Indo Japan Joint Workshop on Cryptography
12th December, 2009

9.30 -10.00	*Inauguration*	
10.00- 10.30	*Tea*	
10.30-11.00	*Constructions of some Multi-Secret Sharing Schemes*	Avishek Adhikari
11.30-12.00	*Hash Function Combiners*	Rishiraj Bhattacharyya
12.00-12.30	*Topic To be Decided*	Naveen Chaudhary
12.00 -12.30	*Tea*	
12.30-13.00	*Some Hot Topics on Code-Based Public-Key Cryptosystems*	Prof. Kazukuni Kobara
13.00-13.30	*Efficient Constructions of Deterministic Encryption from Hybrid Encryption and Code-Based PKE*	Yang Cui
13.30-14.30	*LUNCH*	
14.30- 15.00	*Multiparty Computation for Interval, Equality, and Comparison Without Bit-Decomposition Protocol*	Takashi Nishide
15.00- 15.30	*On Botnet Detection using Sparse Structure Learning*	Junichi Takeuchi
15.30- 16.00	*Undeniable Signatures with Delegatable Verification*	Jacob Schuldt
16.00-16.30	*Tea*	
16.30-17.00	*Topic To Be Decided*	Subhamoy Maitra
17.00-17.30	*Third-order nonlinearities of a subclass of Kasami functions*	Sugata Gangopadhyay
17.30-18.00	*Secret Key Recovery of Keystream Generator LILI-128 Based on a Novel Weakness of the Employed Boolean Function*	Miodrag Mihaljevic