Implementation of various Cryptographic techniques in C++

Nagendra Reddy
150050067

Joshi Kosuru
150050094

Convention:

In the report if not mentioned specifically the terms are defined as

OWP	:	One Way Permutation
HCP	:	Hard Core Predicate
PRG	:	Pseudo-Random Generator
PRF	:	Pseudo-Random Function
CPA-SKE	:	CPA secure Symmetric Key Encryption
MAC	:	Message Authentication Code
CCA-SKE	:	CCA secure Symmetric Key Encryption

Problem Statement:

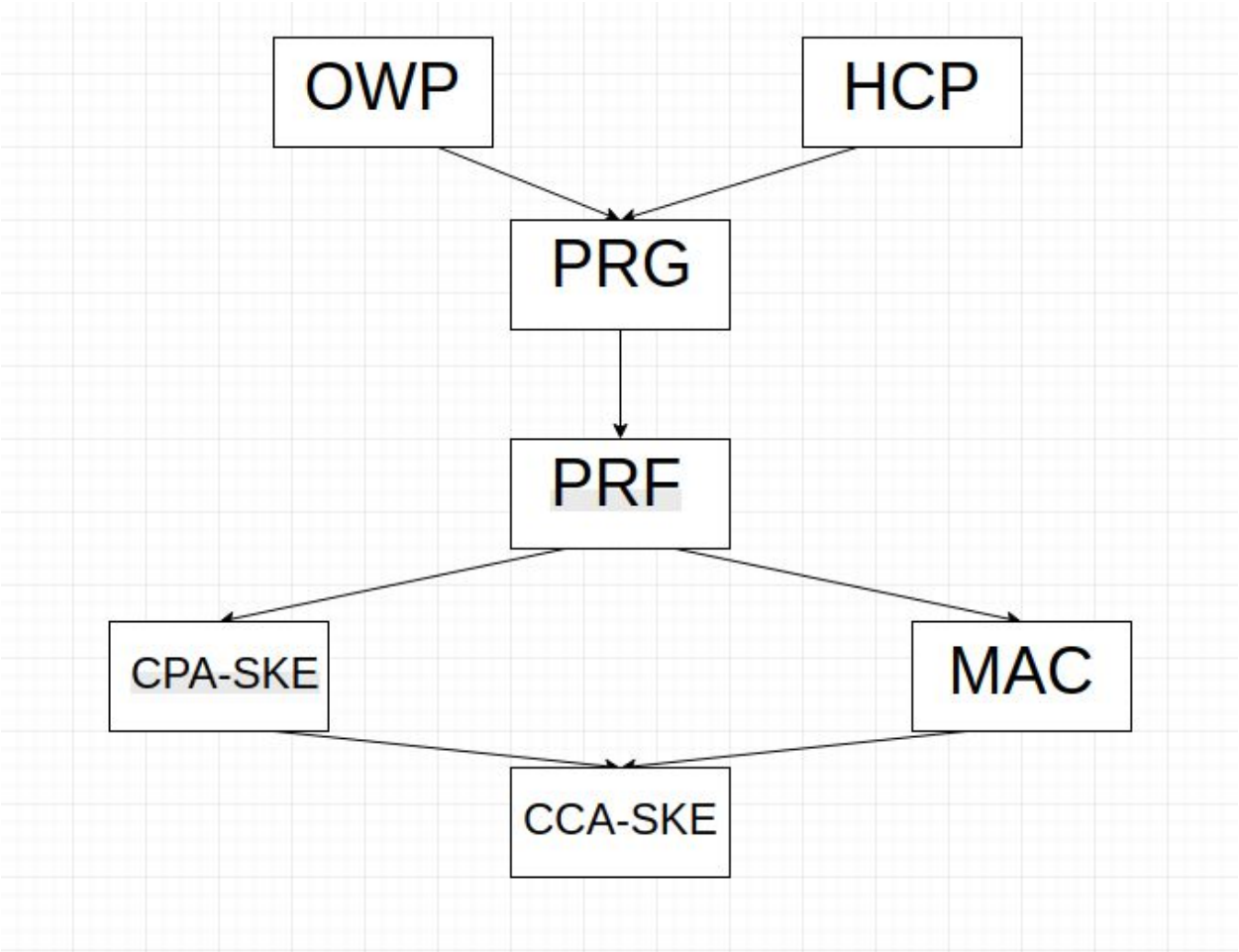
Implementation of classes for PRG, PRF, CPA-SKE, MAC, CCA-SKE from base OWP and HCP

Work Done:

We have implemented one class for each of PRG, PRF, CPA-SKE, MAC, CCA-SKE

We can see the dependencies in cryptolib.h file:

PRG contains a One Way Permutation(OWP) and corresponding Hard Core Predicate.
PRF contains a PRG and a seed
CPA-SKE contains a PRF and length of random that is used in encryption
MAC contains a PRF
CCA-SKE contains a CPA-SKE and a MAC



For truly random generators we have used getrandom() system call which give data based on entropy of system by reading the file /dev/random which contains entropy of system.

We have called this function required number of times to create the string of desired length.
For cases of random number in Encryption we have used much weaker random number generation technique which uses Mersenne Twister 19937.

Brief overview of each function is documented in code as well in doxygen documentation.