MoCrySEN Workshop

Message from the Workshop Organizers

It is my great pleasure to welcome you to the first International Workshop on Modern Cryptography and Security Engineering (MoCrySEn) which takes place at the University of Economics of Prague, Czech Republic from August 20th - 24th , 2012. MoCrySEn aims to bring together researchers working in theoretical aspects of modern cryptography with professionals working on applied aspects of security engineering, particularly people involved in standardization and in industrial deployment of cryptography. The main goal of the workshop is to strengthen the dialogue between these two groups, which is currently perceived to be weak.

Ultimately, we aim to make a start on bridging the gap between what academic cryptographers believe should be the goals of cryptographic design and what is actually implemented in the real world. MoCrySEn intends to provide a better understanding of real-world cryptographic issues to the theoretical community, helping to inform their research and set new research challenges for the theoretical community and enable practitioners to develop a clearer view of the current state-of-the-art in cryptographic research and what it offers to practitioners.

This first edition of MoCrySEn welcomes papers ranging from symmetric and lattice-based cryptography to different protocols for security engineering and cryptographic principles for cloud-based storage.

Moreover, I am grateful to Nicolas Sendrier for accepting my invitation to present the state-of-the-art of code-base cryptography in terms of theory and practice. Last but not least, I would like to express my sincere gratitude to the members of the program committee since without their invaluable help and expertise this workshop would not have been possible. My thanks also extend to the AReS Organizers, in particular Edgar Weippl for providing a venue to MoCrySEn and Yvonne Poul for her assistance in various organization matters.

I hope you enjoy the sessions of MoCrySEn and wishing you a nice stay in the beautiful city of Prague!

The MoCrySEn 2012 Chair

Dimitris E. Simos, *INRIA, France*