Coercion-resistance based on homomorphic encryption schemes

Isaac Misael Olguin Nolasco
Department of Informatics
Technical University of Munich (TUM)
Munich, Germany
isaac.olguin@tum.de

***Abstract*—This document presents an analysis of two online voting systems proposals, which are based on homomorphic encryption and the use of the re-voting paradigm against coercion attacks. When both ideas are merged, it is possible to suggest a realistic approach given the feasibility of changes that are required for its implementation in current democracies. It is also stated the reasons why these systems should be considered for the foreseeable voting systems, despite the current risks they face and the challenges on how their security could be improved. Eventually, it is claimed from the author's perspective whether they represent a real solution to contemporary democracies or not.**

***Index Terms*—voting system, cryptography, coercion-resistance, homomorphic encryption**

I. Introduction

By the end of 2019 and the beginning of 2020, nobody was sure of the severe restrictions that everyone would face in the following weeks and months. Even now (June 2021), nobody can measure the damage the Covid-19 will leave in the economy, health, education, and jobs all around the globe. Democracy has not been exempted from those changes [1] and even though voting systems are not a new topic among technological proposals, it has gained special attention given the current circumstances, recent natural disasters and some interference allegations around the last two elections in the United States of America [2]. It is not enough to propose a internet-based system that allows citizens to cast ballots from the comfort of their homes but also a solution that fulfills all requirements for a confident voting system, i.e. anonymity, confidentiality, verifiability, secrecy, usability, integrity, given that such applications are deployed on uncontrolled environments. Due to these reasons: voting systems that take advantage of homomorphic encryption in order to make the system resistant against coercion attacks are analised. Besides, their challenges for real implementations, usability, and ease of use are also considered for the current study.

This work is organized as follows. Section II presents a brief overview of the fundamentals to understand the online voting systems that implement homomorphic encryption. It begins with a simple definition and a list of the coercion types that can take place of such elections. Moreover, there are also presented the two proposals against coercion, the fundamentals of the homomorphic property and two cryptosystems that allows us to perform certain operations on encrypted data. Section III discusses the two views given by Yang [3] and Wouter [4] and a proposal when both perspectives are merged considering the impact, feasibility and its application in current democracies. Finally, the risks and challenges for the implementation of this and other proposals are presented, along with some ideas about how to achieve its usability and the enhancements to consider in the coming future.

II. Fundamentals

Coercion refers to the use of force, threats and/or promises to persuade someone to do something that they are unwilling to do. According to Kempka [5] and Henrich [6], there is a set of coercion attacks against voting schemes that can be classified as follows:

A. Types of coercion

- *Ballot stuffing.* This happens either when a voter can cast a ballot more than once or when people in charge of empty ballots mark them (polling station officer is forced to do it or they have interest in influencing the final result).
- *Vote buying.* An adversary convinces electors to choose or to not choose a specific person by rewarding them in a certain way.
- *Forced abstention.* People are compelled to not exercise their right to vote.
- *Forced randomization.* People are obliged to cast a randomized ballot.
- *Chain voting.* The attacker obtains an empty ballot, marks it according to his preferences and gives it to a voter. This person is coerced and he has to cast the ballot and bring back the new empty ballot he received from the polling station, to the attacker. Such attacker can continue doing this with another voter.
- *Psychological aspects.* The coercer makes the voter believe he is able to detect whether the elector has followed the instructions or not.
- *Pattern voting.* The coercer forces people to vote following a pattern that could help or harm one (or more) of the candidates.
- *Babble attack.* The attacker has a way of communicating with the voter during the voting phase, probably using a remote audio device which is used to interact with the

voter. The coercer gives instructions of how he has to vote.

- *Shoulder voting.* Also known as ”family voting”, in this case confidentiality is not guaranteed (e.g. using an online voting system). Voter can be observed and forced in a certain way by family members, friends or other people.
- *Mixnets and homomorphic encryption.* Suppose an attacker marks its voting slip and it is encrypted using an homomorphic scheme (e.g. ElGamal [7]). He can look at the results after mixing and counting, then he can figure out how other voter cast his ballot. This way the adversary can coerce n citizens.

B. Proposals against coercion

There are two ideas on how to deal with coercion. The first of these suggestions states that each user has fake and valid voting credentials. Therefore, people are responsible for 1) deceiving their coercers, 2) storing their real and fake credentials, 3) understanding how to use them, and 4) making their oppressor believe in them, to later 5) vote with their valid accreditation. Hence, it is not a realistic solution since it implies many assumptions on the acting of voters and leaves more drawbacks than benefits.

On the other hand, there are systems that rely on the called “re-voting paradigm”, i.e. it lets people cast their vote more than once and their last ballot is considered by the election tallying. Nonetheless, according to Wouter [4] there are many assumptions that should be considered such that, the person/people, whose goal is to influence the election, can coerce any voter but not all voters and it is assumed that after coercion and before the end of the election period, this coercer does not control a voter. This is the kind of proposal described herein.

C. Cryptography

1) ***Homomorphism****:* It is defined by Britannica [8] as a *”special correspondence between the members (elements) of two algebraic systems, such as two groups, two rings, or two fields. Two homomorphic systems have the same basic structure, and, while their elements and operations may appear entirely different, results on one system often apply as well to the other system”*. In other words, it is a method that allows performing mathematical operations on encrypted data instead of on the plaintext (”Fig. 1”).

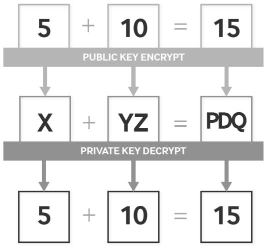

Fig. 1. Source: Adapted from ”PySEAL: A Python wrapper implementation of the SEAL homomorphic encryption library” (p. 2) [9]

2) ***Paillier cryptosystem*** *[10]:* It has additive homomorphism and can be applied to e-voting as follows:

1) Choose two large prime numbers, p and q
2) From numbers, compute:
   - $n = pq$
   - The value of the Carmichael function λ, s.t.

$$\lambda = \text{lcm}(p-1, q-1) \tag{1}$$

3) A random number $g \in \mathbb{Z}^*_{n^2}$ is chosen, s.t. the function L $L(g \mod n^2)$ is invertible $\mod n$ (where $L(u) = \frac{u-1}{n}$).

Hence, the equations for encryption (of the plaintext x) and decryption (of ciphertext y) are (given $r \in \mathbb{Z}^*_n$):

$$\text{Enc}(x, r) = L(y^\lambda \mod n^2) \tag{2}$$

$$\text{Dec}(y) = \frac{L(y^\lambda \mod n^2)}{L(g^\lambda \mod n^2)} \mod n \tag{3}$$

Example [11]: Given three candidates Alice (A), Bob (B), Charlie (C) and six voters, aspirants are assigned with the following number of bits 010000, 000100 and 000001 respectively. Ballots are emitted accordingly to table I.

TABLE I
BALLOT VOTING

Voter	Alice	Bob	Charlie	Bit Score	Decimal value
1			X	000001	1
2		X		000100	4
3		X		000100	4
4			X	000001	1
5	X			010000	16
6			X	000001	1

Assuming $p = 5$ and $q = 7$. It is obtained $n = 35$, $n^2 = 1,225$, and $\lambda = 12$. It is randomly chosen $g = 141$. The cipher text after encryption are shown in table II.

TABLE II
BALLOT VOTING

Voter	Decimal value	Encryption(x,r)
1	1	359
2	4	173
3	4	486
4	1	1,088
5	16	541
6	1	163

Once the time to compute votes has started, all encrypted votes are multiplied and given the additive homomorphism property on the Paillier encryption (i.e. the product of two ciphertexts is equal to the addition of their plain texts when this result is decrypted).
Product:

$$(359 \times 173 \times 486 \times 1,088 \times 541 \times 163) \mod 1,225$$

$$= 983 \mod 1,225$$

Decryption:

$$L(y^{\lambda} \mod n^2) = L(983^{12} \mod 1,225) = \frac{36-1}{35} = 1$$

$$L(g^{\lambda} \mod n^2) = L(141^{12} \mod 1,225) = \frac{456-1}{35} = 13$$

$$\operatorname{dec}(y) = 27$$

when this number is converted to binary representation, it results in 011011, whose interpretation declares Charlie as the winner with three votes.

3) ***ElGamal cryptosystem*** *[7]:* It exhibits multiplicative homomorphism, i.e. if two ciphertexts are multiplied, the decrypted result is equivalent to the multiplication to the original values [12]. It can be applied as follows:

1) A public key is created by selecting a number g, a prime number p and selecting a private key (number) x. Y is computed as $Y = g^x \mod p$.
   Then the public key is (Y, g, p).
2) To encrypt a message M, it is required to select a random value k and then a and b are computed.
   - $a = g^k \mod p$
   - $b = Y^k M \mod p$
3) The encrypted data corresponds to these values $E(M, k) = (a, b)$
4) To decrypt the message, it is performed the following operation $M = \frac{b}{a^x} \mod p$

This cryptosystem works, due to

$$\frac{b}{a^x} \mod p = \frac{y^k M}{(g^k)^x} \mod p = \frac{(g^x)^k M}{(g^k)^x} \mod p$$

$$\frac{g^{xk} M}{g^{xk}} \mod p = M$$

Now, if there were two messages M_1 and M_2, multiplying the encrypted data

$$E(M_1, k_1) = (a_1, b_1)$$

$$E(M_2, k_2) = (a_2, b_2)$$

$$(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$$

$$(g^{k_1} g^{k_2}, Y^{k_1} M_1 Y^{k_2} M_2)$$

$$(g^{k_1+k_2}, Y^{k_1+k_2} M_1 M_2)$$

Decrypting the previous cipher data, we would obtain

$$D(g^{k_1+k_2}, Y^{k_1+k_2} M_1 M_2) = M_1 M_2$$

The main obstacle to use ElGamal in an online voting system is that it exhibits multiplicative homomorphism, whereas such systems require additive homomorphism in order to compute encrypted votes. To do so, the encryption function needs to be modified to exhibit the desired property.

$$E(M, k) = (g^k \mod p, Y^k * g^M \mod p) \tag{4}$$

III. Coercion-Resistant Scheme

This work presents the best of the papers published by Yank [3] on homomorphic encryption's functionality and security in order to fulfill requirements over online voting systems, and Wouter [4] on his approach against coercion given the implementation of the revoting paradigm.

A. Actors

The following actors are considered:

- Voter. Every person who can cast a ballot.
- Candidate. Every person who can be selected and voted by others.
- Polling authority (PA). Responsible for the election, registration of candidates, and process.
- Public Bulleting Board. Public list of all information regarding the ballots, the encrypted data, signatures, proofs and results.
- Tally server (TS). A dedicated IT infrastructure that filters ballots, add data, shuffles, gathers, selects, and tallies.

B. Notation

This paper uses part of the notation stated by [3] (”Tab. III”).

TABLE III
Notation

Notation	Description
n_c	number of candidates
n_v	number of voters
n_a	number of authorities
C_i	i-th candidate $i \in [1, n_c]$
V_i	i-th voter $i \in [1, n_v]$
A_i	i-th authority $i \in [1, n_a]$
B_i	the ballot submitted by V_ii$\in [1, n_v]$
Sig_{V_i}	digital signature of V_i; $i \in [1, n_v]$
pk_{V_i}	public key of V_i; $i \in [1, n_v]$
sk_{V_i}	secret key of V_i; $i \in [1, n_v]$
pk_{A_i}	public key of A_i; $i \in [1, n_a]$
sk_{A_i}	secret key of A_i; $i \in [1, n_a]$
PK	common public key for encrypting ballots

C. Assumptions

- At least, there is one trusted third-party responsible for the election process (polling authority).
- People are provided with their credentials to access the system on the day of the election.
- Credentials are formed by a private key, a public key, and a password.
- Limits on hardware are removed and each voter can access the system from home or another location with access to the internet.
- People know how they have to cast their ballots.
- Coercion takes place during the “voting phase“.
- An attacker can coerce any person but not all voters.
- Absence of coercer after duress and at some point before the end of the valid casting period.
- In contrast with [3], here it is not assumed that a voter can cast their ballot to different candidates (score voting),

assigning different values to each of them. Similarly to paper-based elections, they can only choose one option or their ballot is rejected.
- It can exist either one or more polling authorities. If exists more than one, then all of them are required to compute the result of the election.
- User's credentials are inalienable, i.e. the coercer cannot eliminate nor duplicate them.

D. *Overview of online voting scheme*

Remote voting scheme allows people vote from their homes, jobs or any other location. This implies that voting process is done in an uncontrolled environment where it is more susceptible to large-scale duress. There are three phases in the proposed system:

- Pre-election phase (”Fig. 2”). Every person must be identified and registered into the system such that they are able to vote in the election phase. The government entity or responsible for the election process gives citizens the credentials they have to use to log into the application once the voting phase starts. The third entity must deliver its public key, validate and include all candidates into the system, such that the voters can visualise and choose among them on the day of the election.

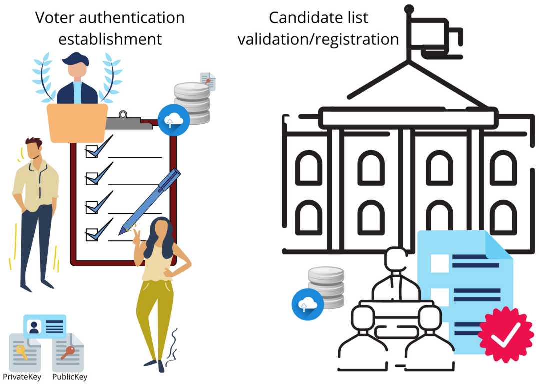
Voter authentication establishment
Candidate list validation/registration
PrivateKey
PublicKey

Fig. 2. Online pre-election phase

- Voting phase (”Fig. 3”). Once the valid period of voting phase starts, valid users are able to use their credentials to log into the application, choose their desired option and cast their ballot. This vote is sent through the internet and received by the BackEnd of the application where different validations are executed and once the ballot has been validated, it is stored into the database until the election voting phase ends and the tallying process starts. The polling authority takes care of the whole process to guarantee the access and and a flawless casting of votes.
- Post-election phase (”Fig. 4”). This phase starts immediately after the voting phase ends. The polling authority decides when election tallying must be executed. Since all votes have been emitted using homomorphic encryption, it is not required to decrypt any of them but it takes advantage of the homomorphic property, which lets the system compute the number of votes that every candidate received. Hence, confidentiality is guaranteed. Once it has been assured the correctness of the results, they are published by the authority.

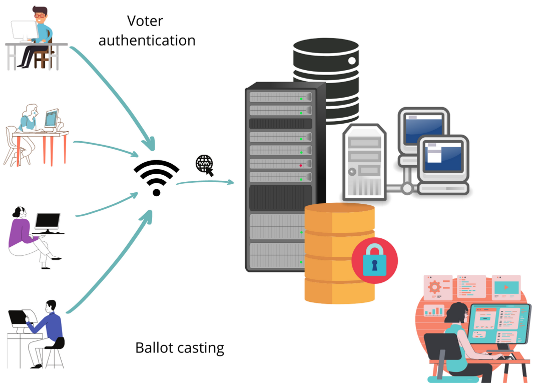

Fig. 3. Online voting phase

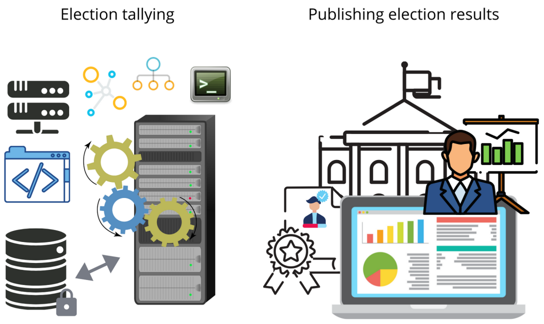

Fig. 4. Online post-election phase

E. *Description of the system*

1) *Pre-election phase:*

- Initialization. It must be decided whether there will be one or more authorities(n_a) in the election, which are in charge of collecting, verifying and counting votes. This step should not be confused. Each democratic country usually has its independent polling authority. However, this responsibility might be centralized or divided among multiple entities (states, zones, regions, Bundeslaender, etc.). This authority creates its pair keys and makes available its public key (PK), which will be used to encrypt the ballot.
- Registration of voters (n_v). Every voter(Vi) is identified using their ID. Then, their private(sk_{V_i}) and public keys(pk_{V_i}) are created and delivered to them. The public key is stored in the Public Key Infrastructure (PKI) and the private key remains under the control and secrecy of its owner.

- Registration of candidates(n_c). Once each candidate(C_i) fulfills all requirements, the polling authority registers these people in the system.

2) Voting phase: During the whole election day,

- Authentication of users. Each voter is authenticated by the system when they log into the application from any device. They need to use their pair-keys and pass phrase (if necessary).
- Ballot casting. Once the user is in the system, they have to choose their desired option/candidate and confirm their preference. Their ballot is encrypted using one of the cryptosystems that exhibits additive homomorphic property using PK of A_i. Users also use their private key sk_{V_i} and pass phrase to sign their ballot using a signature algorithm, e.g. DSA [14].
- Each ballot is represented as a binary number whose values depend on the choice of the voter, given that each bit represents a different candidate.
- Since each voter can vote multiple times, it is required to prevent the system from alerting if the person has re-voted.
- Each encrypted vote is published on the public bulletin board and there are also added some dummies marked as not valid and which are going to be filtered and not counted by the tallying process. The number of inserted dummies depends just on the number of candidates, s.t. after each vote, every one of these candidates has votes.
- Each bullet is received, processed, verified and stored in the infrastructure of the polling authority.

3) Post-election phase:

- Once the valid period to emit votes has ended, the polling authority executes the process for tallying the bullets.
- Dummies and votes, which have been replaced, are filtered.
- Computation is performed on encrypted data to calculate votes without decrypting the information and making this process faster.

F. Risks and challenges

A centralized system allows entities (such as people interested in particular candidates, political parties, foreign governments, etc.) to have a single point for attacks. The paper-based elections can be easily attacked by people who can take advantage of their power in specific areas to affect the ballots, however, to alter the election results is too expensive and requires huge efforts even for those entities. In addition, an online voting system must have a complete infrastructure to support all workload and respond to all requests which imply a huge challenge due to it would be distributed architecture.

1) Attacks models:

- Force abstention. GGermany and the USA are considered two important democracies. According to the official government press of these countries [15] [16], the voter turnout during their elections in 2016 and 2020, which can be seen respectively in table IV), recorded an increase in turnout but remains slow to the participation goal of any democracy. If people do not understand how to use the system, if it represents a challenge for people s.t. they do not use it, if it is proved that it does not fulfill security requirements or if an attack is successfully executed, people will definitely not use it anymore and the system will be a failed project before it can mature or be implemented.

TABLE IV
VOTER TURNOUT IN GERMANY AND USA

Country	Year	Voter turnout
Germany	2017	76.2%
USA	2020	66.8%

- Denial of Service. From population data and the Democracy Index 2018 (published by the Economist Intelligence Unit [17]), it can be observed that any online voting system design requires to ensure its availability for all their voters. Systems have been proposed theoretically, but no one has been implemented successfully given the required resources and computation time. Too many people voting at the same time may represent a bottleneck for processing and verifying votes. Groups of interest might orchestrate attacks against the entry points to undermine the election process.

TABLE V
DEMOCRACY INDEX 2018

Country	Rank	Population
Norway	1	5'300,000
Iceland	2	348,450
Sweden	3	10'120,000
Germany	13	82'800,000
USA	25	327'000,000
India	41	1,353'000,000

- Man in the Middle. This attack model aims to intercept the communication between two entities. Nevertheless, intercepting and/or modifying messages that contain votes do not affect directly the integrity of the elections, since such messages are encrypted, signed and verified, s.t. if any of them has been tampered, the whole message (vote) is rejected. On the other hand, doing this on a large scale would effectively alter the result of the election since one goal might be to cause the rejection of as many votes as possible.
- Man at the End. It has been explained that one of the assumptions of this study depends on the idea that citizens should trust the Polling Authority. Nonetheless, it should not be forgotten that behind the system, infrastructure and procedures, there are human beings who could attack the system using their knowledge. This can be observed mainly in flawed or new democracies. This kind of attack may not be underestimated due to the huge risk and impact on the application, system and result. It could bring the system to an end before it gains people's trust or moreover before it starts.

2) Challenges:

- Time processing and bottleneck. It is required that the proposal achieves, at least, the same benchmark that has been claimed in other works, i.e. that the complexity of the tallying phase is bounded $O(n \log n)$ and avoiding $O(n^2)$. It also needs to consider the total population of the country/democracy on which might be implemented.
- Resistance to change. There is a proverb that claims: "who hits first hits twice" and in order to successfully instrument this new way of voting. It is essential governments and all interested people put effort on introducing the system into their societies making it easy to use and spreading appropriately all information of how it works.
- Training. People have to get used to how the new voting scheme works. The learning curve should be considered for its correct implementation.
- Make it as simple as paper-based. Psychological acceptance is one of the principles of the security, which according to Saltzer and Schroeder [13] states

  > It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly. Also, to the extent that the users mental image of his protection goals matches the mechanisms he must use, mistakes will be minimized. If he must translate his image of his protection needs into a radically different specification language, he will make errors.

- Deletion of temporary credentials. Credentials are valid for a short period of time, then sooner or later they must be changed. This can be seen by citizens as a useless activity.

G. How to improve and achieve its usability

Generation of Cryptographic Keys from Biometrics One improvement to online voting systems could be the replacement of certificates that are valid just for a period of time. They could be replaced by biometrics such that any person could be registered for their entire life and all their information might be under their control. However, there are still some assumptions regarding the feasibility, security, and costs. There are many published works [18]–[20] that involve biometrics and its use for encryption, digital signatures and the development of a Public Key Infrastructure but up to now, there are no real implementation with voting purposes.

Conclusion

There is a pending responsibility for ensuring the exercise of voting rights and the online voting systems are on the eye watching of governments, politicians, and democratic societies given the current circumstances. Hence, it is required to create a technological solution that allows people to vote, hardens democracies' life and protects the rights of candidates and electors.

The security and capability of each nation to elect its rulers are more important than ever. Coercion is considered, one of the biggest problems of the current elections. Either by intimidation or vote-buying, online voting must satisfy not a set of minimal but a complete list of requirements which might be achieved by using homomorphic encryption and certain assumptions which unfortunately at least by now, everyone is forced to accept. Furthermore, taking advantage of cryptosystems that exhibit homomorphic properties enables IT proposals to make operations on encrypted data as they were performed on plaintext. This makes it possible to guarantee secrecy and confidentially of voters' ballots. Nevertheless, there are many risks and drawbacks associated with a voting system that runs over the Internet, specially when interests of a whole nation are to be decided on a specific day. There are not just those who want to be taken into account but also those who want to influence others' decisions.

An online voting system can represent a realistic and doable solution if it does not pretend to change completely the way which most democracies have been working up to now, i.e. not trying to implement a completely new idea such as score voting but implementing improvements that enhance security and gives a response against coercion.

Online voting systems are a cross-cutting problem. Even though, they and the use of homomorphic properties are not a new idea, they have not been implemented in any democracy, not just due to the technological s hurdles, but also all its implications. In consequence, it can not be seen as a real implementation up to now, but it is conceivable for the coming future given the interests of citizens and governments.

Acknowledgment

The author thanks Mr. Fabian Kilger for all his support and feedback throughout the time required for the preparation of this work.

References

[1] Gokhan Karabulut and Klaus F. Zimmermann and Mehmet Huseyin Bilgin and Asli Cansin Doker, "Democracy and COVID-19 outcomes," in Economics Letters, 2021, pp.109840, doi: https://doi.org/10.1016/j.econlet.2021.109840

[2] Mueller, Robert S., "Report on the investigation into russian interference in the 2016 presidential election", March 2019, pp. 36–65

[3] X. Yang, X. Yi, S. Nepal, A. Kelarev and F. Han, "A Secure Verifiable Ranked Choice Online Voting System Based on Homomorphic Encryption," in IEEE Access, vol. 6, pp. 20506-20519, 2018, doi: 10.1109/ACCESS.2018.2817518.

[4] Wouter Lueks, Iñigo Querejeta-Azurmendi and Carmela Troncoso, "VoteAgain: A scalable coercion-resistant voting system," 29th USENIX Security Symposium (USENIX Security 20), 2020, pp. 1553–1570.

[5] C. Kempka, "Matters of Coercion-Resistance in Cryptography Voting Schemes," PhD thesis, 2014

[6] C. Henrich, "Improving and Analysing Bingo Voting,“ PhD thesis, 2012

[7] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469-472, July 1985, doi: 10.1109/TIT.1985.1057074.

[8] Britannica, The Editors of Encyclopaedia. "Homomorphism". Encyclopedia Britannica, 12 Mar. 2008, https://www.britannica.com/science/homomorphism. Accessed 21 June 2021.

[9] Titus, Alexander J. et al. PySEAL: A Python wrapper implementation of the SEAL homomorphic encryption library. ArXiv abs/1803.01891 (2018)

[10] Paillier, Pascal, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes", Advances in Cryptology — EUROCRYPT '99, 1999, pp. 223–238

[11] Lange, Alexander, “An overview of Homomorphic Encryption” https://www.cs.rit.edu/~arl9577/crypto/alange-presentation.pdf. Accessed 15 May 2021

[12] Morris, Liam, “Analysis of Partially and Fully Homomorphic Encryption”, Department of Computer Science, Rocherster Institute of Technology, 10 May. 2013

[13] Saltzer, Jerome H. Schroeder, Michael D. “The Protection of Information in Computer Systems,” 1278-1308. Proceedings of the IEEE 63, 9 (September 1975)

[14] National Institute of Standards and Technology, “A proposed federal information processing standard for digital signature standard (DSS),” Federal Register, vol. 56, no. 169, pp. 42,980-42,982, Aug. 30, 1991

[15] Der Bundeswahlleiter, “Wahlbeteiligung”, https://www.bundeswahlleiter.de/service/glossar/w/wahlbeteiligung.html Accessed May 10th, 2021

[16] Census Bureau, “Record high turnout in 2020 General election”, https://www.census.gov/library/stories/2021/04/record-high-turnout-in-2020-general-election.html Accessed May 10th, 2021.

[17] The Economist, The Economist Intelligence Unit, “Democracy Index 2018: Me too? Political participation, protest and democracy”, 2019, https://pages.eiu.com/rs/753-RIQ-438/images/Democracy_Index_2018.pdf. Accessed 10 May 2021.

[18] Kwon, Taekyoung and Lee, Jae-il, “Practical Digital Signature Generation Using Biometrics”, in Computational Science and Its Applications – ICCSA, 2004, pp. 728–737

[19] Feng Hao, R. Anderson and J. Daugman, “Combining Crypto with Biometrics Effectively,” in IEEE Transactions on Computers, vol. 55, no. 9, pp. 1081-1088, Sept. 2006, doi: 10.1109/TC.2006.138.

[20] J. Jo, J. Seo and H. Lee, “Biometric Digital Signature Key Generation and Cryptography Communication Based on Fingerprint”, in Frontiers in Algorithmics – Springer Berlin Heidelberg, pp. 38–49