Integrating paper-based voting and Belenios
a hybrid voting protocol for an academic organization

Fernando Marques, Ana Almeida Matos, and Jan Cederquist

Instituto Superior Técnico
{fernando.m.marques,ana.matos,jan.cederquist}@tecnico.ulisboa.pt

Abstract. We consider the problem of introducing an electronic voting system in the context of an academic organization. We work under the assumption that such a context fits a profile where integrity of an election is expected to be fully verifiable, privacy must be ensured by the system, and coercion is not of primary concern. Additionally, we assume that a classic paper-voting is already in place, and while the voting community may be expected to be literate in handling web-based applications and in understanding the concept of verifiability, it may exhibit some cultural resistance against shifting to a new voting practice.

We present an integration of a classical paper ballot system with the Belenios e-voting protocol, an on-line voting system which guarantees vote privacy and verifiability. To this end, we propose a specification of a hybrid version of the Belenios protocol which integrates the classical paper ballots. We then present and prove, up to assumptions of security of the two baseline protocols, the relevant security properties of the resulting protocol. Finally, we show that the proposed protocol is well suited to be adopted by an academic organization by presenting an architecture for the proposed solution that fits the current requirements of an existing university.

1 Introduction

Voting has been an important step in decision making for millenia. It has been used in different contexts, ranging from statewide elections and referendums, to those organized at the level of smaller societies [1–3]. Until recently, paper ballot systems have provided the classical medium for expressing votes, but the use of electronic voting (e-voting) has been gaining popularity over the last decades and is even currently being implemented in some countries for government elections.

E-voting allows for a more secure and auditable elections. The results are also published faster than the classical system and is more accessible to the voter. This allows for cost minimization in elections. There is, however, a technical trade-off between managing simultaneously integrity and privacy. Furthermore, there may exist trust issues among the voting population regarding the system where the election is being run, while people with less technical proficiency may find it hard to cast their vote due to not understanding how to work with the system. Indeed, the replacement of a classic paper voting system for an electronic one requires a cultural shift which is not easy.

A wide variety of electronic voting protocols have been proposed with the aim of improving the orchestration of the voting process. Each voting protocol may provide a set of guarantees under certain assumptions, and its suitability for a given election depends on how well the specific context of the election grants those assumptions and what requirements are considered of importance.

Problem. In this paper, we consider the problem of introducing an electronic voting system in the context of an academic organization. We work under the assumption that such a context fits a profile where integrity of an election is expected to be fully verifiable, where privacy must be ensured by the system, but where coercion is not a primary concern. Additionally, we assume that a classic paper-voting system is already in place, and while the voting community may be expected to be literate in handling web-based applications and in understanding the concept of verifiability, it may exhibit some cultural resistance against shifting to a new voting practice.

At an implementation level, we assume that an organization-wide authentication system is already in place, possibly associated to an integrated campus management system. Also, as available computing resources are often restricted, we focus on architectures that require a limited number of servers.

As a running example, we consider the concrete case of Instituto Superior Técnico (IST) of the University of Lisbon, where elections are run using a classical paper voting system. In this environment we have access to an authentication platform provided by IST informatics campus management system Fenix, and are limited to two servers. We expect that the results are applicable to similar organizations.

The main requirements for our voting system are thus:

- To depart as little as possible from the functionality and assurances of the paper ballot system which is already in place.
- To offer the functionality of electronic voting, associated to the desired properties of privacy and full integrity verifiability.
- To make use of the already existing authentication mechanisms for ease of usability.
- To be securely implementable using a low number of servers.

Solution. As already mentioned, beyond any technical arguments towards adopting an e-voting system, the replacement of a classic paper voting system for an electronic one requires a cultural shift. In order to mitigate the impact of this shift, the transition can be made by simultaneously enabling both electronic and paper-based voting methods.

We present an integration of a classical paper ballot system with the Belenios e-voting protocol, an on-line voting system which guarantees vote privacy and verifiability. To this end, we propose a specification of a hybrid version of the Belenios protocol which integrates the classical paper ballots. We then present and prove, up to assumptions of security of the two baseline protocols, the relevant security properties of the resulting protocol.

Belenios [4, 5] was chosen as a base protocol due providing a homomorphic encryption scheme [6] with addictive properties, a credential scheme which allowed to identify a vote to a voter while maintaining a simple specification, and since the protocol also didn't require a large number of servers.

The main security properties and assumptions that hold for our system are:

Integrity Ballots are counted correctly, independently of whether they were cast in paper and/or electronically. This implies in particular consistency between the e-voting and paper voting. Holds under assumptions of correct (human) handling and tallying of the paper votes, and of non-corruptability of both the credential authority and the voting server simultaneously.

Confidentiality The association between the object of a vote and the voter is known only by the voter, up to aggregation of results. Holds under the assumption that the cryptographic scheme used to encrypt the ballots is not broken and that the trustees of the protocol don't work together with malicious intent.

Auditability The voter can verify that her electronic vote is registered correctly. Any user can verify that the counting of the registered electronically cast votes is done correctly. Counting of votes cast by paper can be verified within the defined time frame before they are destroyed. Holds by design of the protocol, under the assumption that it is correctly implemented.

Contributions. The main technical contributions are the following:

- A new hybrid voting system that integrates a modified version of the Belenios e-voting protocol (in which voting credentials are generated on demand) and a classical paper voting protocol.
- Accurate enunciation of the preservation of properties of the baseline protocols and their proofs.
- Proof of concept of applicability to an academic setting, by the design of an architecture for implementing the proposed solution that fits the implementation requirements of an existing organization.

Overview. We start by presenting, in Section 2, the two baseline protocols that are integrated into the proposed hybrid protocol, which we describe in detail. For each we present the assumptions and main security properties. In Section 3 we enunciate and prove the relevant security properties that hold for the hybrid protocol. In Section 4, we present the architecture of the system. Finally, in the last two sections we present the related work, and conclude.

2 Protocols

In this section we present a new hybrid e-voting system which we refer to as *H-Belenios*. We start by summarizing the two baseline protocols that will be integrated into our hybrid protocol and their main security properties: *Baseline*

Protocol A (BP-A), refers to the paper protocol, and *Baseline Protocol B (BP-B)* refers to the e-voting protocol. We then describe and formally specify the H-Belenios protocol.

In all three protocols, we distinguish the following four main phases: The *Set up phase* includes the steps that are necessary to specify the election parties, and to generate and input the necessary configurations for the election to occur; the *Voting phase*, includes the processes by which voters may cast their votes; the *Tally phase*, when all the votes are added and the final result of the election is published; and the *Audit phase*, which may overlap with the voting phase, when (partial) verification of correctness of (partial) results can be performed.

We refer to an *eligible voter* is a user who is authorized to vote in a specific election. Furthermore, the *final vote of an eligible voter* is either the paper vote (if the voter has cast a paper vote), the vote cast electronically (if the voter did not cast a paper vote), or undefined (if the voter did not vote).

2.1 Baseline Protocol A: Paper voting

The following protocol, which we refer to as Baseline Protocol A (BP-A), is based on the regulations for the establishment of organs within IST [7].

The main parties involved in BP-A are the electoral commission, the members present at each table which are the poll workers, and each eligible voter.

Set up phase. Before the election begins, the members of the electoral commission, including the president, are designated. These members cannot be candidates for the election and include, in particular, one member per election candidate which serves as a representative.
On the day of the election, one or more voting tables are available for depositing votes. Each voting table has a group of pool workers (which may include one representative per candidate) designated to it.

Voting phase. In order to vote, the voter first shows his identity to the voting table president, who also verifies his voting right. The voting secretary notes on the electoral roll that this voter has voted and the president hands out a paper ballot. The voter goes to a voting booth, and fills in the ballot secretly by placing an ‘X’ next to the candidate of choice. Any other type of mark on the ballot invalidates it. Finally, the voter hands in the folded ballot to a person present at the voting table who inserts it into the ballot box.

Tally phase. At the end of the election the pool workers at each table proceed to count the votes and their distribution. The minutes are then written, recording the information gathered from the votes. The partial results are then handed to the electoral commission who will add all the votes from different tables and calculate the tally. The results must be released 24 hours after the end of the voting phase, and the paper votes must be destroyed 30 days after the election has passed.

Audit phase. After the tally phase complaints can be made to the electoral commission with a time limit of one day after the results are published. Every pool worker also has the option of complaining in the table report against decisions made by that table.

Assumptions.

- Nobody, including the pool workers, interferes with the paper votes in the ballot boxes.
- The pool workers perform the tally and publication of the results according to regulations.

Security properties.

- Only and all eligible voters are able to vote.
- Each vote is kept confidential (regarding both existence of vote and vote content), up to aggregation of results.
- The regulations specify a correct procedure for counting exactly one vote per voter.
- It is possible to retally the votes, within a specified time frame.

2.2 Baseline Protocol B: Belenios

The following protocol, which we refer to as Baseline Protocol B (BP-B), summarizes the core of the Belenios electronic election protocol (see [5] for the full formal specification) on which we base the elctronic part of our voting system. Other features, such as the possibility of credential recovery, are omitted.

The main parties involved in BP-B are the voting server, the server administrator, the credential authority, the each eligible voter and each trustee.

Set up phase. An election in Belenios starts with the creation of the credentials. The server administrator sends a unique universal identifier (uuid) to the credential authority. There, a list of credentials and their public parts is created. Each credential is sent to the respective voter, and the list of shuffled public parts for the credentials is generated and sent to the server administrator.

Then, each trustee generates her own public key and sends it to the server administrator, who verifies that the trustee has the secret part of it, and in the end combines all of the trustees keys in order to generate the election public key. With both the list of public credentials and the election public key, the server administrator is able to create the election. The protocol uses a public key encryption scheme with additive homomorphic properties.

Voting phase. In order to vote, the voter obtains the election parameters, creates a ballot which is formed from the encrypted votes and proofs (proofs of membership and proofs that the vote are formed correctly), the signature, the election uuid and hash. If all the data present in the ballot is valid then the voting server publishes it.

Tally phase. The election is terminated by the server administrator. The homomorphic properties of the encryption scheme are used to aggregate all the votes into an encrypted tally which is sent to each trustee to perform a partial decryption. Finally, the server administrator verifies the partial decryptions and aggregates them in order to create the decrypted tally, which is then published.

Audit phase. During the voting phase and tally phase, each voter is able to verify that their vote was cast correctly using the smart ballot tracker (hash of the serialization of the ballot) which was published on the bulletin board when the ballot was cast. It is also possible to verify that the encrypted tally was calculated correctly. The greater the number of voters performing this verification, then stronger is the confidence in the outcome of the election.

Assumptions.

- Not both the voting server and the credential authority are simultaneously corrupt.
- The client software does not leak information about the electronic votes.
- The trustees will not work together in a malicious way.

Security properties.

- Only and all eligible voters are able to vote.
- Each vote is kept confidential (regarding vote content), up to aggregation of results.
- The protocol specifies a correct procedure for counting exactly one vote per voter.
- Each voter is able to verify that their vote was cast correctly.
- Each voter is able to verify that the tally is correct.

2.3 Hybrid Protocol: H-Belenios

The parties that participate in the hybrid protocol include those of BP-B – the voting server (**VS**), the credential authority (**CA**), the server administrator (**SA**), each eligible voter (**V**) and each trustee (**T**) –, as well as that which is present in the paper part of the protocol – the poll worker (**PW**).

In order to formally describe the integration of the two baseline protocols, we make explicit the different structures where data is saved: The **EL**, which is a list of all the elections, including their parameters (dates, descriptions, names) and their uuid; the eligible voter list **EVL**, which maps each voter identifier to their respective public credential; the list **TL** of trustees; the table of electronic votes **TEV** which contain all the e-votes done by eligible voters; the list of identifiers paper voters **LPV**, that is the representation of the paper voters on the system and the table of final electronic votes **TFEV**. We also have **pLPV** which is the same as **LPV** but only in paper format, as is currently used in BP-A. From these structures, during the voting phase the smart ballot tracker of each ballot in **TEV** will be published and after the tally the smart ballot tracker of each ballot in **TFEV** will be made available together with the voter identifiers of those who voted by paper. The data structure which are made public will be available to view in the smart bulletin board **SBB**.

In the following description of H-Belenios, in order to avoid redundancy, we focus on the differences with respect to the baseline protocols. For each phase of the election, a table presents the corresponding formal description. We also assume secure channels are being used for message exchange.

We omit details regarding common message exchange security. We assume secure channels.

Set up phase. As in BP-B, to create the electronic counterpart of an election, we require the basic parameters of the election (name, dates and other information, denoted by eParam), the list of eligible voters with their voter identifiers **EVL** and the list of trustees **TL**, the election public key Pk_e which is made from the trustee's ($t \in \mathbf{TL}$) public key shares and proofs that they each have the secret key share δ_t, and the election identifier which is an uuid e_{id} (which is sent in all message exchanges throughout the protocol). The cryptographic keys that are needed for electronic voting are also generated similarly to as in BP-B. However, in H-Belenios, they are generated on demand for voters who wish to vote electronically.

#	Message Exchange	Voting Server & Administrator
1	$\mathbf{SA} \to \mathbf{VS}$: eParam	
2		$\mathbf{EL} := \mathbf{EL} \cup \{\langle e_{id}, \text{eParam}\rangle\}$
3		publish($\langle e_{id}, \text{eParam}\rangle$)
4	$\mathbf{SA} \to \mathbf{VS} : \mathbf{TL}$	
5	$t \to \mathbf{VS} : Pk_t, \delta_t,\ \forall t \in \mathbf{TL}$	
6		publish(Pk_t), $\forall t \in \mathbf{TL}$
7	$\mathbf{VS} \to \mathbf{SA} : Pk_t, \delta_t,\ \forall t \in \mathbf{TL}$	
8		validate(δ_t), $\forall t \in \mathbf{TL}$
9	$\mathbf{SA} \to \mathbf{VS} : Pk_e = \sum_{t \in \mathbf{TL}} Pk_t$	
10		publish(Pk_e)
11	$\mathbf{SA} \to \mathbf{VS} : \mathbf{EVL}$	

Voting phase. The voting procedure can be initiated by any voter $v \in \mathbf{EVL}$ during this phase. In order to vote electronically, voter v must first request the credentials. This will not prevent v from also voting by paper (which would take precedence over the electronic vote). The voter will then receive by email from **CA** the public and secret credentials, respectively denoted by Pc and Sc, that are necessary to vote. The connection between the Pc and the voter's Id is maintained in **EVL** in order to allow revocation of electronic votes due to paper vote being cast. In the following, p and q denote the large prime numbers, and g the generator for the cyclic group of order p, which are used for the encryption and signature schemes that allow to confidentially send electronic ballots (eBallot) carrying the encrypted answers (ans) to the question of the election.

#	Message Exchange	Voting Server
1	$v \to \mathbf{VS} : Id_v$, request	
2	$\mathbf{VS} \to \mathbf{CA} : Id_v, p, q, g$	
3	$\mathbf{CA} \to \mathbf{VS} : Pc_v, Id_v$	
4		$\mathbf{EVL} := \mathbf{EVL}[Id_v \mapsto Pc_v]$
5	$\mathbf{CA} \to v : Pc_v, Sc_v$	
6	$\mathbf{VS} \to v$: eParam, p, q, g, Pk_e	
7	$v \to \mathbf{VS}$: eBallot $= ans, s\{ans\}_{Sc_v}, \delta_{ans}, Pc_v$	
8		validate($Pc_v \notin \mathbf{TEV}$)
9		$\mathbf{TEV} := \mathbf{TEV} \cup \{\langle Pc_v, \text{eBallot}\rangle\}$
10		publish(**TEV**)

For the sake of consistency with BP-B, we allow a single electronic vote per voter. However, there is no technical obstacle to generalise this phase in order to allow any number of electronic votes, whilst only the latest one would be considered (without affecting the precedence of a paper vote over it).

The steps for voting by paper are the same as in BP-A. The only difference is that at the end of this phase, the list of paper voters of the voting tables **pLPV** must be delivered to **SA** who must form **LPV** and input it to **VS**. We denote by **BB** the set of paper votes cast in the ballot box, and each paper ballot is denoted as pBallot.

#	Message Exchange	Server & Administrator	Voting Table
1	$v \rightarrow \mathbf{PW} : Id_v$		
2			$\text{validate}(Id_v \in \text{dom}(\mathbf{EVL}) \setminus \mathbf{pLPV})$
3	$v \rightarrow \mathbf{PW} : \text{pBallot}$		
4		$\mathbf{pLPV} \coloneqq \mathbf{pLPV} \cup \{Id_v\}$	
5			$\mathbf{BB} \coloneqq \mathbf{BB} \cup \{\text{pBallot}_{id}\}$
6	$\mathbf{PW} \rightarrow \mathbf{SA} : \mathbf{pLPV}$		
7		$\mathbf{LPV} \coloneqq \mathbf{pLPV}$	
8	$\mathbf{SA} \rightarrow \mathbf{VS} : \mathbf{LPV}$		

Tally phase. At this phase the **VS** aggregates all the final electronic votes using the homomorphic properties of the encryption scheme. The electronic votes from the voters who also voted by paper are omitted in **TFEV**. These votes are identified by using the connection between their voter *Id* and the *Pc* which is present in the electronic ballot. This partial encrypted tally (denoted bellow by eRes) is sent to each trustee ($t \in \mathbf{TL}$) who computes a partial decryption ($D_t\{\text{eRes}\}$) and a proof of correct decryption. The **SA** in the end verifies all decryptions, and aggregates them ($D\{\text{eRes}\}$). At this time the **SA** must input the paper results to the server. After the tally and the verifications are done, then the results can be posted on the bulletin board.

#	Message Exchange	Server & Administrator	Voting Table
1		$\mathbf{TFEV} \coloneqq \mathbf{TEV}\vert_{\overline{\mathbf{EVL(LPV)}}}$	
2		$\text{eRes} \coloneqq \text{tally}(\mathbf{TFEV})$	
3			$\text{pRes} \coloneqq \text{tally}(\mathbf{BB})$
4	$\mathbf{VS} \rightarrow t : \text{eRes}, \forall t \in \mathbf{TL}$		
5	$x \rightarrow \mathbf{VS} : D_t\{\text{eRes}\}, \delta_{D_t}, \forall t \in \mathbf{TL}$		
6	$\mathbf{VS} \rightarrow \mathbf{SA} : D_t\{\text{eRes}\}, \delta_{D_t}, \forall t \in \mathbf{TL}$		
7		$\text{validate}(\delta_{D_t}), \forall t \in \mathbf{TL}$	
8	$\mathbf{SA} \rightarrow \mathbf{VS} : D\{\text{eRes}\}$		
9	$\mathbf{SA} \rightarrow \mathbf{VS} : \text{pRes}$		
10		$\text{fRes} \coloneqq D\{\text{eRes}\} + \text{pRes}$	
11		$\text{publish}(\mathbf{TFEV}, \mathbf{LPV})$	
12		$\text{publish}(\text{fRes})$	

Audit phase. The auditing of the paper and the electronic part of the voting process will occur in a similar fashion as for BP-A and BP-B, respectively. The main difference is that at the end of the election, only the smart ballot trackers of the final electronic votes are published. For those voters who voted by paper, their identifier will appear saying that they voted as such. Furthermore, we add a checksum that validates de total number of votes against those that appear in the smart ballot tracker and the votes done by paper (given by $|\text{finalResult}| == |\mathbf{TFEV}| + |\mathbf{LPV}|$). This enables to detect any mismatch between the number of counted paper votes and those that appear in the smart ballot tracker.

Assumptions and Security properties. See following Section 3.

Remove if vertical space is needed

3 Security

We now present and prove the relevant security properties for H-Belenios.

Assumptions. The union of those enunciated for the baseline protocols A and B.

Property 1. Only and all eligible voters are able to vote.

Proof.

- All eligible voters can vote. If an eligible voter wants to vote by paper he can do so as in BP-A. If a voter wishes to vote electronically he can do so, as in BP-B, from any web browser so long as he registers to vote electronically and authenticates himself in the process.
- Only eligible voters can vote. As in BP-A, a voter has to prove his identity in order to vote by paper. If a voter wants to vote electronically, he must register as such using a web browser, as in BP-B. To do so he must authenticate himself using his authentication credentials and to cast a vote he must be authenticated and have both credentials that are sent to him when he registers himself to vote.

Property 2 (Confidentiality). Each vote is kept confidential (regarding vote content), up to aggregation of results.

Proof. Confidentiality (regarding vote content) of votes up to publication of the results is guaranteed for paper votes in the same manner as for BP-A, and for electronic votes as for BP-B. The publication of **LPV**, as well as the construction of **TFEV** does not reveal vote content.

Property 3 (Integrity). The protocol specifies a correct procedure for counting exactly one vote per voter.

Proof. For space reasons, we only present the intermediate results and omit the remaining details.

1. The protocol specifies a correct procedure for building a list of paper voters **LPV** and a table of final electronic votes **TFEV**.
2. The protocol specifies a correct procedure for tallying tables **LPV**, **TEV** and **TFEV**.

3. All and only final votes are counted.
4. An eligible voter will have exactly one counted vote if and only if he has issued at least one vote.

Property 4 (Auditability). It is possible to retally the paper votes, within a specified time frame. Furthermore, assuming that the tally of the paper votes is correct, every voter is able to verify that the final tally is correct.

Proof. The partial tallies (paper and electronic votes) can be verified as in BP-A and B. The combination of both enables to verify the final tally.

Make more explicit results about what can be concluded from reading the bulleting board

Coercion resistance. While BP-A is considered to be strongly coercion resistant, BP-B suffers from the fact that vote receipts can be produced. Although this is assumed to not be of primary concern in the context of this work, we observe that as a result of the integration of the protocol with a paper-based voting system, the new protocol improves on the level of coercion resistance that is provided by BP-B. Indeed, the voter now has a choice of also casting a paper ballot, which is preferred over the electronic ballot during the tally. As such there is no way to prove who he voted for, up to aggregation of the results.

Relaxing assumptions. The integrity properties of BP-A rely on strong assumptions of correctness of the actions of the poll workers. How ever, these assumptions can be relaxed in face of the new possibility of detecting a mismatch between the counted number of paper votes and the electronic votes published in the smart bulletin board. More precisely, it is no longer necessary to assume that fake ballots or votes cannot be added to or removed from the ballot boxes or tally, but only that they are not changed.

4 Architecture

As described in Figure 1, the system will have two servers running, the voting server which will work as a bulletin board and ballot box and the credential authority which will be responsible for the generation and distribution of the elections. The connections between every component and entity will be done using TLS connections in order to avoid man in the middle attacks. The entities will connect to the voting server using a web browser, that will run a web application, and they will need to authenticate themselves using Fenix platform authentication credentials, which is possible due to the use of Oauth2.

5 Related Work

Internet voting protocols. In this paper we base the electronic part of our hybrid e-voting protocol on Belenios. Belenios is a purely e-voting protocol which is in turn based on Helios [8] and Helios-C [9].

Helios was created by Ben Adida in order to allow voters to audit their ballots before casting them. Over the years, various versions of Helios have been released,

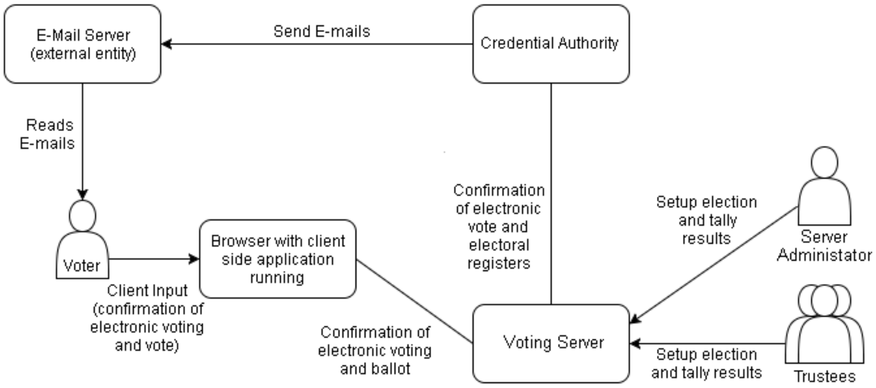
E-Mail Server (external entity)
Send E-mails
Credential Authority
Reads E-mails
Confirmation of electronic vote and electoral registers
Setup election and tally results
Voter
Browser with client side application running
Server Administator
Client Input (confirmation of electronic voting and vote)
Confirmation of electronic voting and ballot
Voting Server
Setup election and tally results
Trustees

Fig. 1: Architecture of the protocol

improving the security of the protocol. One of the changes that occurred during this versions was the substitution of mix-networks [10] for the anonymization of the ballots for the use of homomorphic encryption using El Gamal encryption scheme [11]. One of the main differences between Helios protocol and Belenios is that the later uses a credential system in order to avoid ballot stuffing.

Helios-C is an improvement over the Helios system proposed by Veronique Cortier et al., which adds the idea of using credentials to Helios. This protocol uses an El Gamal encryption scheme with homomorphic properties for anonymization and a Schnorr signature scheme [12] for ballot authenticity. Belenios is very similar to this protocol, being the main difference between the two that the former does not have threshold support for the key generation.

Hybrid voting protocols. TrustVote [13] is a hybrid e-voting system which includes a paper-based and an electronic-based voting components, designed to be used by governments and organizations. The e-voting component is based on FOO92 [14], being one of the main improvements the introduction of threshold blind signatures. This system also allows the possibility of revoking a previous electronic vote. In order to integrate the paper voting with their e-voting system, paper voting is allowed during a new period that starts after the electronic vote casting ended. If the voter had cast an electronic vote, then during the paper voting he may chose to revoke it. In order to revoke an electronic vote, the vote must present his voter secret which is used in order to identify his e-vote. The tally is then computed with the sum of all electronic votes minus the sum of all revoked electronic votes and finally adding the sum of all paper votes. Unlike our system, paper voting and e-voting phases are thus kept separate in TrustVote. It is also necessary to submit additional documents in the act of paper voting.

Another implementation of a hybrid e-voting system was proposed by Oliver Spycher and Rolf Haenni [15]. This system makes use of pseudonyms created from the credentials given to the voters. These pseudonyms are shuffled with the public credentials. The voter can then cast an electronic ballot with the pseudonym created from the credentials, the encrypted vote and zero knowledge proof, which are published on the public bulletin board. If a voter chooses to vote by paper he must present at the polling station his public credential, his pseudonym and a zero knowledge proof that verifies that he gave the right pseudonym. If there is a vote associated with the pseudonym, then that vote must be revoked and the voter may then vote by paper; otherwise the voter can vote by paper since he has proven with the credentials, pseudonym and zero knowledge proof that he is an eligible voter. Similarly to TrustVote, this protocol also needs the submission of the voter's public credential.

Voting in academic organizations. Many academic organizations still rely exclusively on a classical paper voting but there are some who have started to adopt electronic voting systems. Some examples of such universities are Princeton who currently have a Helios server running for elections [16], Université Catholique de Louvain (UCL) in Louvain-la-Neuve, Belgium, which also uses a version of Helios [17] and MIT who used EVOX for its Undergraduate Association elections [18].

6 Conclusions and Future Work

This paper presents a hybrid voting protocol that integrates a well-studied e-voting protocol with a standard paper-based protocol. By minimizing the changes to the later, we aim to mitigate the cultural shift that is required in a transition towards a full e-voting system.

We consider the concrete case of an existing academic organization (IST) as a proof-of-concept that the proposed solution satisfies the enunciated requirements. Furthermore, the solution is currently being developed for coupling with IST's integrated campus management system (Fenix). We expect that other academic organizations have similar requirements and computing contexts (eg., an internal authentication system), and that therefore our proposed protocol is useful beyond the specific case of IST.

As future work, we envision to extend the protocol with full receipt freeness, as proposed and previously discussed for BeleniosRF. Another possible improvement would be to adapt the protocol in order to distribute the credentials in more secure ways, as for instance by means of smart cards. There is also the possibility of having a centralized list of voters so that each voter can vote by paper in any of the tables which are available.

Besides offering an intermediate step towards the change from a exclusive paper voting community to one that embraces with a bit more ease the idea of e-voting, new advantages entail from preserving the possibility of paper voting: On one hand, partial coercion freeness is added to the electronic component of the protocol, simply entailed from the possibility of overriding any electronic vote by means of a paper vote. On another hand, prevention of ballot stuffing elimination in the paper-based protocol, which relied solely on assumptions of trust on the pool workers, can be detected thanks to the publication of a mapping from voters to voting means.

References

1. Heiberg, S., Willemson, J.: Verifiable internet voting in estonia. In: Electronic Voting: Verifying the Vote (EVOTE), 2014 6th International Conference on, IEEE (2014) 1–8
2. CDL, U., CAPC, U.: Scantegrity ii municipal election at takoma park: the first e2e binding governmental election with ballot privacy. (2010)
3. Gerlach, J., Gasser, U.: Three case studies from switzerland: E-voting. Berkman Center Research Publication No **3** (2009) 2009
4. Glondu, Stéphane, and Cortier, Véronique and Gaudry, Pierrick: Belenios – Verifiable online voting system. http://belenios.gforge.inria.fr/ Accessed: 2017-07-02.
5. Glondu, S.: Belenios specification. (2013) 1–8
6. Rivest, R.L., Adleman, L., Dertouzos, M.L.: On data banks and privacy homomorphisms. Foundations of secure computation **4**(11) (1978) 169–180
7. Instituto Superior Técnico: Regulamento para eleição dos órgãos do ist – normas gerais. Diário da República, 2.ª série — N.º 143 — 25 de julho de 2012 (2012) 26500–26505
8. Adida, B.: Helios: Web-based open-audit voting. In: USENIX security symposium. Volume 17. (2008) 335–348
9. Cortier, V., Galindo, D., Glondu, S., Izabachene, M.: Election verifiability for helios under weaker trust assumptions. In: European Symposium on Research in Computer Security, Springer (2014) 327–344
10. Chaum, D.L.: Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM **24**(2) (1981) 84–90
11. ElGamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE transactions on information theory **31**(4) (1985) 469–472
12. Schnorr, C.P.: Efficient signature generation by smart cards. Journal of cryptology **4**(3) (1991) 161–174
13. Haenni, R., Koenig, R., Fischli, S., Dubuis, E.: Trustvote: A proposal for a hybrid e-voting system. Bern University of Applied Sciences, Höheweg **80** (2009)
14. Fujioka, A., Okamoto, T., Ohta, K.: A practical secret voting scheme for large scale elections. In: Advances in Cryptology—AUSCRYPT'92, Springer (1993) 244–251
15. Spycher, O., Haenni, R.: A novel protocol to allow revocation of votes in a hybrid voting system. In: Information Security for South Africa (ISSA), 2010, IEEE (2010) 1–8
16. University, P.: Princeton Helios. https://princeton.heliosvoting.org/ Accessed: 2017-06-23.
17. Adida, B., De Marneffe, O., Pereira, O., Quisquater, J.J., et al.: Electing a university president using open-audit voting: Analysis of real-world use of helios. EVT/WOTE **9**(10) (2009)
18. Herschberg, M.A.: Secure electronic voting over the world wide web. PhD thesis, Massachusetts Institute of Technology (1997)