Summary: We show that partial information of plaintext can be used to simplify the decryption problem in the case of the GGH cryptosystem. Combined with Nguyen’s previous attack, we solve the numerical GGH challenge of the highest dimension 400, proposed on the Internet by the authors of the cryptosystem. We also discuss how to avoid this attack.

MSC:
94A60 Cryptography
11T71 Algebraic coding theory; cryptography (number-theoretic aspects)

Keywords:
lattice reduction; GGH; gap; partial information

Software:
NTL; NTRU

Full Text: DOI

References:

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.