INTERNATIONAL CRYPTO-WEBINAR, 2020

26th to 30th August, 2020

Inaugural Speech: Prof. Basab Chaudhuri, Vice Chancellor, West Bengal State University

Welcome Speech: Prof. Arun Hota, Director, IQAC, West Bengal State University

Keynote Address: Prof. Rajeeva Karandikar, Director, Chennai Mathematical Institute

Chief Guest: Prof. Bimal Kumar Roy, Padma Shri, Head, R.C. Bose Centre for Cryptology and Security, ISI, Kolkata; Former Director of ISI; Chairperson, National Statistical Commission

Honourable Guest: Prof. Subhamoy Maitra, Professor, Indian Statistical Institute, Kolkata.

Programme Committee

Dr. Mrinal Nandi, West Bengal State University email: mrinal.nandi1@gmail.com

Dr. Nilanjan Datta, IAI, TCG CREST, email: nilanjan_isi_jrf@yahoo.com

Prof. Mridul Nandi, Indian Statistical Institute, Kolkata, email: mridul.nandi@gmail.com

Contact us @ crypto.twenty20@gmail.com

Website: https://www.isical.ac.in/~mridul/workshop/index.html

https://wbsu.ac.in/events/statistics-department-5-days-international-webinars/

https://wbsu.ac.in/event-notice/

Department of Statistics, West Bengal State University
R. C. Bose Centre for Cryptology and Security, Indian Statistical Institute
Institute for Advancing Intelligence, TCG CREST, Kolkata

Programme Schedule (Technical Session):

Date and Time	Speaker/Session Chair	Affiliation	Topic
Day 1: 26.08.20 Session 1	Prof. Mridul Nandi		**Session Chair**
11-30 to 12 noon	Prof. Rajeeva Karandikar	Director, CMI	Randomness and its relevance to Cryptology
12 to 12-45 pm.	Prof. Bimal Kumar Roy	ISI, Kolkata	Some Recent issues in Cryptology
12-45 to 1-30pm.	Prof. Subhomay Maitra	ISI, Kolkata	Recent results in stream cipher
Session 2	Dr. Nilanjan Datta		**Session Chair**
2 pm to 3 pm.	Prof. Mridul Nandi	ISI, Kolkata	How to know Security Contact of Covid-Positive Person
3 pm. to 4 pm.	Dr. Avijit Dutta	IIT, Kharagpur	History of Mirror Theory and its Application
Day 2: 27.08.20 Session 3	Dr. Sanghamitra Pal	West Bengal State University	**Session Chair**
11 to 12 noon	Dr. Mrinal Nandi	West Bengal State University	Cryptographic Randomised Response Techniques
12 to 1 pm.	Prof. Avishek Adhikari	Presidency University	Mathematical Aspects of Few Secret Sharing Schemes
Session 4	Dr. Avijit Dutta		**Session Chair**
2 pm. to 3 pm.	Prof. Somitra Kumar Sanadhya	IIT, Ropar	Format Preserving Encryption
3 pm. to 4 pm.	Dr. Arpita Maitra	IAI, TCG CREST, Kolkata	Quantum Supremacy and its implication to cryptology
Day 3: 28.08.20 Session 5	Dr. Mrinal Nandi		**Session Chair**
3 pm. to 4 pm.	Dr. kaushik Chakraborty	QuTech Academy, Delft, Netherlands	Cryptography with the space-time constraints
4 pm. to 5 pm.	Dr. Rishiraj Bhattacharya	NISER, Bhubaneswar	Memory Efficiency of Cryptographic Reductions
5 pm. to 6 pm.	Dr. Donghoon Chang	National Institute of Standards and Technology, USA	Introduction of cube attacks on MAC and AEAD schemes
Day 4: 29.08.20 Session 6	Dr. Avik Chakraborti		**Session Chair**
11 to 12 noon	Dr. Sourav Sengupta	Nanyang Technological University, Singapore	Bitcoin and Cryptocurrencies
12 to 1 pm.	Dr. Sucheta Chakrabarti	DRDO	Algebraic Structures and its applications in Cryptology
Session 7	Dr. Sumanta Adhya	West Bengal State University	**Session Chair**
2 pm. to 3 pm.	Dr. Indivar Gupta	DRDO	Public Key Cryptography
3 pm. to 4 pm.	Dr. Avik Chakraborti	ISI, Kolkata	White box Cryptography
Day 2: 30.08.20 Session 8	Dr. Sucheta Chakrabarti		**Session Chair**
11 to 12 noon	Dr. Dhiman Saha	IIT, Bhilai	The Curious Case of Embedding Yoyo within Boomerang
12 to 1 pm.	Prof. Debdeep Mukhopadhyay	IIT, Kharagpur	Security of Things and their Low Cost Authenticated Interaction in the world of IoT
Session 9	Prof. Avishek Adhikari		**Session Chair**
2 pm. to 3 pm.	Dr. Sikhar Patranabis	ETH Zurich, Switzerland	Minicrypt Primitives with Algebraic Structures
3 pm. to 4 pm.	Dr. Nilanjan Datta	IAI, TCG CREST, Kolkata	Lightweight Crypto and Classification of Authenticated Encryption Modes
	Dr. Sibnarayan Guria	West Bengal State University	**Vote of Thanks**

Randomness and its relevance to Cryptology

Prof. Rajeeva Karandikar
Director, CMI
e-mail:

Everyone working in cryptography has heard about various Randomness tests for the crypto systems. Some researchers must be wondering as to what is Random in a crypto-system: The message, the crypto algorithm, the keys are all deterministic - so what is random?
In this talk, I will elaborate as to why a proper understanding and appreciation of the notion of randomness is important for researchers in cryptography.

Some Recent issues in Cryptology

Prof. Bimal Kumar Roy
Indian Statistical Institute, Kolkata
e-mail: bimal@isical.ac.in

Abstract

In this talk, we shall discuss four different areas of Cryptography. Firstly, the issue of privacy that includes two components viz. anonymization and masking will be introduced. Secondly, we discuss Zero Knowledge Proof which gives the identity proof of one person without sharing any information about the person. Next, we discuss multi-party computation that may be applied in e-voting. Finally, we discuss hash functions and block chains with applications.

Recent results in stream cipher

Prof. Subhomay Maitra
Indian Statistical Institute, Kolkata
e-mail: subho@isical.ac.in

Abstract

In this talk first, we will describe basics of Stream Cipher Design and Cryptanalysis. Then we will discuss on basic design ideas of stream cipher. We also describe Light weight and LFSR based stream ciphers. We give overview on SNOW and ZUC. Finally we discuss on software stream cipher like RC4 and HC-128.

Contact Tracing

Prof. Mridul Nandi
Indian Statistical Institute, Kolkata
e-mail: mridul.nandi@gmail.com

Abstract

In this talk I will describe what we mean by privacy preserving contact tracing. In the last few months several such designs were proposed. Some of them are centralized and some are decentralized. We discuss some security concerns and how cryptographic tools such as Private Set Intersection can help to resolve some issues.

History of Mirror Theory and its Application

Dr. Avijit Dutta
Visiting scientist in the Dept of Computer Science
IIT Kharagpur
e-mail: avirocks.dutta13@gmail.com

Abstract

Mirror theory is a celebrated combinatorial result that says that for a system of bivariate affine equations over WOR samples, its number of solutions is very close to the average number of solutions. This result has a great impact on the security analysis of a number of symmetric cryptographic objects including PRFs, MACs, and AEs. However, the correctness of the proof of mirror theory is a subject of debate. From the time of its origin, Patarin, the inventor of this result has given many proofs, but all of them are either incomplete or contain some non-trivial flaws which are not easy to fix. This talk will present the history of mirror theory covering the problem statement, its journey, current status and application in cryptography. Moreover, I will also mention some of our recent contributions on mirror theory and conclude with interesting open problems on Mirror theory.

.

Cryptographic Randomised Response Techniques

Dr. Mrinal Nandi
Assistant Professor, Department of Statistics
West Bengal State University
e-mail: mrinal.nandi1@gmail.com

Abstract

In Warner propose well known Randomized Response Technique in sample survey. In Cryptographic Randomized Response Technique, we deal with two-party protocol: Interviewer and Responder. The responder has a private bit b. The parties exchange some information. At the end of the protocol, the interviewer gets to know a bit c which is equal to b with probability p and equal to $1 - c$ with probability $1 - p$.
This technique can be used for election. Interviewer may be honest but curious: he follows the protocol, but may perform computation to learn the secret bit of the responder. Interviewer may be malicious: he can deviate from the protocol in an attempt to learn the secret bit of the responder. Responder may be honest but curious: he follows the protocol but is interested in learning the outcome of the survey. Responder may be malicious: he can deviate from the protocol in an attempt to bias the outcome of the survey.

Mathematical Aspects of Few Secret Sharing Schemes

Prof. Avishek Adhikari
Department of Mathematics
Presidency University, Kolkata
e-mail: avishek.adh@gmail.com

Abstract

Secret Sharing, an important primitive in the field of Cryptography, is a method of sharing a secret information among a set P of n persons in such a way that certain predefined sets of qualified participants can reconstruct the secret information while certain predefined forbidden sets of participants will have no information about the secret even if they come together. Due to its applications in Multiparty Computations, Private Information Retrieval, Private Distributed Storage etc. secret sharing has become a pivot in research in information sciences. In this talk I shall mainly emphasize on different secret sharing schemes. Finally, I shall discuss about a special kind of secret sharing scheme on a set P of n participants known as Visual Cryptographic scheme in which a secret image, consisting of a collection of black and white pixels, is encoded into n shadow images called shares, where each participant in P receives one share. Certain qualified subsets of P can visually recover the secret image by photocopying their shares onto transparencies and stacking them, but any forbidden set of participants have no information about the secret image. The novelty of visual cryptography lies in the fact that the encrypted message can be decrypted directly by the human visual system, no complex computation or computer participation is required. In this talk I shall discuss various open issues related to Visual Cryptographic scheme.

Format preserving encryption

Prof. Somitra Kumar Sanadhya
Indian Institute of Technology, Ropar
e-mail: somitra@iitrpr.ac.in

Abstract

Abstract: Encryption of data destroys the format of the data and produces random looking ciphertexts. However, there are situations where the data format needs to be preserved. For example, database encryption is one of the most prominent use cases. Format Preserving Encryption (FPE) schemes are encryption algorithms which allow input format to be maintained while promising certain security guarantees. Initiated by the work of Black and Rogaway (CT-RSA 2002), many academic solutions have been proposed in literature that have focused on designing efficient FPE schemes. The US government standards body NIST has standardized two FPE schemes FF1 and FF3-1. However, these schemes are almost 10 times slower than the conventional encryption scheme like AES. In this talk, we present our two new efficient FPE schemes SPF and eSPF. Both these designs are at least 5 times efficient than the existing NIST standards. We also present some initial results showing security weaknesses in the NIST standard schemes as well as Korean standard FPE schemes.

Quantum Supremacy and its implication to cryptology

Dr. Arpita Maitra
Assistant Professor at the Institute for Advancing Intelligence (IAI) of
TCG Centres for Research and Education in Science and Technology (TCG CREST).
e-mail: arpita76b@gmail.com

Abstract

We will discuss quantum supremacy and its implications on classical cryptography. Generally, Post Quantum Cryptography (PQC) implies classical (public-key) cryptosystems that are resistant to quantum attacks. From a broader perspective, we need to analyse how one can achieve certain advantages in quantum world. Quantum supremacy can be attained in processor/circuit form, in communication, and in secrecy. In the present talk, we will present an overview of these topics.

Cryptography with the space-time constraints

Dr. kaushik Chakraborty
Post-Doctoral Fellow
QuTech Academy, Delft, Netherlands
e-mail: kaushik.chakraborty9@gmail.com

Abstract

Cryptography with the spacetime constraint or relativistic cryptography is a subdomain of multi-party cryptography where we use the concept of no-superluminal signaling (NSS) principle for designing secure cryptographic primitives. According to the NSS principle, no physical carrier of information can travel faster than the speed of light. Certain two-party cryptographic primitives like Bit Commitment, Oblivious Transfer are impossible to design without any assumptions on the computational capacity of the adversaries. Most of the no-go theorems for the construction of these primitives are based on a single prover and single verifier model. However, in the late eighties, Ben-Or et al first considered designing an information-theoretically secure bit commitment scheme in the two-prover model. In their seminal work, they proved that if the provers don't communicate then it is possible to design a secure bit commitment scheme. Later in 1999 Adrian Kent used the NSS principle to relax the non-communication assumption and proposed a secure relativistic bit commitment scheme. Unfortunately, the lifespan of Kent's protocol depends upon the communication time between the two provers. Later Lunghi et al increased the life span of the relativistic bit commitment protocol by adding multiple rounds of commitments. In this presentation, I will talk about the multi-round relativistic bit commitment protocol by Lunghi et al and show its security against classical adversaries. I will conclude by discussing the security of such schemes in the post-quantum era.

Memory Efficiency of Cryptographic Reductions

Dr. Rishiraj Bhattacharyya
Reader, School of Computer Science of NISER
e-mail: rishi@niser.ac.in

Abstract

Modern cryptographic constructions are often paired with a reduction from a hard problem. For optimized parameter choices, the reductions are required to be as efficient as possible. Traditionally, efficiency of a reduction was measured in terms of time complexity and success probability. Recent cryptanalytic techniques have established the importance of memory as an additional important parameter. In this talk, I shall review the recent techniques to improve the memory efficiency of cryptographic reductions.

Introduction of cube attacks on MAC and AEAD schemes

Dr. Donghoon Chang
Guest researcher at Computer Security Division of NIST in Gaithersburg, Maryland, USA
Associate professor and head of Cryptology Research Group (CRG) at IIIT Delhi
email: pointchang@gmail.com

Abstract

The cube attack is a method of cryptanalysis applicable to a wide variety of symmetric-key algorithms. A cipher is vulnerable by the cube attack if an output bit can be represented as a sufficiently low degree polynomial over GF(2) of key and input bits. In this talk, I will introduce cube attack basics and explain how the cube attack works for MAC and Authenticated Encryption with low degrees.

Bitcoin and Cryptocurrencies -The World of Cryptocurrencies

Dr. Sourav Sengupta
Lecturer, Nanyang Technological University, Singapore
e-mail: sg.sourav@gmail.com

Abstract

Although the idea of cryptographic digital cash had been around for a while, the advent of Bitcoin in October 2008 ushered a new era in the world of cryptocurrencies. Since then, a number of decentralized cryptocurrencies have been introduced, and the recent boom in the price and market capitalization of some of these currencies has taken the world by storm. In this talk, we will try to understand the evolution of decentralized peer-to-peer cryptocurrencies, by deconstructing them into their major components -- the blockchain architecture, the cryptographic primitives, the multi-party consensus, and the design of the incentive mechanism. We will try to touch upon a variety of cryptocurrency technologies in this domain -- starting from the old proposals like b-cash and bit-gold to the newest constructs like Bitcoin, Ethereum, Ripple, Litecoin and Zcash. This talk does not assume any prior background in Cryptology, as such, and anyone interested in the subject may feel free to attend.

Algebraic Structures and its Applications in Cryptography

Dr. Sucheta Chakrabarti
Scientist-'G', Scientific Analysis Group
DRDO, Delhi
e-mail- suchetadrdo@hotmail.com

Abstract

Information Security plays a very important role in today's digital communication era. It is well known that information is a driver of development of society and hence its integrity, confidentiality authenticity and availability must be ensured. Digital privacy is highly in demand from individual and as well as authority (i.e. Govt. military, corporate sectors) to protect their valuable assets. Security methods and techniques are critical components of required infrastructure for protecting information and secure communication over open networks. Cryptography is the building block of the development of these methods & techniques to ensure the security. It is a multidisciplinary Fields. The growth of cryptology in any Nation highly depends on the level of development of science & technology in the society.

The famous Russian mathematician P.L. Chebyshev nicely express the connection between theoretical and practical development of mathematics – "The bringing together of theory and practice leads to the most favourable results; not only does practice benefit, but the sciences themselves develop under the influence of practice, which reveals new subjects for investigation and new aspects of familiar subjects."

Crypto algorithms and crypto primitives are mainly designed on proper algebraic structures which provides the strength of the schemes. The combination of the set and operations that are applied on the elements of the set is called an algebraic structure. Here an algebra means a universal algebra which is a set together with finitary operations satisfying some / none identities. For example, Groupids- algebras with a single binary operation, Semigroups- algebras with one binary operation with associative identity etc. In my talk I will discuss about the goal, component and secrecy of the cryptosystem. Briefly discuss the role of probability and entropy of secure communication from information theoretic approach. Also discuss till now commonly used underlying algebraic structure in cryptography which are mainly are viz. Groups (Abelian / cyclic), Fields and Rings. which are commutative and associative i.e., they satisfy the identities $(i) a \cdot (b \cdot c)$ & $(ii) a \cdot (b \cdot c) = (a \cdot b) \cdot c$. It means the outcome is independent of order of the operation.

In late eighties part of crypto community, mainly European has been visualized the great potentiality of using non-commutative and non-associative algebraic structures in cryptography. It gives a new direction of cryptology. The use of these algebraic structures also play a significant role to protect many known attacks. In this direction there are some algebraic structures with great scopes of applications in cryptography. They are namely quasigroups, *n*-ary quasigroups. The quasigroup based cryptography is a new potential area in cryptography.

Finite quasigroups / n-ary quasigroups having one-to-one correspondence to Latin squares / Latin hypercubes are very suitable algebraic structures to use in cryptography. Quasigroups of some specific orders have connection with vector Boolean functions. Algebraic systems of these structures represent by Boolean functions. Current research shows that these structures have great potential to enhance security of cryptographic schemes based on their algebraic properties, identities, large numbers, different transformations and computational simplicity of operations. Now a days it is one of the challenging research areas to design new crypto primitives, algorithms and codes based on quasigroups / n-ary quasigroups. The choice of cryptographically suitable quasigroups is one of the ongoing research problems to strengthen the crypto-design based on these structures. In my talk I will discuss some of these issues also.

Public Key Cryptography

Dr. Indivar Gupta
DRDO, Delhi
e-mail: indivar_gupta@yahoo.com

Abstract

In the age of information and communication technology, the demand for cryptographic algorithms is growing rapidly to provide security in communication among the users connected through the network such as LAN/WAN, internet, mobile, telephone, wireless communication, Wi-Fi, Bluetooth etc for speech, text data and fax. Nowadays, secure communication has not only been limited to the Defence and commercial applications like internet banking but it has also become essential in any type of personal communication.

As we know, cryptography broadly classified into two categories namely Symmetric Key and Public Key cryptography. The idea of Public Key Cryptography was introduced by Hellman Merkle and Diffie in 1976. Presently, in many communication systems, Public Key Cryptography (PKC) is being used for key exchange mechanism and ensuring confidentiality. Public key cryptography is also an important mean to provide authentication and data integrity. The security of any public-key cryptographic scheme relies on some computationally hard problem derived from algebraic and number-theoretic structures.

In this talk, firstly the basic concept of complexity theory required to measure the strength of the crypto-systems will be discussed. Then, the basic concept of number theory and algebra required for understanding public key crypto-systems will be reviewed. Thereafter the complexity of some poplar algorithms will be presented. Finally, some well-known public key crypto-systems such as RSA, ElGamal and elliptic curve public key crypto-systems with their security analysis will also be discussed.

White Box Cryptography

Dr. Avik Chakraborti
lecturer cum Post-doc Fellow at the R.C Bose Centre for Cryptology and Security
ISI, Kolkata
e-mail: avikchkrbrti@gmail.com

Abstract

White box cryptography aims to protect the secrets corresponding to cryptographic implementations from an attacker that has full access to the underlying implementation codes. Precisely white box crypto is an obfuscation technique used for implementations executed on open devices such as smartphones, tablets, PCs where the developer wants to get rid of hardware secure elements to store secret information. In this talk, we cover the basics of obfuscation, white box crypto along with a concrete example of white box implementation of AES.

The Curious Case of Embedding Yoyo within Boomerang

Dr. Dhiman Saha
Department of Electrical Engineering and Computer Science
Indian Institute of Technology, Bhilai
e-mail: saha.dhiman@gmail.com

Abstract

In this talk we will try to investigates a generic way of combining two very effective and well-studied cryptanalytic tools, proposed almost 18 years apart, namely the Boomerang attack proposed by Wagner in FSE 1999 and the Yoyo attack by Ronjom et al. in Asiacrypt 2017.
While doing so to set the context we will first introduce these techniques individually. Then we will revisit some of the Boomerang switching techniques primarily the Sbox-switch and Ladder-switch techniques which have been shown in literature as very effective increasing the probability of a Boomerang distinguisher. The main aim is to embed a Yoyo trail within a Boomerang trail and study the interaction between both trails to devise a generic distinguisher. We will also see how this approach fares in the light of other contemporary techniques. Finally a possible application will be discussed which is currently an on-going work. To the best of our knowledge, this is the first attempt to merge the Yoyo and Boomerang techniques to analyze SPN ciphers and has the potential of becoming an important cryptanalysis tool.

Security of Things and their Low Cost Authenticated Interaction in the world of IoT

Prof. Debdeep Mukhopadhyay
Dept of Computer Science and Engineering,
Indian Institute of Technology, Kharagpur
e-mail: debdeep.mukhopadhyay@gmail.com

Abstract

With the advent of the Internet of Things (IoT) the need and challenges of security have increased manifold. While the "things" of the IoT have to be secured against adversaries and are fortified by conventional cryptography, they are the hotbeds of the growingly menacing side channel attacks, which target weaknesses in implementations. On the other hand, cost is a major constraint for many of these devices and hence IoT devices are routinely being sold with proprietary authentication and security mechanisms, which can be subverted quite easily. This motivates the study of unconventional secured authentication and key establishment protocols using novel hardware primitives called Physically Unclonable Functions.

In this talk, we summarize research directions of Secured Embedded Architecture Laboratory (SEAL), IIT Kharagpur, India in the broad area of hardware security. Subsequently, we present an overview on side channel attacks. These vulnerabilities can be potentially used by skilled adversaries to compromise trusted executions which are considered to be the base of various emerging applications like automotive.

Finally, we present an overview on PUFs and their usages in developing low-cost authentication suitable for IoT environments. In particular, we present designs being developed in SEAL using PUF based authentications which can also lead to key establishment without the need of Public-Key-Infrastructures, which are a major bottleneck for IoTs.

Minicrypt Primitives with Algebraic Structure

Dr. Sikhar Patranabis
Postdoctoral fellow at Applied Cryptography group ETH Zurich, Switzerland.
email: sikharpatranabis@gmail.com

Abstract

Algebraic structure lies at the heart of much of Cryptomania as we know it. An interesting question is the following: instead of building (Cryptomania) primitives from concrete assumptions, can we build them from simple Minicrypt primitives endowed with additional algebraic structure? In this work, we affirmatively answer this question by adding algebraic structure to the following Minicrypt primitives: one-way functions, weak unpredictable functions and weak pseudorandom functions. The algebraic structure that we consider is group homomorphism over the input/output spaces of these primitives. We show that these structured primitives can be used to construct several Cryptomania primitives in a generic manner.

Our results make it substantially easier to show the feasibility of building many cryptosystems from novel assumptions in the future. In particular, we show how to realize any CDH/DDH-based protocol with certain properties in a generic manner from input-homomorphic weak unpredictable/pseudorandom functions, and hence, from any concrete assumption that implies the existence of these structured primitives.

Our results also allow us to categorize many cryptographic protocols based on which structured Minicrypt primitive implies them. In particular, endowing Minicrypt primitives with increasingly richer algebraic structure allows us to gradually build a wider class of crypto-primitives. This seemingly provides a hierarchical classification of many Cryptomania primitives based on the "amount" of structure inherently necessary for realizing them.

Lightweight Cryptography and Classification of Authenticated Encryption Modes

Dr. Nilanjan Datta
Assistant professor of IAI, TCG-CREST
Email: nilanjan_isi_jrf@yahoo.com

Abstract

The era of the so-called Internet of Things (IoT) - communication networks interconnecting several small devices - is rapidly emerging. Security is one of the biggest concerns in widespread adoption of IoT technologies. Authenticated encryption or AE is a symmetric-key cryptographic primitive that is expected to play a key role in securing IoT networks. This expectation is largely due to the fact that AE schemes can achieve both confidentiality and authenticity - two major concerns in information security. In particular lightweight AE schemes have seen a sudden surge in demand. The recently concluded CAESAR competition and the ongoing NIST LwC project gave new impetus to the design and analysis of lightweight AE schemes. In this talk, we will first discuss the motivation of lightweight Cryptography, and the ongoing NIST LwC project on authenticated encryption. Next, we will talk about general desirable properties and some application-specific properties of authenticated encryption modes. Finally, we will classify all the existing authenticated encryption schemes based on their design structure, discuss general design-rationale and applications corresponding to each category, and provide concrete examples.