622.755 – Introduction to Cybersecurity Summer Term, 2022/23

Project Write Up

Massimo Calabrigo 12247382

Contents

1 Introduction

Nowadays cryptography is fast becoming more and more present in the life of the public. Cryptography allows secure HTTP connections through TLS/SSL[8], End to End encryption [6], blockchain technology [9], Multi Party Computation and many more applications [6].
In this work we are going to look at Multi Party Computation (MPC), a branch of cryptography regarding the computation of a shared output between a set of parties, without any party knowing any of the inputs of the others. Specifically we are going to explore two practical use cases of this technology: Double auctions[5] and Genetic Testing [1].

In section 2 we will briefly introduce a MPC solution applied to a double auction.

In section 3 we will see applications of specific MPC solutions: Yao circuits and Homorphic Encryption, used in the context of Generic Testing, a technique used to analyze DNA, while discussing the social and legal implications of Genetic Testing with and without MPC.

2 Danish Sugar Beet Auction

In January 2008 the Danish company "Danisco", which processes Sugar Beets, needed to find the new market price for Sugar Beets due to reduced subsidies from the European Union and lowered prices, and thought to organize an auction in which both the producers and Danisco would state their desidered prices, and a new market price would be computed [5].

The fact that Danisco knew the offers of each producer was a problem though. If Danisco had this information, then it could have learned about the financial situation of every producer, and use these informations against them, so, to solve this problem, Danisco proposed a double auction, that is an auction in which buyers and sellers can propose some price p_i, and then, based on a set of p_i values from both buyers and seller, a market price p would be computed.
To achieve privacy of the offers in the auction MPC was employed, in this way the market price was computed without Danisco knowing the market price proposal of any producer, while everyone having access to the new shared market price.

The MPC solution to the Danish Sugar Beet Auction was advantageous to every party: Danisco ensured that the offers from the producers were honest, and the market price fair, and producers ensured that their offer was secret, and couldn't be used against them by Danisco.

3 DNA and Genetic Testing

DNA is a chemical structure, composed of 4 ”nucleotides”: A,C,T,G , which defines many characteristic of a person, and influences many more.
From DNA, with a set of techniques called Genetic Testing, it is possible to extract informations like predisposal toward good mental health [3], auto-immune conditions [2], and even specific personality traits [4].

3.1 DNA: privacy concerns

Since DNA is the ultimate source of personal information, sharing of this data is particularly dangerous. DNA can reveal information about disease susceptibility and ancestry not only of the individual but of his or her extended family. Disclosure of this information could result in discrimination by insurance companies or reveal unnecessarily intimate information about an individual or even a family member [1]; for these reasons a person should not make public its DNA.

3.2 Extract information from DNA: Genetic Testing

Genetic Testing is a set of techniques performed on a genome, which aims to predict predisposal toward specific diseases or genetic traits, by searching for certain matching subsequences in the genome, breaking the DNA into fragments, using subsequences, and measure their length, finding mismatches in specific positions of the subsequences, . . .

3.2.1 Privacy and Social aspects

If a medical provider wants to perform Genetic Testing on a customer DNA, then the customer should trust the medical provider not to make the DNA public. Even if it’s legally feasible to make a contract such that the medical provider won’t make the genome public, and many genome sequence companies have such privacy policy [10], it could always happen that the customer genome leaks out anyway by hacking, or the company may be sold and the privacy contract would be changed.
In the end the customer has to trust the company, and even if the company has interest in not disappointing this trust, there may be out of control conditions, such as the ones listed earlier, in which data leaks out anyway, and once it happens, all sort of informations of the customer become available 3.

3.2.2 Legal aspects

In the USA, which is currently the largest market in DNA sequencing, the only law protecting DNA privacy is the Genetic Information Non-discrimination Act (GINA) [7], which is a 25 years old law which barring employers and insurance companies access to DNA data, but does nothing to impede a large big data DNA market, which could be

exploited by big companies to better classify their users.
There is much space for legislation in this field not only in the USA, but also in the rest of the world.

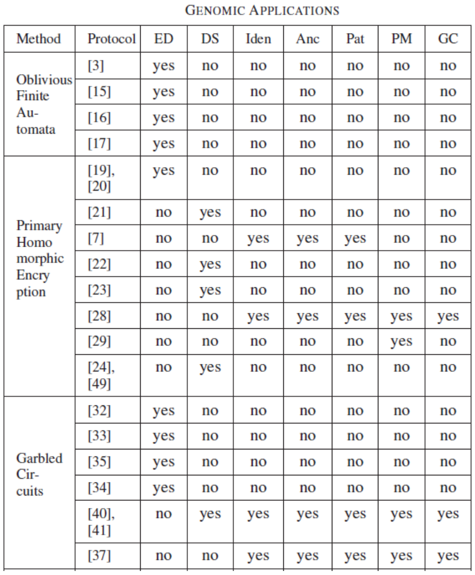
3.3 Genetic Testing and Multi Party Computation

For the aformentioned privacy problems, Genetic Testing requires to do computations on the genome, without knowing it in clear, and this can be achieved by Multi Party Computation.
Various Multi Party Computation solutions have been studied for application in the Genetic Testing problem [1]:

- Yao's Garbled Circuits for the **Edit Distance**, a measure of similarity between subsequences, that is the minimum number of insertions, deletions, and substitutions needed to convert the subsequence a into the subsequence b

- Homomorphic Encryption for **Disease susceptibility**

The result of the application of MPC to Genetic Testing is that with one MPC technique or the other, all the Genetic Testing techniques can be applied (see figure 1) with reasonable efficiency [1], while mantaining both the customer genome and the company specific subsequences private.



GENOMIC APPLICATIONS

Method	Protocol	ED	DS	Iden	Anc	Pat	PM	GC
Oblivious Finite Automata	[3]	yes	no	no	no	no	no	no
	[15]	yes	no	no	no	no	no	no
	[16]	yes	no	no	no	no	no	no
	[17]	yes	no	no	no	no	no	no
Primary Homo morphic Encry ption	[19], [20]	yes	no	no	no	no	no	no
	[21]	no	yes	no	no	no	no	no
	[7]	no	no	yes	yes	yes	no	no
	[22]	no	yes	no	no	no	no	no
	[23]	no	yes	no	no	no	no	no
	[28]	no	no	yes	yes	yes	yes	yes
	[29]	no	no	no	no	no	yes	no
	[24], [49]	no	yes	no	no	no	no	no
Garbled Circuits	[32]	yes	no	no	no	no	no	no
	[33]	yes	no	no	no	no	no	no
	[35]	yes	no	no	no	no	no	no
	[34]	yes	no	no	no	no	no	no
	[40], [41]	no	yes	yes	yes	yes	yes	yes
	[37]	no	no	yes	yes	yes	yes	yes

Figure 1: ED: Edit Distance, DS: Disease Susceptibility, protocol column defines specific implementations of MPC, method column defines different types of MPC, while the remaining columns contains Genetic Testing techniques we didn't cover in this paper. We can see that both Edit Distance and Disease Susceptibility are covered by some MPC technique [1]

4 Conclusions

We saw two main applications of Multi Party Computation: MPC applied to the Sugar Beet Auction protected the privacy of the customers, and impeded the company ”Danisco” to exploit the offer proposals to infer their financial situations, while MPC applied to Genetic Testing enabled both the customer to not revealing his genome, and the medical provider not revealing for which specific subsequences it tested the genome with, hence protecting both the privacy of the customer, and the privacy of the medical provider.

MPC shows itself as a promising and effective technique in all that cases where an output must be computed without the parties knowing the inputs of the other parties, and without needing to trust a central authority.
In the case of Genetic Testing MPC solves the problem of trusting DNA to a company, hence, in order to ensure DNA privacy, it should become standard for medical providers and DNA sequencing companies to use this technique.

References

[1] A Survey of Secure Multiparty Computation Protocols for Privacy Preserving Genetic Tests, *IEEE First International Conference on Connected Health: Applications, Systems and Engineering Technologies*, 2016.

[2] Cracking the genetic code of autoimmune disease

[3] Looking at My Genes: What Can They Tell Me About My Mental Health?

[4] The genetics of human personality *ICISC*, 2003.

[5] Danish Sugar Beet Auction

[6] How Is Cryptography Used In Applications?

[7] Genetic Information Non-discrimination Act

[8] Transport Layer Security

[9] Blockchain

[10] Vertitas Privacy Policy