

Curriculum Vitae

Palash Sarkar
Professor
Applied Statistics Unit

Sanjit Chatterjee (PhD 2006).

Dissertation: Construction of (Hierarchical) Identity Based Encryption Protocols Using Bi-

6. **Cryptology and Data Security**, Aug{Dec, 1999, 2002, 2003.
7. **Discrete Mathematics-I (Algebraic Structures)**, Aug{Dec, 1999.
8. **Discrete Mathematics-II (Combinatorics, Graph Theory and Logic)**, Aug{Dec, 1996, 1997, 1998, 2006, 2007.
9. **Design and Analysis of Algorithms**, MTech (CS), Jan{May, 1998, 1999, 2002.
10. **Selected Topics in Algorithms and Complexity**, MTech (CS), Jan{May, 1999, 2009.
11. **Theory of Automata, Languages, Computability and Complexity**, MTech (CS), Jan{May, 1997, 2000, 2005.
12. **Programming in Assembly and Systems Programming**, MTech (CS), Aug-Dec, 1995.
13. **Information Storage and Retrieval (C Programming and Database)**

7 Editorial Work

1. **Program co-chair and co-editor** (with Professor Alfred Menezes) for the **proceedings of Indocrypt 2002**, published by **Springer-Verlag** in the **Lecture Notes in Computer Science** series, number 2551.
2. **Program committee member** for **Crypto 2010, 2007**; annual North American conference of the

9 Publications

9.1 Book Chapters and Expository Articles

1. Sanjit Chatterjee and Palash Sarkar. Identity-Based Encryption and Hierarchical Identity-Based Encryption. In **Identity-Based Cryptography**, An edited volume of IOS Press

9. Debrup Chakraborty and Palash Sarkar. A General Construction of Tweakable Block Ciphers and Different Modes of Operations. **IEEE Transactions on Information Theory**, 54(5): 1991{2006 (2008).

22. Rana Barua and Palash Sarkar, On the Kernel of First Order Correlation Immune Boolean Functions, **Journal of Indian Statistical Association**, special issue on cryptology, Volume 42, Number 2, December 2004, pages 131-143.

45. Somitra Kumar Sanadhya and Palash Sarkar. A New Hash Family Obtained by Modifying the SHA-2 Family. **Proceedings of ACM Symposium on Information, Computer and Communications Security (ASIACCS '09)**, pages 353{363.
46. (*) Somitra Kumar Sanadhya and Palash Sarkar. New Collision attacks Against Up To 24-step

57. Sanjit Chatterjee and Palash Sarkar. Multi-Receiver Identity-Based Key Encapsulation with Shortened Ciphertext, **Proceedings of Indocrypt 2006**, LNCS, volume 4329, pp 394{408.
58. Sourav Mukhopadhyay and Palash Sarkar. On the Effectiveness of TMTO and Exhaustive Search Attacks, **Proceedings of the First International Workshop on Security**, LNCS, volume 4266, pp 337{352.

69. (*) Palash Sarkar. Masking Based Domain Extenders for UOWHFs: Bounds and Constructions, **Proceedings of Asiacrypt 2004**, LNCS 3329, pp. 187-200, 2004.

82. (*) Kishan Chand Gupta and Palash Sarkar. Construction of Perfect Nonlinear and Maximally

96. Palash Sarkar, Bimal K. Roy, Pabitra Pal Choudhury. VLSI Implementation of Modulo Multi-