Applications of Secure Multiparty Computation
P. Laud and L. Kamm (Eds.)
© 2015 The authors and IOS Press.
This article is published online with Open Access by IOS Press and distributed under the terms of the Creative Commons Attribution Non-Commercial License.
doi:10.3233/978-1-61499-532-6-246

Chapter 12
Practical Applications of Secure Multiparty Computation

Riivo TALVISTE [a]
[a] *Cybernetica AS, Estonia*

Abstract. As secure multiparty computation technology becomes more mature, we see more and more practical applications where computation moves from a lab setting to an actual deployment where each computation node is hosted by a different party. In this chapter, we present some of the practical SMC applications that have worked on real data. A few of these have been developed by Cybernetica AS, while others have been found from public sources. All scientific prototypes or simulations that work on generated or public data have been left out of this chapter. For each chosen SMC application, we give a brief overview and refer the reader to the corresponding published sources for more details.

1. Danish Sugar Beet Auction

1.1. Overview

Secure multiparty computation was first used in a large-scale practical application in Denmark in 2008 when it was used to reallocate sugar beet production contracts between farmers and a sugar production company [1]. SMC technology was used to carry out a double auction that would find the optimal quantities and price for both the farmers and the sugar production company Danisco.

In a double auction, buyers specify the quantity of goods they are willing to buy at each price for a number of different potential prices. Similarly, for each price, sellers give the quantity of goods they are willing to sell. From these bids, an auctioneer computes the *market clearing price* where total demand equals total supply. In this application, the clearing price was computed using secure multiparty computation. This allowed to keep the' production capabilities of individual farmers secret so that the information could not be misused.

1.2. Scheme and Roles

The application was based on 3-party Shamir's secret sharing scheme over a field $\mathbb{Z}_p$, where p is a 64-bit prime number. It was designed for the semi-honest security setting. The three independent computation parties were represented by the sugar production company Danisco, the representative of the farmers (DKS, the sugar beet growers' association) and the SMC technology provider (SIMAP project).

1.3. Process

The whole process was divided into two phases: bidding and tallying. The latter involves secure multiparty computation.

As there were more than a thousand input parties, it was important to make the bidding application easily accessible to the farmers. This was accomplished by distributing the input application as a Java applet accessible from a web page. Each of the 1,229 bidders had the option of submitting a bid for selling, buying or both for 4,000 different prices. It was decided that the three computation parties would not be online during the bidding phase. Thus, instead of sending the input shares directly from the input application to the computation parties, they were stored in a central proxy database. To protect against the reconstruction of shares to the original input value at the proxy server, each individual share was encrypted with a public key of one of the computation parties. These public keys were bundled with the input application and the encryption was performed also in the input application so the original input value never left the application.

The second phase — secure multiparty computation — was carried out in a local setting. First, the representatives of the three computation parties downloaded the shares that were encrypted with their public key from the proxy database, and used their private key to decrypt them. Second, with their decrypted shares they initiated the secure multiparty computation protocol that used about 12 secure comparisons to calculate the market clearing price by binary search. The second phase was done over a 100 Mbit local network (LAN) and took about 30 minutes in total. However, most of it was spent on decrypting individual shares.

1.4. Conclusion

As a result of the application, about 25 tonnes-worth of production rights changed owners [1]. Since its first use in 2008, this application has been used again on subsequent years to reallocate the sugar beet growing contracts in Denmark [2].

2. Financial Data Analysis

2.1. Overview

In 2010, the Estonian Association of Information Technology and Telecommunications (officially abbreviated as ITL), a consortium of ICT companies, decided that it would start periodically collecting and publishing economic benchmarking data on its members to promote their business. The idea was to collect economic indicators such as total return, number of employees, percentage of export, labour costs, profit, and release statistics about these values to ITL member companies so they could quickly react to changes in the economic sector. As such indicators are confidential, it was decided that the data collection and computation would be done using SMC technology [3,4].

2.2. Scheme and Roles

The application was built on the SHAREMIND secure multiparty computation platform that used a three-party additive secret sharing scheme over 32-bit integers. The three

computing parties hosting the servers were ITL members: Zone Media, Microlink and Cybernetica. It must be noted that although the three computation servers were hosted by separate companies, due to the lack of resources, they were administered by the same person. This means that it was not an ideal deployment as this single administrator could potentially recombine the original input.

2.3. Process

As in the Danish secure auction application, the process was split into two phases: data collection and data analysis. An overview of the whole process is given in Fig. 1.

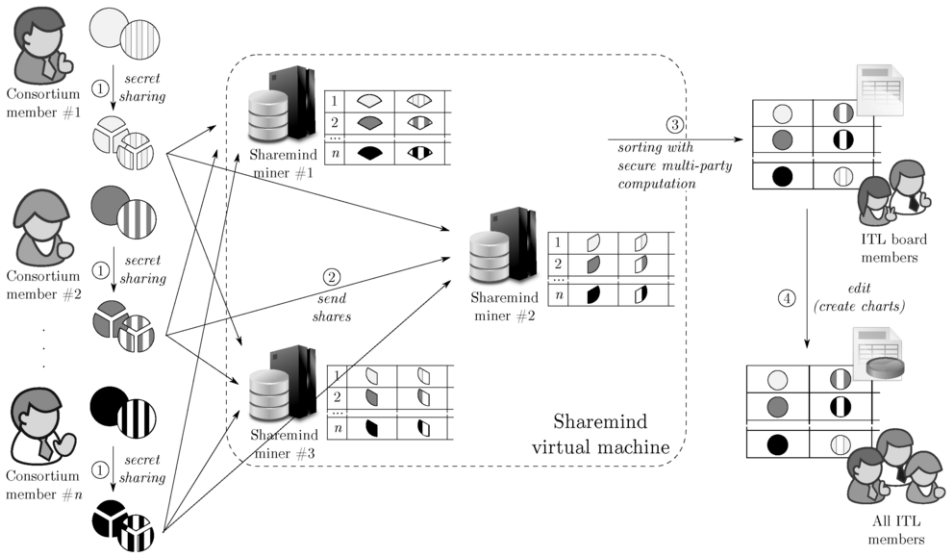

Figure 1. Data flow in the ITL application

Data was collected from ITL members using a a web-based form integrated with the member area of the official web page of ITL. Using the member area allowed ITL members to authenticate themselves to the application using the credentials they already had. In every secure multiparty application, the input values have to be secret shared at the source, in this case the user's web browser. However, instead of encrypting each share with a different public key and sending them all to the same storage server, as was the case with the Danish sugar beet auction, each share was sent directly to a different proxy server over a secure HTTPS channel. Using web-based forms instead of Java applets or other plug-ins is more accessible and transparent for the end user. The three proxy servers were hosted by the three computing parties.

The data analysis phase started after the first phase was completed and the input form was closed. First, each computing party started its SHAREMIND node and input shares were moved from the proxy to the corresponding secure multiparty computation server. For that, each of the computing parties ran a proxy application that loaded shares from the proxy server and contacted the other two proxy applications to coordinate the correct set intersection and order of input shares. After that, the SMC process was triggered and its results were made available to the ITL board, which reviewed the results and

published them to the rest of the ITL members. The secure multiparty computations performed in this applications were simple — the values for each collected economic indicator were sorted independently using the bubble sort algorithm so the ties between different indicators for one company were broken.

2.4. Conclusion

It was the first practical SMC application where computation was carried out over the public Internet. ITL used this application to collect economic health information from its members twice in 2011. After that, the ITL board did not feel the need for the enhanced privacy provided by the application and switched to a more open method of collecting financial data from its members.

3. Privacy-preserving Statistical Studies

3.1. Overview

In Estonia, there is a high drop-out rate among IT students. Universities believe that this is due to the fact that there is high demand for IT specialists on the market, and so a lot of the students are employed during their studies. Consequently, they cannot keep up with their studies and either postpone graduation or drop out altogether. The Estonian Association of Information Technology and Telecommunications (ITL) has put forth a question if and how much does working during one's studies affect graduation on time. The data to answer this question is already there — we could link students' educational records and tax records to see how one's income and work information affect the length of one's studies. However, linking such data poses a privacy risk as tax data is highly confidential. In the EU-funded project "Privacy-preserving statistical studies on linked databases"[1] (PRIST), this privacy risk was mitigated by linking and analyzing educational and tax records using secure multiparty computation technology.

3.2. Scheme and Roles

This study used a newer version of the SHAREMIND platform than the one used in the financial benchmarking application described in Sec. 2. Similarly to the financial data analysis application, it uses a three-party additive secret sharing scheme in the semi-honest security setting, but supports many different data types, including floating point numbers [5] required for implementig statistical analysis methods (see Chapter 4). The three computing parties were the Information Technology Center of the Ministry of Finance, the Estonian Information System Authority, and the technology provider Cybernetica AS. The input data was collected from the Estonian Ministry of Education and Research that holds the education records, and the Estonian Tax and Customs Board that holds tax information. The statistical analysis was carried out by the Estonian Center for Applied Research (CentAR) acting as a result party.

[1] Privacy-preserving statistical studies on linked databases, funded by the European Regional Development Fund from the sub-measure of supporting the development of the R&D of information and communication technology through the Archimedes Foundation: `http://cyber.ee/en/research/research-projects/prist/`

3.3. Process

Each computing party deployed their SHAREMIND server instance on their premises and they were connected over the public Internet using mutually authenticated TLS connections.

In this deployment, there was no need for a widely accessible web interface as there were only two input parties. The input parties first exported a relevant data view from their database, and used a command-line application that secret-shared each individual value. The application also distributed the shares among the computing parties. In total, about 16 million tax records and 200,000 education records were imported into the system. After the data was imported, CentAR used a statistical analysis toolset RMIND [6] to process and query the data using secure multiparty computation.

3.4. Conclusion

The data was imported and the analysis conducted at the beginning of 2015. At the time of writing this book, the analyses were ongoing.

4. Energiauktion.dk — Automated Electricity Broker

Energiauktion.dk[2] is a practical SMC application for electricity procurement for small and medium sized companies in Denmark.

4.1. Deployment and Process

Energiauktion.dk provides electricity procurement as a secure software-as-a-service auction[3]. Thus, it works similarly to the sugar beet auction system described in Sec. 1. However, in the case of Energiauktion.dk, the computing parties are deployed in the Amazon cloud so the actual secure multiparty computation takes place over the public Internet and not over the local network. No more technical details are provided in public documentation.

5. Dyadic Security

5.1. Overview

All modern cryptographic operations are only as secure as the keys used in them. However, in many practical use cases, such as SSL/TLS, the secret key has to be kept online.

Dyadic [7] is a company that takes away this kind of single point of failure by secret sharing the secret key and distributing the shares among many parties. Thus, an attacker, even an insider, must attack all parties to get hold of the key. All operations that require this key (e.g. signing, creating an SSL/TLS connection or other type of encryption) are done using SMC between the parties holding the shares of the secret key. Similarly, this system can be used to check the correctness of the password on login so that the user password database itself is secret shared.

[2] Energiauktion.dk — `https://energiauktion.dk/`

[3] Auctions-as-a-Service — `http://www.partisia.dk/thepartisiaway/pages/aaas.aspx`

5.2. Technology

According to Dyadic's website [8], it uses both secure two-party (Yao garbled circuits) and secure multiparty (SPDZ) computation technologies, and the protocols are secure against an active adversary. Moreover, the system performs periodic resharing of the secrets so that an attacker has only a small timeframe to break into the databases of all the parties holding the shares.

References

[1] Peter Bogetoft, Dan Lund Christensen, Ivan Damgård, Martin Geisler, Thomas P. Jakobsen, Mikkel Krøigaard, Janus Dam Nielsen, Jesper Buus Nielsen, Kurt Nielsen, Jakob Pagter, Michael I. Schwartzbach, and Tomas Toft. Secure multiparty computation goes live. In *Financial Cryptography*, pages 325–343, 2009.

[2] Tomas Toft. The Danish Sugar Beet Auctions. Presented at Privacy Enhancing Cryptography (PEC'11), 2011.

[3] Riivo Talviste. Deploying secure multiparty computation for joint data analysis - a case study. Master's thesis, University of Tartu, 2011.

[4] Dan Bogdanov, Riivo Talviste, and Jan Willemson. Deploying secure multi-party computation for financial data analysis - (short paper). In Angelos D. Keromytis, editor, *Financial Cryptography*, volume 7397 of *Lecture Notes in Computer Science*, pages 57–64. Springer, 2012.

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

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

[7] Dyadic. Dyadic Security White Paper. Technical report, 2014. Published online at `https://www.dyadicsec.com/`.

[8] Dyadic. Secure Computation: A Technical Primer. Technical report, 2014. Published online at `https://www.dyadicsec.com/`.