Hello,

I’m wondering if implementing ElGamal encryption over the group G1 of alt_bn128 is semantically secure?

If alt_bn128 has GDH groups, one can easily compute the DDH, which breaks ElGamal encryption’s security.