Quantum Attack on LWE/LPN

(A strategy for a)

September 15, 2016

Alan Szepieniec

KU Leuven, ESAT/COSIC

Introduction

- LWE/LPN boils down to *noisy linear algebra* : $M \times \mathbf{v} + \mathbf{e}$
  - Gaussian elimination: $\mathbf{e}$ blows up
  - Least-Squares: undefined — $\mathbb{F}_q$
- ... but quantum computers are notoriously robust against noise ...
  - quantum-error correcting codes
  - quantum function learning (with superposition oracle queries)
  - quantum image recognition
- so maybe also robust against LWE/LPN noise

LWE/LPN

target space

secret space

Given $A \in \mathbb{F}_q^{m \times n}$ and $\hat{\mathbf{b}} \in \mathbb{F}_q^m$, find $\mathbf{s} \in \mathbb{F}_q^n$ such that $\|A\mathbf{s} - \hat{\mathbf{b}}\|_2 < \ell_\xi$

$\Leftrightarrow$ find $\boldsymbol{\varepsilon} \sim \xi^m$ s.t. $A\mathbf{s} = \hat{\mathbf{b}} - \boldsymbol{\varepsilon} = \mathbf{b} \longleftarrow$ target

$\Leftrightarrow$ find $\mathbf{s} \in \mathbb{F}_q^n$ from

secret

$$\begin{cases} A_{1,1}s_1 + A_{1,2}s_2 + \ldots + A_{1,n}s_n \approx b_1 \\ A_{2,1}s_1 + A_{2,2}s_2 + \ldots + A_{2,n}s_n \approx b_2 \\ \vdots \\ A_{m,1}s_1 + A_{m,2}s_2 + \ldots + A_{m,n}s_n \approx b_m \end{cases}$$

where $\approx$ holds up to an error $\varepsilon \sim \xi$.

$\rightarrow$ get to ask more equations!

Key takeaways:

1. ξ has little entropy
2. $m > n$ (overdetermined)

Phase One

1. Sample $|\mathbf{e}\rangle = \bigotimes_{j=1}^{m} \mathcal{S}_\xi(|r_j\rangle)$.
2. Compute $|\hat{\mathbf{b}} - \mathbf{e}\rangle$
3. Set $|R\rangle$ to *superposition of all row-dropping matrices* $R \in \{0,1\}^{n\times m}$ such that RA is invertible.
4. Compute $|RA\rangle$, $|(RA)^{-1}\rangle$ and $|R(\hat{\mathbf{b}} - \mathbf{e})\rangle$
5. Compute $|\mathbf{c}\rangle = |(RA)^{-1}R(\hat{\mathbf{b}} - \mathbf{e})\rangle$.
6. Measure $|\mathbf{c}\rangle$.

   Intuition.

- $|\mathbf{e}\rangle$ corrects $\varepsilon \implies$ *all* R lead to $\mathbf{s}$

  $\uparrow$ negl. amplitude $\uparrow$ exponentially many paths
- $|\mathbf{e}\rangle$ no correction $\implies$ *some* R lead to $\mathbf{s}$; most to *random points* in $\mathbb{F}_q^n$

Phase One

1. Sample $|\mathbf{e}\rangle = \bigotimes_{j=1}^{m} \mathcal{S}_\xi(|r_j\rangle)$.
2. Compute $|\hat{\mathbf{b}} - \mathbf{e}\rangle$
3. Set $|R\rangle$ to *superposition of all row-dropping matrices* $R \in \{0,1\}^{n \times m}$ such that RA is invertible.
4. Compute $|RA\rangle$, $|(RA)^{-1}\rangle$ and $|R(\hat{\mathbf{b}} - \mathbf{e})\rangle$
5. Compute $|\mathbf{c}\rangle = |(RA)^{-1}R(\hat{\mathbf{b}} - \mathbf{e})\rangle$.
6. Measure $|\mathbf{c}\rangle$.

Analysis.

- ... (lots of calculus) ...
- $\mathsf{E}[\langle \mathbf{s}|\mathbf{c}\rangle] = \bar{\eta}^n$ where $\bar{\eta} = \sum_{\varepsilon \in \mathbb{F}_q} \xi(\varepsilon)^{3/2}$

$\longrightarrow$ uses small entropy of ξ $\checkmark$

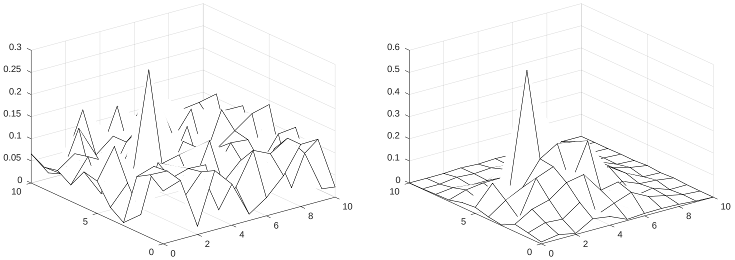
$\longrightarrow$ independent of m $\times$

Phase Two

1. Start with $|\mathbf{c}\rangle = |(RA)^{-1}R(\hat{\mathbf{b}} - \mathbf{e})\rangle$
2. Use A to map to target space: $|\boldsymbol{b}\rangle = |A\mathbf{c}\rangle$

$\rightarrow$ $\mathrm{E}[\langle A\mathbf{s}|\boldsymbol{b}\rangle] = \bar{\eta}^n$

- the rest of the amplitude of $|\boldsymbol{b}\rangle$ is distributed randomly across col$A$
- strategy: send back to cloud around $\hat{\mathbf{b}}$



- amplitude amplification ?
- quantum walk ?

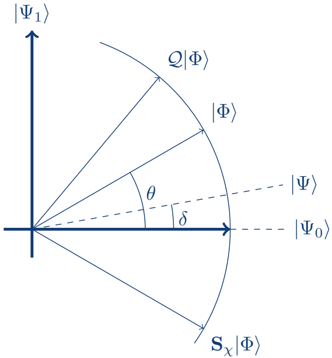
Phase Two

1. Start with $|\mathbf{c}\rangle = |(RA)^{-1}R(\hat{\mathbf{b}} - \mathbf{e})\rangle$
2. Use A to map to target space: $|\boldsymbol{b}\rangle = |A\mathbf{c}\rangle$

- send $|\boldsymbol{b}\rangle$ to cloud around $\hat{\mathbf{b}}$

amplitude amplification

$$\mathbf{S}_\chi : |\mathbf{x}\rangle \mapsto \begin{cases} -|\mathbf{x}\rangle & \text{if} \quad \|\mathbf{x} - \hat{\mathbf{b}}\| < \alpha \\ |\mathbf{x}\rangle & \text{else.} \end{cases}$$



$$|\Psi_1\rangle \propto \sum_{\{\mathbf{x} \mid \|\mathbf{x}-\hat{\mathbf{b}}\|<\alpha\}} |\mathbf{x}\rangle$$

$$|\Psi_0\rangle \propto \sum_{\{\mathbf{x} \mid \|\mathbf{x}-\hat{\mathbf{b}}\|\geq\alpha\}} |\mathbf{x}\rangle$$

Phase Two

1. Start with $|\mathbf{c}\rangle = |(RA)^{-1}R(\hat{\mathbf{b}} - \mathbf{e})\rangle$
2. Use A to map to target space: $|\boldsymbol{b}\rangle = |A\mathbf{c}\rangle$

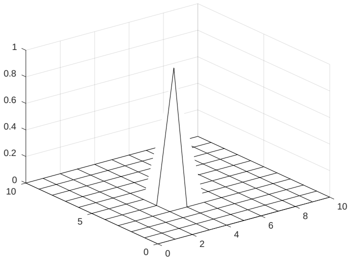
- send $|\boldsymbol{b}\rangle$ to cloud around $\hat{\mathbf{b}}$

  amplitude amplification

  $$\mathbf{S}_\chi : |\mathbf{x}\rangle \mapsto \begin{cases} -|\mathbf{x}\rangle & \text{if} \quad \|\mathbf{x} - \hat{\mathbf{b}}\| < \alpha \\ |\mathbf{x}\rangle & \text{else.} \end{cases}$$

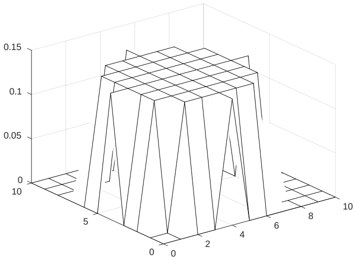
$|\Psi_1\rangle =$

α too small



exponential running time

α too large



negligible success probability

Phase Two

1. Start with $|\mathbf{c}\rangle = |(RA)^{-1}R(\hat{\mathbf{b}} - \mathbf{e})\rangle$
2. Use A to map to target space: $|\boldsymbol{b}\rangle = |A\mathbf{c}\rangle$

- send $|\boldsymbol{b}\rangle$ to cloud around $\hat{\mathbf{b}}$

quantum walk

- graph $G = (V, E)$ with $V = \{0, \ldots, q-1\}^m$ and $E(\mathbf{v}_1, \mathbf{v}_2) = 1 \Leftrightarrow \|\mathbf{v}_1 - \mathbf{v}_2\|_1 = 1$
- transition function follows ξ^m:
- maps $\mathbf{v} \mapsto \mathbf{v}' \in N(\mathbf{v})$ with probability

$$\frac{\xi^m(\mathbf{v}' - \hat{\mathbf{b}})}{\sum_{\mathbf{x} \in N(\mathbf{v}) \cup \{\mathbf{v}\}} \xi^m(\mathbf{x} - \hat{\mathbf{b}})}$$

- and $\mathbf{v} \mapsto \mathbf{v}$ with probability

$$\frac{\xi^m(\mathbf{v} - \hat{\mathbf{b}})}{\sum_{\mathbf{x} \in N(\mathbf{v}) \cup \{\mathbf{v}\}} \xi^m(\mathbf{x} - \hat{\mathbf{b}})}$$

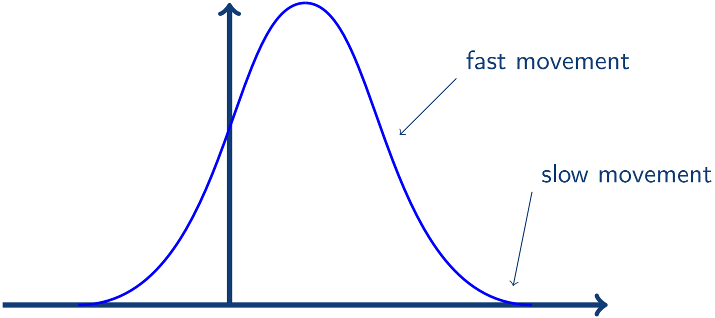
Phase Two

1. Start with $|\mathbf{c}\rangle = |(RA)^{-1}R(\hat{\mathbf{b}} - \mathbf{e})\rangle$
2. Use A to map to target space: $|\boldsymbol{b}\rangle = |A\mathbf{c}\rangle$

- send $|\boldsymbol{b}\rangle$ to cloud around $\hat{\mathbf{b}}$

quantum walk

- graph $G = (V, E)$ with $V = \{0, \ldots, q-1\}^m$ and $E(\mathbf{v}_1, \mathbf{v}_2) = 1 \Leftrightarrow \|\mathbf{v}_1 - \mathbf{v}_2\|_1 = 1$
- transition function follows ξ^m



Phase Two

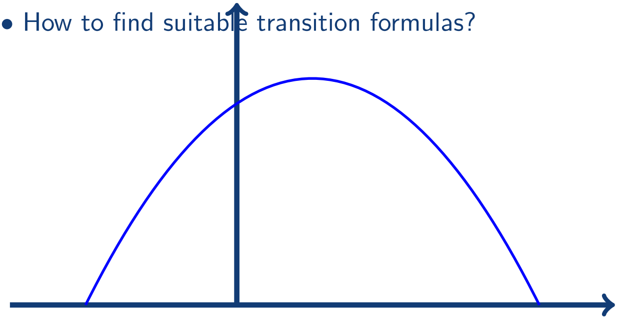
1. Start with $|\mathbf{c}\rangle = |(RA)^{-1}R(\hat{\mathbf{b}} - \mathbf{e})\rangle$
2. Use A to map to target space: $|\boldsymbol{b}\rangle = |A\mathbf{c}\rangle$

- send $|\boldsymbol{b}\rangle$ to cloud around $\hat{\mathbf{b}}$

quantum walk

- graph $G = (V, E)$ with $V = \{0, \ldots, q-1\}^m$ and $E(\mathbf{v}_1, \mathbf{v}_2) = 1 \Leftrightarrow \|\mathbf{v}_1 - \mathbf{v}_2\|_1 = 1$
- transition function — something more convex

  - How to find suitable transition formulas?



Algorithm Outline

1. sample $\mathcal{S}_\xi$, get cloud $|\hat{\mathbf{b}} - \mathbf{e}\rangle$
    2. send to secret space, get $|\boldsymbol{c}\rangle$
    3. multiply with A, get $|\boldsymbol{b}\rangle$
    4. resample wrong amplitudes, densify cloud
5. repeat 2—4

intuition:

- every iteration a fraction of the wrong amplitude is sent to $|\mathbf{b}\rangle$ or $|\mathbf{s}\rangle$
- the amplitude associated with $|\mathbf{b}\rangle$ or $|\mathbf{s}\rangle$ never decreases

Last slide

- LWE: find $\mathbf{s}$ from A and $\hat{\mathbf{b}} = A\mathbf{s} + \mathbf{e}$ with $\mathbf{e} \sim \xi^m$
- phase 1
  - $|R\rangle$ — superposition of row-dropping matrices R such that RA is invertible
  - $|\mathbf{e}\rangle$ — sampled according to ξ^m
  - $|\mathbf{c}\rangle = |(RA)^{-1}R(\hat{\mathbf{b}} - \mathbf{e})\rangle$ contains $|\mathbf{s}\rangle$
  - $\mathrm{E}[\langle \mathbf{c}|\mathbf{s}\rangle] = \bar{\eta}^n$ with $\bar{\eta} = \sum_{\varepsilon \in \mathbb{F}_q} \xi(\varepsilon)^{3/2}$
- phase 2
  - use all of A to map $|\mathbf{c}\rangle$ back to $\mathbb{F}_q^m$: $|\boldsymbol{b}\rangle = |A\mathbf{c}\rangle$
  - $|\boldsymbol{b}\rangle$ has lots of amplitude "far" from $\hat{\mathbf{b}}$ — send it back!
  - use amplitude amplification or quantum walk
- repeat
- suggestions / questions / comments?
- `alan.szepieniec@esat.kuleuven.be`