Leaky Estimator, light version (DBDD_predict), general (non-smooth) case for modular hints with k=q

PASS Encrypt

d	1024
t=d/3	341
d-t	683
D_s = D_e	{-1: 0.33, 0: 0.34, 1: 0.33}
q (prime, q=1%2d)	12289
Key Recovery Attack (bikz)	474,89
bits of quantum security (*0,265)	125
Randomness Recovery Attack (bikz)	171,09
bits of quantum security (*0,265)	45
Plaintext Recovery Using Hints Attack (bikz)	202,87
bits of quantum security (*0,265)	53
min of atatcks	45

d	256	512	1024	2048
t=d/2	128	256	512	1024
d-t	128	256	512	1024
D_s = D_e	{-1: 0.33, 0: 0.34, 1: 0.33}	{-1: 0.33, 0: 0.34, 1: 0.33}	{-1: 0.33, 0: 0.34, 1: 0.33}	{-1: 0.33, 0: 0.34, 1: 0.33}
q (prime, q=1%2d)	7681	12289	12289	12289
Key Recovery Attack (bikz)	15,35	110,14	298,87	710,11
bits of quantum security (*0,265)	4	29	79	188
Randomness Recovery Attack (bikz)	15,35	110,14	298,87	710,11
bits of quantum security (*0,265)	4	29	79	188
Plaintext Recovery Using Hints Attack (bikz)	14,12	109,34	298,14	712,95
bits of quantum security (*0,265)	3	28	79	188
min of atatcks	3	28	79	188

d	1024
t=2d/3	682
d-t	342
D_s = D_e	{-1: 0.33, 0: 0.34, 1: 0.33}
q (prime, q=1%2d)	12289
Key Recovery Attack (bikz)	171,82
bits of quantum security (*0,265)	45
Randomness Recovery Attack (bikz)	473,45
bits of quantum security (*0,265)	125
Plaintext Recovery Using Hints Attack (bikz)	430,49
bits of quantum security (*0,265)	114
min of atatcks	45