

WANG Huaxiong
Associate Professor
Division of Mathematical Sciences
School of Physical and Mathematical Sciences
PhD (Math) University of Haifa, Israel
PhD (Comp. Sci.) University of Wollongong, Australia



Major Research Interest: **Cryptography, Information Security
Coding, Combinatorics, Theoretical Computer Science**

Email: hxwang@ntu.edu.sg
<http://www.ntu.edu.sg/home/hxwang/>
Tel: (65) 67903733

Secure Multi-Party Computation

Secure multi-party computation (MPC) allows a set of players to compute an arbitrary function of their private inputs. The computation guarantees the correctness of the result while preserving the privacy of the players' inputs, even if some of the players are corrupted by an adversary and misbehave in an arbitrary and malicious way. Almost any distributed cryptographic protocol can be realised using a general MPC protocol. We are interested in developing theories, techniques and tools that can be used for analysis and assessment of secure MPCs; and design efficient and practical MPCs for different real-life applications.

Security Service for Group-oriented Communication

Multicast communication is a relatively recent mode of communication that allows a sender to efficiently broadcast a message to a group of users. It has been becoming the basis for a growing number of applications such as broadcasting stock quotes, special sporting events, Internet news, and pay TV. It is therefore critical to provide sound security mechanisms for multicast communication. Yet, existing security protocols for multicast offer only partial solutions. Our research goal is to provide the two basic security services, secrecy and authentication, in the context of multicast stream communication.

Algebraic Cryptanalysis

The aims of our research are: (i) to apply the algebraic attacks to Rijndael, the new proposed Advanced Encryption Standard (AES), to Serpent (the second algorithm in the AES competition), and to other algorithms including hash functions; (ii) to develop a theoretical framework for algebraic cryptanalysis of modern private-key cryptographic algorithms; (iii) to search for new more efficient factoring algorithms using algebraic approach; (iv) to develop new design criteria for S-boxes that provide immunity against algebraic attacks.



Applications of coding theory and cryptography range from correcting scratches and dust for a music CD, correcting the fading and noise of high frequency radio transmission in the Cell phones conversations, to ATM cards, computer passwords, and on-line payments

Selected Publications

Tartary, C, and H Wang, Efficient Multicast Stream Authentication for Fully Adversarial Network Model. International Journal of Security and Networks (IJSN) - Special Issue on Cryptography in Networks, (in press, 2007).

Tilborg van H, J Pieprzyk, R Steinfeld and H Wang, New Constructions of Anonymous Membership Broadcasting Schemes. Advances in Mathematics of Communications, 1:1, 29 - 44 (2007).

Steinfeld R, J Pieprzyk and H Wang, Lattice-Based Threshold-Changeability for Standard CRT Secret-Sharing Schemes. Finite Fields and Their Applications, 12:4, 653 - 680 (2006).

Wang H and J Pieprzyk, Shared generation of pseudo-random functions. Journal of Complexity, 20, 458 - 472 (2004).

Wang H, C Xing and R Safavi-Naini, Linear Authentication Codes: Bounds and Constructions. IEEE Trans. on Info. Theory, Vol. 49, No. 4, 866-872 (2003).

Safavi-Naini R and H Wang, Multireceiver Authentication Codes: Model, Bounds, Constructions and Extensions, Information and Computation, Vol. 151, No. 1/2, 148-172 (1999).