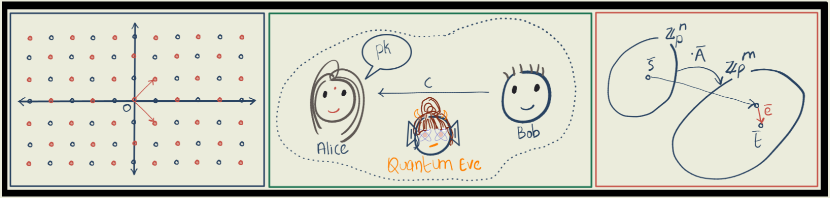


CS758: Advanced Tools from Modern Cryptography

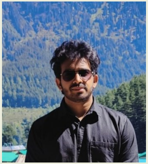
Lattice-Based Cryptography

Lecture 01 (06/Jan/26)

Instructor: Chethan Kamath

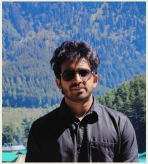
Administrivia..

- When and where: Slot 10 (14:00-15:25, Tuesdays and Fridays), CC101
- Contact hours: drop by my office (CC305) any time!
- Teaching assistant: Priyanshu Singh (24M2101)



Administrivia..

- When and where: Slot 10 (14:00-15:25, Tuesdays and Fridays), CC101
- Contact hours: drop by my office (CC305) any time!
- Teaching assistant: Priyanshu Singh (24M2101)



- Announcements/online discussion on Moodle:
  - moodle.iitb.ac.in/course/view.php?id=9123
- Any volunteers for class rep?
  - Please set up WhatsApp/Signal group for coordination

Administrivia..

- Grading Scheme

Weightage	Towards
30%	End-sem
25%	Mid-sem
20%	Paper presentation (two students per paper)
15%	Two quizzes
5%	Class participation
5%	Scribing (1-2 lectures per student)

Administrivia..

- Grading Scheme

Weightage	Towards
30% +5	End-sem
25% +5	Mid-sem
~~20%~~	~~Paper presentation (two students per paper)~~
15% +10	Two quizzes
5%	Class participation
5%	Scribing (1-2 lectures per student)

  - Please submit scribe notes within two weeks
  - Will scrap paper presentation and readjust grades if strength > 20
  - Attendance is not mandatory (but encouraged)

Administrivia..

- Resources can be found on course website
  - cse.iitb.ac.in/∼ckamath/courses/2026s/CS758.html

Administrivia..

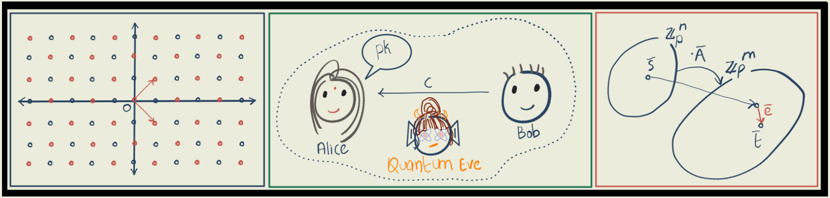
- Resources can be found on course website
  - cse.iitb.ac.in/∼ckamath/courses/2026s/CS758.html
- Not based on textbook. Related courses:
  1. CS206A, Lattices Algorithms and Applications (Spring 2007) by Daniele Micciancio, for Module I
  2. CS294: Lattices, Learning with Errors and Post-Quantum Cryptography by Vinod Vaikuntanathan, for Modules II and III
- Handwritten notes will be posted on Moodle after lectures

Administrivia..

- Resources can be found on course website
  - cse.iitb.ac.in/∼ckamath/courses/2026s/CS758.html
- Not based on textbook. Related courses:
  1. CS206A, Lattices Algorithms and Applications (Spring 2007) by Daniele Micciancio, for Module I
  2. CS294: Lattices, Learning with Errors and Post-Quantum Cryptography by Vinod Vaikuntanathan, for Modules II and III
- Handwritten notes will be posted on Moodle after lectures

⚠ Pre-requisites

- ⚠ Will assume basic cryptography (CS409/CS409m/CS783)
- ☆ Brush up your linear algebra
- ☆ Useful to know basic coding theory and complexity theory
  - TA will conduct recitation sessions for these topics



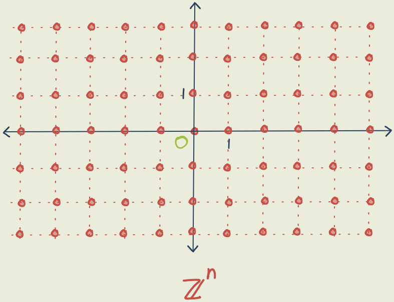
CS758: Advanced Tools from Modern Cryptography

Lattice-Based Cryptography

Lecture 01 (06/Jan/26)

Instructor: Chethan Kamath

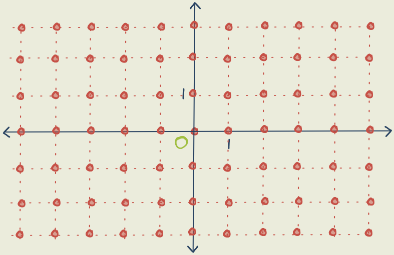
What are Lattices?



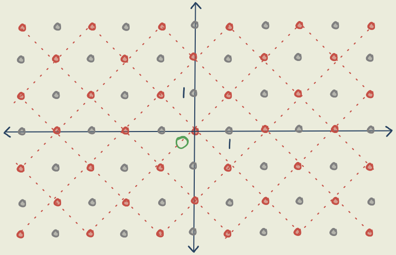
Informal Definition 1

Discrete subspace of (vector space) $\mathbb{R}^n$

What are Lattices?



$\mathbb{Z}^n$

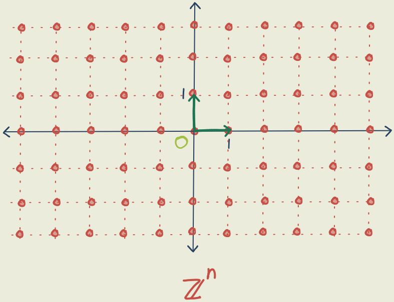


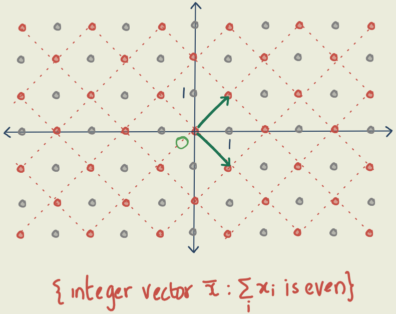
$\{\text{integer vector } \bar{x} : \sum_i x_i \text{ is even}\}$

Informal Definition 1

Discrete subspace of (vector space) $\mathbb{R}^n$

What are Lattices?





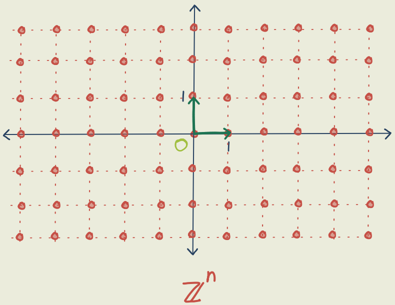
Informal Definition 1

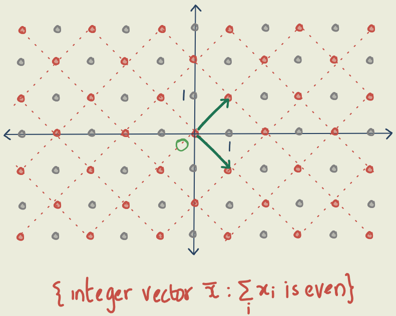
Discrete subspace of (vector space) $\mathbb{R}^n$

Informal Definition 2

Integer linear combinations of linearly-independent vectors $\bar{b}_1, \ldots, \bar{b}_m \in \mathbb{R}^n$

What are Lattices?





Informal Definition 1

Discrete subspace of (vector space) $\mathbb{R}^n$

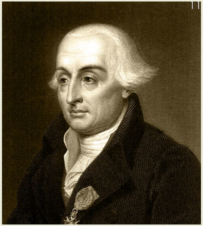
Informal Definition 2

Integer linear combinations of linearly-independent vectors $\bar{b}_1, \ldots, \bar{b}_m \in \mathbb{R}^n$

rank

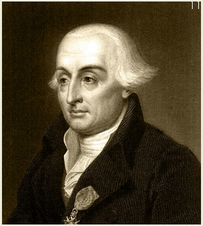
dimension

How are Lattices Useful?



- Historical applications
  1. Tool to study pure mathematics
     - E.g., as a bridge between number theory and geometry: can prove Fermat's theorem on sums of two squares using lattices

How are Lattices Useful?



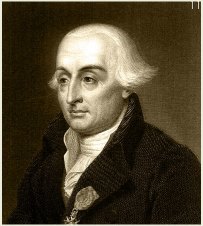
Lagrange

Gauß

Minkowski

- Historical applications
  1. Tool to study pure mathematics
     - E.g., as a bridge between number theory and geometry: can prove Fermat's theorem on sums of two squares using lattices

How are Lattices Useful?..


Lagrange


Gauß


Minkowski


Bravais

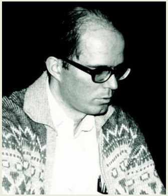
- Historical applications
  1. Tool to study pure mathematics
     - E.g., as a bridge between number theory and geometry: can prove Fermat's theorem on sums of two squares using lattices
  2. Chemistry: to study crystal structure (crystallography)

  ...

How are Lattices Useful?..

Coppersmith

Lagarias



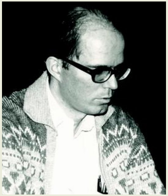
Odłyżko

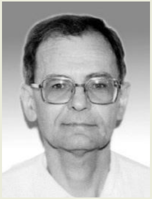
- Modern applications
  1. Coding theory
  2. Cryptanalysis: breaking schemes using lattice algorithms

How are Lattices Useful?


Coppersmith


Lagarias


Odłyżko

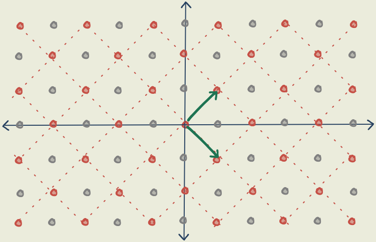

Ajtai


Regev

- Modern applications
  1. Coding theory
  2. Cryptanalysis: breaking schemes using lattice algorithms
  3. Lattice-based cryptography: constructing cryptographic primitives assuming hardness of lattice problems

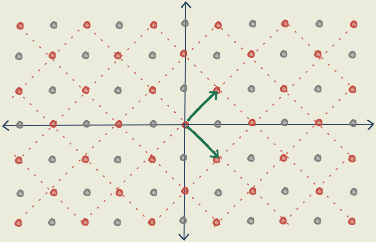
  ...

How are Lattices Useful?..



- Why lattice-based cryptography?
    1. Fast (linear) operations ⚡

How are Lattices Useful?..

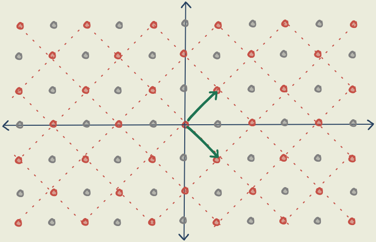


- Why lattice-based cryptography?

    1. Fast (linear) operations
    2. Worst-case to average-case reductions

        $\Rightarrow$ Cryptography based on worst-case assumptions!

How are Lattices Useful?..

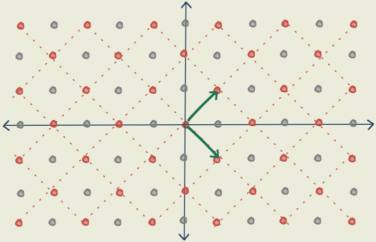


- Why lattice-based cryptography?
  1. Fast (linear) operations
  2. Worst-case to average-case reductions

     $\Rightarrow$ Cryptography based on worst-case assumptions!
  3. No efficient quantum algorithms known

     $\Rightarrow$ Post-quantum cryptography

How are Lattices Useful?..

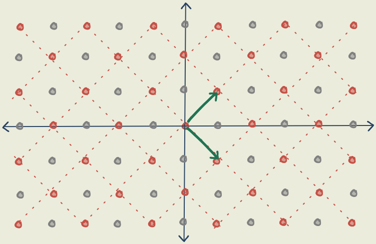


- Why lattice-based cryptography?
  1. Fast (linear) operations
  2. Worst-case to average-case reductions

     $\Rightarrow$ Cryptography based on worst-case assumptions!
  3. No efficient quantum algorithms known

     $\Rightarrow$ Post-quantum cryptography
  4. Expressive! We know how to construct certain primitives only from lattices
     - E.g., Fully-Homomorphic Encryption (FHE)

CS758: Course Overview



1. Module I: Introduction to Lattices
2. Module II: Basic Cryptography from Lattices
3. Module III: Advanced Cryptography from Lattices

Module I: Introduction to Lattices.

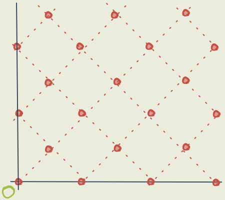
- Study computational problems on lattices

Module I: Introduction to Lattices

- Study computational problems on lattices

Shortest Vector Problem (SVP)

- I/p: lattice Λ



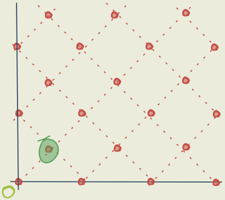
- Solution: *shortest* non-zero lattice vector $\bar{x}$ in Λ

Module I: Introduction to Lattices

- Study computational problems on lattices

Shortest Vector Problem (SVP)

- I/p: lattice Λ



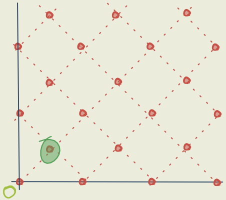
- Solution: *shortest* non-zero lattice vector $\bar{x}$ in Λ

Module I: Introduction to Lattices

- Study computational problems on lattices

Shortest Vector Problem (SVP)

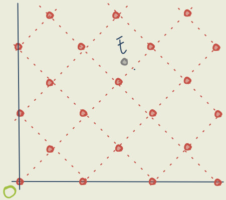
- I/p: lattice Λ



- Solution: *shortest* non-zero lattice vector $\bar{x}$ in Λ

Closest Vector Problem (CVP)

- I/p: lattice Λ, target $\bar{t} \in \mathbb{R}^n$



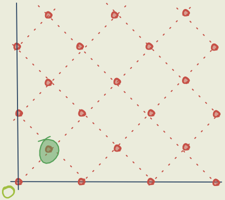
- Solution: lattice vector $\bar{x}$ *closest* to $\bar{t}$

Module I: Introduction to Lattices

- Study computational problems on lattices

Shortest Vector Problem (SVP)

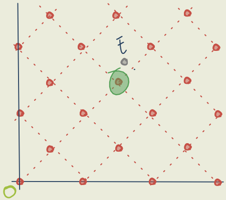
- I/p: lattice Λ



- Solution: *shortest* non-zero lattice vector $\bar{x}$ in Λ

Closest Vector Problem (CVP)

- I/p: lattice Λ, target $\bar{t} \in \mathbb{R}^n$



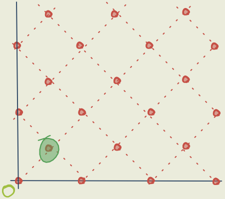
- Solution: lattice vector $\bar{x}$ *closest* to $\bar{t}$

Module I: Introduction to Lattices

- Study computational problems on lattices

Shortest Vector Problem (SVP)

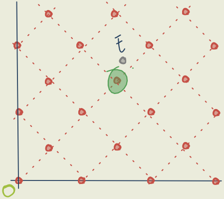
- I/p: lattice Λ



- Solution: *shortest* non-zero lattice vector $\bar{x}$ in Λ

Closest Vector Problem (CVP)

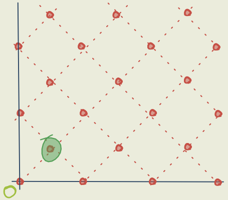
- I/p: lattice Λ, target $\bar{t} \in \mathbb{R}^n$



- Solution: lattice vector $\bar{x}$ *closest* to $\bar{t}$

- Also look at *estimation* and *approximation* variants
- Most problems hard to solve in the *worst case* ($\mathbf{NP}$-hard, in fact)

Module I: Introduction to Lattices.

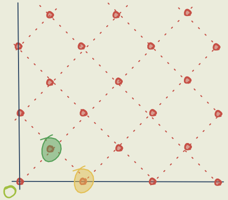


- Algorithms for lattice problems, e.g., LLL algorithm

Informal Theorem 1 ([LLL82])

There exists a polynomial-time algorithm that solves SVP up to an *exponential* (in n) approximation factor

Module I: Introduction to Lattices.

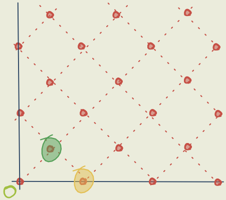


- Algorithms for lattice problems, e.g., LLL algorithm

Informal Theorem 1 ([LLL82])

There exists a polynomial-time algorithm that solves SVP up to an *exponential* (in n) approximation factor

Module I: Introduction to Lattices.



- Algorithms for lattice problems, e.g., LLL algorithm

Informal Theorem 1 ([LLL82])

There exists a polynomial-time algorithm that solves SVP up to an *exponential* (in n) approximation factor

Cryptanalysis using lattice algorithms:

- Factorise integers
- Solve low-exponent RSA
- Break Linear Congruential Generators (LCG)

Module II: Basic Cryptography from Lattices..

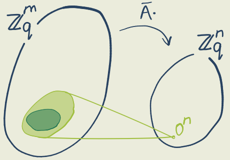
- Cryptography requires *average-case* hard problems
    - E.g., integer factorisation, discrete-logarithm problem (DLP)

Module II: Basic Cryptography from Lattices..

- Cryptography requires *average-case* hard problems
  - E.g., integer factorisation, discrete-logarithm problem (DLP)
- Lattice-based average-case hard problems (think $m > n$ below):

Short Integer Solution (SIS)

- I/p: matrix $\overline{A} \leftarrow \mathbb{Z}_q^{n \times m}$



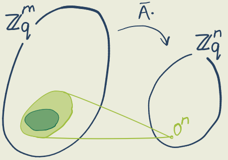
- Solution: "short" $\bar{x} \neq 0^m$ such that $\overline{A}\bar{x} = 0^n \bmod q$

Module II: Basic Cryptography from Lattices..

- Cryptography requires *average-case* hard problems
  - E.g., integer factorisation, discrete-logarithm problem (DLP)
- Lattice-based average-case hard problems (think $m > n$ below):

Short Integer Solution (SIS)

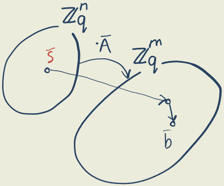
- I/p: matrix $\overline{A} \leftarrow \mathbb{Z}_q^{n\times m}$



- Solution: "short" $\bar{x} \neq 0^m$ such that $\overline{A}\bar{x} = 0^n \bmod q$

Learning With Errors (LWE)

- I/p: matrix $\overline{A} \leftarrow \mathbb{Z}_q^{n\times m}$ and $\bar{b}^t \approx \bar{s}^t\overline{A}$, where $\bar{s} \leftarrow \mathbb{Z}_q^n$



- Solution: $\bar{s}$

Module II: Basic Cryptography from Lattices..

- What is the connection to lattices?

Module II: Basic Cryptography from Lattices..

- What is the connection to lattices? Can be viewed as *average-case* variants of CVP

Informal Theorem 2 ([Ajt96] (resp., [Reg05]))

SIVP (resp., BDD) is worst-case hard $\Rightarrow$ SIS (resp., LWE) is average-case hard

Module II: Basic Cryptography from Lattices..

- What is the connection to lattices? Can be viewed as *average-case* variants of CVP

Informal Theorem 2 ([Ajt96] (resp., [Reg05]))

SIVP (resp., BDD) is worst-case hard $\Rightarrow$ SIS (resp., LWE) is average-case hard

- What can we construct assuming SIS and LWE?

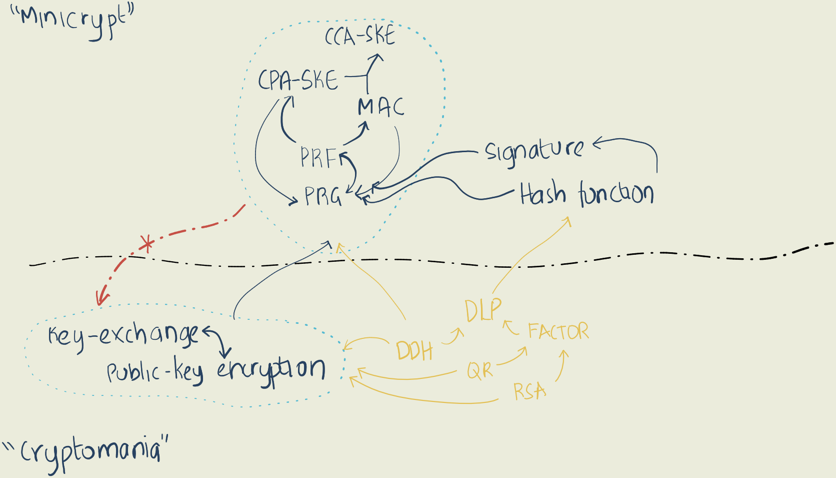
Informal Theorem 3 ([Ajt96])

SIS $\Rightarrow$ one-way function (OWF) and collision-resistant hash function

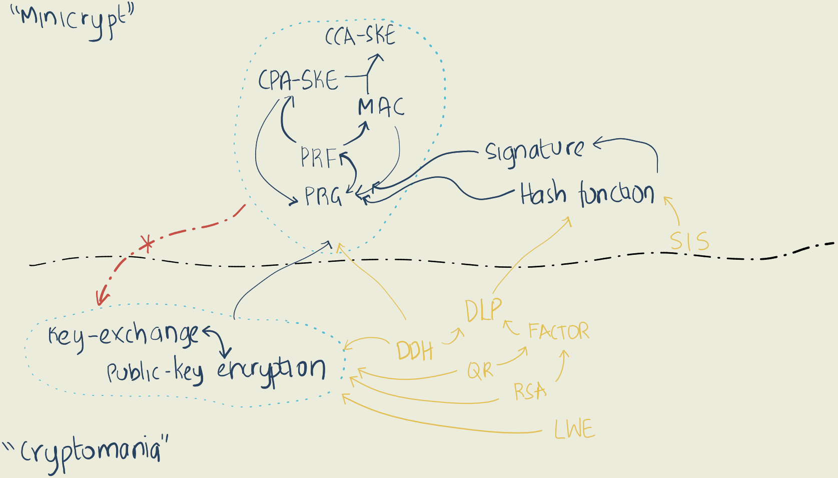
Informal Theorem 4 ([Reg05])

LWE $\Rightarrow$ public-key encryption (PKE)

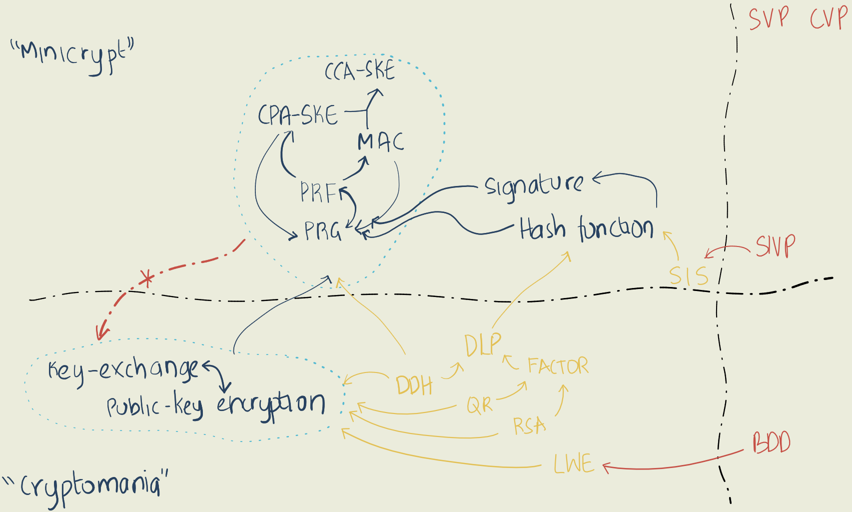
The Cryptographic Landscape



The Cryptographic Landscape



The Cryptographic Landscape

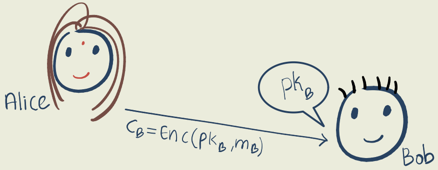


Module III: Advanced Cryptography from Lattices..

Advanced Primitive I: Identity-Based Encryption (IBE) [Sha84]

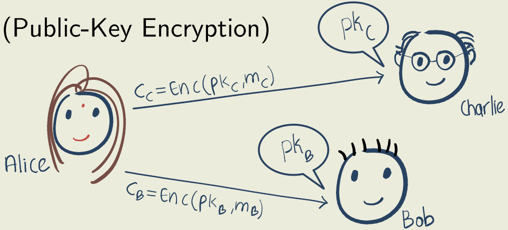
Advanced Primitive I: Identity-Based Encryption (IBE) [Sha84]

- Recall PKE (Public-Key Encryption)



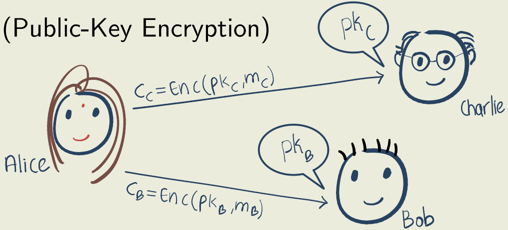
Advanced Primitive I: Identity-Based Encryption (IBE) [Sha84]

- Recall PKE (Public-Key Encryption)



Advanced Primitive I: Identity-Based Encryption (IBE) [Sha84]

- Recall PKE (Public-Key Encryption)

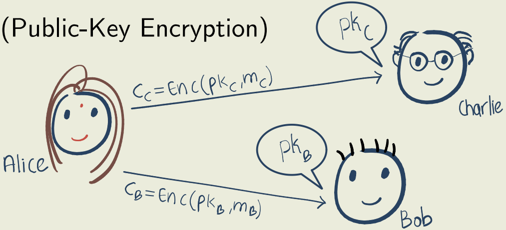


Drawback: need to maintain (authenticated) directory with identity (e.g., e-mail address) and PK pairs

Module III: Advanced Cryptography from Lattices..

Advanced Primitive I: Identity-Based Encryption (IBE) [Sha84]

- Recall PKE (Public-Key Encryption)



Drawback: need to maintain (authenticated) directory with identity (e.g., e-mail address) and PK pairs

IBE solves this issue: identity *itself* is the public key!

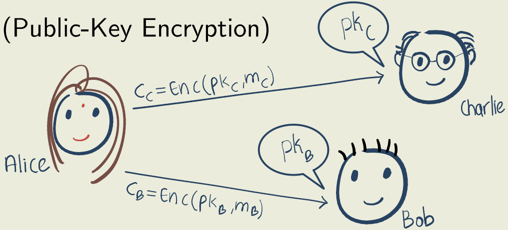
Informal Theorem 5 ([GPV08])

$\mathrm{LWE} \Rightarrow$ IBE

Module III: Advanced Cryptography from Lattices..

Advanced Primitive I: Identity-Based Encryption (IBE) [Sha84]

- Recall PKE (Public-Key Encryption)



Drawback: need to maintain (authenticated) directory with identity (e.g., e-mail address) and PK pairs

IBE solves this issue: identity *itself* is the public key!

Informal Theorem 5 ([GPV08])

$\text{LWE} \Rightarrow$ IBE

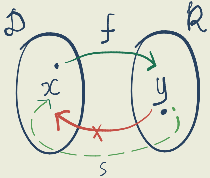
++ Generalisation of IBE: attribute-based encryption (ABE) [SW04]

- Application: secure access control (e.g., Cloudflare's GeoV2)

Module III: Advanced Cryptography from Lattices..

Advanced Primitive I: Identity-Based Encryption (IBE) [Sha84]

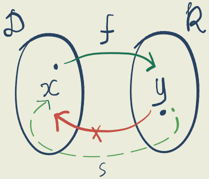
- Recall trapdoor functions: OWF that is easy to invert given a "secret" s



Module III: Advanced Cryptography from Lattices..

Advanced Primitive I: Identity-Based Encryption (IBE) [Sha84]

- Recall trapdoor functions: OWF that is easy to invert given a "secret" s



Key tool: lattice trapdoors, e.g., a "short" basis

Informal Theorem 6 ([Ajt96; MP12])

There exists a PPT algorithm that samples a SIS matrix $\overline{A} \leftarrow \mathbb{Z}_q^{n\times m}$ along with a "short" matrix $\overline{S} \in \mathbb{Z}^{m\times m}$ such that $\overline{A}\,\overline{S} = 0^{n\times m} \bmod q$

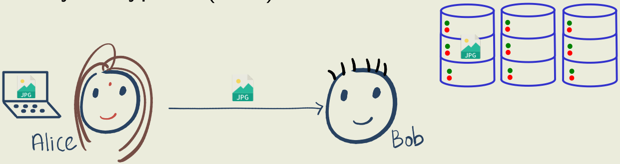
Module III: Advanced Cryptography from Lattices..

Advanced Primitive II: FHE (Fully-Homomorphic Encryption) [RAD78]

Module III: Advanced Cryptography from Lattices..

Advanced Primitive II: FHE (Fully-Homomorphic Encryption) [RAD78]

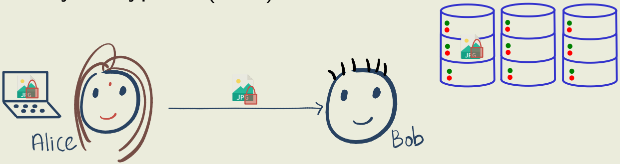
- Recall secret-key encryption (SKE)



Module III: Advanced Cryptography from Lattices..

Advanced Primitive II: FHE (Fully-Homomorphic Encryption) [RAD78]

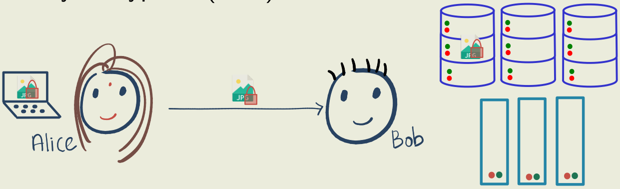
- Recall secret-key encryption (SKE)



Module III: Advanced Cryptography from Lattices..

Advanced Primitive II: FHE (Fully-Homomorphic Encryption) [RAD78]

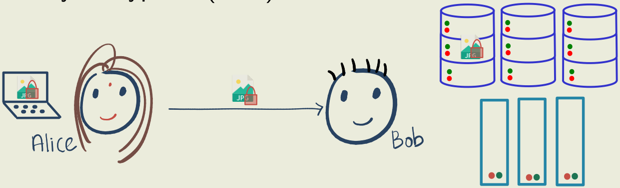
- Recall secret-key encryption (SKE)



Module III: Advanced Cryptography from Lattices..

Advanced Primitive II: FHE (Fully-Homomorphic Encryption) [RAD78]

- Recall secret-key encryption (SKE)

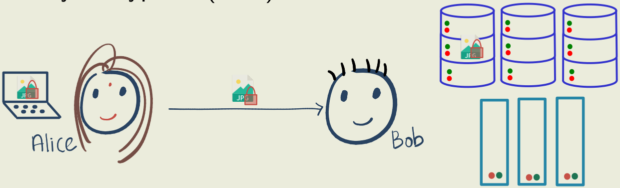


Drawback: no “fine-grained” access

Module III: Advanced Cryptography from Lattices..

Advanced Primitive II: FHE (Fully-Homomorphic Encryption) [RAD78]

- Recall secret-key encryption (SKE)



Drawback: no “fine-grained” access

FHE: allows computing *over the ciphertext*!

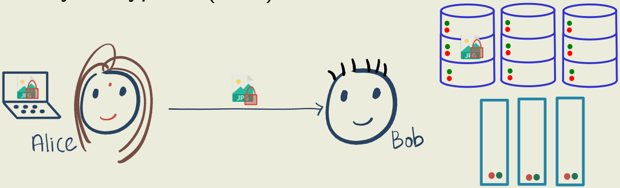
Informal Theorem 7 ([GSW13])

$\mathrm{LWE} \Rightarrow$ FH(PK)E

Module III: Advanced Cryptography from Lattices..

Advanced Primitive II: FHE (Fully-Homomorphic Encryption) [RAD78]

- Recall secret-key encryption (SKE)



Drawback: no "fine-grained" access

FHE: allows computing *over the ciphertext*!

Informal Theorem 7 ([GSW13])

$\mathrm{LWE} \Rightarrow$ FH(PK)E

- Applications:
  - Private (zero-trust) outsourcing of computation
  - Encrypted search (e.g., see Zama)

Lecture Resources

1. *Lecture 1: Introduction* of CSE206A (Spring 2007), by Micciancio (PDF)
2. *Historical Talk on Lattice-Based Cryptography*, Micciancio (YouTube)
3. *Mathematics of Lattices*, Micciancio (YouTube)

References

- Ajtai, Miklós. "Generating Hard Instances of Lattice Problems (Extended Abstract)". In: *28th ACM STOC*.
- Gentry, Craig, Chris Peikert, and Vinod Vaikuntanathan. "Trapdoors for hard lattices and new cryptographic constructions". In: *40th ACM STOC*.
- Gentry, Craig, Amit Sahai, and Brent Waters. "Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based". In: *CRYPTO 2013, Part I*.
- Lenstra, A. K., H. W. Lenstra, and L. Lovász. "Factoring polynomials with rational coefficients". In: *Mathematische Annalen* 4 ().
- Micciancio, Daniele and Chris Peikert. "Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller". In: *EUROCRYPT 2012*.
- Regev, Oded. "On lattices, learning with errors, random linear codes, and cryptography". In: *37th ACM STOC*.
- Rivest, Ronald L, Len Adleman, and Michael L Dertouzos. "On data banks and privacy homomorphisms". In: *Foundations of secure computation* 11 ().
- Sahai, Amit and Brent Waters. *Fuzzy Identity Based Encryption*. Cryptology ePrint Archive, Report 2004/086.
- Shamir, Adi. "Identity-Based Cryptosystems and Signature Schemes". In: *CRYPTO'84*.