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

PV Regev 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%2n)	12289
Key Recovery Attack (bikz)	171,86
bits of quantum security (*0,265)	45
Randomness Recovery Attack (bikz)	476,45
bits of quantum security (*0,265)	126
Plaintext Recovery Using Hints Attack (bikz)	433,18
bits of quantum security (*0,265)	114
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)	15,76	110,99	299,64	711,06
bits of quantum security (*0,265)	4	29	79	188
Randomness Recovery Attack (bikz)	16,94	111,1	299,64	711,06
bits of quantum security (*0,265)	4	29	79	188
Plaintext Recovery Using Hints Attack (bikz)	15,76	110,99	299,64	711,06
bits of quantum security (*0,265)	4	29	79	188
min of atatcks	4	29	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)	432,39
bits of quantum security (*0,265)	114
Randomness Recovery Attack (bikz)	172,59
bits of quantum security (*0,265)	45
Plaintext Recovery Using Hints Attack (bikz)	172,59
bits of quantum security (*0,265)	45
min of atatcks	45