Crypto Projects 2021-22

Ι. Θεωρητικά

1. *Ryan Amos and Marios Georgiou and Aggelos Kiayias and Mark Zhandry.* **One-shot Signatures and Applications to Hybrid Quantum/Classical Authentication.** <https://eprint.iacr.org/2020/107>
2. *Juan Garay, Aggelos Kiayias, and Nikos Leonardos*. **Full Analysis of Nakamoto Consensus in Bounded-Delay Networks.** <https://eprint.iacr.org/2020/277>
3. *Erica Blum, Aggelos Kiayias, Cristopher Moore, Saad Quader, Alexander Russell*. **The Combinatorics of the Longest-Chain Rule: Linear Consistency for Proof-of-Stake Blockchains.** SODA 2020: 1135-1154. <https://eprint.iacr.org/2017/241.pdf>
4. *Dan Boneh and Elette Boyle and Henry Corrigan-Gibbs and Niv Gilboa and Yuval Ishai.* **Zero-Knowledge Proofs on Secret-Shared Data via Fully Linear PCPs.** <https://eprint.iacr.org/2019/188>
5. *Benedikt Bünz and Shashank Agrawal and Mahdi Zamani and Dan Boneh.* **Zether: Towards Privacy in a Smart Contract World.** <https://eprint.iacr.org/2019/191>
6. *Maksim Tsikhanovich, Malik Magdon-Ismail, Muhammad Ishaq, Vassilis Zikas.* **PD-ML-Lite: Private Distributed Machine Learning from Lightweight Cryptography.** [CoRR abs/1901.07986](https://arxiv.org/abs/1901.07986) (2019)
7. *Thomas Haines and Johannes Mueller,* **SoK: Techniques for Verifiable Mix Nets,** IEEE Computer Security Foundations Symposium, 2020.  
   <https://orbilu.uni.lu/bitstream/10993/45022/1/main.pdf>
8. *Eleanor McMurtry and Olivier Pereira and Vanessa Teague,* **When is a test not a proof?** European Symposium on Research in Computer Security, 2020.  
   [https://eprint.iacr.org/2020/909](https://eprint.iacr.org/2020/909.pdf)
9. *Chelsea Komlo and Ian Goldberg.* **FROST: Flexible Round-Optimized Schnorr Threshold Signatures,** [https://eprint.iacr.org/2020/852](https://eprint.iacr.org/2020/852.pdf)
10. *Leonie Reichert and Samuel Brack and Björn Scheuermann.* **A Survey of Automatic Contact Tracing Approaches Using Bluetooth Low Energy.** [https://eprint.iacr.org/2020/672](https://eprint.iacr.org/2020/672.pdf)
11. *Ashley Fraser and Elizabeth A. Quaglia,* **Protecting the Privacy of Voters: New Definitions of Ballot Secrecy for E-Voting,** Selected Areas in Cryptography (SAC), 2020**,** <https://eprint.iacr.org/2020/1332>
12. *Elizabeth C. Crites and Mary Maller and Sarah Meiklejohn and Rebekah Mercer,* **Reputable List Curation from Decentralized Voting,** Privacy Enhancing Technologies Symposium (PETS) 2020, <https://eprint.iacr.org/2020/709>
13. *Yehuda Lindell, Benny Pinkas, Nigel P. Smart, Avishay Yanai*: **Efficient Constant-Round Multi-party Computation Combining BMR and SPDZ**. J. Cryptology 32(3): 1026-1069 (2019) [2 άτομα]
14. 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.tau.ac.il/~fiat/crypt07/papers/mmpc.pdf>
15. Herlihy, M. (2018). **Atomic cross-chain swaps.** arXiv preprint arXiv:1801.09515.
16. Shay Gueron, Yehuda Lindell, Ariel Nof, Benny Pinkas: **Fast Garbling of Circuits Under Standard Assumptions**. J. Cryptology 31(3): 798-844 (2018) [2 άτομα]
17. Alkadri, Nabil Alkeilani, Rachid El Bansarkhani, and Johannes Buchmann. "**BLAZE: Practical Lattice-Based Blind Signatures for Privacy-Preserving Applications**." [https://eprint.iacr.org/2019/1167](https://eprint.iacr.org/2019/1167/20191211:104859)
18. Olivier Blazy, Georg [Fuchsbauer](https://dblp.uni-trier.de/pers/hd/f/Fuchsbauer:Georg), David Pointcheval, Damien Vergnaud: S**ignatures on Randomizable Ciphertexts.** [Public Key Cryptography 2011](https://dblp.uni-trier.de/db/conf/pkc/pkc2011.html#BlazyFPV11): 403-422. <http://www.di.ens.fr/users/pointche/Documents/Papers/2011_pkc.pdf> με εφαρμογές στο σύστημα ψηφοφορίας BeleniosRF: <https://eprint.iacr.org/2015/629> [2 άτομα]
19. Thomas Haines, Clémentine [Gritti](https://dblp.org/pers/hd/g/Gritti:Cl=eacute=mentine): **Improvements in Everlasting Privacy: Efficient and Secure Zero Knowledge Proofs.** [E-VOTE-ID 2019](https://dblp.org/db/conf/voteid/voteid2019.html#HainesG19): 116-133. <https://eprint.iacr.org/2019/901>
20. Thomas Haines, "**Cronus: Everlasting Privacy with Audit and Cast**." In Nordic Conference on Secure IT Systems, pp. 53-68. Springer, Cham, 2019.
21. Willy Quach, Daniel Wichs, Giorgos Zirdelis: **Watermarking PRFs Under Standard Assumptions: Public Marking and Security with Extraction Queries**. TCC (2) 2018: 669-698. <https://eprint.iacr.org/2018/906> [2 άτομα]
22. Tassos Dimitriou: **Efficient, Coercion-free and Universally Verifiable Blockchain-based Voting** <https://eprint.iacr.org/2019/1406>
23. Yossi Gilad and Rotem Hemo and Silvio Micali and Georgios Vlachos and Nickolai Zeldovich: **Algorand: Scaling Byzantine Agreements for Cryptocurrencies**, <https://eprint.iacr.org/2017/454> [2 άτομα]
24. Juan Garay and Aggelos Kiayias and Nikos Leonardos: **The Bitcoin Backbone Protocol: Analysis and Applications**, IACR-EUROCRYPT-2015, pp 281-310. Link: <https://eprint.iacr.org/2014/765.pdf> [2 άτομα]
25. Badertscher C., Garay J., Maurer U., Tschudi D. and Zikas V.: **But Why Does It Work?** **A Rational Protocol Design Treatment of Bitcoin,** Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, <https://eprint.iacr.org/2018/138.pdf> [2 άτομα]
26. Jun Wan, Hanshen Xiao, Srinivas Devadas and Elaine Shi: **Round-Efficient Byzantine Broadcast under Strongly Adaptive and Majority Corruptions**, TCC 2020, <https://eprint.iacr.org/2020/1236.pdf>
27. *Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil Vadhan, Ke Yang:* **On the (Im)possibility of Obfuscating Programs**, Journal of the ACM, 2012,   
    <https://dl.acm.org/doi/pdf/10.1145/2160158.2160159?casa_token=dOErTVqbdzgAAAAA:99QW4J5ykbC2rjSFJdqs9DSZ0rteG3-ffLx7HxLfWJgb04JyW_edBA_bu-2-x63esK_RLgkZN6Dlfk0>
28. *Aayush Jain and Huijia Lin and Amit Sahai.* **Indistinguishability Obfuscation from Well-Founded Assumptions**. [Cryptology ePrint Archive: Report 2020/1003](https://eprint.iacr.org/2020/1003)
29. *Sanjam Garg and Craig Gentry and Shai Halevi and Mariana Raykova and Amit Sahai and Brent Waters*. **Candidate Indistinguishability Obfuscation and Functional Encryption for all circuits**. [Cryptology ePrint Archive, Report 2013/45](https://ia.cr/2013/451)
30. [*Ania Piotrowska*](https://arxiv.org/search/cs?searchtype=author&query=Piotrowska%2C+A)*,* [*Jamie Hayes*](https://arxiv.org/search/cs?searchtype=author&query=Hayes%2C+J)*,* [*Tariq Elahi*](https://arxiv.org/search/cs?searchtype=author&query=Elahi%2C+T)*,* [*Sebastian Meiser*](https://arxiv.org/search/cs?searchtype=author&query=Meiser%2C+S)*,* [*George Danezis*](https://arxiv.org/search/cs?searchtype=author&query=Danezis%2C+G)**. The Loopix Anonymity System**. <https://arxiv.org/abs/1703.00536>
31. *Matthew Franklin and Haibin Zhang*. **A Framework for Unique Ring Signatures.** FC 2012**.** <https://eprint.iacr.org/2012/577>
32. *Luca De Feo and Bertram Poettering and Alessandro Sorniotti,* **On the (in)security of ElGamal in OpenPGP.** ACM CCS 21. <https://eprint.iacr.org/2021/923>
33. *Thomas Haines and Johannes Mueller.* **Optimal Randomized Partial Checking for Decryption Mix Nets*,*** 26th ACISP 21,<https://eprint.iacr.org/2021/520>
34. *Ashley Fraser and Elizabeth A. Quaglia,* **Report and Trace Ring Signatures,** CNS 2021, <https://eprint.iacr.org/2021/1300>
35. [*Olivier Blazy*](https://dblp.dagstuhl.de/pid/24/8243.html)*,* [*Xavier Bultel*](https://dblp.dagstuhl.de/pid/179/7523.html)*,* [*Pascal Lafourcade*](https://dblp.dagstuhl.de/pid/l/PascalLafourcade.html)*,* [*Octavio Perez-Kempner*](https://dblp.dagstuhl.de/pid/233/3468.html): **Generic Plaintext Equality and Inequality Proofs**. FC 21, <https://eprint.iacr.org/2021/426>.
36. *Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Jens Groth, Christophe Petit:* **Efficient Zero-Knowledge Arguments for Arithmetic Circuits in the Discrete Log Setting**. EUROCRYPT 2016, <https://eprint.iacr.org/2016/263>
37. *Gabrielle Beck, Julia Len, Ian Miers and Matthew Green*, **Fuzzy Message Detection**.ACM CCS 21, <https://eprint.iacr.org/2021/089>
38. [*Daniel Benarroch*](https://dblp.dagstuhl.de/pid/195/3261.html)*,* [*Matteo Campanelli*](https://dblp.dagstuhl.de/pid/22/7530.html)*,* [*Dario Fiore*](https://dblp.dagstuhl.de/pid/99/2744-1.html)*,* [*Kobi Gurkan*](https://dblp.dagstuhl.de/pid/284/2574.html)*,* [*Dimitris Kolonelos*](https://dblp.dagstuhl.de/pid/253/1725.html): **Zero-Knowledge Proofs for Set Membership: Efficient, Succinct, Modular**. FC 21, <https://eprint.iacr.org/2019/1255>.
39. *Adi Akavia, Rio LaVigne and Tal Moran*, **Topology-Hiding Computation on all Graphs**, CRYPTO 2017, <https://eprint.iacr.org/2017/296>

ΙΙ. Προγραμματιστικά

1. **Υλοποίηση ενός στοιχειώδους blockchain με υποστήριξη smart contracts**.<https://hackernoon.com/how-to-implement-a-blockchain-project-in-5-steps-9c78353666f7> Βλ.
2. **Smart contracts** **σε cardano** -- βλ. <https://docs.cardano.org/introduction/>, <https://developers.cardano.org/home/>
3. **Smart contracts σε ethereum** -- βλ. <https://ethereum.org/en/smart-contracts/>
4. **Aνώνυμα ερωτηματολόγια με χρήση ομομορφικής κρυπτογραφίας**, βλ. και ANONIZE <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6956576>
5. Υλοποίηση **Designated Verifier Linkable Ring Signatures (DVLRS)** χρησιμοποιώντας ελλειπτικές καμπύλες. Περισσότερες πληροφορίες μπορείτε να βρείτε στο <https://1drv.ms/b/s!As0Lxh56lNaisIF8JcnHRF27PI-vPQ?e=B0P29s> (η υλοποίηση αφορά τις διαφάνειες 15-18) και στο <https://1drv.ms/v/s!As0Lxh56lNaisIIVCgvMnP0S63lYtQ?e=CE9Cs4> (βίντεο). Η υλοποίηση μπορεί να βασιστεί στις υπογραφές Schnorr. Μία απλή εκπαιδευτική υλοποίηση (σε Python) μπορεί να βρεθεί στο <https://gitlab.esat.kuleuven.be/Jori.Winderickx/imoCps/blob/9005ef8d32e3bab703789c2b5c254016cbad9c18/python/schnorr.py>. Υπάρχουν πολλές άλλες υλοποιήσεις στο Web σε όλες τις δημοφιλείς γλώσσες προγραμματισμού. Για απορίες μπορείτε να επικοινωνήσετε στο [pgrontas@corelab.ntua.gr](mailto:pgrontas@corelab.ntua.gr)
6. **Βελτιώσεις / επεκτάσεις στο σύστημα DEMOS** -- βλ. μεταπτυχιακή εργασία Θ. Σουλιώτη, <https://project-archive.inf.ed.ac.uk/msc/20182796/msc_proj.pdf>
7. **Bελτιώσεις / επεκτάσεις στο OTR / mpOTR** -- βλ. διπλωματική Κ. Ανδρικόπουλου - Δ. Κολοτούρου, <http://artemis.cslab.ece.ntua.gr:8080/jspui/handle/123456789/13301>
8. **Υλοποίηση** [**τυχερών παιγνίων με χρήση τεχνολογίας blockchain**](http://dspace.lib.ntua.gr/xmlui/handle/123456789/47628) -- βλ. διπλωματική Βλ. Κουτσού, <https://dspace.lib.ntua.gr/xmlui/handle/123456789/47628>