Lattice-based Cryptography

J.C. Deneuville[1]
jean-christophe.deneuville@xlim.fr
Advisors: *P. Gaborit*[1] *& C. Aguilar Melchor*[1]

[1]XLIM-DMI, Université de Limoges
123 avenue Albert Thomas
87060 Limoges CEDEX, France

XLIM - 4th Students Workshop
September the 25th, 2014

Outline

Outline

Fundamental Goals

<u>Context:</u> 

wants to send message  to 

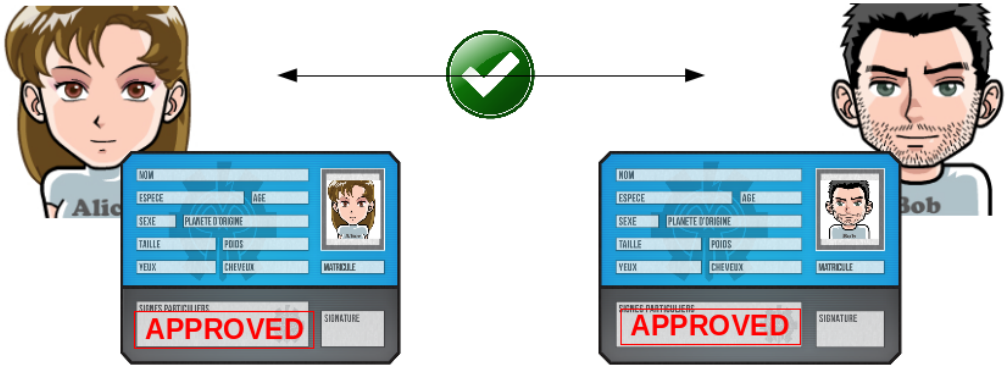
Fundamental Goals

Context: 

wants to send message  to 

Cryptography aims for ensuring:

- Authentication
- Confidentiality
- Integrity
- Non-Repudiation



Fundamental Goals

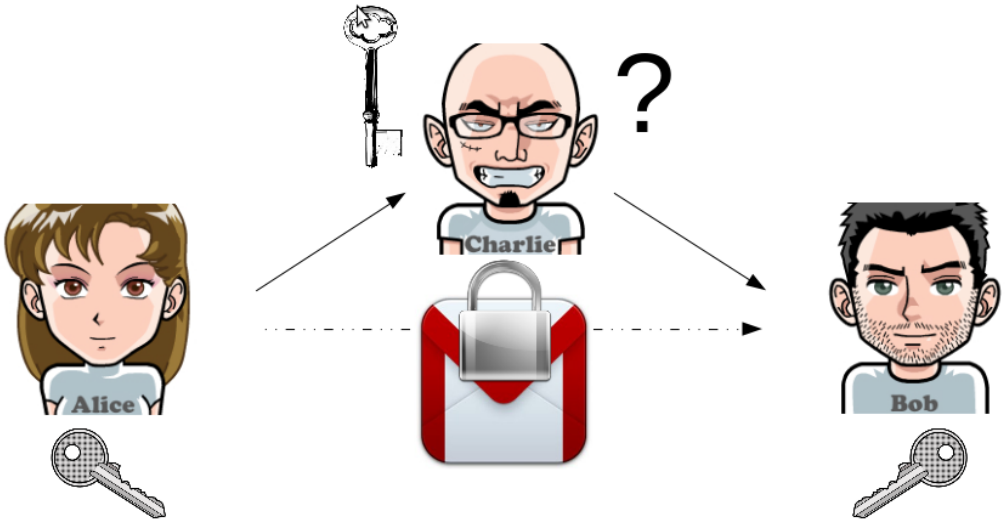
Context: 

wants to send message  to 

Cryptography aims for ensuring:

- Authentication 

- Confidentiality
- Integrity
- Non-Repudiation



Fundamental Goals

Context: 

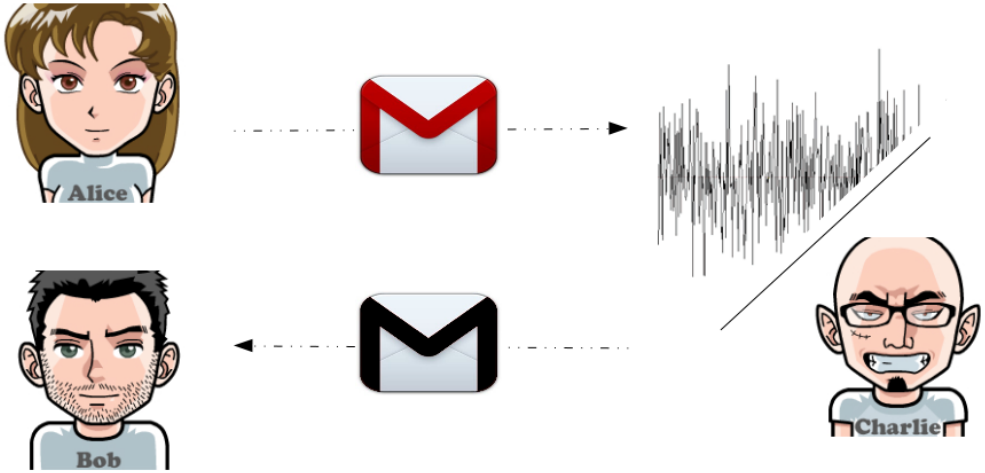
wants to send message  to 

Cryptography aims for ensuring:

- Authentication 

- Confidentiality 

- Integrity
- Non-Repudiation



Fundamental Goals

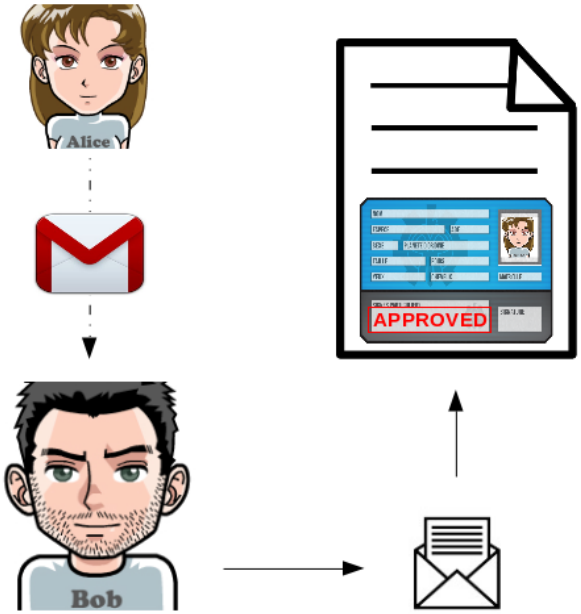
Context: 

wants to send message  to 

Cryptography aims for ensuring:

- Authentication 

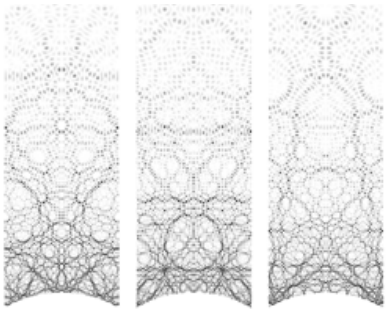
- Confidentiality 
- Integrity 
- Non-Repudiation



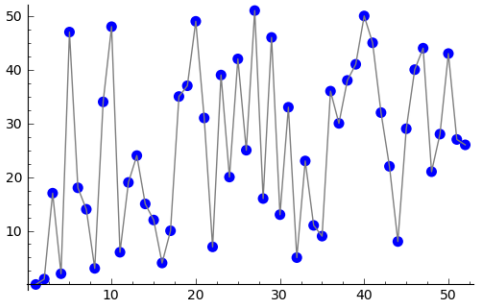
Outline

Techniques and Limitations

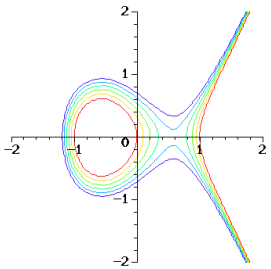
Big Integer Factorization



Finite Field Discrete Logarithm



Elliptic Curves Discrete Logarithm



Advantages

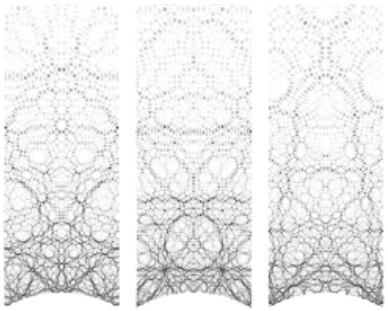
- Old problems: meaning well-studied, therefore trustable
- Wide-spread: already embedded in most cryptographic devices

Drawbacks

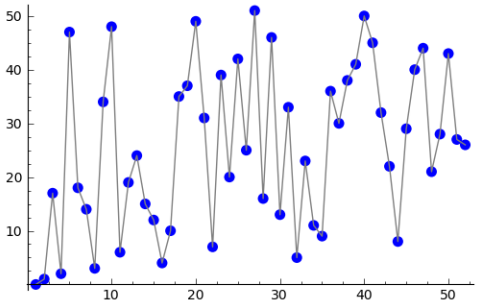
- Greedy: Require **huge** integers ($\approx$ 500 digits) $\Rightarrow$ pretty **slow** and **costly**!

Techniques and Limitations

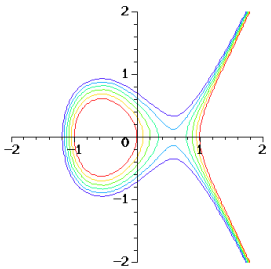
Big Integer Factorization



Finite Field Discrete Logarithm



Elliptic Curves Discrete Logarithm



Advantages

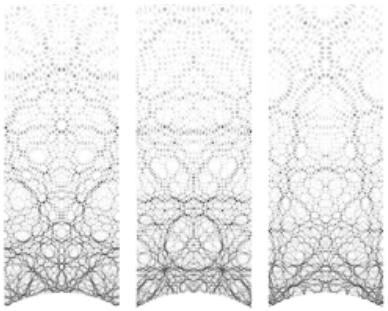
- Old problems: meaning well-studied, therefore trustable
- Wide-spread: already embedded in most cryptographic devices

Drawbacks

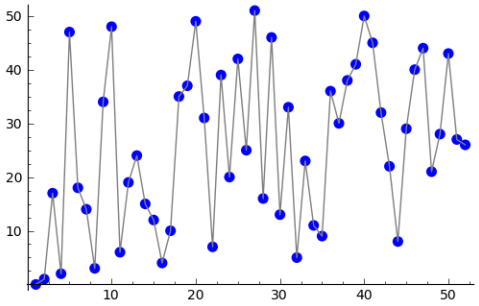
- Greedy: Require **huge** integers ($\approx$ 500 digits) $\Rightarrow$ pretty **slow** and **costly**!

Techniques and Limitations

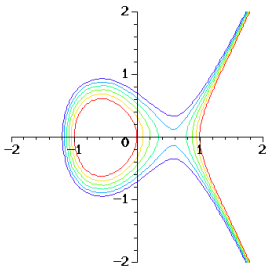
Big Integer Factorization



Finite Field Discrete Logarithm



Elliptic Curves Discrete Logarithm



Advantages

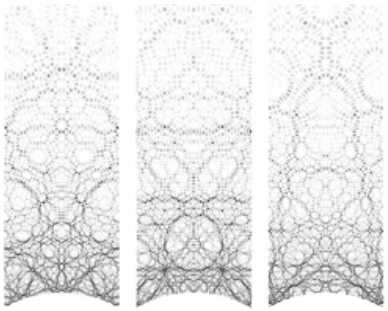
- Old problems: meaning well-studied, therefore trustable
- Wide-spread: already embedded in most cryptographic devices

Drawbacks

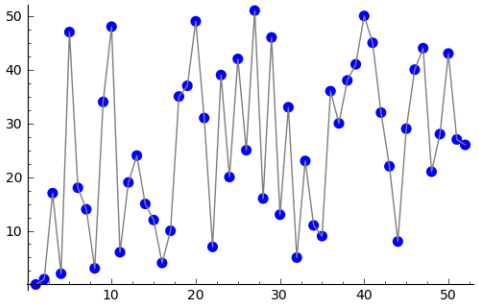
- Greedy: Require **huge** integers ($\approx$ 500 digits) $\Rightarrow$ pretty **slow** and **costly**!

Techniques and Limitations

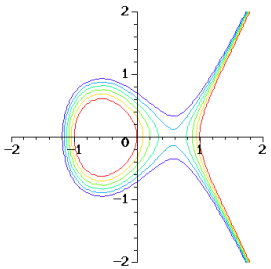
Big Integer Factorization



Finite Field Discrete Logarithm



Elliptic Curves Discrete Logarithm



Advantages

- Old problems: meaning well-studied, therefore trustable
- Wide-spread: already embedded in most cryptographic devices

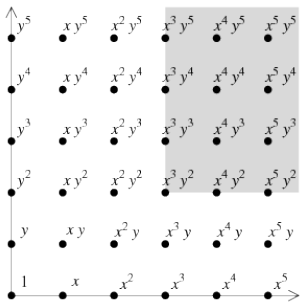
Drawbacks

- Greedy: Require **huge** integers ($\approx$ 500 digits) $\Rightarrow$ pretty **slow** and **costly**!
- ALREADY BROKEN BY QUANTUM COMPUTERS ! [Shor94]

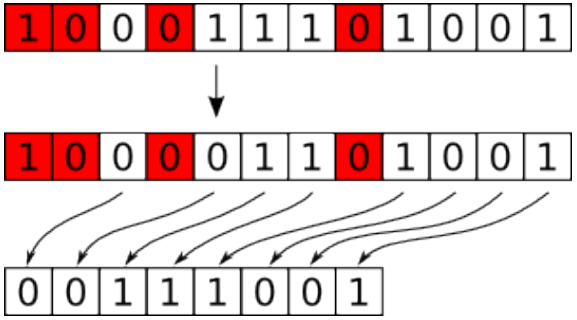
Outline

Candidates

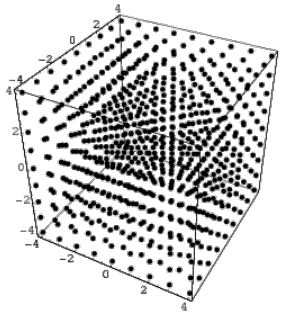
Multivariate



Error Correcting Codes



Euclidian Lattices



Advantage

- Quantum Computing doesn't seem to improve known attacks

Drawback

- Scarce: alternative crypto isn't implemented everywhere

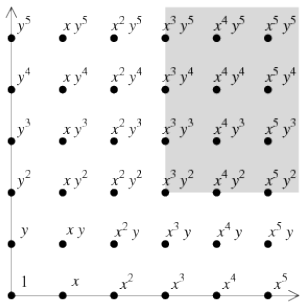
Mid-Way

- Pretty new schemes: not (yet) efficient enough to be practical BUT many ways to improve them

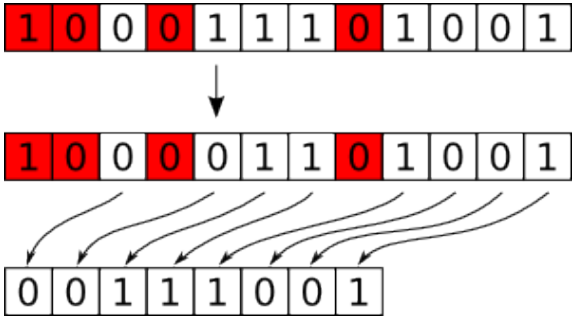
Disclaimer: *Other post-quantum alternatives exist (hash-based, supersingular elliptic curves isogeny, symmetric), these are off this topic*

Candidates

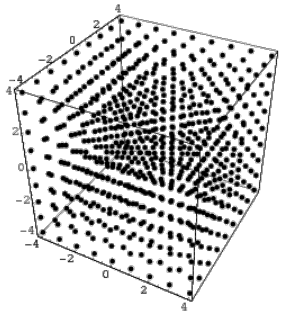
Multivariate



Error Correcting Codes



Euclidian Lattices



Advantage

- Quantum Computing doesn't seem to improve known attacks

Drawback

- Scarce: alternative crypto isn't implemented everywhere

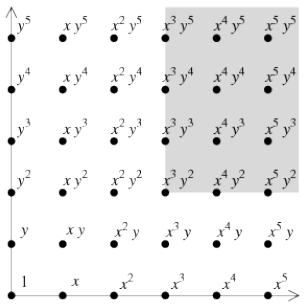
Mid-Way

- Pretty new schemes: not (yet) efficient enough to be practical BUT many ways to improve them

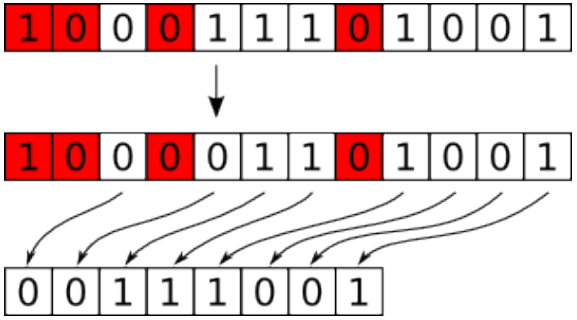
Disclaimer: *Other post-quantum alternatives exist (hash-based, supersingular elliptic curves isogeny, symmetric), these are off this topic*

Candidates

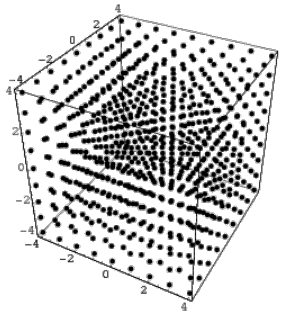
Multivariate



Error Correcting Codes



Euclidian Lattices



Advantage

- Quantum Computing doesn't seem to improve known attacks

Drawback

- Scarce: alternative crypto isn't implemented everywhere

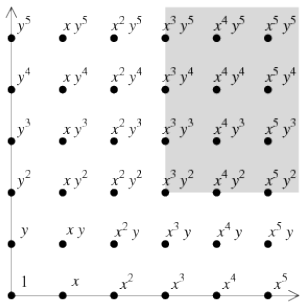
Mid-Way

- Pretty new schemes: not (yet) efficient enough to be practical BUT many ways to improve them

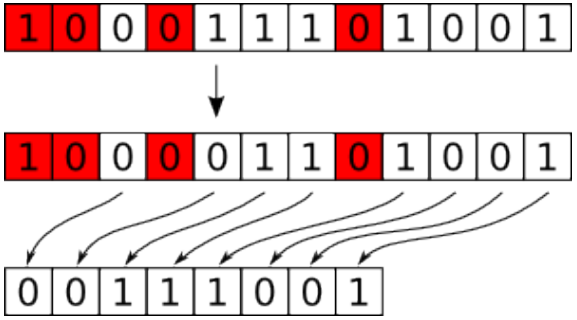
Disclaimer: *Other post-quantum alternatives exist (hash-based, supersingular elliptic curves isogeny, symmetric), these are off this topic*

Candidates

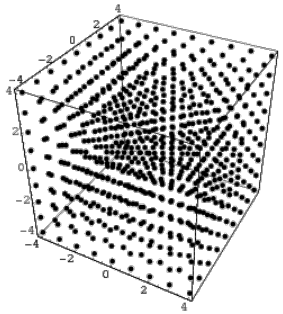
Multivariate



Error Correcting Codes



Euclidian Lattices



Advantage

- Quantum Computing doesn't seem to improve known attacks

Drawback

- Scarce: alternative crypto isn't implemented everywhere

Mid-Way

- Pretty new schemes: not (yet) efficient enough to be practical BUT many ways to improve them

Disclaimer: *Other post-quantum alternatives exist (hash-based, supersingular elliptic curves isogeny, symmetric), these are off this topic*

Outline

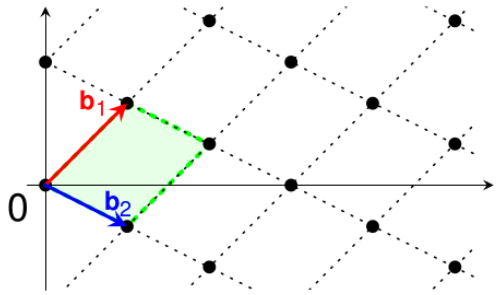
Lattices

Lattices own every thing you need for Public-Key Cryptography

Lattices

Lattices own every thing you need for Public-Key Cryptography

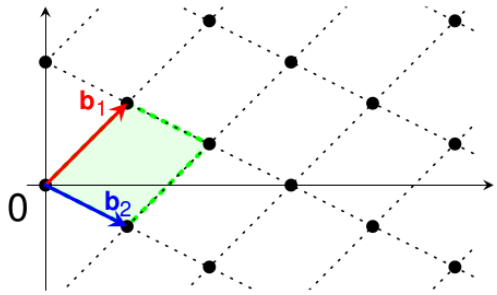
- Good/Bad basis as Private/Public keys



Lattices

Lattices own every thing you need for Public-Key Cryptography

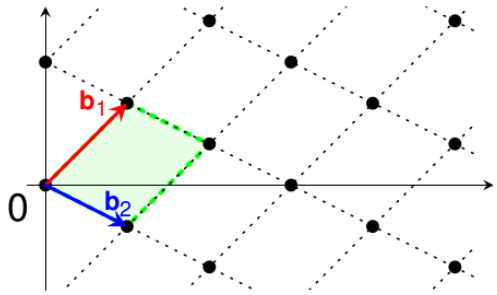
- Good/Bad basis as Private/Public keys
- Exponential algorithms for exact problems



Lattices

Lattices own every thing you need for Public-Key Cryptography

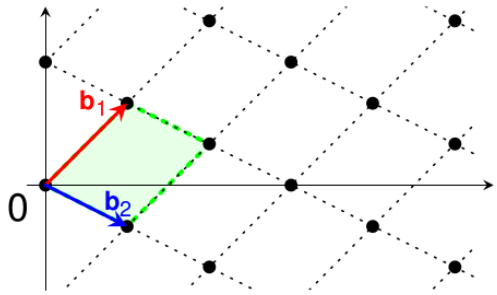
- Good/Bad basis as Private/Public keys
- Exponential algorithms for exact problems
- Polynomial algorithms are exponentially bad



Lattices

Lattices own every thing you need for Public-Key Cryptography**, and even more!**

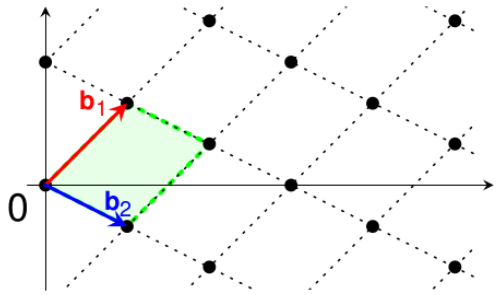
- Good/Bad basis as Private/Public keys
- Exponential algorithms for exact problems
- Polynomial algorithms are exponentially bad

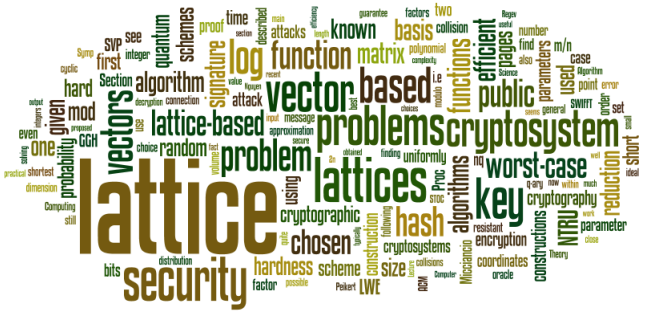


Lattices

Lattices own every thing you need for Public-Key Cryptography, **and even more!**

- Good/Bad basis as Private/Public keys
- Exponential algorithms for exact problems
- Polynomial algorithms are exponentially bad
- Small Integer operations $\underbrace{(\approx 20 \text{ digits!})}_{25\times \text{ less than NT}}$

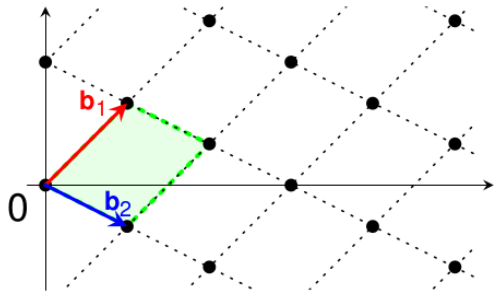


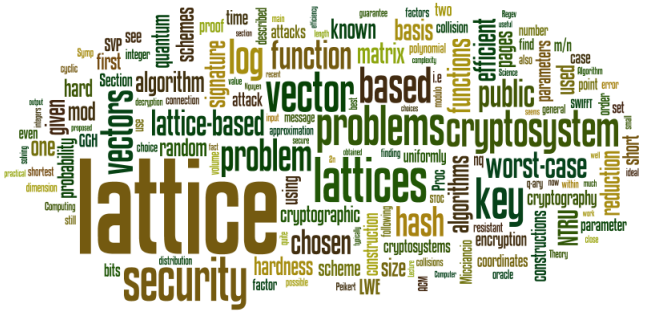


Lattices

Lattices own every thing you need for Public-Key Cryptography**, and even more!**

- Good/Bad basis as Private/Public keys
- Exponential algorithms for exact problems
- Polynomial algorithms are exponentially bad
- Small Integer operations ($\approx$ 20 digits!)
- $\underbrace{\text{Strong security reductions}}_{\text{Worst-case to Average-case}}$ [Ajtai96]

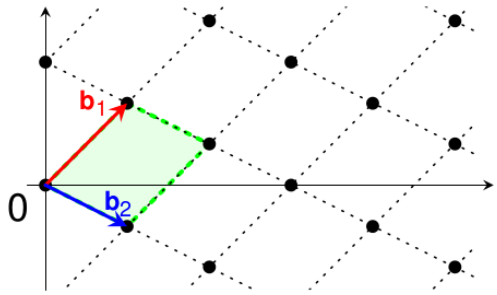


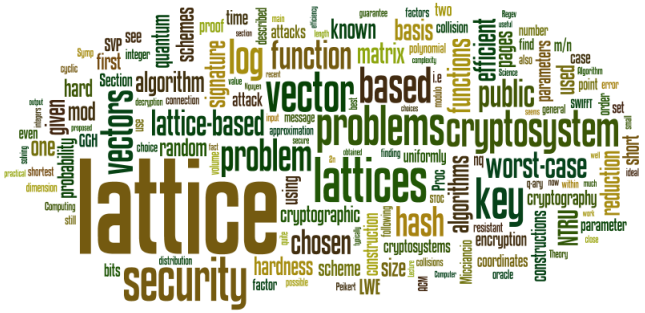


Lattices

Lattices own every thing you need for Public-Key Cryptography**, and even more!**

- Good/Bad basis as Private/Public keys
- Exponential algorithms for exact problems
- Polynomial algorithms are exponentially bad
- Small Integer operations ($\approx$ 20 digits!)
- Strong security reductions [Ajtai96]
- Fully Homomorphic Schemes [Gentry09]

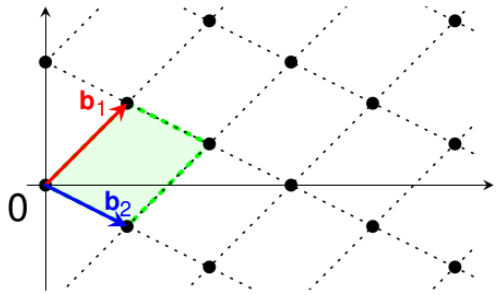


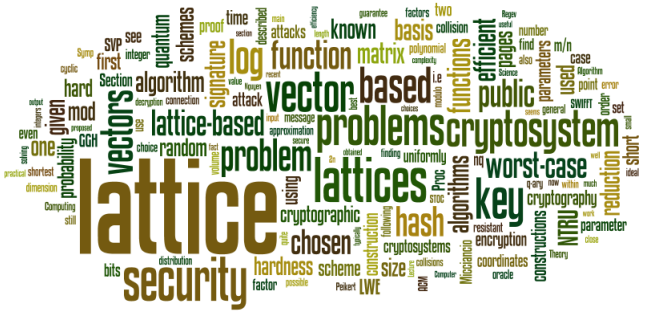


Lattices

Lattices own every thing you need for Public-Key Cryptography**, and even more!**

- Good/Bad basis as Private/Public keys
- Exponential algorithms for exact problems
- Polynomial algorithms are exponentially bad
- Small Integer operations ($\approx$ 20 digits!)
- Strong security reductions [Ajtai96]
- Fully Homomorphic Schemes [Gentry09]
- ... and many more nice features!





Outline

Results and Perspectives

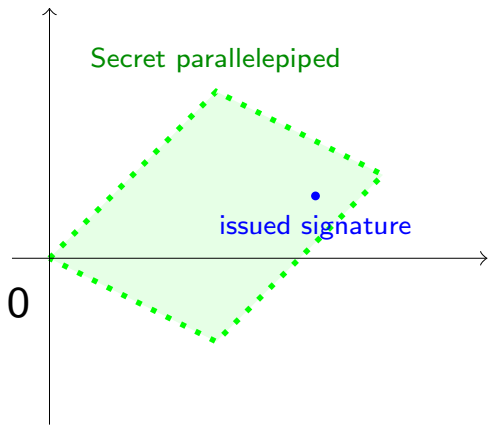
Lattice-based Signature

We proposed an efficent scheme by fixing a broken one using lattice techniques
[ABDG14] *Sealing the Leak on Classical NTRU Signatures*. Post-Quantum Cryptography 2014

Results and Perspectives

Lattice-based Signature

We proposed an efficent scheme by fixing a broken one using lattice techniques
[ABDG14] *Sealing the Leak on Classical NTRU Signatures*. Post-Quantum Cryptography 2014

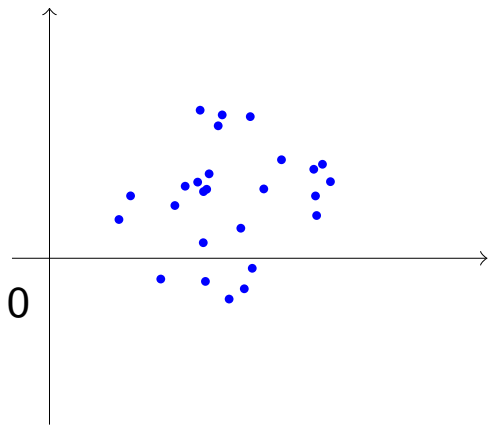


Number of signature: 1

Results and Perspectives

Lattice-based Signature

We proposed an efficent scheme by fixing a broken one using lattice techniques
[ABDG14] *Sealing the Leak on Classical NTRU Signatures*. Post-Quantum Cryptography 2014

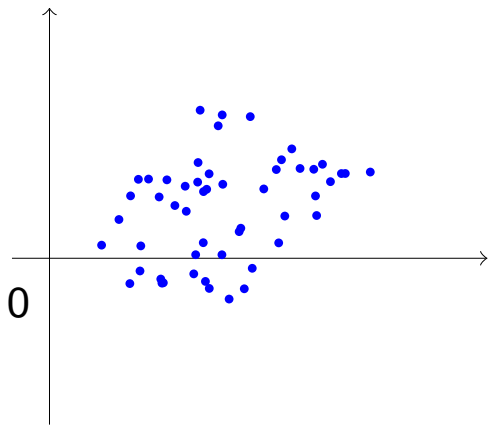


Number of signatures: 25

Results and Perspectives

Lattice-based Signature

We proposed an efficent scheme by fixing a broken one using lattice techniques
[ABDG14] *Sealing the Leak on Classical NTRU Signatures*. Post-Quantum Cryptography 2014

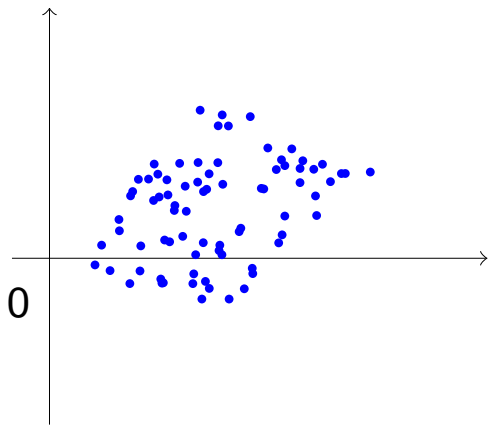


Number of signatures: 50

Results and Perspectives

Lattice-based Signature

We proposed an efficent scheme by fixing a broken one using lattice techniques
[ABDG14] *Sealing the Leak on Classical NTRU Signatures*. Post-Quantum Cryptography 2014

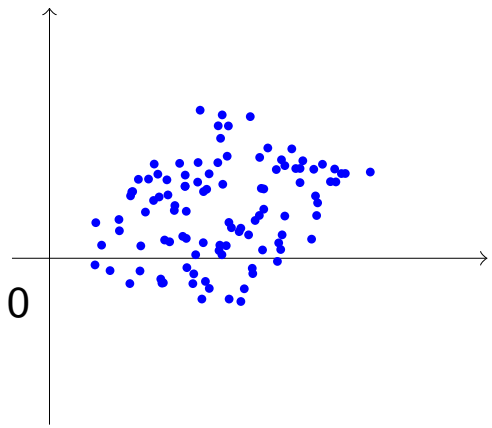


Number of signatures: 75

Results and Perspectives

Lattice-based Signature

We proposed an efficent scheme by fixing a broken one using lattice techniques
[ABDG14] *Sealing the Leak on Classical NTRU Signatures*. Post-Quantum Cryptography 2014

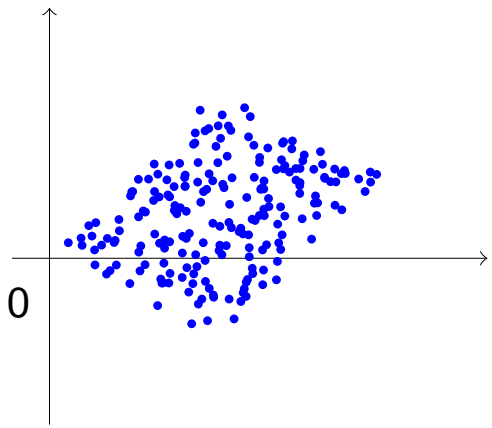


Number of signatures: 100

Results and Perspectives

Lattice-based Signature

We proposed an efficent scheme by fixing a broken one using lattice techniques
[ABDG14] *Sealing the Leak on Classical NTRU Signatures*. Post-Quantum Cryptography 2014

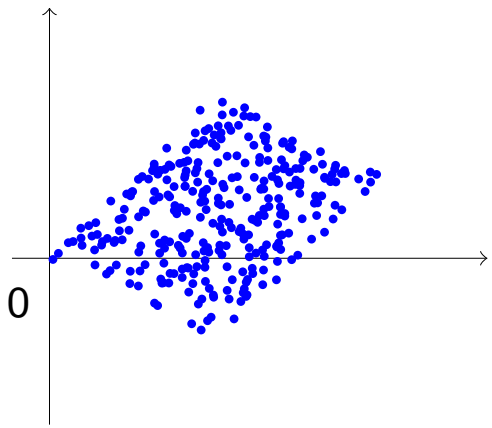


Number of signatures: 200

Results and Perspectives

Lattice-based Signature

We proposed an efficent scheme by fixing a broken one using lattice techniques
[ABDG14] *Sealing the Leak on Classical NTRU Signatures*. Post-Quantum Cryptography 2014

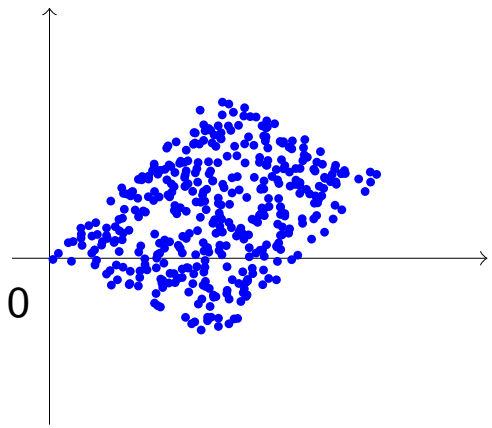


Number of signatures: 300

Results and Perspectives

Lattice-based Signature

We proposed an efficent scheme by fixing a broken one using lattice techniques
[ABDG14] *Sealing the Leak on Classical NTRU Signatures*. Post-Quantum Cryptography 2014

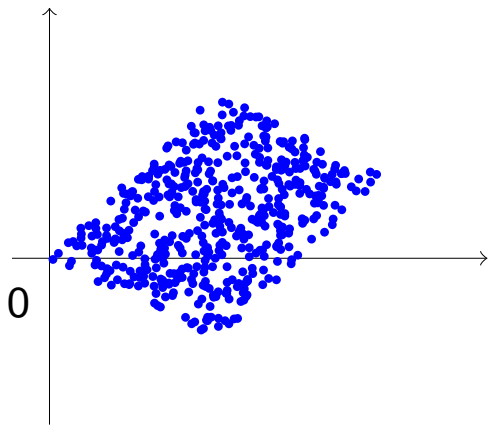


Number of signatures: 400

Results and Perspectives

Lattice-based Signature

We proposed an efficent scheme by fixing a broken one using lattice techniques
[ABDG14] *Sealing the Leak on Classical NTRU Signatures*. Post-Quantum Cryptography 2014

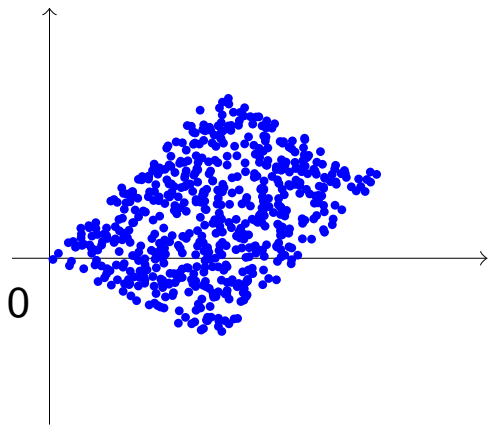


Number of signatures: 500

Results and Perspectives

Lattice-based Signature

We proposed an efficent scheme by fixing a broken one using lattice techniques
[ABDG14] *Sealing the Leak on Classical NTRU Signatures*. Post-Quantum Cryptography 2014

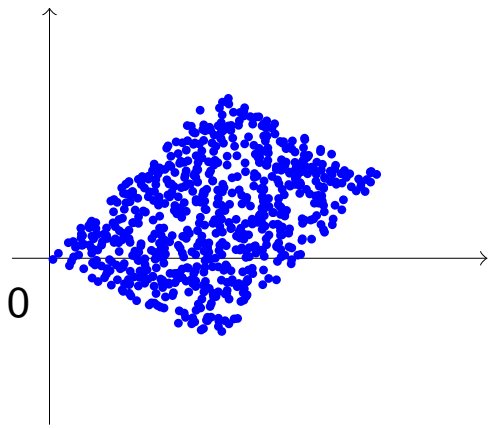


Number of signatures: 600

Results and Perspectives

Lattice-based Signature

We proposed an efficent scheme by fixing a broken one using lattice techniques
[ABDG14] *Sealing the Leak on Classical NTRU Signatures*. Post-Quantum Cryptography 2014

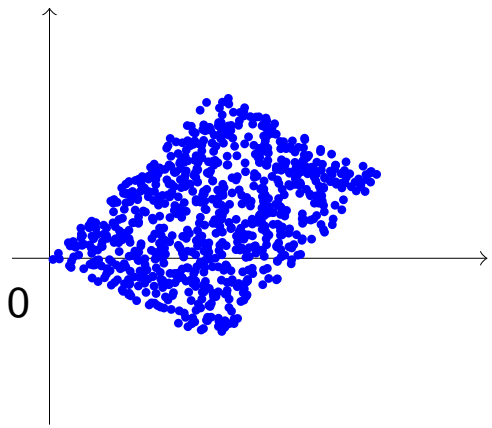


Number of signatures: 700

Results and Perspectives

Lattice-based Signature

We proposed an efficent scheme by fixing a broken one using lattice techniques
[ABDG14] *Sealing the Leak on Classical NTRU Signatures*. Post-Quantum Cryptography 2014

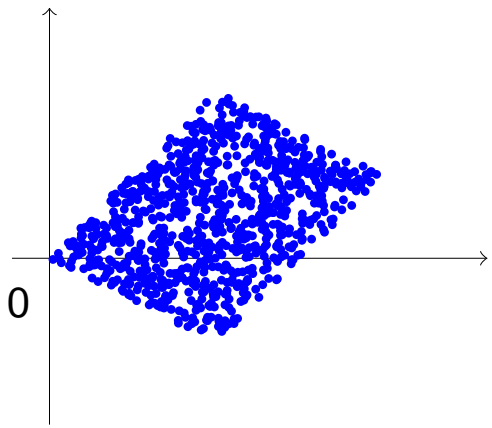


Number of signatures: 800

Results and Perspectives

Lattice-based Signature

We proposed an efficent scheme by fixing a broken one using lattice techniques
[ABDG14] *Sealing the Leak on Classical NTRU Signatures*. Post-Quantum Cryptography 2014

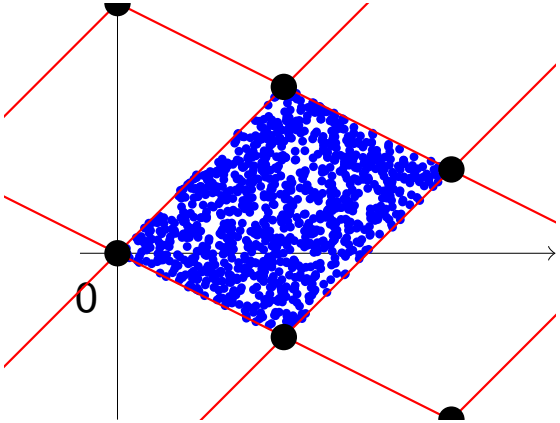


Number of signatures: 900

Results and Perspectives

Lattice-based Signature

We proposed an efficent scheme by fixing a broken one using lattice techniques
[ABDG14] *Sealing the Leak on Classical NTRU Signatures*. Post-Quantum Cryptography 2014

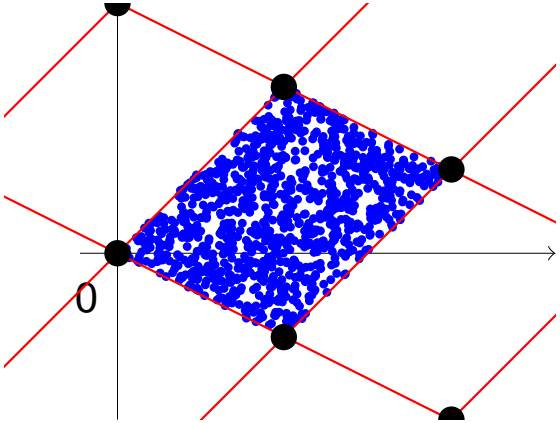


Number of signatures: 1000

Results and Perspectives

Lattice-based Signature

We proposed an efficent scheme by fixing a broken one using lattice techniques [ABDG14] *Sealing the Leak on Classical NTRU Signatures*. Post-Quantum Cryptography 2014



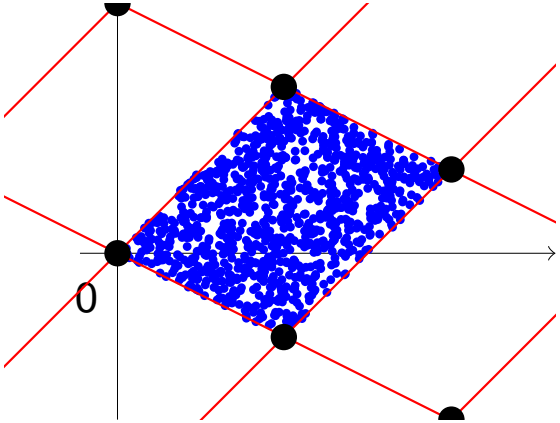
Number of signatures: 1000

Solution:
Rejection Sampling [Lyu12]

Results and Perspectives

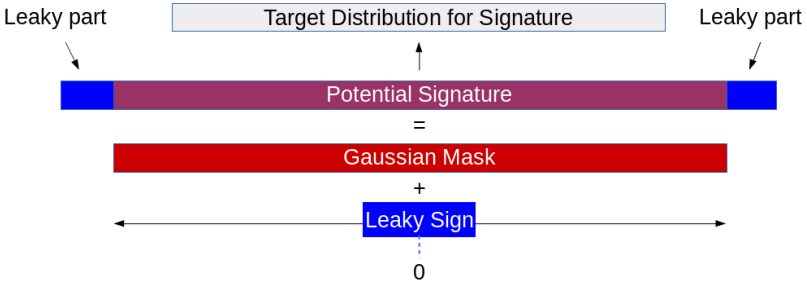
Lattice-based Signature

We proposed an efficent scheme by fixing a broken one using lattice techniques
[ABDG14] *Sealing the Leak on Classical NTRU Signatures*. Post-Quantum Cryptography 2014



Number of signatures: 1000

Solution:
Rejection Sampling [Lyu12]



Results and Perspectives

Lattice-based Signature

We proposed an efficent scheme by fixing a broken one using lattice techniques
[ABDG14] *Sealing the Leak on Classical NTRU Signatures*. Post-Quantum Cryptography 2014

Code-based Signature

We improved the efficiency of a class of signatures (namely threshold ring ones)
[DS14-15] *Improved Code-based Threshold Ring Signature Scheme*. Ongoing work

Results and Perspectives

Lattice-based Signature

We proposed an efficent scheme by fixing a broken one using lattice techniques
[ABDG14] *Sealing the Leak on Classical NTRU Signatures*. Post-Quantum Cryptography 2014

Code-based Signature

We improved the efficiency of a class of signatures (namely threshold ring ones)
[DS14-15] *Improved Code-based Threshold Ring Signature Scheme*. Ongoing work

Fully Homomorphic Encryption

Ongoing work in order to improve praticality...

References

[AB**D**G14] Aguilar Melchor, C., Boyen, X., **Deneuville, J.C.**, Gaborit, P. *Sealing the Leak on Classical NTRU Signatures*. Post-Quantum Cryptography 2014

[Ajtai96] Ajtai, M. *Generating Hard Instances of Lattice Problems*. STOC'96

[**D**S14-15] **Deneuville, J.C.**, Schrek, J. *Improved Code-based Threshold Ring Signature Scheme*. Ongoing Work...

[DN12] Ducas, L., Nguyen, Phong Q. *Learning a Zonotope and More: Cryptanalysis of NTRUSign Countermeasures*. AsiaCrypt'12

[Gentry09] Gentry, C. *A fully homomorphic encryption scheme*. Thesis, Stanford University

[HHPSW03] Hoffstein, J., Howgrave-graham, N., Pipher, J., Silverman, J.H., Whyte, W. *NTRUSign: Digital Signatures Using the NTRU Lattice*. AsiaCrypt'12

[Lyu12] Lyubashevsky, V. *Lattice Signatures Without Trapdoors*. EuroCrypt'12

[Shor94] Shor, P. W. *Algorithms for Quantum Computation: Discrete Logarithms and Factoring*. FOCS'94

Thank You !