Crypto Projects 2018-2019

I. Θεωρητικά

1. SoK: A Consensus Taxonomy in the Blockchain Era, Juan Garay and Aggelos Kiayias, https://eprint.iacr.org/2018/754 [Κυτέας Απόστολος, ΗΜΜΥ]
2. Prime and Prejudice: Primality Testing Under Adversarial Conditions, Martin R. Albrecht and Jake Massimo and Kenneth G. Paterson and Juraj Somorovsky, https://eprint.iacr.org/2018/749 [Σαντοριναίος Χριστόδουλος ΗΜΜΥ]
3. Verifiable Delay Functions, Dan Boneh, Joseph Bonneau, Benedikt Bünz, Ben Fisch, https://eprint.iacr.org/2018/601[Διαμαντίδης Δημήτρης ΣΕΜΦΕ]
4. Pinocchio: Nearly practical verifiable computation. Parno, B., Howell, J., Gentry, C., Raykova, M. (2013, May). In Security and Privacy (SP), 2013 IEEE Symposium on (pp. 238-252). https://eprint.iacr.org/2013/279.pdf
5. Steven Goldfeder, Harry Kalodner, Dillon Reisman, Arvind Narayanan: When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies, https://arxiv.org/abs/1708.04748, [ΒΑΣΙΛΕΙΟΣ ΜΑΡΚΟΠΟΥΛΟΣ ΕΜΕ]
6. Private Intersection-Sum Protocol with Applications to Attributing Aggregate Ad Conversions, Mihaela Ion and Ben Kreuter and Erhan Nergiz and Sarvar Patel and Shobhit Saxena and Karn Seth and David Shanahan and Moti Yung, https://eprint.iacr.org/2017/738 [ΣΤΑΘΑΤΟΣ ΝΙΚΗΤΑΣ ΣΕΜΦΕ]
7. Lysyanskaya A, Triandopoulos N (2006). Rationality and adversarial behavior in multi-party computation. In: Dwork C (ed) CRYPTO 2006. Springer, Heidelberg, pp 180–197. http://www.cs.bu.edu/~nikos/papers/RCMPC-Crypto06.pdf
8. Ronen Gradwohl, Noam Livne, Alon Rosen. Sequential Rationality in Cryptographic Protocols. FOCS 2010. [Αργύρης Μουζάκης (ΗΜΜΥ)]
9. Chou, T. and Orlandi, C., 2015, August. The simplest protocol for oblivious transfer. In International Conference on Cryptology and Information Security in Latin America (pp. 40-58). https://eprint.iacr.org/2015/267.pdf [ΘΕΟΧΑΡΟΥΣ ΛΕΩΝΙΔΑΣ ΣΕΜΦΕ]

10. Herlihy, M. (2018). Atomic cross-chain swaps. arXiv preprint arXiv:1801.09515. [OIKONOMOU CHRYSA (ECE)]
11. Zamyatin, A., Harz, D., Lind, J., Panayiotou, P., Gervais, A., & Knottenbelt, W. J. Xclaim: Interoperability with cryptocurrency-backed tokens. Cryptology ePrint Archive, Report 2018/643, 2018. https://eprint. iacr. org/2018/643. [Porandokht Behrouz]
12. David A. McGrew and John Viega: The Security and Performance of the Galois/Counter Mode of Operation (Full Version), Cryptology ePrint Archive: Report 2004/193, https://eprint.iacr.org/2004/193 [Μιχάλης Ξεφτέρης (ΗΜΜΥ)]

13. Silvio Micali. ALGORAND: the efficient and democratic ledger. CoRR, abs/1607.01341, 2016.
14. Miguel Castro and Barbara Liskov, Practical Byzantine Fault Tolerance. MIT, 1999. pdf [Αλιρεζα Χακσαρι]
15. Leslie Lamport. Fast paxos. Distributed Computing, 19(2):79–103, October 2006. https://www.microsoft.com/en-us/research/publication/fast-paxos/
16. David Mazieres, The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus. Stellar Development Foundation, 2016. Link: [Νιμαρα Δημητρης ΣΕΜΦΕ] https://www.stellar.org/developers/guides/concepts/scp.html

II. Προγραμματιστικά

17. Υλοποίηση Publicly Auditable Conditional Blind Signatures, από: Towards everlasting privacy and efficient coercion resistance in remote electronic voting https://fc18.ifca.ai/voting/papers/GPZZ18.pdf [ΚΑΤΣΑΡΟΥ ΠΑΝΑΓΙΩΤΑ ΦΙΛΙΤΣΑ (ΣΕΜΦΕ)]

18. Βελτιώσεις / επεκτάσεις σε σύστημα ψηφοφοριών κατάταξης -- βλ. διπλωματική Θ. Σουλιώτη, http://artemis.cslab.ece.ntua.gr:8080/jspui/handle/123456789/13362 [ΤΣΑΚΟ ΜΑΡΙΟΥΣ ECE]
19. Βελτιώσεις / επεκτάσεις στο OTR / mpOTR -- βλ. διπλωματική Α. Ανδρικόπουλου - Δ. Κολοτούρου, http://artemis.cslab.ece.ntua.gr:8080/jspui/handle/123456789/13301
20. Ανώνυμα ερωτηματολόγια με χρήση ομομορφικής κρυπτογραφίας, βλ. και ANONIZE http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6956576
21. Υλοποίηση smart contracts σε Ethereum -- δείτε περισσότερες πληροφορίες εδώ: http://solidity.readthedocs.io/en/develop/introduction-to-smart-contracts.html [ΙΩΑΝΝΗΣ ΑΣΜΑΝΗΣ + ΑΘΗΝΑΓΟΡΑΣ ΣΚΙΑΔΟΠΟΥΛΟΣ (ECE NTUA UNDERGRAD)]