Faster Template Building and SASCA Procedure

Shih-Chun You

June 23, 2022

Table 1: Results of recovering the functions in the SHA-3 family with different invocations (four rounds).

Function	c	#Inv.	#Rec.	#Iteration*			
				Med.	Mean	σ	Max
SHA3-512	1024	1	1000	25	25.399	0.804	28
		2	1000	26	25.629	0.619	29
		4	1000	26	25.575	0.611	29
		5	1000	26	25.615	0.621	31
		10	1000	25	25.364	0.552	28
SHA3-384	768	1	1000	27	26.838	0.942	29
		2	1000	27	27.061	0.662	30
SHA3-256	512	1	1000	29	28.646	1.246	32
		2	998	29	28.679	0.761	33
SHAKE256		1	997	29	29.054	1.272	34
		2	996	29	28.996	0.926	37
SHA3-224	448	1	1000	29	29.106	1.255	33
		2	996	29	29.440	0.971	37
SHAKE128	256	1	979	31	30.897	1.512	39
		2	971	31	31.206	1.212	39

* Only the invocations successfully reaching a steady state are take into account.

Table 2: Results of recovering the functions in the SHA-3 family with different invocations (four rounds, fast version).

Function	c	#Inv.	#Rec.	#Iteration*			
				Med.	Mean	σ	Max
SHA3-512	1024	1	1000	25	25.399	0.804	28
		2	1000	26	25.629	0.619	29
		4	1000	26	25.575	0.611	29
		5	1000	26	25.615	0.621	31
		10	1000	25	25.364	0.552	28
SHA3-384	768	1	1000	27	26.838	0.942	29
		2	1000	27	27.061	0.662	30
SHA3-256	512	1	1000	29	28.646	1.246	32
		2	998	29	28.679	0.761	33
SHAKE256		1	997	29	29.054	1.272	34
		2	996	29	28.996	0.926	37
SHA3-224	448	1	1000	29	29.106	1.255	33
		2	996	29	29.440	0.971	37
SHAKE128	256	1	979	31	30.897	1.512	39
		2	971	31	31.206	1.212	39

* Only the invocations successfully reaching a steady state are take into account.

Table 3: Results of recovering the functions in the SHA-3 family with different invocations (three rounds).

Function	c	#Inv.	#Rec.	#Iteration*			
				Med.	Mean	σ	Max
SHA3-512	1024	1	1000	30	30.064	1.720	35
		2	1000	30	30.577	1.285	36
		4	1000	30	30.485	1.277	37
		5	1000	30	30.519	1.306	36
		10	1000	30	30.273	1.282	37
SHA3-384	768	1	1000	34	34.066	2.057	41
		2	1000	34	34.420	1.497	41
SHA3-256	512	1	999	38	38.023	2.924	46
		2	997	38	38.323	1.700	45
SHAKE256		1	999	39	38.789	2.727	50
		2	994	39	38.785	1.902	50
SHA3-224	448	1	992	39	39.284	2.947	52
		2	979	40	40.086	2.138	55
SHAKE128	256	1	921	43	43.512	5.033	107
		2	861	44	44.192	3.561	116

* Only the invocations successfully reaching a steady state are take into account.

Table 4: Results of recovering the functions in the SHA-3 family with different invocations (three rounds, fast version).

Function	c	#Inv.	#Rec.	#Iteration*			
				Med.	Mean	σ	Max
SHA3-512	1024	1	1000	30	30.064	1.720	35
		2	1000	30	30.577	1.285	36
		4	1000	30	30.485	1.277	37
		5	1000	30	30.519	1.306	36
		10	1000	30	30.273	1.282	37
SHA3-384	768	1	1000	34	34.066	2.057	41
		2	1000	34	34.420	1.497	41
SHA3-256	512	1	999	38	38.023	2.924	46
		2	997	38	38.323	1.700	45
SHAKE256		1	999	39	38.789	2.727	50
		2	994	39	38.785	1.902	50
SHA3-224	448	1	992	39	39.284	2.947	52
		2	979	40	40.086	2.138	55
SHAKE128	256	1	921	43	43.511	5.021	106
		2	862	44	44.191	3.560	116

* Only the invocations successfully reaching a steady state are take into account.

Table 5: Results of recovering the functions in the SHA-3 family with different invocations (two rounds).

Function	c	#Inv.	#Rec.	#Iteration*			
				Med.	Mean	σ	Max
SHA3-512	1024	1	1000	51	50.879	5.334	70
		2	998	51	52.182	5.519	163
		4	999	52	52.199	4.905	104
		5	1000	52	52.243	5.079	161
		10	999	51	51.550	4.769	105
SHA3-384	768	1	997	65	65.992	10.484	154
		2	993	66	67.052	8.328	132
SHA3-256	512	1	942	89	95.353	29.346	199
		2	913	90	97.654	25.979	198
SHAKE256		1	869	95	101.281	30.409	199
		2	829	93	101.098	28.007	199
SHA3-224	448	1	424	94	98.206	30.737	195
		2	148	104	110.499	27.980	199
SHAKE128	256	1	35	59	63.571	14.541	111
		2	0	89	89.000	0.000	89

* Only the invocations successfully reaching a steady state are take into account.

Table 6: Results of recovering the functions in the SHA-3 family with different invocations (two rounds, fast version).

Function	c	#Inv.	#Rec.	#Iteration*			
				Med.	Mean	σ	Max
SHA3-512	1024	1	1000	51	50.909	5.362	71
		2	998	51	52.189	5.550	163
		4	999	52	52.217	4.914	104
		5	1000	52	52.266	5.082	161
		10	999	51	51.566	4.762	107
SHA3-384	768	1	997	65	66.025	10.526	154
		2	993	66	67.035	8.254	130
SHA3-256	512	1	940	89	95.240	29.147	198
		2	912	90	97.705	26.110	198
SHAKE256		1	867	95	100.993	30.085	198
		2	828	93	101.265	28.166	199
SHA3-224	448	1	419	94	98.173	30.634	195
		2	140	105	111.207	28.667	199
SHAKE128	256	1	35	59	63.943	14.485	110
		2	0	89	89.000	0.000	89

* Only the invocations successfully reaching a steady state are take into account.