From Helios to Zeus

Georgios Tsoukalas, Kostas Papadimitriou, Panos Louridas
Greek Research and Technology Network (GRNET) S.A.
{gtsouk,kpap,louridas}@grnet.gr

Panayiotis Tsanakas
National Technical University of Athens
panag@cs.ntua.gr

EVT/WOTE, Washington D.C.
August 12, 2013

Layout

- Zeus's Background
- Short Introduction to Helios
- From Helios to Zeus
  - Modifications due to algorithmic and usability requirements
- Running the Elections
  - Setup, incidents, issues
- Conclusions and Future Plans

Zeus's Background

- Greek academia under tight-schedule reforms
- Universities must elect their new governing councils
- Bill mandates electronic voting option, GRNET shall support
- Reforms controversial in some circles
  - Traditional elections being physically shut down by protesters
  - Numerous incidents in Zeus elections too
- All Zeus elections successful with good turnout
  - Used by many institutions in the country, including the biggest ones

Helios Introduction

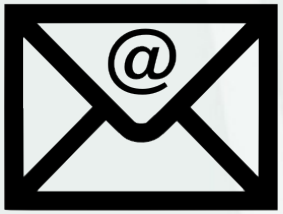
- Verifiable, all-digital voting
- Two versions, originally used mixnets, then switched to homomorphic tallying
  - Software available only for homomorphic (Helios3)
- Voters may repeatedly revise their vote to counter coercion
- Voters invited by e-mail
  - optionally cast audit ballots until satisfied that browser is not compromised
  - then login and cast authentic vote
- Encryption key split across trustees and server
  - Nobody ever holds the entire key

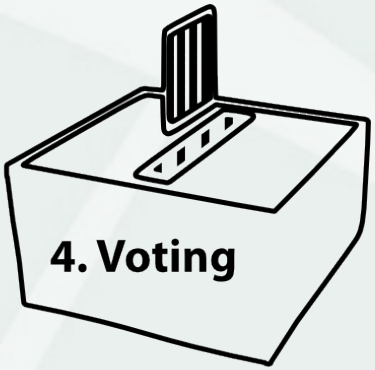
Zeus uses Helios' Workflow

1. Registration

2. Trustee Keys

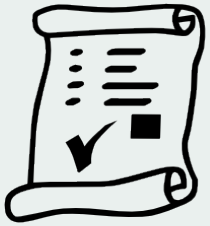
3. Voter Invitation





5. Mixing

6. Decrypt



7. Results, transcript, & proofs

Zeus Crypto Overview

2048-bit safe prime ElGamal group on quadratic residues

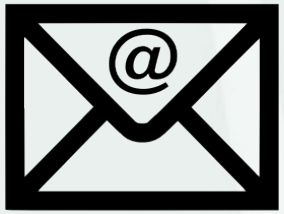
1. Registration

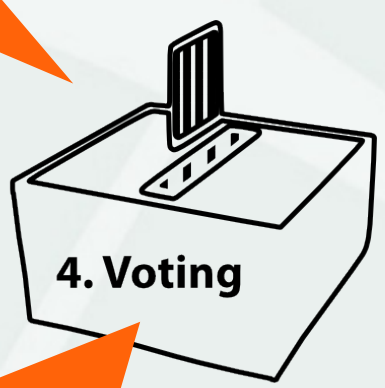
Schnorr DLOG proof

2. Trustee Keys

Chaum-Pedersen DDH tuple proof

3. Voter Invitation



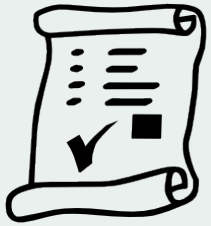


ElGamal signatures on SHA256 digest

5. Mixing

Zero-knowledge proof 128 rounds

6. Decrypt



7. Results, transcript, & proofs

SHA-1 & SHA256 for Fiat-Shamir

Zeus Modifications Overview

STV & party-lists election types

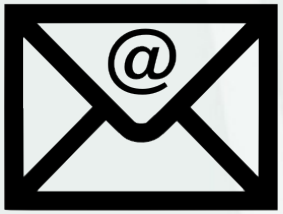
Pre-authenticated invitation link

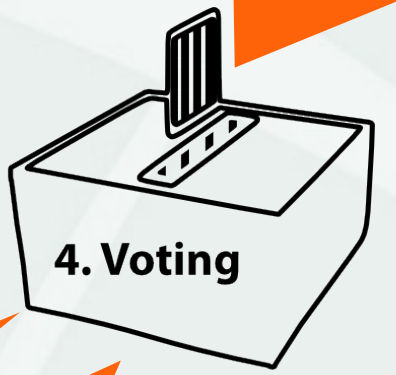
Signed vote submission receipt—no BB

1. Registration

2. Trustee Keys

3. Voter Invitation



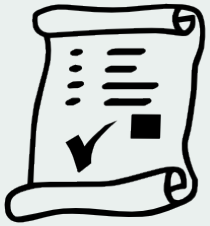


Specialized booth for election type

Modified Audit

5. Mixing

6. Decrypt



7. Results, transcript, & proofs

Exclude voters during voting

Parallel Sako-Killian Mixnet

Parallel decryption in-browser & shell

Structured Proof Document

Modifications: Single Transferable Vote (STV)

- Single Transferable Vote required
  - Special requirement: ties broken by traditional (manual) lot by the electoral committee, not electronically
  - A pre-existing counting system was to be used
- Could not do it with Helios3
  - We moved away from homomorphic tallying
- Implemented a Sako-Killian mixnet
  - Outputs whole ballots as they were encrypted
- Modified ballot structure and encryption proof
  - Encoded ranked candidate list as an integer
  - Discrete log knowledge proof (Schnorr) for encryption validation

Modifications due to Usability Constraints

- Original plan for (mobile phone) two-factor authentication
  - logistically impossible in the timeframe, no usable registry
- Forced choice between audit and normal vote deemed too confusing/dangerous
  - we replaced it with an “audit code”-based, more obscure auditing procedure, based on our two-factor authentication primitives
- Login page between clicking invitation link and voting booth deemed too cumbersome and confusing
  - voters might have tried their webmail or other credentials
  - credentials were embedded in the invitation link

Further Concerns Addressed

- Access to election data and proofs at the discretion of trustees
  - no anonymous access for coercers
  - signed vote submission receipts to compensate for lack of public bulletin board
- Voters can be disqualified during voting and their votes cancelled
  - error, misbehavior, or other valid reason
  - this is logged in the proofs document

Zeus Audit Votes

- Helios' repeated “pretend” audit votes helps prove that the local browser does not cheat
  - Audit votes are revealed as such after uploading to server, so browser can no longer interfere
- Zeus server and voter share secret codes
  - The browser does not have them
  - Voter optionally attaches a code to a submission
  - If the code is among the secret shared it's a real vote
  - if not, it's an audit vote and the browser is asked to reveal the encryption, the user is asked to confirm publishing the audit vote
  - If code attachement is made mandatory, it becomes a second authentication factor

Ranked List to ElGamal Group Element Encoding

- Enumerate all possible candidate selections
  - give smaller ordinals to ballots with fewer candidates
  - this saves a lot of plaintext bit-space if only a few selections are allowed
- 0 is blank vote
- greater than the total selections is a spoilt vote
- we embed more election types within this encoding
  - e.g. multiple party elections

Party List Elections

- Zeus ballot is a ranked list of “candidates”
- Encode party lists as a “candidate” list with standard format
  - include parameters for validation at counting:

    min/max selections per party, whether selections from multiple parties are allowed, etc.
- Each election type has its specialized creation form and booth

Vote Submission Receipt

- Signed by the server
- Contains election key, candidate list, ciphertext, superseded vote (if any)
  - to be used in claims to the trustees, forensics
- Does not identify voter, is publishable
  - No name, IP, time, session, etc.
- Compensates for lack of a safe BB

Running Elections

- Trustees ultimately responsible for elections
  - handled communication with voters
- Helpdesk supports trustees and voters with usability
  - helpdesk member on site in many elections
- Engineering team supports incident handling
  - Help with investigation, reports, public statements
- Trustees negotiated details in many cases
  - asked for specialized reports, requested features, etc.

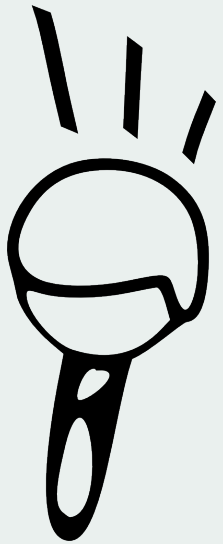
Election Incidents Handled

Attacks against Elections

- Network DoS attempts (2 x slowloris)
- Voter posts his voting link on Facebook
  - he was excluded during voting
- Occupation of infrastructure premises
  - shut network or e-mail servers down
  - circumvented by setting up alternate servers, extending voting for days until resolution
- Social engineering to change voter's registered e-mail
  - detected by us, corrected before election day
- Fake voting e-mails from compromised university machines
  - frustrated voters but ultimately overcome with new servers

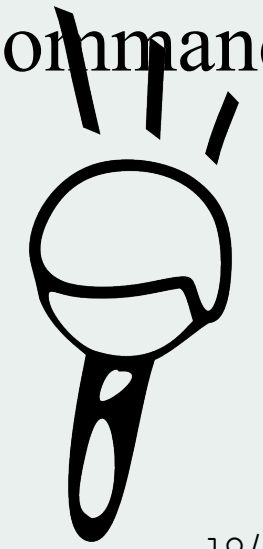
Issues With Voters

- Replies to the e-mail with secret credentials
  - also, “vacation” auto-replies with body
- Failing to open the submission receipt
  - while plaintext, deliberately not named *.txt
- Webmail applications distorting the voting link
  - e.g. using some “exit” gateway
- Browser compatibility
  - hard decision but we dropped IE support
  - not a big problem after all
- Good helpdesk is essential



Issues with Trustees

- USB device with election key fails
  - fortunately our instructions were to have 2 such devices
- Trustees often trust each other too much
  - e.g. exchange their keys for “backup”
- Trustees often needed a tech-savvy “operator” for handling the computer interactions at their command
  - usually someone trusted from IT support



Answering to Skeptics

- Complaint that remote voting destroys the critical social character of election day
- There was detailed documentation of how it works, in layman terms
- Numerous (valid and invalid) objections but obviously politically motivated
- There were no objections on the real problem
  - complete trust in the election service provider

Observations about Trust

- Easier to trust if it **feels** like traditional elections
- An election was cancelled and rescheduled because voting started earlier than announced
- Some were not comfortable with elections running for more than a day, or even at night hours
- Trappings of officialdom and procedure are reassuring
- Most trustee committees were eager to follow due procedure and safeguard elections
  - Some created detailed documentation for the voters
  - Some took extensive counter measures to ensure elections could not be stopped
- Flexibility to answer specialized report & feature requests important
- Trustee insights invaluable to predict behaviors and sentiments

Risks not addressed during elections

- Almost nobody audited their booth in an official election
  - indeed, we made auditing obscure on purpose
- No committee chose to make additional mix
  - even though a lot of effort went into organisation and incident response
  - not even the experts bothered because they trusted us and did not want the overhead

Standardization and Independent Verification are Really Needed

- The most trustees can do is safeguard a proper procedure
  - Only an expert can really evaluate safety and security
- Even if the election service provider is an expert there must be someone **else** checking on them
  - at the least, mixing votes and verifying results
- The independent verifier's job is easy
  - After setting up a server there is no more overhead with any administrative or other issue while running elections
- We are very interested in such independent verifier collaborations
  - maybe work on procedure standardization too

Future Plans for Zeus

- There's more elections scheduled
- Clean-up, start proper development project
- Implement faster mixing
- Work on standalone mixing & verification service and associated standardization
- Optimize usage, browser support
- Consider mobile devices as better trusted clients

Thank You

For inquiries or collaborations, please contact:

{gtsouk,kpap,louridas}@grnet.gr
panag@cs.ntua.gr