Iraqi Elections in 2014: a Privacy Requirement Evaluation Based on a Polling Place Experience

Ali Fawzi Najm Al-Shammari[1] and Adolfo Villafiorita [2]

[1]Computer Science Dept., University of Kerbala, Kerbala, Iraq
[1]Computer Science Dept., Free University of Bolzano, Bolzano, Italy
[1,2]ICT4G, Fondazione Bruno Kessler, Trento, Italy
[1]alifawzi@uokerbala.edu.iq
[2]adolfo.villafiorita@fbk.eu

Abstract: Democracy was not a well known term for the Iraqi people till 2003, when the US and coalition forces begun a military action against the Iraqi regime at that time. After that, the new constitution in Iraq allows the citizen to elect the government, the local governments, and the parliament, every 4 years. For this reason, the Independent High Electoral Commission (IHEC) was established to manage, control, and run the elections. In the first two elections, the voting system was a "regular" paper-based system. Recently, in 2014, the process has been improved by making the voter authorization process electronic. In this paper, we will describe the latest voting system used in the Iraqi election and make some evaluation about the system fulfillments of privacy requirements, based on a polling station experience.

1 Introduction

The voting system used in the parliament Iraqi elections in 2005 and 2009 was a paper-based voting system. This system has the advantage of being usable, since it has a simple voting procedure that allows most of the voters to vote in autonomy. Public verifiability is supported, since the cast votes are tallied publicly in each polling station after closing the poll. Authorised public entities, i.e., observers, monitor this process and can keep a copy of the tallied station result.

In the recent election, in 2014, the IHEC introduced a new component, implemented by Andra [Ind14], to partially automate the voting procedure. More specifically, they added a component that can manage the voter identification process. This component uses a smart card reader and a biometric fingerprint scanner to identify voters. Each voter, therefore, is provided with a smart identification card (SID) in the pre-election phase to be used in the election day as an identifier. The IHEC claims that this improvement can mitigate the risk of double voting, vote changing and vote stuffing, since it allows them to verify that each tallied vote belongs to single eligible voter. This is what we call the "eligibility verifiability" [KRS10].

However, based on the current available resources on this system [IHE14, II14], we were

able to analyse the election process in a polling station. This analysis shows that the system is vulnerable to a set of risks that can compromise the privacy requirements, namely: anonymity, receipt freeness, and coercion resistance. More in details [LSVB09], by compromising *anonymity* we mean that it is possible to know which voter has cast a particular vote. By compromising *receipt freeness* we mean that it is possible for a voter to present evidence about his/her selection. Finally, by compromising *coercion resistance* we mean that there is a way for a third party to control a voter's selection. In this paper, we also define the term *risk* as an exposure to a failure in a system functionality, caused by an attack.

Such risks might cause violations of the Iraqi legislation. For instance, Article 5 of the Iraqi constitution states that "The people are the source of authority and legitimacy, which they shall exercise in a direct, general, secret ballot and through their constitutional institutions" [Com05]. Also, Article 5-3 of the IHEC election law number 13 on 2013 states that a voter must cast a vote secretly [oC13].

In this paper, we describe the voting procedures adopted in the recent elections in Iraq. We start by describing the election components in the poll, the stakeholders, and the voting procedures. After that, we highlight the possible risk scenarios and the assumptions under which these are made possible. Finally, we provide our recommendation to mitigate such risks by proposing a slight modification to procedures and to components.

2 Polling Station Experience

The election in Iraq divides the precincts at a provincial level. Each province has a number of polling places, which are voting centers that contain one or more polling station. The polling station is where voters can cast their votes. In this section, we describe the election procedure in a polling station. First, we describe the station materials and stakeholder, and second the voting procedures.

2.1 Station Materials

There are two types of materials in a polling station: sensitive and non-sensitive. The sensitive materials include those materials that could be used to influence the election result, namely: paper ballot, ballot stamp, voters list, voting ink, station forms, smart card reader device, and supervisor smart card. The non-sensitive materials includes the logistic materials, for instance, the voting cabin, the empty ballot box, pens, and guideline materials. Beside these materials, we mention the voter smart card, since it is used also inside a polling station. More in details:

- **Paper Ballot Pack:** It contains 50 ballots that are serialised with a unique serial number. This number is written on the ballot in two formats. The first in clear text, and the second encoded in a QR code. A voter can vote either by selecting a party

or by selecting a party and a candidate. An example of the ballot is shown Figure 1.

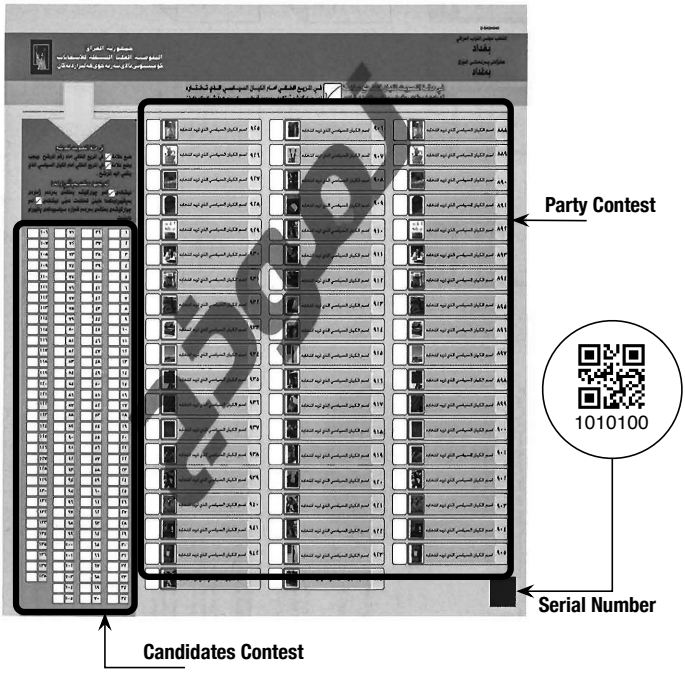

Figure 1: Sample ballot [IHE14].

- **Ballot Stamp:** a manual stamp used to mark the back of a ballot issued to a voter.
- **Voters List:** A hard copy list that contains the names of the eligible voter of a specific station. Each station has a different voters list, since each voter must cast a vote in a dedicated station, that is fixed in the pre-election phase, i.e., during the voter registration process.
- **Voting Ink:** It is used to mark the index finger of any voter who cast a vote. The ink lasts for a few days. Therefore, it considered as a voting evidence that is used to mitigate any malicious try of multiple voting.
- **Station Forms:** hard copy forms used to record voting process output in a station by a station manager. More details about the recorded date is provided in Section 2.3.
- **Voter Smart Identification Card (SID):** a smart card that stores a voter's information, namely: name, date of birth, address, biometric fingerprint, polling place name, and polling station number. This card is used to identify a voter in the election day.

- **Smart Card Reader System (SCRS):** An electronic system that is used to identify eligible voters in a polling station, and also to collect the serial numbers of cast votes to support verifiability. It contains an offline database of the eligible voters. More details about its functionality are provided in Section 2.3.

  Technically, this system comprises three main hardware components, as shown in Figure 2, namely: a tablet provided with a front camera (BQ Maxwell Plus), a thermal printer with a smart card reader (DATECS DPP-250 2"), a fingerprint reader (Futronic FS80). All of these components are gathered in a single box that could be sealed to avoid any unauthorised access. The software of the SCRS is an application installed in Android 4.1 Jelly Bean system.

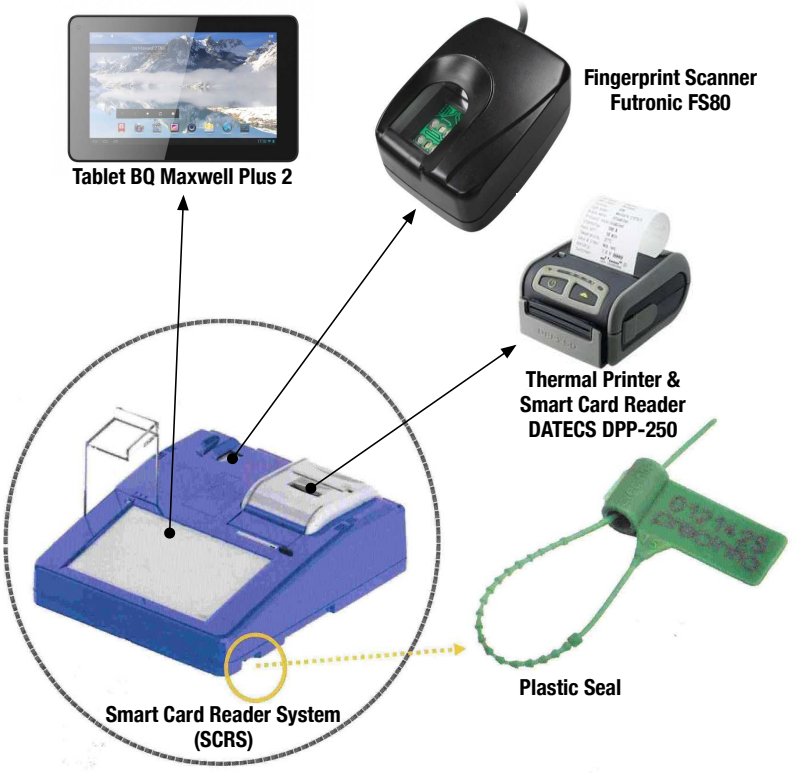

Figure 2: The components of the Smart Card Reader System (SCRS) [II14].

- **Supervisor Smart Card (SSC):** A smart card used to activate the SCRS, and to collect the election data from SCRS after closing the poll.
- **Security Seal:** Plastic seal provided with a unique serial number, used to secure the ballot box, and the SCRS.
- **Ballot Box:** Transparent plastic box where the voter can cast his/her vote.

- **Voting Cabin:** Portable voting cabin where a voter can fill a ballot privately.
- **Secure Plastic Bag:** Special plastic bags used to secure the sensitive materials, e.g., forms, SSC, after closing the poll. They are secure since each one has a unique number and it is not possible to take any material outside the bag without ripping it.

2.2 Stakeholders

Various stakeholders can and need to access a polling station during an election. All of them can positively or negatively impact the security of an election. Understanding who they are and their role is therefore important to reason about the security of an election.

More in details, for the Iraqi election, we distinguish:

- **Polling Place Manager (PPM):** an employee that is responsible for administrating and controlling the general processes in a polling place.
- **Station Manager (SM):** an employee that is responsible for receiving the station materials (sensitive and non-sensitive) in the pre-election phase, installing the station materials before starting the election, administrating voting process during the election, opening and closing the poll, administrating the tallying process after closing the poll, delivering the polling station output, e.g., tallying result, and station materials to the election officials at the end of the election day.
- **Authorization Officer (AO):** an employee that is responsible for verifying voters' eligibility for voting during the election.
- **Ballot Issuer (BI):** an employee that is responsible for issuing paper ballots to eligible voters.
- **Ballot Box Observer (BBO):** an employee that is responsible for observing the ballot box during election, and verifying that each voter marks his/her finger in the permanent voting ink before casting a vote in the ballot box.
- **Technician:** an employee that is responsible for troubleshooting and maintaining the technical components of the SCRSs in a polling place.
- **Election Observer (EO):** an authorised public entity or candidate's agent that is responsible for observing the election process in a polling station during the election day. One or more observers can access a polling station with a maximum limit.

Other authorised people can access a polling station, namely: observer's translators, the press, election officials, and security.

2.3 Election Procedures

We divide the description into three different phases, namely: before opening the station, during the election, and after closing the station.

Before opening the polling station. The day starts when the SM receives a set of ballot packs from the PPM and records the range of their serial numbers in the station form. After that, the SM seals the ballot box using four plastic seals, one for each side, and records their serial numbers. Before opening the poll, the voting equipment is placed in the polling station in a specific configuration: the SCRS and the ballot packs placed on the first side of the room, the voting cabin on the second side, the ballot box and the voting ink on the third side, and finally, the fourth side contains the chairs where the election observers can sit to observe the election.

To open the poll, the AO turns on and starts the SCRS using the SSC. Note that the SCRS is programmed to start only on a specific day and at a specific time.

During the election. A voter arrives at the authorisation desk, where the SCRS is installed, holding his/her SID card and other identification document, e.g., national ID or passport. The AO inserts voter's SID to the SCRS, and scans voter's fingerprint in order to verify his/her eligibility to vote. Voter's data is verified with the database. If the voter is eligible, then the SCRS does the following: displays the voter is authorised to cast a vote, saves the time of the voter's access, blocks the voter's SID (so it cannot be used again in this election), and update the voter's status in the database.

After that, the AO passes the voter's document to the BI, who holds the ballot packs and the voters list. The BI checks the voter's name in the voter's list and issue the paper ballot. Before giving the issued ballot to the voter, the AO take it and scans its QR code with the SCRS. This is done in order to store the issued ballot serial number in the SCRC. After that, the voter takes the ballot to the voting cabin to vote privately, and then cast the vote in the ballot box. The ballot box observer controls that each voter marks his/her finger in the voting ink before casting the ballot.

There is a special case to be discussed here, namely what happens if the SCRS fails in reading the SID of a voter, or if the data in the SID does not correspond to any record in the system database. In this case, the SM checks the existence of the voter's name in the voters list. If it exists, then the voter can vote. In this case, the SM takes the voter's SID, puts it in an envelope, and writes on the envelope the name of the voter, the card serial number, and the reason for collecting the SID. Then, the BI releases a ballot for the voter without being scanned by the SCRS. Also, the voter signs in the voter's list, and the AO signs the back of the ballot with a statement "Smart card was not readable". This is to indicate that the serial number of this ballot has not been scanned by the system.

After closing the station. At the end of the election day, the SCRS stops accepting any voter's SID. At this point, the SM closes the poll and starts the tallying process. In the first

step, the SM secures the ballot box by locking the top hole of the box using a plastic seal, and record its serial number. Then, the station manager asks the AO to store the SCRS data into the SSC and prints the SCRS report. This report includes the polling place name, the polling station name, the total number of eligible voters, the total number of voters who accessed the station, the total number of scanned fingerprints, the total number of the scanned QR codes, the time and date of opening and closing the poll, and finally, the list of scanned ballots serial numbers. The SM updates the station forms with the report data.

After that, the polling officer collects the SSC and the SCRS printed report and puts them in a secure plastic bag. The secure bag serial number is also recorded in the station form. All other sensitive information, e.g., the remaining blank ballot and voting ink, are also secured in plastic bags.

After that, the election employees in the station perform the tallying process publicly. The SM records the count result in the station form. Note that the public observers can keep a copy of this form for verification purposes. However, all of the sensitive materials are secured and sent to the central election office, where the election officials tally and audit the final election result. More specifically, they count the cast votes, compare the result with the station forms, and verify that the serial numbers of the cast votes are the same as the serial numbers of the scanned blank ballots by the SCRS, this to verify that there were no votes stuffed or changed.

Note that, at any time during the election day, the technician of the polling place could be called to solve any technical issue if it occurs.

3 The System Privacy Issues

The IHEC claims that the current system mitigates the chance of compromising the cast votes in the after-election phase. For instance, changing or stuffing a vote requires to hack the data collected from the SCRS (that is, the data in the SSCs and the printed reports) in order to perform a non-detectable attack.

However, in elections there is a trade-off between ensuring the correctness of elections and ensuring secrecy of votes. This is evident, for instance, in the use of ink to mark the finger of voters. While it helps ensure no one can vote twice, at the same time it makes evident to anyone who voted in an election. A similar reasoning can be performed on the new electoral procedures and, based on our evaluation, we found that this system is vulnerable to a set of risks against privacy. More specifically, there are different possible scenarios allow to compromise the anonymity, coercion resistance, and receipt freeness.

Before describing the vulnerabilities, Table 1 recaps the different access privileges stakeholders' have to electoral assets. This is done to undersstand what actor could compromise or access assets to alter assets or disclose private information. For instance, the table shows that the BI and the AO can read (access) the serial number of each issued ballot, and the name of each eligible voter. This could compromise the privacy, as we will describe in the risks scenarios later.

Stakeholder	Access during the election	Access after closing a station	Access in after election phase
Voter	-Ballot number	-	-
Station Manager	-Eligible Voter's information that has failed in SID verification	-Cast vote (Station)	-
Ballot Issuer	-Ballot number -Voter's information -Voters list data -Eligible Voter's information that has failed in SID verification	-Cast vote (Station)	-
Authorization Officer	-Ballot number -Voter's information - Eligible Voter's information that has failed in SID verification	-Cast vote (Station)	-
Election Official	-SCRS component (Precinct)	-	-Cast votes (Precinct) -SCRS data (Precinct) -Voters list data -Eligible Voter's information that has failed in SID verification
Component Firm	-SCRS component (Precinct)	-	-SCRS component (Precinct)
Technician	-SCRS component (Precinct & Station)	-	-SCRS component (Precinct & Station)

Table 1: The different access abilities for the election stakeholders. Note that the (Station) refers to a station access level, and the (Precinct) refers to a precinct access level.

In the following we show how the different access privileges allows one or more actors to compromise the secrecy of elections. All risks requires one or more assumptions to be in place: therefore, the probability of enacting them varies. Still, it is non-zero and understanding under what conditions these attacks can be performed is a first step to devise procedures which enforce stricter privacy requirements while not compromising any of the traceability requirements that help ensure elections are fair.

Scenario 1. A third party could know how the voter voted. More specifically, a malicious third party could ask a voter to write down the ballot's serial number on a piece of paper during the vote casting process, i.e., in the voting cabin, and provide it as an evidence about how he/she voted. The malicious third party could collaborate with a malicious election official, who has a sufficient access to the ballot box, to reveal the vote of a given ballot serial number.

Scenario 2. A malicious AO could reveal the link between vote and voter. More specifically, when a voter arrives, the AO asks him/her for the SID to be verified by the SCRS. At this time, the AO write down the voter's name on a piece of paper, or memorise it. After that, the AO asks the BI to issue a blank ballot. When the AO scans the ballot QR code using the SCRS, he/she can read the ballot serial number. This means that the AO could also write the ballot number in front of the voter's name in the same paper, or memorise it. There are now different ways and occasions during which the voters' votes can

be revealed. The first is during the vote tallying: the AO could consult his/her list of serial numbers-voter's name to disclose all votes; a systematic approach, however, would be easy to detect. The second is after the tallying process, if an actor has access to the ballots and the list **after** the tallying process. This attack would be more difficult to detect, but also more difficult to enact, since it requires the cooperation of more actors. Notice that this attack could be performed on a subset of voters (and thus become easier to perform), for instance to make vote selling easier to perform.

Scenario 3. A malicious SM, AO, BI, and election official could reveal the vote of voters whose SID failed verification, but who are still eligible to vote. More specifically, if the card fails, he/she asks the BI to check the name of the voter in the voters' list. If the name exists, then the voter is eligible to vote. At this point, a malicious AO and BI could write down or memorise, the name of the voter. After that, the SM collects the failed SID in a secure envelope. At this stage, the SM knows the name of the voter. After the voting process, the voter signs the voters' list, and the BI signs the back of the blank ballot before giving it to the voter. This means that the vote, in this special case, will be cast on a ballot signed on the back and, thus, easily recognizable. This allows any stakeholder who has a sufficient access to the cast votes to recognise the specific ballot.

The SM, AO, and BI can then easily associate vote and voters. Regarding the election officials, since they have the access to the voters' list, the collected failed SID, the SCRD report and the cast votes. This allows them to link the special case vote with its voter, if it happened just one time per a single station. For instance, linking the marked vote with voter's signature on the voters list.

As an additional special case, the voters selling their votes could compromise their SID's on purpose, to ensure their votes get cast in ballots signed by the election officials. This could ensure all the vote sold are easily recognizable, although an easier scenario is just taking a picture of one's vote in the cabin.

Scenario 4. A malicious or hacked SCRS could save data that links the voters' identity and their ballot serial numbers. The malicious data could be saved either in the internal memory of the SCRS tablet component, or in the tablet removable memory. In this case, a malicious election official who has a sufficient access to the malicious data could collaborate with another malicious election official who has a sufficient access to the cast votes, both of them could be the same person, in order link between vote, serial number and voter.

Scenario 5. A malicious or hacked SCRS could use the tablet wireless interface, e.g., the WiFi or the Bluetooth, to broadcast malicious data that links a voter with ballot serial number during the election day. More specifically, when the SCRS reads both of a voter data and ballot QR code, it broadcasts the linking data to a malicious device, e.g., a smart phone with a malicious application, that could be handled by a malicious person nearby. For instance, malicious observer, employee, and security. The secret could be revealed by

providing the collected data to a malicious election official who has a sufficient access to the cast votes.

In our analysis, the root failure causes of the scenarios mentioned above can be traced to two main issues. The first issue is that the SCRS is used both for voter authentication and for ballot issuing. While this simplifies traceability (one voter-one vote), it also gives the possibility for a malicious SCRS to link a voter and his/her ballot, i.e., by linking the voter identification data and ballot serial number. The second issue is that the ballot number is not protected, i.e., it is written in clear text. This makes it possible for a malicious employee and voter to keep this number in order to break the anonymity later by collaborating with a malicious stakeholder who has a sufficient access to the cast votes.

4 Improvement Recommendations

We propose two approaches to mitigate the possible system vulnerabilities. The first is to change the procedure, and the second makes a slight change in the ballot.

Considering the procedures, the scanning of the ballot QR must not be performed during the voter identification process. We recommend that this done after closing the election, during the vote tallying process. This can avoid the possibility of a malicious SCRS to link a vote by ballot, since the votes' serial numbers will be scanned randomly. Furthermore, such approach would not compromise the integrity, since it is not possible to stuff a vote to the box during the election, while the entire day process is observed by the public observers and by the station employees.

The second recommendation is to hide the ballot serial number, in a way that prevents anyone from reading it during the election, and allows the SM to reveal it later, during the tallying process. Hiding the ballot serial number could be performed by using different techniques, for instance scratch to reveal the QR code, similar mechanism used in this system [AR06], or by using invisible ink and marking pen as used by [CCC+08]. Furthermore, we recommend that the ballot number should be randomised instead of being serialised. Since, with a serialised ballot pack, revealing the serial number of a single ballot means revealing the numbers of all ballots in the pack.

Considering our recommendations, the voting process could be described as the following: the voter identifies him/herself using SCRS, receives the ballot with the anonymous code, fills the ballot privately, cast the filled ballot in the ballot box. The design of the ballot must allow the box observer to check that the ballot code is maintained hidden (not revealed) while the ballot folded in voter's hand (i.e., if the voter maliciously revealed the ballot number, then it must be avoided). After closing the election and during the tallying process, the SM reveals the ballots code, using a sufficient tool, and scans them using the SCRS. This would mitigate the possibility of performing the mentioned risk scenarios, while keeping the same level of traceability of the current implementation.

5 Conclusion

Iraqi has recently transitioned to a democracy and it is defining its procedures to ensure elections are fair and all voters are given the possibility of voting in secrecy. Simplifying quite a lot on the research in the area, there is, traditionally, a trade-off between these conflicting requirements: to ensure elections are fair, more traceability on the process is required; to ensure voters' votes are secret, less traceability is usually called upon.

In new democracies, where also the apparatus of the Public Administration needs to be reinforced (consider, for instance, the introduction of identification cards or the maintenance of voters' lists), the Iraqi electoral commission has introduced various novelties to make the improve traceability and fairness of elections.

This is an important step to make elections more credible. However, it also comes with new risks and this paper envisages that the Iraqi voting system has a set of vulnerabilities that could compromise the privacy requirements. The vulnerabilities are caused by two main issues, which are the mix of two critical processes to be performed by the same component, and the use of serialised ballots with a readable serial number. We proposed some system modification to avoid these issues with the consideration of minimal changes. It includes changing the voting procedure slightly, changing the physical ballot (the serial code only), and modifying the component software slightly. These changes will add an extra cost caused by the change in ballot production depending on the used code hiding technique, plus the cost of the software modification.

References

[AR06] Ben Adida and Ronald L. Rivest. Scratch & Vote: Self-contained Paper-based Cryptographic Voting. In *Proceedings of the 5th ACM Workshop on Privacy in Electronic Society*, WPES '06, pages 29–40. ACM, 2006.

[CCC+08] 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 *Proceedings of the Conference on Electronic Voting Technology*, EVT'08, pages 14:1–14:13. USENIX Association, 2008.

[Com05] Iraqi Constitutional Committee. Iraqi Constitution. `http://www.iraqinationality.gov.iq/attach/iraqi_constitution.pdf`, 2005.

[IHE14] IHEC. Elections and tallying Procedures for Iraqi Parliament Election 2014 - Training Kit Manual . Iraqi Independent High Electoral Commission, 2014.

[II14] IHEC and Indra. Election Components - Training Kit Manual . Iraqi Independent High Electoral Commission, 2014.

[Ind14] Indra. ELECTORAL PROCESSES INDRA. `http://www.indracompany.com/en/soluciones-y-servicios/solucion/electoral-processes/1361/offering`, 2014.

[KRS10] Steve Kremer, Mark Ryan, and Ben Smyth. Election Verifiability in Electronic Voting Protocols. In *Proceedings of the 15th European Conference on Research in Computer Security*, ESORICS'10, pages 389–404. Springer-Verlag, 2010.

[LSVB09] Lucie Langer, Axel Schmidt, Melanie Volkamer, and Johannes Buchmann. Classifying Privacy and Verifiability Requirements for Electronic Voting, 2009.

[oC13] Iraqi Board of Commissioners. IHEC election law number 13. `http://www.ihec.iq/ihecftp/2014/sys-2014/sys-13.pdf`, 2013.