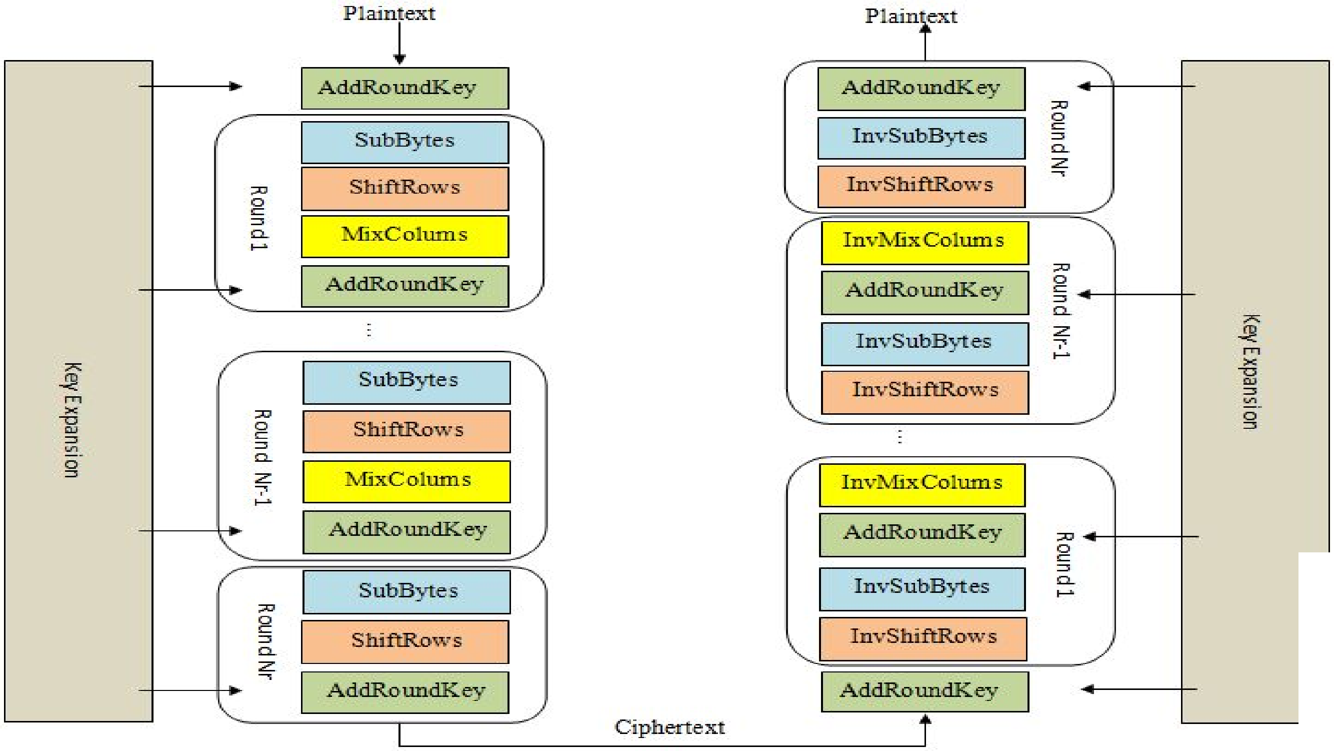
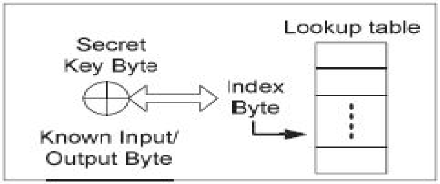
Design and Implementation of an Espionage Network for Cache-based Side Channel Attacks on AES

Bholanath Roy
Research Scholar

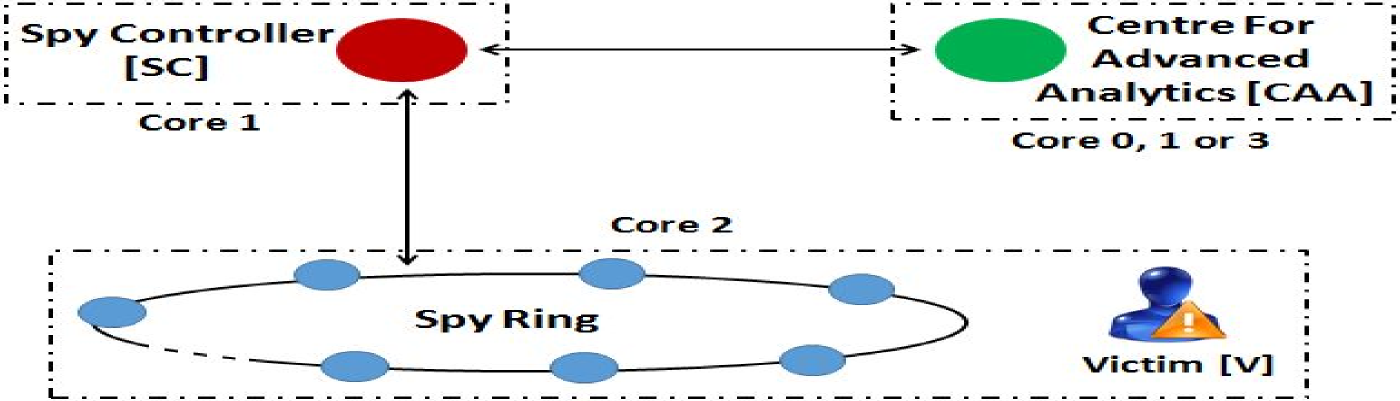
Advanced Encryption Standard(AES)



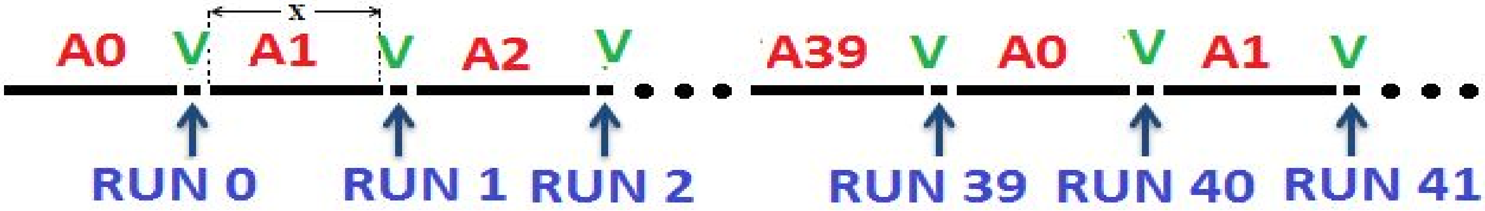


Vulnerable table lookup operations in the AES.

Design of an Espionage Network : Attack Architecture



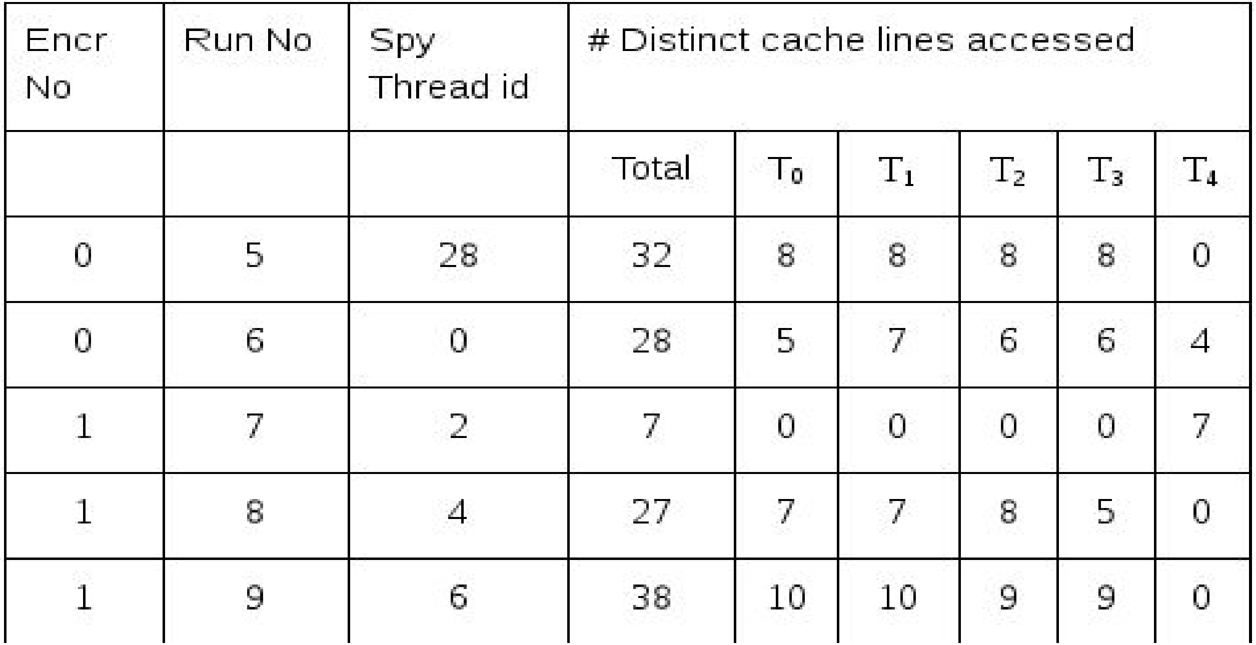
Espionage Infrastructure



Execution Timeline

Result: Attacking OpenSSL-0.9.8a in Core2Duo

Sample number of distinct accesses per table in consecutive runs in Core2Duo



Encr No	Run No	Spy Thread id	# Distinct cache lines accessed					
			Total	T_0	T_1	T_2	T_3	T_4
0	5	28	32	8	8	8	8	0
0	6	0	28	5	7	6	6	4
1	7	2	7	0	0	0	0	7
1	8	4	27	7	7	8	5	0
1	9	6	38	10	10	9	9	0