

# Program – CosyProofs 2010

## Monday 12th April

- 9h15** : Welcome - Coffee  
**9h45** : Opening  
**10h00** : PH. ROGAWAY  
*Reconciling two views of cryptography*  
**12h00** : Lunch  
**14h30** : M. ABADI  
*Layout randomization and computational soundness*  
**15h10** : S. KREMER  
*Computational Soundness of Symbolic Security Proofs - (part I)*  
**16h10** : Coffee break  
**16h40** : S. KREMER  
*Computational Soundness of Symbolic Security Proofs - (part II)*  
**18h10** :

## Tuesday 13th April

- 9h00** : D. UNRUH  
*Composition of cryptographic protocols - (part I)*  
**10h30** : Coffee break  
**11h00** : D. UNRUH  
*Composition of cryptographic protocols - (part II)*  
**12h00** : Lunch  
**14h00** : CH. SPRENGER  
*Abstractions for Cryptographically Faithful Proofs of Security Protocols*  
**14h40** : G. BARTHE  
*CertiCrypt : Formal Proofs for Computational Cryptography - (part I)*  
**15h40** : Coffee break  
**16h10** : G. BARTHE  
*CertiCrypt : Formal Proofs for Computational Cryptography - (part II)*  
**17h40** :

## Wednesday 14th April

- 8h30** : R. CANETTI  
*Using composability to speed up automated security proofs - (part I)*  
**10h00** : Coffee break  
**10h30** : R. CANETTI  
*Using composability to speed up automated security proofs - (part II)*  
**11h30** : C. FOURNET  
*Formal/computational verification of protocol implementations by typing - (part I)*  
**12h30** : Lunch  
**14h30** : C. FOURNET  
*Formal/computational verification of protocol implementations by typing - (part II)*  
**16h00** : Coffee break

## Thursday 15th April

- 8h50** : Welcome  
**9h00** : T. OKAMOTO – *Hierarchical design and security proofs*  
**10h00** : H. SAKURADA , Y. KAWAMOTO, and M. HAGIYA  
*Bisimulation for the computational soundness of the applied pi calculus*  
**10h25** : H. COMON-LUNDH, M. HAGIYA, Y. KAWAMOTO, and H. SAKURADA  
*Proving computational soundness of the applied pi-calculus without using computable parsing*  
**10h50** : Coffee break  
**11h20** : M. YOSHIDA and T. FUJIWARA  
*All-or-Nothing Property for Efficient Symbolic Analysis*  
**11h45** : G. STEEL – *Verifying Security APIs by Typing*  
**12h10** : S. CIOBACA AND V. CORTIER – *Protocol composition for arbitrary primitives*  
**12h35** : Lunch  
**14h30** : R. KUSTERS and M. TUENGERHAL  
*Computational Soundness for Key Exchange Protocols with Symmetric Encryption*  
**14h55** : R. KUSTERS and M. TUENGERHAL  
*Extending an Ideal Symmetric encryption functionality*  
**15h20** : D. NOWAK and Y. ZHANG – *A calculus for game-based security proofs*  
**15h45** : H. COMON-LUNDH, S. KREMER, and J.-K. TSAY  
*Modular Soundness Proofs via Deduction Games*  
**16h10** : Coffee break  
**16h40** : B. BLANCHET – *Automatic, computational proof of EKE using CryptoVerif*  
**17h05** : G. BANA, K. HASEBE, and M. OKADA  
*Secrecy-Oriented First-Order Logical Analysis of Cryptographic Protocols*  
**17h30** : D. POINTCHEVAL  
*Smooth Projective Hash Functions and Security against Adaptive Corruptions*  
**17h55** : G. BARTHE, A. HEVIA, Z. LUO, T. REZK, and B. WARINSCHI  
*Robustness Guarantees for Anonymity*  
**18h20** :

## Friday 16th April

- 8h45** : Y. LAKHNECH – *Computational Indistinguishability Logic*  
**9h45** : S. STILLER  
*Protocol Composition Logic*  
**10h10** : Coffee break  
**10h45** : S. DELAUNE, S. KREMER, and O. PEREIRA  
*Simulation based security in the applied pi calculus*  
**11h10** : R. CANETTI AND S. GAJEK  
*Universally Composable Symbolic Analysis of Diffie-Hellman Key Exchange and Certification*  
**11h35** : T. ARARAGI and T. ITO  
*Application of Polynomially Accurate Simulation Relations to a Proof of UC Security : A Case Study of Group Key Exchange*  
**12h00** : Lunch  
**13h30** : Departure of the shuttle