ERCIM "Alain Bensoussan" Fellowship Scientific Report

Fellow: Yanling Chen
Visited Location: NTNU/Q2S
Duration of Visit: 9 months, 01/04/2009-31/12/2009

I - Scientific activity

The center NTNU/Q2S has provided a friendly and supporting platform for me, to learn from and exchange ideas with experts in related areas. I have enjoyed the intellectually stimulating atmosphere at Q2S at large.

In the first month, I gave a presentation at the Q2S Colloquium to introduce my research background and seek for potential cooperation. I soon found my belonging and joined the security group. At the weekly security group seminar, I had close discussions with colleagues of similar interest. I gave two presentations at the seminar, regarding my previous and ongoing research, respectively. Furthermore, due to the close collaboration between Q2S and the Department of Telematics, the Department of Electronics and Telecommunications, I also had the opportunity to attend the ITEM Colloquium and the monthly Information Security Meeting at the Department of Telematics. All these experiences have helped me to improve my knowledge and broaden my research horizon.

Roughly to say, my research activities during my fellowship period at Q2S involve the continuation of my earlier research work and new cooperation with Professor Svein J. Knapskog and Professor Danilo Gligoroski. My research activities center on security issues and can be divided in three subtopics. The first is to explore the optimum distance profiles of the linear codes [2], especially the second order Reed-Muller codes [2, 5, 6]. The aim of this work is to improve the fault-tolerant capability of the current communication or storage system. Our special interest in the second order Reed-Muller codes comes from the fact that the second order Reed-Muller codes of short length are used in the current CDMA systems. The second subtopic is to design code for the binary symmetric wiretap channel [4], so as to guarantee a certain provable security. This work not only presents theoretic results on the random coding which achieves asymptotic perfect secrecy, but also gives insight into the practical code construction for a secure transmission with limited information leakage. The third subtopic is on the Multivariate Quadratic Quasigroups (MQQs) [1], which are the basis of one class of public key cryptosystems. This work solves several open research problems about MQQs, concerning the construction, size and complexity of MQQs of specific types. It is worth mentioning that, this work is inspired by a talk given at the security group seminar by Rune Ødegård, a PhD student at Q2S.

With the generous financial supports from the ERCIM fellowship and Q2S, I have visited several conferences, where I disseminate my research results and learn the advances and the trends of the related research fields. Besides, during this fellowship period, I have been a reviewer of the 14th Nordic Conference on Secure IT Systems (NordSec'09) and a technical program committee member of the IEEE International Workshop on Management of Emerging Networks and Services (ICUMT'09). Now I am a member of the Networking Networking Women (N2Women) and a technical program committee member of the 1st International Workshop on QoS enable Sensor Networks (QoS2N2010).

II- Publication(s) during your fellowship

[1] Yanling Chen, Svein J. Knapskog and Danilo Gligoroski, *Multivariate Quadratic Quasigroups (MQQ): Construction, Bounds and Complexity*, Submitted to the 2010 International Symposium on Information Theory.

> **Abstract:** In this paper, we study a class of MQQs introduced by Gligoroski et al and solve several open research problems about MQQs. Our main contributions are threefold. The first is the construction of MQQs of higher orders which so far was an open problem. Secondly we give a lower bound on the number of MQQs. The last but not least, we refine the definition of MQQs of different types and characterize the complexity of MQQs, by introducing the notion of "MQQs of strict type", and we show that previously defined MQQs are all isotopes to our new category of MQQs of strict type. We also present constructions of MQQs of different types and a lower bound on their number.

[2] Yanling Chen and Han Vinck, *A Lower Bound on the Optimum Distance Profiles of the Second Order Reed-Muller Codes*, Submitted to the IEEE Transaction on Information Theory.

> **Abstract:** In this paper, we give a lower bound for the optimum distance profiles of the second order Reed-Muller code in the dictionary order and in the inverse dictionary order. In particular, we show that the bound is tight, in both orders for the codes of length equal to or less than 128, which improves the result given in [5]. To support our result, we present a constructive linear sub-code family, which can be considered as a complementary case of Corollary 17 of Ch. 15 in the coding book by MacWilliams and Sloane. As another interesting result, we derive an additive commutative group of the symplectic matrices with full rank.

[3] Yuan Luo, Han Vinck and Yanling Chen, *On the Optimum Distance Profiles about Linear Block Codes*, Appear in the IEEE Transaction on Information Theory, March, 2010.

> **Abstract:** In this paper, for some linear block codes, two kinds of optimum distance profiles are introduced to consider how to construct and then exclude (or include) the basis codewords one by one while keeping a distance profile as large as possible in a dictionary order (or in an inverse dictionary order respectively). The aim is to improve fault-tolerant capability by selecting sub-codes in communications and storage systems. One application is to serve a suitable code for the realization of the transport format combination indicators (TFCI) of CDMA systems. Another application is in the field of address retrieval on optical media.

[4] Yanling Chen and Han Vinck, *On the Binary Symmetric Wiretap Channel*, Appear in the Proceeding of the 2010 International Zurich Seminar on Communications, Zurich, March, 2010.

> **Abstract:** In this paper, we investigate the binary symmetric wiretap channel. We show that the secrecy capacity can be achieved by using random linear codes. Furthermore, we explore the coset coding scheme constructed by linear codes. As a result, we give an upper bound on the total information loss, which sheds light on the design of the applicable coset codes for the secure transmission with limited information leakage.

[5] Yanling Chen and Han Vinck, *The Optimum Distance Profiles of the Second Order Reed-Muller Codes*, Proceeding of the 2009 International Symposium on Information Theory, Seoul, Korea, June 28-July 3, 2009; (A slightly different version is in Proceeding of the 2nd International Workshop on Advances in Communications, Boppard am Rhein, Germany, May 13-15, 2009.)

> **Abstract:** In this paper, we give a lower bound for the optimum distance profiles of the second order Reed-Muller code in the dictionary order and in the inverse dictionary order. In particular, we investigate the second order Reed-Muller codes of length equal to or less than 256. We show that the bound is tight, in the dictionary order for the code of length equal to or less than 32, and in the inverse dictionary order for the codes of length equal to or less than 128.

[6] Yanling Chen and Han Vinck, *Uniqueness of the First Order Reed-Muller Code*, Proceeding of the 10th Winter School on Coding and Information Theory, Loen, Norway, March 29-April 3, 2009.

Abstract: In this paper, we prove that the first order Reed-Muller code is unique in the sense that any linear code with the same length, dimension and minimum distance must be the first order Reed-Muller code.

III -Attended Seminars, Workshops, and Conferences

1. Weekly Security Group Seminar at NTNU/Q2S.
2. Norsk Informasjonssikkerhetskonferanse (*NISK'09*) , November 23-25, 2009, Trondheim, Norway.
3. Norwegian Academy of Technological Sciences (*NTVA'09*) Technology Forum 2009, September 9, 2009, Trondheim, Norway.
4. 2009 IEEE International Symposium on Information Theory (*ISIT'09*), June 28-July 3, 2009, Seoul, Korea.
5. The 1st International Workshop on Security and Communication Networks (*IWSCN'09*), May 20-22, 2009, Trondheim, Norway.
6. Q2S Advisory Board Meeting and Planning Seminar, May 18-19, 2009, Trondheim, Norway.
7. The 2nd International Workshop on Advances in Communications (*IWAC'09*), May 13-15, 2009, Boppard am Rhein, Germany.
8. The 10th Winter School on Coding and Information Theory (*WSIT'09*), March 29-April 3, Loen, Norway.