On the Printing of Ballots

Nyimbi Odero

November 18, 2014

Abstract

The traditional ballot paper is a secure document that is has historically been expensive to print. In this monograph I explore certain novel possibilities that may be implemented to reduce the cost, time and difficulty of printing, distribution, collation, tallying and collection of electoral ballot papers. The system under contemplation is to be used for decision making in ultra low-trust environments. The subject is treated in a non-mathematical manner, but should the reader wish to delve further into the matter, references and a detailed bibliography are provided.

1 Background

1.1 Actors and Gross System Features

In order to deliver objective and subjectively free, fair, and open elections in an environment where the electorate do not trust either their government or the administrators of elections, every effort must be made not only to be free and fair but also to be seen to be free and fair. If we understand the dimensions of distrust, we can better elucidate the transparency needs of every constituency and actor. We model this as a closed system, consisting of the following actors, whose roles we do not define:

Voters: All persons/entities entitled to express a valid choice. (This is a super-set of all groups)

Politicians: A subset of the electorate who seek elective office

Political Parties: Mutually exclusive Groups/Sets of politicians

Government: A subset of politicians holding elective office, simplistically belonging to one of the political parties

Civil Service: Part of the government responsible for supporting elections (Security services, funding mechanisms, etc)

Electoral Administration: An independent organ whose task it is to manage and run elections

1.2 Selection Mechanisms

There are many possible selection mechanisms from sortition to elections, we focus here on a paper ballot scheme in a first to the post competition.

In our model, it is understood that no group as a body trusts itself nor does it trust anybody else. For example the Electoral Administration must satisfy itself that no part or member of the agency is working against the common good or allying itself with any other actor to the detriment of the enterprise. This applies to every actor - with a specific emphasis on the Voting public, for groups of whom, elections are a perceived zero-sum game.

In this simplistic model, in order to ensure incontestable outcomes, any instrument of choice (say a ballot or voting) must have the following qualities:

Finity: There must be a finite number of ballots cast, the number not to exceed the population of the electorate either generally or locally

Uniqueness: Each ballot cast must embody the will of one voter only

Induplicability: No non-ballot should be used as a ballot

Singularity: Two or more people may not cast one ballot

Temporality: A ballot may only be used in one election

Incontrovertibility: A cast ballot may not be uncast

Clarity: The choice given and made must be clear and unambiguous i.e the intention of the voter cannot be nebulous

Non-repudiability: A ballot cast must be counted and accounted for

Validity: Only a recognized voter may cast a ballot

Particularity: A vote must be for only one of the choices given

Specificity: A ballot should only be used in the ballot box/area for which it is intended

Indelibility: A marked ballot cannot be unmarked

Tamper Proofing: Make manifest any changes to the ballot paper

Completeness: Every valid voter must vote

The typical solution to this challenge is a serialized, security printed ballot. This addresses the requirements as follows::

Serialization: Ensures the finity, induplicability, incontroverbility and non-repudiablity of a vote

Security Printing: Ensures the temporality, uniqueness,specificity, tamper-proofing and clarity of the ballot paper. (In the limited sense of our definitions)

Operational Measures: Ensure the validity and Indelibility of the ballot

The completeness, particularity and singularity criteria are a function of the implementation of the voting process, and not of the ballot paper.

2 Other Concepts

2.1 The Four Color Theorem

This mathematical theorem states that on a map of contiguous countries (I.e where no country consists of multiple separate territories) four colors are sufficient to ensure that no two adjacent countries are painted the same color. In actuality the condition of sufficiency and computational ease are quite different - whereas four colors are mathematically sufficient on a plane, it is far easier to use more colors.

2.2 Cryptographic Hashes

In the very simplest description, a cryptographic hash function produces a number h from some text m that is impossible to invert - you cannot get the text by processing the hash value in any way. So that given a message m and a hash h, where $h = hash(m)$, there should be no way to get m from h i.e there does not exist a function $invert$ such that $m = invert(h)$. A cryptographic has is one-way. Also given a message m_1 it should be difficult to find another message m_2 such that $hash(m_1) = hash(m_2)$.

In terms of the electoral application of cryptographic hashes, it is possible to mark a ballot paper with a hash of, say, the election date, polling station and serial number of the ballot, so that nobody can fake a ballot with the same serial number. This guarantees the Specificity of the ballot paper.

3 Attacks and Threats to Paper Based Voting Systems

Broadly speaking there are two broad categories of threat to the integrity of a paper based voting system Threats due to errors and Threats due to deliberate Fraud. Any system of voting must take account of the necessity to diminish both the opportunity and the ability to execute those threats. In broad terms

3.1 Phase Taxonomy of Threats

A taxonomy of threats to the electoral process can be determined by looking at the phase of activities

prior, contemporaneous or after the electoral event:

1. Registration of Voters(Gerrymandering, etc)
2. Polling Place Access (Intimidation, Violence,...)
3. Vote Manipulation (repeat voting,violation of secrecy,...)
4. Ballot Manipulation Prior to Tabulation
5. Threats to the tabulation process
6. Threats to the results of the tabulation process

In this discussion we restrict the discourse to those matters specifically concerning ballot papers and their design, to wit, vote and ballot manipulation and threats to the tabulation process.

3.2 Specific Threats

Multiple Voting: When a voter casts more than one ballot in either the same or a different concomitant election for the same post.

Confirmation: Establishing how a voter voted by circumventing secrecy. Confirmation may be antecedent to or a consequence of bribery, treating, intimidation, or violence

Chain Balloting: Marking a ballot outside the polling booth for a voter who returns a blank ballot after depositing the marked vote.

Voiding: Acting to cancel or invalidate another or ones own validly cast vote (e.g. a counting official adding a mark to a valid vote to make it invalid)

False Balloting: Using fake ballot papers/boxes to falsely convince others that they have validly voted

Substitution: Swapping a validly cast vote with another authentic vote for another candidate and canceling the first, or changing the mark on a validly cast vote

Proxy Voting: Voting on behalf of another against their will (Proxy voting is allowed in some jurisdictions with the permission of the voter)

Personation: A non-voter voting

Biasing: Design of the ballot paper to favor a particular or group of candidates (use of colors, placement, size or font to provide psychological bias)

Incapacitation: Preventing confirmed (in the sense above) voters from voting (e.g by giving them fading ink markers, booth capturing etc)

Ballot Stuffing: Adding ballots that have not been validly cast to a boxes

Destruction: Destroying validly cast ballots in a box (e.g surreptitiously introducing iodine or ink solvent)

Classically, evidence of tampering with the ballot is adduced or prevented by one or more of the following methods:

1. The ballot paper must have been folded to be cast. Should a ballot not have evidently been folded before being cast is is assumed to have been stuffed. This is achieved my making the slot in the ballot box smaller than the ballot.
2. Indelible ink is used to ensure that the marks do not fade over time. The use of pencils and other erasable marks is discouraged.
3. Psychological proscription - using a fingerprint to mark a ballot, though of no forensic value, gives a psychological sense of personalization and security.
4. Voter Identification - making voters use an incontrovertible photo ID ensures a sense of accountability and reinforces the psychological proscription.
5. Voter marking - Marking the person of the voter with some mark that will last for the duration of the election, ensures that there is physical evidence of voting and prevents repeat voting.
6. Ballot box transparency - ensuring that the ballot box is widely and clearly visible and its contents perceptible creates a social barrier to ballot stuffing

7. Continuous Observation - throughout an election every ballot box must be under continuous observation by the competing parties and/or their agents

8. Open Counting - Ballots should be counted in the presence of voters

4 Concerning Implementation

In considering enhancements to the current process, some of the questions that we ask are:

1. What are the major costs in ballot paper acquisition?

2. What are the challenges with the current system?

3. Are there any improvements that can be made in terms of cost efficiency and flexibility?

4. What are the principal challenges to implementation and security?

5. Does the entire ballot paper need to be security printed?

6. Are there other ways of ensuring the security of ballot papers?

7. Can ballot papers be economically printed incountry?

8. Can the IEBC print it's own ballot papers, if so how?

9. Which combination of security and cryptographic techniques will ensure that ballot papers are adequately secure?

10. How do these features ensure security against the catalog of attacks?

11. What procedural protections can enhance the security of the process?

4.1 Possibilities

Conceptually an irreproducible, voter and voting station unique ballot would serve the purposes identified above. A ballot paper should only be used at the polling station for which it is intended and no other. All ballot papers used be associated with a voter physically present at the polling station, and all unused ballot papers should be accounted for. Ideally this ballot paper should be easy and inexpensive to produce legitimately and infeasible to forge, fake or duplicate. The authenticity of the ballot needs to be ascertainable in the field, and the parameters for authentication should be changeable from election to election, at the will of the Commission.

Here is a potential way to satisfy these requirements:

1. The ballot should be printed on copy-evident (void Pantograph) paper `http://www.amgraf.com/pages/voidmaker.html`. This is by printing a pattern on the paper that make it copy and tamper evident. These patterns are inexpensive, irreproducible and unique. The Commission will design a pattern for every type of ballot paper.

2. Each ballot will have a serial number which consists of a sequence and check digit - so that by adding up the digits and dividing by the number of characters you can check the validity of the serial number. (For completeness, the commission should exclude certain terminal digits - (e.g. the last 2 digits should not be a prime number) This, made known at the last minute will make duplication a nightmare for any attempted fraud.

3. A six or seven digit hash should be printed on the ballot paper to guarantee that a ballot can be confirmed on inspection to be genuine. The hash should be generated by the serial number of the ballot, a secret password and the name of the polling station. The hash should be printed as both a number and a bar code. A freely available mobile application can be developed and distributed to make this check easy in the field.

4. Give each polling station a unique color and apply a sticker or stamp to the ballot when it is issued to the voter. By doing this, we ensure that there can be no wholesale ballot stuffing. An attacker can only usefully attack one polling station but would be helpless against any other. We can guarantee that the color

will not repeat at any neighboring polling station.

5. Standard, locally available paper can be used to print this ballot. The mathematically provable security is in the design of the ballot and not in the materials used. (The ballot can be black and white and still be secure - should it be necessary for aesthetic purposes, color may be used in the printing).

5 Elucidatory Matters

Heawoods Conjecture: The topological result known as Heawoods conjecture postulates that the bound for the number of colors which are sufficient for map coloring on an unbounded surface of genus g is

$$\gamma(g) = \left\lfloor \frac{1}{2}\left(7 + \sqrt{48g+1}\right) \right\rfloor$$

where $\gamma(g)$ is called the chromatic number[1]. The genus g can be thought of as the number of holes in the topological surface, so a plane has a genus of 0, a doughnut has a genus of 1 and a figure 8 has a genus of 2. (Interestingly a coffee mug has genus of 1). Heawoods conjecture holds for almost all surfaces except Klein bottles. The first few chromatic numbers are:

g	$\gamma(g)$
0	4
1	7
2	8
3	9

A map of counties or constituencies, which are a plane of genus 0, even though not unbounded, can thus be uniquely colored in a minimum of four colors. With four colors, Heawoods conjecture assures us that, no two adjacent areas will be of the same color.

We apply this result to the color coding of ballot papers and their assignment to polling stations. Total graph coloring (read map coloring) can be automated using Brelaz's Heuristic algorithm, so with a little bit of work, we can increase the amount of work required to nearly infeasible levels for anybody intent on ballot stuffing.

Cryptographic Hash functions: A hash function is a process that is used to mutate digital data of any size to another of fixed length. A small difference in the input leads to a large change in the output. The input is called the message m and the output is variously called the hash code, hash value or merely the hash h. The ideal cryptographic hash function has four main properties[2]:

- it is easy to compute the hash value for any given message
- it is infeasible to generate a message that has a given hash
- it is infeasible to modify a message without changing the hash
- it is infeasible to find two different messages with the same hash.

In generating a hash to use on a ballot, it can be salted (add a secret text or password) and a hash of the polling station, election name and serial number generated for the ballot. The short hash key can be used to ensure that no ballot is fake.

[1] Chartrand, G. "A Scheduling Problem: An Introduction to Chromatic Numbers." section 9.2 in Introductory Graph Theory. New York: Dover, pp. 202-209, 1985.

[2] Cryptographic hash function, `http://en.wikipedia.org/w/index.php?title=Cryptographic_hash_function&oldid=624695751` (last visited Sept. 29, 2014).