SSA Experiments on SMALLPRESENT-[8]

Md. Mohsin Ali Khan

May 13, 2015

1 SSA Capacities

Table 1: SSA Capacities

Round	$C = \frac{1}{2^8}\sum_{a\in\mathbb{F}_2^8} C(a)$	$\sigma^2_{C(a)}$ (Experimental)	$\sigma^2_{C(a)}$ (Theoretical)	Distance	Variance of $\sigma^2_{p_\eta(a)}$ (over all η)
1	1.25000000	0.5781250000000	0.01225490196078	0.56587009803921	0.000000000000000000000000
2	0.27648926	0.0145425647497	0.00059957889949	0.01394298585022	0.000000000000916679926410
3	0.08090577	0.0019491542362	0.00005133916322	0.00189781507307	0.000000000000237786179678
4	0.01151728	0.0000308265434	0.00000104037363	0.00002978616979	0.000000000000004380139875
5	0.00155004	0.0000008116343	0.00000001884419	0.00000079279016	0.000000000000000082168489
6	0.00025617	0.0000000244511	0.00000000051470	0.00000002393643	0.000000000000000005158124
7	0.00004981	0.0000000003949	0.00000000001945	0.00000000037548	0.000000000000000000057306

2 Statistic $T(\phi, a)$:

Let N be the size of the sample ϕ for a given fixation a. Let us assume that ϕ is chosen without replacement. Y is the set of possible values at the output of the trail. Let C be the capacity of the the distribution at the output of the trail. In this circumstances the formulas for theoretical mean and standard deviation of $T(\phi, a)$ are following:

$$\begin{aligned} \mu_{T(\phi,a)} &= (|Y|-1)B + NC \\ \sigma_{T(\phi,a)} &= \sqrt{\frac{2}{|Y|-1}} \times \mu_{T(\phi,a)} \end{aligned}$$

where $B = \left(1 - \frac{N}{|\phi|_{max}}\right)$. In this case, $|\phi|_{max} = 2^{24}$ and $|Y| = 2^8$.

In the below plots, we observe how the value $T(\phi, a)$ evolves as the value N grows. There are 9 different plots for rounds $3, 4, 5, 6, 7, 8, 9, 10$ and 13.

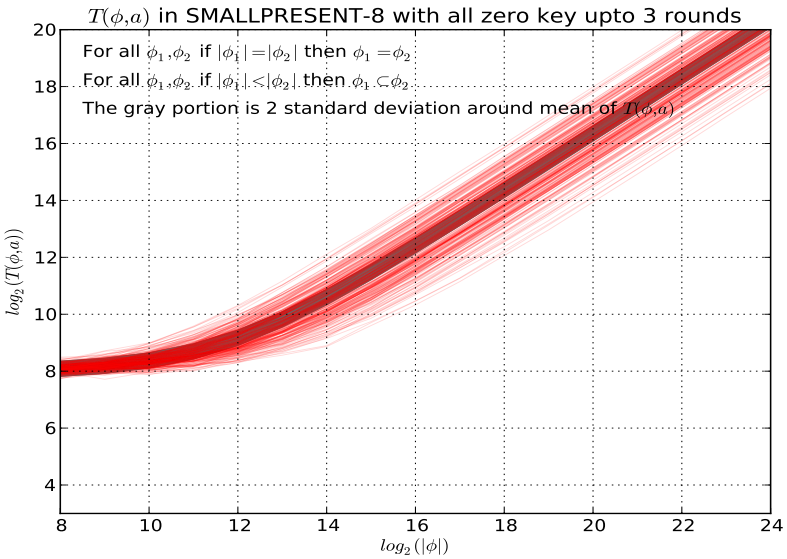

Figure 1: $T(\phi, a)$ with 3 rounds

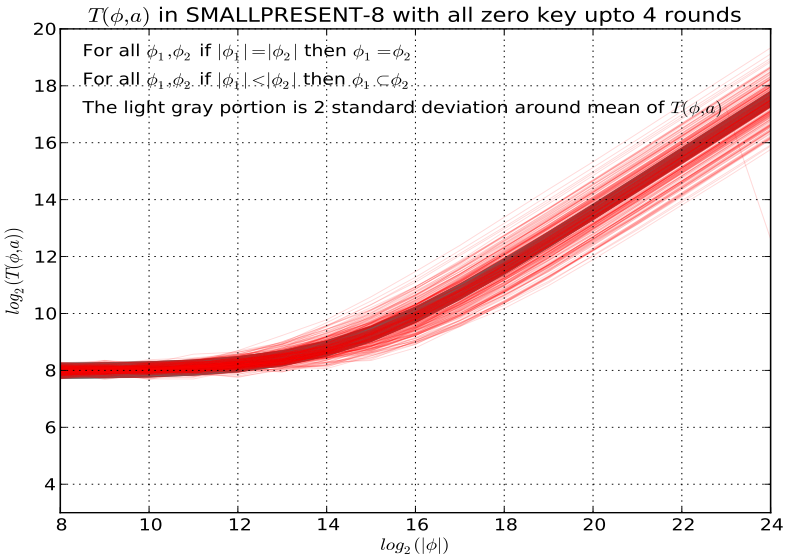

Figure 2: $T(\phi, a)$ with 4 rounds

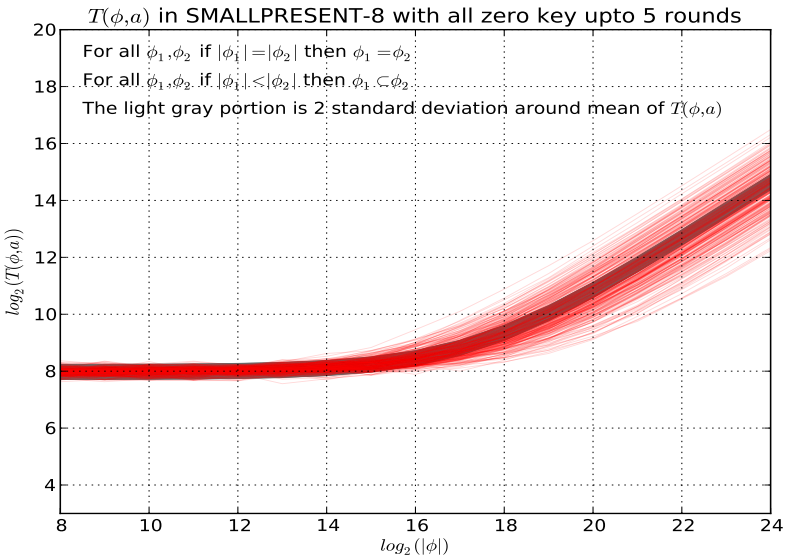

Figure 3: $T(\phi, a)$ with 5 rounds

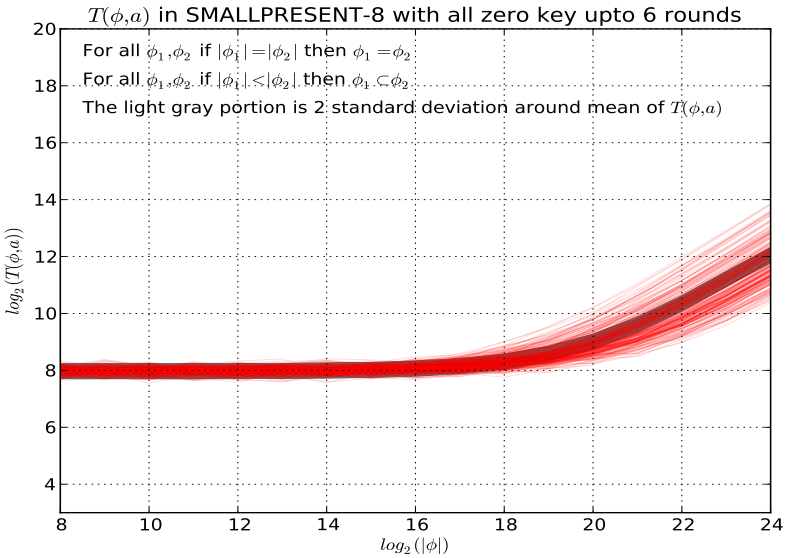

Figure 4: $T(\phi, a)$ with 6 rounds

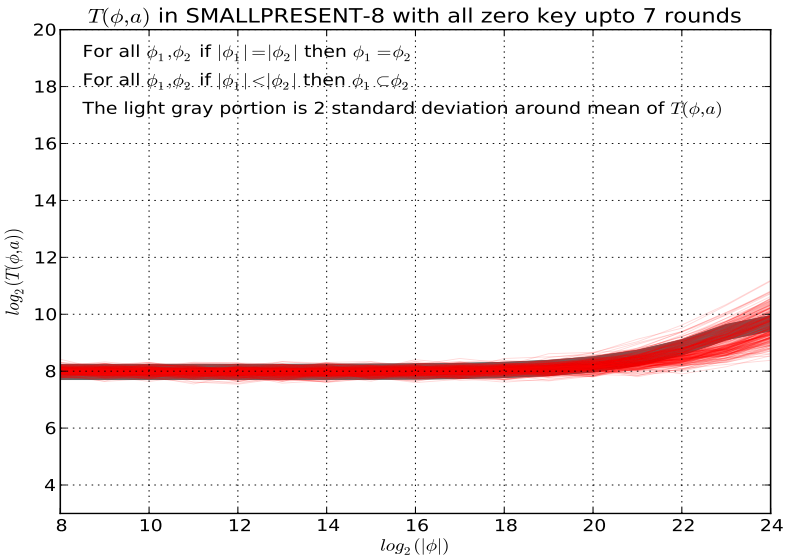

Figure 5: $T(\phi, a)$ with 7 rounds

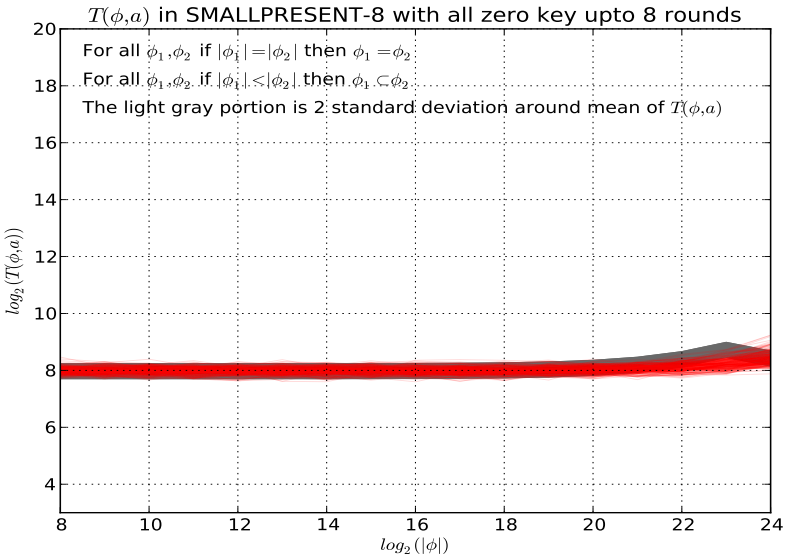

Figure 6: $T(\phi, a)$ with 8 rounds

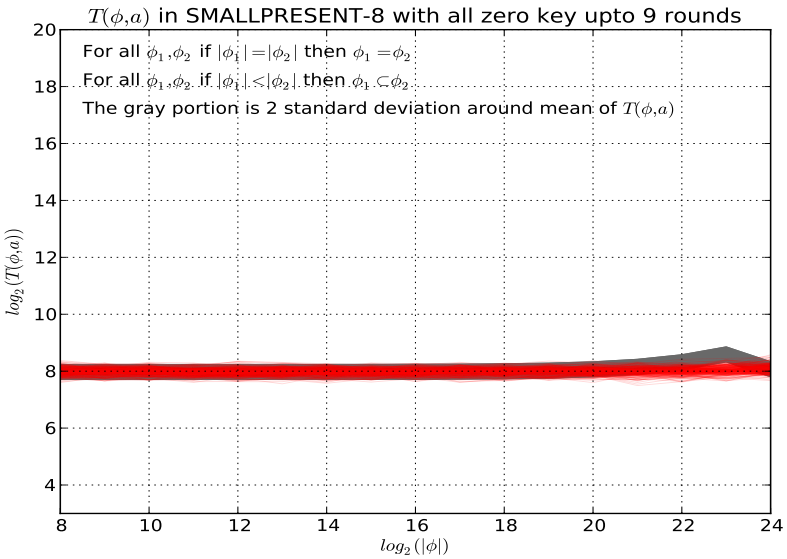

Figure 7: $T(\phi, a)$ with 9 rounds

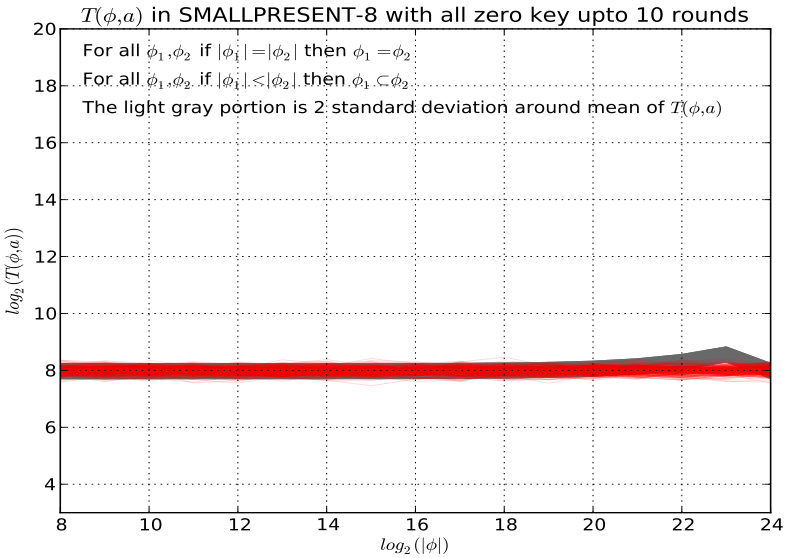

Figure 8: $T(\phi, a)$ with 10 rounds

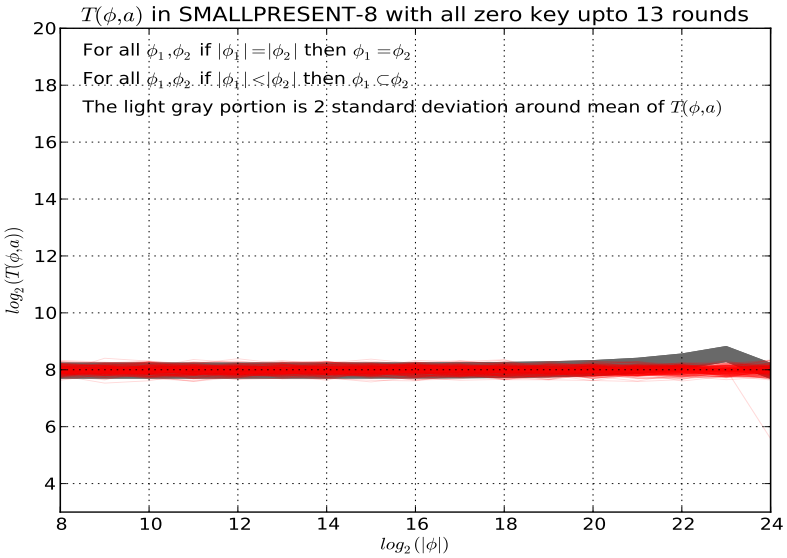

Figure 9: $T(\phi, a)$ with 13 rounds