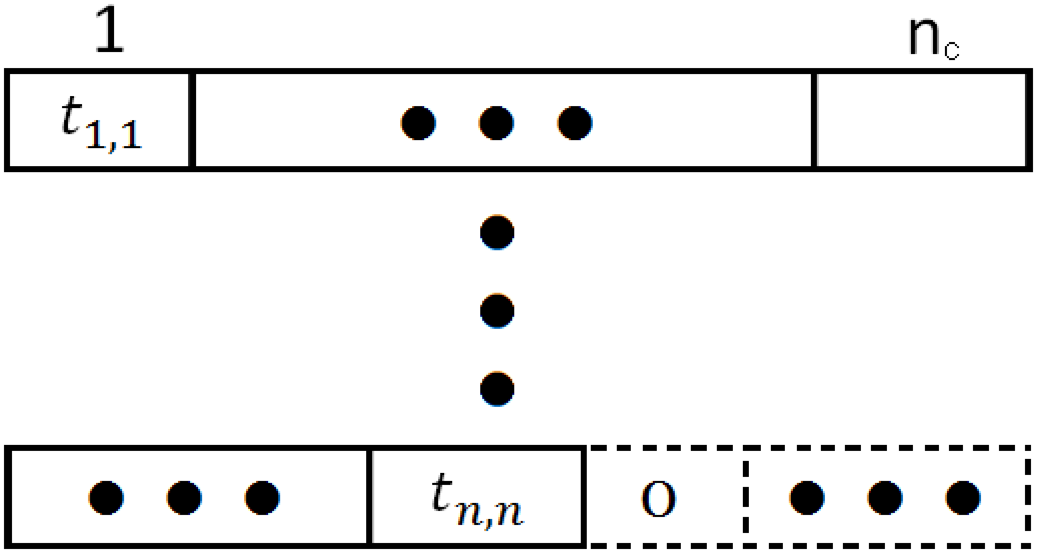


Parallelization Method 2

- Treat a polynomial as a vector



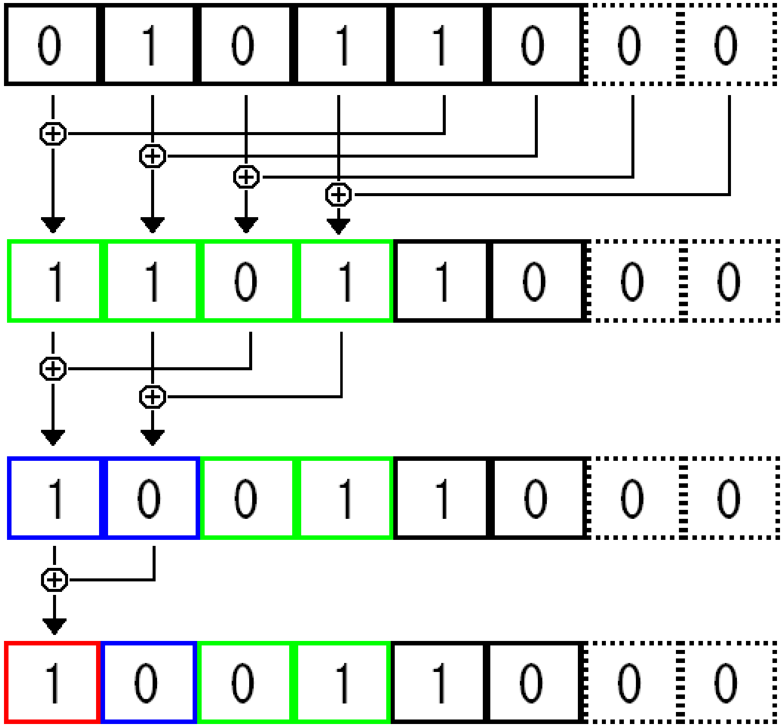
- Separate subvectors



Parallelization Method 2

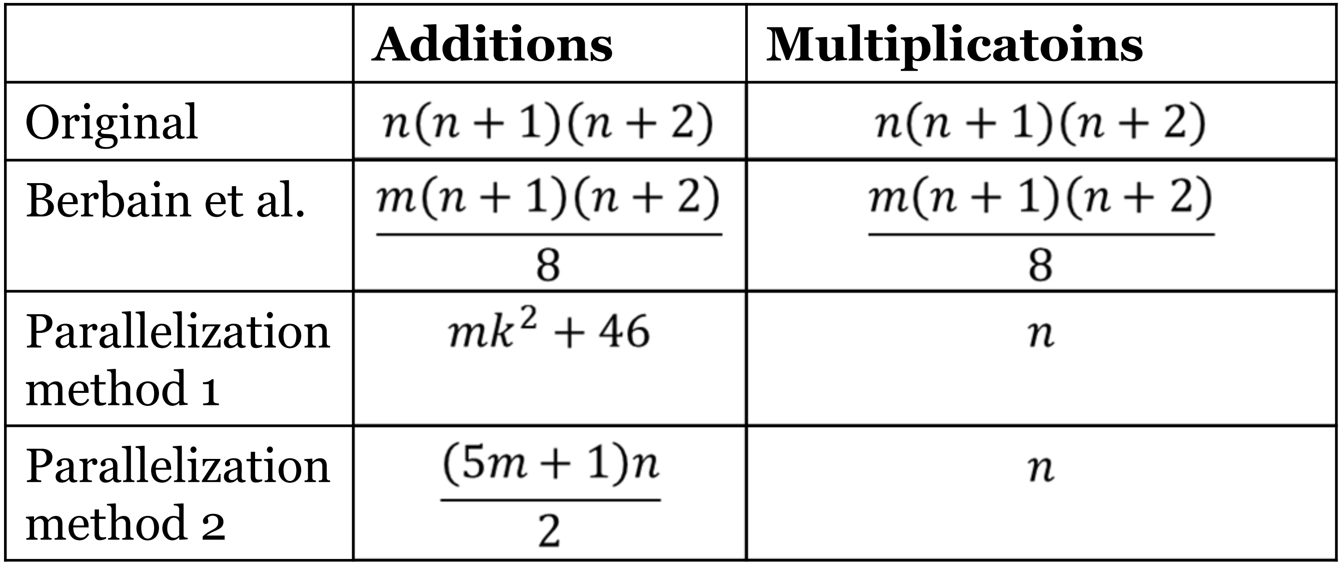
- Parallel reduction technique

1. Substitute the length of subvectors for n_c
2. $x_i = x_i + x_{\frac{n_c}{2}+i}$
3. $n_c = n_c/2$
4. When $\mathrm{n_c} > 1$, iterate step 2 and 3



Analysis

- Computational time of QUAD$(2, n, n)$



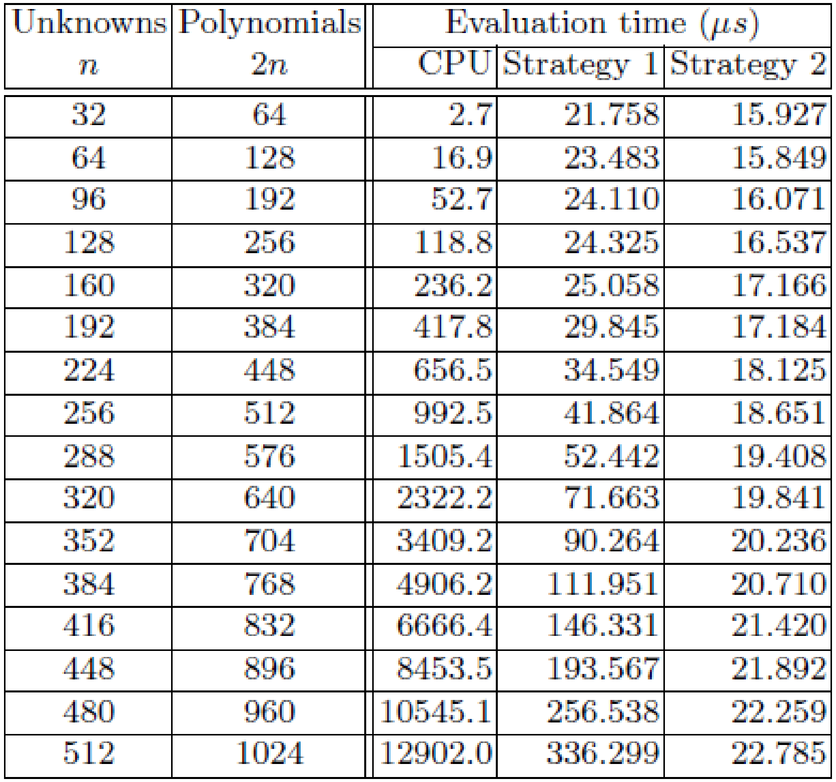
	Additions	**Multiplicatoins**
Original	$n(n+1)(n+2)$	$n(n+1)(n+2)$
Berbain et al.	$\frac{m(n+1)(n+2)}{8}$	$\frac{m(n+1)(n+2)}{8}$
Parallelization method 1	mk^2+46	n
Parallelization method 2	$\frac{(5m+1)n}{2}$	n

$(m = 2n/32)$

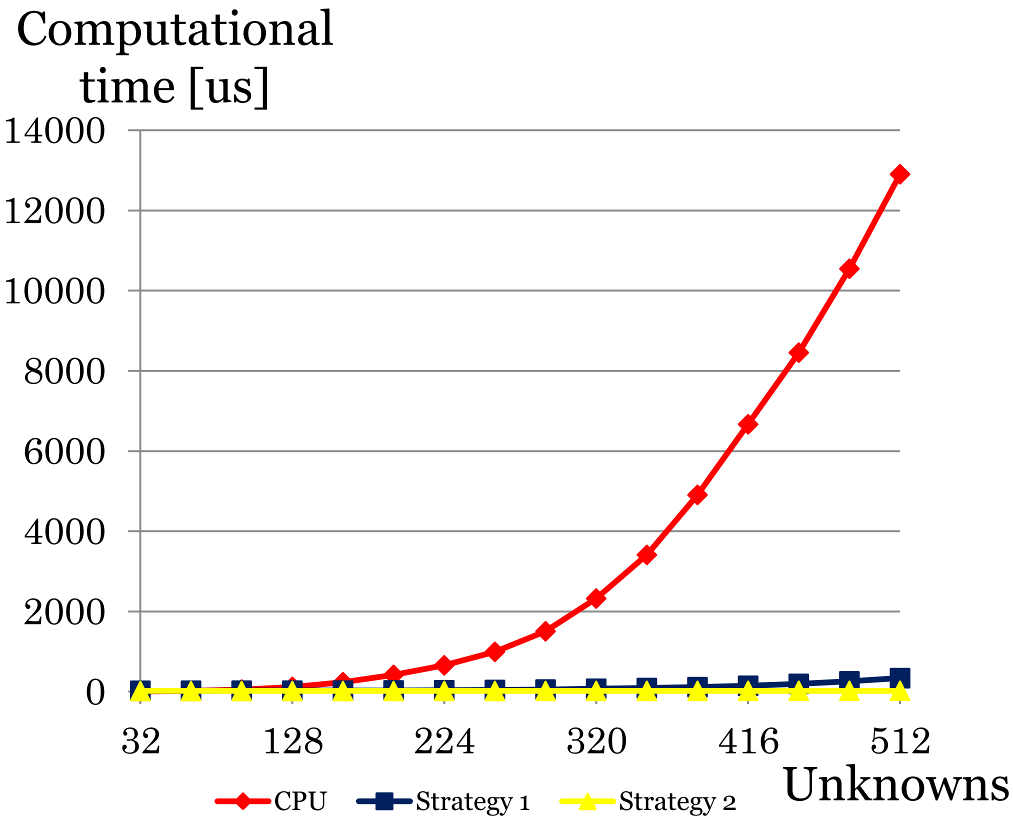
Experimentation

- Implement n unknowns and $2n$ polynomials system on CPU and GPU
  - $n = 32, 64, 96, \dots, 512$
- Implementation environment
  - CPU: Intel Core i7
  - GPU: NVIDIA GeForce GTX 580
  - Memory: 8 GB
  - Languages:
    - CPU: C language, GPU: CUDA

Result

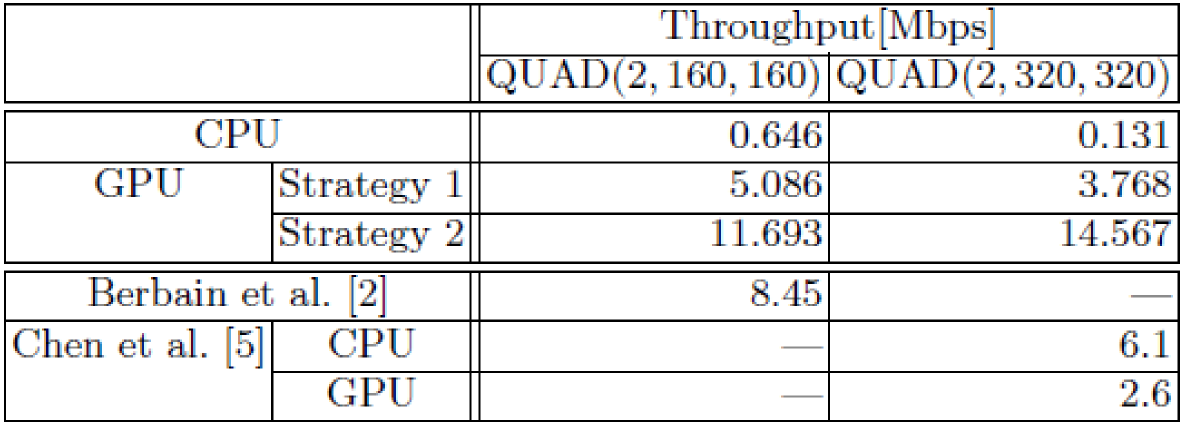


Unknowns n	Polynomials $2n$	Evaluation time (μs)		
		CPU	Strategy 1	Strategy 2
32	64	2.7	21.758	15.927
64	128	16.9	23.483	15.849
96	192	52.7	24.110	16.071
128	256	118.8	24.325	16.537
160	320	236.2	25.058	17.166
192	384	417.8	29.845	17.184
224	448	656.5	34.549	18.125
256	512	992.5	41.864	18.651
288	576	1505.4	52.442	19.408
320	640	2322.2	71.663	19.841
352	704	3409.2	90.264	20.236
384	768	4906.2	111.951	20.710
416	832	6666.4	146.331	21.420
448	896	8453.5	193.567	21.892
480	960	10545.1	256.538	22.259
512	1024	12902.0	336.299	22.785



Result

- Encryption throughput of QUAD



		Throughput[Mbps]	
		QUAD(2, 160, 160)	QUAD(2, 320, 320)
CPU		0.646	0.131
GPU	Strategy 1	5.086	3.768
	Strategy 2	11.693	14.567
Berbain et al. [2]		8.45	—
Chen et al. [5]	CPU	—	6.1
	GPU	—	2.6

Conclusion

- We present two parallelization methods for accelerating the evaluation of multivariate quadratic polynomial systems
    - Parallelization strategy 2 is the fastest
    - We expect QUADs with the strategy 2 will become efficient and secure stream ciphers
- Our approaches can be applied to other multivariate cryptosystems

Multivariate Quadratic Crypto Workshop

- 2013, March, 2nd&3rd 福岡(ISIT/SRP)
  - (Just after PKC@奈良)
- Support by GCOE-program of Math/MI@KyushuUniv.
- Locally organized by Institute of Systems, Information Technologies and Nanotechnologies(ISIT) , IT-security Division

- Two Invited Speakers (Appointed/Confirmed) from 台湾
  - 鄭振牟（Chen-Mou Cheng）国立台湾大学
  - 楊柏因（Bo-Yin Yang） 中央研究院

Thank you