Crypto Algorithm Design and Evaluation: Directions

Successful and secure design and implementation of cryptography has become more and more critical because of ever increasing use of internet and computing tools in the services affecting our daily lives. It does not only affect us as an individual but also as an organization and as a nation.

There is a need to deploy cryptography weapons depending upon the power of the adversary.

Now it is essential that people who are doing research in cryptography follow the standard procedures to define, prove and implement the techniques. It becomes very late if the strength of a particular cryptographic method is proved after someone executes a successful attack on the system with that implementation.

Now it is well established fact that cryptography has to be based on the problems which are proved to be in the classification of NP-Complete or similar categories. So if a particular mathematical problem is very difficult to solve by computers then that can be one of the ingredients of cryptography techniques.

Few problems in Number Theory are few of such methods. So there is a need to understand the Basics of Number Theory which is the main ingredient of any modern crypto technique. We need to know the essentials to design any new cryptographic technique/algorithm. Another dimension that requires attention is that what can be achieved in terms of security and what we need to understand in terms of power of the adversary. Similarly as we cannot deploy nuclear warheads if we have a workers problem in a factory or other small issues in a country; we should not deploy cryptography without understanding the levels of Security to be decided based on the problem/situation.

Researchers need to see few case studies where there were attacks in the past on the well-known cryptographic techniques. Some case studies will be useful to understand such instances. System vulnerabilities also need to be understood so as to plug the gaps in our security deployment for our computing and online systems. To give more clarity to this topic some of the PKI based vulnerabilities may be explored. For any crypto scientist it is essential to know current status and future directions.

Prof. Deepak Garg
Head, Computer Science and Engineering Department, Bennett University, Greater Noida