## Lattices in the context of post-quantum cryptography

Mădălina Bolboceanu

The Ninth Congress of Romanian Mathematicians July 2, 2019


## Bitdefender

## Who are we?

A global technology company in the cybersecurity field.


## Research \& Development team at the center of Bitdefender

- Bitdefender Labs in Timisoara, Cluj-Napoca, lasi, Bucharest
- Research areas:
- Machine Learning
- Networking and Cloud Infrastructure
- Security and Privacy
- Cryptography


## Research in cryptography

- studying security foundations and building advanced post-quantum cryptographic solutions, mainly lattice-based


Miruna Roșca


Mădălina Bolboceanu


Radu Tițiu
\{mrosca, mbolboceanu, rtitiu\}@bitdefender.com

- collaborations: ENS Lyon, Weizmann Institute of Science etc.


## How do we build public-key

 crypto?



The scheme is secure if the underlying mathematical problem is computationally hard.

## RSA cryptosystem



- If one knows how to factorize $N=p q$ $\rightsquigarrow$ RSA is broken


## Can one factorize?

## What is a quantum computer?

A quantum computer is a theoretical device whose functionality relies on the laws of quantum physics.

- fundamentally different from a classical computer
- can perform faster on particular tasks


## The threat of quantum computers



## How close are we to quantum computing?



IBM (2017)

50 qubits


Intel (2018)
49 qubits


Google (2018)
72 qubits
...still laboratory experiments

## So... what to do?

## - projects to protect data against quantum computers


－many post－quantum cryptography conferences，workshops

PQCrypto 2006：International Workshop on Post－Quantum Cryptography

| Introduction |
| :--- |
| Speakers |
| Organization |
| Registration |
| Contact |
| Schedule |
| Contributions |
| Participants |
| Deadlines |
| Location |
| Facilities |
| Lodging |
| Maps |
| Directions |
| Driving |
| Weather |
| Alphabetical： |
| Contact |
| Contributions |
| Deadlines |
| Directions |
| Driving |

[^0]
## NIST is calling!

Call for Proposals Announcement (information retained for historical purposes-call closed 11/30/2017)

NIST has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. Currently, public-key cryptographic algorithms are specified in FIPS 186-4, Digital Signature Standard, as well as special publications SP 800-56A Revision 2, Recommendation for PairWise Key Establishment Schemes Using Discrete Logarithm Cryptography and SP 800-56B Revision 1, Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography. However, these algorithms are vulnerable to attacks from large-scale quantum computers (see NISTIR 8105, Report on Post Quantum Cryptography).

It is intended that the new public-key cryptography standards will specify one or more additional unclassified, publicly disclosed digital signature, public-key encryption, and key-establishment algorithms that are available worldwide, and are capable of protecting sensitive government information well into the foreseeable future, including after the advent of quantum computers.

## How to work post-quantum?

The public-key scheme is quantum secure if the underlying mathematical problem is quantum resistant.

## Which hard problems should we pick?

## Let's work post-quantum!



## Let's work post-quantum!



## Let's work post-quantum!




$$
\begin{gathered}
x_{0} x_{1}+x_{1} x_{3}=2 \\
x_{1} x_{2}+x_{0} x_{3}=0 \\
x_{1}^{2}+x_{3}^{2}=1 \\
x_{1} x_{3}+x_{2}^{2}=0 \\
\text { in } \mathbb{F}_{3} \\
\text { multivariate } \\
\text { equations }
\end{gathered}
$$

## Let's work post-quantum!



isogenies

## Let's work post-quantum!



equations


$$
\begin{array}{r}
x_{0} x_{1}+x_{1} x_{3}=2 \\
x_{1} x_{2}+x_{0} x_{3}=0 \\
x_{1}^{2}+x_{3}^{2}=1 \\
x_{1} x_{3}+x_{2}^{2}=0 \\
\text { in } \mathbb{F}_{3} \\
\text { multivariate }
\end{array}
$$

$$
\sum_{1}
$$

isogenies

hash functions

## More about NIST competition

- 82 submissions until Nov 2017
- 69 first-round candidates on Dec 2017 (5 withdrawn)
- 26 second-round candidates on Jan 26, 2019:

|  | Encryption/KEM | Digital signatures | Total |
| :--- | :--- | :--- | :--- |
| Lattices | 9 | 3 | $\mathbf{1 2}$ |
| Codes | 7 |  | 7 |
| Multivariate eqs |  | 4 | 4 |
| Hashes |  | 2 | 2 |
| Isogenies | 1 |  | 1 |
| Total | 17 | 9 | 26 |

- expected to last 12-18 months, after possibly a $3^{\text {rd }}$ round


## Lattice-based cryptography

## What is a lattice?

## Lattice

Let $\mathbf{v}_{1}, \mathbf{v}_{2}, \ldots, \mathbf{v}_{n}$ be linearly independent vectors from $\mathbb{R}^{m}$. Then $L=L\left(\mathbf{v}_{1}, \ldots, \mathbf{v}_{n}\right)=\left\{\sum_{i=1}^{n} a_{i} \mathbf{v}_{i} \mid a_{i} \in \mathbb{Z}\right\}$ is the lattice generated by them.


## Shortest Vector Problem

$\lambda_{1}(L):=$ the length of a shortest nonzero vector from $L$.

## ApproxSVP ${ }_{\gamma}$

Find a short nonzero $\mathbf{v} \in L$ (in Euclidean norm). (e.g. $\left.\|\mathbf{v}\| \leq \gamma \lambda_{1}(L)\right)$.

## Closest Vector Problem

## ApproxCVP $_{\gamma}$

Given $\mathbf{t}$, find a point from the lattice close to $\mathbf{t}$.


## How hard are SVP/CVP?



SVP and CVP conjectured to be hard to solve using quantum or classical algorithms $\rightsquigarrow$ use them in crypto!

## A particular lattice

Let $\mathbf{A} \in \mathbb{Z}_{q}^{m \times n}$. Then

$$
\Lambda_{\mathbf{A}}=\left\{y \in \mathbb{Z}^{n} \mid y=\mathbf{A} \cdot \mathbf{s} \bmod q, \text { for } \mathbf{s} \in \mathbb{Z}_{q}^{n}\right\} \text { is a lattice. }
$$

## A particular lattice

Let $\mathbf{A} \in \mathbb{Z}_{q}^{m \times n}$. Then

$$
\Lambda_{\mathbf{A}}=\left\{y \in \mathbb{Z}^{n} \mid y=\mathbf{A} \cdot \mathbf{s} \bmod q, \text { for } \mathbf{s} \in \mathbb{Z}_{q}^{n}\right\} \text { is a lattice. }
$$

This is also equal to

$$
\Lambda_{\mathbf{A}}=\mathbf{A} \cdot \mathbb{Z}_{q}^{n}+q \cdot \mathbb{Z}^{m}
$$

## Easy or not?

Suppose bach vector to $\Lambda_{\mathbf{A}}$. Then

$$
\mathbf{b}=\mathbf{A} \cdot \mathbf{s}+\mathbf{e}(\bmod q)
$$

for $\mathbf{s}$ unknown and $\mathbf{e}$ small. How to find $\mathbf{s}$ ?

## Easy or not?

Suppose bache vector to $\Lambda_{\mathbf{A}}$. Then

$$
\mathbf{b}=\mathbf{A} \cdot \mathbf{s}+\mathbf{e}(\bmod q)
$$

for $\mathbf{s}$ unknown and $\mathbf{e}$ small. How to find $\mathbf{s}$ ?
Equivalently, find $\mathbf{s} \in \mathbb{Z}_{q}^{n}$ from this linear system of noisy equations:

$$
\begin{gathered}
a_{11} s_{1}+a_{12} s_{2}+\ldots+a_{1 n} s_{n} \simeq b_{1}(\bmod q) \\
a_{21} s_{1}+a_{22} s_{2}+\ldots+a_{2 n} s_{n} \simeq b_{2}(\bmod q) \\
\vdots \\
a_{m 1} s_{1}+a_{m 2} s_{2}+\ldots+a_{m n} s_{n} \simeq b_{m}(\bmod q)
\end{gathered}
$$

- expected to be hard problem


## Learning with Errors?

Let $\mathbf{s} \in \mathbb{Z}_{q}^{n}, m \geq n, \alpha q>\sqrt{n}$

$$
\left\{\begin{array}{l}
\mathbf{A} \stackrel{u}{\hookleftarrow} \mathbb{Z}_{q}^{m \times n} \\
\mathbf{e} \hookleftarrow D_{\alpha q}
\end{array}\right.
$$

$\mathrm{LWE}_{q, \alpha q}$ distribution:


Search: Given LWE samples, find s.
Decision: Distinguish LWE samples from uniform samples.
?: Solve Search- LWE $_{q, \alpha q} \xrightarrow{\text { quantum }}$ Solve ApproxSVP ${ }_{\gamma}$, for $\gamma \leq \operatorname{poly}(n)$. Conclusion: use LWE in post-quantum crypto!

## LWE in crypto



## Pros and cons of LWE-based schemes

$\checkmark$ simple operations
$\checkmark$ quantum resistant
$\checkmark$ all known algorithms of
$X$ large size of keys
$X$ slow computations
ApproxSVP are exponential in
$n$ for polynomial approx.
factor.

## Take structured matrices!



example: $f=X^{4}+1$

## vectors/matrices

$$
\left(\begin{array}{cccc}
a_{0} & -a_{3} & -a_{2} & -a_{1} \\
a_{1} & a_{0} & -a_{3} & -a_{2} \\
a_{2} & a_{1} & a_{0} & -a_{3} \\
a_{3} & a_{2} & a_{1} & a_{0}
\end{array}\right) \cdot\left(\begin{array}{c}
s_{0} \\
s_{1} \\
s_{2} \\
s_{3}
\end{array}\right)
$$

polynomials
$a \cdot s \bmod f$

## Polynomial LWE ?

$R:=\mathbb{Z}[X] /(f), R_{q}:=R / q R \simeq \mathbb{Z}_{q}[X] /(f)$.
Let $s \in R_{q}$.

$$
\mathrm{PLWE}_{q, D_{\alpha q}}^{f} \text { distribution : }\left\{\begin{array}{l}
a \stackrel{u}{\hookleftarrow} R_{q} \\
e \hookleftarrow D_{\alpha q} \text { over } \mathbb{R}^{n} \simeq \mathbb{R}[X] /(f) \\
\text { output: }(a, a \cdot s+e \bmod q R)
\end{array}\right.
$$

Search: Given PLWE samples, find $s$.
Decision: Distinguish PLWE samples from uniform samples.

## More algebraic number theory:RLWE and RLWE ${ }^{\vee}$ ?

$$
\mathbb{Z}[X] /(f) \subseteq K:=\mathbb{Q}[X] /(f) \text { number field }
$$

$\mathcal{O}_{K}:=\{x \in K \mid x$ root of monic polynomial in $\mathbb{Z}[X]\}$ ring of integers

## More algebraic number theory:RLWE and RLWE ${ }^{\vee}$ ?

$$
\mathbb{Z}[X] /(f) \subseteq K:=\mathbb{Q}[X] /(f) \text { number field }
$$

$\mathcal{O}_{K}:=\{x \in K \mid x$ root of monic polynomial in $\mathbb{Z}[X]\}$ ring of integers


## More algebraic number theory:RLWE and RLWE ${ }^{\vee}$ ?

$$
\mathbb{Z}[X] /(f) \subseteq K:=\mathbb{Q}[X] /(f) \text { number field }
$$

$\mathcal{O}_{K}:=\{x \in K \mid x$ root of monic polynomial in $\mathbb{Z}[X]\}$ ring of integers $\mathcal{O}_{K}^{\vee}:=\left\{y \in K \mid \operatorname{Tr}(x \cdot y) \in \mathbb{Z}\right.$ for any $\left.x \in \mathcal{O}_{K}\right\}$ dual of $\mathcal{O}_{K}$


## Variants of RLWE



## RLWE in crypto



## How hard is SVP on special lattices?

- hot topic of research: ????



## Pros and cons of PLWE/RLWE-based schemes

$\checkmark$ compact operations
$\checkmark$ quantum resistant
$X$ working with $\mathcal{O}_{K}$ relies on $f$ $X$ approximation factor depends on $f$

## Solution:


[RSSS17]
$a \cdot b \rightsquigarrow$ take its middle $d$ coefficients $\rightarrow$ get $a \odot_{d} b$

## State of the art and contributions



## An LWE application

## Long-term encryption



## Long-term encryption



## Long-term encryption



Oh no...

## Long-term encryption



## Long-term encryption



## Long-term encryption

We can help you store the key!


## Long-term encryption

We can help you store the key!


## Long-term encryption



Yay, I can safely store my key!



## Thank you.

## References

- [BBPS19]: M. Bolboceanu, Z. Brakerski, R. Perlman, D. Sharma, Order-LWE and the Hardness of Ring-LWE with Entropic Secrets. Available at https://eprint.iacr.org/2018/494
- [BEF+17]: J.-F. Biasse, T. Espitau, P.-A. Fouque, A. Gélin, P. Kirchner, Computing Generator in Cyclotomic Integer Rings - A Subfield Algorithm for the Principal Ideal Problem in $\mathbf{L}_{\left|\Delta_{K}\right|}\left(\frac{1}{2}\right)$ and Application to the Cryptanalysis of a FHE Scheme. In Proc. of EUROCRYPT, 2017
- [CDPR16]: R. Cramer, L. Ducas, C. Peikert, O. Regev, Recovering Short Generators of Principal Ideals in Cyclotomic Rings. In Proc. of EUROCRYPT, 2016
- [CDW17]: R. Cramer, L. Ducas, B. Wesolowski, Short Stickelberger Class Relations and Application to Ideal-SVP. In Proc. of EUROCRYPT,2017
- [LPR10]: V. Lyubashevsky, C. Peikert, O. Regev, On Ideal Lattices and Learning with Errors over Rings. In JACM, 2013
- [LS15]: A. Langlois, D. Stehlé, Worst-case to average-case reductions for module lattices. In Des. Codes Cryptography, 2015
- [LST18]: B. Libert, D.Stehlé, R. Titiu, Adaptively Secure Distributed PRFs from LWE. In Proc. of TCC, 2018
- [Reg05]: O. Regev, On lattices, learning with errors, random linear codes, and cryptography. In Proc. of STOC, 2005
- [RSSS17]: M. Rosca, A. Sakzad, D. Stehlé, R. Steinfeld, Middle-Product Learning With Errors. In Proc. of CRYPTO, 2017
- [RSW18]: M. Rosca, D. Stehlé, A. Wallet, On the Ring-LWE and Polynomial-LWE problems. In Proc. of EUROCRYPT, 2018
- [SSTX09]: D. Stehlé, R. Steinfeld, K. Tanaka, K. Xagawa, Efficient Public Key Encryption Based on Ideal Lattices. In Proc. of ASIACRYPT, 2009


[^0]:    Will large quantum computers be built？If so，what will they do to the cryptographic landscape？
    Anyone who can build a large quantum computer can break today＇s most popular public－key cryptosystems：e．g．，RSA，DSA，and ECDSA．But there are several other cryptosystems that are conjectured to resist quantum computers：e．g．，the Diffie－Lamport－Merkle signature system，the NTRU encryption system，the McEliece encryption system，and the HFE signature system．Ex which of these systems are secure？How efficient are they，in theory and in practice？

    PQCrypto 2006，the International Workshop on Post－Quantum Cryptography，will look ahead to a possible future of quantum computers，and will begin preparing the cryptographic world for future．

    Update：PQCrypto 2006 is done！The workshop record，except for three papers restricted by the copyright holders，is now online：pqcry．pto2006record．pdf

    ## Speakers

    Invited speakers：
    －Sean Hallgren，NEC Laboratories，USA．＂Quantum algorithms．＂
    －Phong Nguyen，École Normale Superieure，France．＂Post－quantum lattice－based cryptography．＂
    －Oded Regev，Tel－Aviv University，Israel．＂More quantum algorithms．＂
    －Nicolas Sendrier，Institut National de Recherche en Informatique et en Automatique，France．＂Post－quantum code－based cryptography．＂
    －Jacques Stern，Ecole Normale Supérieure，France．＂Post－quantum multivariate－quadratic public key schemes．＂
    －Michael Szydlo，RSA Laboratories，USA．＂Post－quantum hash－based cryptography．＂
    －Lieven Vandersypen，Technische Universiteit Delft，the Netherlands．＂Can quantum computers be built？＂
    Contributed talks：See below．

