Title of Document

Name of Author

August 16, 2015

1 Some observations

For $p = 101$, modulus switching seems to fail at $d = 20$. It worked for other smaller degrees, and the smaller the degree is, the better the attack (it seems).

Maybe when the index is larger, it will be better?

Saturday: degree gets to 12, it is already uniform. (What?)

Maybe try some more general Galois extensions with BKZ.

2 Galois Split prime

Galois instances vulnerable to the χ^2 uniform test.

$p = 101, d = 10, q = 5437$.

3 Modulus switching

Instances vulnerable to modulus switching. Here r is the success rate, d_v the adjustment factor, and σ the actual standard deviation used (ideally, $\sigma = \sigma_0 d_v$).

$p = 101, d = 10, d_v = 8, \sigma = 5, r = 63/100$. Number of samples used is around 5000.

$p = 211, d = 14, d_v = 8.48, \sigma = 4, r = 56/100$. Number of samples: 4000.

$p = 307, d = 17, \sigma = 7, d_v = 14.8, normbound = 13, r = 40/100$