TumbleBitSetup
Benchmark results

August 3, 2017

All of following Benchmarks were computed on a platform with Intel Core i7-4790K and 16GB of RAM using Windows OS.

1 Distribution of random values

Along are CDFs for each of the function in the protocol that generate random values. Due to variable size limitations for graphing, a small key length is used.

1.1 ρ values in permutationTest

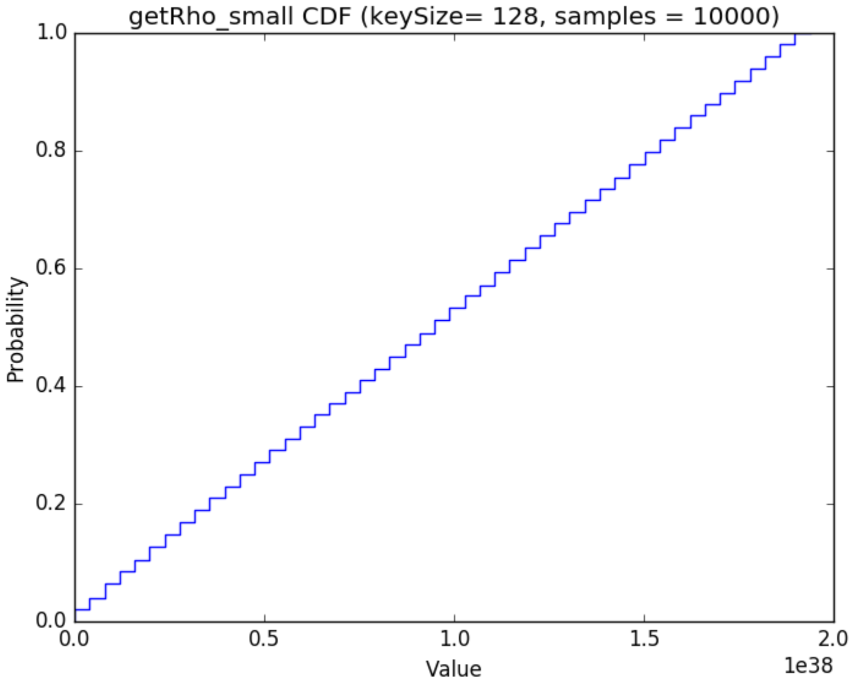


Figure 1: CDF for the samples

1.2 random value r in poupardStern

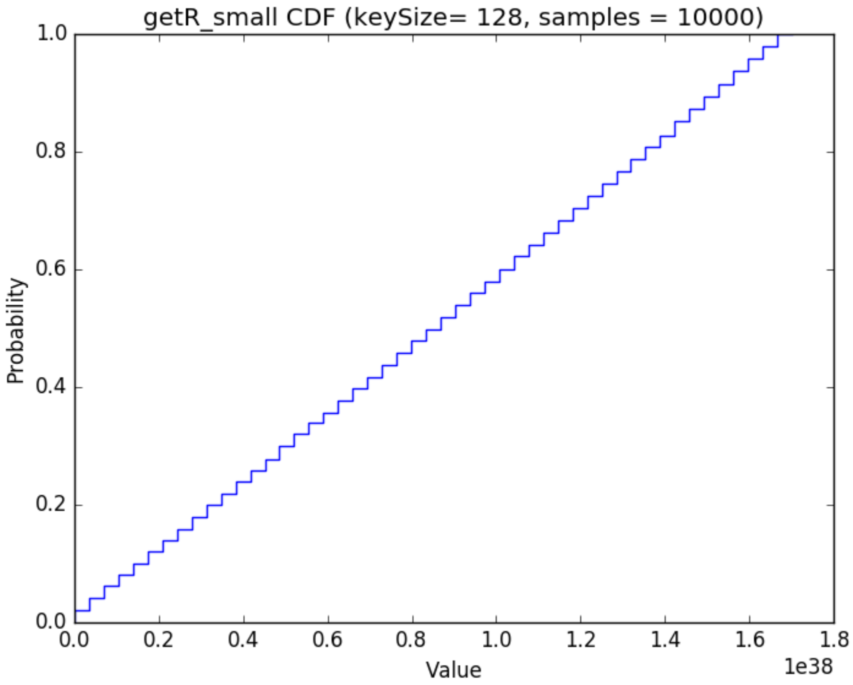


Figure 2: CDF for r

1.3 Samples from Z_N^* in poupardStern

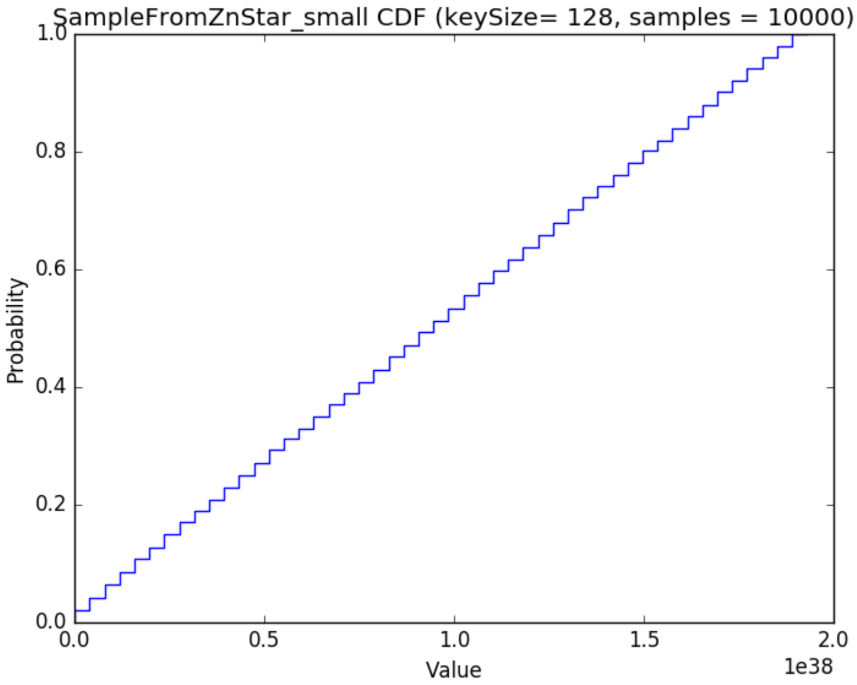


Figure 3: CDF for the samples

1.4 value w in poupardStern

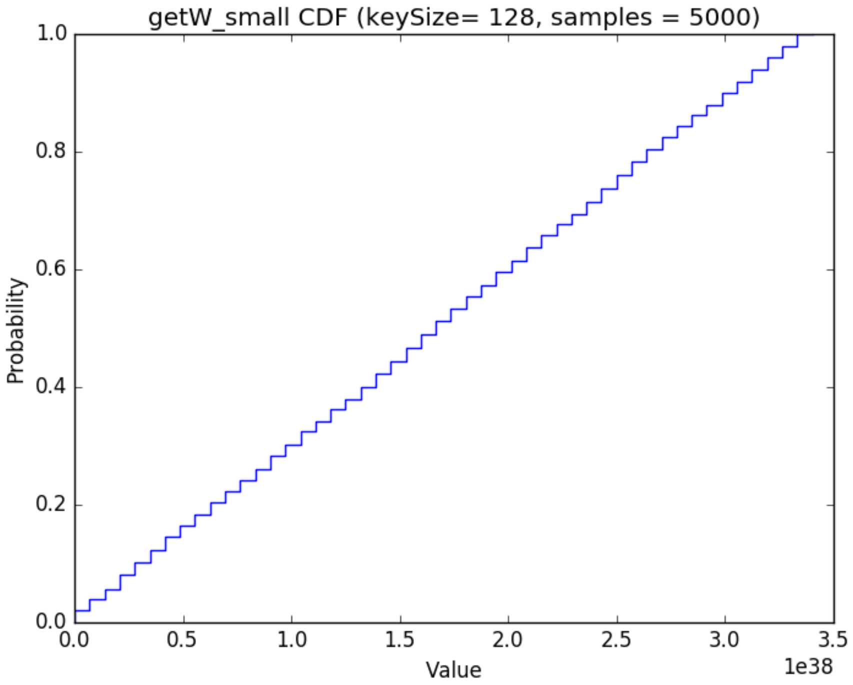
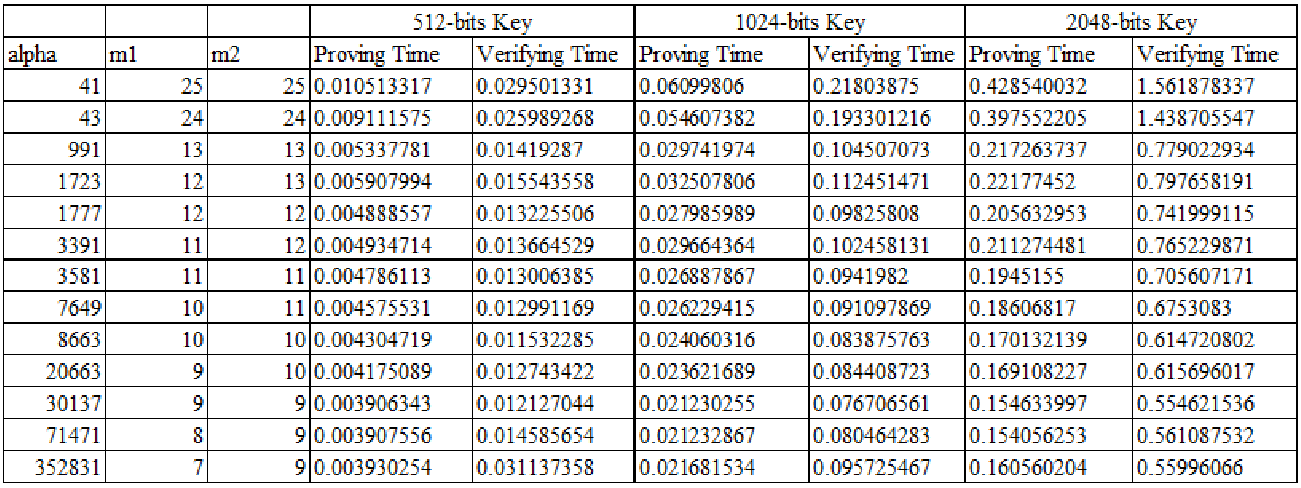


Figure 4: CDF for the samples

2 Running time of ”proving” and ”verifying”

2.1 permutationTest

The k value is fixed to 128.



			512-bits Key		1024-bits Key		2048-bits Key	
alpha	m1	m2	Proving Time	Verifying Time	Proving Time	Verifying Time	Proving Time	Verifying Time
41	25	25	0.010513317	0.029501331	0.06099806	0.21803875	0.428540032	1.561878337
43	24	24	0.009111575	0.025989268	0.054607382	0.193301216	0.397552205	1.438705547
991	13	13	0.005337781	0.01419287	0.029741974	0.104507073	0.217263737	0.779022934
1723	12	13	0.005907994	0.015543558	0.032507806	0.112451471	0.22177452	0.797658191
1777	12	12	0.004888557	0.013225506	0.027985989	0.09825808	0.205632953	0.741999115
3391	11	12	0.004934714	0.013664529	0.029664364	0.102458131	0.211274481	0.765229871
3581	11	11	0.004786113	0.013006385	0.026887867	0.0941982	0.1945155	0.705607171
7649	10	11	0.004575531	0.012991169	0.026229415	0.091097869	0.18606817	0.6753083
8663	10	10	0.004304719	0.011532285	0.024060316	0.083875763	0.170132139	0.614720802
20663	9	10	0.004175089	0.012743422	0.023621689	0.084408723	0.169108227	0.615696017
30137	9	9	0.003906343	0.012127044	0.021230255	0.076706561	0.154633997	0.554621536
71471	8	9	0.003907556	0.014585654	0.021232867	0.080464283	0.154056253	0.561087532
352831	7	9	0.003930254	0.031137358	0.021681534	0.095725467	0.160560204	0.55996066

Figure 5: Table with running times averaged over 100 iterations

2.2 poupardStern

The case were keyLength=2048-bits and alpha=41.

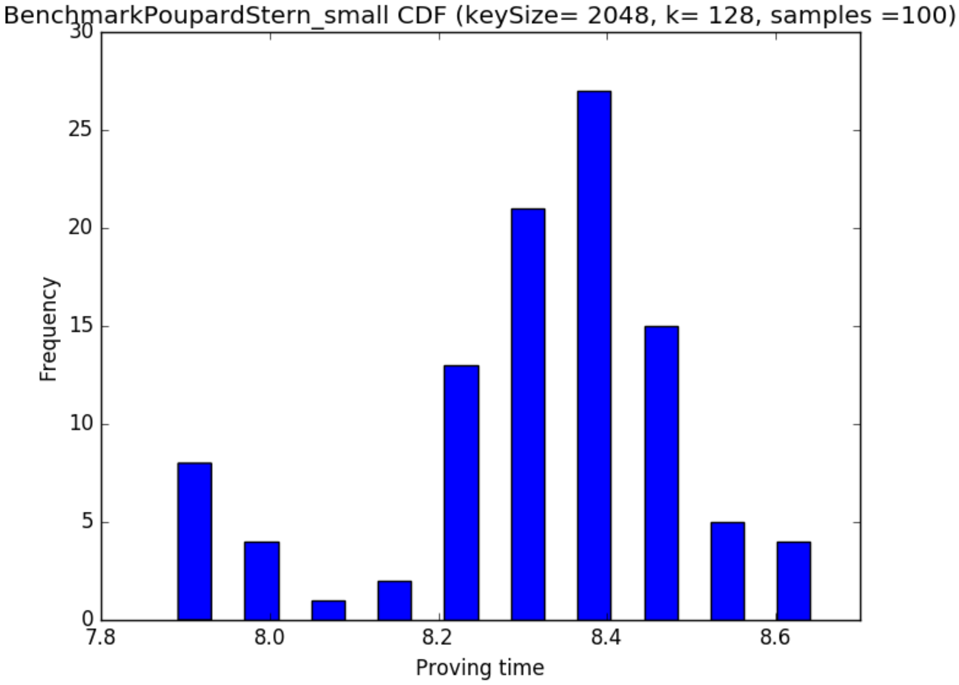


Figure 6: Histogram for the "proving" running time

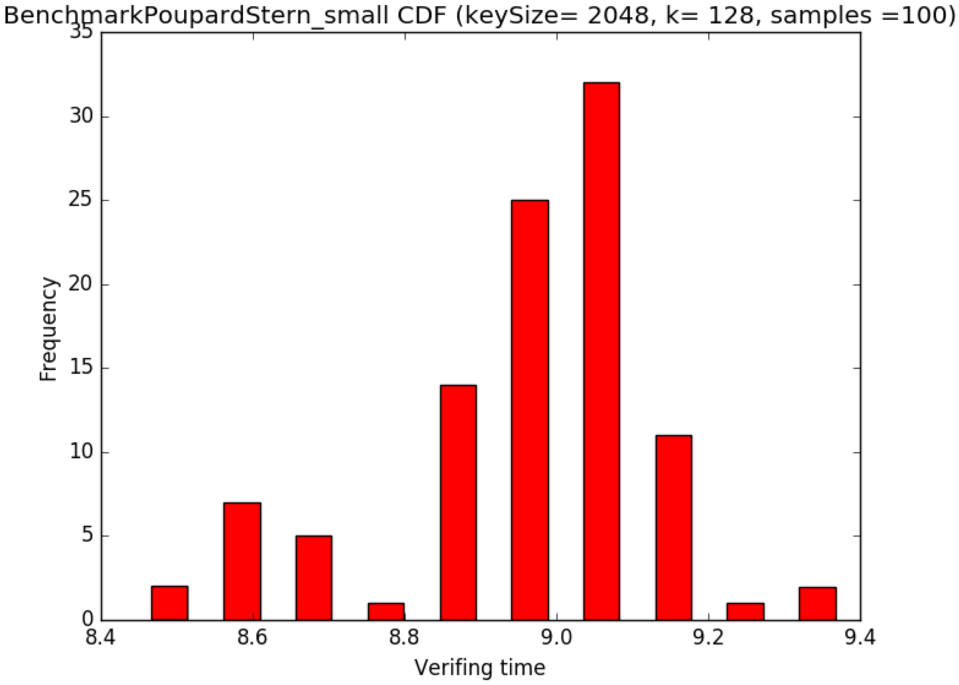


Figure 7: Histogram for the "verifying" running time