TABLE 3: Fault Distribution

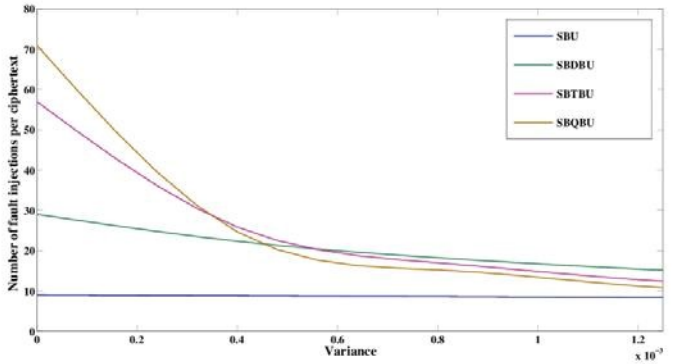
(a) Fault Distribution - Time Redundancy

Fast Clock Frequency (MHz)	FF	SBU	SBDBU	SBTBU	SBQBU	OSB	MB
125.0	512	0	0	0	0	0	0
125.1	503	9	0	0	0	0	0
125.2	489	22	1	0	0	0	0
125.3	456	50	6	0	0	0	0
125.4	425	59	22	6	0	0	0
125.5	396	45	43	28	0	0	0
125.6	354	34	112	32	0	0	0
125.7	303	23	101	85	0	0	0
125.8	260	11	55	86	0	0	0
125.9	208	5	46	147	6	0	0
126.0	176	1	39	228	68	0	0
126.1	143	0	18	211	136	4	0
126.2	115	0	10	94	178	15	0
126.3	101	0	8	95	251	49	8
126.4	65	0	9	45	232	141	20
126.5	32	0	5	16	131	187	141
126.6	13	0	3	8	98	101	289
126.7	5	0	1	4	32	112	358
126.8	0	0	1	2	5	105	399
126.9	0	0	1	2	3	88	421
127.0	0	0	0	1	2	33	476
127.1	0	0	0	0	1	12	499
127.2	0	0	0	0	0	0	512
127.3	0	0	0	0	0	0	512
127.4	0	0	0	0	0	0	512
127.5	0	0	0	0	0	0	512

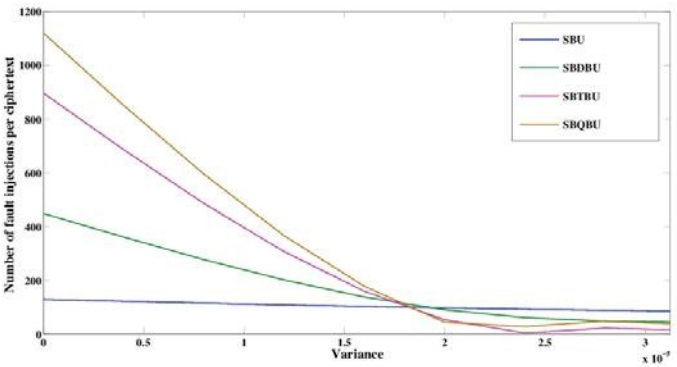
(b) Fault Distribution - Hardware Redundancy

Fast Clock Frequency (MHz)	FF	SBU	SBDBU	SBTBU	SBQBU	OSB	MB
70.0	512	0	0	0	0	0	0
70.1	512	0	0	0	0	0	0
70.2	504	8	0	0	0	0	0
70.3	475	34	3	0	0	0	0
70.4	460	47	5	0	0	0	0
70.5	416	63	29	4	0	0	0
70.6	378	38	71	25	0	0	0
70.7	345	29	120	32	0	0	0
70.8	299	21	164	28	0	0	0
70.9	234	14	120	144	2	0	0
71.0	216	4	39	247	6	0	0
71.1	189	2	35	220	66	0	0
71.2	130	0	15	180	176	11	0
71.3	105	0	10	104	278	15	0
71.4	83	0	10	66	227	100	26
71.5	50	0	8	46	157	162	90
71.6	27	0	5	16	113	125	226
71.7	21	0	4	10	98	118	261
71.8	13	0	3	6	50	103	337
71.9	7	0	3	5	21	107	369
72.0	5	0	3	2	10	99	393
72.1	2	0	1	1	8	44	456
72.2	1	0	0	1	6	19	485
72.3	1	0	0	0	2	8	501
72.4	0	0	0	0	1	5	506
72.5	0	0	0	0	0	0	512

Fig. 4: Number of Fault Attacks per Faulty Ciphertext vs Variance of Fault Probability Distribution



(a) Adversary has perfect control over target byte



(b) Adversary has no control over target byte

recover the full key under different fault models. In the second half, we vary the probability distribution for each fault model to confirm the correlation of the bias with the fault collision probability, as described by Equation 2. We quantify the bias of the fault model using the variance of the fault probability distribution, and the fault collision probability by the number of fault injections required per faulty ciphertext.

TABLE 6: Number Of Faulty Ciphertexts Required To Guess the Entire Key With 99% Probability

Round	Fault Model	N_C
8	SBU	320-340
	SBDBU	580-600
	SBTBU	1000-1040
	SBQBU	1900-2000
9	SBU	288-320
	SBDBU	608-640
	SBTBU	832-880
	SBQBU	1360-1440

5.3.1 Simulation: Part-1

In this part of the simulation, we assume identical faults in both the original and redundant computation rounds and aim to estimate the average number of faulty ciphertexts required to recover the entire key. Note that since the actual attack procedure is independent of the countermeasure scheme being targeted (time or hardware redundancy), the simulation results are presented for a general attack on either countermeasure scheme.

In the simulation, a byte of the state at the desired attack point is chosen at random and then fault is introduced into a certain number of bits belonging to that byte, varying from 1 to 4. Note that these bits are also chosen at random. We simulate the attacks in rounds 8 and 9 respectively. In each case, the appropriate distinguisher function is used to choose the key hypothesis. Table 6 summarizes the number of faulty ciphertexts required for each fault model to guess the entire 128-bit key with 99% accuracy for the attacks on rounds 8 and 9.

5.3.2 Simulation: Part-2

In the second half of the simulation, we varied the degree of bias for each fault model by controlling the variance of the