A Pragmatic Introduction to Secure Multi-Party Computation

Other titles in Foundations and Trends® in Privacy and Security

Contextual Integrity through the Lens of Computer Science
Sebastian Benthall, Seda Gurses and Helen Nissenbaum
ISBN: 978-1-68083-384-3

Methods for Location Privacy: A comparative overview
Kostantinos Chatzikokolakis, Ehab ElSalamouny, Catuscia Palamidessi and Pazii Anna
ISBN: 978-1-68083-366-9

Principles and Implementation Techniques of Software-Based Fault Isolation
Gang Tan
ISBN: 978-1-68083-344-7

Modeling and Verifying Security Protocols with the Applied Pi Calculus and ProVerif
Bruno Blanchet
ISBN: 978-1-68083-206-8

A Pragmatic Introduction to Secure Multi-Party Computation

David Evans
University of Virginia
evans@virginia.edu

Vladimir Kolesnikov
Georgia Institute of Technology
kolesnikov@gatech.edu

Mike Rosulek
Oregon State University
rosulekm@eecs.oregonstate.edu

now
the essence of knowledge
Boston — Delft

Foundations and Trends® in Privacy and Security

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
United States
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is

D. Evans, V. Kolesnikov and M. Rosulek. *A Pragmatic Introduction to Secure Multi-Party Computation*. Foundations and Trends® in Privacy and Security, vol. 2, no. 2-3, pp. 70–246, 2018.

ISBN: 978-1-68083-509-0

Foundations and Trends® in Privacy and Security
Volume 2, Issue 2-3, 2018

Editorial Board

Editors-in-Chief

Editors

Editorial Scope

Topics

Foundations and Trends® in Privacy and Security publishes survey and tutorial articles in the following topics:

- Access control
- Accountability
- Anonymity
- Application security
- Artifical intelligence methods in security and privacy
- Authentication
- Big data analytics and privacy
- Cloud security
- Cyber-physical systems security and privacy
- Distributed systems security and privacy
- Embedded systems security and privacy
- Forensics
- Hardware security
- Human factors in security and privacy
- Information flow
- Intrusion detection
- Malware
- Metrics
- Mobile security and privacy
- Language-based security and privacy
- Network security
- Privacy-preserving systems
- Protocol security
- Security and privacy policies
- Security architectures
- System security
- Web security and privacy

Information for Librarians

Foundations and Trends® in Privacy and Security, 2018, Volume 2, 4 issues. ISSN paper version 2474-1558. ISSN online version 2474-1566. Also available as a combined paper and online subscription.

Contents

Full text available at: http://dx.doi.org/10.1561/3300000019

A Pragmatic Introduction to Secure Multi-Party Computation

David Evans[1], Vladimir Kolesnikov[2] and Mike Rosulek[3]

[1] *University of Virginia; evans@virginia.edu*
[2] *Georgia Institute of Technology; kolesnikov@gatech.edu*
[3] *Oregon State University; rosulekm@eecs.oregonstate.edu*

ABSTRACT

Secure multi-party computation (MPC) has evolved from a theoretical curiosity in the 1980s to a tool for building real systems today. Over the past decade, MPC has been one of the most active research areas in both theoretical and applied cryptography. This book introduces several important MPC protocols, and surveys methods for improving the efficiency of privacy-preserving applications built using MPC. Besides giving a broad overview of the field and the insights of the main constructions, we overview the most currently active areas of MPC research and aim to give readers insights into what problems are practically solvable using MPC today and how different threat models and assumptions impact the practicality of different approaches.

David Evans, Vladimir Kolesnikov and Mike Rosulek (2018), "A Pragmatic Introduction to Secure Multi-Party Computation", Foundations and Trends® in Privacy and Security: Vol. 2, No. 2-3, pp 70–246. DOI: 10.1561/3300000019.

1

Introduction

Secure multi-party computation (MPC) enable a group to jointly perform a computation without disclosing any participant's private inputs. The participants agree on a function to compute, and then can use an MPC protocol to jointly compute the output of that function on their secret inputs without revealing them. Since its introduction by Andrew Yao in the 1980s, multi-party computation has developed from a theoretical curiosity to an important tool for building large-scale privacy-preserving applications.

This book provides an introduction to multi-party computation for practitioners interested in building privacy-preserving applications and researchers who want to work in the area. We provide an introduction to the foundations of MPC and describe the current state of the art. Our goal is to enable readers to understand what is possible today, and what may be possible in the future, and to provide a starting point for building applications using MPC and for developing MPC protocols, implementations, tools, and applications. As such, we focus on practical aspects, and do not provide formal proofs.

The term *secure computation* is used to broadly encompass all methods for performing computation on data while keeping that data secret. A computation method may also allow participants to confirm the result is indeed the output of the function on the provided inputs, which is known as *verifiable computation*.

There are two main types of secure and verifiable computation: *outsourced computation* and *multi-party computation*. Our focus is on multi-party computation, but first we briefly describe outsourced computation to distinguish it from multi-party computation.

1.1 Outsourced Computation

In an outsourced computation, one party owns the data and wants to be able to obtain the result of computation on that data. The second party receives and stores the data in an encrypted form, performs computation on the encrypted data, and provides the encrypted results to the data owner, without learning anything about the input data, intermediate values, or final result. The data owner can then decrypt the returned results to obtain the output.

Homomorphic encryption allows operations on encrypted data, and is a natural primitive to implement outsourced computation. With *partially-homomorphic encryption* schemes, only certain operations can be performed. Several efficient partially-homomorphic encryption schemes are known (Paillier, 1999; Naccache and Stern, 1998; Boneh *et al.*, 2005). Systems built on them are limited to specialized problems that can be framed in terms of the supported operations.

To provide *fully homomorphic encryption* (FHE), it is necessary to support a Turing-complete set of operations (e.g., both addition and multiplication) so that any function can be computed. Although the goal of FHE was envisioned by Rivest *et al.* (1978), it took more than 30 years before the first FHE scheme was proposed by Gentry (2009), building on lattice-based cryptography. Although there has been much recent interest in implementing FHE schemes Gentry and Halevi (2011), Halevi and Shoup (2014), and Chillotti *et al.* (2016), building secure, deployable, scalable systems using FHE remains an elusive goal.

In their basic forms, FHE and MPC address different aspects of MPC, and as such shouldn't be directly compared. They do, however, provide similar functionalities, and there are ways to adapt FHE to use multiple keys that enables multi-party computation using FHE (Asharov *et al.*, 2012; López-Alt *et al.*, 2012; Mukherjee and Wichs, 2016). FHE offers an asymptotic communication improvement in comparison with MPC, but at the expense of computational efficiency. State-of-the-art FHE implementations (Chillotti *et al.*, 2017) are thousands of times slower than two-party and multi-party secure computation in typical applications and settings considered in literature. Ultimately, the relative performance of FHE and MPC depends on the relative costs of computation and bandwidth. For high-bandwidth settings, such as where devices connected within a data center, MPC vastly outperforms FHE. As FHE techniques improve, and the relative cost of bandwidth over computation increases, FHE-based techniques may eventually become competitive with MPC for many applications.

We do not specifically consider outsourcing computation or FHE further in this book, but note that some of the techniques developed to improve multi-party computation also apply to FHE and outsourcing. Shan *et al.* (2017) provide a survey of work in the area of outsourcing.

1.2 Multi-Party Computation

The goal of secure multi-party computation (MPC) is to enable a group of independent data owners who do not trust each other or any common third party to jointly compute a function that depends on all of their private inputs. MPC differs from outsourced computation in that all of the protocol participants are data owners who participate in executing a protocol. Chapter 2 provides a more formal definition of MPC, and introduces the most commonly considered threat models.

Brief history of MPC. The idea of secure computation was introduced by Andrew Yao in the early 1980s (Yao, 1982). That paper introduced a general notion of secure computation, in which m parties want to jointly compute a function $f(x_1, x_2, \ldots, x_m)$ where x_i is the i^{th} party's private input. In a series of talks over the next few years (but not included in any formal publication), Yao introduced the Garbled Circuits Protocol which we describe in detail in Section 3.1. This protocol remains the basis for many of the most efficient MPC implementations.

Secure computation was primarily of only theoretical interest for the next twenty years; it was not until the 2000s that algorithmic improvements and computing costs had reached a point where it became realistic to think about building practical systems using general-purpose multi-party computation. Fairplay (Malkhi *et al.*, 2004) was the first notable implementation of a general-purpose secure computation system. Fairplay demonstrated the possibility that a privacy-preserving program could be expressed in a high level language and compiled to executables that could be run by the data-owning participants as a multi-party protocol. However, its scalability and performance limited its use to toy programs — the largest application reported in the Fairplay paper was computing the median two sorted arrays where each party's input is ten 16-bit numbers in sorted order, involving execution of 4383 gates and taking over 7 seconds to execute (with both parties connected over a LAN). Since then, the speed of MPC protocols has improved by more than five orders of magnitude due to a combination of cryptographic, protocol, network and hardware improvements. This enabled MPC applications to scale to a wide range of interesting and important applications.

Generic and specialized MPC. Yao's garbled circuits protocol is a *generic* protocol—it can be used to compute any discrete function that can be represented as a fixed-size circuit. One important sub-area of MPC focuses on specific functionalities, such as private set intersection (PSI). For specific functionalities, there may be custom protocols that are much more efficient than the best generic protocols. Specific functionalities can be interesting in their own right, but also can be natural building blocks for use in other applications. We focus mostly on generic MPC protocols, but include discussion of private set intersection (Section 3.8.1) as a particularly useful functionality.

1.3 MPC Applications

MPC enables privacy-preserving applications where multiple mutually distrusting data owners cooperate to compute a function. Here, we highlight a few illustrative examples of privacy-preserving applications that can be built using MPC. This list is far from exhaustive, and is meant merely to give an idea of the range and scale of MPC applications.

Yao's Millionaires Problem. The toy problem that was used to introduce secure computation is not meant as a useful application. Yao (1982) introduces it simply: "Two millionaires wish to know who is richer; however, they do not want to find out inadvertently any additional information about each other's wealth." That is, the goal is to compute the Boolean result of $x_1 \leq x_2$ where x_1 is the first party's private input and x_2 is the second party's private input.

Although its a toy problem, Yao's Millionaires Problem can still be useful for illustrating issues in MPC applications.

Secure auctions. The need for privacy in auctions is well understood. Indeed, it is crucial for all participants, both bidders and sellers, to be able to rely on the privacy and non-malleability of bids. *Bid privacy* requires that no player may learn any other player's bid (other than perhaps revealing the winning bid upon the completion of the auction). *Bid non-malleability* means that a player's bid may not be manipulated to generate a related bid. For example, if a party generates a bid of $\$n$, then another party should not be able to use this bid to produce a bid of $\$n + 1$. Note that bid privacy does not necessarily imply bid non-malleability — indeed it is possible to design auction protocols that would hide a bid of $\$n$ while still allowing others to generate a related bid $\$n + 1$.

These properties are crucial in many standard bidding processes. For example, a sealed bid auction is an auction where bidders submit private (sealed) bids in attempts to purchase property, selling to the highest bidder. Clearly, the first bidder's bid value must be kept secret from other potential bidders to prevent those bidders from having an unfair advantage. Similarly, bid malleability may allow a dishonest bidder Bob to present a bid just slightly over Alice's bid, again, gaining an unfair advantage. Finally, the auction itself must be conducted correctly, awarding the item to the highest bidder for the amount of their bid.

A Vickrey auction is a type of sealed-bid auction where instead paying the value of their own bid, the highest bidder wins but the price paid is the value of the second-highest bid. This type of auction gives bidders an incentive to bid their true value, but requires privacy and non-malleability of each bid, and correctness in determining the winner and price.

MPC can be used to easily achieve all these features since it is only necessary to embed the desired properties into the function used to jointly execute the auction. All the participants can verify the function and then rely on the MPC protocol to provide high confidence that the auction will be conducted confidentially and fairly.

Voting. Secure electronic voting, in a simple form, is simply computation of the addition function which tallies the vote. Privacy and non-malleability of the vote (properties discussed above in the context of auctions) are essential for similar technical reasons. Additionally, because voting is a fundamental civil process, these properties are often asserted by legislation.

As a side note, we remark that voting is an example of an application which may require properties *not covered* by the standard MPC security definitions. In particular, the property of *coercion resistance* is not standard in MPC (but can be formally expressed and achieved (Küsters *et al.*, 2012)). The issue here is the ability of voters to *prove* to a third party how they voted. If such a proof is possible (e.g., a proof might exhibit the randomness used in generating the vote, which the adversary may have seen), then voter coercion is also possible. We don't delve into the specific aspects of secure voting beyond listing it here as a natural application of MPC.

Secure machine learning. MPC can be used to enable privacy in both the inference and training phases of machine learning systems.

Oblivious model inference allows a client to submit a request to a server holding a pre-trained model, keeping the request private from the server $\mathcal{S}$ and the model private from the client $\mathcal{C}$. In this setting, the inputs to the MPC are the private model from $\mathcal{S}$, and the private test input from $\mathcal{C}$, and the output (decoded only for $\mathcal{C}$) is the model's prediction. An example of recent work in this setting include MiniONN (Liu *et al.*, 2017), which provided a mechanism for allowing any standard neural network to be converted to an oblivious model service using a combination of MPC and homomorphic encryption techniques.

In the training phase, MPC can be used to enable a group of parties to train a model based on their combined data without exposing that data. For the large scale data sets needed for most machine learning applications, it is not feasible to perform training across private data sets as a generic many-party computation. Instead, hybrid approaches have been designed that combine MPC with homomorphic encryption (Nikolaenko *et al.*, 2013b; Gascón *et al.*, 2017) or develop custom protocols to perform secure arithmetic operations efficiently (Mohassel and Zhang, 2017). These approaches can scale to data sets containing many millions of elements.

Other applications. Many other interesting applications have been proposed for using MPC to enable privacy. A few examples include privacy-preserving network security monitoring (Burkhart *et al.*, 2010), privacy-preserving genomics (Wang *et al.*, 2015a; Jagadeesh *et al.*, 2017), private stable matching (Doerner *et al.*, 2016), contact discovery (Li *et al.*, 2013; De Cristofaro *et al.*, 2013), ad conversion (Kreuter, 2017), and spam filtering on encrypted email (Gupta *et al.*, 2017).

1.3.1 Deployments

Although MPC has seen much success as a research area and in experimental use, we are still in the early stages of deploying MPC solutions to real problems. Successful deployment of an MPC protocol to solve a problem involving independent and mutually distrusting data owners requires addressing a number of challenging problems beyond the MPC execution itself. Examples of these problems include building confidence in the system that will execute the protocol, understanding what sensitive information might be inferred from the revealed output of the MPC, and enabling decision makers charged with protecting sensitive data but without technical cryptography background to understand the security implications of participating in the MPC.

Despite these challenges, there have been several successful deployments of MPC and a number of companies now focus on providing MPC-based solutions. We emphasize that in this early stage of MPC penetration and awareness, MPC is primarily deployed as an *enabler* of data sharing. In other words, organizations are typically not seeking to use MPC to add a layer of privacy in an otherwise viable application (we believe this is yet forthcoming). Rather, MPC is used to enable a feature or an entire application, which otherwise would not be possible (or would require trust in specialized hardware), due to the value of the shared data, protective privacy legislation, or mistrust of the participants.

Danish sugar beets auction. In what is widely considered to be the first commercial application of MPC, Danish researchers collaborated with the Danish government and stakeholders to create an auction and bidding platform for sugar beet production contracts. As reported in Bogetoft *et al.* (2009), bid privacy and auction security were seen as essential for auction participants. The farmers felt that their bids reflected their capabilities and costs, which they did not want to reveal to Danisco, the only company in Denmark that processed sugar beets. At the same time, Danisco needed to be involved in the auction as the contracts were securities directly affecting the company.

The auction was implemented as a three-party MPC among representatives for Danisco, the farmer's association (DKS) and the researchers (SIMAP project). As explained by Bogetoft *et al.* (2009), a three party solution was selected, partly because it was natural in the given scenario, but also because it allowed using efficient information theoretic tools such as secret sharing. The project led to the formation of a company, Partisia, that uses MPC to support auctions for industries such as spectrum and energy markets, as well as related applications such as data exchange (Gallagher *et al.*, 2017).

Estonian students study. In Estonia, a country with arguably the most advanced e-government and technology awareness, alarms were raised about graduation rates of IT students. Surprisingly, in 2012, nearly 43% of IT students enrolled in the previous five years had failed to graduate. One potential explanation considered was that the IT industry was hiring too aggressively, luring students away from completing their studies. The Estonian Association of Information and Communication Technology wanted to investigate by mining education and tax records to see if there was a correlation. However, privacy legislation prevented data sharing across the Ministry of Education and the Tax Board. In fact, k-anonymity-based sharing was allowed, but it would have resulted in low-quality analysis, since many students would not have had sufficiently large groups of peers with similar qualities.

MPC provided a solution, facilitated by the Estonian company Cybernetica using their Sharemind framework (Bogdanov *et al.*, 2008a). The data analysis was done as a three-party computation, with servers representing the Estonian Information System's Authority, the Ministry of Finance, and Cybernetica. The study, reported in Cybernetica (2015) and Bogdanov (2015), found that there was no correlation between working during studies and failure to graduate on time, but that more education was correlated with higher income.

Boston wage equity study. An initiative of the City of Boston and the Boston Women's Workforce Council (BWWC) aims to identify salary inequities across various employee gender and ethnic demographics at different levels of employment, from executive to entry-level positions. This initiative is widely supported by the Boston area organizations, but privacy concerns prevented direct sharing of salary data. In response, Boston University researchers designed and implemented a web-based MPC aggregation tool, which allowed employers to submit the salary data privately and with full technical and legal protection, for the purposes of the study.

As reported by Bestavros *et al.* (2017), MPC enabled the BWWC to conduct their analysis and produce a report presenting their findings. The effort included a series of meetings with stakeholders to convey the risks and benefits of participating in the MPC, and considered the importance of addressing usability and trust concerns. One indirect result of this work is inclusion of secure multi-party computation as a requirement in a bill for student data analysis recently introduced in the United States Senate (Wyden, 2017).

Key management. One of the biggest problems faced by organizations today is safeguarding sensitive data as it is being used. This is best illustrated using the example of authentication keys. This use case lies at the core of the product offering of Unbound Tech (Unbound Tech, 2018). Unlike other uses of MPC where the goal is to protect data owned by multiple parties from exposure, here the goal is to protect from compromise the data owned by a single entity.

To enable a secure login facility, an organization must maintain private keys. Let's consider the example of shared-key authentication, where each user has shared a randomly chosen secret key with the organization. Each time the user U authenticates, the organization's server S looks up the database of keys and retrieves U's public key sk_U, which is then used to authenticate and admit U to the network by running key exchange.

The security community has long accepted that it is nearly impossible to operate a fully secure complex system, and an adversary will be able to penetrate and stealthily take control over some of the network nodes. Such an advanced adversary, sometimes called Advanced Persistent Threat (APT), aims to quietly undermine the organization. Naturally, the most prized target for APT and other types of attackers is the key server.

MPC can play a significant role in *hardening* the key server by splitting its functionality into two (or more) hosts, say, S_1 and S_2, and secret-sharing key material among the two servers. Now, an attacker must compromise *both* S_1 and S_2 to gain access to the keys. We can run S_1 and S_2 on two different software stacks to minimize the chance that they will both be vulnerable to the exploit available to the malware, and operate them using two different sub-organizations to minimize insider threats. Of course, routine execution does need access to the keys to provide authentication service; at the same time, key should never be reconstructed as the reconstructing party will be the target of the APT attack. Instead, the three players, S_1, S_2, and the authenticating user U, will run the authentication inside MPC, *without ever reconstructing any secrets*, thus removing the singular vulnerability and hardening the defense.

1.4 Overview

Because MPC is a vibrant and active research area, it is possible to cover only a small fraction of the most important work in this book. We mainly discuss generic MPC techniques, focusing mostly on the two-party scenario, and emphasizing a setting where all but one of the parties may be corrupted. In the next chapter, we provide a formal definition of secure multi-party computation and introduce security models that are widely-used in MPC. Although we do not include formal security proofs in this book, it is essential to have clear definitions to understand the specific guarantees that MPC provides. Chapter 3 describes several fundamental MPC protocols, focusing on the most widely-used protocols that resist any number of corruptions. Chapter 4 surveys techniques that have been developed to enable efficient implementations of MPC protocols, and Chapter 5 describes methods that have been used to provide sub-linear memory abstractions for MPC.

Chapters 3–5 target the weak semi-honest adversary model for MPC (defined in Chapter 2), in which is it assumed that all parties follow the protocol as specified. In Chapter 6, we consider how MPC protocols can be hardened to provide security against active adversaries, and Chapter 7 explores some alternative threat models that enable trade-offs between security and efficiency. We conclude in Chapter 8, outlining the trajectory of MPC research and practice, and suggesting possible directions for the future.

References

Afshar, A., Z. Hu, P. Mohassel, and M. Rosulek. 2015. “How to Efficiently Evaluate RAM Programs with Malicious Security”. In: *Advances in Cryptology – EUROCRYPT 2015, Part I*. Ed. by E. Oswald and M. Fischlin. Vol. 9056. *Lecture Notes in Computer Science*. Springer, Heidelberg. 702–729. DOI: 10.1007/978-3-662-46800-5_27.

Aly, A., M. Keller, E. Orsini, D. Rotaru, P. Scholl, N. Smart, and T. Wood. 2018. “SCALE and MAMBA Documentation”. https://homes.esat.kuleuven.be/~nsmart/SCALE/Documentation.pdf.

Ames, S., C. Hazay, Y. Ishai, and M. Venkitasubramaniam. 2017. “Ligero: Lightweight Sublinear Arguments Without a Trusted Setup”. In: *ACM CCS 17: 24th Conference on Computer and Communications Security*. Ed. by B. M. Thuraisingham, D. Evans, T. Malkin, and D. Xu. ACM Press. 2087–2104.

Araki, T., A. Barak, J. Furukawa, T. Lichter, Y. Lindell, A. Nof, K. Ohara, A. Watzman, and O. Weinstein. 2017. “Optimized Honest-Majority MPC for Malicious Adversaries - Breaking the 1 Billion-Gate Per Second Barrier”. In: *2017 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press. 843–862.

Araki, T., J. Furukawa, Y. Lindell, A. Nof, and K. Ohara. 2016. “High-Throughput Semi-Honest Secure Three-Party Computation with an Honest Majority”. In: *ACM CCS 16: 23rd Conference on Computer and Communications Security*. Ed. by E. R. Weippl, S. Katzenbeisser, C. Kruegel, A. C. Myers, and S. Halevi. ACM Press. 805–817.

Asharov, G., A. Beimel, N. Makriyannis, and E. Omri. 2015a. “Complete Characterization of Fairness in Secure Two-Party Computation of Boolean Functions”. In: *TCC 2015: 12th Theory of Cryptography Conference, Part I*. Ed. by Y. Dodis and J. B. Nielsen. Vol. 9014. *Lecture Notes in Computer Science*. Springer, Heidelberg. 199–228. DOI: 10.1007/978-3-662-46494-6_10.

Asharov, G., A. Jain, A. López-Alt, E. Tromer, V. Vaikuntanathan, and D. Wichs. 2012. “Multiparty computation with low communication, computation and interaction via threshold FHE”. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques (EuroCrypt)*. Springer. 483–501.

Asharov, G., Y. Lindell, T. Schneider, and M. Zohner. 2015b. “More Efficient Oblivious Transfer Extensions with Security for Malicious Adversaries”. In: *Advances in Cryptology – EUROCRYPT 2015, Part I*. Ed. by E. Oswald and M. Fischlin. Vol. 9056. *Lecture Notes in Computer Science*. Springer, Heidelberg. 673–701. DOI: 10.1007/978-3-662-46800-5_26.

Asharov, G. and C. Orlandi. 2012. “Calling Out Cheaters: Covert Security with Public Verifiability”. In: *Advances in Cryptology – ASIACRYPT 2012*. Ed. by X. Wang and K. Sako. Vol. 7658. *Lecture Notes in Computer Science*. Springer, Heidelberg. 681–698. DOI: 10.1007/978-3-642-34961-4_41.

Aumann, Y. and Y. Lindell. 2007. “Security Against Covert Adversaries: Efficient Protocols for Realistic Adversaries”. In: *TCC 2007: 4th Theory of Cryptography Conference*. Ed. by S. P. Vadhan. Vol. 4392. *Lecture Notes in Computer Science*. Springer, Heidelberg. 137–156.

Bahmani, R., M. Barbosa, F. Brasser, B. Portela, A.-R. Sadeghi, G. Scerri, and B. Warinschi. 2017. “Secure multiparty computation from SGX”. In: *International Conference on Financial Cryptography and Data Security*. 477–497.

Ball, M., T. Malkin, and M. Rosulek. 2016. “Garbling Gadgets for Boolean and Arithmetic Circuits”. In: *ACM CCS 16: 23rd Conference on Computer and Communications Security*. Ed. by E. R. Weippl, S. Katzenbeisser, C. Kruegel, A. C. Myers, and S. Halevi. ACM Press. 565–577.

Bar-Ilan Center for Research in Applied Cryptography and Cyber Security. 2014. “SCAPI: Secure Computation API”. https://cyber.biu.ac.il/scapi/.

Beaver, D. 1992. “Efficient Multiparty Protocols Using Circuit Randomization”. In: *Advances in Cryptology – CRYPTO’91*. Ed. by J. Feigenbaum. Vol. 576. *Lecture Notes in Computer Science*. Springer, Heidelberg. 420–432.

Beaver, D. 1995. “Precomputing Oblivious Transfer”. In: *Advances in Cryptology – CRYPTO’95*. Ed. by D. Coppersmith. Vol. 963. *Lecture Notes in Computer Science*. Springer, Heidelberg. 97–109.

Beaver, D. 1996. “Correlated Pseudorandomness and the Complexity of Private Computations”. In: *28th Annual ACM Symposium on Theory of Computing*. ACM Press. 479–488.

Beaver, D., S. Micali, and P. Rogaway. 1990. “The Round Complexity of Secure Protocols (Extended Abstract)”. In: *22nd Annual ACM Symposium on Theory of Computing*. ACM Press. 503–513.

Beerliová-Trubíniová, Z. and M. Hirt. 2008. “Perfectly-Secure MPC with Linear Communication Complexity”. In: *TCC 2008: 5th Theory of Cryptography Conference*. Ed. by R. Canetti. Vol. 4948. *Lecture Notes in Computer Science*. Springer, Heidelberg. 213–230.

Beimel, A. and B. Chor. 1993. “Universally Ideal Secret Sharing Schemes (Preliminary Version)”. In: *Advances in Cryptology – CRYPTO’92*. Ed. by E. F. Brickell. Vol. 740. *Lecture Notes in Computer Science*. Springer, Heidelberg. 183–195.

Bellare, M., V. T. Hoang, S. Keelveedhi, and P. Rogaway. 2013. “Efficient Garbling from a Fixed-Key Blockcipher”. In: *2013 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press. 478–492.

Bellare, M., V. T. Hoang, and P. Rogaway. 2012. “Foundations of garbled circuits”. In: *ACM CCS 12: 19th Conference on Computer and Communications Security*. Ed. by T. Yu, G. Danezis, and V. D. Gligor. ACM Press. 784–796.

Bellare, M. and P. Rogaway. 1993. "Random Oracles are Practical: A Paradigm for Designing Efficient Protocols". In: *ACM CCS 93: 1st Conference on Computer and Communications Security*. Ed. by V. Ashby. ACM Press. 62–73.

Ben-Or, M., S. Goldwasser, and A. Wigderson. 1988. "Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation (Extended Abstract)". In: *20th Annual ACM Symposium on Theory of Computing*. ACM Press. 1–10.

Bendlin, R., I. Damgård, C. Orlandi, and S. Zakarias. 2011. "Semi-homomorphic Encryption and Multiparty Computation". In: *Advances in Cryptology – EUROCRYPT 2011*. Ed. by K. G. Paterson. Vol. 6632. *Lecture Notes in Computer Science*. Springer, Heidelberg. 169–188.

Bestavros, A., A. Lapets, and M. Varia. 2017. "User-centric Distributed Solutions for Privacy-preserving Analytics". *Communications of the ACM*. 60(2): 37–39. ISSN: 0001-0782. DOI: 10.1145/3029603.

Biryukov, A., D. Khovratovich, and I. Nikolic. 2009. "Distinguisher and Related-Key Attack on the Full AES-256". In: *Advances in Cryptology – CRYPTO 2009*. Ed. by S. Halevi. Vol. 5677. *Lecture Notes in Computer Science*. Springer, Heidelberg. 231–249.

Bogdanov, D. 2015. "Smarter decisions with no privacy breaches - practical secure computation for governments and companies". https://rwc.iacr.org/2015/Slides/RWC-2015-Bogdanov-final.pdf, retrieved March 9, 2018.

Bogdanov, D., S. Laur, and J. Willemson. 2008a. "Sharemind: A Framework for Fast Privacy-Preserving Computations". In: *ESORICS 2008: 13th European Symposium on Research in Computer Security*. Ed. by S. Jajodia and J. López. Vol. 5283. *Lecture Notes in Computer Science*. Springer, Heidelberg. 192–206.

Bogdanov, D., S. Laur, and J. Willemson. 2008b. "Sharemind: A framework for fast privacy-preserving computations". In: *European Symposium on Research in Computer Security*. Springer. 192–206.

Bogetoft, P., D. L. Christensen, I. Damgård, M. Geisler, T. Jakobsen, M. Krøigaard, J. D. Nielsen, J. B. Nielsen, K. Nielsen, J. Pagter, M. I. Schwartzbach, and T. Toft. 2009. "Secure Multiparty Computation Goes Live". In: *FC 2009: 13th International Conference on Financial Cryptography and Data Security*. Ed. by R. Dingledine and P. Golle. Vol. 5628. *Lecture Notes in Computer Science*. Springer, Heidelberg. 325–343.

Boneh, D., E.-J. Goh, and K. Nissim. 2005. “Evaluating 2-DNF formulas on ciphertexts”. In: *Theory of Cryptography Conference*. Springer. 325–341.

Boyle, E., N. Gilboa, and Y. Ishai. 2016a. “Breaking the circuit size barrier for secure computation under DDH”. In: *Annual Cryptology Conference*. Springer. 509–539.

Boyle, E., N. Gilboa, and Y. Ishai. 2016b. “Function Secret Sharing: Improvements and Extensions”. In: *ACM CCS 16: 23rd Conference on Computer and Communications Security*. Ed. by E. R. Weippl, S. Katzenbeisser, C. Kruegel, A. C. Myers, and S. Halevi. ACM Press. 1292–1303.

Boyle, E., Y. Ishai, and A. Polychroniadou. 2018. “Limits of Practical Sublinear Secure Computation”. In: *Annual Cryptology Conference*. Springer.

Brandão, L. T. A. N. 2013. “Secure Two-Party Computation with Reusable Bit-Commitments, via a Cut-and-Choose with Forge-and-Lose Technique - (Extended Abstract)”. In: *Advances in Cryptology – ASIACRYPT 2013, Part II*. Ed. by K. Sako and P. Sarkar. Vol. 8270. *Lecture Notes in Computer Science*. Springer, Heidelberg. 441–463. DOI: 10.1007/978-3-642-42045-0_23.

Brickell, J., D. E. Porter, V. Shmatikov, and E. Witchel. 2007. “Privacy-preserving remote diagnostics”. In: *ACM CCS 07: 14th Conference on Computer and Communications Security*. Ed. by P. Ning, S. D. C. di Vimercati, and P. F. Syverson. ACM Press. 498–507.

Buescher, N. and S. Katzenbeisser. 2015. “Faster Secure Computation through Automatic Parallelization.” In: *USENIX Security Symposium*. 531–546.

Buescher, N., A. Weber, and S. Katzenbeisser. 2018. “Towards Practical RAM Based Secure Computation”. In: *European Symposium on Research in Computer Security*. Springer. 416–437.

Bulck, J. V., M. Minkin, O. Weisse, D. Genkin, B. Kasikci, F. Piessens, M. Silberstein, T. F. Wenisch, Y. Yarom, and R. Strackx. 2018. “Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution”. In: *27th USENIX Security Symposium*. Baltimore, MD: USENIX Association. 991–1008.

Burkhart, M., M. Strasser, D. Many, and X. Dimitropoulos. 2010. “SEPIA: Privacy-preserving aggregation of multi-domain network events and statistics”. In: *Proceedings of the 19th USENIX Security Symposium*. Washington, DC, USA: USENIX Association.

Calctopia, Inc. 2017. “SECCOMP — The Secure Spreadsheet”. https://www.calctopia.com/.

Canetti, R. 2001. “Universally Composable Security: A New Paradigm for Cryptographic Protocols”. In: *42nd Annual Symposium on Foundations of Computer Science*. IEEE Computer Society Press. 136–145.

Canetti, R., A. Cohen, and Y. Lindell. 2015. “A Simpler Variant of Universally Composable Security for Standard Multiparty Computation”. In: *Advances in Cryptology – CRYPTO 2015, Part II*. Ed. by R. Gennaro and M. J. B. Robshaw. Vol. 9216. *Lecture Notes in Computer Science*. Springer, Heidelberg. 3–22. DOI: 10.1007/978-3-662-48000-7_1.

Canetti, R., O. Goldreich, and S. Halevi. 1998. “The Random Oracle Methodology, Revisited (Preliminary Version)”. In: *30th Annual ACM Symposium on Theory of Computing*. ACM Press. 209–218.

Canetti, R., A. Jain, and A. Scafuro. 2014. “Practical UC security with a Global Random Oracle”. In: *ACM CCS 14: 21st Conference on Computer and Communications Security*. Ed. by G.-J. Ahn, M. Yung, and N. Li. ACM Press. 597–608.

Carter, H., B. Mood, P. Traynor, and K. Butler. 2013. “Secure outsourced Garbled Circuit Evaluation for Mobile Devices”. In: *22nd USENIX Security Symposium*. USENIX Association.

Carter, H., B. Mood, P. Traynor, and K. Butler. 2016. “Secure outsourced garbled circuit evaluation for mobile devices”. *Journal of Computer Security*. 24(2): 137–180.

Cash, D., P. Grubbs, J. Perry, and T. Ristenpart. 2015. “Leakage-Abuse Attacks Against Searchable Encryption”. In: *ACM CCS 15: 22nd Conference on Computer and Communications Security*. Ed. by I. Ray, N. Li, and C. Kruegel: ACM Press. 668–679.

Chan, T.-H. H., K.-M. Chung, B. Maggs, and E. Shi. 2017. “Foundations of Differentially Oblivious Algorithms”. Cryptology ePrint Archive, Report 2017/1033. https://eprint.iacr.org/2017/1033.

Chandran, N., J. A. Garay, P. Mohassel, and S. Vusirikala. 2017. “Efficient, Constant-Round and Actively Secure MPC: Beyond the Three-Party Case”. In: *ACM CCS 17: 24th Conference on Computer and Communications Security*. Ed. by B. M. Thuraisingham, D. Evans, T. Malkin, and D. Xu. ACM Press. 277–294.

Chase, M., D. Derler, S. Goldfeder, C. Orlandi, S. Ramacher, C. Rechberger, D. Slamanig, and G. Zaverucha. 2017. "Post-Quantum Zero-Knowledge and Signatures from Symmetric-Key Primitives". In: *ACM CCS 17: 24th Conference on Computer and Communications Security*. Ed. by B. M. Thuraisingham, D. Evans, T. Malkin, and D. Xu. ACM Press. 1825–1842.

Chaum, D. 1983. "Blind Signature System". In: *Advances in Cryptology – CRYPTO'83*. Ed. by D. Chaum. Plenum Press, New York, USA. 153.

Chaum, D., C. Crépeau, and I. Damgård. 1988. "Multiparty Unconditionally Secure Protocols (Extended Abstract)". In: *20th Annual ACM Symposium on Theory of Computing*. ACM Press. 11–19.

Chillotti, I., N. Gama, M. Georgieva, and M. Izabachène. 2016. "Faster Fully Homomorphic Encryption: Bootstrapping in Less Than 0.1 Seconds". In: *Advances in Cryptology – ASIACRYPT 2016, Part I*. Ed. by J. H. Cheon and T. Takagi. Vol. 10031. *Lecture Notes in Computer Science*. Springer, Heidelberg. 3–33. DOI: 10.1007/978-3-662-53887-6_1.

Chillotti, I., N. Gama, M. Georgieva, and M. Izabachène. 2017. "Faster Packed Homomorphic Operations and Efficient Circuit Bootstrapping for TFHE". In: *Advances in Cryptology – ASIACRYPT 2017, Part I*. Ed. by T. Takagi and T. Peyrin. Vol. 10624. *Lecture Notes in Computer Science*. Springer, Heidelberg. 377–408.

Choi, S. G., K.-W. Hwang, J. Katz, T. Malkin, and D. Rubenstein. 2012a. "Secure Multi-Party Computation of Boolean Circuits with Applications to Privacy in On-Line Marketplaces". In: *Topics in Cryptology – CT-RSA 2012*. Ed. by O. Dunkelman. Vol. 7178. *Lecture Notes in Computer Science*. Springer, Heidelberg. 416–432.

Choi, S. G., J. Katz, R. Kumaresan, and H.-S. Zhou. 2012b. "On the Security of the "Free-XOR" Technique". In: *TCC 2012: 9th Theory of Cryptography Conference*. Ed. by R. Cramer. Vol. 7194. *Lecture Notes in Computer Science*. Springer, Heidelberg. 39–53.

Chor, B., O. Goldreich, E. Kushilevitz, and M. Sudan. 1995. "Private Information Retrieval". In: *36th Symposium on Foundations of Computer Science*. IEEE. 41–50.

Clarke, E., D. Kroening, and F. Lerda. 2004. "A tool for checking ANSI-C programs". In: *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*. Springer. 168–176.

Cleve, R. 1986. "Limits on the Security of Coin Flips when Half the Processors Are Faulty (Extended Abstract)". In: *18th Annual ACM Symposium on Theory of Computing*. ACM Press. 364–369.

Cybernetica. 2015. "Track Big Data Between Government and Education". https://sharemind.cyber.ee/big-data-analytics-protection/, retrieved March 9, 2018.

D'Arco, P. and R. De Prisco. 2014. "Secure Two-Party Computation: A Visual Way". In: *ICITS 13: 7th International Conference on Information Theoretic Security*. Ed. by C. Padró. Vol. 8317. *Lecture Notes in Computer Science*. Springer, Heidelberg. 18–38. doi: 10.1007/978-3-319-04268-8_2.

D'Arco, P. and R. De Prisco. 2016. "Secure computation without computers". 651(Sept.).

Damgård, I. and M. Jurik. 2001. "A generalisation, a simpli. cation and some applications of Paillier's probabilistic public-key system". In: *International Workshop on Public Key Cryptography*. 119–136.

Damgård, I., M. Keller, E. Larraia, C. Miles, and N. P. Smart. 2012a. "Implementing AES via an actively/covertly secure dishonest-majority MPC protocol". In: *International Conference on Security and Cryptography for Networks*. Springer. 241–263.

Damgård, I., J. B. Nielsen, M. Nielsen, and S. Ranellucci. 2017. "The TinyTable Protocol for 2-Party Secure Computation, or: Gate-Scrambling Revisited". In: *Advances in Cryptology – CRYPTO 2017, Part I*. Ed. by J. Katz and H. Shacham. Vol. 10401. *Lecture Notes in Computer Science*. Springer, Heidelberg. 167–187.

Damgård, I., V. Pastro, N. P. Smart, and S. Zakarias. 2012b. "Multiparty Computation from Somewhat Homomorphic Encryption". In: *Advances in Cryptology – CRYPTO 2012*. Ed. by R. Safavi-Naini and R. Canetti. Vol. 7417. *Lecture Notes in Computer Science*. Springer, Heidelberg. 643–662.

Damgård, I. and S. Zakarias. 2013. "Constant-Overhead Secure Computation of Boolean Circuits using Preprocessing". In: *TCC 2013: 10th Theory of Cryptography Conference*. Ed. by A. Sahai. Vol. 7785. *Lecture Notes in Computer Science*. Springer, Heidelberg. 621–641. doi: 10.1007/978-3-642-36594-2_35.

De Cristofaro, E., M. Manulis, and B. Poettering. 2013. "Private Discovery of Common Social Contacts". *International Journal of Information Security*. 12(1): 49–65.

Demmler, D., T. Schneider, and M. Zohner. 2015. "ABY - A Framework for Efficient Mixed-Protocol Secure Two-Party Computation". In: *ISOC Network and Distributed System Security Symposium – NDSS 2015*. The Internet Society.

Dessouky, G., F. Koushanfar, A.-R. Sadeghi, T. Schneider, S. Zeitouni, and M. Zohner. 2017. "Pushing the communication barrier in secure computation using lookup tables". In: *Network and Distributed System Security Symposium*.

Doerner, J., D. Evans, and A. Shelat. 2016. "Secure Stable Matching at Scale". In: *ACM CCS 16: 23rd Conference on Computer and Communications Security*. Ed. by E. R. Weippl, S. Katzenbeisser, C. Kruegel, A. C. Myers, and S. Halevi. ACM Press. 1602–1613.

Doerner, J. and A. Shelat. 2017. "Scaling ORAM for Secure Computation". In: *ACM CCS 17: 24th Conference on Computer and Communications Security*. Ed. by B. M. Thuraisingham, D. Evans, T. Malkin, and D. Xu. ACM Press. 523–535.

Dwork, C. and A. Roth. 2014. "The algorithmic foundations of differential privacy". *Foundations and Trends in Theoretical Computer Science*. 9(3–4): 211–407.

Ejgenberg, Y., M. Farbstein, M. Levy, and Y. Lindell. 2012. "SCAPI: The Secure Computation Application Programming Interface". Cryptology ePrint Archive, Report 2012/629. https://eprint.iacr.org/2012/629.

Faber, S., S. Jarecki, S. Kentros, and B. Wei. 2015. "Three-party ORAM for secure computation". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 360–385.

Fan, X., C. Ganesh, and V. Kolesnikov. 2017. "Hashing Garbled Circuits for Free". In: *Advances in Cryptology – EUROCRYPT 2017, Part II*. Ed. by J. Coron and J. B. Nielsen. Vol. 10211. *Lecture Notes in Computer Science*. Springer, Heidelberg. 456–485.

Fisch, B. A., B. Vo, F. Krell, A. Kumarasubramanian, V. Kolesnikov, T. Malkin, and S. M. Bellovin. 2015. "Malicious-Client Security in Blind Seer: A Scalable Private DBMS". In: *2015 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press. 395–410. DOI: 10.1109/SP.2015.31.

Fraser, C. W. and D. R. Hanson. 1995. *A retargetable C compiler: design and implementation*. Addison-Wesley Longman Publishing Co., Inc.

Frederiksen, T. K., T. P. Jakobsen, J. B. Nielsen, and R. Trifiletti. 2015. "TinyLEGO: An Interactive Garbling Scheme for Maliciously Secure Two-Party Computation". Cryptology ePrint Archive, Report 2015/309. https://eprint.iacr.org/2015/309.

Frederiksen, T. K., T. P. Jakobsen, J. B. Nielsen, P. S. Nordholt, and C. Orlandi. 2013. "MiniLEGO: Efficient Secure Two-Party Computation from General Assumptions". In: *Advances in Cryptology – EUROCRYPT 2013*. Ed. by T. Johansson and P. Q. Nguyen. Vol. 7881. *Lecture Notes in Computer Science*. Springer, Heidelberg. 537–556. DOI: 10.1007/978-3-642-38348-9_32.

Furukawa, J., Y. Lindell, A. Nof, and O. Weinstein. 2017. "High-Throughput Secure Three-Party Computation for Malicious Adversaries and an Honest Majority". In: *Advances in Cryptology – EUROCRYPT 2017, Part II*. Ed. by J. Coron and J. B. Nielsen. Vol. 10211. *Lecture Notes in Computer Science*. Springer, Heidelberg. 225–255.

Gallagher, B., D. Lo, P. F. Frandsen, J. B. Nielsen, and K. Nielsen. 2017. "Insights Network – A Blockchain Data Exchange". https://s3.amazonaws.com/insightsnetwork/InsightsNetworkWhitepaperV0.5.pdf.

Gascón, A., P. Schoppmann, B. Balle, M. Raykova, J. Doerner, S. Zahur, and D. Evans. 2017. "Privacy-Preserving Distributed Linear Regression on High-Dimensional Data". *Proceedings on Privacy Enhancing Technologies*. 2017(4): 248–267.

Gentry, C. 2009. "Fully homomorphic encryption using ideal lattices". In: *41st ACM Symposium on Theory of Computing*.

Gentry, C. and S. Halevi. 2011. "Implementing Gentry's Fully-Homomorphic Encryption Scheme". In: *Advances in Cryptology – EUROCRYPT 2011*. Ed. by K. G. Paterson. Vol. 6632. *Lecture Notes in Computer Science*. Springer, Heidelberg. 129–148.

Giacomelli, I., J. Madsen, and C. Orlandi. 2016. "ZKBoo: Faster Zero-Knowledge for Boolean Circuits". In: *25th USENIX Security Symposium*. Austin, TX: USENIX Association. 1069–1083.

Gilboa, N. and Y. Ishai. 2014. "Distributed Point Functions and Their Applications". In: *Advances in Cryptology – EUROCRYPT 2014*. Ed. by P. Q. Nguyen and E. Oswald. Vol. 8441. *Lecture Notes in Computer Science*. Springer, Heidelberg. 640–658. DOI: 10.1007/978-3-642-55220-5_35.

Goldreich, O. 2004. *Foundations of Cryptography: Volume 2*. Cambridge University Press.

Goldreich, O., S. Micali, and A. Wigderson. 1987. "How to Play any Mental Game or A Completeness Theorem for Protocols with Honest Majority". In: *19th Annual ACM Symposium on Theory of Computing*. Ed. by A. Aho. ACM Press. 218–229.

Goldreich, O. and R. Ostrovsky. 1996. "Software Protection and Simulation on Oblivious RAMs". *Journal of the ACM*. 43(3).

Goldwasser, S. and S. Micali. 1984. "Probabilistic Encryption". *Journal of Computer and System Sciences*. 28(2): 270–299.

Goldwasser, S., S. Micali, and C. Rackoff. 1985. "The Knowledge Complexity of Interactive Proof-Systems (Extended Abstract)". In: *17th Annual ACM Symposium on Theory of Computing*. ACM Press. 291–304.

Gordon, S. D., C. Hazay, J. Katz, and Y. Lindell. 2008. "Complete fairness in secure two-party computation". In: *40th Annual ACM Symposium on Theory of Computing*. Ed. by R. E. Ladner and C. Dwork. ACM Press. 413–422.

Gordon, S. D., J. Katz, V. Kolesnikov, F. Krell, T. Malkin, M. Raykova, and Y. Vahlis. 2012. "Secure two-party computation in sublinear (amortized) time". In: *ACM CCS 12: 19th Conference on Computer and Communications Security*. Ed. by T. Yu, G. Danezis, and V. D. Gligor. ACM Press. 513–524.

Goyal, V., Y. Ishai, A. Sahai, R. Venkatesan, and A. Wadia. 2010. "Founding Cryptography on Tamper-Proof Hardware Tokens". In: *TCC 2010: 7th Theory of Cryptography Conference*. Ed. by D. Micciancio. Vol. 5978. *Lecture Notes in Computer Science*. Springer, Heidelberg. 308–326.

Goyal, V., P. Mohassel, and A. Smith. 2008. "Efficient Two Party and Multi Party Computation Against Covert Adversaries". In: *Advances in Cryptology – EUROCRYPT 2008*. Ed. by N. P. Smart. Vol. 4965. *Lecture Notes in Computer Science*. Springer, Heidelberg. 289–306.

Gueron, S., Y. Lindell, A. Nof, and B. Pinkas. 2015. "Fast Garbling of Circuits Under Standard Assumptions". In: *ACM CCS 15: 22nd Conference on Computer and Communications Security*. Ed. by I. Ray, N. Li, and C. Kruegel: ACM Press. 567–578.

Gupta, D., B. Mood, J. Feigenbaum, K. Butler, and P. Traynor. 2016. "Using Intel Software Guard Extensions for efficient two-party secure function evaluation". In: *International Conference on Financial Cryptography and Data Security*. Springer. 302–318.

Gupta, T., H. Fingler, L. Alvisi, and M. Walfish. 2017. "Pretzel: Email encryption and provider-supplied functions are compatible". In: *Proceedings of the Conference of the ACM Special Interest Group on Data Communication (SIGCOMM)*. ACM. 169–182.

Halevi, S. and V. Shoup. 2014. "Bootstrapping for HElib". Cryptology ePrint Archive, Report 2014/873. https://eprint.iacr.org/2014/873.

Hazay, C. and Y. Lindell. 2008. "Constructions of truly practical secure protocols using standardsmartcards". In: *ACM CCS 08: 15th Conference on Computer and Communications Security*. Ed. by P. Ning, P. F. Syverson, and S. Jha. ACM Press. 491–500.

He, X., A. Machanavajjhala, C. J. Flynn, and D. Srivastava. 2017. "Composing Differential Privacy and Secure Computation: A Case Study on Scaling Private Record Linkage". In: *ACM CCS 17: 24th Conference on Computer and Communications Security*. Ed. by B. M. Thuraisingham, D. Evans, T. Malkin, and D. Xu. ACM Press. 1389–1406.

Henecka, W., S. Kögl, A.-R. Sadeghi, T. Schneider, and I. Wehrenberg. 2010. "TASTY: tool for automating secure two-party computations". In: *ACM CCS 10: 17th Conference on Computer and Communications Security*. Ed. by E. Al-Shaer, A. D. Keromytis, and V. Shmatikov. ACM Press. 451–462.

Hofheinz, D. and V. Shoup. 2011. "GNUC: A New Universal Composability Framework". Cryptology ePrint Archive, Report 2011/303. http://eprint.iacr.org/2011/303.

Holzer, A., M. Franz, S. Katzenbeisser, and H. Veith. 2012. "Secure two-party computations in ANSI C". In: *ACM CCS 12: 19th Conference on Computer and Communications Security*. Ed. by T. Yu, G. Danezis, and V. D. Gligor. ACM Press. 772–783.

Huang, Y., P. Chapman, and D. Evans. 2011a. "Privacy-Preserving Applications on Smartphones". In: *6th USENIX Workshop on Hot Topics in Security*.

Huang, Y., D. Evans, and J. Katz. 2012a. "Private Set Intersection: Are Garbled Circuits Better than Custom Protocols?" In: *ISOC Network and Distributed System Security Symposium – NDSS 2012*. The Internet Society.

Huang, Y., D. Evans, J. Katz, and L. Malka. 2011b. "Faster Secure Two-Party Computation Using Garbled Circuits". In: *20th USENIX Security Symposium*.

Huang, Y., J. Katz, and D. Evans. 2012b. "Quid-Pro-Quo-tocols: Strengthening Semi-honest Protocols with Dual Execution". In: *2012 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press. 272–284.

Huang, Y., J. Katz, V. Kolesnikov, R. Kumaresan, and A. J. Malozemoff. 2014. "Amortizing Garbled Circuits". In: *Advances in Cryptology – CRYPTO 2014, Part II*. Ed. by J. A. Garay and R. Gennaro. Vol. 8617. *Lecture Notes in Computer Science*. Springer, Heidelberg. 458–475. DOI: 10.1007/978-3-662-44381-1_26.

Huang, Y., L. Malka, D. Evans, and J. Katz. 2011c. "Efficient Privacy-Preserving Biometric Identification". In: *ISOC Network and Distributed System Security Symposium – NDSS 2011*. The Internet Society.

Husted, N., S. Myers, A. Shelat, and P. Grubbs. 2013. "GPU and CPU parallelization of honest-but-curious secure two-party computation". In: *Proceedings of the 29th Annual Computer Security Applications Conference*. ACM. 169–178.

Impagliazzo, R. and S. Rudich. 1989. "Limits on the Provable Consequences of One-Way Permutations". In: *21st Annual ACM Symposium on Theory of Computing*. ACM Press. 44–61.

Ishai, Y., J. Kilian, K. Nissim, and E. Petrank. 2003. "Extending Oblivious Transfers Efficiently". In: *Advances in Cryptology – CRYPTO 2003*. Ed. by D. Boneh. Vol. 2729. *Lecture Notes in Computer Science*. Springer, Heidelberg. 145–161.

Ishai, Y., E. Kushilevitz, R. Ostrovsky, and A. Sahai. 2007. "Zero-knowledge from secure multiparty computation". In: *39th Annual ACM Symposium on Theory of Computing*. Ed. by D. S. Johnson and U. Feige. ACM Press. 21–30.

Ishai, Y., M. Prabhakaran, and A. Sahai. 2008. "Founding Cryptography on Oblivious Transfer - Efficiently". In: *Advances in Cryptology – CRYPTO 2008*. Ed. by D. Wagner. Vol. 5157. *Lecture Notes in Computer Science*. Springer, Heidelberg. 572–591.

Islam, M. S., M. Kuzu, and M. Kantarcioglu. 2012. "Access Pattern disclosure on Searchable Encryption: Ramification, Attack and Mitigation". In: *ISOC Network and Distributed System Security Symposium – NDSS 2012*. The Internet Society.

Jagadeesh, K., D. Wu, J. Birgmeier, D. Boneh, and G. Bejerano. 2017. "Deriving Genomic Diagnoses Without Revealing Patient Genomes". *Science*. 357(6352): 692–695.

Jakobsen, T. P., J. B. Nielsen, and C. Orlandi. 2016. "A Framework for Outsourcing of Secure Computation". Cryptology ePrint Archive, Report 2016/037. https://eprint.iacr.org/2016/037 (subsumes earlier version published in 6th ACM Workshop on Cloud Computing Security).

Jarecki, S. and V. Shmatikov. 2007. "Efficient Two-Party Secure Computation on Committed Inputs". In: *Advances in Cryptology – EUROCRYPT 2007*. Ed. by M. Naor. Vol. 4515. *Lecture Notes in Computer Science*. Springer, Heidelberg. 97–114.

Jawurek, M., F. Kerschbaum, and C. Orlandi. 2013. "Zero-knowledge using garbled circuits: how to prove non-algebraic statements efficiently". In: *ACM CCS 13: 20th Conference on Computer and Communications Security*. Ed. by A.-R. Sadeghi, V. D. Gligor, and M. Yung. ACM Press. 955–966.

Juma, A. and Y. Vahlis. 2010. "Protecting Cryptographic Keys against Continual Leakage". In: *Advances in Cryptology – CRYPTO 2010*. Ed. by T. Rabin. Vol. 6223. *Lecture Notes in Computer Science*. Springer, Heidelberg. 41–58.

Kairouz, P., S. Oh, and P. Viswanath. 2015. "Secure multi-party differential privacy". In: *Advances in Neural Information Processing Systems*. 2008–2016.

Kamara, S., P. Mohassel, M. Raykova, and S. S. Sadeghian. 2014. "Scaling Private Set Intersection to Billion-Element Sets". In: *FC 2014: 18th International Conference on Financial Cryptography and Data Security*. Ed. by N. Christin and R. Safavi-Naini. Vol. 8437. *Lecture Notes in Computer Science*. Springer, Heidelberg. 195–215. DOI: 10.1007/978-3-662-45472-5_13.

Kamara, S., P. Mohassel, and B. Riva. 2012. "Salus: a system for server-aided secure function evaluation". In: *ACM CCS 12: 19th Conference on Computer and Communications Security*. Ed. by T. Yu, G. Danezis, and V. D. Gligor. ACM Press. 797–808.

Katz, J. 2007. “Universally Composable Multi-party Computation Using Tamper-Proof Hardware”. In: *Advances in Cryptology – EUROCRYPT 2007*. Ed. by M. Naor. Vol. 4515. *Lecture Notes in Computer Science*. Springer, Heidelberg. 115–128.

Katz, J., V. Kolesnikov, and X. Wang. 2018. “Improved Non-Interactive Zero Knowledge with Applications to Post-Quantum Signatures”. Cryptology ePrint Archive, Report 2018/475. https://eprint.iacr.org/2018/475.

Keller, M., E. Orsini, and P. Scholl. 2015. “Actively Secure OT Extension with Optimal Overhead”. In: *Advances in Cryptology – CRYPTO 2015, Part I*. Ed. by R. Gennaro and M. J. B. Robshaw. Vol. 9215. *Lecture Notes in Computer Science*. Springer, Heidelberg. 724–741. doi: 10.1007/978-3-662-47989-6_35.

Keller, M., E. Orsini, and P. Scholl. 2016. “MASCOT: Faster Malicious Arithmetic Secure Computation with Oblivious Transfer”. In: *ACM CCS 16: 23rd Conference on Computer and Communications Security*. Ed. by E. R. Weippl, S. Katzenbeisser, C. Kruegel, A. C. Myers, and S. Halevi. ACM Press. 830–842.

Keller, M., V. Pastro, and D. Rotaru. 2018. “Overdrive: making SPDZ great again”. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 158–189.

Keller, M. and P. Scholl. 2014. “Efficient, oblivious data structures for MPC”. In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 506–525.

Kempka, C., R. Kikuchi, and K. Suzuki. 2016. “How to circumvent the two-ciphertext lower bound for linear garbling schemes”. In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 967–997.

Kennedy, W. S., V. Kolesnikov, and G. T. Wilfong. 2017. “Overlaying Conditional Circuit Clauses for Secure Computation”. In: *Advances in Cryptology – ASIACRYPT 2017, Part II*. Ed. by T. Takagi and T. Peyrin. Vol. 10625. *Lecture Notes in Computer Science*. Springer, Heidelberg. 499–528.

Kerschbaum, F., T. Schneider, and A. Schröpfer. 2014. “Automatic Protocol Selection in Secure Two-Party Computations”. In: *ACNS 14: 12th International Conference on Applied Cryptography and Network Security*. Ed. by I. Boureanu, P. Owesarski, and S. Vaudenay. Vol. 8479. *Lecture Notes in Computer Science*. Springer, Heidelberg. 566–584. DOI: 10.1007/978-3-319-07536-5_33.

Kilian, J. 1988. “Founding Cryptography on Oblivious Transfer”. In: *20th Annual ACM Symposium on Theory of Computing*. ACM Press. 20–31.

Kiraz, M. and B. Schoenmakers. 2006. “A protocol issue for the malicious case of Yao’s garbled circuit construction”. In: *27th Symposium on Information Theory in the Benelux*. 283–290.

Knudsen, L. R. and V. Rijmen. 2007. “Known-Key Distinguishers for Some Block Ciphers”. In: *Advances in Cryptology – ASIACRYPT 2007*. Ed. by K. Kurosawa. Vol. 4833. *Lecture Notes in Computer Science*. Springer, Heidelberg. 315–324.

Kolesnikov, V. 2005. “Gate Evaluation Secret Sharing and Secure One-Round Two-Party Computation”. In: *Advances in Cryptology – ASIACRYPT 2005*. Ed. by B. K. Roy. Vol. 3788. *Lecture Notes in Computer Science*. Springer, Heidelberg. 136–155.

Kolesnikov, V. 2006. “Secure Two-party Computation and Communication”. University of Toronto Ph.D. Thesis.

Kolesnikov, V. 2010. “Truly Efficient String Oblivious Transfer Using Resettable Tamper-Proof Tokens”. In: *TCC 2010: 7th Theory of Cryptography Conference*. Ed. by D. Micciancio. Vol. 5978. *Lecture Notes in Computer Science*. Springer, Heidelberg. 327–342.

Kolesnikov, V. and R. Kumaresan. 2013. “Improved OT Extension for Transferring Short Secrets”. In: *Advances in Cryptology – CRYPTO 2013, Part II*. Ed. by R. Canetti and J. A. Garay. Vol. 8043. *Lecture Notes in Computer Science*. Springer, Heidelberg. 54–70. DOI: 10.1007/978-3-642-40084-1_4.

Kolesnikov, V., R. Kumaresan, M. Rosulek, and N. Trieu. 2016. “Efficient Batched Oblivious PRF with Applications to Private Set Intersection”. In: *ACM CCS 16: 23rd Conference on Computer and Communications Security*. Ed. by E. R. Weippl, S. Katzenbeisser, C. Kruegel, A. C. Myers, and S. Halevi. ACM Press. 818–829.

Kolesnikov, V. and A. J. Malozemoff. 2015. "Public Verifiability in the Covert Model (Almost) for Free". In: *Advances in Cryptology – ASIACRYPT 2015, Part II*. Ed. by T. Iwata and J. H. Cheon. Vol. 9453. *Lecture Notes in Computer Science*. Springer, Heidelberg. 210–235. doi: 10.1007/978-3-662-48800-3_9.

Kolesnikov, V., N. Matania, B. Pinkas, M. Rosulek, and N. Trieu. 2017a. "Practical Multi-party Private Set Intersection from Symmetric-Key Techniques". In: *ACM CCS 17: 24th Conference on Computer and Communications Security*. Ed. by B. M. Thuraisingham, D. Evans, T. Malkin, and D. Xu. ACM Press. 1257–1272.

Kolesnikov, V., P. Mohassel, B. Riva, and M. Rosulek. 2015. "Richer Efficiency/Security Trade-offs in 2PC". In: *TCC 2015: 12th Theory of Cryptography Conference, Part I*. Ed. by Y. Dodis and J. B. Nielsen. Vol. 9014. *Lecture Notes in Computer Science*. Springer, Heidelberg. 229–259. doi: 10.1007/978-3-662-46494-6_11.

Kolesnikov, V., P. Mohassel, and M. Rosulek. 2014. "FleXOR: Flexible Garbling for XOR Gates That Beats Free-XOR". In: *Advances in Cryptology – CRYPTO 2014, Part II*. Ed. by J. A. Garay and R. Gennaro. Vol. 8617. *Lecture Notes in Computer Science*. Springer, Heidelberg. 440–457. doi: 10.1007/978-3-662-44381-1_25.

Kolesnikov, V., J. B. Nielsen, M. Rosulek, N. Trieu, and R. Trifiletti. 2017b. "DUPLO: Unifying Cut-and-Choose for Garbled Circuits". In: *ACM CCS 17: 24th Conference on Computer and Communications Security*. Ed. by B. M. Thuraisingham, D. Evans, T. Malkin, and D. Xu. ACM Press. 3–20.

Kolesnikov, V., A.-R. Sadeghi, and T. Schneider. 2009. "Improved Garbled Circuit Building Blocks and Applications to Auctions and Computing Minima". In: *CANS 09: 8th International Conference on Cryptology and Network Security*. Ed. by J. A. Garay, A. Miyaji, and A. Otsuka. Vol. 5888. *Lecture Notes in Computer Science*. Springer, Heidelberg. 1–20.

Kolesnikov, V., A.-R. Sadeghi, and T. Schneider. 2010. "From Dust to Dawn: Practically Efficient Two-Party Secure Function Evaluation Protocols and their Modular Design". https://eprint.iacr.org/2010/079.

Kolesnikov, V., A.-R. Sadeghi, and T. Schneider. 2013. "A Systematic Approach to Practically Efficient General Two-party Secure Function Evaluation Protocols and Their Modular Design". *J. Comput. Secur.* 21(2): 283–315. ISSN: 0926-227X. URL: http://dl.acm.org/citation.cfm?id=2590614.2590617.

Kolesnikov, V. and T. Schneider. 2008a. "A Practical Universal Circuit Construction and Secure Evaluation of Private Functions". In: *FC 2008: 12th International Conference on Financial Cryptography and Data Security*. Ed. by G. Tsudik. Vol. 5143. *Lecture Notes in Computer Science*. Springer, Heidelberg. 83–97.

Kolesnikov, V. and T. Schneider. 2008b. "Improved Garbled Circuit: Free XOR Gates and Applications". In: *ICALP 2008: 35th International Colloquium on Automata, Languages and Programming, Part II*. Ed. by L. Aceto, I. Damgård, L. A. Goldberg, M. M. Halldórsson, A. Ingólfsdóttir, and I. Walukiewicz. Vol. 5126. *Lecture Notes in Computer Science*. Springer, Heidelberg. 486–498.

Kreuter, B. 2017. "Secure MPC at Google". Real World Crypto.

Kreuter, B., a. shelat abhi, B. Mood, and K. Butler. 2013. "PCF: A Portable Circuit Format for Scalable Two-Party Secure Computation." In: *USENIX Security Symposium*. 321–336.

Küsters, R., T. Truderung, and A. Vogt. 2012. "A game-based definition of coercion resistance and its applications". *Journal of Computer Security*. 20(6): 709–764.

Launchbury, J., I. S. Diatchki, T. DuBuisson, and A. Adams-Moran. 2012. "Efficient lookup-table protocol in secure multiparty computation". In: *ACM SIGPLAN Notices*. Vol. 47. No. 9. ACM. 189–200.

Lee, J., J. Jang, Y. Jang, N. Kwak, Y. Choi, C. Choi, T. Kim, M. Peinado, and B. B. Kang. 2017a. "Hacking in Darkness: Return-oriented Programming Against Secure Enclaves". In: *Proceedings of the 26th USENIX Conference on Security Symposium. SEC'17*. Vancouver, BC, Canada: USENIX Association. 523–539. ISBN: 978-1-931971-40-9. URL: http://dl.acm.org/citation.cfm?id=3241189.3241231.

Lee, S., M.-W. Shih, P. Gera, T. Kim, H. Kim, and M. Peinado. 2017b. "Inferring Fine-grained Control Flow Inside SGX Enclaves with Branch Shadowing". In: *Proceedings of the 26th USENIX Conference on Security Symposium. SEC'17*. Vancouver, BC, Canada: USENIX Association. 557–574. ISBN: 978-1-931971-40-9. URL: http://dl.acm.org/citation.cfm?id=3241189.3241233.

Li, M., S. Yu, N. Cao, and W. Lou. 2013. "Privacy-preserving distributed profile matching in proximity-based mobile social networks". *IEEE Transactions on Wireless Communications*. 12(5): 2024–2033.

Lindell, Y. 2013. "Fast Cut-and-Choose Based Protocols for Malicious and Covert Adversaries". In: *Advances in Cryptology – CRYPTO 2013, Part II*. Ed. by R. Canetti and J. A. Garay. Vol. 8043. *Lecture Notes in Computer Science*. Springer, Heidelberg. 1–17. DOI: 10.1007/978-3-642-40084-1_1.

Lindell, Y. and B. Pinkas. 2007. "An Efficient Protocol for Secure Two-Party Computation in the Presence of Malicious Adversaries". In: *Advances in Cryptology – EUROCRYPT 2007*. Ed. by M. Naor. Vol. 4515. *Lecture Notes in Computer Science*. Springer, Heidelberg. 52–78.

Lindell, Y. and B. Pinkas. 2009. "A Proof of Security of Yao's Protocol for Two-Party Computation". *Journal of Cryptology*. 22(2): 161–188.

Lindell, Y. and B. Pinkas. 2011. "Secure Two-Party Computation via Cut-and-Choose Oblivious Transfer". In: *TCC 2011: 8th Theory of Cryptography Conference*. Ed. by Y. Ishai. Vol. 6597. *Lecture Notes in Computer Science*. Springer, Heidelberg. 329–346.

Lindell, Y., B. Pinkas, and N. P. Smart. 2008. "Implementing Two-Party Computation Efficiently with Security Against Malicious Adversaries". In: *SCN 08: 6th International Conference on Security in Communication Networks*. Ed. by R. Ostrovsky, R. D. Prisco, and I. Visconti. Vol. 5229. *Lecture Notes in Computer Science*. Springer, Heidelberg. 2–20.

Lindell, Y. and B. Riva. 2014. "Cut-and-Choose Yao-Based Secure Computation in the Online/Offline and Batch Settings". In: *Advances in Cryptology – CRYPTO 2014, Part II*. Ed. by J. A. Garay and R. Gennaro. Vol. 8617. *Lecture Notes in Computer Science*. Springer, Heidelberg. 476–494. DOI: 10.1007/978-3-662-44381-1_27.

Lindell, Y. and B. Riva. 2015. “Blazing Fast 2PC in the Offline/Online Setting with Security for Malicious Adversaries”. In: *ACM CCS 15: 22nd Conference on Computer and Communications Security*. Ed. by I. Ray, N. Li, and C. Kruegel: ACM Press. 579–590.

Liu, J., M. Juuti, Y. Lu, and N. Asokan. 2017. “Oblivious Neural Network Predictions via MiniONN Transformations”. In: *ACM CCS 17: 24th Conference on Computer and Communications Security*. Ed. by B. M. Thuraisingham, D. Evans, T. Malkin, and D. Xu. ACM Press. 619–631.

López-Alt, A., E. Tromer, and V. Vaikuntanathan. 2012. “On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption”. In: *44th Annual ACM Symposium on Theory of Computing*. ACM. 1219–1234.

Lu, S. and R. Ostrovsky. 2013. “How to Garble RAM Programs”. In: *Advances in Cryptology – EUROCRYPT 2013*. Ed. by T. Johansson and P. Q. Nguyen. Vol. 7881. *Lecture Notes in Computer Science*. Springer, Heidelberg. 719–734. DOI: 10.1007/978-3-642-38348-9_42.

Malkhi, D., N. Nisan, B. Pinkas, and Y. Sella. 2004. “Fairplay-Secure Two-Party Computation System”. In: *USENIX Security Symposium*.

Marlinspike, M. 2017. “Technology preview: Private contact discovery for Signal”. https://signal.org/blog/private-contact-discovery/.

Micali, S. and L. Reyzin. 2004. “Physically Observable Cryptography (Extended Abstract)”. In: *TCC 2004: 1st Theory of Cryptography Conference*. Ed. by M. Naor. Vol. 2951. *Lecture Notes in Computer Science*. Springer, Heidelberg. 278–296.

Mishra, P., R. Poddar, J. Chen, A. Chiesa, and R. A. Popa. 2018. “Oblix: An Efficient Oblivious Search Index”. In: *2018 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press.

Mohassel, P. and M. Franklin. 2006. “Efficiency Tradeoffs for Malicious Two-Party Computation”. In: *PKC 2006: 9th International Conference on Theory and Practice of Public Key Cryptography*. Ed. by M. Yung, Y. Dodis, A. Kiayias, and T. Malkin. Vol. 3958. *Lecture Notes in Computer Science*. Springer, Heidelberg. 458–473.

Mohassel, P. and B. Riva. 2013. “Garbled Circuits Checking Garbled Circuits: More Efficient and Secure Two-Party Computation”. In: *Advances in Cryptology – CRYPTO 2013, Part II*. Ed. by R. Canetti and J. A. Garay. Vol. 8043. *Lecture Notes in Computer Science*. Springer, Heidelberg. 36–53. DOI: 10.1007/978-3-642-40084-1_3.

Mohassel, P., M. Rosulek, and Y. Zhang. 2015. “Fast and Secure Three-party Computation: The Garbled Circuit Approach”. In: *ACM CCS 15: 22nd Conference on Computer and Communications Security*. Ed. by I. Ray, N. Li, and C. Kruegel: ACM Press. 591–602.

Mohassel, P. and Y. Zhang. 2017. “SecureML: A System for Scalable Privacy-Preserving Machine Learning”. In: *2017 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press. 19–38.

Mood, B., D. Gupta, H. Carter, K. Butler, and P. Traynor. 2016. “Frigate: A validated, extensible, and efficient compiler and interpreter for secure computation”. In: *IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE. 112–127.

Mukherjee, P. and D. Wichs. 2016. “Two round multiparty computation via multi-key FHE”. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques (EuroCrypt)*. Springer. 735–763.

Naccache, D. and J. Stern. 1998. “A New Public Key Cryptosystem Based on Higher Residues”. In: *ACM CCS 98: 5th Conference on Computer and Communications Security*. ACM Press. 59–66.

Naor, M., B. Pinkas, and R. Sumner. 1999. “Privacy Preserving Auctions and Mechanism Design”. In: *1st ACM Conference on Electronic Commerce*.

Naveed, M., S. Kamara, and C. V. Wright. 2015. “Inference Attacks on Property-Preserving Encrypted Databases”. In: *ACM CCS 15: 22nd Conference on Computer and Communications Security*. Ed. by I. Ray, N. Li, and C. Kruegel: ACM Press. 644–655.

Nielsen, J. B., P. S. Nordholt, C. Orlandi, and S. S. Burra. 2012. “A New Approach to Practical Active-Secure Two-Party Computation”. In: *Advances in Cryptology – CRYPTO 2012*. Ed. by R. Safavi-Naini and R. Canetti. Vol. 7417. *Lecture Notes in Computer Science*. Springer, Heidelberg. 681–700.

Nielsen, J. B. and C. Orlandi. 2009. “LEGO for Two-Party Secure Computation”. In: *TCC 2009: 6th Theory of Cryptography Conference*. Ed. by O. Reingold. Vol. 5444. *Lecture Notes in Computer Science*. Springer, Heidelberg. 368–386.

Nikolaenko, V., S. Ioannidis, U. Weinsberg, M. Joye, N. Taft, and D. Boneh. 2013a. "Privacy-preserving matrix factorization". In: *ACM CCS 13: 20th Conference on Computer and Communications Security*. Ed. by A.-R. Sadeghi, V. D. Gligor, and M. Yung. ACM Press. 801–812.

Nikolaenko, V., U. Weinsberg, S. Ioannidis, M. Joye, D. Boneh, and N. Taft. 2013b. "Privacy-Preserving Ridge Regression on Hundreds of Millions of Records". In: *2013 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press. 334–348.

Ohrimenko, O., F. Schuster, C. Fournet, A. Mehta, S. Nowozin, K. Vaswani, and M. Costa. 2016. "Oblivious Multi-Party Machine Learning on Trusted Processors." In: *USENIX Security Symposium*. 619–636.

Ostrovsky, R. and V. Shoup. 1997. "Private Information Storage". In: *ACM Symposium on Theory of Computing*.

Pagh, R. and F. F. Rodler. 2004. "Cuckoo hashing". *J. Algorithms*. 51(2): 122–144. DOI: 10.1016/j.jalgor.2003.12.002.

Paillier, P. 1999. "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes". In: *Advances in Cryptology – EUROCRYPT'99*. Ed. by J. Stern. Vol. 1592. *Lecture Notes in Computer Science*. Springer, Heidelberg. 223–238.

Pappas, V., F. Krell, B. Vo, V. Kolesnikov, T. Malkin, S. G. Choi, W. George, A. D. Keromytis, and S. Bellovin. 2014. "Blind Seer: A Scalable Private DBMS". In: *2014 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press. 359–374. DOI: 10.1109/SP.2014.30.

Patra, A. and D. Ravi. 2018. "On the Exact Round Complexity of Secure Three-Party Computation". In: *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference*. Ed. by H. Shacham and A. Boldyreva. Vol. 10992. *Lecture Notes in Computer Science*. Springer. 425–458. DOI: 10.1007/978-3-319-96881-0.

Peikert, C., V. Vaikuntanathan, and B. Waters. 2008. "A Framework for Efficient and Composable Oblivious Transfer". In: *Advances in Cryptology – CRYPTO 2008*. Ed. by D. Wagner. Vol. 5157. *Lecture Notes in Computer Science*. Springer, Heidelberg. 554–571.

Pettai, M. and P. Laud. 2015. "Combining differential privacy and secure multiparty computation". In: *31st Annual Computer Security Applications Conference*. ACM. 421–430.

Pfitzmann, B. and M. Waidner. 2000. "Composition and Integrity Preservation of Secure Reactive Systems". In: *ACM CCS 00: 7th Conference on Computer and Communications Security*. Ed. by S. Jajodia and P. Samarati. ACM Press. 245–254.

Pinkas, B., T. Schneider, G. Segev, and M. Zohner. 2015. "Phasing: Private Set Intersection Using Permutation-based Hashing". In: *24th USENIX Security Symposium*. Ed. by J. Jung and T. Holz. USENIX Association. 515–530. URL: https://www.usenix.org/conference/usenixsecurity15.

Pinkas, B., T. Schneider, N. P. Smart, and S. C. Williams. 2009. "Secure Two-Party Computation Is Practical". In: *Advances in Cryptology – ASIACRYPT 2009*. Ed. by M. Matsui. Vol. 5912. *Lecture Notes in Computer Science*. Springer, Heidelberg. 250–267.

Pippenger, N. and M. J. Fischer. 1979. "Relations among Complexity Measures". *Journal of the ACM*. 26(2).

Poddar, R., T. Boelter, and R. A. Popa. 2016. "Arx: A strongly encrypted database system." *IACR Cryptology ePrint Archive*. 2016: 591.

Priebe, C., K. Vaswani, and M. Costa. 2018. "EnclaveDB: A Secure Database using SGX". In: *2018 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press.

Rastogi, A., M. A. Hammer, and M. Hicks. 2014. "Wysteria: A Programming Language for Generic, Mixed-Mode Multiparty Computations". In: *2014 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press. 655–670. DOI: 10.1109/SP.2014.48.

Rivest, R. L., L. Adleman, and M. L. Dertouzos. 1978. "On Data Banks and Privacy Homomorphisms". In: *Foundations of Secure Computation*.

Rogaway, P. 1991. "The Round Complexity of Secure Protocols". Massachusetts Institute of Technology Ph.D. Thesis.

Sadeghi, A.-R., T. Schneider, and I. Wehrenberg. 2010. "Efficient Privacy-Preserving Face Recognition". In: *ICISC 09: 12th International Conference on Information Security and Cryptology*. Ed. by D. Lee and S. Hong. Vol. 5984. *Lecture Notes in Computer Science*. Springer, Heidelberg. 229–244.

Schneider, T. and M. Zohner. 2013. “GMW vs. Yao? Efficient Secure Two-Party Computation with Low Depth Circuits”. In: *FC 2013: 17th International Conference on Financial Cryptography and Data Security*. Ed. by A.-R. Sadeghi. Vol. 7859. *Lecture Notes in Computer Science*. Springer, Heidelberg. 275–292. doi: 10.1007/978-3-642-39884-1_23.

Shamir, A. 1979. “How to share a secret”. *Communications of the ACM*. 22(11): 612–613.

Shan, Z., K. Ren, M. Blanton, and C. Wang. 2017. “Practical Secure Computation Outsourcing: A Survey”. *ACM Computing Surveys*.

Shannon, C. E. 1937. “A symbolic analysis of relay and switching circuits”. Massachusetts Institute of Technology Master’s Thesis.

Shaon, F., M. Kantarcioglu, Z. Lin, and L. Khan. 2017. “SGX-BigMatrix: A Practical Encrypted Data Analytic Framework With Trusted Processors”. In: *ACM CCS 17: 24th Conference on Computer and Communications Security*. Ed. by B. M. Thuraisingham, D. Evans, T. Malkin, and D. Xu. ACM Press. 1211–1228.

shelat, a. and C.-H. Shen. 2011. “Two-Output Secure Computation with Malicious Adversaries”. In: *Advances in Cryptology – EUROCRYPT 2011*. Ed. by K. G. Paterson. Vol. 6632. *Lecture Notes in Computer Science*. Springer, Heidelberg. 386–405.

shelat, a. and C.-H. Shen. 2013. “Fast two-party secure computation with minimal assumptions”. In: *ACM CCS 13: 20th Conference on Computer and Communications Security*. Ed. by A.-R. Sadeghi, V. D. Gligor, and M. Yung. ACM Press. 523–534.

Shi, E., T.-H. H. Chan, E. Stefanov, and M. Li. 2011. “Oblivious RAM with $O((\log N)^3)$ Worst-Case Cost”. In: *Advances in Cryptology – ASIACRYPT 2011*. Ed. by D. H. Lee and X. Wang. Vol. 7073. *Lecture Notes in Computer Science*. Springer, Heidelberg. 197–214.

Songhori, E. M., S. U. Hussain, A.-R. Sadeghi, T. Schneider, and F. Koushanfar. 2015. “TinyGarble: Highly Compressed and Scalable Sequential Garbled Circuits”. In: *2015 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press. 411–428. doi: 10.1109/SP.2015.32.

Stefanov, E., M. van Dijk, E. Shi, C. W. Fletcher, L. Ren, X. Yu, and S. Devadas. 2013. “Path ORAM: an extremely simple oblivious RAM protocol”. In: *ACM CCS 13: 20th Conference on Computer and Communications Security*. Ed. by A.-R. Sadeghi, V. D. Gligor, and M. Yung. ACM Press. 299–310.

Unbound Tech. 2018. “How to Control Your Own Keys (CYOK) in the Cloud”. White Paper available from https://www.unboundtech.com.

Wagh, S., P. Cuff, and P. Mittal. 2018. “Differentially Private Oblivious RAM”. *Proceedings on Privacy Enhancing Technologies*. 2018(4): 64–84.

Waksman, A. 1968. “A Permutation Network”. *Journal of the ACM*. 15(1).

Wang, X. S., Y. Huang, T.-H. H. Chan, A. Shelat, and E. Shi. 2014a. “SCORAM: Oblivious RAM for Secure Computation”. In: *ACM CCS 14: 21st Conference on Computer and Communications Security*. Ed. by G.-J. Ahn, M. Yung, and N. Li. ACM Press. 191–202.

Wang, X. S., Y. Huang, Y. Zhao, H. Tang, X. Wang, and D. Bu. 2015a. “Efficient Genome-Wide, Privacy-Preserving Similar Patient Query based on Private Edit Distance”. In: *ACM CCS 15: 22nd Conference on Computer and Communications Security*. Ed. by I. Ray, N. Li, and C. Kruegel: ACM Press. 492–503.

Wang, X. S., K. Nayak, C. Liu, T.-H. H. Chan, E. Shi, E. Stefanov, and Y. Huang. 2014b. “Oblivious Data Structures”. In: *ACM CCS 14: 21st Conference on Computer and Communications Security*. Ed. by G.-J. Ahn, M. Yung, and N. Li. ACM Press. 215–226.

Wang, X., T.-H. H. Chan, and E. Shi. 2015b. “Circuit ORAM: On Tightness of the Goldreich-Ostrovsky Lower Bound”. In: *ACM CCS 15: 22nd Conference on Computer and Communications Security*. Ed. by I. Ray, N. Li, and C. Kruegel: ACM Press. 850–861.

Wang, X., A. J. Malozemoff, and J. Katz. 2017a. “EMP-toolkit: Efficient MultiParty computation toolkit”. https://github.com/emp-toolkit.

Wang, X., S. Ranellucci, and J. Katz. 2017b. “Authenticated Garbling and Efficient Maliciously Secure Two-Party Computation”. In: *ACM CCS 17: 24th Conference on Computer and Communications Security*. Ed. by B. M. Thuraisingham, D. Evans, T. Malkin, and D. Xu. ACM Press. 21–37.

Wang, X., S. Ranellucci, and J. Katz. 2017c. “Global-Scale Secure Multiparty Computation”. In: *ACM CCS 17: 24th Conference on Computer and Communications Security*. Ed. by B. M. Thuraisingham, D. Evans, T. Malkin, and D. Xu. ACM Press. 39–56.

Winternitz, R. S. 1984. “A Secure One-Way Hash Function Built from DES”. In: *IEEE Symposium on Security and Privacy*. 88–88.

Wyden, R. 2017. “S.2169 — Student Right to Know Before You Go Act of 2017”. https://www.congress.gov/bill/115th-congress/senate-bill/2169/.

Xu, Y., W. Cui, and M. Peinado. 2015. "Controlled-Channel Attacks: Deterministic Side Channels for Untrusted Operating Systems". In: *2015 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press. 640–656. DOI: 10.1109/SP.2015.45.

Yao, A. C.-C. 1982. "Protocols for Secure Computations (Extended Abstract)". In: *23rd Annual Symposium on Foundations of Computer Science*. IEEE Computer Society Press. 160–164.

Zahur, S. and D. Evans. 2013. "Circuit Structures for Improving Efficiency of Security and Privacy Tools". In: *2013 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press. 493–507.

Zahur, S. and D. Evans. 2015. "Obliv-C: A Lightweight Compiler for Data-Oblivious Computation". Cryptology ePrint Archive, Report 2015/1153. http://oblivc.org.

Zahur, S., M. Rosulek, and D. Evans. 2015. "Two Halves Make a Whole - Reducing Data Transfer in Garbled Circuits Using Half Gates". In: *Advances in Cryptology – EUROCRYPT 2015, Part II*. Ed. by E. Oswald and M. Fischlin. Vol. 9057. *Lecture Notes in Computer Science*. Springer, Heidelberg. 220–250. DOI: 10.1007/978-3-662-46803-6_8.

Zahur, S., X. S. Wang, M. Raykova, A. Gascón, J. Doerner, D. Evans, and J. Katz. 2016. "Revisiting Square-Root ORAM: Efficient Random Access in Multi-party Computation". In: *2016 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press. 218–234. DOI: 10.1109/SP.2016.21.

Zhang, Y., A. Steele, and M. Blanton. 2013. "PICCO: a general-purpose compiler for private distributed computation". In: *ACM CCS 13: 20th Conference on Computer and Communications Security*. Ed. by A.-R. Sadeghi, V. D. Gligor, and M. Yung. ACM Press. 813–826.

Zheng, W., A. Dave, J. G. Beekman, R. A. Popa, J. E. Gonzalez, and I. Stoica. 2017. "Opaque: An Oblivious and Encrypted Distributed Analytics Platform". In: *NSDI*. 283–298.

Zhu, R. and Y. Huang. 2017. "JIMU: Faster LEGO-Based Secure Computation Using Additive Homomorphic Hashes". In: *Advances in Cryptology – ASIACRYPT 2017, Part II*. Ed. by T. Takagi and T. Peyrin. Vol. 10625. *Lecture Notes in Computer Science*. Springer, Heidelberg. 529–572.

Zhu, R., Y. Huang, and D. Cassel. 2017. “Pool: Scalable On-Demand Secure Computation Service Against Malicious Adversaries”. In: *ACM CCS 17: 24th Conference on Computer and Communications Security*. Ed. by B. M. Thuraisingham, D. Evans, T. Malkin, and D. Xu. ACM Press. 245–257.

Zhu, R., Y. Huang, J. Katz, and A. Shelat. 2016. “The Cut-and-Choose Game and Its Application to Cryptographic Protocols.” In: *USENIX Security Symposium*. 1085–1100.