Lattice-based Encryption Over Standard Lattices In Hardware

James Howe, Ciara Moore, & Máire O'Neill, Centre of Secure Information Technologies (CSIT), Queen's University Belfast, UK.

Francesco Regazzoni, Advanced Learning and Research Institute, Università della Svizzera Italiana, Switzerland.

Tim Güneysu, Horst Görtz Institute for IT-Security, Ruhr-University Bochum, Germany.

Kevin Beeden, Thales UK, Research and Technology, UK.

@CSIT_QUB

@SAFEcrypto

jhowe02@qub.ac.uk

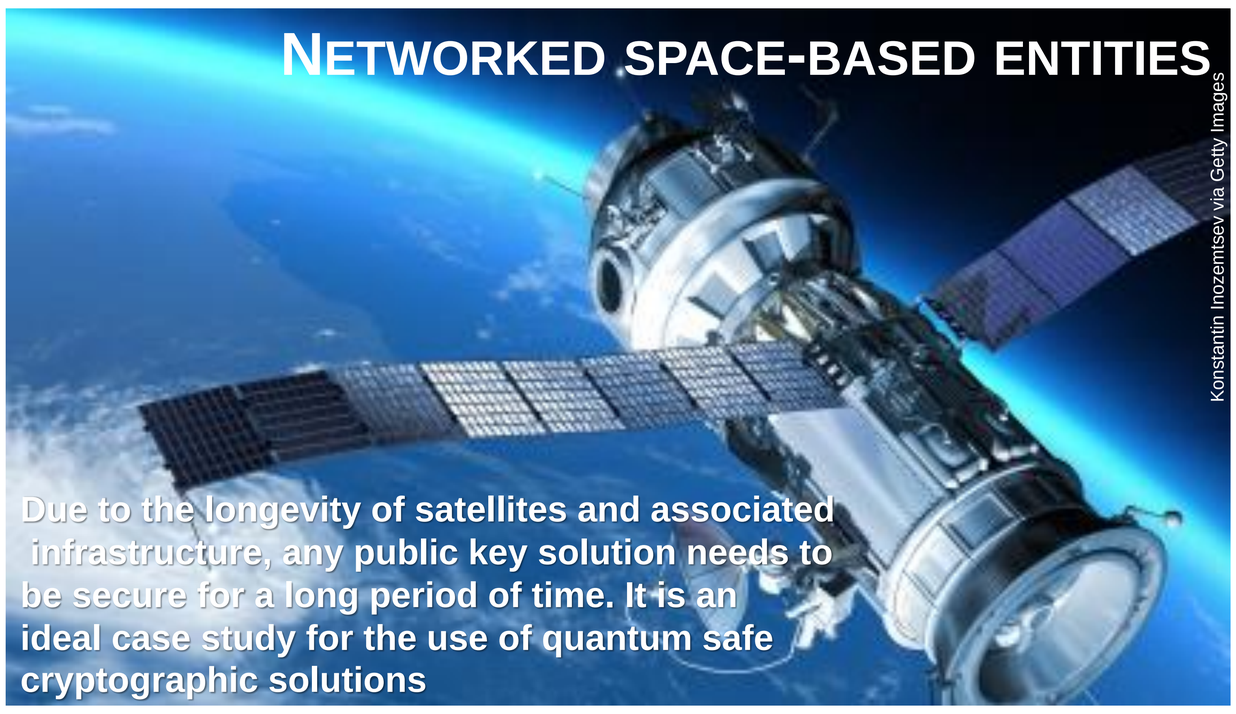
@JamesHowe1729

Aims and Objectives

This project aims to provide:

- **The first hardware architecture for standard lattice-based crypto.**
- **A benchmark for future standard lattice-based cryptography.**
- **Area-optimised hardware architectures for encryption/decryption.**
- **Highly optimised discrete Gaussian sampler which is the first to investigate the hardware impact of $\lambda \rightarrow \frac{1}{2}\lambda$ precision reduction.**

Networked Space-based Entities



Konstantin Inozemtsev via Getty Images

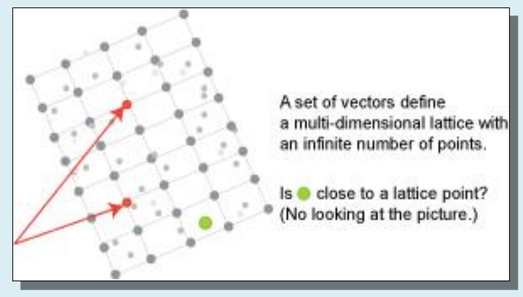
Due to the longevity of satellites and associated infrastructure, any public key solution needs to be secure for a long period of time. It is an ideal case study for the use of quantum safe cryptographic solutions

Quantum Safe Cryptography

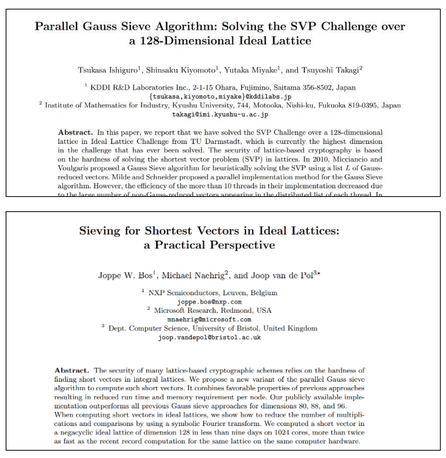
Conventional non-quantum cryptographic algorithms that will remain secure even after practical quantum computing is a reality.

Advantages of lattice-based crypto:

- Underlying operations can be implemented efficiently.
- Most promising as allows for other constructions/applications beyond encryption/signatures, e.g. IBE, ABE, homomorphic encryption etc.



Ring-LWE (vs Standard) Vulnerabilities



Parallel Gauss Sieve Algorithm: Solving the SVP Challenge over a 128-Dimensional Ideal Lattice

Tsukasa Ishiguro[1], Shinsaku Kiyomoto[1], Yutaka Miyake[1], and Tsuyoshi Takagi[2]

[1] KDDI R&D Laboratories Inc., 2-1-15 Ohara, Fujimino, Saitama 356-8502, Japan
{tsukasa,kiyomoto,miyake}@kddilabs.jp
[2] Institute of Mathematics for Industry, Kyushu University, 744, Motooka, Nishi-ku, Fukuoka 819-0395, Japan
takagi@imi.kyushu-u.ac.jp

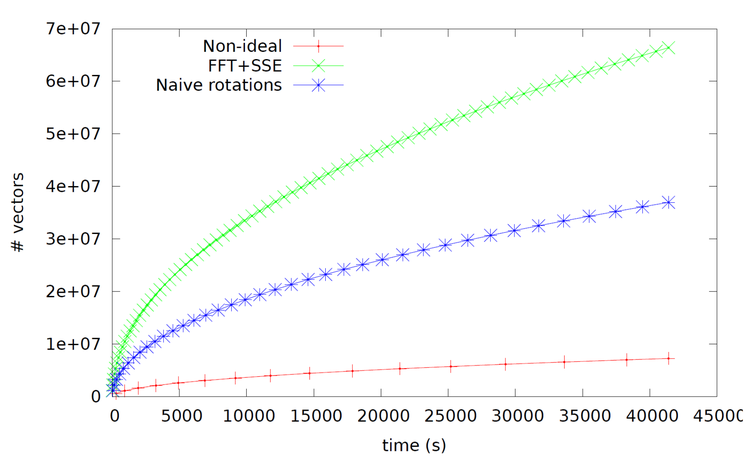
Abstract. In this paper, we report that we have solved the SVP Challenge over a 128-dimensional lattice in Ideal Lattice Challenge from TU Darmstadt, which is currently the highest dimension in the challenge that has ever been solved. The security of lattice-based cryptography is based on the hardness of solving the shortest vector problem (SVP) in lattices. In 2010, Micciancio and Voulgaris proposed a Gauss Sieve algorithm for heuristically solving the SVP using a list L of Gauss-reduced vectors. Milde and Schneider proposed a parallel implementation method for the Gauss Sieve algorithm. However, the efficiency of the more than 10 threads in their implementation decreased due to the large number of non-Gauss-reduced vectors appearing in the distributed list of each thread. In

Sieving for Shortest Vectors in Ideal Lattices: a Practical Perspective

Joppe W. Bos[1], Michael Naehrig[2], and Joop van de Pol[3]*

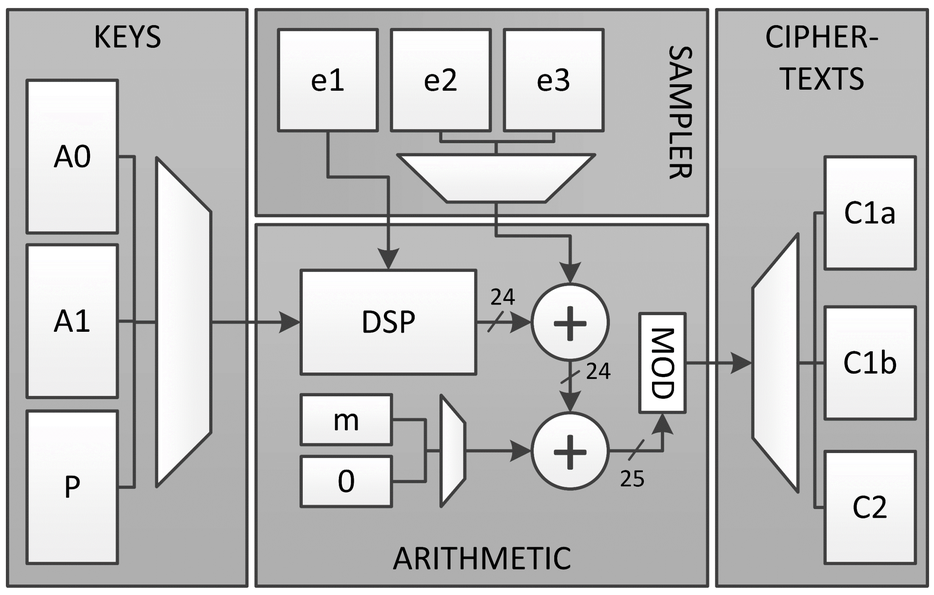
[1] NXP Semiconductors, Leuven, Belgium
joppe.bos@nxp.com
[2] Microsoft Research, Redmond, USA
mnaehrig@microsoft.com
[3] Dept. Computer Science, University of Bristol, United Kingdom
joop.vandepol@bristol.ac.uk

Abstract. The security of many lattice-based cryptographic schemes relies on the hardness of finding short vectors in integral lattices. We propose a new variant of the parallel Gauss sieve algorithm to compute such short vectors. It combines favorable properties of previous approaches resulting in reduced run time and memory requirement per node. Our publicly available implementation outperforms all previous Gauss sieve approaches for dimensions 80, 88, and 96. When computing short vectors in ideal lattices, we show how to reduce the number of multiplications and comparisons by using a symbolic Fourier transform. We computed a short vector in a negacyclic ideal lattice of dimension 128 in less than nine days on 1024 cores, more than twice as fast as the recent record computation for the same lattice on the same computer hardware.



Standard-LWE	Ring-LWE
Large keys required (size N^2).	Reduced key sizes can be used - due to ideal lattice assumption (size N).
Matrix-vector multiplications required.	Ideal representation reduces computations to polynomial multiplication, allowing use of fast NTT multiplication.
Security is based on the LWE problem.	Security is based on the LWE problem with an additional security assumption to use an ideal lattice structure.

Standard Lattice-based LWE Encryption Hardware Architecture



Hardware results on a Spartan 6 – LX45 FPGA, compared with other ring-LWE hardware results. Despite there being a 128x increase in key sizes, as well as the number of extra multiplications, most of the results compare well with, or even better, other ring-LWE schemes.

Operation & Algorithm	Device	LUT/FF/SLICE	BRAM/DSP	MHz	Cycles	Ops/s
LWE Encrypt ($\lambda = 128$)	S6LX45	6152/4804/1866	73/1	125	98304	1272
LWE Encrypt ($\lambda = 64$)	S6LX45	6078/4676/1811	73/1	125	98304	1272
LWE Decrypt	S6LX45	63/58/32	13/1	144	32768	4395
RLWE Encrypt [14]	V6LX240T	298016/ – /143396	–/–	–	–	–
RLWE Decrypt [14]	V6LX240T	124158/ – /65174	–/–	–	–	–
RLWE Encrypt [26]	S6LX16	4121/3513/–	14/1	160	6861	23321
RLWE Decrypt [26]	S6LX16	4121/3513/–	14/1	160	4404	36331
RLWE Encrypt [26]	V6LX75T	4549/3624/1506	12/1	262	6861	38187
RLWE Decrypt [26]	V6LX75T	4549/3624/1506	12/1	262	4404	59492
RLWE Encrypt [27]	S6LX9	282/238/95	2/1	144	136212	1057
RLWE Decrypt [27]	S6LX9	94/87/32	1/1	189	66338	2849
RLWE Encrypt [32]	V6LX75T	1349/860/–	2/1	313	6300	49751
RLWE Decrypt [32]	V6LX75T	1349/860/–	2/1	313	2800	109890
ECC-P224 Encrypt	XC4VFX12	1825/1892/–	11/26	487	178000	2740
ECC-P256 Encrypt	XC5VLX85T	18097/ – /5644	–/–	156	-	81300

www.**safe**crypto.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 644729