Ideal Lattices: cryptographic applications and open problems

Daniele Micciancio (UCSD)

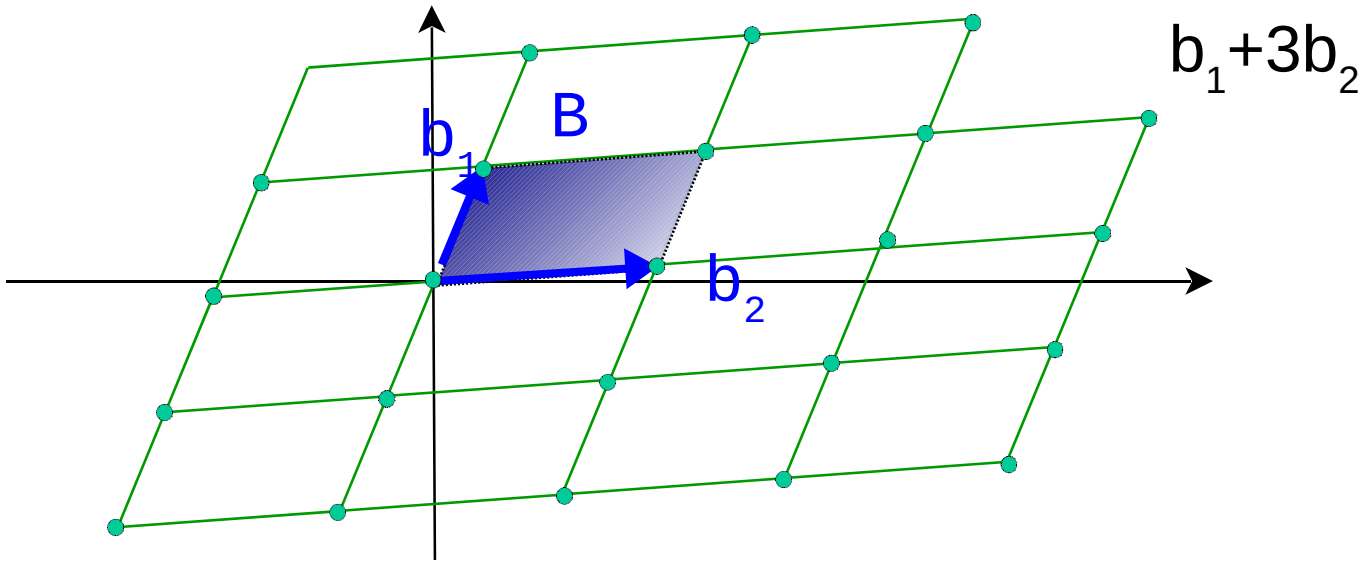
based on joint work with
Vadim Lyubashevsky (UCSD)

Outline

- Basing cryptography on *lattices*
- Average-case vs. worst-case complexity
- *Cyclic lattices* and generalizations
- Connections to *algebraic number theory*
- (Implementation issues)
- Open problems

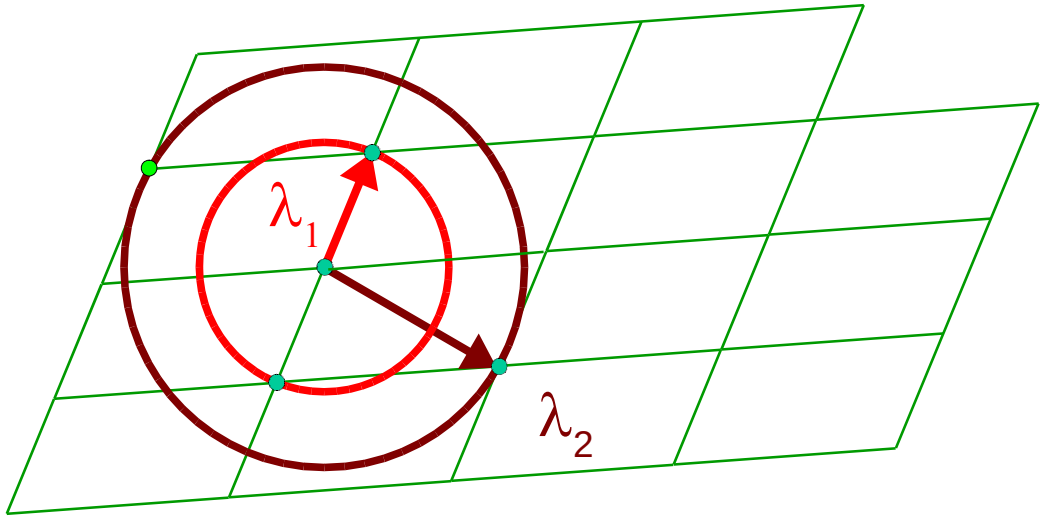
Point Lattices

- Set of all integer linear combinations of basis vectors $B = [b_1,...,b_n] \subset R^n$
- $L(B)=\{Bx: x \in Z^n\} \subset \text{span}(B)=\{Bx: x \in R^n\}$



Successive Minima

- For every n-dimensional lattice L, and i=1,...,n, the i*th* successive minimum $l_i(L)$ is the smallest radius r such that Ball(0,r) contains i linearly independent lattice vectors



Lattice problems

- Shortest Vector Problems (SVP)
  - Given a lattice L, find the nonzero lattice vector v closest to the origin (||v|| g $l_1(L)$)
- Shortest Independent Vect. Prob. (SIVP)
  - Given a lattice L, find n lin. independent vectors $v_1,...,v_n$ of length $\max_i ||v_i||$ g $l_n(L)$
- Approximation factor g(n) usually a function of the lattice dimension n.

Complexity of SVP & SIVP

- No polytime algorithm is known for $g(n)=n^{O(1)}$
- Best polytime algorithm achieve $g(n)=2^{O(n \log \log n/\log n)}$ [LLL'82, Schnorr'87+Ajtai,Kumar,Sivakumar'01]
- NP-hard for any constant approximation factors [Ajtai98, Mic98/01, Khot04, Blomer&Seifert'99]
- Conjecture: SVP and SIVP are hard to approximate within polynomial factors.
- Hardness of approximating SVP and SIVP used in cryptography

Hard in practice?

- [LLL] & variants perform much better on random lattices than exponential worst case bound
- Approximating SVP and SIVP is in coAM for factors $O((n/\log n)^{1/2})$ and in coNP for factors $O(n^{1/2})$ [Goldreich&Goldwasser'01, Aharonov&Regev'04, Guruswami,Micciancio&Regev'04]
- Conjecture: SVP/SIVP are hard to approximate
  - in the worst-case
  - for small polynomial factors

Cyclic Lattices

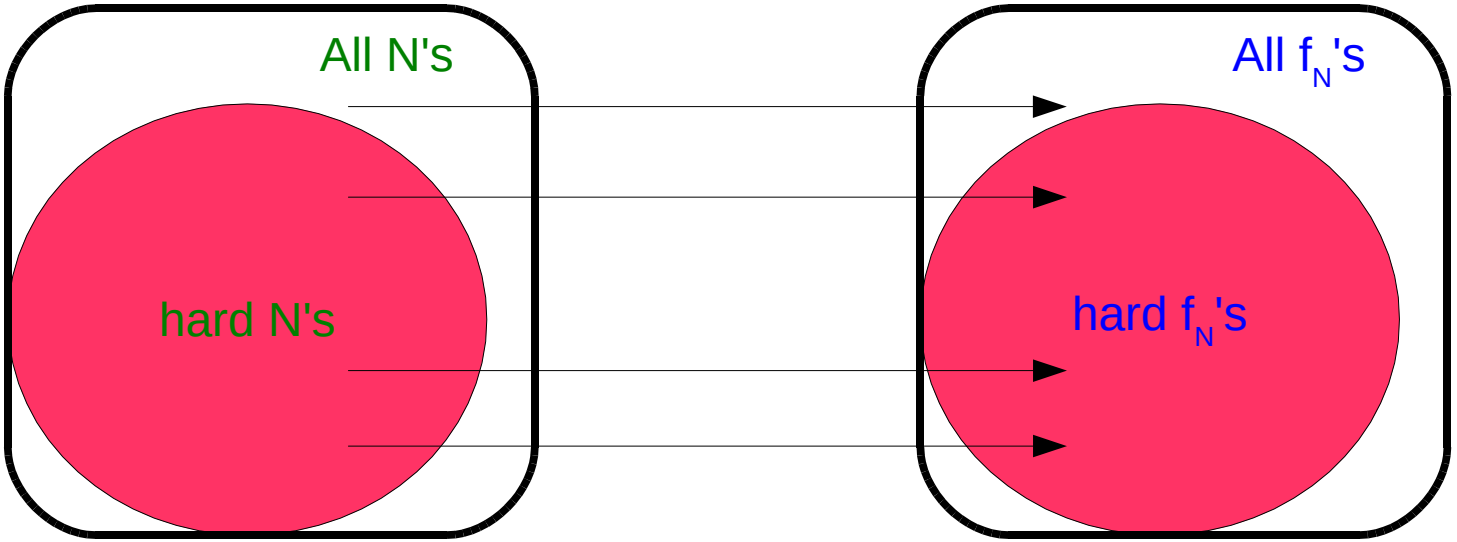
- Define $rot[x_1,\ldots,x_n] = [x_n,x_1,\ldots,x_{n-1}]$
- Lattice L is cyclic if rot(L) = L
  - {B | L(B) is cyclic} is polytime decidable
- All lattice problems SVP, SIVP can be restricted to cyclic lattices:
  - CyclicSVP: Given cyclic L(B), solve SVP(B)
- CyclicSVP potentially easier than SVP ... will get back to cyclic lattices later

Lattice based cryptography

- Public key encryption
  - Aitai&Dwork97, Regev04, Regev05
- One-way hash functions
  - Based on worst-case hardness of SIVP & SVP for $g(n)=n^c$
  - Ajtai96 ($c>8$), Cai&Nerurkar97, Mic.02/04, Micciancio&Regev04 ($c > 1$)
- Provably secure based on worst-case intractability assumptions!

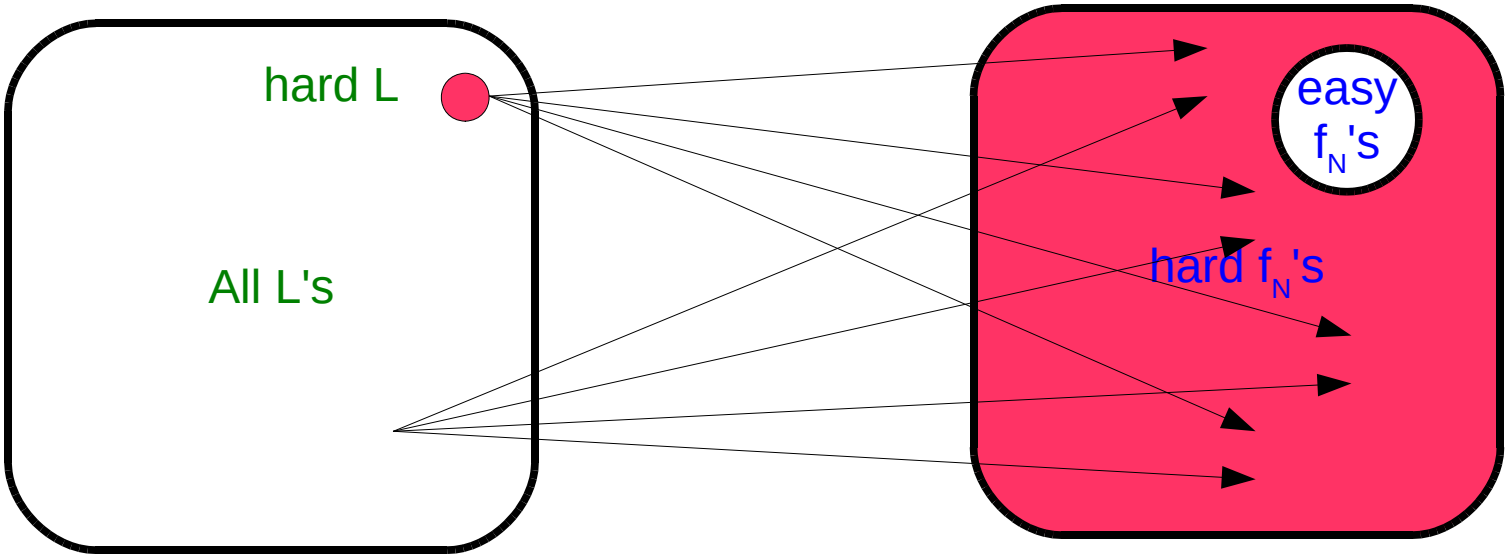
Provable security (from average case hardness)

- Example: (Rabin) modular squaring
  - $f_N(x) = x^2 \bmod N$, where $N=pq$, ...
  - Inverting f_N is as hard as factoring N
- f_N is a one-way function, provided *most* N are hard to factor

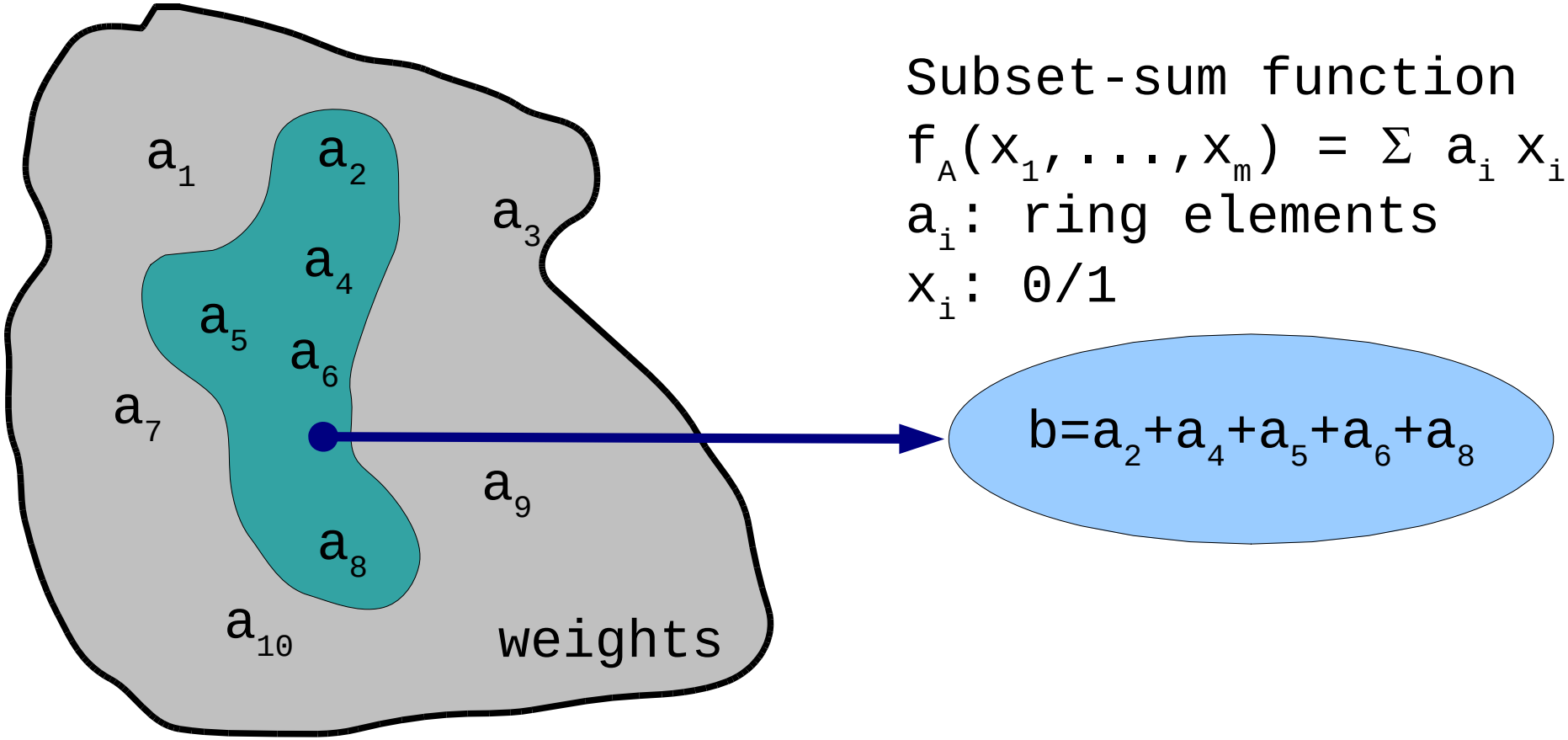


Provable security (from worst case hardness)

- Any fixed L is mapped to random f_N
- f_N is a one-way function assuming lattice problem L is hard in the worst case



The Subset-sum Problem



Subset-sum function

$f_A(x_1,...,x_m) = \Sigma\ a_i\ x_i$

a_i: ring elements

x_i: 0/1

Subset Sum Problem: Given weights $A = (a_1,...,a_m)$ and find coefficients $x_1,...,x_m$ such that $f_A(x_1,...,x_m) =$

Brief history of Knapsack Cryptosystems

- Merkle&Hellman [1978]
  - Broken by [Shamir82] and [Brickell84]
- Goodman and McAuley [1984]
  - Broken [Joux&Stern93]
- Chor and Rivest [1984]
  - Broken [Vaudenay01]
- Many other systems
  - All broken!!!

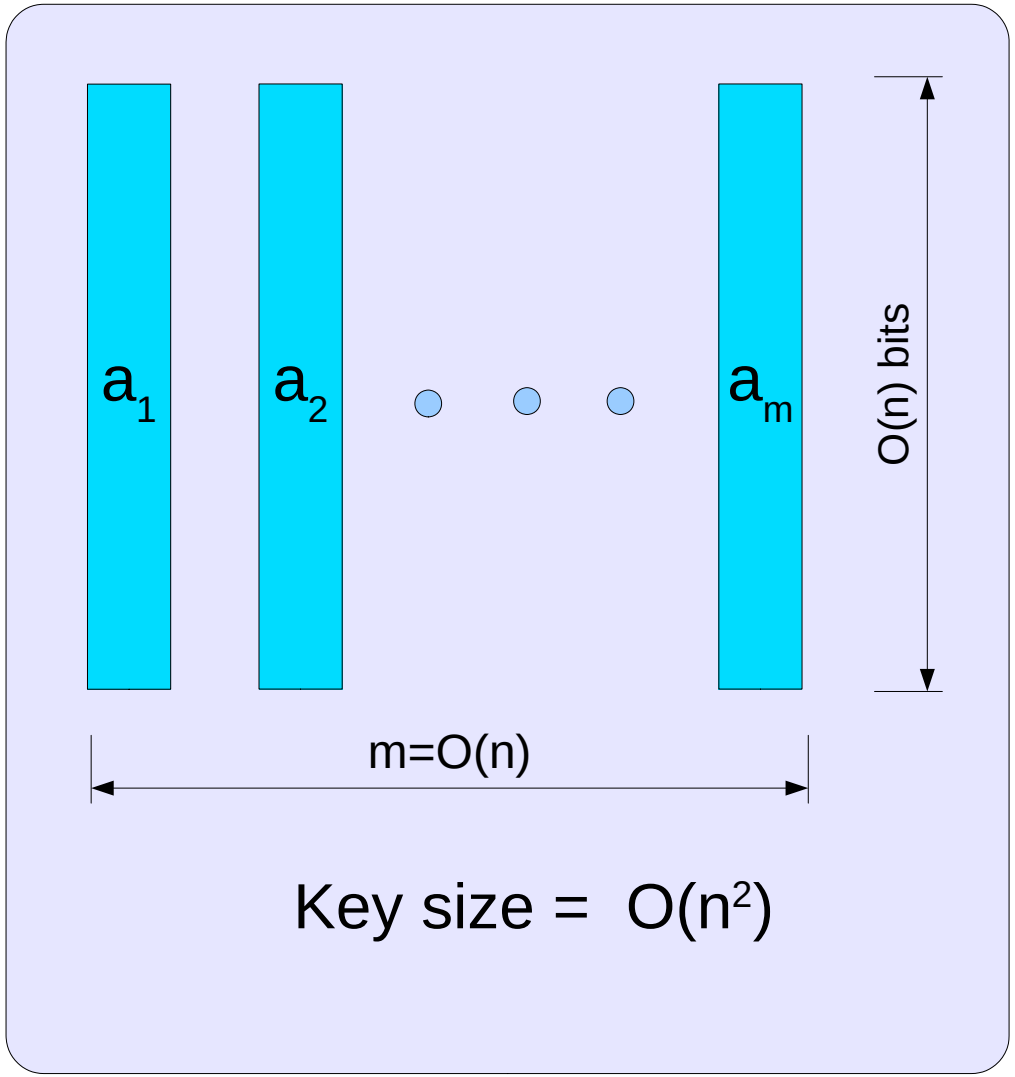
Ajtai's one-way function

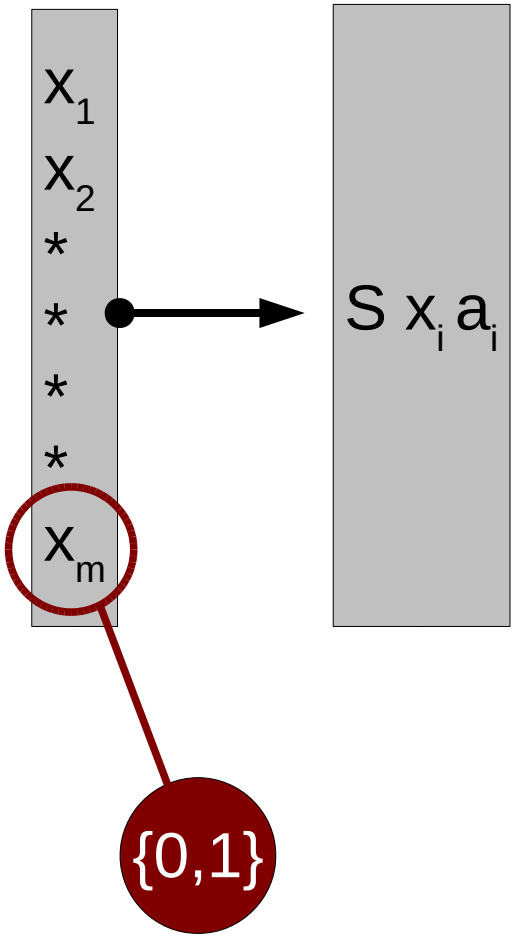
- Sub-setsum function over product ring Z_p^n
  - n: security parameter
  - $p(n) = n^{O(1)}$ small modulus
- Provably one-way
  - Worst case assumption: hardness of SIVP within $g(n) = n^c$ (for c>8)
- [Micciancio&Regev]: improve to any c>1
- Still may be subject to lattice attacks

Taxonomy of Attacks

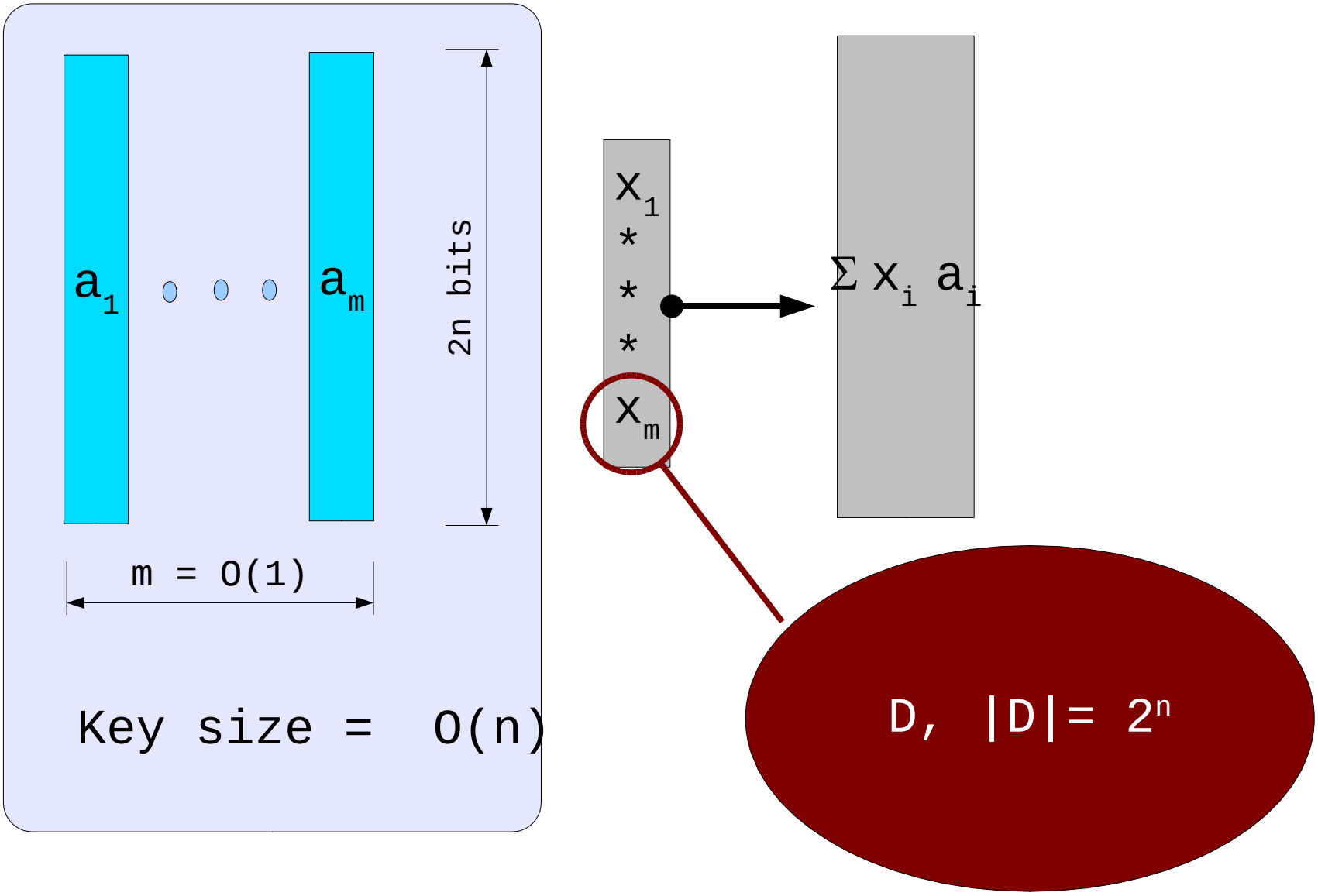
- Attacks to trapdoor knapsacks
  - exploit special structure (e.g., trapdoor)
  - provably good, often work in polynomial time
- Generic attacks (e.g., low-density attacks)
  - can be applied to knapsack without trapdoor
  - usually only heuristics
  - avoided increasing the security parameter
  - still can be devastating in practice

Key Size of subset-sum function





Compact knapsack key size



Compact knapsack

- $f_A(x_1,...,x_m)=Sx_ia_i$, $f: D^m \dashrightarrow R$
  - Weights $a_1,...,a_m$ are chosen from ring R
  - Inputs $x_1,...,x_m$ are chosen from some restricted subset D of R
- Examples: $R=Z_N$ where $N=2^{2n}$
  - $D = \{0,1\}$ $(m=4n)$
  - $D = \{0,..,(2^n - 1)\}$ $(m=4)$
- Brute force attack takes $|D|^m = 2^{4n}$

Bad idea!

- Compact knapsack function can be inverted in polynomial time for any fixed m = O(1)
  - [Amirazizi, Karnin, Reyneri 81]
- Compact knapsack function can be inverted in quasi polynomial time $n^{O(\log \log n)}$ for m=O(log n)
  - Follows from [Kannan 87] algorithms to solve SVP and CVP in $O(m^m)$ time

Polynomial rings

- $R = Z[x] / (x^n-1,p)$
- E.g., if p=5, n = 3
  - $(x+2) + (x^2+3) = x^2+x+5 = x^2+x$
  - $(x+2)(x^2+1) = x^3+2x^2+x+2 = 2x^2+x+3$
- Elements of R can be represented as vectors in Z_p^n
  - $2x^2+x+3 = [2,1,3]$
  - Vector sum: [0,1,2] + [1,0,3] = [1,1,0]
  - Convolution: [0,1,2]*[1,0,1] = [2,1,3]

Secure compact knapsacks

- Use ring of modular polynomials instead of ring of integers
- $R = Z_p[X] / q(X)$
  - E.g. $q(X) = X^n - 1$ (or $q(X) = X^n+1$)
- $D = \{0,...,p^d\}^n$: degree n polynomials with small coefficients (d<1)
- [Micciancio02] Generalized compact knapsack is one-way, assuming worst case hardness of SIVP over cyclic lattices

Summary

- One-way function based on cyclic lattices
  - Secure in theory, based on worst-case assumption on cyclic lattices
  - Efficient and secure in practice, based on the use of compact knapsack
- Rest of this talk
  - Hash functions based on Ideal lattices
  - Connection to algebraic number theory
  - Open problems

Ideal lattices

- $q(X)$: monic polynomial in $Z[X]$ of deg. n
  - $R = Z[X] / q(X)$ is isomorphic to Z^n
  - h: $g(X)$ -> coefficients of $g(X) \bmod q(X)$
- Cyclic lattices: $q(X) = X^n - 1$
  - $h(X*g(X)) = rot(h(g(X))$
  - $h(S)$ is a cylic lattice iff S is an ideal of R
- Ideal lattices
  - $q(X)$ arbitrary monic polynomial
  - $h(S)$ where S is an ideal of $Z[X]/q(X)$

Ideal lattices and Cryptography

- Choice of $q(X)$
  - irreducible polynomial, e.g., $q(X) = X^n + 1$
  - $\| X^n \cdot g(X) \bmod q(X) \| \sim \|g(X)\|$
- Compact knapsacks are secure based on
  - worst-case hardness of approximating SVP in $q(X)$-Ideal lattices within factor ~n.
- Proof ingredients
  - Geometric ideas from lattices
  - Algebraic properties of polynomials

Proof idea

- Worst case problem:
  - Given ideal S of $Z[X]/f(X)$
  - find short vector in S
- Iterative proof
  - Given S and a vector $||v|| >> l_1(S)$
  - Find v' in S such that $||v'|| < ||v||/2$
- Most techniques borrowed from general lattices [Micciancio&Regev'04]

SVP and SIVP in ideal lattices

- Assume $q(X) = X^n + 1$, for $n = 2^k$
  - q(X) is irreducible
- Let S be an ideal of $Z[X] / q(X)$
- For any nonzero g(X)
  - $||X^i \cdot g(X) \bmod q(X)|| = ||g||$
  - $X^i \cdot g(X) \bmod q(X)$ (i=0,...,n-1) are linearly independent
- $l_1(S) = l_n(S)$ and $SVP_g <--> SIVP_g$

Complexity of Ideal lattices

- New area, nothing is known
  - Are SVP and SIVP still NP-hard?
- Best known polynomial time algorithm achieve almost exponential approximation factor
- LLL is geometric: cannot not see algebraic structure
- It is reasonable to conjecture that SVP, SIVP are hard to approximate within polynomial factors (in the worst case)

Algebraic Numbers

- Q: Rationals, c: complex number
- c is algebraic iff there is a (monic) polynomial q in Q[X] such that q(c)=0
- Minimal polynomial of c:
  - Lowest degree q(X) such that q(c)=0
  - g(c)=0 iff q(X) | g(X)
  - Unique
- Two numbers are conjugates ($c_1 \sim c_2$) if they have the same minimal polynomial

Number fields

- $Q(c)$: smallest subfield of C containing both Q and c.
  - $Q(2^{1/2}) = \{ a+2^{1/2}b: a,b \text{ in } Q\}$
- If q is the minimal polynomial of c then
  - $Q[X] / q(X) \sim Q(c)$
  - Isomorphism: $[g(X)] \rightarrow g(c)$
- If c_1 and c_2 are conjugates then
  - $Q(c_1) \sim Q(c_2)$
  - Isomorphism: $c_1 \rightarrow c_2$

Algebraic integers

- c is an algebraic integer if $q(c)=0$ for some monic $q(X)$ in $Z[X]$
- $Z[c]$: smallest subring of C that contains both Z and c
- c is an algebraic integer iff
  - $Z[c] \sim Z^n$
- Can think of $Z[c]$ as abstract lattice with basis $\{1,c,c^2,...,c^{n-1}\}$

Smallest Conjugates Problem

- Input:
  - Algebraic integer c
  - Ideal S of the integers Z[c] of Q(c)
- Goal:
  - Find element v in S such that max {|w|: v~w} is as small as possible
- How is c specified?
  - E.g., minimal polynomial of c
  - Solution is independent of which root is used

Ideal lattices and small conjugates

- Let $q(X)=X^n + 1$
- S: Ideal lattice in Z[X]/q(X)
  - Goal: Find g(X) in S such that ||g|| is small.
- $S(w_{2n})$ ideal of $Z(w_{2n})$ where $q(w_{2n})=0$
  - Find $g(w_{2n})$ in $S(w_{2n})$ such that max. conjugate of $g(w_{2n})$ is small
- Theorem:
  - $||g||/n^{1/2} < \text{Max.Conj.}(g(w_{2n})) < n^{1/2}||g||$

$IdealSVP_{ng}$ -->$Small\ Conjugates_{g}$

- Given Ideal S of Z[X] / q(X)
  - Let f(X) mod q(X) shortest vector in S
- Consider ideal $S(w_{2n})$ of $Z(w_{2n})$
  - Max.Conj.($f(w_{2n})$) < $n^{1/2}||f||$
  - Find $g(w_{2n})$ with Max.Conj.($g(w_{2n})$) < g $n^{1/2}||f||$
- Output g(X)
  - ||g(X)|| < $n^{1/2}$ Max.Conj.($g(w_{2n})$) < g n ||g||

$SmallConjugate_{ng}$ -->$IdealSVP_{g}$

- Given Ideal $S(w_{2n})$ of $Z(w_{2n})$
  - Let $g(w_{2n})$ be smallest conjugate solution
- Consider ideal lattice S mod q(X)
  - $||g|| < n^{1/2}\, MaxConj(g(w_{2n}))$
  - Find f(X) with $||f|| < g\ n^{1/2}\, MaxConj(g(w_{2n}))$
- Output $f(w_{2n})$
  - $||f(w_{2n})\ || < n^{1/2}\, ||g|| < g\ n\ ||g(w_{2n})||$

Open Problems (Complexity)

- Is SVP over ideal lattices NP-hard?
  - Special case: is CyclicSVP NP-hard
  - In the exact case?
  - Approximate Version
- Similar question in coding theory
  - Minimum distance of cyclic codes, NP-hard?
  - Guruswami&Vardy: ML RS-codes is NP-hard

Open Problems (Complexity)

- Is there a reduction from general lattices to cyclic or ideal lattices?
  - Worst-case to worst-case reduction is enough for crypto applications
  - Paz&Schnorr: reduction from arbitrary lattices to lattices with cyclic factor group
- Goldreich,Micciancio,Safra&Seifert 99
  - SVP reduces to CVP
  - Is the same true for cyclic or ideal lattices?

Open Problems (Algorithms)

- Performance of LLL on cyclic lattices
  - LLL does not “see” algebraic structure: cyclic structure is not preserved under isometries
- No reason to believe LLL should do any better on cyclic lattices
- Questions:
  - Find cyclic (or ideal) lattices where LLL achieves worst-case approximation factor
  - Invent algebraic LLL?

Open Problems (Cryptograpy)

- So far:
  - One-way and collision resistant hash functions based on cyclic/ideal lattices
  - Imply also efficient commitment schemes
- Question: Use ideal lattices for efficient
  - Pseudo-random generators
  - Pseudo-random functions
  - Digital signatures

Open Problems (Cryptography)

- Lattice based Public key encryption
  - NTRU: lattice based cryptosystem based on quasi-cyclic lattices
- Code based Public key encryption
  - Quasi-cyclic codes improve efficiency of cryptosystems based on codes
- Question:
  - Can any of these constructions be proved secure based on worst-case hardness of quasi-cyclic lattices/codes?

Open Problem (Algebraic Number Theory)

- Algebraic number theory
  - Can tools from algebra be used to efficiently solve problems in ideal lattices
  - Can lattice reduction + average case problems be used to solve problems in algebraic number theory?
- Worst-case/average-case connection
  - Can cryptography be based directly on worst-case hardness of problems from algebraic number theory

Open Problems (Quantum)

- Recent results on quantum algorithms for algebraic number theory problems
  - Compute unit and class groups of number fields [Hallgren05, Schmidt&Vollmer05]
- Find efficient quantum algorithms for
  - Solving the smallest conjugate problem
  - Solving SVP on Ideal lattices
- Efficient version of Regev's quantum-SVP cryptosystem based on ideal lattices

References

- One-way function based on cyclic lattices
  - Micciancio FOCS'02
  - Computational Complexity, to appear
- Hash functions and generalization to ideals lattices
  - Peikert&Rosen TCC'06
  - Lyubashevsky&Micciancio ICALP'06
- Very efficient instantiation based on FFT
  - [LMPR] 2nd NIST hash function workshop '06.