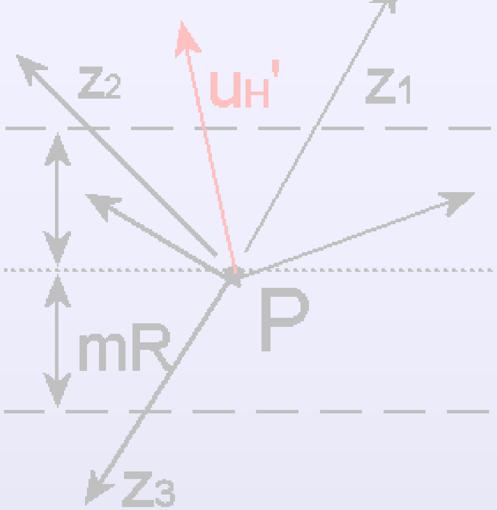
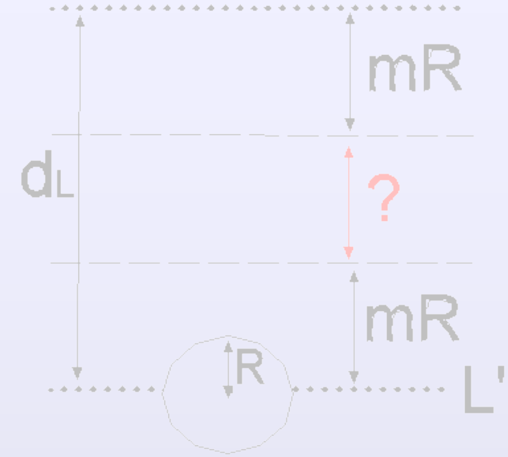
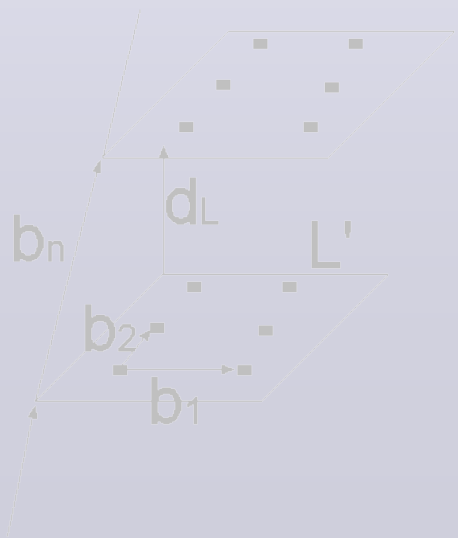


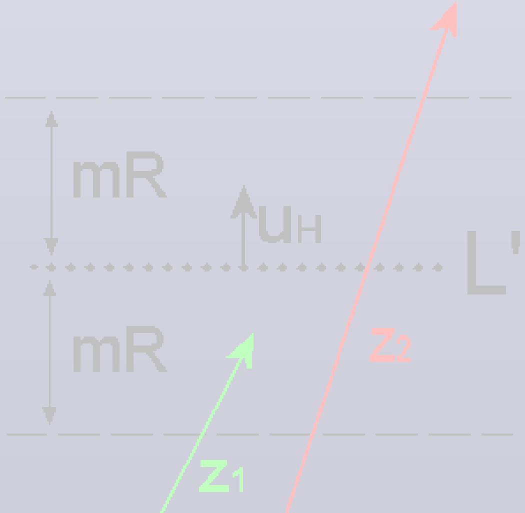


Gitterbasierte Kryptosysteme

(Ajtai-Dwork, Regev)

Sebastian Pape





Überblick

- Motivation
- Gitter
  - SVP, uSVP, Gitterbasisreduktion
- Kryptosysteme
  - Ajtai-Dwork
  - Regev (2003), Regev (2005)
- Zusammenfassung

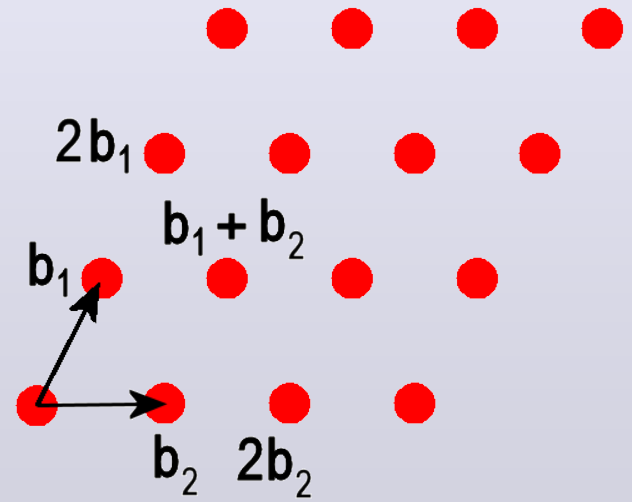
Motivation

- “Standard”-Kryptographie
  - z.B. Faktorisieren, diskrete Logarithmen
  - durch Quantencomputer lösbar

- Gitter-basierte Kryptographie
  - z.T. Worst-Case-Härte (AD, Regev $\leftrightarrow$ NTRU)
  - bis jetzt nicht durch Quantencomputer lösbar
  - keine besseren Quantenalgorithmen bekannt

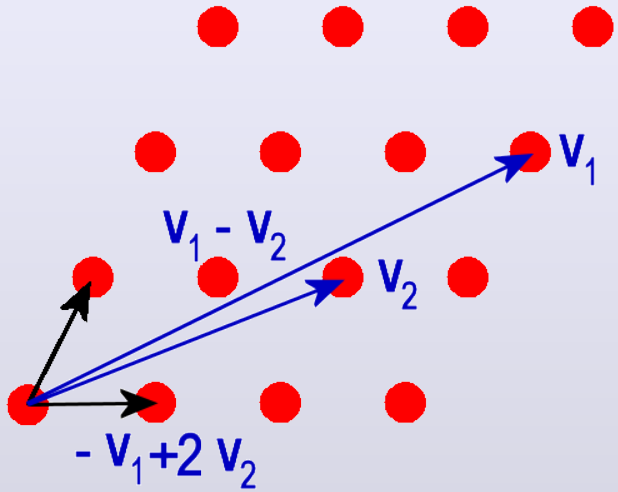
Gitter

- Basis: $b_1, \ldots, b_n$ in Υ^n
- Gitter: $\Sigma\lambda_i b_i$ für λ_i in ∞
- Was ist der kürzeste Vektor?



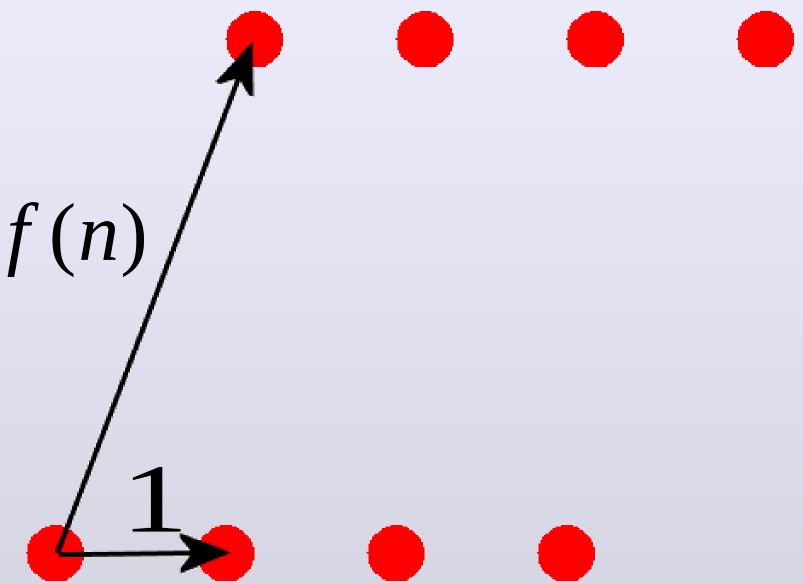
Shortest Vector Problem

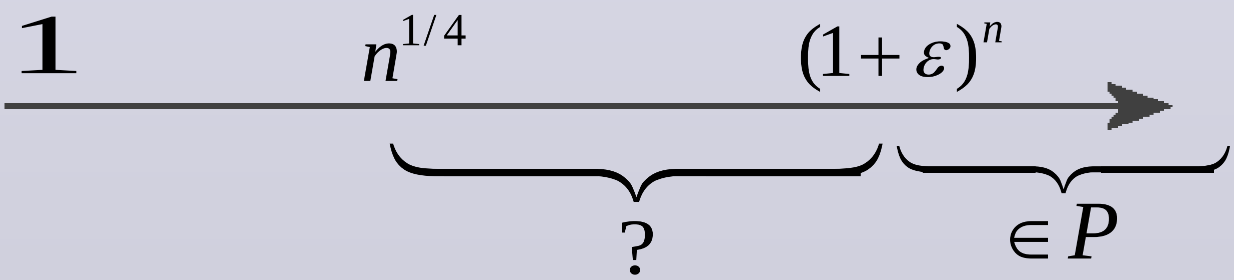
- Doch nicht so leicht?
- exp. Approx. polyn. Laufzeit
  - LLL, Schnorr
- exakte Ber. exp. Laufzeit
- Approx. auf $\sqrt{2}$ NP-Hart (rand. Reduktion)
- determ. Redukt. offen



unique Shortest Vector Problem

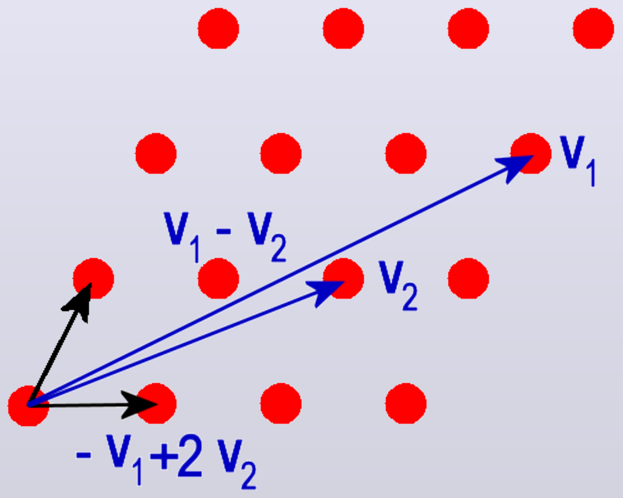
- kürzester Vektor ist bis auf Faktor f(n) eindeutig
- $(1+\varepsilon)^n$-uSVP-Alg.
- $n^{1/4}$-uSVP nicht NP-hart





Gitterbasisreduktion

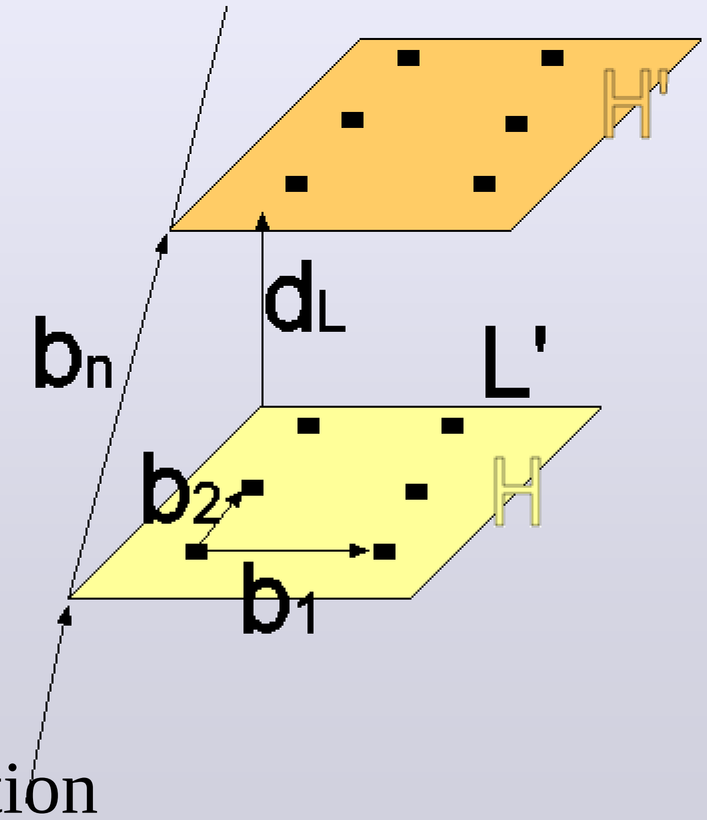
- gesucht: Basis aus kurzen, orthogonalen Vektoren
- verschiedene Definitionen von reduzierten Basen



(d,M)-Gitter

- Gitter L'
  - Basis B mit Länge $\leq$ M
  - (n-1) dimensional
- Hyperebene H
  - L' $\in$ H
  - Abstand zu H': $d_L > d$
- eindeutig wenn d > M

  $\rightarrow L^{(d,M)}$
- Hidden Hyperplane Assumption



Kryptosysteme

- Ajtai-Dwork (1996)
  - Goldreich, Goldwasser, Halevi (1997)
  - Ngyuen, Stern (1998, 1999)
- Oded Regev (2003)
- Oded Regev (2005)

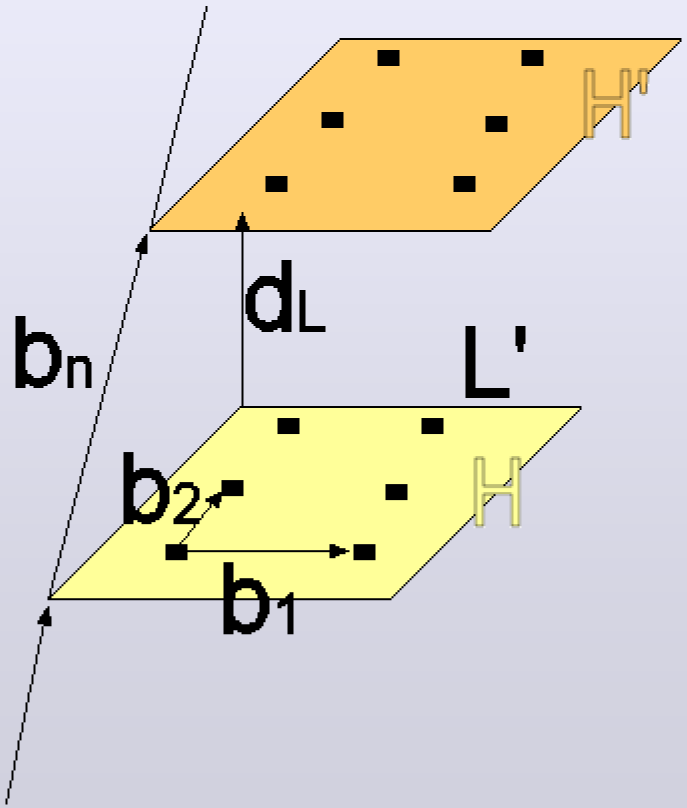
Kryptosysteme II

- Gemeinsamkeiten
  - bitweise Verschlüsselung

  $\Rightarrow$ probabilistische Verschlüsselung
  - Sicherheit beruht auf Worst-Case-Problemen
    - brechen des KS → Lösung für beliebige Instanz des Problems
  - benutzen “Rauschen”
- Ajtai-Dwork, Regev (2003)
  - nicht sicher gegen CCA
    - folgt fast direkt aus Reduktionsbeweisen

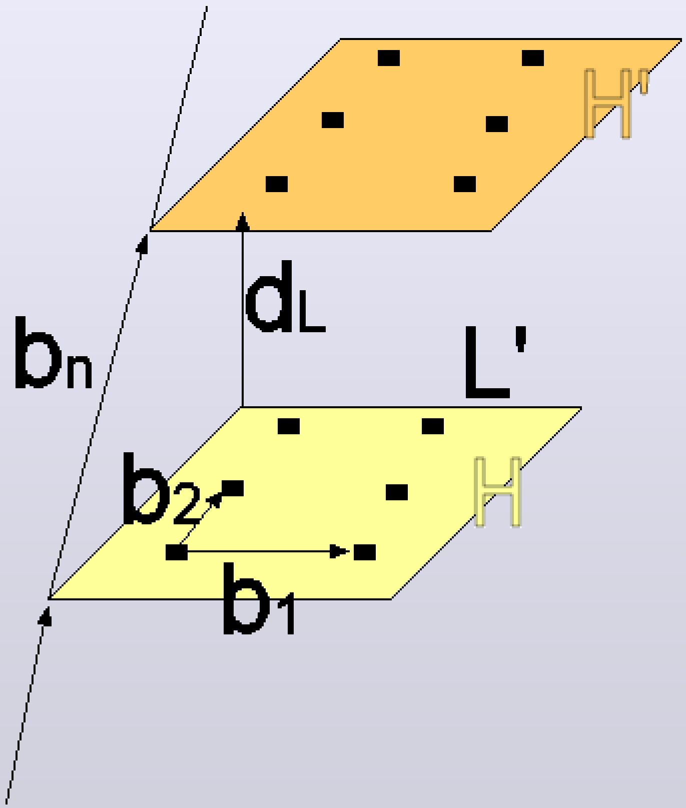
Ajtai-Dwork – Gitter generieren

- Generieren
  - zufällige Basis für L’ mit $||b_i|| \leq M$
  - wähle $d \geq n^5 M$
  - wähle b_n mit Abstand $d \leq d_L \leq 2d$ von H



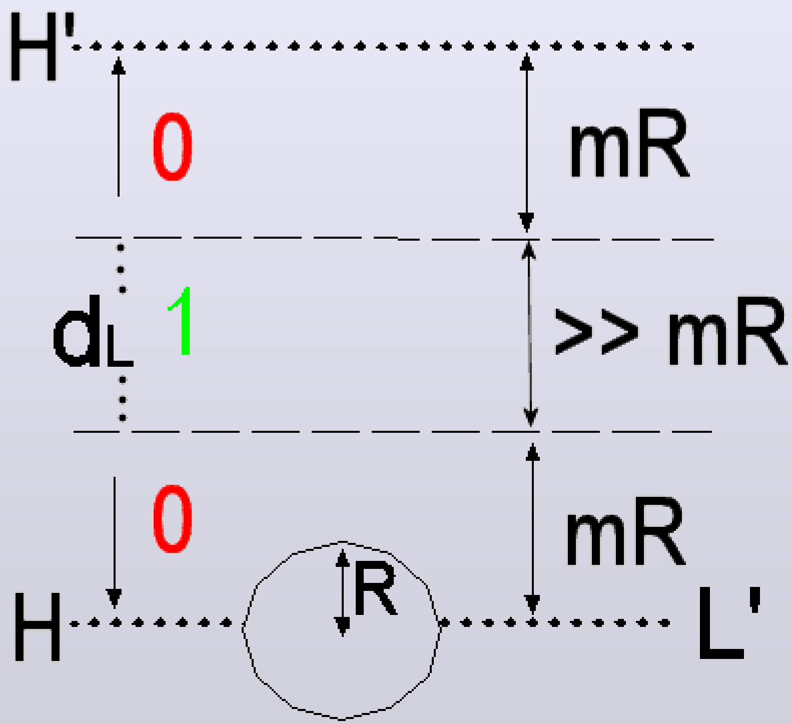
Ajtai-Dwork – Schlüssel

- Privater Schlüssel
  - beliebige Basis von $L' = L^{(d,M)}$ oder H
- Öffentlicher Schlüssel
  - zufällige Basis B` für L
  - M



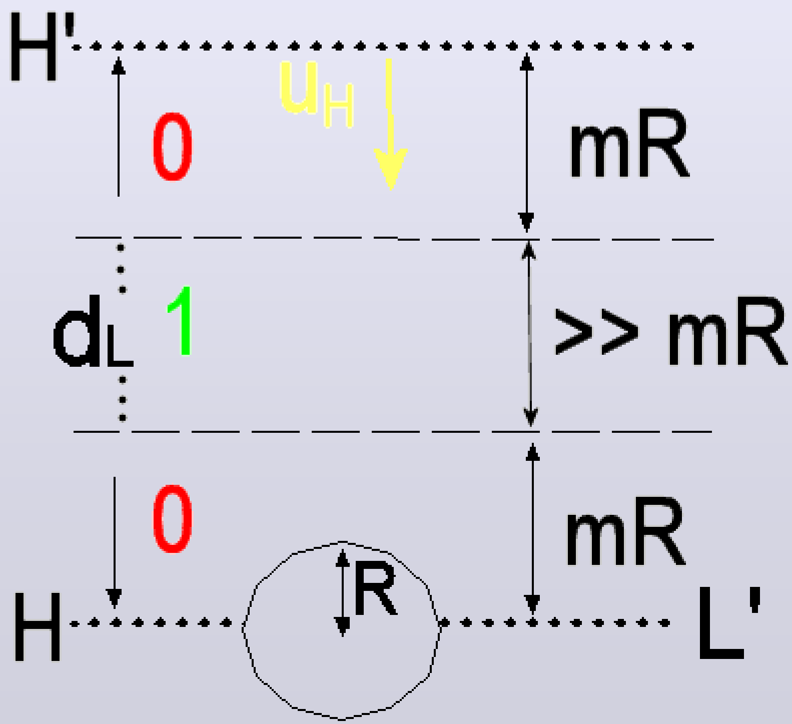
Ajtai-Dwork – Verschlüsselung

- $1 \rightarrow u$
  - zufälliger Punkt u
- $0 \rightarrow v + w$
  - zufälliger Punkt v in L
  - Störung $w = pert(n^3M,m)$
- Störung pert(R,m)
  - $m \geq 4n$ zufällige Vektoren aus der Kugel mit Radius R



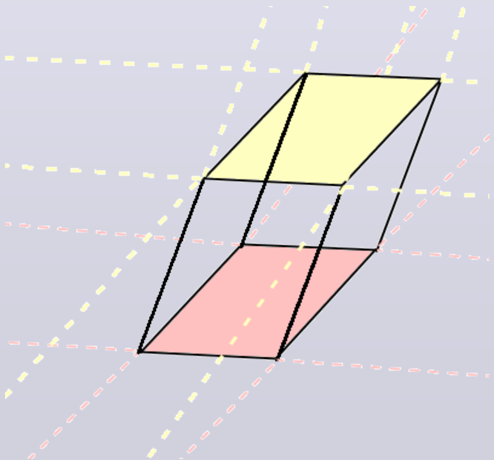
Ajtai-Dwork – Entschlüsselung

- u_H zu H orthogonaler Einheitsvektor.
- frac $\langle u_H, z \rangle / d_L$
- 0: im Bereich mR/d_L von 0 oder 1
- 1: sonst



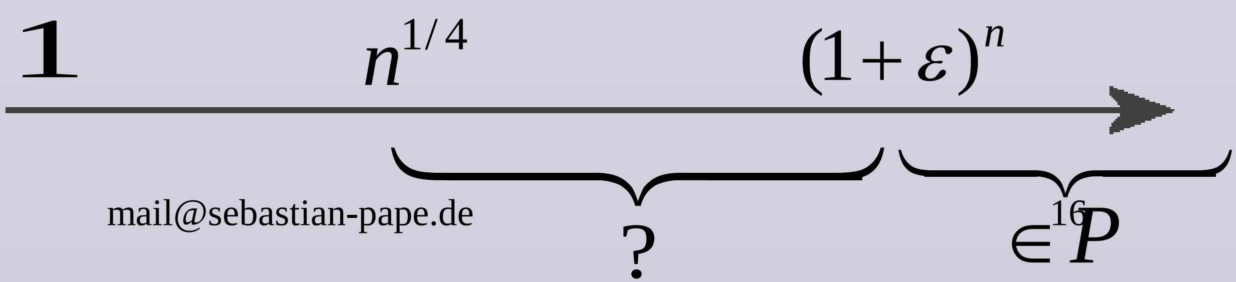
Ajtai-Dwork Hauptvariante (Skizze)

- privater Schlüssel ist zufälliger Vektor u_H
- öffentlicher Schlüssel sind “verrauschte” Gitterpunkte der durch u_H erzeugten Hyperebenen, Teil der Gitterpunkte spannt Parallelepiped PE auf
- V0: Wahl zufälliger Punkte des PK
  Summe und Reduktion in PE
- V1: zufälliger Punkt in PE
- E: $\langle z,u_H \rangle$ fast ganzzahlig $\rightarrow 0$



Ajtai-Dwork Zusammenfassung

- Originalsystem von Ajtai und Dwork
  - Entschlüsselungsfehler
  - $O(n^8)$-uSVP
- Goldreich, Goldwasser, Halevi
  - beseitigen Fehler
  - $O(n^7)$-uSVP
- Angriff von Nguyen und Stern
  - mit $n^{0,5-\varepsilon}$-SVP-Approx.
  - Parameter fuer AD zu schlecht fuer realistischen Einsatz
  - n=32, PK~20MB,1b→768B



Regev (2003) – Schlüssel

- Generieren
  - grosse, ganze Zahl N
- Privater Schlüssel
  - $h \in [\sqrt{N}, 2\sqrt{N}) \cap \mathbb{N}$
- Öffentlicher Schlüssel
  - m = O(log N) Zahlen a_i aus {0, 1, …, N-1} nahe bei ganzzahligen Vielfachen von N / h
  - Index i_0, so dass a_{i0} nahe bei einem ungeraden Vielfachen von N / h
  - h muss N nicht teilen

Regev (2003) – Verschlüsselung

- Öffentlicher Schlüssel
  - $m = O(\log N)$ Zahlen a_i aus $\{0, 1, \ldots, N-1\}$ nahe bei ganzzahligen Vielfachen von N / h
  - Index i_0, so dass a_{i0} nahe bei einem ungeraden Vielfachen von N / h
  - h muss N nicht teilen
- Verschlüsselung
  - 0: Summe aus einer zufälligen Teilmenge $\{a_1, \ldots, a_m\}$ modulo N
  - 1: wie Verschlüsselung von 0, aber $\lfloor a_{i0} / 2 \rfloor$ addieren

Regev (2003) – Entschlüsselung

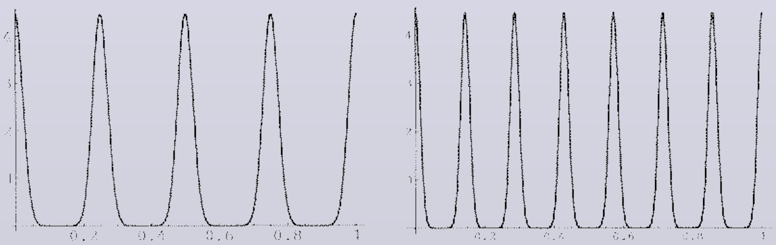
- Verschlüsselung
  - 0: Summe aus einer zufälligen Teilmenge $\{a_1, \ldots, a_m\}$ modulo N
  - 1: wie Verschlüsselung von 0, aber $\lfloor a_{i0} / 2 \rfloor$ addieren
- Entschlüsselung
  - betrachte Rest von z / (N/h)
  - 0: klein
  - 1: sonst
- Grund
  - a_i nahe bei Vielf. N/h
  - also auch alle Summen
  - $\lfloor a_{i0} / 2 \rfloor$ weit entfernt

Regev (2003) – Hash

- m=O(log N) Zufallszahlen aus {0, 1, …, N-1}
- Hashfunktion: $f(b) = \sum_{i=1}^{m} b_i a_i \bmod N \text{ mit } b \in \{0,1\}^m$
- Kollision: $\sum_{i=1}^{m} b_i a_i \equiv 0 \bmod N \text{ mit } b \in \{-1,0,1\}^m$

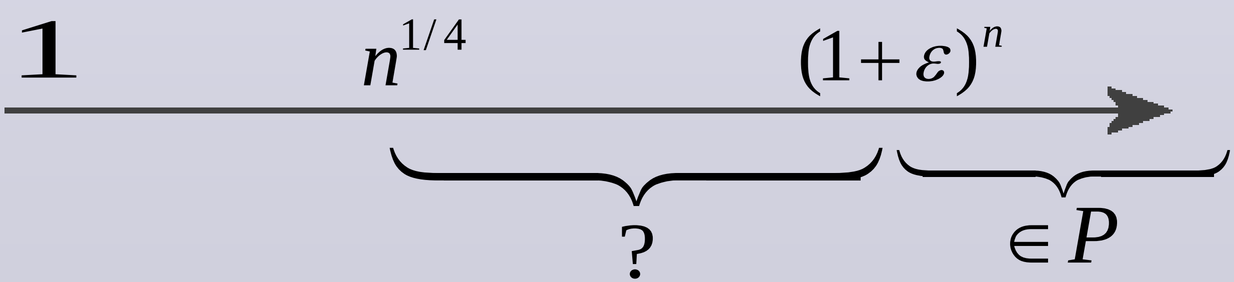
Regev (2003) – Sicherheit (Skizze)

- Unterscheiden zwischen 0 und 1 bzw. finden eines Kollisionsvektors
- $\Rightarrow$ Unterscheiden zwischen Gleichverteilung U und einer Verteilung T_h um ganzzahlige Vielfache von 1/h für ein unbekanntes h
- $\Rightarrow O(n^{1,5})$-uSVP



Regev (2003) Zusammenfassung

- Gitter werden nur implizit benutzt
- Sicherheit beruht auf
  - $O(n^{1,5})$-uSVP
  - AD: ($O(n^7)$-uSVP)
- nicht nur Public-Key-System, sondern auch Hash-Funktion



Regev (2005) – Schlüssel

- Generieren
  - m, p, Wahrscheinlichkeitsverteilung χ auf $\mathbb{Z}_p$
- Privater Schlüssel
  - $s \in \mathbb{Z}_p^n$
- Vorbereitung
  - $a_1, \ldots, a_m \in \mathbb{Z}_p^n$
  - $e_1, \ldots, e_m \in \mathbb{Z}_p$ nach χ
- Öffentlicher Schlüssel:
  - (a_i, b_i) mit
  - $b_i = \langle a_i, s \rangle + e_i$

Regev (2005) – Verschlüsselung

- Vorbereitung
  - $a_1,\ldots,a_m \in \mathbb{Z}_p^n$
  - $e_1,\ldots,e_m \in \mathbb{Z}_p$ nach χ
- Öffentlicher Schlüssel:
  - (a_i,b_i) mit
  - $b_i = \langle a_i, s\rangle + e_i$
- Verschlüsselung
  - zufällige Teilmenge S aus [m]
  - 0: $(\sum_{i\in S} a_i, \sum_{i\in S} b_i)$
  - 1: $(\sum_{i\in S} a_i, \left\lfloor \frac{p}{2} \right\rfloor + \sum_{i\in S} b_i)$

Regev (2005) – Entschlüsselung

- Verschlüsselung
  - zufällige Teilmenge S aus [m]
  - 0: $(\sum_{i \in S} a_i, \sum_{i \in S} b_i)$
  - 1: $(\sum_{i \in S} a_i, \left\lfloor \frac{p}{2} \right\rfloor + \sum_{i \in S} b_i)$

- Entschlüsselung von (a,b):
  - 0: b - <a,s> ist näher an 0 als an $\lfloor p/2 \rfloor$
  - 1: sonst

Regev (2005) – Entschlüsselung II

- Entschlüsselung:
  - 0: b - <a,s> ist näher an 0 als an $\lfloor p/2 \rfloor$
  - 1: sonst

$$b_i = (e_i + <a_i, s>)$$

$$\sum_{i \in S} e_i \leq \left\lfloor \frac{p}{2} \right\rfloor / 2 \text{ wegen } \chi$$

$$b - <a, s> =$$

$$\sum_{i \in S} b_i - \sum_{i \in S} <a_i, s> =$$

$$\sum_{i \in S} (e_i + <a_i, s>) - \sum_{i \in S} <a_i, s> =$$

$$\sum_{i \in S} e_i$$

Regev (2005) - Zusammenfassung

- Sicherheit beruht auf Worst-Case Quantum-Härte von SVP und SIVP ($O(n^{1,5})$-Approx.)
  - Reduktion benutzt QC, Kryptosystem nicht
  - Reduktion auch klassisch?
- effizienter
  - Öffentlicher Schlüssel: $O(n^4) \rightarrow O(n^2)$
  - Nachrichten: $O(n^2) \rightarrow O(n)$

Zusammenfassung

- Kryptosysteme noch zu ineffizient
- bis jetzt keine Quantenalgorithmen, die klassische bei Gitterproblemen übertreffen
- Quantencomputer unter bestimmten Annahmen bis $n^{2,5}$-uSVP
- Evtl. zukunftsträchtig (Worst-Case!)
  - Effizienz $\leftrightarrow$ stärkere Angriffe