Cats and Dogs An Integrity for Voting Systems Based on Paper Ballots

İhsan Haluk Akın

***Abstract*—Voting systems based on paper ballots has a long history with various problems. Vote-selling and correct outcome are two major problems among many. In this work, we propose a new solution to these problems by using UltraViolet (UV) fiber paper Physical Unclonable Function (PUF). When applied this solution not only prevents vote-selling but also ensures the correctness of the outcome. With these two problems eliminated, the voting systems based on paper ballots will have complete integrity.**

***Index Terms*—Paper ballot, Paper PUF, Voting Integrity, Vote-selling**

I. Introduction

VOTING plays a crucial role in the democracy, and it is a necessary part of it. Though there are various needs for voting, representative, presidential, and mayor elections are main voting reasons. They have a big impact on the future of a country. In the digitized age, although many e-voting systems are proposed, implemented, produced, and used [1]–[4], the tides are strongly back to voting system using the paper ballots [5], [6].

In this work, our attention is on the voting systems using paper ballots. The verifiability and correct outcome of the voting process are the two main requirements. In elections with little voters, these two requirements are easy to achieve. The voters can wait to the end of voting process and join/observe the counting process from the opening of the ballot box. When the number of voters are overwhelming, the election system may become quite complex, and may differ according to the country or the region. There are various groups involved in the voting process. When considering the integrity of the voting process, many groups such as; the officers, the tally, the parties (or the candidates), the Voting Management Center (VMC), and even the voters can be malicious.

Considering these malicious parties in the voting process, the integrity of the voting is a crucial problem. The ballot box rooms may be filled with malicious people to change the results. The votes can be easily changed during the counting process. In the case that the VMC collects all of the ballots after the local counting process, the undecided ballots are subject to modification. Another interesting case is the vote-selling, in which a voter agrees with a party to cast his ballot as they required in exchange for money. This action, of course, requires a validation for the vote buying party of the casted vote.

In this work, we concentrate on these two problems, **vote-stealing (integrity)** and **vote-selling** of the voting system based on paper ballots. Our solution is based on the works of Bulens, Standaerty, and Quisquater [7]. They proposed to pour ultra-violet fibers into the paper mixture to create identities for papers. In our solution, we propose a highly controlled ballot distribution, where each party; the VMC, the political parties, and judges, calculates the identity of each ballot and agrees on the identities. Once the agreement is done for the required amount of ballots, the ballots with these identities are assigned and distributed among each ballot box, and these information is made publicly available on the cloud. Under these assumptions, the proposed solution prevents vote-stealing and provides the integrity, with high probability. The cost of successful malicious actions are extremely increased.

This paper consist of 6 sections. In Section II, we talk about the previous works on voting systems based on paper ballots. In Section III , we model a base voting system and discuss the integrity and vote-stealing problems over the model. In Section IV, the model is extended with the UV paper PUF, and honest judges. In Section V, the analysis of the proposed solution is performed. We conclude this work in the Section VI.

II. Previous Works

The problems with the US presidential elections in 2000 increased the awareness towards the problems of the current US voting system. The California Institute of Technology and the Massachusetts Institute of Technology set up a collaborative project to assess the magnitude of the problems of the voting processes, their main causes, and see how technology can scale them down [8]. As of today, 125 works has been listed on their site on various aspect of the voting systems. Jardí-Cedó et al. studied poll-site voting systems under a proposed framework [9]. Among the proposed solutions in the literature 4 of them are notable for us.

1) **Prêt à Voter :** is an end-to-end (e2e) verifiable Vote Verification System (VVS), introduced by Chaum et al. [10], Ryan et al. [11], and Ryan [12]. It uses a detachable ballot. The left side contains randomized list of candidates and the right side contains the selection and the encrypted information for the randomized list of the candidates. The encryption is performed with

İ. H. Akın is with Department of Computer Engineering, Fatih University, Istanbul, Turkey, e-mail: ihakin@fatih.edu.tr. This work is granted by TUBITAK-2219

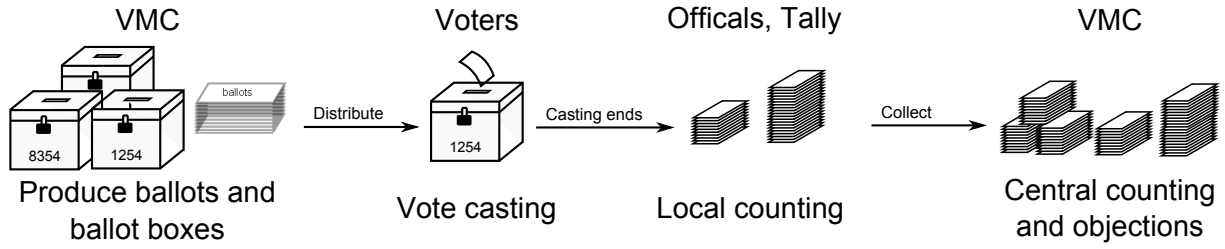

Fig. 1. The Base model for paper based voting process

with shared secret key. The voter marks his selection, detaches the left side, and takes a copy of the right side as a receipt before casting. This receipt may be stamped by the officials to become a proof. The voter can check his receipt at the public bulletin boards. Ryan extended this idea with Paillier encryption [13].

2) **Punchscan :** is also an e2e voting system, introduced by Fisher et al. [14]. Punchscan is designed to offer integrity, privacy, and transparency. Punch Scan's ballots has two pages to form two layers. In the ballots, the orders of the candidates are pseudo-randomly generated. The vote is marked by an ink dauber larger than the holes. The pages, when viewed alone, gives no information. One layer is destroyed and other layer is scanned and kept as receipt, and can be used to check at the public bulletin boards.
3) **Scantegrity-II :** is evolved from Scantegrity by Chaum et al. [15], [16]. It has permuted ballots not to have a connection between the ballot and the receipt. The ballots have unique identification. The verification based on special ink that reveals the verification code. The code, after some minutes, disappears. The ballot id and verification code can be used as an e2e verification.
4) **Scratch and Vote :** is developed by Adiada and Rivest [17]. In Scracth and Vote, an encrypted 2D-barcode stores the orders of the candidates. There is also a scratch surface that can be used to verify the orders of the candidates or that can be left it intact to cast as a vote. The left side of the vote must be destroyed as in Prêt à Voter and Punchscan.

All of the briefly described solutions above are e2e verifiable VVSs. Our proposed solution is not e2e verifiable, the voters cannot verify the ballots easily. The verification of the ballots is performed by the parties.

III. The Model and The Problems

In this section, we model an election system based on paper ballots. In our model, local counting is valid and official; however the model is a centralized model and is very different form the other models.

A. The Base Model

In this work, the punching and stamping types are in consideration. In the punching type ballots are punched via a machine, whereas in the stamping, ballots are stamped with an officially designed stamp. In our model, 6 different main groups, see Figure 1, are participating in the voting system;

- **Voting Management Center (VMC):** The voting process and organization, the printing, the distribution of the ballots, and ballot boxes are managed by the VMC. For each ballot box, the voters are assigned so that each voter can only cast one vote in a pre-determined ballot box. The votes are counted locally at the end of the voting process in the ballot boxes' room where the ballot boxes reside. During the counting, observing is encouraged for the voters. After the counting, the ballot and the local results are collected by the VMC. In this system, the VMC is assumed **malicious**.
- **Political Parties (PP):** PP's (or political individuals) are entering the election to acquire political power. The PP's are also assumed to be **malicious**. PP and their members, by any means possible, try to have advantage over the other PPs. They are allowed to observe any stage of the voting process.
- **Voters :** Voters are casting their vote in favor of the PP they supported. They are also considered as **malicious**. They can try to steal votes or purchase other voters' votes to favor the PP they are supported.
- **Officers :** The officers are assigned to the ballot boxes' rooms by the VMC to organize the casting and the counting stages of the voting process. They are also assumed to be **malicious**.
- **Tally :** Tallies are unofficial private observers of the counting process. They are also assumed to be **malicious**.
- **Judges:** Judges are **honest** party in the voting process. They have the final judgment in any conflict between parties.

B. The Two Problems

Integrity (Cats): In the base model, each party can act maliciously to gain advantage. Besides, a malicious PP, can **purchase** the officials, tally, voters, or the VMC. As a result, the PP can modify the results during the counting, collecting and post-election audit in favor of itself. A good example of such an action can be performed during an bogus electricity shortage [18], [19]

Vote-Selling (Dogs): A malicious party can print ballots and pre-stamp (or pre-punch) them for vote purchasing purposes. The malicious party can purchase a vote from a voter simply

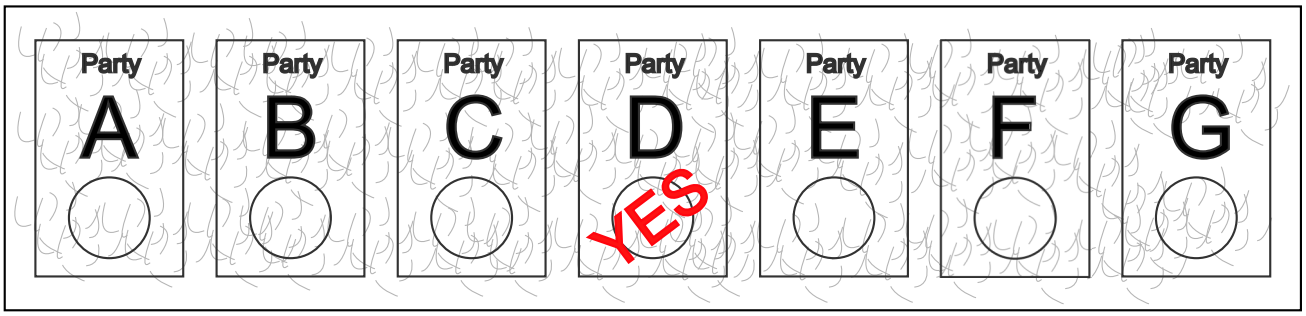

Fig. 2. An imprinted ballot with UV fiber paper PUF. The fibers are made visible for this figure.

by asking the voter to cast the pre-stamped ballot and bring an original ballot back to them. [1]

In next section, we will talk about paper ballots which are designed by the UV fiber paper PUF. We will also talk about the new process. In the section fallowing next section we look at provided integrity for the proposed voting system.

IV. Integrated Model

In this section, we describe the suggested ballot and the voting process based on the UV fiber paper PUF ballot. The integrity of our voting system is based on the UV fiber paper PUF, which is suggested and analyzed by Bulens, Standaert, and Quisquater [7].

RowID	BallotID	BoxID	iSign
721	0x55E30731A7D	7361	0xB78431A
722	0xF57823D0845	9811	0x7561AA1
723	0xAD693CE13D3	2139	0x6DB821E

TABLE I: A ballot identification table

A. The Paper PUF Ballot

In their work, Bulens et al. used fuzzy extractors to build the identifiers of the UV fiber PUF papers. They have extracted 128-bit strings from the UV fiber PUF with a 96-bit entropy that provides 72-bit identifiers with applied ECC. Finding a collusion will require much effort for malicious actions. We will discuss this in our analysis. They also noted that more randomness, robustness, and unclonability can be achieved with the same technology with an additional cost.

In our integrated model, the ballot is formed with the UV fiber PUF technique. We do not consider putting a signature into the ballots like Bulens et al. proposed. See the next section for the details.

[1] A very similar scenario can be applied to receipt based digital ballots.

B. The Voting Process

Our voting system consists of 7 main steps: the ballot formation; the identification of the ballots by the PPs, VMC, and the judges where they must reach a consensus; the distribution of the ballots; the casting of the ballots by the voters; the local counting in the ballot box rooms; the collection of the results and the ballots by the VMC; and the investigation if necessary.

- **The Ballot Formation :** The ballot papers are mixed with the UV fiber during the paper preparation process, see Figure 3. The papers are printed and cut to form the ballots. The order of the candidate PPs in the ballots are randomly arranged.
- **The Ballot Identification and the Consensus:** In the identification step, the VMC, the PPs, and the judges (in short we call all of them as identifiers) have different but open source and public system to identify the ballots. They extract the features, identify the ballots and have a consensus on each paper ballot.
  Once the identifiers have a consensus on a ballot, it is assigned to a ballot box by the VMC. With this assignment, the identifiers insert the ballot's information into a cloud database. Each of the identifiers has a unique table, and public and private keys. They sign their tables

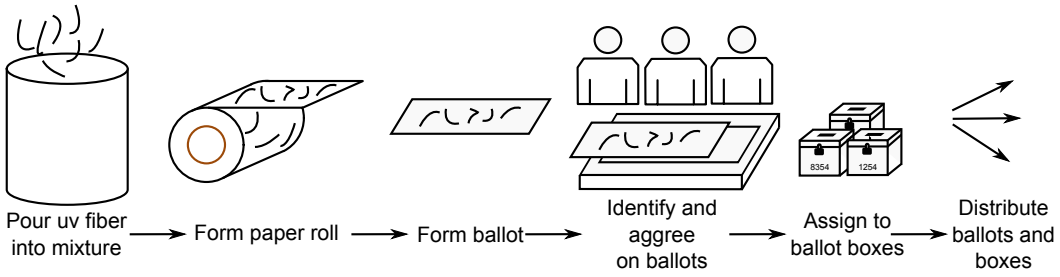

Fig. 3. Ballot preparation and distribution process

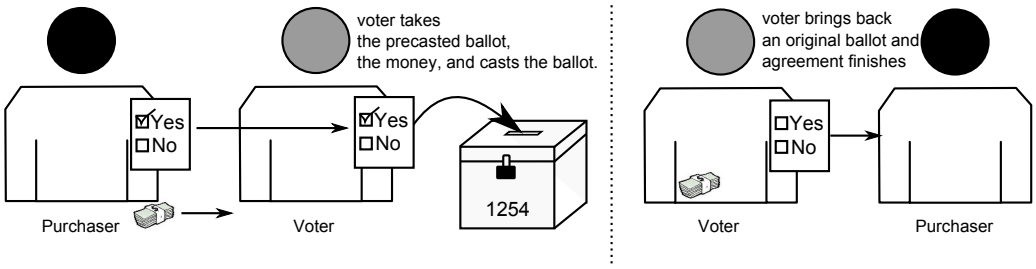

Fig. 4. An example of Dogs action. Left side is before casting and the right site after the vote casted

by their private keys, and integrate the tables, see Table I.

In Table I, the iSign column that stores the incremental signature is a simplified approach of Narasimha et al. [20]. The signature can be calculated as

$$iSign_{row_i} = Sign_{SK}(RowID \parallel BallotID \parallel BoxID \parallel iSign_{i-1}),$$

where $i = 2, ..., n$, $iSign_0 = 0$, and SK is the secret key of the identifiers. The last iSigns are published at the web site with the public keys. The judges keep a copy of the last signatures of each table. The database administrator on the cloud can be malicious, and his malicious actions can be easily detected by the provided signatures.

- **The Ballot distribution :** The distribution of the ballots can be performed by the traditional ways. The only concern is that the ballots must be secured against tampering so that the voting takes place as planned.
- **The Vote casting :** In the casting stage, the voters cast their votes by stamping or punching. In the punching case, the punching area must be outside of the identification region of the ballots. In our system, the voters don't have an e2e verification for their votes; however, they can join the local counting process as observes. At the end of the vote casting, the unused ballots must be stamped with a "not casted" stamp in the presence of the observers.
- **The Local counting :** In the local counting stage, the ballot boxes' seals are opened, and the officers and the tallies count the casted votes in the presence of the observers.
- **The Collection of the Results:** In this stage, the counted results are sent back to the VMC with the ballots. The result of each ballot box is publicly announced.
- **The Investigation** : This stage can be on demand or required. If it is on demand and the voters or the PPs are not satisfied with the counted results of the ballot boxes, they can require investigation. In this process, the ballots in the ballot boxes that are under investigation are re-identified and compared to the old identifications. More discussion on this topic is in the next section.

V. The Integrity of the Voting System

In this section, with some games, we analyze what kind of integrity our voting system is providing. We deeply look at the actions of the cats and the dogs on our system. Also, we discuss the success probabilities of these actions.

Game 1 : The Dogs: Single Vote-Purchasing

- A dog approaches a voter outside the ballot box room before the voter casts his vote.
- The dog offers some money to the voter to cast a pre-stamped ballot and return an original ballot from the ballot box room.
- The voter agrees, takes the money, inserts the pre-stamped ballot into his pocket, goes to the casting room, takes an original one, inserts it into his pocket, and casts the pre-stamped ballot.
- He returns back to the dog, gives the original ballot, and the agreement finishes.
- The output of Game 1 is a success, if this malicious action is not revealed in the investigation step. Otherwise, the output is a failure.

To calculate the successfulness of Game 1, we assume that each ballot have 70-bit identification, i.e. there are 2^{70} different paper ballots that can be created. As noted by Bulens at al. identification space can be increased on demand. We, however, continue our analyze on 70-bit identification. Also, we assume that each ballot box contains exactly 2^{10} assigned voters, and there are 2^{20} ballot boxes. To be successful in Game 1, the malicious party must produce at least 1 ballot with the same identity as the ballots for the targeted ballot box, B_1.

The probability that a ballot produced by the malicious party is in the set of real ballots for B_1 is given by;

$$Pr(Game\ 1 = Success) = \frac{2^{10}}{2^{70}} = \frac{1}{2^{60}} \quad (1)$$

The malicious party must spend a lot of time and money to prepare an original ballot. Even if they are successful in producing a valid ballot for the target B_1, there are two problems. First, the voters cannot identify the ballots. Second, they cannot get any ballot as they wanted. As as result, for a success in Game 1, there is an additional $\frac{1}{2^{10}}$ probability, which makes the probability for Game 1 to be successful $\frac{1}{2^{70}}$.

In the next game, the dogs try to purchase all of the ballots for a specific ballot box, B_2.

Game 2 : The Dogs: Whole Ballot Box Vote-Purchasing

- **Step 1:** A dog approaches a voter outside the ballot box room before a voter casts his vote.
- The dog offers some money to the voter to cast a pre-stamped ballot and return an original ballot from the ballot box room.
- The voter agrees, takes the money, inserts the pre-stamped ballot into his pocket, goes to the casting room, takes an original one, inserts it into his pocket, and casts the pre-stamped ballot.
- He returns back to the dog, gives the original ballot, and the agreement finishes.
- Return to the Step 1, until all the voters' votes are purchased.
- The output of Game 2 is a success, if this malicious action is not revealed in the investigation step. Otherwise, the output is a failure.

The probability of successfully producing 2^{10} ballots that match the ballots for the ballot box B_2 can be given by;

$$Pr(Game\ 2 = Success) = \frac{(2^{10})!}{(2^{70})^{2^{10}}} \approx \frac{1}{2^{62914}}, \qquad (2)$$

as seen from the Equation 2, producing 2^{10} ballots with matching identity is very improbable. Also, note that the votes that are not casted can be a huge problem for the dogs. For simplicity, we assumed that all of the votes are casted. Even a single voter, who has not casted his vote, can create an additional problem for the dogs.

Game 3 : The Cats: Whole Vote-Stealing from a Ballot Box

- Immediately after a ballot box's seal is just opened, a cat performs a magical operation [2].
- During this magical operation, the cat changes the casted ballots with the pre-stamped ballots.
- Output of Game 3 is success, if in the investigation step, this malicious action is not revealed. Otherwise the output is failure.

Assuming that every voter casted their vote, the success probability of Game 3 is equal to Game 2. If there are some voters that have not casted their votes, the success probability success is much less than Game 2.

In the investigation step, even in the case that the malicious action is successful, there is another approach to identify a malicious action; the **fingerprints and DNA** [21], [22]. The ballots, in total, at least must contain 2^{10} different fingerprints. Actually, the fingerprints on the ballots can help to identify the voter's selection! Recently, governments have started to take fingerprints of the citizens and the aliens in their country. Malicious groups within governments can use this database to identify the selection of the voters. Actually, this is a common problem for every paper based voting systems [11], [17], [23].

The next game is a very realistic malicious action on the paper ballots. During the local counting of the ballots, some of the votes are discarded due to bad stamping (or punching). Due to very close results, some parties request re-counting for some ballot boxes at the VMC and, occasionally, the results change after re-counting. By using this knowledge, the cats can play on these **badly** casted votes.

[2]Malicious ballot box room or performing during bogus electricity shortage.

Game 4 : The Cats: Single Vote-Stealing

- A malicious party A request a new counting from the VMC for a ballot box.
- The VMC accepts this request and announce the date of the counting.
- Before the counting date, the cats look at the votes and notice a discarded vote.
- The cat replaces this ballot with a new one.
- Output of the game is success, if in the investigation step, this malicious action is not revealed. Otherwise the output is failure.

The successfulness of Game 4, same as Game 1. The cats, however, may be able to identify the ballot's PUF. With this, they have only $\frac{1}{2^{60}}$ probability to construct a valid ballot. This game can also be played for as many times as there are badly stamped ballots.

In the next game, although it is not realistic, we will look at the probability that a malicious party somehow steals all the casted votes before counting. For simplicity, we assume that all the votes are casted.

Game 4 : The Cats: Whole Vote-Stealing

- Just before the counting process after the ballot boxes are opened, the cats perform magical operations.
- During this magical operation, the cats changes the casted ballots with pre-stamped ballots.
- Output success if in the investigation step, this malicious action is not revealed, else output failure.

The probability of successfully producing 2^{30} ballots can be given by;

$$Pr(Game\ 4 = Success) = \frac{(2^{30})!}{(2^{70})^{2^{30}}} \approx \frac{1}{2^{62914}}, \qquad (3)$$

VI. Conclusion

In this work, we have approached the integrity and vote-selling problems of paper based voting systems by deploying paper PUF constructed with UV fibers. Our proposed solution requires only a group of honest judges The remaining parties can be malicious. The integrity and vote-selling problems can be solved with a high probability. The cost of malicious action within the voting process becomes very improbable for any malicious party. With the increase of the identification space, the proposed solution will provide have better security.

References

[1] Ari Juels, Dario Catalano, and Markus Jakobsson. Coercion-resistant electronic elections. *IACR Cryptology ePrint Archive*, 2002:165, 2002.

[2] Premier/Diebold (Dominion) AccuVote TS and TSx. https://www.verifiedvoting.org/resources/voting-equipment/premier-diebold/accuvote-tsx/, 2014. [Online; accessed 17-July-2014].

[3] Rop Gonggrijp and Willem-Jan Hengeveld. Studying the nedap/groenendaal es3b voting computer: A computer security perspective. In *Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology*, EVT'07, pages 1–1, Berkeley, CA, USA, 2007. USENIX Association.

[4] Ferguson, Louise. *UPA Voting and Usability Project*. UPA, United States, 2004-04-19.

[5] Scott Neumann. Norway Does A Ctrl+Alt+Delete On E-Voting Experiment. http://www.npr.org/blogs/thetwo-way/2014/06/27/326221089/norway-does-a-ctrl-alt-delete-on-e-voting-experiment, 2014. [Online; accessed 17-July-2014].
[6] Michael Alvarez, Jonathan N. Katz, Charles Stewart III, Ronald L. Rivest, Stephen Ansolabehere, and Thad E. Hall. Voting: What Has Changed, What Hasn't, & What Needs Improvement. http://vote.caltech.edu/content/voting-what-has-changed-what-hasnt-what-needs-improvement, 2012. [Online; accessed 17-July-2014].
[7] Philippe Bulens, François-Xavier Standaert, and Jean-Jacques Quisquater. How to strongly link data and its medium: the paper case. *IET Information Security*, 4(3):125–136, 2010.
[8] Voting - What Is, What Could Be. http://vote.caltech.edu/content/voting-what-what-could-be, 2014. [Online; accessed 17-July-2014].
[9] Roger Jardí-Cedó, Jordi Pujol Ahulló, Jordi Castellà-Roca, and Alexandre Viejo. Study on poll-site voting and verification systems. *Computers & Security*, 31(8):989–1010, 2012.
[10] Chaum, Ryan, and Schneider. A practical voter-verifiable election scheme. In *ESORICS: European Symposium on Research in Computer Security*. LNCS, Springer-Verlag, 2005.
[11] Peter Y. A. Ryan, David Bismark, James Heather, Steve Schneider, and Zhe Xia. Prêt à voter: a voter-verifiable voting system. *IEEE Transactions on Information Forensics and Security*, 4(4):662–673, 2009.
[12] Peter Y. A. Ryan. A variant of the chaum voter-verifiable scheme. pages 81–88. ACM, 2005.
[13] Peter Y. A. Ryan. Prêt à voter with paillier encryption. *Mathematical and Computer Modelling*, 48(9-10):1646–1662, 2008.
[14] Sherman AT Fisher K, Carback R. Punchscan: Introduction and system definition of a high-integrity election system. In *Proceedings of the Workshop on Trustworthy Elections 2006*, pages 1–8. Springer, 2006.
[15] David Chaum, Richard Carback, Jeremy Clark, Aleksander Essex, Stefan Popoveniuc, Ronald L. Rivest, Peter Y. A. Ryan, Emily Shen, and Alan T. Sherman. Scantegrity II: End-to-end verifiability for optical scan election systems using invisible ink confirmation codes. In David L. Dill and Tadayoshi Kohno, editors, *2008 USENIX/ACCURATE Electronic Voting Workshop, July 28-29, 2008, San Jose, CA, USA, Proceedings*. USENIX Association, 2008.
[16] Stefan Popoveniuc, Jeremy Clark, Richard Carback, Aleksander Essex, and David Chaum. Securing optical-scan voting. In David Chaum, Markus Jakobsson, Ronald L. Rivest, Peter Y. A. Ryan, Josh Benaloh, Miroslaw Kutylowski, and Ben Adida, editors, *Towards Trustworthy Elections*, volume 6000 of *Lecture Notes in Computer Science*, pages 357–369. Springer, 2010.
[17] Ben Adida and Ronald L. Rivest. Scratch & vote: self-contained paper-based cryptographic voting. In *WPES*, pages 29–40. ACM, 2006.
[18] Hileli Yerel Seçim 2014 Belgeleri ve Fotoğrafları. http://hilelisecim2014.tumblr.com/, 2014. [Online; accessed 17-July-2014].
[19] CHP ve MHP'den Seçimde Hile Yapıldı İddiası. http://www.bianet.org/bianet/siyaset/113469-chp-ve-mhp-den-secimde-hile-yapildi-iddiasi, 2014. [Online; accessed 17-July-2014].
[20] Maithili Narasimha and Gene Tsudik. DSAC: An approach to ensure integrity of outsourced databases using signature aggregation and chaining. *IACR Cryptology ePrint Archive*, 2005:297, 2005.
[21] Paul-Jean Coulier. Les vapeurs diode employes comme moyen de reconnaitre laltration des critures (iodine vapors used as a means of recognizing the alteration of writing. *LAnne scientifique et industrielle*, 8:157–160, 1863.
[22] M.Kinga Balogh, Joachim Burger, Klaus Bender, eter M Schneider, and Kurt W Alta. Str genotyping and mtdna sequencing of latent fingerprint on paper. *Forensic Science International*, 137(2-3):188–195, 2003.
[23] David Chaum, Aleks Essex, Richard Carback, Jeremy Clark, Stefan Popoveniuc, Alan Sherman, and Poorvi Vora. Scantegrity: End-to-end voter-verifiable optical-scan voting. *IEEE Security & Privacy*, 6(3):40–46, May/June 2008.

İhsan Haluk Akın finished his bachelor studies at the department of mathematics, METU in Ankara, Turkey in 1999. He finished Masters degree at Sabanci University, Turkey in 2002. He finished his Ph.D. at METU in 2009 on Spectral Modular Multiplication. He worked at several places including TUBITAK BILGEM between 2000 and 2010. He worked at Fatih University between 2010 and 2013. He finished his postdoc at Worcester Polytechnic Institute and continues his research at Fatih University. His current research areas are: database security on the cloud, side channel attacks.