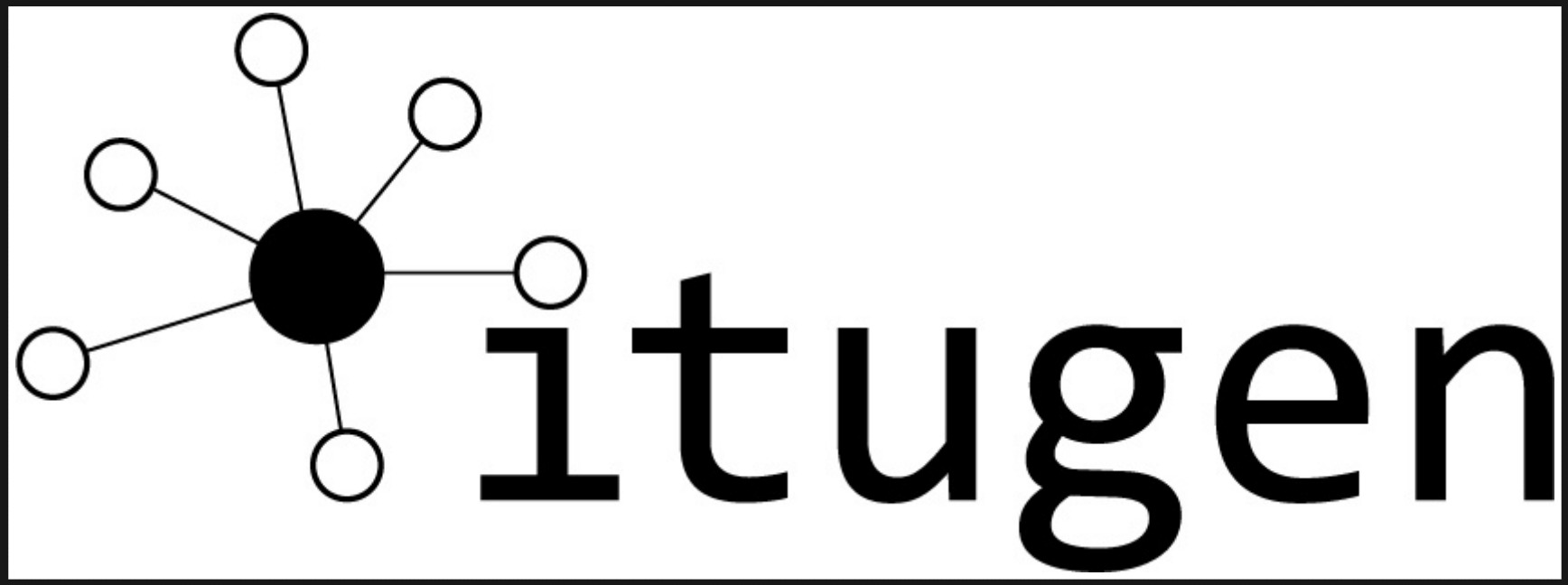


Transparent and anonymous voting on blockchain

Design is similar to Semaphore

- Vote organiser publishes the list of voters on the blockchain
- Users vote anonymously by sending their vote to the blockchain along with a ZKP that they belong to the list and their nullifier is correct.

Itugen: Transparent and Anonymous voting without Tallying Authorities

Guillaume Drevon[1], Vincenzo Iovino[2], and Aleksander Kampa[1]

[1]Sikoba Research
{gd,ak}@sikoba.com
[2]University of Salerno,
vinciovino@gmail.com

6 December 2019

Abstract

We propose itugen, a new verifiable e-voting system that enjoys very strong security guarantees. Our scheme strictly divides ballot allocation from voting, and the voting system ensures both privacy and verifiability. Authorities are trusted only to guarantee the validity and independence of the ballots but cannot break the privacy of any individual voter or subvert the result of the election even if they collude.

Our system is based on isekai, a versatile and powerful implementation of the major recent variants of succinct zero-knowledge proofs including SNARKs, Aurora, Ligero and Bulletproofs. Integrating these mechanisms in a modular way, our e-voting scheme can be instantiated from a number of currently-mature *post-quantum secure* primitives, with the possibility of adding new schemes in the future.

Keywords: e-voting, zero-knowledge, system design.

1 Introduction

E-voting technologies, in particular Internet voting, can help increase voter turnout in elections while reducing the cost of organising them. This could lead to major democratic changes in the coming digital society.

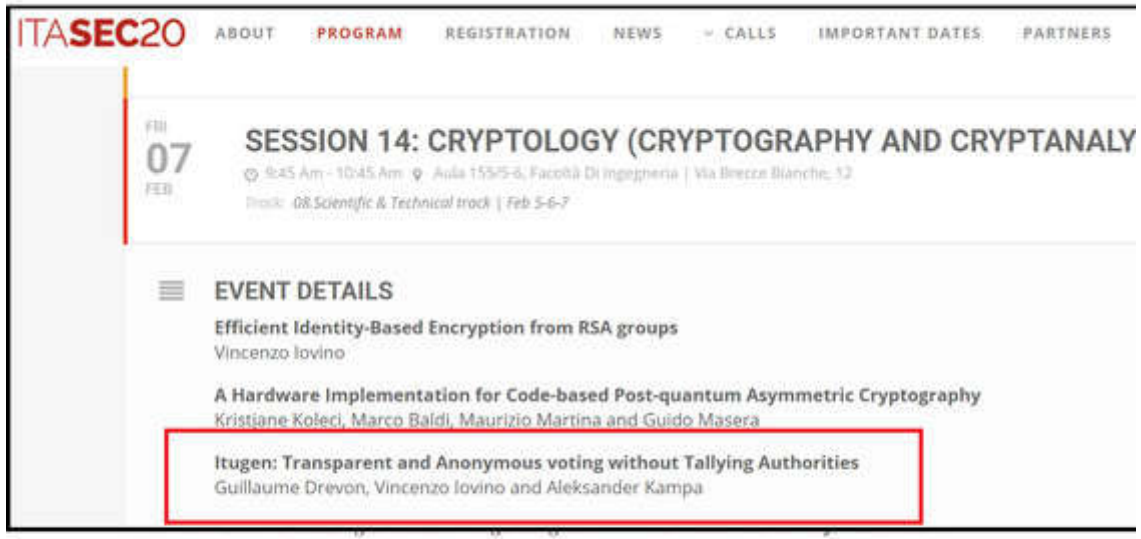
In this paper, we propose and implement itugen, a new e-voting system that we believe to be the first to simultaneously satisfy the following properties:

- **Easy tallying.** The ballots appear on the bulletin board in clear text, so the tally can be easily computed and checked "by hand", as in traditional paper-based elections.
- **Anonymity.** A vote cannot be associated with any of the eligible voters. However, only eligible voters are allowed to vote, and they can cast one and only one valid vote.
- **Individual and universal verifiability.** Each eligible voter can quickly check that

Itugen: Transparent and Anonymous voting without Tallying Authorities

Guillaume Drevon[1], Vincenzo Iovino[2], and Aleksander Kampa[1]

[1]Sikoba Research
{gd,ak}@sikoba.com
[2]University of Salerno,
vinciovino@gmail.com



changes in the coming digital society.

In this paper, we propose and implement itugen, a new e-voting system that we believe to be the first to simultaneously satisfy the following properties:

- **Easy tallying.** The ballots appear on the bulletin board in clear text, so the tally can be easily computed and checked "by hand", as in traditional paper-based elections.
- **Anonymity.** A vote cannot be associated with any of the eligible voters. However, only eligible voters are allowed to vote, and they can cast one and only one valid vote.
- **Individual and universal verifiability.** Each eligible voter can quickly check that

Powered by isekai

- Write statement in C++
- Support Elliptic Curve operation
- Can link to various ZKP schemes, incl. transparent setup

Mass Elections

😀 Large scale e-voting is a 👍 for democracy.

😱 But it implies many constraints

Blockchain Requirements

- Public
- Robust
- Performant
- Cheap

Our Solution

- Dedicated Blockchain
- One platform for all votes
- Tokenomics 
- Double voting is permitted
- Spam filters

Properties

- **Eligibility**: *Only the registered voters can vote, and nobody can submit more votes than allowed (typically only one vote per voter is counted, even if several ballots can be cast).*
- **Robustness**: *The protocol can tolerate a certain number of misbehaving voters.*
- **Integrity**: *Assurance of the accuracy and consistency of votes.*

Properties

- **Individual Verifiability**: *Each voter can check whether his vote was counted correctly.*
- **Universal Verifiability**: *Anybody can verify that the announced result corresponds to the sum of all votes.*
- **Vote-Privacy**: *The votes are kept private. This can also be modelled as an unlinkability between the voter and his vote.*

Challenges

- **Fairness**: *No preliminary results that could influence other voters' decisions are made available.*
- **Receipt-Freeness**: *A voter cannot construct a receipt that allows him to prove to a third party that he voted for a certain candidate. This is to prevent vote-buying.*
- **Coercion-Resistance**: *Even when a voter interacts with a coercer during the entire voting process, the coercer cannot be sure of the vote.*

Challenges

- **Open Blockchain**: *Anybody can join and participate in the protocol*
- **List of Voters**: *The list must contain only legitimate users*
- **Standardization**: *Proofs should have a common format used by the community*

Thank you!

- itugen: https://itugen.com/
- isekai: https://github.com/sikoba/isekai