A new blockchain-based secure e-voting protocol

Chiara Spadafora
University of Trento

Crittografia: dalla teoria alle applicazioni
July 9^{th}, 2021

Table of Contents

Historical introduction

Athenian Democracy, 500 a.C.

The practice of the Athenians, was to hold a show of hands, except on questions affecting the status of individuals: these cases, which included all lawsuits and proposals of ostracism were determined by secret ballot.

State of Venice, 1268 - 1797

The Venetians' method for electing the Doge was a particularly convoluted process, consisting of five rounds of drawing lots (sortition) and five rounds of approval voting.

Historical introduction

Chartists, 1838

The first major proposal for the use of voting machines came from the *Chartists* in 1838. Among the radical reforms called for in *The People's Charter* there was universal (male) suffrage and voting by secret ballot.

- *Schedule A:* description of how to run a polling place.
- *Schedule B:* description of a voting machine to be used in such a polling place. The Chartist voting machine, attributed to Benjamin Jolly in Bath, allowed each voter to cast one vote in a single race.

Physical vs remote e-voting

In general, two main types of e-voting can be identified:

Definition (Physical E-Voting)

The voter submits electronically its vote in a polling station, supervised by representatives of governmental or independent electoral authorities.

Definition (Remote e-voting)

The voter submits its vote via internet to the election authorities, from any location.

E-voting machines

Machine Types

- **DRE** (Direct Recording Electronic) voting machines,
- **IRE** (Indirect Recording Electronic) voting machines,
- **PCOS** (Precint Count Optical Scan) voting machines,
- **EBM** (Electronic Ballot Marker),
- **VVPAT** (Voter Verified Paper Audit Trail) machines
- **Punched Cards** (discarded, received considerable notoriety in 2000 when their uneven use in Florida was alleged to have affected the outcome of the U.S. presidential election).

Real use cases

Physical e-voting

- USA, 1964 $\rightarrow$ DRE, PCOS.
- India, 1990 $\rightarrow$ M3 + VVPAT.
- Belgium, 1991 $\rightarrow$ IRE.
- Brazil, 2018 $\rightarrow$ no paper ballots.

Real use cases

Internet voting

- Estonia, 2009 $\rightarrow$ Helios.
- New South Wales (Australia), 2011 $\rightarrow$ iVote.
- Switzerland, 2015 $\rightarrow$ Swiss Post.
- Canada, France, Armenia.

Real use cases

E-voting failures

- The Netherlands, 2007.
- Germany, 2009.
- Kazakhstan, 2011.
- Ireland, 2012.
- Norway, 2014.

Real use cases

Blockchain voting trials

- Colombia, 2016.
- City of Zug (Switzerland), 2018.
- Tsukuba City (Japan), 2018.
- USA, 2018-2020.
- Russia, 2020.

Sommaire

Type of e-voting	*Country*
Physical e-voting	Australia, Belgium, Brazil, India, Namibia, Philippines, South Korea, Spain, United Arab Emirates, Russia, Salta Province and Buenos Aires, Albania, Bangladesh, Bhutan, Bulgaria, Canada, Republic of Congo, Dominican Republic, Fiji, France, Honduras, Iran, Iraq, Kyrgyzstan, Mexico, Moldova, Peru, Oman, Pakistan, Venezuela.
Online voting	New South Wales, Switzerland, Canada, France, Gujarat, Philippines, South Korea, El Hoyo de Pinales, Armenia, Åland Islands, New Zealand, Oman, Pakistan, Panama.
Blockchain voting	City of Zug, India, South Korea, Thailand, Tsukuba City, Russia, Colombia, Ukraine.
Discontinued	The Netherlands, United Kingdom, Norway, Finland, Germany, Ireland, Kazakhstan, Japan.

Table: Sommaire of e-voting by country

E-voting requirements

Definition (Correctness)

An adversary cannot alter or cancel votes nor cause voters to double vote.

Definition (Fairness)

Any participant cannot gain knowledge of the voting result before its final publication.

E-voting requirements

Definition (Transparency)

Anyone should be able to audit the system.

Definition (Privacy)

No entity involved in the voting process can link a cast ballot to the voter who cast it.

E-voting requirements

Definition (Universal Verifiability)

The correctness of elections results can be verified by all observers.

Definition (Individual Verifiability)

Every voter can check that its vote has been cast correctly and has been accurately counted in tallied results.

- **Cast-as-intended verifiability:** every voter can control that his vote was correctly cast.
- **Recorded-as-cast verifiability:** every voter can control that his vote was recorded as he cast it.

Security requirements

Definition (Coercion resistance)

Voters should be able to cast their ballots as they want, even if someone tries to coerce them.

Definition (Vote selling resistance)

Voters should not be able to sell their vote.

Table of Contents

Zero-knowledge proof

Definition (Completeness)

If the statement is true then the verifier should accept the proof.

Definition (Soundness)

If the prover wants to convince the verifier to know something that it does not know or the validity of a property that is actually false then the verifier should only accept with negligible probability.

Zero-knowledge proof

Definition (Zero knowledge)

For every verifier $\mathbb{V}$ there exists an efficient simulator that can generate transcripts that are indistinguishable from real interaction between a real prover and $\mathbb{V}$.

Equality of discrete logarithms

Protocol (Equality of discrete logarithms)

Let $\mathbb{G}$ be a cyclic group of prime order p, let $u, \bar{u}$ be generators of $\mathbb{G}$, and let $z, \bar{z} \in \mathbb{G}$, $\omega \in \mathbb{Z}_p$. The prover knows ω and wants to convince the verifier that:

$$u^{\omega} = z \quad \text{and} \quad \bar{u}^{\omega} = \bar{z},$$

without disclosing ω. The values of u, z, $\bar{u}$ and $\bar{z}$ are publicly known.

Blockchain

A *blockchain* is a decentralised data structure containing a list of *transactions* with the following properties:

- **public:** the contents of the blockchain is publicly readable and examinable by anyone,
- **append-only:** an attacker is not able to reorder, delete or modify past transactions.

DDH assumption

Definition (DDH Assumption)

Let a, b, $z \in \mathbb{Z}_p$ be chosen at random and g be a generator of the cyclic group $\mathbb{G}$ of prime order p. The decisional Diffie-Hellman assumption holds if no probabilistic polynomial-time algorithm $\mathbb{B}$ can efficiently distinguish between the tuples (g, g^a, g^b, g^{ab}) and (g, g^a, g^b, g^z).

Table of Contents

Overview

Aim of the research

Design and formalize an e-voting protocol which achieves:

- coercion resistance;
- vote-selling resistance;
- universal verifiability;
- individual verifiability:
  - cast-as-intended verifiability;
  - recorded-as-cast verifiability.

Problem

We want to find a way such that, given the set $\mathcal{V}$ of votes and the set $\mathcal{PK}$ of public data, is possible to determine how many votes each candidate received while given $\mathcal{V}' \subset \mathcal{V}$ it is impossible to do so.
At the same time we want to create a set of private data $\mathcal{SK}_i$ for each voter that allows the individual verifiability, via a zero knowledge proof, only to the direct recipient.

Solution

We constructed two sets of votes: one of valid votes, the other comprising the fake ones. Every voter owns a number of voting tokens equal to the number of candidates. Some of them are real, some fake but they are ***indistinguishable***. When voting, every token must be spent.

- $\mathbb{G} = \langle g \rangle$ of prime order p,
- fixed $k \in \mathbb{Z}_p^*$, $\mathcal{R} = \{g^{y \cdot (x+k)}\}_{x,y \in \mathbb{Z}_p^*}$,
- fixed $\lambda \in \mathbb{Z}_p^*$, $\mathcal{F} = \{g^{z \cdot (w+\lambda)}\}_{z,w \in \mathbb{Z}_p^*}$.

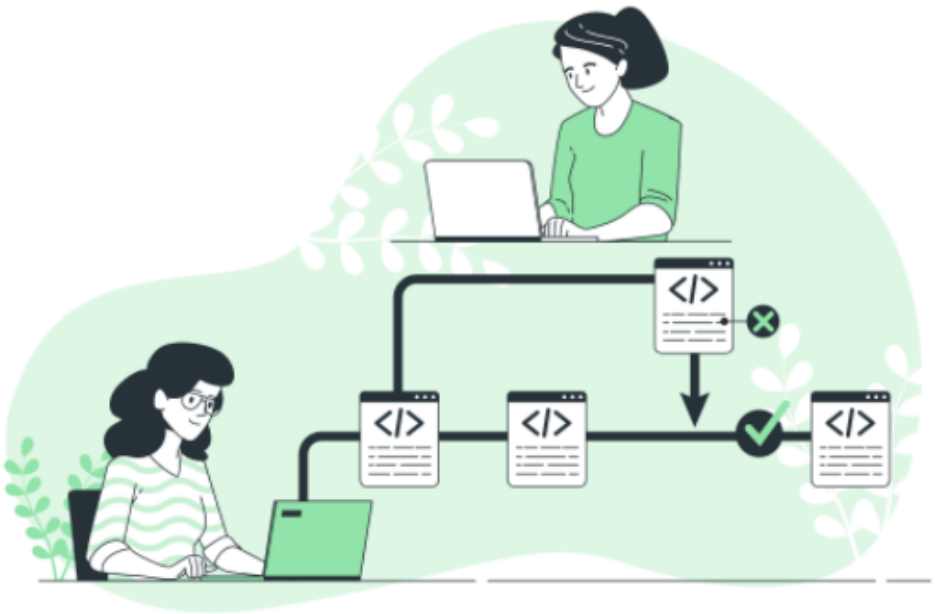
Two-Candidate Protocol - Key Components

The key components involved in my protocol are:

- A finite set of voters $V = \{v_1, \ldots, v_N\}$ with $N \in \mathbb{N}$ the number of eligible voters.
- Two distinct candidates named *Alpha* and *Beta*.
- Two different trusted authorities $\mathcal{A}_1$ and $\mathcal{A}_2$.
- One ballot b_i comprising two *v-tokens* for $i \in \{1 \ldots N\}$, i.e. one for each eligible voter.

- A group $\mathbb{G}$ of prime order p, in which the DDH assumption holds, along with a generator $g \in \mathbb{G}$.
- A zero-knowledge proof derived from the Schnorr protocol.

High level description: Setup

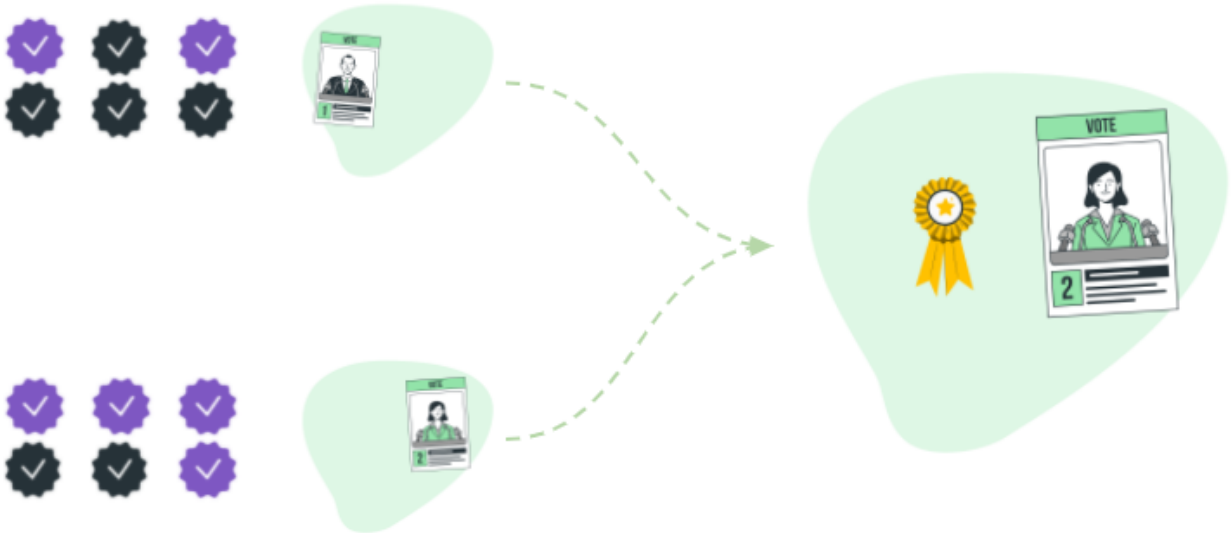


High level description: Registrar

High level description: Voting Phase

High level description: Tallying

High level description: Tallying



Mathematical description: Setup

The authority $\mathcal{A}_1$ selects a secure group $\mathbb{G}$ of prime order p in which the DDH assumption holds, along with a generator $g \in \mathbb{G}$, then it publishes $\mathbb{G}$, g, p.

- $\mathcal{A}_1$ generates the private values: k, λ, α_1', α_2' and x_i', y_i' for every $i \in \{1 \dots N\}$ and publishes g^k, g^λ, $g^{\alpha_1'}$, $g^{\alpha_2'}$, and the pairs $(v_i, g^{x_i'})$, $(v_i, g^{y_i'})$ for every $i \in \{1 \dots N\}$.
- $\mathcal{A}_2$ generates the private values: α_1'', α_2'' and x_i'', y_i'' for every $i \in \{1 \dots N\}$ and publishes $g^{\alpha_1''}$, $g^{\alpha_2''}$, and the pairs $(v_i, g^{x_i''})$, $(v_i, g^{y_i''})$ for every $i \in \{1 \dots N\}$.

Mathematical description: Registrar

For every voter v_i the ballot is constructed:

$$b_i = (b_{i,1}, b_{i,2}) = \left(g^{y_i(x_i+k)}, g^{y_i(x_i+\lambda)}\right)$$

with

- $y_i = y_i' \cdot y_i''$,
- $x_i = x_i' \cdot x_i''$.

Mathematical description: Voting Phase

- Voters express their preference sending the valid token to the preferred candidate, and the fake token to the other candidate. The two *v-tokens* are sent with a transaction on the blockchain to the respective candidates.
- Each voter receives the receipt of the vote (which basically is the insertion of the transaction in the blockchain), moreover the assumed properties of the blockchain guarantee that no vote is changed or deleted.

Mathematical description: Tallying

In order to count the votes, the authorities have to process the tokens received by each candidate, substituting the *voter's mask* y_i with the appropriate *candidate mask* α_l.

$$\left(g^{y_i(x_i+k)}, g^{y_i(x_i+\lambda)}\right) \rightarrow \left(g^{\alpha_1(x_i+k)}, g^{\alpha_2(x_i+\lambda)}\right)$$

with

- $\alpha_i = \alpha'_i \cdot \alpha''_i$.

Mathematical description: Tallying

The number of valid and fake votes received by each candidate is:

$$\prod_{i=1}^{N} g^{\alpha_1(x_i+k)} = g^{\alpha_1(\sum_{i=1}^{N} x_i + R_1 k + F_1 \lambda)}$$

then

$$\left(g^{\alpha_1 \sum_{i=1}^{N} x_i}\right)^{-1} \cdot g^{\alpha_1(\sum_{i=1}^{N} x_i + R_1 k + F_1 \lambda)} = \left(g^{\alpha_1 k}\right)^{R_1} \cdot \left(g^{\alpha_1 \lambda}\right)^{F_1}$$

Proof of security

Definition (Security Game)

The security game for a two-candidate protocol proceeds as follows:

- **Init.** The adversary $\mathcal{A}$ chooses the authority and the $N-2$ users that it controls.
- **Phase 0.** $\mathcal{A}$ and $\mathcal{C}$ run the *Setup* and *Registrar* phases of the protocol, interacting as needed.
- **Phase 1.** $\mathcal{A}$ votes with some or all of the voters it controls.
- **Challenge.** Let C_0 and C_1 be the two candidates, $\mathcal{C}$ flips a random coin $\mu \in \{0,1\}$ and votes with the *v-tokens* of the free voters accordingly: the first free voter votes for C_μ, the second one for $C_{\mu \oplus 1}$.

- **Phase 2.** $\mathcal{A}$ votes with some or all of the voters it controls which did not vote in Phase 1.
- **Phase 3.** $\mathcal{A}$ and $\mathcal{C}$ run the *Tallying* phase of the protocol, and the election result is published.
- **Guess.** $\mathcal{A}$ outputs a guess μ' of the coin flip that randomly assigned the voting preferences of the two free voters.

Proof of security

Theorem

Suppose that the commitment scheme is perfectly hiding and computationally binding. If an adaptive distinguisher adversary can break the scheme, then a simulator can be constructed to play the decisional Diffie-Hellman game with non-negligible advantage.

Sketch of the proof

- Suppose there exists a polynomial-time adversary $\mathcal{A}$ that can guess μ with advantage ε, i.e. $\mathbb{P}[\mu' = \mu] \geq \frac{1}{2} + \varepsilon$. We will show how a simulator $\mathcal{S}$ can play the DDH game with advantage $\frac{\varepsilon}{2}$ interacting with $\mathcal{A}$.
- The simulator starts with considering a DDH challenge:

$$(g, A = g^a, B = g^b, T),$$

with $T = g^{ab}$ or $T = R = g^{\xi}$ and constructs the ballot of the *free voters*.

Sketch of the proof

- Eventually the adversary will output a guess μ' of the coin flip performed by $\mathcal{S}$ during the Challenge. The simulator then outputs 0 to guess that $T = g^{ab}$ if $\mu' = \mu$, otherwise it outputs 1 to indicate that T is a random group element in $\mathbb{G}$.
- When T is not random the simulator gives a perfect simulation, this means that the advantage is preserved. On the contrary when T is a random element $R \in \mathbb{G}$, every token and vote belonging to the free voters becomes independent so $\mathcal{A}$ can gain no information.

Multi-candidate e-voting protocol

This protocol extends the two-candidate's protocol to the multi-candidate case, making it applicable to elections where each voter expresses P preferences among M possible choices.

- With $M > 2$ distinct candidates, the ballot b_i must comprehend M *v-tokens*, one valid and the others fake.
- The voter masks y_i must become lists $(y_{i,1}, \ldots, y_{i,M})$ with $y_{i,I} \neq y_{i,I'}$ for all $I \neq I' \in \{1, \ldots, M\}$ in order to properly conceal fake tokens.
- To assure ballot privacy, three authorities are needed.

Table of Contents

Security considerations

- The underlying blockchain infrastructure and the system of ZKPs ensure transparency and full auditability of the whole process.
- The protocol also achieves extensive security properties, including *coercion* and *vote-selling* resistance, while retaining receipts.
- The two authorities have the same amount of knowledge.
- In a real case scenario, the work of the two authorities can be divided between various pairs of independent authorities, each managing a restricted pool of voters (like a voting district).
- The protocol deals with the possibility of DOS attacks.

References

Articles

- Chiara Spadafora, R. Longo and M. Sala, *A coercion-resistant blockchain-based E-voting protocol with receipts* (2021), in *Advances in Mathematics of Communications*, American Institute of Mathematical Sciences, doi:10.3934/amc.2021005.
- Chiara Spadafora, R. Longo, *Multiple Candidates Coercion-Resistant Blockchain-Based E-Voting Protocol With Receipts* (2021), in *Cryptology ePrint Archive*, Report 2021/851, https://eprint.iacr.org/2021/851.

Thank you!