ERCIM "Alain Bensoussan" Fellowship Scientific Report

Fellow: Yanling Chen
Visited Location: FhG-IESE
Duration of Visit: 9 months, 14/01/2010-13/10/2010

I - Scientific activity

For more than a decade, the Fraunhofer Institute for Experimental Software Engineering (FhG-IESE) has been enjoying a worldwide reputation for methods and processes based on empirical evidence. Out of the ivory tower and into the real world ─ this is a dream workplace for researchers to solve problems from the people and for the people.

I arrived at FhG-IESE in January 2010 with a warm welcome from Prof. Pretschner and his group members. The group is young, passionate and has great potential. It has been active not only in academic communications with top research institutes and laboratories, but also in close cooperation with enterprises enjoying global reputation. Thus it provides researchers with an ideal platform for performing basic research and empirical studies in close proximity to industrial practice.

With full support from Prof. Pretschner and FhG-IESE, I soon got settled in my new working environment and could devote myself to a new research topic: quantitative information flow. Nowadays, ever increasing amounts of digital data require procedures and mechanisms for secured access to and usage of that data. Experience has shown that prior declarations of obligations, which have long been in use in business transactions, only constitute limited means for avoiding damages resulting from unauthorized data usage. Current procedures are mostly limited to controlling access in the past and in the present. However, it is hardly possible to retroactively change the usage possibilities of data once they are in circulation, unless precautionary measures are taken. As a useful tool, the quantitative theory of information flow offers an attractive way to analyze or measure the data flow and hence gives insight into how to enforce limits on the dissemination of information. In the first month, I gave a presentation at the AG-Security group seminar to introduce some concepts in information theory that are favored in information flow measurement. Thereafter, I reviewed the most up-to-date literature on this topic so as to attain a thorough understanding of the problems and the progress achieved so far. As a summary of the investigation, I gave a report at the AG-Security group seminar regarding the concepts of quantitative information flow, some automatic approaches, the difficulty of the problem and possible new approaches under consideration. My work has provided the basis for combining usage control with quantitative information flow detection, which is now being explored in further projects. A special thank goes to Enrico Lovat, a Ph.D. student of Prof. Pretschner, for his willingness to help and brainstorm with me on relevant and irrelevant topics.

Besides, I am deeply grateful to Prof. Pretschner for his understanding and for granting me great freedom to continue my previous research. Thanks to the travel grant from the ERCIM fellowship, and generous financial support from FhG-IESE and NTNU/Q2S, I visited several conferences, where I disseminated my research results or acquired knowledge in related research fields. Besides, during this fellowship period, I have been a reviewer of the 2010 International Symposium on Information Theory and its Applications (ISITA2010), and a reviewer of the SAIEE Africa Research Journal. Moreover, I serve as a technical program committee member of the 2010 International Conference on Progress in Informatics and Computing (PIC2010), and a technical program committee member of the 2011 International Conference on Network Computing and Information Security (NCIS2011).

II- Publication(s) during the fellowship

[1] Yanling Chen, Svein J. Knapskog and Danilo Gligoroski, *Multivariate Quadratic Quasigroups (MQQ): Construction, Bounds and Complexity*, Appear in the Proceeding of the 6th China International Conference on Information Security and Cryptology, October, 2010.

> **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. 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, *Secrecy Coding for the Binary Symmetric Wiretap Channel*, Security and Communication Networks, Wiley Interscience, September, 2010. (An extended version of [5])

> **Abstract:** In this paper, we propose a random linear coding scheme which achieves the secrecy capacity of the binary symmetric wiretap channel. Further, we adopt the code structure of the linear coding scheme and explore the coset coding scheme constructed by binary linear codes. As a result, we give an upper bound on the total information loss of the coset coding scheme, which sheds light on design of applicable codes for secure transmission with limited information leakage over the wiretap channel.

[3] Yanling Chen and Han Vinck, *A Lower Bound on the Optimum Distance Profiles of the Second Order Reed-Muller Codes*, IEEE Transaction on Information Theory, September, 2010.

> **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. 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.

[4] Yuan Luo, Han Vinck and Yanling Chen, *On the Optimum Distance Profiles about Linear Block Codes*, 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.

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

III -Attended Seminars, Workshops, and Conferences

1. Weekly AG-Security Group Seminar at FhG-IESE.
2. Weekly Seminar from the Division of Information Systems at FhG-IESE.
3. The 6th China International Conference on Information Security and Cryptology (Inscrypt 2010), October 20-23, 2010, Shanghai, China.
4. Dagstuhl Seminar 10141on Distributed Usage Control, April 6-9, 2010, Dagstuhl, Germany.
5. 2010 International Zurich Seminar on Communications, March 3-5, 2010, Zurich, Switzerland.