## INTERNATIONAL CRYPTO-WEBINAR, 2020

## **Programme Schedule (Technical Session):**

Day 2: 22.08.20 Dr. Mrinal Nandi Session 1 12 to 12-45 pm. Prof. Bimal Kumar Roy ISI, Kolkata Prof. Subhomay Maitra Session 2 Dr. Nilanjan Datta Session 2 Dr. Nilanjan Datta Session 3 Dr. Mrinal Nandi Session 3 Dr. Sanghamitra Pal Session 3 II to 12 noon Dr. Avijit Dutta IIT, Kharagpur Session 4 Dr. Avijit Dutta IIT, Kharagpur Session 4 Dr. Arpitu Maitra Session 4 Dr. Arpitu Maitra Session 4 Dr. Arpitu Maitra Session 4 Dr. Avijit Dutta Session 4 Dr. Arpitu Maitra Session 4 Dr. Arpitu Maitra Session 5 Dr. Sanghamitra Pal Session 5 Session 4 Dr. Avijit Dutta Session 6 Dr. Avijit Dutta Session 5 Dr. Arpitu Maitra Session 6 Dr. Avijit Dutta Session 6 Dr. Sourav Sengupta Session 6 Dr. Sourav Sengupta Session 7 Dr. Avik Chakraborti Session 7 Dr. Sumanta Adhya Session 7 Dr. Sumanta Adhya Session 7 Dr. Sumanta Adhya Session 8 Ur. Kharagpur Session 9 Prof. Avishek Adhikari Se	Date and Time	Speaker/Session Chair	Affiliation	Topic
12 to 12-45 pm. 12 to 13 pm. 15 pm. 16 pm. 17 pm. 18 pm. 1	Day 2: 26.08.20	Dr. Mrinal Nandi		Session Chair
Cryptology   Cryptology   Prof. Subhomay Maitra   Session 2   Dr. Nilanjan Datta   Session 2   Dr. Nilanjan Datta   Session 2   Dr. Nilanjan Datta   Session Chair   Contact Tracing   Cryptographic Randomised   Response Techniques   Response Techniques   Response Techniques   Session 3   Dr. Avijit Dutta   History of Mirror Theory and its   Application   Application   Application   Prof. Avijit Dutta   History of Mirror Theory and its   Application   Applicat	Session 1			
12-45 to 1-30 pm.   Prof. Subhomay Maitra   ISI, Kolkata   Session Chair	12 to 12-45 pm.	Prof. Bimal Kumar Roy	ISI, Kolkata	
Session 2   Dr. Nilanjan Datta   Session Chair				**
2 pm to 3 pm. Prof. Mridul Nandi SI, Kolkata Contact Tracing 3 pm, to 4 pm. Dr. Mrinal Nandi West Bengal State University Cryptographic Randomised Response Techniques Response Techniques Response Techniques Response Techniques Session 3 Pr. Sanghamitra Pal West Bengal State University Session Chair Session 3 Pr. Avijit Dutta IIT, Kharagpur History of Mirror Theory and its Application Mathematical Aspects of Few Secret Sharing Schemes Session 4 Prof. Mridul Nandi Session 4 Prof. Mridul Nandi Session 4 Prof. Mridul Nandi Session 5 Prof. Somitra Kumar Sanadhya IIT, Ropar Format preserving encryption Session 5 Pr. Avijit Dutta Session 5 Pr. Avijit Dutta Session 5 Pr. Avijit Dutta Session 5 Pr. Rishiraj Bhattacharya NISER, Bhubaneswar post-snowden cryptography with the space-time constraints Prof. Donghoon Chang Dr. Avijit Dutta Session 6 Pr. Sourav Sengupta Nanonal Institute of Standards Session 6 Pr. Sourav Sengupta Nanonal Institute of Standards Session 6 Pr. Sourav Sengupta Nanonal Institute of Standards Session 6 Pr. Sourav Sengupta Nanonal Institute of Standards Session 6 Pr. Sourav Sengupta Nanonal Institute of Standards Session 6 Pr. Sourav Sengupta Nanonal Institute of Standards Session 6 Pr. Sourav Sengupta Nanonal Institute of Standards Session 6 Pr. Sourav Sengupta Nanonal Institute of Standards Session 6 Pr. Sourav Sengupta Nanyang Technological University, Singapore Algebraic Structures and its applications in Cryptocurrencies University Session 7 Pr. Sucheta Chakrabarti DRDO Algebraic Structures and its applications in Cryptocurrencies DRDO Public Key Cryptography Dr. Avik Chakraborti Session 7 Pr. Avik Chakraborti Session 9 Prof. Avishek Adhikari Prof. Dr. Dr. Dr. Dr. Dr. Dr. Dr. Dr. Dr. Dr		· ·	ISI, Kolkata	*
3 pm. to 4 pm.  Dr. Mrinal Nandi  West Bengal State University  Session 2  11 to 12 noon  Dr. Avijit Dutta  IIT, Kharagpur  Prof. Avishek Adhikari  Presidency University  Session 4  Prof. Mridul Nandi  2 pm. to 3 pm.  Prof. Smirta Kumar  Sanadhya  3 pm. to 4 pm.  Dr. Avijit Dutta  IIT, Ropar  Sanadhya  3 pm. to 4 pm.  Dr. Avijit Dutta  IIT, Ropar  Sanadhya  3 pm. to 4 pm.  Dr. Avijit Dutta  Session 4  Prof. Avijit Dutta  Jor. Avijit Dutta  Session 4  Prof. Avijit Dutta  Session 5  Dr. Avijit Dutta  Session 6  Dr. Avijit Dutta  Session 7  Dr. Dongboon Chang  Dr. Avik Chakraborti  Session 7  Dr. Sucheta Chakrabarti  DRDO  Dr. Sucheta Chakrabarti  DRDO  Dr. Sucheta Chakrabarti  DRDO  Dr. Avijit Auman  Dr. Avijtar Gutta  Dr. Dongboon Charg  DRDO  Prof. Sucheta Chakrabarti  DRDO  Dr. Dongboon Charg  DRDO  Public Key Cryptography  Dr. Jordya Sunda Adhya  Dr. Jordya Gutta Chakrabarti  DRDO  Public Key Cryptography  Dr. Avik Chakraborti  Session 8  II to 12 noon  Dr. Dhiman Saha  IIT, Kharagpur  Session Chair  Session Chair  Session P  Prof. Avishek Adhikari  Dr. Nilanjan Datta  IIT, Kharagpur  Security of Things and their Low Cost Authenticated Interaction in the world of IoT  Session P  Prof. Nilanjan Datta  IAI, TCG CREST, Kolkata  Dr. Nilanjan Datta  IAI, TCG CREST, Kolkata  Cryptography  Dr. Nilanjan Datta  IAI, TCG CREST, Kolkata  Dr. Nilanjan Datta  IAI, TCG CREST, Kolkata  Cryptography  Dr. Nilanjan Datta  IAI, TCG CREST, Kolkata  Classification of Authenticated Encryption Modes				
Response Techniques   Session 2   Dr. Sanghamitra Pal   West Bengal State University   Session Chair   Session 3	2 pm to 3 pm.		r e e e e e e e e e e e e e e e e e e e	
Session 3	3 pm. to 4 pm.	Dr. Mrinal Nandi	West Bengal State University	** * *
11 to 12 moon	Day 2: 27.08.20	Dr. Sanghamitra Pal	West Bengal State University	Session Chair
Application	Session 3			
Session 4  2 pm. to 3 pm.  2 pm. to 4 pm.  Dr. Arpita Maitra  Dr. Arjit Dutta  Session Chair  Dr. Avijit Dutta  Session 5  3 pm. to 4 pm.  Dr. Rishiraj Bhattacharya  Dr. Dr. Dr. Donghoon Chang  Dr. Avik Chakraborti  Session 6  11 to 12 noon  Dr. Sucheta Chakrabarti  Dr. Sumanta Adhya  Dr. Sumanta Adhya  Dr. Sumanta Adhya  Dr. Dr. Sumanta Adhya  Dr.	11 to 12 noon	Dr. Avijit Dutta	IIT, Kharagpur	
Session 4   Prof. Mridul Nandi   Session Chair	12 to 1 pm.	Prof. Avishek Adhikari	Presidency University	
Sanadhya  3 pm. to 4 pm.  Dr. Arpita Maitra  IAI, TCG CREST, Kolkata  Quantum Supremacy and its implication to cryptology  Session 5  3 pm. to 4 pm.  Dr. Avijit Dutta  Session Chair  Session Chair  Session Chair  Session Chair  Session Chair  Session Chair  Dr. Rishiraj Bhattacharya  Dr. Donghoon Chang  Attional Institute of Standards and Technology, USA  Dr. Avik Chakraborti  Session 6  Dr. Avik Chakraborti  Dr. Sucheta Chakrabarti  DRDO  Dr. Sucheta Chakrabarti  DRDO  Dr. Sumanta Adhya  Dr. Indivar Gupta  Dr. Dr. Indivar Gupta  Dr. Avik Chakraborti  DRDO  Dr. Avik Chakraborti  Session 8  IIT, Bhilai  The Curious Case of Embedding Yoyo within Boomerang  Session 9  Prof. Avishek Adhikari  Dr. Sikhar Patranabis  ETH Zurich, Switzerland  Minicrypt Primitives with Algebraic Structures  Classification of Authenticated Encryption Modes  III, TCG CREST, Kolkata  Quantum Supremacy and its implication to cryptology  Session Chair  Cryptography with the space-time constraints  Post-snowden cryptography introduction of cube attacks on MAC and AFAD schemes  Session Chair  Session 6  Dr. Avik Chakraborti  DRDO  Algebraic Structures and its applications in Cryptology  Session 7  Dr. Indivar Gupta  DRDO  Public Key Cryptography  Session Chair  Session 8  IIT, Bhilai  The Curious Case of Embedding Yoyo within Boomerang  Security of Things and their Low Cost Authenticated Interaction in the world of IoT  Session 9  Prof. Avishek Adhikari  Dr. Sikhar Patranabis  ETH Zurich, Switzerland  Minicrypt Primitives with Algebraic Structures  Algebraic Structures  Classification of Authenticated Encryption Modes	Session 4	Prof. Mridul Nandi		_
Implication to cryptology   Day 3: 28.08.20   Dr. Avijit Dutta   Session 5	2 pm. to 3 pm.		IIT, Ropar	Format preserving encryption
Day 3: 28.08.20   Session 5   Session Chair	3 pm. to 4 pm.	Dr. Arpita Maitra	IAI, TCG CREST, Kolkata	*
3 pm. to 4 pm.  Dr. kaushik Chakraborty Netherlands  Dr. Rishiraj Bhattacharya NISER, Bhubaneswar  Dr. Dr. Donghoon Chang Dr. Donghoon Chang Dr. Donghoon Chang Dr. Avik Chakraborti Session 6  Dr. Sourav Sengupta Dr. Sucheta Chakrabarti DRDO Dr. Sumanta Adhya Dr. Dr. Indivar Gupta Dr. Dr. Avik Chakraborti Dr. Dr. Avik Chakraborti Dr. Dr. Sumanta Adhya Dr. Dr. Sumanta Adhya Dr. Dr. Sucheta Chakrabarti DRDO Dr. Sumanta Adhya Dr. Dr. Sucheta Chakrabarti DRDO Dr. Sumanta Adhya Dr. Dr. Sucheta Chakrabarti DRDO Dr. Sumanta Adhya Dr. Dr. Hidivar Gupta DRDO Dr. Sucheta Chakrabarti DRDO Dr. Sucheta Chakrabarti DRDO Dr. Sumanta Adhya Dr. Jor. Hidivar Gupta DRDO Dr. Avik Chakraborti Dr. Sucheta Chakrabarti Dr. Sucheta Chakrabarti Session 8  Dr. Sucheta Chakrabarti Dr	Day 3: 28.08.20	Dr. Avijit Dutta		
Netherlands   time constraints	Session 5			
5 pm. to 6 pm.  Dr. Donghoon Chang National Institute of Standards and Technology, USA  Day 4: 29.08.20 Session 6  Dr. Avik Chakraborti Session 6  Dr. Sourav Sengupta Nanyang Technological University, Singapore  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. Avik Chakraborti DRDO Public Key Cryptography  3 pm. to 4 pm. Dr. Avik Chakraborti Session 8  Dr. Sucheta Chakrabarti Session Chair  The Curious Case of Embedding Yoyo within Boomerang  12 to 1 pm. Prof. Debdeep Mukhopadhyay  IIT, Kharagpur Session Chair Session 9 Prof. Avishek Adhikari 2 pm. to 3 pm. Dr. Sikhar Patranabis ETH Zurich, Switzerland Algebraic Structures Classification of Authenticated Encryption Modes	3 pm. to 4 pm.	Dr. kaushik Chakraborty	• • • • • • • • • • • • • • • • • • • •	
and Technology, USA  MAC and AEAD schemes  Day 4: 29.08.20 Session 6  Dr. Avik Chakraborti  Session Chair  Session Chair  Bitcoin and Cryptocurrencies University, Singapore  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  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 loT  Session 9 Prof. Avishek Adhikari Dr. Sikhar Patranabis ETH Zurich, Switzerland Algebraic Structures  J pm. to 4 pm. Dr. Nilanjan Datta IAI, TCG CREST, Kolkata Classification of Authenticated Encryption Modes	4 pm. to 5 pm.	Dr. Rishiraj Bhattacharya	NISER, Bhubaneswar	post-snowden cryptography
Day 4: 29.08.20   Dr. Avik Chakraborti   Session Chair	5 pm. to 6 pm.	Dr. Donghoon Chang		
Dr. Sourav Sengupta   Nanyang Technological University, Singapore   Bitcoin and Cryptocurrencies	Day 4: 29.08.20	Dr. Avik Chakraborti	337	
University, Singapore  Dr. Sucheta Chakrabarti DRDO Algebraic Structures and its applications in Cryptology  Session 7 Dr. Sumanta Adhya West Bengal State University Session Chair  DRDO Public Key Cryptography  The Sumanta Adhya Dr. Avik Chakraborti DRDO Dr. Avik Chakraborti Dr. Avik Chakraborti Dr. Sucheta Chakrabarti Session 8  IIT, Bhilai The Curious Case of Embedding Yoyo within Boomerang  Dr. Dhiman Saha IIT, Bhilai The Curious Case of Embedding Yoyo within Boomerang  The Curious Case of Embedding Yoyo within Boomerang  Dr. Debdeep Mukhopadhyay The Curious Case of Embedding Yoyo within Boomerang  Dr. Session 9 Prof. Avishek Adhikari Session Chair  Session 9 Prof. Avishek Adhikari ETH Zurich, Switzerland Minicrypt Primitives with Algebraic Structures  The Curious Case of Embedding Yoyo within Boomerang  Dr. Sikhar Patranabis ETH Zurich, Switzerland Minicrypt Primitives with Algebraic Structures  Algebraic Structures  Classification of Authenticated Encryption Modes	Session 6			
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 Dr. Sucheta Chakrabarti Session 8  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 Classification of Authenticated Encryption Modes	11 to 12 noon	Dr. Sourav Sengupta		Bitcoin and Cryptocurrencies
Session 7Dr. Sumanta AdhyaWest Bengal State UniversitySession Chair2 pm. to 3 pm.Dr. Indivar GuptaDRDOPublic Key Cryptography3 pm. to 4 pm.Dr. Avik ChakrabortiISI, KolkataWhite box CryptographyDay 2: 30.08.20 Session 8Dr. Sucheta ChakrabartiSession Chair11 to 12 noonDr. Dhiman SahaIIT, BhilaiThe Curious Case of Embedding Yoyo within Boomerang12 to 1 pm.Prof. Debdeep MukhopadhyayIIT, KharagpurSecurity of Things and their Low Cost Authenticated Interaction in the world of IoTSession 9Prof. Avishek AdhikariSession Chair2 pm. to 3 pm.Dr. Sikhar PatranabisETH Zurich, SwitzerlandMinicrypt Primitives with Algebraic Structures3 pm. to 4 pm.Dr. Nilanjan DattaIAI, TCG CREST, KolkataClassification of Authenticated Encryption Modes	12 to 1 pm.	Dr. Sucheta Chakrabarti	DRDO	
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 Dr. Sucheta Chakrabarti Session 8  11 to 12 noon Dr. Dhiman Saha IIT, Bhilai The Curious Case of Embedding Yoyo within Boomerang 12 to 1 pm. Prof. Debdeep Mukhopadhyay 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 Classification of Authenticated Encryption Modes	Session 7	Dr. Sumanta Adhya	West Bengal State University	**
3 pm. to 4 pm.  Dr. Avik Chakraborti  Day 2: 30.08.20 Session 8  Dr. Sucheta Chakrabarti Session 8  IIT, Bhilai  The Curious Case of Embedding Yoyo within Boomerang  IIT, Kharagpur  Security of Things and their Low Cost Authenticated Interaction in the world of IoT  Session 9  Prof. Avishek Adhikari  Prof. Session Chair  Session Chair  Security of Things and their Low Cost Authenticated Interaction in the world of IoT  Session 9  Prof. Avishek Adhikari  ETH Zurich, Switzerland  Minicrypt Primitives with Algebraic Structures  3 pm. to 4 pm.  Dr. Nilanjan Datta  IAI, TCG CREST, Kolkata  Classification of Authenticated Encryption Modes		•		
Day 2: 30.08.20 Session 8Dr. Sucheta ChakrabartiSession Chair11 to 12 noonDr. Dhiman SahaIIT, BhilaiThe Curious Case of Embedding Yoyo within Boomerang12 to 1 pm.Prof. Debdeep MukhopadhyayIIT, KharagpurSecurity of Things and their Low Cost Authenticated Interaction in the world of IoTSession 9Prof. Avishek AdhikariSession Chair2 pm. to 3 pm.Dr. Sikhar PatranabisETH Zurich, SwitzerlandMinicrypt Primitives with Algebraic Structures3 pm. to 4 pm.Dr. Nilanjan DattaIAI, TCG CREST, KolkataClassification of Authenticated Encryption Modes				
Session 8  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  Dr. Sikhar Patranabis  ETH Zurich, Switzerland  Minicrypt Primitives with Algebraic Structures  3 pm. to 4 pm.  Dr. Nilanjan Datta  IAI, TCG CREST, Kolkata  Classification of Authenticated Encryption Modes	^ ^		101, KUIKAIA	
11 to 12 noon  Dr. Dhiman Saha  IIT, Bhilai  The Curious Case of Embedding Yoyo within Boomerang  12 to 1 pm.  Prof. Debdeep Mukhopadhyay  Bession 9  Prof. Avishek Adhikari  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  Classification of Authenticated Encryption Modes	•	DI. Sucheta Chakradard		SESSION CHAIT
12 to 1 pm.  Prof. Debdeep Mukhopadhyay  Prof. Avishek Adhikari  2 pm. to 3 pm.  Dr. Sikhar Patranabis  ETH Zurich, Switzerland  Dr. Nilanjan Datta  IIT, Kharagpur  Security of Things and their Low Cost Authenticated Interaction in the world of IoT  Session Chair  Minicrypt Primitives with Algebraic Structures  IAI, TCG CREST, Kolkata  Classification of Authenticated Encryption Modes		Dr. Dhiman Saha	IIT, Bhilai	
Mukhopadhyay  Cost Authenticated Interaction in the world of IoT  Session 9  Prof. Avishek Adhikari  Session Chair  Dr. Sikhar Patranabis  ETH Zurich, Switzerland  Minicrypt Primitives with Algebraic Structures  3 pm. to 4 pm.  Dr. Nilanjan Datta  IAI, TCG CREST, Kolkata  Classification of Authenticated Encryption Modes	12 to 1 nm	Prof Dehdeen	HT Kharagnur	,
Session 9Prof. Avishek AdhikariSession Chair2 pm. to 3 pm.Dr. Sikhar PatranabisETH Zurich, SwitzerlandMinicrypt Primitives with Algebraic Structures3 pm. to 4 pm.Dr. Nilanjan DattaIAI, TCG CREST, KolkataClassification of Authenticated Encryption Modes	12 to 1 pm.	•	111, Kilaragpur	Cost Authenticated Interaction in
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  Classification of Authenticated Encryption Modes	Session 9	Prof. Avishek Adhikari		
3 pm. to 4 pm. Dr. Nilanjan Datta IAI, TCG CREST, Kolkata Classification of Authenticated Encryption Modes			ETH Zurich, Switzerland	Minicrypt Primitives with
	3 pm. to 4 pm.	Dr. Nilanjan Datta	IAI, TCG CREST, Kolkata	Classification of Authenticated
	Vote of Thanks	Dr. Sibnarayan Guria	West Bengal State University	Ziterypiton Wodes