- GGH Public Key Cryptosystem

==== Key Creation ====

1. Choose a good basis v1,..., vn.
2. Choose an integer matrix U satisfying det(U) = ±1.
3. Compute a bad basis w1,..., wn as the rows of W = UV.
4. Publish the public key w1,..., wn.

==== Encryption ====

1. Choose small plaintext vector m.
2. Choose random small vector r.
3. Use Alice's public key to compute $e = x_1 v_1 + \cdots + x_n v_n + r$.
4. Send the ciphtertext e to Alice.

==== Decryption ====

1. Use Babai's algorithm to compute the vector $v \in L$ closest to e.
2. Compute vW^{-1} to recover m.