12th Athens Colloquium on Algorithms and Complexity
ACAC '17

Everlasting privacy and efficient coercion resistance in remote electronic voting

Panagiotis Grontas, Aris Pagourtzis and Alexandros Zacharakis

In a nutshell...

- We propose a new electronic voting framework that provides:
  - Efficient coercion resistance
  - Everlasting privacy
- By combining:
  - The coercion resistance framework of Juels, Catalano and Jakobsson (**JCJ**)
  - The blind signature based protocol of Fujioka, Okamoto and Ohta (**FOO**)
- Using a new primitive:
  - Conditional Blind Signatures

Electronic Voting is hard

- Voting is a general decision making process that follows each era's technology
- Why can't we vote with our computers?
- Because voting is **inherently hard**, as it must reconcile many **conflicting** properties
- **Integrity**: The result reflects the aggregate choices of the voters
  - No votes are altered, deleted or inserted by an adversary
  - Implemented by **End-To-End-Verifiability**
    - Cast as intended
    - Recorded as cast
    - Counted as recorded

Electronic Voting is hard

- **Privacy**: A means to and end (the voters express their true opinion)
  - Secrecy: The vote is protected against the talliers – (anonymity will also do)
  - Receipt – Freeness: The vote is protected against malicious voters wanting to sell their votes
  - Coercion Resistance: Active adversary that can dictate voter behavior
    - Specific/Random Vote
    - Impersonation
    - Forced Abstention
    - Essential for *remote* electronic voting
- Many more desirable properties
  - Fairness
  - Availability
  - Usability …

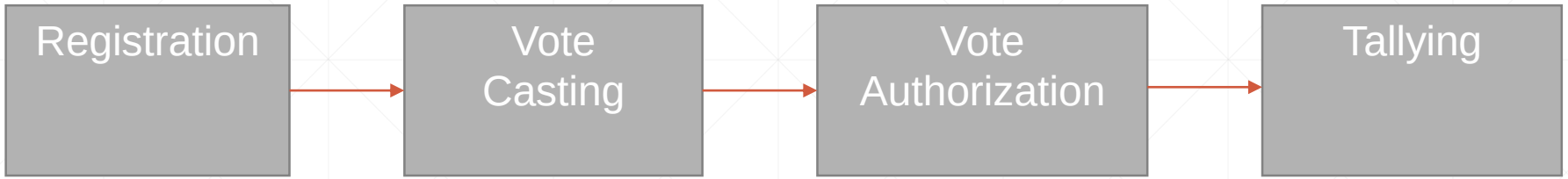
Everlasting Privacy

- **Moran and Naor (2006)**
- Integrity is ephemeral - useful until all parties concede
- Privacy has to outlast the election:
  - Fear of a future oppressive regime
  - Theoretical and practical advances work against computational assumptions
  - In 30 years time all current cryptographic keys will be useless (Adi Shamir ~ 2010)
- Verifiability makes election data widely available
- Information theoretic (*everlasting*) privacy is required

The JCJ Coercion Resistance Framework

- **Juels - Catalano - Jakobsson (2005)**
- **Main idea:** A coercer has no incentive to attack if he cannot tell if his attack succeeded or not.
- **Implementation**: Each voter can cast **many** indistinguishable votes –**fake** and **real**
  - The validity is determined by an accompanying **credential**
  - A single credential is registered as **valid** during a one-time untappable registration process
  - Under coercion the voter generates a random but indistinguishable credential to cast an **invalid vote**
  - Using an assumed moment of privacy the voter casts the **real vote** using the **correct credential**
- Before counting, invalid votes must be removed in a manner undetectable by the coercer

The JCJ Coercion Resistance Framework



- Vote authorization:
  - The valid credentials are published encrypted during registration
  - The counters check them against the supplied ones – in encrypted form
  - If the check is ok the vote is counted
- Complexity: Quadratic in the number of votes – **very** inefficient
- Many efforts have tried to provide linear complexity
- Our approach:
  - Uses 2 phases to reduce complexity
  - Combines coercion resistance with everlasting privacy

Cryptography and Voting

- Cryptographic Primitives have been proposed to implement
  - Vote secrecy and anonymity (Mixnets, Blind Signatures, Homomorphic Encryption)
  - Integrity (Zero Knowledge Proofs)
- Many schemes have been proposed but few have been applied in practice
- The majority of proposals in the literature focus on **integrity**
- Privacy is achieved under:
  - Computational Assumptions: Factoring, DLOG etc. have no PT algorithm
  - Distributed Trust Assumptions: We trust the majority of the voting authorities' members

Basic Cryptographic Assumptions

- **The DLOG Problem is hard**

Given a cyclic group $G = < g >$ of prime order q and a random element $y \in G$ compute $\mathrm{x} \in \mathbb{Z}_q : y = g^x$

- **The CDH Problem is hard**

Given a cyclic group $G = < g >$ of prime order q and a 2 elements $y_{1,} = g^{x_1}, y_2 = g^{x_2} \in G$ compute $g^{x_1 x_2}$

- **The DDH Problem is hard**

Given a cyclic group $G = < g >$ of prime order q, a random element y and 2 elements $y_1 = g^{x_1}, y_2 = g^{x_2} \in G$ decide if $\mathrm{y} = g^{x_1 x_2}$

- The DLOG problem is *believed to be* the hardest.
- There are groups with easy DDHP and difficult CDHP and DLOG

Basic Cryptographic Primitives

- Homomorphic Encryption Scheme
  - $Enc_h(m_1 r_1)\ Enc_h(m_2, r_2) =$ $Enc_h(m_1 m_2, r_1 + r_2)$
  - Reencryption
  - Modified El Gamal (for proofs)
  - Group of prime order q where the DDH problem is hard
    - Private key: $x \in \mathbb{Z}_q$
    - Public key: $h = g_1^x$
    - $Enc_h(m, r) = (g_1^r, g_2^r, mh^r)$
    - $Dec_x(a, b, c) = ca^{-x}$
- Plaintext Equivalence Test (PET) (Jakobsson - Juels 2000)
  - Prove that two ciphertexts indeed encrypt the same plaintext without decrypting them
  - $\frac{Enc_h(m,r_1)^z}{Enc_h(m,r_2)^z} = (g_1^{r_1 - r_2}, g_2^{r_1 - r_2}, \frac{(mh^{r_1})}{(mh^{r_2})})^z = Enc_h(1)^z$
- Zero knowledge proofs
  - Prove possession of credential and vote
  - Prove candidate selection validity
  - Prove correct decryption

Blind Signatures

- A variation of digital signatures for anonymity (Chaum 1982) with many instantiations
- The signer receives and signs a *blinded version of* a message
- The user unblinds the signature and obtains a regular one
- Security properties:
  - **Blindness**: Cannot associate messages with signing sessions
  - **Unforgeability**: Cannot generate valid signatures without the private key

- A useful real world analogy:
  - A message and a piece of carbon paper is placed in an envelope
  - The signer signs the envelope
  - Because of the carbon the signature is transferred to the message
  - The user removes the signed message from the envelope

Conditional Blind Signatures

- Blind signatures that can only be verified by a designated verifier
- Inject a secret bit of information to the signature
- The designated verifier can use his secret key to extract this information
- The signer passes embedded information to the verifier using the signature
- This information is hidden from the user
- Extra Security properties
  - Conditional Verifiability

An instantiation using Okamoto – Schnorr Blind Signatures

(s_1, s_2) b

$< q, g_1, g_2, H >, v, h, k$

m

$r_1, r_2 \leftarrow_r \mathbb{Z}_q$

$x \leftarrow g_1^{r_1} g_2^{r_2}$

x

$u_1, u_2, d \leftarrow_r \mathbb{Z}_q$

$x^* \leftarrow x g_1^{u_1} g_2^{u_2} v^d$

$e^* \leftarrow H(m, x^*)$

$e \leftarrow e^* - d$

e

$y_1 \leftarrow r_1 + e s_1$

$y_2 \leftarrow r_2 + e s_2$

if b =1

$bsig_1 \leftarrow Enc_h(k^{y_1})$

else

$bsig_1 \leftarrow_R \mathbb{Z}_q^3$

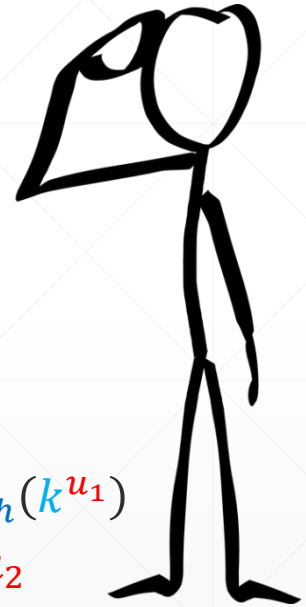
$bsig_2 \leftarrow y_2$

$bsig_1, bsig_2$

$sig_1 \leftarrow bsig_1 \, Enc_h(k^{u_1})$

$sig_2 \leftarrow bsig_2 + u_2$

output (x^*, e^*, sig_1, sig_2)



An instantiation using Okamoto – Schnorr Blind Signatures

Signature Verification

$\mathrm{m}, (x^*, e^*, sig_1, sig_2), z, s$

$e^{*\prime} \leftarrow_r H(m, x^*)$

$y'_1 \leftarrow \quad Dec_z\ (sig_1)$

$y'_2 \leftarrow \quad sig_2$

Check:

$e^{*\prime} = e^*$

$x^{*s} = y'_1 g_2^{y'_2 s} v^{e^* s}$

Round Reduction

- The first step of the interaction can be removed:
  - The signer and the user preagree on a common way to generate the randomness

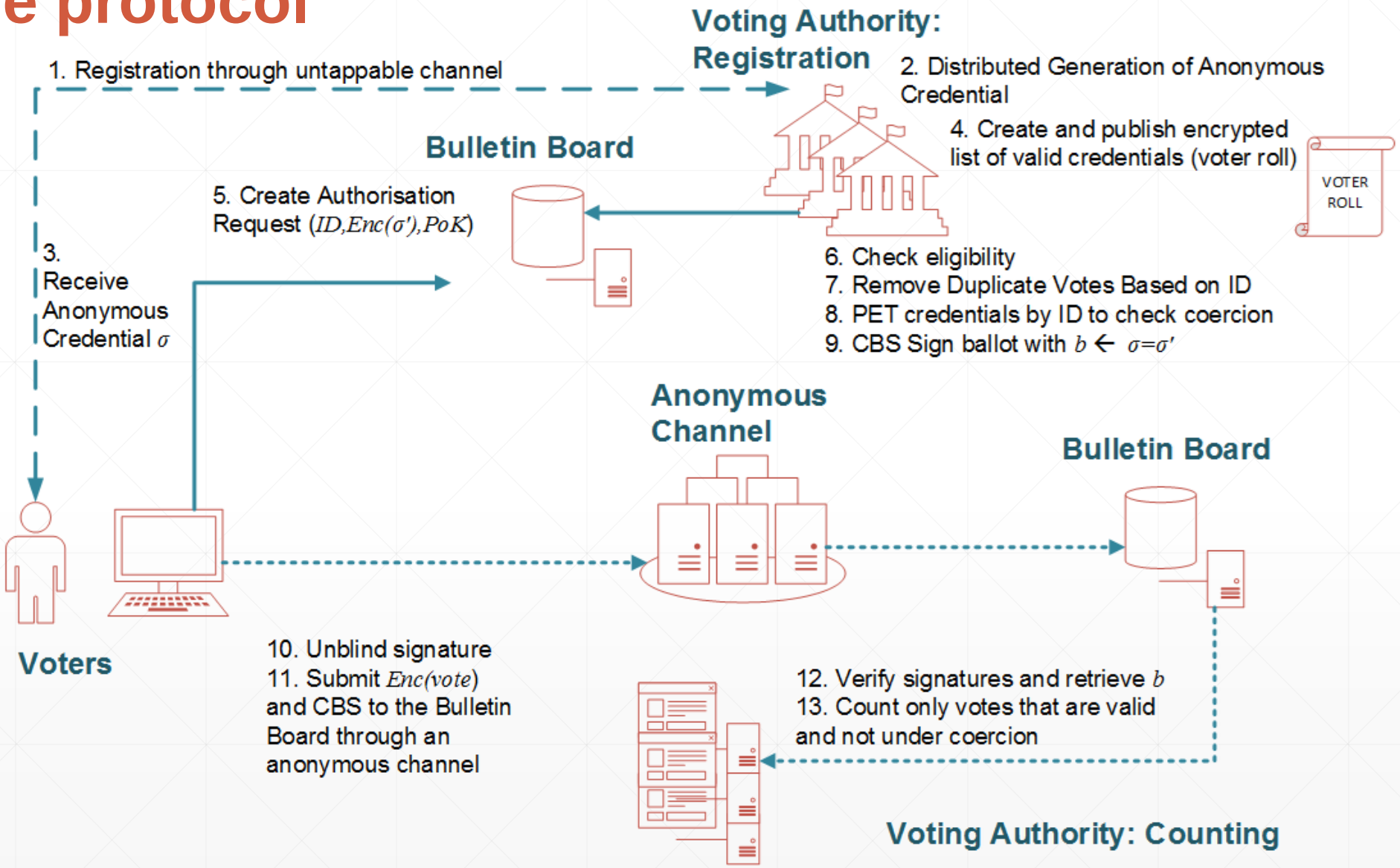
Security

- Blindness: Information Theoretic
- Unforgeability: CDHP
- Conditional Verifiability: DDHP

Using CBS for coercion resistance: Main idea

- Vote authorization occurs during registration and not during counting
- Each ballot is signed using a conditional blind signature
- If the ballot carries the valid registration credential the bit 1 is embedded in the signature
- If the ballot carries a random credential (**coercion**) then the bit 0 is embedded in the signature
- **Efficiency**: We can use the voter id to retrieve the credential
- **Privacy**: The blindness of the scheme hides the ballot contents

The protocol



Security Analysis

- Eligibility
  - Only the eligible voters vote
  - Based on the Unforgeability of CBS Scheme
- Everlasting Privacy
  - Perfect Blindness of the CBS Scheme
- Coercion Resistance
  - Simulation based argument based on the DDH Assumption
- Verifiability
  - Standard Zero Knowledge Proofs
  - Voting Authority actions to be verified:
    - **Registration**: A vote is valid iff the credential is valid
    - **Tallying**: A vote is counted iff it is valid
    - Depends on Conditional Verifiability of CBS
  - Distributed Voting Authority
    - Threshold CBS with honest majority
    - Real world conflict of interest
    - This is the same assumption that most voting schemes do for **privacy**

Questions - Discussion