Προτεινόμενα θέματα για project 2016-17

Προθεσμία επιλογής: 15/12/2016
Προθεσμία υποβολής: 7/1/2017

Η εργασία περιλαμβάνει προετοιμασία παρουσίασης 10 λεπτών (ενδεικτικά: 10-15 slides) και σύντομης αναφοράς (ενδεικτικά 3-5 σελίδες). Η αναφορά και η παρουσίαση θα πρέπει να παραδίδονται σε μορφή PDF. Μπορείτε να αναλαμβάνετε τα θέματα ατομικά ή σε ομάδες των δύο. Τα θέματα που ανατίθενται θα σημειώνονται με αστερίσκο (*).

Α. Θεωρητικά θέματα

I. Functional Encryption – Obfuscation
Susan Hohenberger, Amit Sahai, Brent Waters: Replacing a Random Oracle: Full Domain Hash from Indistinguishability Obfuscation. EUROCRYPT 2014: 201-220

Amit Sahai, Brent Waters: How to use indistinguishability obfuscation: deniable encryption, and more. STOC 2014: 475-484

Máté Horváth, Survey on Cryptographic Obfuscation, Cryptology ePrint Archive: Report 2015/412

II. Zero knowledge proofs and arguments
Groth, J., Ostrovsky, R., Sahai, A.: New Techniques for Non-interactive Zero Knowledge. Journal of the ACM 59(3) (2012)

Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Jens Groth: Efficient Zero-Knowledge Proof Systems. FOSAD 2016: 1-31

J. Groth, A Verifiable Secret Shuffle of Homomorphic Encryptions, J. Cryptology, 23(4), 2010, pp. 546-579.

III. Homomorphic encryption
Fully homomorphic encryption over the integers, M van Dijk, C Gentry, S Halevi, V Vaikuntanathan, Eurocrypt 2010

Fully homomorphic encryption with relatively small key and ciphertext sizes
NP Smart, F Vercauteren Public Key Crypto, 2010

R. Cramer, I. Damgard, and J.B. Nielsen. Multiparty computation from threshold homomorphic encryption. Eurocrypt 2001, http://iacr.org/archive/eurocrypt2001/20450279.pdf

IV. Cryptocurrencies

Juan A. Garay, Aggelos Kiayias, Nikos Leonardos: The Bitcoin Backbone Protocol: Analysis and Applications. EUROCRYPT (2) 2015: 281-310

Zerocash: Decentralized Anonymous Payments from Bitcoin, Eli Ben-Sasson Alessandro Chiesa Ian Miers Eran Tromer Christina Garman Madars Virza

TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub, Ethan Heilman, Leen Alshenibr, Foteini Baldimtsi, Alessandra Scafuro, Sharon Goldberg

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names Sarah Meiklejohn Marjori Pomarole Grant Jordan, Kirill Levchenko Damon McCoy, Geoffrey M. Voelker Stefan Savage

V. Elections

Aggelos Kiayias, Thomas Zacharias, Bingsheng Zhang: End-to-End Verifiable Elections in the Standard Model. EUROCRYPT (2) 2015: 468-498

Ηλεκτρονικές ψηφοφορίες στην Εσθονία (και τα 3 μαζί)
a. Security Analysis of the Estonian Internet Voting System, J. Alex Halderman, Harri Hursti, Jason Kitcat, Margaret MacAlpine, Travis Finkenauer, Drew Springall
b. Verifiable Internet Voting in Estonia, Sven Heiberg and Jan Willemson
c. Homomorphic Tallying for the Estonian Internet Voting System Arnis Parsovs

VI. Attacks

Crying Wolf: An Empirical Study of SSL Warning Effectiveness

I Am Robot: (Deep) Learning to Break Semantic Image CAPTCHAs, Suphannee Sivakorn, Iasonas Polakis and Angelos D. Keromytis

On the Practical (In-)Security of 64-bit Block Ciphers Collision Attacks on HTTP over TLS and OpenVPN, Karthikeyan Bhargavan and Gaëtan Leurent, https://sweet32.info/SWEET32_CCS16.pdf

A Systematic Analysis of the Juniper Dual EC Incident, Stephen Checkoway (University of Illinois at Chicago), Jacob Maskiewicz (UC San Diego), Christina Garman (Johns Hopkins University), Joshua Fried (University of Pennsylvania), Shaanan Cohney (University of Pennsylvania), Matthew Green (Johns Hopkins University), Nadia Heninger (University of Pennsylvania), Ralf-Philipp Weinmann (Comsecuris), Eric Rescorla and Hovav Shacham (UC San Diego)

VII. Theoretical Foundations

Christoph Bader, Tibor Jager, Yong Li, Sven Schäge (Ruhr-Universität Bochum), On the Impossibility of Tight Cryptographic Reductions. EUROCRYPT 2016.

Ran Canetti, Oded Goldreich, Shai Halevi: The random oracle methodology, revisited. J. ACM 51(4): 557-594 (2004)

Divesh Aggarwal, Ueli Maurer: Breaking RSA Generically Is Equivalent to Factoring. IEEE Trans. Information Theory 62(11): 6251-6259 (2016)

VIII. Pairings

D. Boneh and M. K. Franklin, Identity based encryption from the Weil pairing, SIAM J. Comput., Vol. 32, 2003.

D. Boneh, B. Lynn and H. Shacham, Short signatures from the Weil pairing, ASIACRYPT 2001 or Journal of Cryptology, Vol. 17, 2004.

IX. Rational Cryptography / Secure Multi-party Computation

Rational protocol design: Cryptography against incentive-driven adversaries
J Garay, J Katz, U Maurer, B Tackmann, V Zikas, Foundations of Computer Science (FOCS), 2013

Gillat Kol, Moni Naor. Cryptography and Game Theory: Designing Protocols for Exchanging Information. TCC'08, pp. 320-339.

Lysyanskaya A, Triandopoulos N (2006) Rationality and adversarial behavior in multi-party computation. In: Dwork C (ed) CRYPTO 2006. Springer, Heidelberg, pp 180–197

Halpern J, Teague V (2004) Rational secret sharing and multiparty computation: extended abstract. In: STOC ’04: proceedings of the thirty-sixth annual ACM symposium on theory of computing. ACM, New York, NY, USA, pp 623–632

Sequential Rationality in Cryptographic Protocols, Ronen Gradwohl, Noam Livne, Alon Rosen, FOCS 2010.

Β. Προγραμματιστικά θέματα

Υλοποίηση πρωτοκόλλου ηλεκτρονικής ψηφοφορίας με mixnet.

Υλοποίηση πρωτοκόλλου ηλεκτρονικής ψηφοφορίας με blind signatures.

Υλοποίηση συστήματος ανώνυμης πιστοποίησης (anonymous credentials) με blind signatures.

Υλοποίηση συστήματος αξιολόγησης / ψηφοφορίας με χρήση ανώνυμης πιστοποίησης.

Υλοποίηση app για secure mobile messaging.

Υλοποίηση app για secure chat (OTR).

Προσομοίωση κατανεμημένων αλγορίθμων για προβλήματα τύπου Byzantine Agreement / Reliable Broadcast.

Υλοποιήσεις σχετικές με bitcoin / digital currency.

Υλοποίηση smart contract σε Ethereum.