Goldreich, Goldwasser, Halevi (GGH) Encryption, based on CVP

Alice: Key creation

Pick good basis $\vec{v}_1, \ldots, \vec{v}_n$ and put in rows of matrix V
Choose matrix U with integer coefficients such that $\det(U) = \pm 1$
Compute bad basis as rows $\vec{w}_1, \ldots, \vec{w}_n$ of $W = UV$
Publish public key $\vec{w}_1, \ldots, \vec{w}_n$

Bob: Encryption

Plaintext vector $\vec{m} = (m_1, \ldots, m_n) \in \mathbb{Z}^n$
$\vec{v} = \vec{m}W = m_1\vec{w}_1 + \cdots + m_n\vec{w}_n \in L$
Choose small random vector $\vec{r} \in \mathbb{R}^n$
Send ciphertext $\vec{e} = \vec{v} + \vec{r} \in \mathbb{R}^n$

Alice: Decryption

Use good basis to recover $\vec{v} \in L$ *(will see details shortly)*
$\vec{m} = \vec{v}\,W^{-1}$

1. Use the values of V and W given in the Mathematica notebook for today. Let $L \subset \mathbb{R}^3$ be the lattice with basis in the rows of V.

(a) Verify that W is also a basis for L.

(b) Compute the Hadamard ratios of V and W.
Is V a good choice for a private key for GGH?
Is W a good choice for a public key for GGH?

(c) Encrypt $m = \{3, 7, 8\}$ using the ephemeral $r = \{-1, 1, 1\}$
What is the ciphertext?

(d) Verify your ciphertext by decrypting using V.
What plaintext do you get if you decrypt using the skewed basis W?

(e) You receive the ciphertext $e = \{-828256, -634219, 467126\}$. Use V to decrypt.

2. Use the public basis W for this problem given in the Mathematica notebook.

(a) Compute the Hadamard ratio of W to confirm that it is a good choice for a public key.

(b) Encrypt the plaintext $m = \{0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1\}$ using
$r = \{0, -1, -1, -1, 1, -1, 1, 1, 0, 0, 1, 0, -1, -1, 0\}$
What is the ciphertext?

(c) Suppose Eve intercepts the message
$e_1 = \{-414029, 1700490, 960750, -1305481, 681165, 258496, 576404, -394471, 75691, -922500, 327721, 1509749, -310890, -71686, -5264\}$
and tries to decrypt using W. What will Eve get for the plaintext?

(d) Now use Mathematica's LatticeReduce[W] to apply the LLL algorithm to generate a more orthogonal basis V for the lattice.

  (i) Compute the Hadamard ratio of V.

  (ii) Use V to decrypt e_1. What is the actual plaintext?