

l9-lattice-LWE

April 23, 2025

1 LWE na mriežkach

1.0.1 Globálne parametre

```
[1]: n = 4
      m = 2*n
      #q = 101
      q = 3329
      eta = 3
```

```
[2]: def genLWE(n, m, q, eta):
      A = MatrixSpace(GF(q), m, n).random_element()
      #s = VectorSpace(GF(q), n).random_element()
      s = vector(ZZ, [randint(-eta, eta) for _ in range(n)])
      e = vector(ZZ, [randint(-eta, eta) for _ in range(m)])
      b = A * s + e
      return (A, s, e, b)

      (A, s, e, b) = genLWE(n, m, q, eta)
      print(f'e = {e}')
      print(f's = {s}')
```

```
e = (1, 1, 3, 1, 3, 2, 3, -3)
s = (2, 3, 1, -1)
```

1.0.2 Bai-Galbraith embedding

```
[3]: def getBG(A, b, n, m):
      mA = -A.change_ring(ZZ).transpose()
      B = block_matrix(ZZ, [[q*identity_matrix(ZZ,m), zero_matrix(m, n),
      ↪zero_matrix(m,1)],
      [mA, identity_matrix(ZZ,n), zero_matrix(n,1)],
      [matrix(ZZ, b), zero_matrix(1, n), identity_matrix(ZZ,
      ↪1)]]])
      return B

      B = getBG(A, b, n, m)
      B
```

```
[3]: [ 3329      0      0      0      0      0      0      0|      0      0      0      0|      0]
[      0 3329      0      0      0      0      0      0|      0      0      0      0|      0]
[      0      0 3329      0      0      0      0      0|      0      0      0      0|      0]
[      0      0      0 3329      0      0      0      0|      0      0      0      0|      0]
[      0      0      0      0 3329      0      0      0|      0      0      0      0|      0]
[      0      0      0      0      0 3329      0      0|      0      0      0      0|      0]
[      0      0      0      0      0      0 3329      0|      0      0      0      0|      0]
[      0      0      0      0      0      0      0 3329|      0      0      0      0|      0]
[-----+-----+-----]
[-1440 -2320 -859 -1367 -1234 -1149 -872 -2378|      1      0      0      0|      0]
[-636 -1892 -2955 -745 -1197 -1603 -1654 -920|      0      1      0      0|      0]
[-1478 -2508 -3059 -968 -2853 -24 -2616 -1535|      0      0      1      0|      0]
[-1725 -190 -1991 -2520 -2564 -866 -2259 -1170|      0      0      0      1|      0]
[-----+-----+-----]
[ 1213  2648  1667      89  3022  2938   408 1220|      0      0      0      0|      1]
```

```
[4]: BL = B.LLL()
BL
```

```
[4]: [  1   1   3   1   3   2   3  -3   2   3   1  -1   1]
[ -26  11  41 -19  51  43 -74 -67 -90 -41  24 -56 -58]
[  46  67   6 -14  11  -7   1 -84 -96 -12 -152 -40 -22]
[  24  84 -17  57 -38  86 -61  68  85 -31  63 -64  32]
[ -25  68 -51  70  11 -96  99 -56  -4 -17 -36 155 -21]
[  32  -4  18  92 108 -144 -71 -66 -66 -28  10   7  -5]
[  17 -38 -43 -39  81 -22 -105 -41 -116 114  15  -5  54]
[ -37  37  26 116  12 -44  -1  58  76 -50 -164 -71  98]
[  45  24  42 125 -53 -34  -8  21 -93  30  95  47  66]
[ -44  20 -30 -57 -21 -144 -31 -33  74 122 -72 -48  15]
[  94  49  56  38   3  28  -6  20 -53  36 -91 166 -56]
[ -10 -151 -34 110 -47 -65  13  16  64  73  21 -98 -16]
[   4 145  59 -12  64  24  39 173 -24 -27  46 -48 -107]
```

```
[5]: print(BL[0][:m])
print(BL[0][m:m+n])
print(f'comparing error vector: {e == BL[0][:m]}')
print(f'comparing secret s: {s == BL[0][m:m+n]}')
```

```
(1, 1, 3, 1, 3, 2, 3, -3)
(2, 3, 1, -1)
comparing error vector: True
comparing secret s: True
```

1.0.3 Skúsme postupne zvyšovať n

```
[6]: for n in range(10, 101, 10):  
    print(f'n = {n} ')  
    m = 2*n  
    (A, s, e, b) = genLWE(n, m, q, eta)  
    B = getBG(A, b, n, m)  
    BL = B.LLL()  
    print(f's is OK? {s == BL[0][m:m+n]}\t ||(e,s,1)|| = {vector(ZZ, list(e) +  
↪ list(s) + [1]).norm().n(20):.2f}\t ||BL[0]|| = {BL[0].norm().n(20):.2f}')
```

```
n = 10  
s is OK? True      ||(e,s,1)|| = 11.31      ||BL[0]|| = 11.31  
n = 20  
s is OK? True      ||(e,s,1)|| = 15.33      ||BL[0]|| = 15.33  
n = 30  
s is OK? True      ||(e,s,1)|| = 18.74      ||BL[0]|| = 18.74  
n = 40  
s is OK? True      ||(e,s,1)|| = 21.52      ||BL[0]|| = 21.52  
n = 50  
s is OK? True      ||(e,s,1)|| = 24.80      ||BL[0]|| = 24.80  
n = 60  
s is OK? False     ||(e,s,1)|| = 26.32      ||BL[0]|| = 3329.00  
n = 70  
s is OK? False     ||(e,s,1)|| = 28.58      ||BL[0]|| = 3329.00  
n = 80  
s is OK? False     ||(e,s,1)|| = 32.14      ||BL[0]|| = 3329.00  
n = 90  
s is OK? False     ||(e,s,1)|| = 33.44      ||BL[0]|| = 3329.00  
n = 100  
s is OK? False     ||(e,s,1)|| = 35.18      ||BL[0]|| = 3329.00
```

```
[ ]:
```