viewpoints. Finally, the long execution time in practically solving lattice problems has proved the security of lattice based cryptosystems from the other side.

Efficient NTRU Implementations [4] by Colleen consist of both software and hardware designs. In the software design, involved operations such as addition, convolution production, random polynomial generation, and multiplicative inverse calculation have all been explained. Additionally, an improved version of the convolution production was proposed for better scalability. The hardware pipeline design was developed base on the analysis of NTRU algorithm features. NTRU multiplier and adder were proposed for higher CPI (Cycles per Instruction) and more efficient hardware utilization over the traditional CPU pipeline.

6. Conclusions and Future Work

As Nth-degree truncated polynomial ring (NTRU) becomes a major quantum-resistant candidate in lattice based cryptographic systems, its processing speed turns in to a major concern. This paper analyzes NTRU structure and utilizes Graphics Processing Unit (GPU) to accelerate NTRU encryption. The single GPU version parallelizes NTRU encryption on GPU to overcome the CPU hardware restriction. Although considerable execution speedup has been achieved, relatively narrow data transfer bandwidth between the host and device impedes further performance gains. Multi-GPU version implants device-level parallelism to promote both data transfer efficiency and computation capability.

GPU zero copy technique has been used to overlap the communication and computation in CPU/GPU bus (PCIe) and GPU itself. However, the factual performance is undermined by high frequent data transfer requests and low bus utilization. Obviously, NTRU is not a good candidate for such optimization.

The future work includes pushing NTRU to distributed systems in Big Data cases and supporting NTRU with OpenCL across heterogeneous platforms for flexibility and scalability.

References

1. D. Cremer and J. A. Pople, General definition of ring puckering coordinates, Journal of the American Mathematic Society, pp. 1354–1358, 1975.
2. Andreas Enge, The extended euclidian algorithm on polynomials and the computational efficiency of hyperelloptic cryptosystems, Designs Codes and Cryptograhpy, 2001
3. Jozef Gruska and Czech Republik, Quantum Computing, 2004
4. Fei Hu, Kyle Wilhelm, Michael Schab, Marcin Lukowiak, Stanislaw Radziszouske, and Yang Xiao, Ntru-based sensor network security: a low-power hardware implementation perspective, Security and Communication Networks, pp. 71–81, 2009.
5. Andrew Kerr, Gregory Diamos, and Sudhakar Yalamanchili, A characterization and analysis of ptx kernels, In Workload Charaterization, 2009
6. Thijs Laarhoven, Joop van de Pol, and Benne de Weger, Solving hard lattice problems and the security of lattice-based cryptosystems, IACR Cryptology ePrint Archive, 2012
7. Peter D. Lax and Ralph S. Phillips, Translation representations for automorphic solutions of the wave equation in non-euclidean spaces, In Communications on pure and applied mathematics, pp. 303–328, 1994.
8. Shahn Majid, q-euclidean space and quantum wick rotation by twisting, Journal of Mathematical Physics, pp. 5025–5034, 1994.
9. CUDA Nvidia, Programming guide, 2008
10. Kazuhiko Ohashi, Security innovation on several assets under asymmetric information, Japanese Economic Review, pp. 75–95, 1999.
11. Jason Sanders and Edward Kandrot, Cuda by example, An Introduction to General-Purpose GPU Programming/J. Sanders, E. Kandrot-Addision Wesley Professional, 2010.
12. Claus-Peter Schnorr and Martin Euchner, Lattice basis reduction: improved practical algorithms and sloving subset sum problems, Mathematical programming, pp. 181–199, 1994.
13. Lieven M. K. Vandersypen, Matthias Steffen, Gregory Breyta, Costantino S. Yannoni, Mark H. Sherwood, and Isaac L. Chuang, Experimental realization of shor's quantum factoring algorithm using nuclear magnetic resonance, Nature, pp. 883–887, 2001.
14. Stanislaw H. Zak and Kai Hwang, Polynomial division on systolic arrays, IEEE Trasnsactions on Computers, pp. 577–578, 1985.