The LWE Challenge

19th Workshop on
Elliptic Curve Cryptography

Rump Session

September 28, 2015

The LWE Problem

- $n, m, q \in \mathbb{N}$
- uniformly random matrix $\mathbf{A} \in \mathbb{Z}_{\mathbf{q}}^{\mathbf{m} \times \mathbf{n}}$
- uniformly random vector $\mathbf{s} \in \mathbb{Z}_{\mathbf{q}}^{\mathbf{n}}$
- error vector $\mathbf{e} \leftarrow \chi^{\mathbf{m}}$
- discrete Gaussian distribution χ on $\mathbb{Z}_q$

$$\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \in \mathbb{Z}_{\mathbf{q}}^{\mathbf{m}}$$

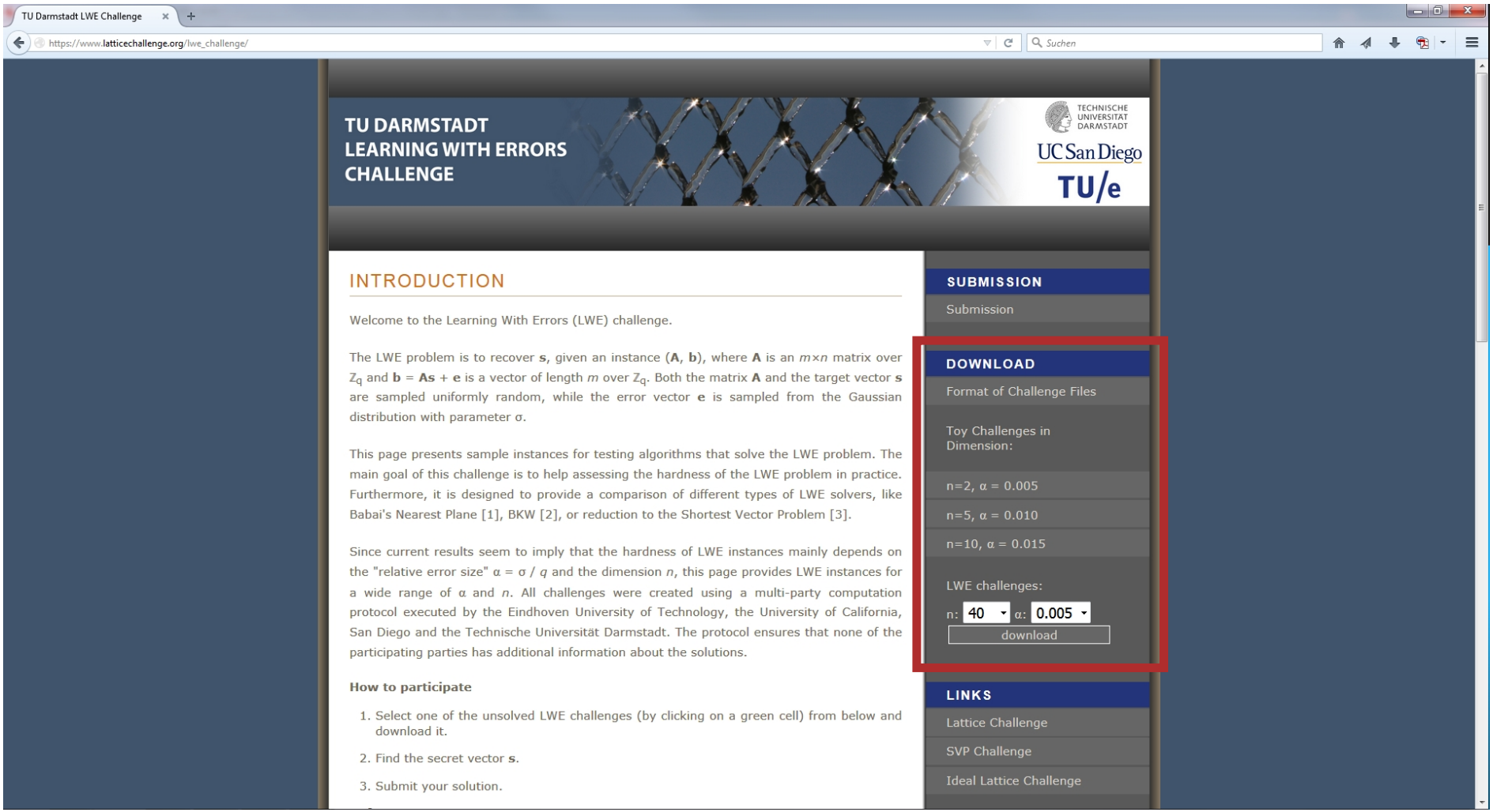
The LWE problem is to recover $\mathbf{s}$, given $\mathbf{A}$ and $\mathbf{b}$.

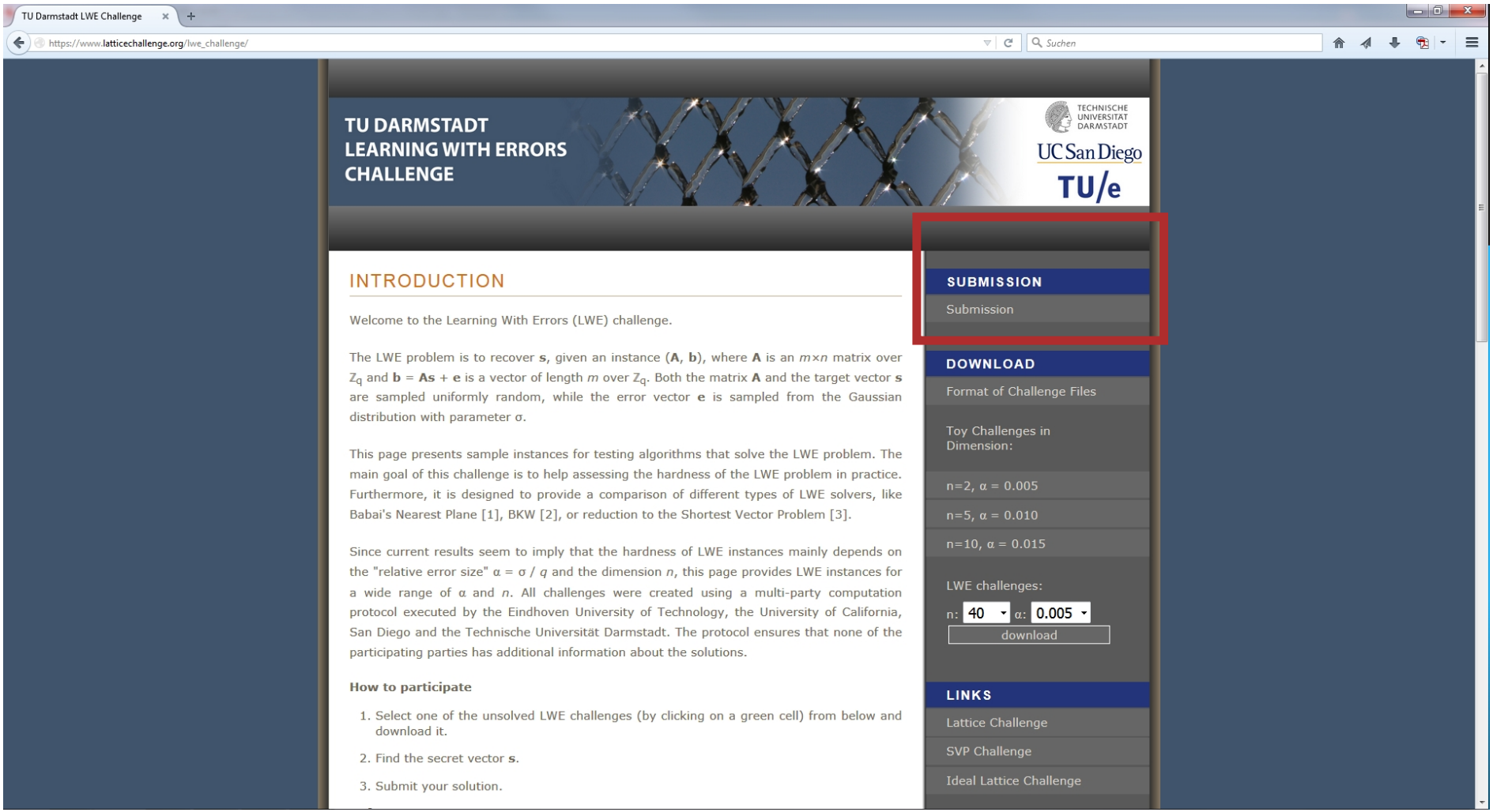
The LWE Problem

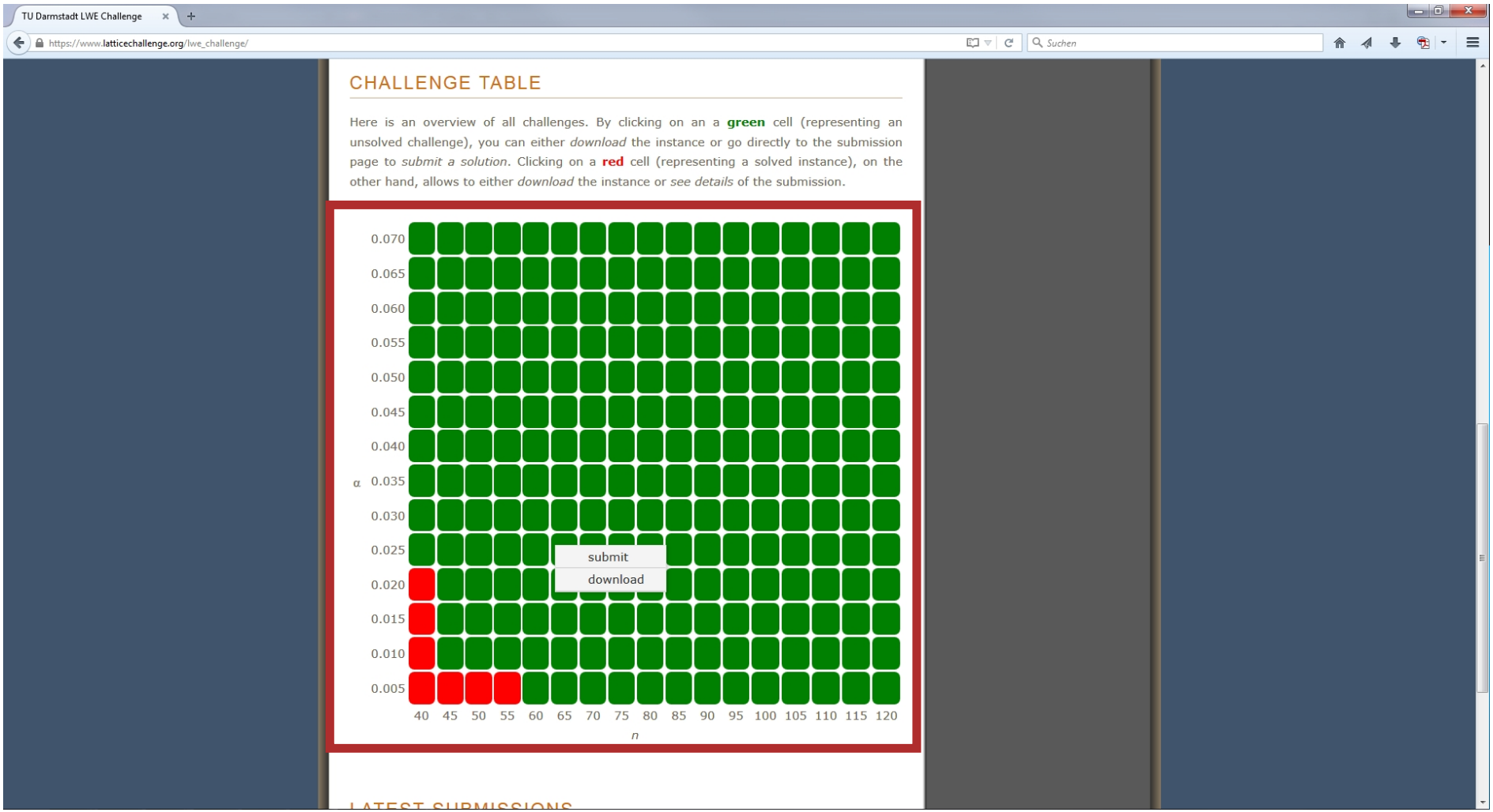
- $n, m, q \in \mathbb{N}$
- uniformly random matrix $\mathbf{A} \in \mathbb{Z}_{\mathbf{q}}^{\mathbf{m} \times \mathbf{n}}$
- uniformly random vector $\mathbf{s} \in \mathbb{Z}_{\mathbf{q}}^{\mathbf{n}}$
- error vector $\mathbf{e} \leftarrow \chi^{\mathbf{m}}$
- discrete Gaussian distribution χ on $\mathbb{Z}_q$

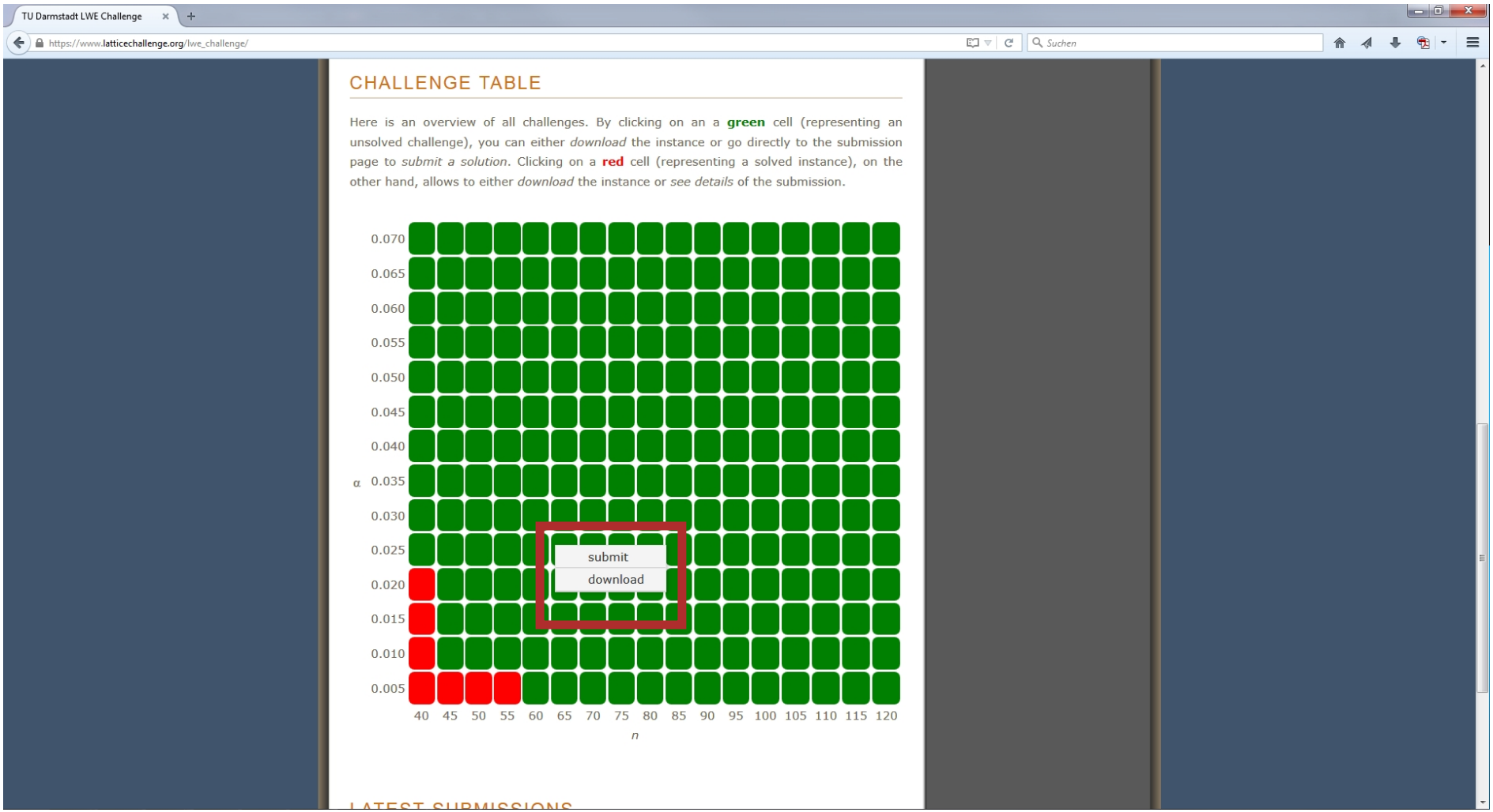
$$\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \in \mathbb{Z}_{\mathbf{q}}^{\mathbf{m}}$$

The LWE problem is to recover $\mathbf{s}$, given $\mathbf{A}$ and $\mathbf{b}$.


TU Darmstadt LWE Challenge
https://www.latticechallenge.org/lwe_challenge/
Suchen
TU DARMSTADT
LEARNING WITH ERRORS
CHALLENGE
TECHNISCHE UNIVERSITÄT DARMSTADT
UC San Diego
TU/e
INTRODUCTION
Welcome to the Learning With Errors (LWE) challenge.
The LWE problem is to recover s, given an instance (A, b), where A is an m×n matrix over Z_q and b = As + e is a vector of length m over Z_q. Both the matrix A and the target vector s are sampled uniformly random, while the error vector e is sampled from the Gaussian distribution with parameter σ.
This page presents sample instances for testing algorithms that solve the LWE problem. The main goal of this challenge is to help assessing the hardness of the LWE problem in practice. Furthermore, it is designed to provide a comparison of different types of LWE solvers, like Babai's Nearest Plane [1], BKW [2], or reduction to the Shortest Vector Problem [3].
Since current results seem to imply that the hardness of LWE instances mainly depends on the "relative error size" α = σ / q and the dimension n, this page provides LWE instances for a wide range of α and n. All challenges were created using a multi-party computation protocol executed by the Eindhoven University of Technology, the University of California, San Diego and the Technische Universität Darmstadt. The protocol ensures that none of the participating parties has additional information about the solutions.
How to participate
1. Select one of the unsolved LWE challenges (by clicking on a green cell) from below and download it.
2. Find the secret vector s.
3. Submit your solution.
SUBMISSION
Submission
DOWNLOAD
Format of Challenge Files
Toy Challenges in Dimension:
n=2, α = 0.005
n=5, α = 0.010
n=10, α = 0.015
LWE challenges:
n: 40 α: 0.005
download
LINKS
Lattice Challenge
SVP Challenge
Ideal Lattice Challenge


TU Darmstadt LWE Challenge
https://www.latticechallenge.org/lwe_challenge/
TU DARMSTADT
LEARNING WITH ERRORS
CHALLENGE
TECHNISCHE UNIVERSITÄT DARMSTADT
UC San Diego
TU/e
INTRODUCTION
Welcome to the Learning With Errors (LWE) challenge.
The LWE problem is to recover s, given an instance (A, b), where A is an m×n matrix over Zq and b = As + e is a vector of length m over Zq. Both the matrix A and the target vector s are sampled uniformly random, while the error vector e is sampled from the Gaussian distribution with parameter σ.
This page presents sample instances for testing algorithms that solve the LWE problem. The main goal of this challenge is to help assessing the hardness of the LWE problem in practice. Furthermore, it is designed to provide a comparison of different types of LWE solvers, like Babai's Nearest Plane [1], BKW [2], or reduction to the Shortest Vector Problem [3].
Since current results seem to imply that the hardness of LWE instances mainly depends on the "relative error size" α = σ / q and the dimension n, this page provides LWE instances for a wide range of α and n. All challenges were created using a multi-party computation protocol executed by the Eindhoven University of Technology, the University of California, San Diego and the Technische Universität Darmstadt. The protocol ensures that none of the participating parties has additional information about the solutions.
How to participate
1. Select one of the unsolved LWE challenges (by clicking on a green cell) from below and download it.
2. Find the secret vector s.
3. Submit your solution.
SUBMISSION
Submission
DOWNLOAD
Format of Challenge Files
Toy Challenges in Dimension:
n=2, α = 0.005
n=5, α = 0.010
n=10, α = 0.015
LWE challenges:
n: 40 α: 0.005
download
LINKS
Lattice Challenge
SVP Challenge
Ideal Lattice Challenge


TU Darmstadt LWE Challenge
https://www.latticechallenge.org/lwe_challenge/
Suchen
CHALLENGE TABLE
Here is an overview of all challenges. By clicking on an a green cell (representing an unsolved challenge), you can either download the instance or go directly to the submission page to submit a solution. Clicking on a red cell (representing a solved instance), on the other hand, allows to either download the instance or see details of the submission.
0.070
0.065
0.060
0.055
0.050
0.045
0.040
α 0.035
0.030
0.025
0.020
0.015
0.010
0.005
submit
download
40 45 50 55 60 65 70 75 80 85 90 95 100 105 110 115 120
n
LATEST SUBMISSIONS


TU Darmstadt LWE Challenge
https://www.latticechallenge.org/lwe_challenge/
CHALLENGE TABLE
Here is an overview of all challenges. By clicking on an a green cell (representing an unsolved challenge), you can either download the instance or go directly to the submission page to submit a solution. Clicking on a red cell (representing a solved instance), on the other hand, allows to either download the instance or see details of the submission.
0.070
0.065
0.060
0.055
0.050
0.045
0.040
α 0.035
0.030
0.025
0.020
0.015
0.010
0.005
submit
download
40 45 50 55 60 65 70 75 80 85 90 95 100 105 110 115 120
n
LATEST SUBMISSIONS

lwe_challenge@cdc.tu-darmstadt.de