Incomplete reference list from INDOCRYPT Tutorial, Claudio Orlandi

1. Cryptographic Computing Lecture Notes http://orlandi.dk/crycom
2. Bar-Ilan Winter School on MPC (with YouTube videos)
    a. 2015 edition http://crypto.biu.ac.il/5th-biu-winter-school
    b. 2011 edition http://u.cs.biu.ac.il/~lindell/mpcschool.html
3. One-Time Truth Table
    a. Yuval Ishai, Eyal Kushilevitz, Sigurd Meldgaard, Claudio Orlandi, Anat Paskin-Cherniavsky: On the Power of Correlated Randomness in Secure Computation. TCC 2013
4. Circuit Based Computation BeDOZa/TinyOT
    a. Rikke Bendlin, Ivan Damgård, Claudio Orlandi, Sarah Zakarias: Semi-homomorphic Encryption and Multiparty Computation. EUROCRYPT 2011
    b. Jesper Buus Nielsen, Peter Sebastian Nordholt, Claudio Orlandi, Sai Sheshank Burra: A New Approach to Practical Active-Secure Two-Party Computation. CRYPTO 2012
5. SPDZ/MiniMACs/MASCOT/… (not covered)
    a. Ivan Damgård, Valerio Pastro, Nigel P. Smart, Sarah Zakarias: Multiparty Computation from Somewhat Homomorphic Encryption. CRYPTO 2012
    b. Ivan Damgård, Marcel Keller, Enrique Larraia, Valerio Pastro, Peter Scholl, Nigel P. Smart: Practical Covertly Secure MPC for Dishonest Majority - Or: Breaking the SPDZ Limits. ESORICS 2013
    c. Ivan Damgård, Rasmus Lauritsen, Tomas Toft: An Empirical Study and Some Improvements of the MiniMac Protocol for Secure Computation. SCN 2014
    d. Marcel Keller, Emmanuela Orsini, Peter Scholl: MASCOT: Faster Malicious Arithmetic Secure Computation with Oblivious Transfer.
6. OT Basics
    a. Cryptographic Computing Foundations, Lecture Notes (Claudio Orlandi)
    b. (Book) Carmit Hazay, Yehuda Lindell: Efficient Secure Two-Party Protocols - Techniques and Constructions. Information Security and Cryptography, Springer 2010
7. OT Based Multiplication
    a. Niv Gilboa: Two Party RSA Key Generation. CRYPTO 1999
8. Passive Secure OT Extension
    a. Yuval Ishai, Joe Kilian, Kobbi Nissim, Erez Petrank: Extending Oblivious Transfers Efficiently. CRYPTO 2003
    b. Gilad Asharov, Yehuda Lindell, Thomas Schneider, Michael Zohner: More efficient oblivious transfer and extensions for faster secure computation. ACM Conference on Computer and Communications Security 2013
9. Active Secure OT Extension (not covered)
    a. Jesper Buus Nielsen, Peter Sebastian Nordholt, Claudio Orlandi, Sai Sheshank Burra: A New Approach to Practical Active-Secure Two-Party Computation. CRYPTO 2012
    b. Gilad Asharov, Yehuda Lindell, Thomas Schneider, Michael Zohner: More Efficient Oblivious Transfer Extensions with Security for Malicious Adversaries. EUROCRYPT (1) 2015

    c. Marcel Keller, Emmanuela Orsini, Peter Scholl: Actively Secure OT Extension with Optimal Overhead. CRYPTO (1) 2015
10. OT Protocols from DDH
    a. Moni Naor, Benny Pinkas: Computationally Secure Oblivious Transfer. J. Cryptology 18(1)
    b. Chris Peikert, Vinod Vaikuntanathan, Brent Waters: A Framework for Efficient and Composable Oblivious Transfer. CRYPTO 2008
    c. Tung Chou, Claudio Orlandi: The Simplest Protocol for Oblivious Transfer. LATINCRYPT 2015
11. Garbled Circuits, definitions
    a. Mihir Bellare, Viet Tung Hoang, Phillip Rogaway: Foundations of garbled circuits. ACM Conference on Computer and Communications Security 2012
12. Optimized Garbling Schemes
    a. Vladimir Kolesnikov, Thomas Schneider: Improved Garbled Circuit: Free XOR Gates and Applications. ICALP (2) 2008
13. Other optimized garbling schemes (not covered)
    a. Shay Gueron, Yehuda Lindell, Ariel Nof, Benny Pinkas: Fast Garbling of Circuits Under Standard Assumptions. ACM Conference on Computer and Communications Security 2015
    b. Vladimir Kolesnikov, Payman Mohassel, Mike Rosulek: FleXOR: Flexible Garbling for XOR Gates That Beats Free-XOR. CRYPTO (2) 2014
    c. Tore Kasper Frederiksen, Jesper Buus Nielsen, Claudio Orlandi: Privacy-Free Garbled Circuits with Applications to Efficient Zero-Knowledge. EUROCRYPT (2) 2015
    d. Samee Zahur, Mike Rosulek, David Evans: Two Halves Make a Whole - Reducing Data Transfer in Garbled Circuits Using Half Gates. EUROCRYPT (2) 2015
14. Active Secure GC based protocols
    a. Yehuda Lindell: Fast Cut-and-Choose Based Protocols for Malicious and Covert Adversaries. CRYPTO (2) 2013
    b. Yehuda Lindell, Benny Pinkas: An Efficient Protocol for Secure Two-Party Computation in the Presence of Malicious Adversaries. EUROCRYPT 2007
    c. Payman Mohassel, Matthew K. Franklin: Efficiency Tradeoffs for Malicious Two-Party Computation. Public Key Cryptography 2006
    d. Jesper Buus Nielsen, Claudio Orlandi: Cross&Clean: Amortized Garbled Circuits with Constant Overhead. TCC 2016
    e. Marek Jawurek, Florian Kerschbaum, Claudio Orlandi: Zero-knowledge using garbled circuits: how to prove non-algebraic statements efficiently. ACM Conference on Computer and Communications Security 2013