Research Statement

After the emergance of the internet, there has been a massive growth in electronic mode of services. This has led to participation of heterogenous parties in incessant digital communication of sensitive information. This has urged researchers to ensure the protection of this sensitive exchange of data against intruders through established theories of cryptography. It intrigues me intensely how computationally hard mathematical problems are mapped to solve problems of security. I am excited to design and map these (hard) problems from the foundations of cryptography and apply them to solve several flavors of security-related issues. Consequently I am very much drawn to learn and contribute in the field of applied cryptography and security in a broader sense of term.

My research experience in the field of security started in the beginning of the year 2014, when I joined Indian Institute of Technology Kharagpur as a Research Assistant in a DRDO (Defense Research and Development Organization) sponsored project on Designing Secure Elliptic Curve Cryptography (ECC) Modules for Light-Weight Devices under the supervision of professor Debdeep Mukhopadhyay. I was furthermore fascinated to my introduction to the concept of elliptic curve cryptography, where the geometric representation of a cubic curve equation has been utilized, and a number theoretic group is developed with the distinct points lying on the curve. This developed group sometimes come with unique properties suitable for cryptographic applications. For example, the Elliptic Curve Discrete Logarithm Problem (ECDLP) has been developed which forms the basis of ECC based security. The project that I joined was a long term project of around three years, where I got the opportunity to explore both theoretical foundations of ECC, and its implementation based vulnerabilities.

During this project, we learnt how a safe elliptic curve can be suitably designed, by satisfying the ECDLP criteria of Pollard Rho security, discriminant security and curve rigidity criteria. Besides learning how to theoretically secure an ECC based cryptographic algorithm, we were introduced to the weaknesses that may arise while implementing an ECC algorithm. Whatever (computational) hardness may be accommodated by the theoretical ECC security, an underlying ECC algorithm, if naívely implemented on a software or hardware module leads to many unwanted threats. These attacks are termed as side-channel attacks which imposes a serious threat to any weakly implemented cryptographic module. Side-channel attacks exploit leakage of information through timing data, power or Electro-Magnetic (EM) consumption information or acoustic information during a cryptographic computation. It can also be the information obtained when a running computation undergoes some fault (s) at any algorithmic step. To address such scenarios, a designed elliptic curve must also satisfy the ECC criteria of (Montgomary) ladder security, twist (pertaining to a elliptic curve) security, indistinguishability and the property of completeness. However, implementation-based vulnerabilities were not yet been addressed in the literature to be included into a safe curve check. During our project, we worked towards the goal of strengthening the security criteria of an elliptic curve design to create a safer curve, not only theoretically but also through a implementation-wise perspective.

While I was a research assistant at IIT Kharagpur, I also enrolled as a Masters by research student in the same institute under the guidance of Dr. Debdeep Mukhopadhyay. I took the courses - 1) Design and Analysis of Algorithms 2) Computational Number Theory 3) Cryptography and Network Security and 4) Hardware Security during my MS. My masters (thesis) work is based on the topic of securing an elliptic curve based implementation against horizontal attacks. Among the various side channels mentioned above, our focus was on the leakage from power or EM consumption during a computation. Seminal work in this domain was by Coron published in Conference on Cryptographic Hardware and Embedded Systems (CHES) 1999 which showed the vulnerability of an elliptic curve scalar multiplication against simple power attacks with single trace, differential power attack with multiple traces. However recently a very powerful class of attack has surfaced termed as horizontal attack that threatens a simple as well as differential attack resistant implementation with just a single trace of information leakage. Our research focused on analyzing ECC implementations against horizontal class of attacks. To mitigate this threatening HCCA attack, we designed an effective as well as low-cost countermeasure. It is well-known fact that field multiplications form a core step of ECC computations. In the countermeasure design, we exploit the side-channel leakage characteristics from a school-book long integer multiplication (used for field multiplication). Here we showed how changing the sequence in which the operands (field multiplicands) are passed to the multiplication algorithm introduces dissimilarity in the information leakage. This disparity has been utilized in constructing a low cost countermeasure against HCCA. This countermeasure integrated with an effective randomization

method has been shown to successfully thwart HCCA.

I applied the developed countermeasure in case of unified addition formula (Edwards Curves, Brier-Joye unified formula) as well as atomicity based implementations (short-Weierstrass class of curves). Additionally I experimentally validated the proposed countermeasure technique on a SASEBO platform. My research also includes horizontal attack mitigation possibilities in a recently developed complete addition formula based short-Weierstrass curve proposed in Eurocrypt 2016, having SPA and DPA resistance. The earlier designed countermeasure has been utilized here to strengthen the security of this implementation. During my Masters I got the opportunity to publish my research in several international conference venues such as Selected Areas in Cryptography (SAC) 2015, Asia Public Key Cryptography Workshop (AsiaPKC) 2016, Midwest Symposium on Circuits and Systems (MWSCAS) 2016, Asian Hardware Oriented Trust Symposium (AsianHOST) 2016, PROOFS: Security Proofs for Embedded Systems 2017.

After my MS, I am working as an intern under professor Peter Druschel in the project Study and Design of Privacy-Preserving Identity Management Systems in the Max-Planck Institute for Software Systems since mid-February 2017. My current research focuses on building a comparative study of two existing and popular Identity systems developed; namely U-Prove and Identity Mixer. We are trying to draw an analysis of the existing properties, features, trust model of such systems and their challenges in terms of implementation and practicality. I will be working in this internship till December 2017.

My experience in security and cryptography research so far motivates me to continue my research in this domain. Post internship I am looking forward to join a PhD program broadly in the area of applied cryptography and security. Particularly, I am interested to work in the design of cryptographic protocols and their formal proofs of security and applying them to solve real-world problems (for example, the way zero-Knowledge proof protocols can be used to solve user privacy issues), development of crypto-currencies based on new proof mechanisms (work/ stake etc), also in the area of leakage-resilient cryptography. However, I am open to explore new concepts and learn applying them to solve problems in the broad domain of security and cryptography.