Secure Computation Annotated Bibliography

Jason Perry

Version of March 4, 2015

The references are in chronological order, so that the progress of the field can be more easily followed. The annotations also include forward pointers, to show work that follows up on a specific problem.

We have restricted ourselves to results that apply to general MPC, that is, to results that apply to computing large classes of functionalities securely, and not to specific applications.

The most important related literatures not included in this bibliography (beyond the fundamentals of cryptography) are secret sharing, oblivious transfer and PIR.

Thanks to Dan Bogdanov for contributing new entries and Mahdi Zamani for submitting corrections.

References

[Sha79] Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979.

Presents the now universally-used technique of secret sharing using polynomial interpolation.

[Rab81] Michael O. Rabin. How to exchange secrets by oblivious transfer. Technical Report TR-81, Harvard University, 1981.

The initial presentation of noisy-channel oblivious transfer.

[LSP82] Leslie Lamport, Robert E. Shostak, and Marshall C. Pease. The byzantine generals problem. *ACM Trans. Program. Lang. Syst.*, 4(3):382–401, 1982.

Early algorithms for solving the byzantine agreement problem, a fundamental primitive in MPC.

[Yao82] Andrew Chi-Chih Yao. Protocols for secure computations (extended abstract). In *Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science (FOCS 1982)*, pages 160–164, 1982.

The first of two papers by Yao referenced as the source of the two-party garbled-circuit secure computation protocol, though the construction is not mentioned explicitly in the paper. Gives a solution to the 'millionaires problem'.

[CGMA85] Benny Chor, Shafi Goldwasser, Silvio Micali, and Baruch Awerbuch. Verifiable secret sharing and achieving simultaneity in the presence of faults (extended abstract). In *Proceedings of the 26th Annual IEEE Symposium on Foundations of Computer Science (FOCS 1985)*, pages 383–395, 1985.

Shows how secret-sharing can be strengthened so that players' shares can be verified to remain consistent, and secrets can be reconstructed even if some players are malicious. A key result used in [GMW87], among others.

[Cle86] Richard Cleve. Limits on the security of coin flips when half the processors are faulty (extended abstract). In *Proceedings of the Eighteenth Annual ACM Symposium on Theory of Computing (STOC '86)*, pages 364–369, 1986.

Result that established the impossibility of complete fairness in secure computation when there is no honest majority.

[Yao86] Andrew Chi-Chih Yao. How to generate and exchange secrets (extended abstract). In *Proceedings of the 27th Annual IEEE Symposium on Foundations of Computer Science (FOCS 1986)*, pages 162–167, 1986.

The second of two papers by Yao referenced as the source of the two-party garbled-circuit secure computation protocol. The paper shows, using the assumption of hardness of factoring, how two parties can explicitly generate a shared secret value that enables secure computation.

[GHY87] Zvi Galil, Stuart Haber, and Moti Yung. Cryptographic computation: Secure fault-tolerant protocols and the public-key model. In *Advances in Cryptology – CRYPTO '87*, pages 135–155, 1987.

A formulation of multi-party computation that uses a public-key model, without generating new keys on-line. Shows how and fault recovery (as opposed to mere fault detection) can be achieved in this model.

[GMW87] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or a completeness theorem for protocols with honest majority. In *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing (STOC '87)*, pages 218–229, 1987.

The seminal result showing the possibility of computationally-secure multiparty computation among three or more parties. Describes a "protocol compiler" for transforming protocols secure against semi-honest adversaries into protocols secure against malicious adversaries.

[GV87] Oded Goldreich and Ronen Vainish. How to solve any protocol problem—an efficiency improvement. In *Advances in Cryptology – CRYPTO '87*, pages 73–86, 1987.

An efficiency improvement on [GMW87], by avoiding the black-box use of Yao's 2-party protocol. It introduces a specific solution to the 2-party sub-protocol used in [GMW87], based on the Quadradic Residuosity assumption.

[BGW88] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing (STOC '88)*, pages 1–10, 1988.

The first result giving protocols for information-theoretically secure multiparty computation. Proves that perfectly-secure MPC requires strictly less than $n/2$ corrupted players if the adversary is semi-honest, or less than $n/3$ in the case of a malicious adversary.

[CCD88] David Chaum, Claude Crépeau, and Ivan Damgård. Multiparty unconditionally secure protocols (extended abstract). In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing (STOC '88)*, pages 11–19, 1988.

Gives essentially the same result as [BGW88], but using verifiable secret sharing as the building block; presented at the same conference.

[FM88] Paul Feldman and Silvio Micali. Optimal algorithms for byzantine agreement. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing (STOC '88)*, pages 148–161, 1988.

Seminal result giving a protocol for Byzantine Agreement, which is used to simulate a broadcast channel in secure MPC with malicious corruptions.

[Kil88] Joe Kilian. Founding cryptography on oblivious transfer. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing (STOC '88)*, pages 20–31, 1988.

Shows that existing two-party secure computation results can be built unconditionally on oblivious transfer. Subsequent work includes [CGT95, IPS08].

[AFK89] Martín Abadi, Joan Feigenbaum, and Joe Kilian. On hiding information from an oracle. *J. Comput. Syst. Sci.*, 39(1):21–50, 1989.

Foundational result showing the impossibility of a client holding an input value x obtaining the value of a function $f(x)$ from a single oracle, while perfectly hiding all information about x except its length.

[BB89] Judit Bar-Ilan and Donald Beaver. Non-cryptographic fault-tolerant computing in constant number of rounds of interaction. In *Proceedings of the Eighth ACM Symposium on Principles of Distributed Computing (PODC '89)*, pages 201–209, 1989.

Gives a more efficient protocol for unconditionally secure MPC, which can evaluate NC_1 circuits in a constant number of rounds of communication.

[BG89] Donald Beaver and Shafi Goldwasser. Multiparty computation with faulty majority. In *Advances in Cryptology – CRYPTO '89*, pages 589–590, 1989.

Gives an MPC protocol that is cryptographically secure against up to $n-1$ maliciously corrupted parties, by sacrificing *fairness*, meaning that a malicious party can abort after learning the output. Requires a broadcast channel and the assumption of two-party oblivious transfer.

[Cha89] David Chaum. The spymasters double-agent problem: Multiparty computations secure unconditionally from minorities and cryptographically from majorities. In *Advances in Cryptology – CRYPTO '89*, pages 591–602, 1989.

The first *hybrid security* result, setting, giving a protocol which is both unconditionally secure against less than $n/3$ corrupted parties, and computationally secure against less than $n/2$ corrupted parties. See also [FHW04], [LRM10].

[RB89] Tal Rabin and Michael Ben-Or. Verifiable secret sharing and multiparty protocols with honest majority (extended abstract). In *Proceedings of the 21st Annual ACM Symposium on Theory of Computing (STOC '89)*, pages 73–85, 1989.

Gives an MPC protocol that is unconditionally secure when less than $n/2$ parties are corrupted, with exponentially small error, by assuming a broadcast channel. [BGW88] proved that with no error, the number of corrupted parties must be $< n/3$.

[AF90] Martín Abadi and Joan Feigenbaum. Secure circuit evaluation. *J. Cryptology*, 2(1):1–12, 1990.

Treats Private Function Evaluation, an important subproblem of two-party secure computation in which the function itself must be hidden from one of the parties. This paper shows linear communication complexity PFE, with d rounds of communication, where d is circuit depth. Follow-up work is [KM11].

[BF90] Donald Beaver and Joan Feigenbaum. Hiding instances in multioracle queries. In *7th Annual Symposium on Theoretical Aspects of Computer Science (STACS 1990)*, pages 37–48, 1990.

Shows that all functions have *multioracle instance-hiding schemes*, in which a client can obtain the value of the function f on input x while revealing nothing but the input size. A foundational result for PIR.

[BMR90] Donald Beaver, Silvio Micali, and Phillip Rogaway. The round complexity of secure protocols (extended abstract). In *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing (STOC '90)*, pages 503–513, 1990.

Result showing that cryptographically-secure multiparty computation is achievable in a constant number of rounds, if a broadcast channel is assumed. Important follow-up work on round complexity for MPC includes [KOS03], [DI05].

[GL90] Shafi Goldwasser and Leonid A. Levin. Fair computation of general functions in presence of immoral majority. In *Advances in Cryptology – CRYPTO '90*, pages 77–93, 1990.

Achieves a similar fairness-with-dishonest-majority result as [BG89], also by assuming OT as a primitive. In addition, this construction allows composition of fairness-preserving protocols, and is a precursor to work on universal composability.

[Bea91a] Donald Beaver. Foundations of secure interactive computing. In *Advances in Cryptology – CRYPTO '91*, pages 377–391, 1991.

Work to establish a definitional treatment of secure computation, using the real-ideal framework and the notion of "relative resilience".

[Bea91b] Donald Beaver. Secure multiparty protocols and zero-knowledge proof systems tolerating a faulty minority. *J. Cryptology*, 4(2):75–122, 1991.

Following [BGW88],[CCD88], gives results for unconditionally secure MPC with up to $n/2$ maliciously corrupted parties, by allowing non-zero error probability. Provides security proofs in the "relative resilience" model of [Bea91a].

[MR92] Silvio Micali and Phillip Rogaway. Secure computation. In Joan Feigenbaum, editor, *Advances in Cryptology – CRYPTO 91*, volume 576 of *Lecture Notes in Computer Science*, pages 392–404. Springer Berlin Heidelberg, 1992.

An important early work in estabilishing rigourous security definitions for MPC.

[OY91] Rafail Ostrovsky and Moti Yung. How to withstand mobile virus attacks (extended abstract). In *Proceedings of the Tenth Annual ACM Symposium on Principles of Distributed Computing (PODC '91)*, pages 51–59, New York, NY, USA, 1991. ACM.

The first work to present a multi-party computation protocol information theoretically secure against a *mobile* adversary, who has the ability to "infect" a different subset of parties in each round of the computation.

[FY92] Matthew K. Franklin and Moti Yung. Communication complexity of secure computation (extended abstract). In *Proceedings of the 24th Annual ACM Symposium on Theory of Computing (STOC '92)*, pages 699–710, 1992.

Gives upper and lower bounds for the communication complexity of unconditionally secure MPC, depending on the number of corrupted parties.

[BCG93] Michael Ben-Or, Ran Canetti, and Oded Goldreich. Asynchronous secure computation. In *Proceedings of the 25th Annual ACM Symposium on Theory of Computing (STOC '93)*, pages 52–61, 1993.

The foundational work in *asynchronous* MPC, in which no messages are guaranteed to arrive in bounded time, thus preventing the round enforcement of standard MPC protocols. Shows that asynchronous MPC is possible for up to $n/4$ maliciously corrupted players, or $n/3$ with fail-stop corruption.

[CvdGT95] Claude Crépeau, Jeroen van de Graaf, and Alain Tapp. Committed oblivious transfer and private multi-party computation. In *Advances in Cryptology – CRYPTO '95*, pages 110–123, 1995.

Extending [Kil88], shows how to achieve secure *multi-party* computation using OT and bit commitment, with a more efficient construction for combining the two, termed "Committed Oblivious Transfer". Subsequent work includes [IPS08].

[Bea96] Donald Beaver. Correlated pseudorandomness and the complexity of private computations. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC '96)*, pages 479–488, 1996.

Shows how to expand a short "seed" of oblivious transfers into a polynomially-long sequence of OT's, assuming only the existence of a one-way function. A key result in establishing the computational assumptions required for efficient MPC.

[CFGN96] Ran Canetti, Uriel Feige, Oded Goldreich, and Moni Naor. Adaptively secure multi-party computation. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC '96)*, pages 639–648, 1996.

First result proving security of an MPC protocol against an adaptive adversary, which is able to dynamically choose which parties to corrupt in the course of the computation, based on its view. A protocol is given which is secure against an adaptive adversary corrupting a minority of parties, without requiring that parties be trusted to delete their computation records.

[FH96] Matthew K. Franklin and Stuart Haber. Joint encryption and message-efficient secure computation. *J. Cryptology*, 9(4):217–232, 1996.

An improvement to the efficiency of passively-secure MPC. This is an early preprocessing result (followed by [CDN01]), which requires a secure key exchange phase.

[OS97] Rafail Ostrovsky and Victor Shoup. Private information storage (extended abstract). In *Proceedings of the 29th Annual ACM Symposium on Theory of Computing (STOC '97)*, pages 294–303, 1997.

Contains the core results for secure computation over ORAM, which were developed further in [GKK+12] and [GGH+13].

[Bea98] Donald Beaver. Adaptively secure oblivious transfer. In *Advances in Cryptology—ASIACRYPT '98*, pages 300–314, 1998.

Gives the first protocol for oblivious transfer that is provably secure against an adaptive adversary, and consequently for general two-party computation with an adaptive adversary.

[FHM98] Matthias Fitzi, Martin Hirt, and Ueli M. Maurer. Trading correctness for privacy in unconditional multi-party computation (extended abstract). In *Advances in Cryptology—CRYPTO '98*, pages 121–136, 1998.

The first mixed-adversary result in the purely unconditional security model. Achieves privacy against any minority of corrupted players, even while there are up to $n/3$ actively corrupted players.

[GRR98] Rosario Gennaro, Michael O. Rabin, and Tal Rabin. Simplified vss and fast-track multiparty computations with applications to threshold cryptography. In *Proceedings of the Seventeenth ACM Symposium on Principles of Distributed Computing (PODC '98)*, pages 101–111, 1998.

Gives a new multiplication technique on verifiable shared secrets that improves the efficiency of unconditionally-secure MPC. Also introduces *fault-sensitive* MPC as a more efficient alternative to full security against a malicious adversary.

[CO99] Ran Canetti and Rafail Ostrovsky. Secure computation with honest-looking parties: What if nobody is truly honest? (extended abstract). In *Proceedings of the 31st Annual ACM Symposium on Theory of Computing (STOC '99)*, pages 255–264, 1999.

Shows that secure multi-party computation is possible when even non-corrupted parties may deviate from the protocol, as long as those deviations are not detectable. Precursor to work on covert adversaries [AL07].

[CDD+99] Ronald Cramer, Ivan Damgård, Stefan Dziembowski, Martin Hirt, and Tal Rabin. Efficient multiparty computations secure against an adaptive adversary. In *Advances in Cryptology – EUROCRYPT '99*, pages 311–326, 1999.

Shows that the protocol of [RB89] is not secure against adaptive adversaries, and gives a more efficient protocol that is unconditionally secure (with non-zero error probability) against up to $n/2$ adaptive adversaries, in the broadcast channel model. Can also be modified to support adversary structures.

[NP99a] Moni Naor and Benny Pinkas. Oblivious transfer and polynomial evaluation. In *Proceedings of the 31st Annual ACM Symposium on Theory of Computing (STOC '99)*, pages 245–254, 1999.

A key computational OT result, showing 1-out-of-n oblivious transfer in $O(\log n)$ rounds, an efficient k-out-of-n protocol, and providing a generic transformation of any PIR scheme to SPIR. Full journal version is [NP05].

[NP99b] Moni Naor and Benny Pinkas. Oblivious transfer with adaptive queries. In *Advances in Cryptology—CRYPTO '99*, pages 573–590, 1999.

Provides a protocol for a variation of k-out-of-n oblivious transfer in which the items queried may depend on previous items received. These results are also found in the journal version [NP05].

[SYY99] Tomas Sander, Adam L. Young, and Moti Yung. Non-interactive cryptocomputing for NC^1. In *Proceedings of the 40th Annual IEEE Symposium on Foundations of Computer Science (FOCS 1999)*, pages 554–567, 1999.

Gives a one-round protocol for PFE on NC^1 circuits. Prior results are a constant number of rounds for any circuit.

[Can00] Ran Canetti. Security and composition of multiparty cryptographic protocols. *J. Cryptology*, 13(1):143–202, 2000.

Precursor to the seminal work on *Universal Composability* [Can01], giving a security framework that is secure under *non-concurrent* composition. Also gives a formal definition of stand-alone security. The ePrint version is also commonly referenced as [Can98].

[CDM00] Ronald Cramer, Ivan Damgård, and Ueli M. Maurer. General secure multi-party computation from any linear secret-sharing scheme. In *Advances in Cryptology – EUROCRYPT 2000*, pages 316–334, 2000.

Gives an efficient general construction of Secure MPC from any Linear Secret Sharing Scheme, where security corresponds to the Adversary Structure [HM00] of the secret sharing scheme. Security against a malicious adversary comes from constructing a *verifiable* secret-sharing scheme. Also the first protocol to support adversary structures with complexity polynomial in the number of players.

[HM00] Martin Hirt and Ueli M. Maurer. Player simulation and general adversary structures in perfect multiparty computation. *J. Cryptology*, 13(1):31–60, 2000.

Generalizes theorems on the maximum number of corrupted parties for unconditionally secure MPC, characterizing the adversary in terms of sets of corrupted subsets of players, rather than a single threshold.

[HMP00] Martin Hirt, Ueli Maurer, and Bartosz Przydatek. Efficient secure multi-party computation. In Tatsuaki Okamoto, editor, *Advances in Cryptology – ASIACRYPT 2000*, pages 143–161. 2000.

Efficiency improvements for unconditional MPC in the style of [BGW88].

[SR00a] K. Srinathan and C. Pandu Rangan. Efficient asynchronous secure multiparty distributed computation. In *Progress in Cryptology – INDOCRYPT 2000*, pages 117–129, 2000.

The first significant efficiency improvement to perfectly secure asynchronous MPC. See also [BT07].

[SR00b] K. Srinathan and C. Pandu Rangan. Tolerating generalized mobile adversaries in secure multiparty computation. In *Progress in Cryptology – INDOCRYPT 2000*, pages 130–142, 2000.

Gives the first MPC protocols secure against a mobile adversary using adversary structures, rather than a threshold adversary.

[Kil00] Joe Kilian. More general completeness theorems for secure two-party computation. In *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing (STOC '00)*, pages 316–324, 2000.

Shows that information-theoretic security with fairness can only be achieved with $< n/2$ maliciously corrupted parties in the broadcast channel model.

[Can01] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *Proceedings of the 42nd Annual IEEE Symposium on Foundations of Computer Science (FOCS 2001)*, pages 136–145, 2001.

Seminal work on *Universal Composability*, giving a security framework for proving protocols secure regardless of the environment in which they are executed. Updated version (2005) available at `http://eprint.iacr.org/2000/067`.

[CIK+01] Ran Canetti, Yuval Ishai, Ravi Kumar, Michael K. Reiter, Ronitt Rubinfeld, and Rebecca N. Wright. Selective private function evaluation with applications to private statistics. In *Proceedings of the Twentieth ACM Symposium on Principles of Distributed Computing (PODC 2001)*, pages 293–304, 2001.

Gives sublinear protocols for instances of secure computation in which a client wishes to compute a function of selected entries of a database held by one or more servers.

[CDN01] Ronald Cramer, Ivan Damgard, and Jesper Buus Nielsen. Multiparty computation from threshold homomorphic encryption. In *Advances in Cryptology – EUROCRYPT 2001*, pages 280–299, 2001.

Gives improved efficiency for cryptographically-secure honest-majority MPC ($\mathcal{O}(nk)$ bits broadcast per gate) by making the quadratic residuosity assumption, and requiring a setup phase with key exchange.

[FIM+01] Joan Feigenbaum, Yuval Ishai, Tal Malkin, Kobbi Nissim, Martin Strauss, and Rebecca N. Wright. Secure multiparty computation of approximations. In *ICALP*, pages 927–938, 2001.

Provides a definition of secure multiparty computation of approximations, showing that some approximations leak more information than the exact result. Gives sublinear-communication protocols for approximating Hamming distance and permanent.

[HM01] Martin Hirt and Ueli M. Maurer. Robustness for free in unconditional multi-party computation. In *Advances in Cryptology—CRYPTO 2001*, pages 101–118, 2001.

Gives an efficiency improvement for the malicious case of unconditionally secure multi-party computation protocol with up to $n/3$ corrupted parties.

[NN01] Moni Naor and Kobbi Nissim. Communication complexity and secure function evaluation. *arXiv.org Computing Research Repository (CoRR)*, cs.CR/0109011, 2001.

A key early 'sublinear' result, showing how a function with a sublinear two-party evaluation protocol can be transformed into a secure evaluation protocol that preserves sublinear communication. Includes a modification of the "semi-honest-to-malicious compiler" of [GMW87] that also preserves communication complexity. Two approaches are described for representing the function, one based on branching programs and the other based on circuits with lookup tables.

[NP01] Moni Naor and Benny Pinkas. Efficient oblivious transfer protocols. In *Proceedings of the Twelfth Annual Symposium on Discrete Algorithms (SODA 2001)*, pages 448–457, 2001.

Gives improvements on the amortized complexity of 1-out-of-2 oblivious transfer. Also provides a 1-out-of-N OT protocol which has amortized overhead of a single 1-out-of-2 OT, and does not depend on the random oracle assumption (it uses the DDH.)

[CLOS02] Ran Canetti, Yehuda Lindell, Rafail Ostrovsky, and Amit Sahai. Universally composable two-party and multi-party secure computation. In *Proceedings of the 34th Annual ACM Symposium on Theory of Computing (STOC '02)*, pages 494–503, 2002.

Uses universal composability results of [Can00] to give the first two-party and multi-party protocols secure against up to $n-1$ adaptively and actively corrupted parties. Requires trusted setup of a "common reference string".

[FGMR02] Matthias Fitzi, Nicolas Gisin, Ueli Maurer, and Oliver Rotz. Unconditional byzantine agreement and multi-party computation secure against dishonest minorities from scratch. In LarsR. Knudsen, editor, *Advances in Cryptology – EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 482–501. Springer Berlin Heidelberg, 2002.

Gives a protocol demonstrating the possibility of unconditionally secure MPC with no broadcast and complete fairness for up to $n/2$ maliciously corrupted parties. Skirts the impossibility result by giving a weaker form of broadcast called "detectable broadcast", which seems to be related to covert security.

[GIKR02] Rosario Gennaro, Yuval Ishai, Eyal Kushilevitz, and Tal Rabin. On 2-round secure multiparty computation. In Moti Yung, editor, *Advances in Cryptology – CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 178–193. Springer Berlin Heidelberg, 2002.

Impossibility result for general MPC in less than 3 rounds.

[GL02] Shafi Goldwasser and Yehuda Lindell. Secure computation without agreement. In *Distributed Computing, 16th International Conference (DISC 2002)*, pages 17–32, 2002.

Overcomes known limits on the use of Byzantine agreement to emulate broadcast channels in MPC, by introducing a weaker version of fairness in which not all honest parties may receive the same output. The protocol achieves MPC with this fairness level for a dishonest majority, without a broadcast channel or trusted setup.

[Mau02] Ueli M. Maurer. Secure multi-party computation made simple. In *Security in Communication Networks, Third International Conference (SCN 2002)*, pages 14–28, 2002.

Gives unconditionally secure MPC protocols for general adversary structures, with perfect security for $\mathcal{Q}^3$ structures and statistical security for $\mathcal{Q}^2$ structures. Expanded version is [Maurer06].

[PSR02] B. Prabhu, K. Srinathan, and C. Pandu Rangan. Asynchronous unconditionally secure computation: An efficiency improvement. In *Progress in Cryptology – INDOCRYPT 2002*, pages 93–107, 2002.

Efficiency improvement on [SR00a] for asynchronous MPC.

[BPW03] Michael Backes, Birgit Pfitzmann, and Michael Waidner. A universally composable cryptographic library. Cryptology ePrint Archive, Report 2003/015, 2003. `http://eprint.iacr.org/`.

Defines a composable security framework that is also specified in a formal (symbolic) model.

[CKL03] Ran Canetti, Eyal Kushilevitz, and Yehuda Lindell. On the limitations of universally composable two-party computation without set-up assumptions. In *Advances in Cryptology – EUROCRYPT 2003*, pages 68–86. Springer, 2003.

Gives the well-known impossibility results for UC secure computation with dishonest majority when there are no setup assumptions.

[CFIK03] Ronald Cramer, Serge Fehr, Yuval Ishai, and Eyal Kushilevitz. Efficient multi-party computation over rings. In *Advances in Cryptology – EUROCRYPT 2003*, pages 596–613. Springer, 2003.

Shows how to extend unconditionally-secure MPC protocols to work over arbitrary finite rings (as opposed to fields.) Also gives a constant-round result. Later work in the same model includes [IPS09].

[DN03] Ivan Damgård and Jesper Buus Nielsen. Universally composable efficient multiparty computation from threshold homomorphic encryption. In *Advances in Cryptology – CRYPTO 2003*, pages 247–264, 2003.

Using a specific number-theoretic assumption, obtains improved efficiency for secure multiparty computation against an adversary adaptively corrupting up to $n/2$ parties. Follows on [CDN01] by the addition of adaptive security.

[FHHW03] Matthias Fitzi, Martin Hirt, Thomas Holenstein, and Jürg Wullschleger. Two-threshold broadcast and detectable multi-party computation. In *Advances in Cryptology – EUROCRYPT 2003*, pages 51–67, 2003.

A hybrid security result for MPC, following on [Cha89]. Gives a second threshold of corruption T such that if the number of corrupted parties is greater than t but less than or equal to T, players can detect that there are too many faults and abort.

[KOS03] Jonathan Katz, Rafail Ostrovsky, and Adam Smith. Round efficiency of multi-party computation with a dishonest majority. In *Advances in Cryptology – EUROCRYPT 2003*, pages 578–595, 2003.

Result showing the possibility of computationally-secure multi-party computation with dishonest majority, in $O(\log n)$ rounds with minimal assumptions, and $O(1)$ rounds with stronger assumptions.

[Lin03a] Yehuda Lindell. Parallel coin-tossing and constant-round secure two-party computation. *J. Cryptology*, 16(3):143–184, 2003.

First result showing a version of Yao's protocol with a constant number of rounds that is secure against a malicious adversary. The original construction required a polynomial number of rounds for a malicious adversary.

[Lin03b] Yehuda Lindell. *Composition of Secure Multi-Party Protocols*, volume 2815 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2003.

Monograph surveying results about secure composition of MPC protocols.

[Pin03] Benny Pinkas. Fair secure two-party computation. In *Advances in Cryptology – EUROCRYPT 2003*, pages 87–105, 2003.

A modification to Yao's protocol to achieve *fairness*, that is, to prevent one party from gaining an advantage by terminating the protocol early. This is a more efficient construction than prior work.

[BCNP04] Boaz Barak, Ran Canetti, Jesper Buus Nielsen, and Rafael Pass. Universally composable protocols with relaxed set-up assumptions. In *Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2004)*, pages 186–195. IEEE, 2004.

Paper first showing how to use public-key cryptography instead of a common reference string as a setup assumption (which is required for UC security with no honest majority.)

[FHW04] Matthias Fitzi, Thomas Holenstein, and Jürg Wullschleger. Multi-party computation with hybrid security. In *Advances in Cryptology – EUROCRYPT 2004*, pages 419–438, 2004.

Improves the two-threshold results of [FHM98] by allowing hybrid security. Shows that a system computationally secure against $t < n/4$ actively corrupted players can also be unconditionally secure against up to $n/2$ passively corrupted players.

[GMY04] Juan A. Garay, Philip D. MacKenzie, and Ke Yang. Efficient and secure multi-party computation with faulty majority and complete fairness. *IACR Cryptology ePrint Archive*, 2004:9, 2004.

Circumvents the impossibility result for completely fair computation with dishonest majority, by allowing the protocol to depend on the running time of the adversary, thus formalizing the "gradual release" method. See [GMPY06].

[Gol04] Oded Goldreich. *The Foundations of Cryptography – Volume 2, Basic Applications.* Cambridge University Press, 2004.

Contains a more rigorous exposition of results of [GMW87], as well as developing a framework for organizing and formalizing existing MPC results.

[HT04] Joseph Y. Halpern and Vanessa Teague. Rational secret sharing and multiparty computation: extended abstract. In *Proceedings of the 36th Annual ACM Symposium on Theory of Computing (STOC '04)*, pages 623–632, 2004.

Advances a new adversary model for multi-party computation, in which all parties are *rational* agents seeking to maximize some utility function, as opposed to simply being honest or dishonest. Shows that when all parties prefer to obtain the function value and secret, and to minimize the number of other agents who receive them, there exists no secure MPC protocol with a fixed running time. However, a randomized protocol with constant expected running time is given that does achieve secure MPC for 3 or more parties in this scenario.

[KO04] Jonathan Katz and Rafail Ostrovsky. Round-optimal secure two-party computation. In *Advances in Cryptology – CRYPTO 2004*, pages 335–354, 2004.

Shows that any two-party functionality can be securely computed in the presence of a malicious adversary in **five** rounds but not in four, with respect to black-box proofs. Also extends the result to an adaptive adversary.

[LP04] Yehuda Lindell and Benny Pinkas. A Proof of Yao's Protocol for Secure Two-Party Computation. *Electronic Colloquium on Computational Complexity*, 11:2004, 2004.

The first published rigorous proof of security for Yao's garbled-circuit secure two-party computation protocol.

[MNPS04] Dahlia Malkhi, Noam Nisan, Benny Pinkas, and Yaron Sella. Fairplay – secure two-party computation system. In *USENIX Security Symposium*, pages 287–302, 2004.

The first complete implementation of secure two-party computation, including a compiler from a C-like language to circuits.

[Pas04] Rafael Pass. Bounded-concurrent secure multi-party computation with a dishonest majority. In *Proceedings of the 36th Annual ACM Symposium on Theory of Computing (STOC '04)*, pages 232–241, 2004.

A protocol for universally composable secure MPC that preserves security under concurrent executions. This is the first protocol to achieve this for a dishonest majority without requiring setup assumptions such as a common reference string.

[PS04] Manoj Prabhakaran and Amit Sahai. New notions of security: achieving universal composability without trusted setup. In *Proceedings of the 36th Annual ACM Symposium on Theory of Computing (STOC '04)*, pages 242–251, 2004.

Gives an alternative definition of universal composability, and shows that secure computation can be achieved in it without trusted setup.

[CDI05] Ronald Cramer, Ivan Damgård, and Yuval Ishai. Share conversion, pseudorandom secret-sharing and applications to secure computation. In *Theory of Cryptography – TCC 2005*, pages 342–362, 2005.

Shows how to convert shares between different secret-sharing schemes using only local computation, which is important for efficient programmable implementations of secure computation.

[DI05] Ivan Damgård and Yuval Ishai. Constant-round multiparty computation using a black-box pseudorandom generator. In *Advances in Cryptology – CRYPTO 2005*, pages 378–394, 2005.

Shows constant-round multiparty computation a la [BMR90], secure against a malicious, adaptive adversary corrupting a minority of parties, founded only on the use of a PRG (and requiring a setup phase to emulate a trusted dealer.) It uses error-correcting codes in place of zero-knowledge proofs, for efficiency.

[GL05] Shafi Goldwasser and Yehuda Lindell. Secure multi-party computation without agreement. *J. Cryptology*, 18(3):247–287, 2005.

Journal version of [GL02].

[NP05] Moni Naor and Benny Pinkas. Computationally secure oblivious transfer. *J. Cryptology*, 18(1):1–35, 2005.

Journal version of the OT results in [NP99a], [NP99b].

[ADGH06] Ittai Abraham, Danny Dolev, Rica Gonen, and Joseph Y. Halpern. Distributed computing meets game theory: robust mechanisms for rational secret sharing and multiparty computation. In *Proceedings of the Twenty-fifth ACM Symposium on Principles of Distributed Computing (PODC 2006)*, pages 53–62, 2006.

Extends [HT04] by giving a protocol secure against rational players that form coalitions, as opposed to acting individually.

[BH06] Zuzana Beerliová-Trubíniová and Martin Hirt. Efficient multi-party computation with dispute control. In *Theory of Cryptography – TCC 2006*, pages 305–328, 2006.

Gives an unconditionally secure MPC protocol against up to $n/2$ maliciously corrupted parties, with improved broadcast efficiency over [CDD+99]; only n^2 bits of communication per multiplication.

[CKL06] Ran Canetti, Eyal Kushilevitz, and Yehuda Lindell. On the limitations of universally composable two-party computation without set-up assumptions. *J. Cryptology*, 19(2):135–167, 2006.

Journal version of [CKL03].

[CC06] Hao Chen and Ronald Cramer. Algebraic geometric secret sharing schemes and secure multi-party computations over small fields. In *Advances in Cryptology – CRYPTO 2006*, pages 521–536. 2006.

Introduces a new secret sharing technique that is secure over small fields, reducing the communication complexity of MPC, especially when there are a large number of parties. Applicable for realizing the IPS compiler [IPS08] with good concrete efficiency.

[DFK+06] Ivan Damgård, Matthias Fitzi, Eike Kiltz, Jesper Buus Nielsen, and Tomas Toft. Unconditionally secure constant-rounds multi-party computation for equality, comparison, bits and exponentiation. In *Theory of Cryptography – TCC 2006*, pages 285–304, 2006.

(Current best?) results for information-theoretic security in constant rounds, achieved for a subset of functions.

[DI06] Ivan Damgård and Yuval Ishai. Scalable secure multiparty computation. In *Advances in Cryptology – CRYPTO 2006*, pages 501–520, 2006.

Gives an MPC protocol whose amortized work per player does not grow as the number of players grows. Computationally secure against an adaptive adversary corrupting any constant fraction of players.

[FIM+06] Joan Feigenbaum, Yuval Ishai, Tal Malkin, Kobbi Nissim, Martin J. Strauss, and Rebecca N. Wright. Secure multiparty computation of approximations. *ACM Transactions on Algorithms*, 2(3):435–472, 2006.

Journal version of [FIM+01].

[GMPY06] Juan Garay, Philip MacKenzie, Manoj Prabhakaran, and Ke Yang. Resource fairness and composability of cryptographic protocols. In Shai Halevi and Tal Rabin, editors, *Theory of Cryptography*, volume 3876 of *Lecture Notes in Computer Science*, pages 404–428. Springer Berlin Heidelberg, 2006.

Defines a relaxed notion of fairness that circumvents the impossibility result for completely fair computation with dishonest majority. Journal version is [GMPY11].

[GK06] S. Dov Gordon and Jonathan Katz. Rational secret sharing, revisited. In *SCN*, pages 229–241, 2006.

Circumvents an impossibility result in [HT04], showing a probabilistic protocol for secure 2-party computation with rational players, having a constant expected number of rounds. The protocol also generalizes to $n \geq 3$ parties and is claimed to be simpler than that of [HT04].

[HN06] Martin Hirt and Jesper Buus Nielsen. Robust multiparty computation with linear communication complexity. In *Advances in Cryptology – CRYPTO 2006*, pages 463–482, 2006.

Shows an MPC protocol with computational security and t-robustness [HM01] for up to $n/2$ corrupted parties with linear communication complexity.

[IKLP06] Yuval Ishai, Eyal Kushilevitz, Yehuda Lindell, and Erez Petrank. On combining privacy with guaranteed output delivery in secure multiparty computation. In *Advances in Cryptology – CRYPTO 2006*, pages 483–500, 2006.

Shows there is no constant-round MPC protocol that achieves *both* "full security" (guaranteed output to all players) in the presence of an honest majority, and security with abort (against malicious corruptions) when there is no honest majority. However, it is possible when the adversary is semi-honest in the no-honest-majority case. Full version, combining results from [Kat07], is [IKK+11].

[LT06] Anna Lysyanskaya and Nikos Triandopoulos. Rationality and adversarial behavior in multi-party computation. In *Advances in Cryptology – CRYPTO 2006*, pages 180–197, 2006.

A result in rational MPC in which the parties are a *mixture* of rational agents and adversary-controlled parties. A protocol is given that is secure against a malicious adversary controlling up to $\lceil n/2 \rceil + 2$ parties.

[MF06] Payman Mohassel and Matthew K. Franklin. Efficiency tradeoffs for malicious two-party computation. In *Public Key Cryptography*, pages 458–473, 2006.

A comparison of approaches for securing Yao's garbled circuit protocol against a malicious adversary. Notably, the authors expose and correct a vulnerability in Fairplay [MNPS04].

[AL07] Yonatan Aumann and Yehuda Lindell. Security against covert adversaries: Efficient protocols for realistic adversaries. In *Theory of Cryptography – TCC 2007*, pages 137–156, 2007.

Introduces two-party protocols secure against a *covert adversary*, which captures the notion of an adversary who deviates from the protocol only if the probability of being caught doing so is small. The protocol is more efficient than known protocols secure against a malicous adversary. Also has journal version [AL10].

[BH07] Zuzana Beerliová-Trubíniová and Martin Hirt. Simple and efficient perfectly-secure asynchronous mpc. In *Advances in Cryptology – ASIACRYPT 2007*, pages 376–392, 2007.

A more efficient protocol for perfectly-secure asynchronous MPC with malicious, adaptive adversaries. It achieves the optimal bound of up to $n/4$ corrupted players, and requires $\mathcal{O}(n^3)$ communication per multiplication.

[CGOS07] Nishanth Chandran, Vipul Goyal, Rafail Ostrovsky, and Amit Sahai. Covert multiparty computation. In *Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2007)*, pages 238–248, 2007.

A result for MPC with covert *computation* (not adversary), in which the parties do not know which of the other parties are participating in the computation. Related to steganography.

[DN07] Ivan Damgård and Jesper Buus Nielsen. Scalable and unconditionally secure multiparty computation. In *Advances in Cryptology – CRYPTO 2006*, pages 572–590, 2007.

Gives the first unconditionally secure MPC protocol where the communication complexity is linear in the circuit size (though quadratic in the circuit depth.)

[FGM07] Matthew K. Franklin, Mark Gondree, and Payman Mohassel. Multi-party indirect indexing and applications. In *Advances in Cryptology – ASIACRYPT 2007*, pages 283–297, 2007.

A generalization of [NN01] to the multi-party case, showing that multiparty computation with sublinear communication is achievable for algorithms with sublinear communication complexity. Also introduces a multiparty primitive generalizing oblivious transfer.

[HIK07] Danny Harnik, Yuval Ishai, and Eyal Kushilevitz. How many oblivious transfers are needed for secure multiparty computation? In *Advances in Cryptology – CRYPTO 2007*, pages 284–302, 2007.

Gives upper and lower bounds on the number of OT's required for both information-theoretic and computationally secure MPC with no honest majority.

[JS07] Stanislaw Jarecki and Vitaly Shmatikov. Efficient two-party secure computation on committed inputs. In *Advances in Cryptology – EUROCRYPT 2007*, pages 97–114, 2007.

Presents a version of Yao's garbled circuit protocol that is secure against malicious adversaries, by means of a protocol for committed oblivious transfer. Construction uses a novel homomorphic cryptosystem. This work, along with subsequent two-party work [IPS09], [LP12], also provides proofs of universal composability for two-party computation.

[Kat07] Jonathan Katz. On achieving the "best of both worlds" in secure multiparty computation. In *Proceedings of the 39th Annual ACM Symposium on Theory of Computing (STOC '07)*, pages 11–20, 2007.

Extends the impossibility result of [IKLP06] to show that fairness for honest majority cannot be combined with privacy in the case of dishonest majority in a protocol of any polynomial number of rounds. Full version, combining results from [IKLP06], is [IKK+11].

[LP07] Yehuda Lindell and Benny Pinkas. An efficient protocol for secure two-party computation in the presence of malicious adversaries. In *Advances in Cryptology – EUROCRYPT 2007*, pages 52–78, 2007.

This paper presents a cut-and-choose technique for strenghtening Yao's two-party protocol to be secure against malicious adversaries. Improved in [LP12].

[NS07] Janus Dam Nielsen and Michael I. Schwartzbach. A domain-specific programming language for secure multiparty computation. In *PLAS*, pages 21–30, 2007.

Presents a Java-like domain specific language (DSL) for programming secure computations. It is written in Java and interfaces with a cryptographic runtime library.

[Woo07] David P. Woodruff. Revisiting the efficiency of malicious two-party computation. In *Advances in Cryptology – EUROCRYPT 2007*, pages 79–96, 2007.

Following on [MF06], provides a more efficient scheme for securing Yao's protocol against a malicious adversary, using expander graphs.

[BH08] Zuzana Beerliov-Trubniov and Martin Hirt. Perfectly-secure MPC with linear communication complexity. In Ran Canetti, editor, *Theory of Cryptography*, volume 4948 of *Lecture Notes in Computer Science*, pages 213–230. Springer Berlin Heidelberg, 2008.

The first *perfectly* secure MPC protocol with linear communication complexity ([DN07] was the first unconditionally secure with error.)

[BDNP08] Assaf Ben-David, Noam Nisan, and Benny Pinkas. FairplayMP: a system for secure multi-party computation. In *ACM Conference on Computer and Communications Security*, pages 257–266, 2008.

New version of Fairplay [MNPS04] for multi-party computation. Implements a variation on the protocol of [BMR90].

[BLW08] Dan Bogdanov, Sven Laur, and Jan Willemson. Sharemind: A framework for fast privacy-preserving computations. In *ESORICS*, pages 192–206, 2008.

An implementation of honest-but-curious three-party secure computation using XOR sharing, with a compiler for a C-like language.

[DT08] Ivan Damgård and Rune Thorbek. Efficient conversion of secret-shared values between different fields. *IACR Cryptology ePrint Archive*, 2008:221, 2008.

More efficient share conversion techniques, along the lines of [CDI05].

[GHKL08] S. Dov Gordon, Carmit Hazay, Jonathan Katz, and Yehuda Lindell. Complete fairness in secure two-party computation. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing (STOC '08)*, pages 413–422, 2008.

Reexamines the impossibility result for fairness in two-party computation, showing that fairness can be obtained for certain classes of functions. Journal version appeared in 2011.

[GMS08] Vipul Goyal, Payman Mohassel, and Adam Smith. Efficient two party and multi party computation against covert adversaries. In *Advances in Cryptology – EUROCRYPT 2008*, pages 289–306, 2008.

Gives an improved, constant-round two-party protocol secure against a covert adversary, and a multi-party protocol that is secure against a covert adversary corrupting a majority of parties.

[HMZ08] Martin Hirt, Ueli M. Maurer, and Vassilis Zikas. Mpc vs. sfe : Unconditional and computational security. In *Advances in Cryptology – ASIACRYPT 2008*, pages 1–18, 2008.

A detailed analysis of the conditions under which general SFE and MPC are possible, in the general mixed adversary model. Verifies the separation between two-party (SFE) and multi-party (MPC).

[HNP08] Martin Hirt, Jesper Buus Nielsen, and Bartosz Przydatek. Asynchronous multi-party computation with quadratic communication. In *ICALP (2)*, pages 473–485, 2008.

A new protocol for asynchronous MPC (see [BCG93]) with up to $n/3$ corrupted parties, which improves the communication complexity to quadratic.

[IKOS08] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Cryptography with constant computational overhead. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing (STOC '08)*, pages 433–442, New York, NY, USA, 2008. ACM.

Work showing the possibility of achieving MPC with constant (times the circuit size) computational overhead. This paper describes what is known as the "MPC-in-the-head" technique.

[KS08a] Vladimir Kolesnikov and Thomas Schneider. A practical universal circuit construction and secure evaluation of private functions. In *Financial Cryptography*, pages 83–97, 2008.

Universal circuits are a construction providing a means of achieving PFE, though inefficiently. This is a simpler construction which is slightly worse than the asymptotic $O(n \log n)$ best, but is claimed to be more efficient practically. See also [KM11].

[KS08b] Vladimir Kolesnikov and Thomas Schneider. Improved garbled circuit: Free XOR gates and applications. In *ICALP (2)*, pages 486–498, 2008.

A major breakthrough in practical efficiency for garbled circuits, showing how XOR gates can be evaluated 'for free', that is, with no communication overhead.

[IPS08] Yuval Ishai, Manoj Prabhakaran, and Amit Sahai. Founding cryptography on oblivious transfer—efficiently. In *Advances in Cryptology – CRYPTO 2008*, pages 572–591, 2008.

Presents a compiler for MPC protocols requiring an honest majority into protocols secure with no honest majority, with improved efficiency over prior results (esp. [Kil88].) These results are in a model with an ideal OT oracle.

[BCD+09] Peter Bogetoft, Dan Lund Christensen, Ivan Damgård, Martin Geisler, Thomas Jakobsen, Mikkel Krøigaard, Janus Dam Nielsen, Jesper Buus Nielsen, Kurt Nielsen, Jakob Pagter, Michael Schwartzbach, and Tomas Toft. Secure multiparty computation goes live. In Roger Dingledine and Philippe Golle, editors, *Financial Cryptography and Data Security*, volume 5628 of *Lecture Notes in Computer Science*, pages 325–343. Springer Berlin Heidelberg, 2009.

The "Danish beet auction" paper, which reports on the first successful large-scale application of MPC.

[CDSMW09] Seung Geol Choi, Dana Dachman-Soled, Tal Malkin, and Hoeteck Wee. Simple, black-box constructions of adaptively secure protocols. In *Theory of Cryptography – TCC 2009*, pages 387–402, 2009.

Gives a black-box transformation of an adaptively secure OT protocol in the semi-honest setting to a protocol secure against a malicious adversary, assuming access to an ideal commitment functionality. However, there are problems with composing this using existing protocols for adaptively secure commitment in the multi-party case. See [GS12].

[CEMY09] Seung Geol Choi, Ariel Elbaz, Tal Malkin, and Moti Yung. Secure multi-party computation minimizing online rounds. In *Advances in Cryptology – ASIACRYPT 2009*, pages 268–286, 2009.

Gives universally composable protocols in the preprocessing model for constant-round multi-party computation, secure against an adversary corrupting an arbitrary number of parties. Provides fairness if there are less than $n/2$ corrupted parties.

[DGKN09] Ivan Damgård, Martin Geisler, Mikkel Krøigaard, and Jesper Buus Nielsen. Asynchronous multiparty computation: Theory and implementation. In *Public Key Cryptography*, pages 160–179, 2009.

Argues that the standard means of strengthening MPC against a malicious adversary are too slow for the internet, since they assume a synchronous network. Gives an MPC protocol with active security in which the minimal number of required synchronization points is enforced. Implementation in the VIFF framework is described.

[Gen09] Craig Gentry. Fully homomorphic encryption using ideal lattices. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC '09)*, pages 169–178, 2009.

The celebrated FHE result, which provides arbitrary computation over encrypted data. Used to construct a sublinear secure computation protocol in [GGH+13].

[GK09] S. Dov Gordon and Jonathan Katz. Complete fairness in multi-party computation without an honest majority. In *Theory of Cryptography – TCC 2009*, pages 19–35, 2009.

Expands the study of [GKHL08] to show classes of functions for which fairness can be obtained in the multi-party setting.

[IMSW09] Yuval Ishai, Tal Malkin, Martin J. Strauss, and Rebecca N. Wright. Private multiparty sampling and approximation of vector combinations. *Theor. Comput. Sci.*, 410(18):1730–1745, 2009.

Extends the approximation work of [FIM+06], and defines a primitive "Private multiparty sampling" which sufficies for general sublinear multi-party computation, similar to [FGM07].

[IPS09] Yuval Ishai, Manoj Prabhakaran, and Amit Sahai. Secure arithmetic computation with no honest majority. In *Theory of Cryptography – TCC 2009*, pages 294–314, 2009.

A new construction for universally composable two-party computation of arithmetic circuits over rings [CFIK03], generalizable to multiparty computation, secure against malicious adversaries corrupting a majority of parties. This technique is also referred to as the *Virtual Multiparty* approach.

[LPV09] Huijia Lin, Rafael Pass, and Muthuramakrishnan Venkitasubramaniam. A unified framework for concurrent security: universal composability from stand-alone non-malleability. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC '09)*, pages 179–188, 2009.

Gives a framework based on *non-malleable commitments* for deriving virtually all results in concurrent secure computation, in both relaxed security models and with trusted setup.

[NO09] Jesper Buus Nielsen and Claudio Orlandi. LEGO for two-party secure computation. In *Theory of Cryptography – TCC 2009*, pages 368–386, 2009.

Provides a novel approach for securing Yao's two-party protocol against malicious adversaries. The circuit constructor sends the receiver many gates, some of which are opened and checked for correctness. Then the two parties interact to 'solder' the gates together into the garbled circuit.

[PSSW09] Benny Pinkas, Thomas Schneider, Nigel P. Smart, and Stephen C. Williams. Secure two-party computation is practical. In *Advances in Cryptology – ASIACRYPT 2009*, pages 250–267, 2009.

Gives experimental results showing the efficiency of computing AES in garbled circuits, incorporating the improvements of [KS08b].

[BHN10] Zuzana Beerliová-Trubíniová, Martin Hirt, and Jesper Buus Nielsen. On the theoretical gap between synchronous and asynchronous mpc protocols. In *Proceedings of the Twenty-ninth Annual ACM Symposium on Principles of Distributed Computing (PODC 2010)*, pages 211–218, 2010.

Shows that the $n/3$ bound on corrupted parties for asynchronous MPC given in [BCG93] can be raised to $n/2$ when given an oracle for input distribution.

[BSMD10] Martin Burkhart, Mario Strasser, Dilip Many, and Xenofontas A. Dimitropoulos. SEPIA: Privacy-preserving aggregation of multi-domain network events and statistics. In *USENIX Security Symposium*, pages 223–240, 2010.

An implementation of secure MPC using Shamir secret sharing in the honest-but-curious model.

[DIK10] Ivan Damgård, Yuval Ishai, and Mikkel Krøigaard. Perfectly secure multiparty computation and the computational overhead of cryptography. In Henri Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 445–465. Springer Berlin Heidelberg, 2010.

A protocol aimed at (asymptotically) minimizing the computational overhead of perfectly-secure MPC with honest majority. The overhead is polylogarithmic in the circuit size and n.

[DK10] Ivan Damgård and Marcel Keller. Secure multiparty aes. In *Financial Cryptography*, pages 367–374, 2010.

Gives performance results for several variations of multiparty AES, implemented in VIFF ([Gei10], [DGKN09]).

[DO10] Ivan Damgård and Claudio Orlandi. Multiparty computation for dishonest majority: From passive to active security at low cost. In *Advances in Cryptology – CRYPTO 2010*, pages 558–576, 2010.

The first major efficiency improvement (over [CLOS02]) for MPC against a dishonest majority, and the beginning of the "preprocessing" papers. Adds security against an active adversary by using a cut-and-choose-style technique rather than zero knowledge. Proven secure in the UC framework. Followed by [BDOZ11] and [DPSZ12].

[Gei10] Martin Geisler. *Cryptographic Protocols: Theory and Implementation*. PhD thesis, Aarhus University, 2010.

Describes the VIFF framework, an implementation of secure MPC on arithmetic shares.

[GJ10] Vipul Goyal and Abhishek Jain. On the round complexity of covert computation. In *Proceedings of the 42nd Annual ACM Symposium on Theory of Computing (STOC '10)*, pages 191–200, 2010.

Following on [GMS08], gives a negative result on the possibility of covert computation in a constant number of rounds.

[HL10a] Carmit Hazay and Yehuda Lindell. Efficient protocols for set intersection and pattern matching with security against malicious and covert adversaries. *Journal of Cryptology*, 23(3):422–456, 2010.

Gives multi-party protocols with improved efficiency for the stated functionalities, first with security against a covert adversary, and then against a malicious adversary, but without a fully simulatable security proof.

[HL10b] Carmit Hazay and Yehuda Lindell. *Efficient Secure Two-Party Protocols – Techniques and Constructions*. Information Security and Cryptography. Springer, 2010.

A textbook introduction to secure two-party computation, which also presents the most efficient two-party constructions as of the publication date.

[HKS+10] Wilko Henecka, Stefan Kögl, Ahmad-Reza Sadeghi, Thomas Schneider, and Immo Wehrenberg. Tasty: Tool for automating secure two-party computations. *IACR Cryptology ePrint Archive*, 2010:365, 2010.

An implementation of secure two-party computation. Uses a hybrid of garbled circuits and homomorphic encryption, with a high-level programming language.

[IKP10] Yuval Ishai, Eyal Kushilevitz, and Anat Paskin. Secure multiparty computation with minimal interaction. In Tal Rabin, editor, *Advances in Cryptology – CRYPTO 2010*, volume 6223 of *Lecture Notes in Computer Science*, pages 577–594. Springer Berlin Heidelberg, 2010.

Work further exploring the achievable limits of round complexity for MPC. Works around the 3-round lower bound of [GIKR02] by giving a secure 2-round protocol in the case that only one party is corrupted.

[LRM10] Christoph Lucas, Dominik Raub, and Ueli M. Maurer. Hybrid-secure mpc: trading information-theoretic robustness for computational privacy. In *Proceedings of the Twenty-ninth Annual ACM Symposium on Principles of Distributed Computing (PODC 2010)*, pages 219–228, 2010.

Generalizes hybrid security results of [Cha89] and [FHW04] to achieve an optimal tradeoff between robustness and privacy in the case when there is a broadcast channel. For a parameter ρ, the protocol is unconditionally secure and robust for up to ρ corrupted parties, unconditionally secure without robusness for up to $n/2$ parties, and secure with abort for up to $n - \rho$ parties.

[ACH11] Gilad Asharov, Ran Canetti, and Carmit Hazay. Towards a game theoretic view of secure computation. In *Advances in Cryptology – EUROCRYPT 2011*, pages 426–445, 2011.

Shows how to formulate the notions of secrecy and correctness in secure computation by statements of game theory, and explores game-theoretic formulations of fairness. Gives an impossibility result for fair two-player computation between rational adversaries (but see [GK12].)

[BDOZ11] Rikke Bendlin, Ivan Damgård, Claudio Orlandi, and Sarah Zakarias. Semi-homomorphic encryption and multiparty computation. In *Advances in Cryptology – EUROCRYPT 2011*, pages 169–188, 2011.

Gives an efficency improvement over [DO10] for the "preprocessing" model of MPC, by using a semi-homomorphic encryption scheme to deal the multiplication triples in the preprocessing phase. UC-secure against dishonest majority. Result is improved by [DPSZ12].

[DHP11] Ivan Damgård, Carmit Hazay, and Arpita Patra. Leakage resilient secure two-party computation. *IACR Cryptology ePrint Archive*, 2011:256, 2011.

A result in the "leakage secure" area. Later shown to be secure only for a subset of functionalities. For further work see [BCH12], [BGJK12], [BGJ+13].

[HIK+11] Iftach Haitner, Yuval Ishai, Eyal Kushilevitz, Yehuda Lindell, and Erez Petrank. Black-box constructions of protocols for secure computation. *SIAM Journal on Computing*, 40(2):225–266, 2011.

Shows how oblivious transfer with security against malicious parties (and thereby, maliciously-secure MPC) can be constructed in a black-box manner from semi-honest oblivious transfer.

[HLMR11] Martin Hirt, Christoph Lucas, Ueli Maurer, and Dominik Raub. Graceful degradation in multi-party computation (extended abstract). In *5th International Conference on Information Theoretic Security (ICITS 2011)*, pages 163–180, 2011.

Generalization of results on hybrid security and mixed adversaries in the unconditional security model, giving protocols that trade the number of corrupted adversaries against security guarantees (privacy, correctness, robustness, fairness.)

[HEKM11] Yan Huang, David Evans, Jonathan Katz, and Lior Malka. Faster secure two-party computation using garbled circuits. In *USENIX Security Symposium*, 2011.

An implementation of garbled circuits, incorporating new techniques to provide significant efficiency improvement over Fairplay. AKA "MightBeEvil".

[IKK+11] Yuval Ishai, Jonathan Katz, Eyal Kushilevitz, Yehuda Lindell, and Erez Petrank. On achieving the "best of both worlds" in secure multiparty computation. *SIAM J. Comput.*, 40(1):122–141, 2011.

The full version of [IKLP06] + [Kat07].

[KM11] Jonathan Katz and Lior Malka. Constant-round private function evaluation with linear complexity. In *Advances in Cryptology – ASIACRYPT 2011*, pages 556–571, 2011.

Result showing constant-round PFE without using universal circuits, using public-key crypto and the DDH assumption. Main result is for the semi-honest model, but malicious is also presented.

[LOP11] Yehuda Lindell, Eli Oxman, and Benny Pinkas. The ips compiler: Optimizations, variants and concrete efficiency. In *Advances in Cryptology–CRYPTO 2011*, pages 259–276. Springer, 2011.

Describes refinements to the IPS compiler [IPS08] that improve its concrete efficiency, and shows new constructions using IPS to obtain covert security.

[SS11] Abhi Shelat and Chih-Hao Shen. Two-output secure computation with malicious adversaries. In *Advances in Cryptology – EUROCRYPT 2011*, pages 386–405, 2011.

An improved analysis of the cut-and-choose method, showing the best possible security bound for a certain class of cut-and-choose approaches. Follow-up work is [HKE13].

[AJL+12] Gilad Asharov, Abhishek Jain, Adriana López-Alt, Eran Tromer, Vinod Vaikuntanathan, and Daniel Wichs. Multiparty computation with low communication, computation and interaction via threshold FHE. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology – EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 483–501. Springer Berlin Heidelberg, 2012.

Shows how to construct an MPC protocol secure against any number of corrupted parties, with a constant number of rounds, from a variant of Gentry's FHE called Threshold FHE.

[BHR12] Mihir Bellare, Viet Tung Hoang, and Phillip Rogaway. Foundations of garbled circuits. In *ACM Conference on Computer and Communications Security*, pages 784–796, 2012.

Provides a more formal definition of circuit garbling as a cryptographic primitive. Also shows flaws in several constructions designed to improve efficiency, and posits new efficiency improvements.

[BFO12] Eli Ben-Sasson, Serge Fehr, and Rafail Ostrovsky. Near-linear unconditionally-secure multiparty computation with a dishonest minority. In *Advances in Cryptology – CRYPTO 2012*, pages 663–680, 2012.

A protocol providing unconditional security against a malicious adversary adaptively corrupting $t < n/2$ players, which matches the communication complexity of the semi-honest case.

[BCH12] Nir Bitansky, Ran Canetti, and Shai Halevi. Leakage-tolerant interactive protocols. In *Theory of Cryptography – TCC 2012*, pages 266–284, 2012.

Defines a new framework based on UC for proving leakage tolerance properties of cryptographic protocols, and presents leakage-resilient protocols for various functionalities that are secure against a semi-honest adversary. See also [DHP11], [BGJK12].

[BGJK12] Elette Boyle, Shafi Goldwasser, Abhishek Jain, and Yael Tauman Kalai. Multiparty computation secure against continual memory leakage. In *Proceedings of the 44th Annual ACM Symposium on Theory of Computing (STOC '12)*, pages 1235–1254, 2012.

A protocol that provides security against an arbitrary number of corrupted parties, as well as against an adversary who can *leak* information about the secret state of each honest party. In contrast to earlier results, the security guarantee obtained is not weakened; however, a leakage-free preprocessing stage is required.

[DKL+12] Ivan Damgård, Marcel Keller, Enrique Larraia, Christian Miles, and Nigel P. Smart. Implementing aes via an actively/covertly secure dishonest-majority mpc protocol. In *SCN*, pages 241–263, 2012.

Describes an implementation of the protocol of [DPSZ12], with modifications to improve efficiency by a covert rather than malicious adversary model. Efficiency results are presented for AES.

[DPSZ12] Ivan Damgård, Valerio Pastro, Nigel P. Smart, and Sarah Zakarias. Multiparty computation from somewhat homomorphic encryption. In *Advances in Cryptology – CRYPTO 2012*, pages 643–662, 2012.

An "offline/online" MPC protocol which is statistically UC-secure against a malicious adversary corrupting up to $n-1$ players, with linear computation and communication complexity in the online phase. The offline phase makes use of somewhat homomorphic encryption.

[GKOV12] Sanjam Garg, Abishek Kumarasubramanian, Rafail Ostrovsky, and Ivan Visconti. Impossibility results for static input secure computation. In *Advances in Cryptology – CRYPTO 2012*, pages 424–442, 2012.

Proof of the impossibility of two-party secure computation in the concurrent setting.

[GS12] Sanjam Garg and Amit Sahai. Adaptively secure multi-party computation with dishonest majority. In *Advances in Cryptology – CRYPTO 2012*, pages 105–123, 2012.

Gives the first MPC protocol secure against a malicious, adaptive ([CFGN96]) adversary with no honest majority, with a constant number of rounds, without requiring trusted setup as in [CLOS02]. The new technique is a non-blackbox simulator.

[GKK+12] S. Dov Gordon, Jonathan Katz, Vladimir Kolesnikov, Fernando Krell, Tal Malkin, Mariana Raykova, and Yevgeniy Vahlis. Secure two-party computation in sublinear (amortized) time. In *ACM Conference on Computer and Communications Security (ACM CCS 2012)*, pages 513–524, 2012.

Shows how to use ORAM for sublinear 2-party secure computation. First result giving amortized sublinear *computation* time.

[GK12] Adam Groce and Jonathan Katz. Fair computation with rational players. In *Advances in Cryptology – EUROCRYPT 2012*, pages 81–98, 2012.

Shows that, unlike the case of malicious parties, there is a protocol for two-party computation between *rational* players that guarantees fairness, as long as the parties have a strict incentive to compute the function—thus circumventing the impossibility result of [ACH11].

[HLMR12] Martin Hirt, Christoph Lucas, Ueli Maurer, and Dominik Raub. Passive corruption in statistical multi-party computation (extended abstract). In *6th International Conference on Information Theoretic Security (ICITS 2012)*, pages 129–146, 2012.

Shows mixed adversary results in the statistical security (as opposed to perfect or computational security) model.

[KSS12a] Benjamin Kreuter, Abhi Shelat, and Chih-Hao Shen. Billion-gate secure computation with malicious adversaries. In *Proceedings of the 21st USENIX Conference on Security*, pages 285–300, Berkeley, CA, USA, 2012.

Futher practical improvements on garbled circuits. This work is accompanied by a publicly-available implementation with a circuit compiler.

[KSS12b] Benjamin Kreuter, Abhi Shelat, and Chih-Hao Shen. Towards billion-gate secure computation with malicious adversaries. *IACR Cryptology ePrint Archive*, 2012:179, 2012.

Full version of [KSS12a].

[LDDA12] John Launchbury, Iavor S. Diatchki, Thomas DuBuisson, and Andy Adams-Moran. Efficient lookup-table protocol in secure multiparty computation. In *ACM SIGPLAN International Conference on Functional Programming (ICFP '12)*, pages 189–200, 2012.

Describes programming-language support for an efficient indexing operation in three-party computation using trivial (XOR) sharing. Experimental results shown for speeding up AES. See also [BLW08].

[LP12] Yehuda Lindell and Benny Pinkas. Secure two-party computation via cut-and-choose oblivious transfer. *J. Cryptology*, 25(4):680–722, 2012.

The paper presents a more efficient cut-and-choose scheme for securing Yao's protocol against malicious adversaries, following up on [LP07].

[MSSZ12] John C. Mitchell, Rahul Sharma, Deian Stefan, and Joe Zimmerman. Information-flow control for programming on encrypted data. In *25th IEEE Computer Security Foundations Symposium (CSF 2012)*, pages 45–60, 2012.

A domain-specific functional language for programming secure computations, which uses a type system to guarantee the security of computations. Interfaces with libraries of secure computation primitives.

[NNOB12] Jesper Buus Nielsen, Peter Sebastian Nordholt, Claudio Orlandi, and Sai Sheshank Burra. A new approach to practical active-secure two-party computation. In *Advances in Cryptology – CRYPTO 2012*, pages 681–700, 2012.

Gives a two-party protocol with implementation that is secure against a malicious adversary, using efficient oblivious transfers rather than garbled circuits. The first 2PC implementation to use the OT approach instead of garbled circuits.

[BHKR13] Mihir Bellare, Viet Tung Hoang, Sriram Keelveedhi, and Phillip Rogaway. Efficient garbling from a fixed-key blockcipher. In *IEEE Symposium on Security and Privacy*, pages 478–492, 2013.

A further efficiency improvement on the garbling operation.

[Bog13] Dan Bogdanov. *Sharemind: programmable secure computations with practical applications*. PhD thesis, University of Tartu, 2013.

A more up-to-date description of the Sharemind [BLW08] system, explaining its programming, performance characteristics and real-world use.

[BGJ+13] Elette Boyle, Sanjam Garg, Abhishek Jain, Yael Tauman Kalai, and Amit Sahai. Secure computation against adaptive auxiliary information. In *Advances in Cryptology – CRYPTO 2013*, 2013.

Builds on results in leakage-secure MPC ([BCH12], [BGTK12]) giving a protocol secure against leaked information that is gained adaptively.

[CHP13] Ashish Choudhury, Martin Hirt, and Arpita Patra. Asynchronous multiparty computation with linear communication complexity. In *Distributed Computing – 27th International Symposium (DISC 2013)*, pages 388–402, 2013.

Gives the first amortized linear-communication *asynchronous* MPC protocols, for up to $n/4$ corrupted parties in the pure asynchronous model with statistical security, and with perfect security in a hybrid setting with one synchronous round.

[CLO+13] Ashish Choudhury, Jake Loftus, Emmanuela Orsini, Arpita Patra, and Nigel P. Smart. Between a rock and a hard place: Interpolating between MPC and FHE. *IACR Cryptology ePrint Archive*, 2013:85, 2013.

Presents a computationally secure MPC protocol which can be tuned to trade off interaction required for multiplication for computation time. The practical result is a highly communication efficient protocol. It belongs to the "bootstrapping" family of protocols.

[DKL+13] Ivan Damgård, Marcel Keller, Enrique Larraia, Valerio Pastro, Peter Scholl, and Nigel P. Smart. Practical covertly secure mpc for dishonest majority – or: Breaking the SPDZ limits. In *18th European Symposium on Research in Computer Security (ESORICS 2013)*, pages 1–18, 2013.

Efficiency improvements on [DPSZ12], particularly for covert adversaries, and supporting reactive functionalities without recomputing the preprocessed data.

[DZ13] Ivan Damgård and Sarah Zakarias. Constant-overhead secure computation of boolean circuits using preprocessing. In Amit Sahai, editor, *Theory of Cryptography*, volume 7785 of *Lecture Notes in Computer Science*, pages 621–641. Springer Berlin Heidelberg, 2013.

The first "preprocessing" result for multi-party the Boolean circuit model of computation (But see NNOB12 for two-party.)

[GGH+13] Craig Gentry, Kenny Goldman, Shai Halevi, Charanjit S. Julta, Mariana Raykova, and Daniel Wichs. Optimizing ORAM and using it efficiently for secure computation. *IACR Cryptology ePrint Archive*, 2013:239, 2013.

An improved (over [GKK+12]) secure-computation-over-ORAM result, employing the somewhat-homomorphic encryption of [Gen09].

[GKP+13] Shafi Goldwasser, Yael Tauman Kalai, Raluca A. Popa, Vinod Vaikuntanathan, and Nickolai Zeldovich. Reusable garbled circuits and succinct functional encryption. In *Proceedings of the 45th Annual ACM Symposium on Theory of Computing (STOC '13)*, pages 555–564, 2013.

Develops a functional encryption scheme with short ciphertexts, which is used to construct a reusable circuit garbling scheme.

[GKM+13] Juan Garay, Jonathan Katz, Ueli Maurer, Björn Tackmann, and Vassilis Zikas. Rational Protocol Design: Cryptography Against Incentive-driven Adversaries. *IACR Cryptology ePrint Archive*, 2013:43, 2013.

Presents a new model of cryptography with rational adversaries, in which the rational agents are not the parties but the protocol *designer* and a protocol *attacker* who tries to break the protocol by corrupting parties. Gives a protocol for multi-party computation which is secure assuming the attacker must "pay" for corrupted parties. To appear in FOCS 2013.

[GMPY11] Juan A. Garay, Philip D. MacKenzie, Manoj Prabhakaran, and Ke Yang. Resource fairness and composability of cryptographic protocols. *J. Cryptology*, 24(4):615–658, 2011.

Journal version of [GMPY06].

[HML13] Martin Hirt, Ueli Maurer, and Christoph Lucas. A dynamic tradeoff between active and passive corruptions in secure multi-party computation. *IACR Cryptology ePrint Archive*, 2013:17, 2013.

A new result in mixed adversary/hybrid security for MPC, which provides a *dynamic tradeoff* between active and passive (semi-honest) corruptions: the number of active and passive corruptions tolerated does not have to be fixed beforehand. The protocol is secure for any k active corruptions as long as fewer than $n - k$ parties are corrupted in total.

[HT13] Martin Hirt and Daniel Tschudi. Efficient general-adversary multi-party computation. *IACR Cryptology ePrint Archive*, 2013:17, 2013.

Gives unconditionally secure general-adversary ([HM00]) protocols with improved efficiency, requiring communication linear in the number of subsets of corrupted players for statistical security, and quadratic for perfect security. The previous results were cubic.

[HKE13] Yan Huang, Jonathan Katz, and Dave Evans. Efficient secure two-party computation using symmetric cut-and-choose. *IACR Cryptology ePrint Archive*, 2013:81, 2013.

Shows how to reduce by a factor of 3 (over [SS11]) the number of garbled circuits required in the cut-and-choose method for security in two-party computation. The innovation is that *both* parties generate garbled circuits to be checked by the other party, hence the title *symmetric* cut-and-choose.

[IKM+13] Yuval Ishai, Eyal Kushilevitz, Sigurd Meldgaard, Claudio Orlandi, and Anat Paskin-Cherniavsky. On the power of correlated randomness in secure computation. In Amit Sahai, editor, *Theory of Cryptography*, volume 7785 of *Lecture Notes in Computer Science*, pages 600–620. Springer Berlin Heidelberg, 2013.

Gives a minimum communication result for MPC, showing a protocol with statistical security against malicious parties with communication linear in the parties' *input* size.

[KMTZ13] Jonathan Katz, Ueli Maurer, Björn Tackmann, and Vassilis Zikas. Universally composable synchronous computation. In *Theory of Cryptography – TCC 2013*, pages 477–498, 2013.

Shows that prior proposals for adding synchrony to the UC framework actually do not provide the expected guarantees of synchrony, and presents a new approach to defining synchrony in UC that does provide input completeness and guaranteed termination.

[Lin13] Yehuda Lindell. Fast cut-and-choose based protocols for malicious and covert adversaries. In *Advances in Cryptology – CRYPTO 2013*, pages 1–17. 2013.

An improvement on the efficiency of cut-and-choose-based two-party protocols, in the case of covert adversaries.

[LO13] Steve Lu and Rafail Ostrovsky. How to garble ram programs. In *Advances in Cryptology – EUROCRYPT 2013*, pages 719–734, 2013.

Achieves secure two-party computation in the RAM model, enabling secure computation with communication complexity sublinear in the input size. Unlike ORAM, this is non-interactive, requiring a constant number of rounds.

[MT13] Daniele Micciancio and Stefano Tessaro. An equational approach to secure multiparty computation. In *Proceedings of the 4th conference on Innovations in Theoretical Computer Science – ITCS 2013*, pages 355–372, 2013.

Presents a new formalism for modeling multi-party computation, with the potential to simplify rigorous reasoning about protocols. The innovation is a formalism using objects of domain theory, in which protocols can be stated without an explicit notion of time.

[MR13] Payman Mohassel and Ben Riva. Garbled circuits checking garbled circuits: More efficient and secure two-party computation. *IACR Cryptology ePrint Archive*, 2013:51, 2013.

A more efficient construction for two-party computation secure against a malicious adversary. The construction uses garbled circuits themselves to check input consistency, and multi-stage cut-and-choose.

[MS13] Payman Mohassel and Seyed Saeed Sadeghian. How to hide circuits in MPC – an efficient framework for private function evaluation. In *Advances in Cryptology – EUROCRYPT 2013*, pages 557–574, 2013.

A new and more efficient construction for constructing PFE on secure two-party and multi-party computation protocols.

[BDO14] Carsten Baum, Ivan Damgrd, and Claudio Orlandi. Publicly auditable secure multiparty computation. *IACR Cryptology ePrint Archive*, 2014:75, 2014.

An augmentation of the SPDZ protocol [DPSZ12] to provide secure auditing, meaning that the transcript of the protocol can be examined after-the-fact to establish that the output was computed correctly.

[BKLS14] Dan Bogdanov, Liina Kamm, Sven Laur, and Ville Sokk. Rmind: a tool for cryptographically secure statistical analysis. *IACR Cryptology ePrint Archive*, 2014:512, 2014.

Describes the implementation of R-like tool for statistical analysis that has an MPC backend.

[KW14] Liina Kamm and Jan Willemson. Secure floating point arithmetic and private satellite collision analysis. *International Journal of Information Security*, pages 1–18, 2014.

A demonstration of numerical analysis and floating-point arithmetic on secret-shared data.

[Kam15] Liina Kamm. *Privacy-preserving statistical analysis using secure multi-party computation.* PhD thesis, University of Tartu, 2015.

Describes the design and implementation of a large-scale privacy-preserving statistical study on MPC, including data cleaning, transformation, linking, aggregating and final analysis.

[PS15] Pille Pullonen and Sander Siim. Combining secret sharing and garbled circuits for efficient private IEEE 754 floating-point computations. In *3rd Workshop on Encrypted Computing and Applied Homomorphic Cryptography (WAHC '15)*, 2015.

Achieves new ways of designing MPC protocols by combining garbled circuits and secret sharing, demonstrated by implementing IEEE 754 floating point arithmetic on Sharemind (See [Bog13]).