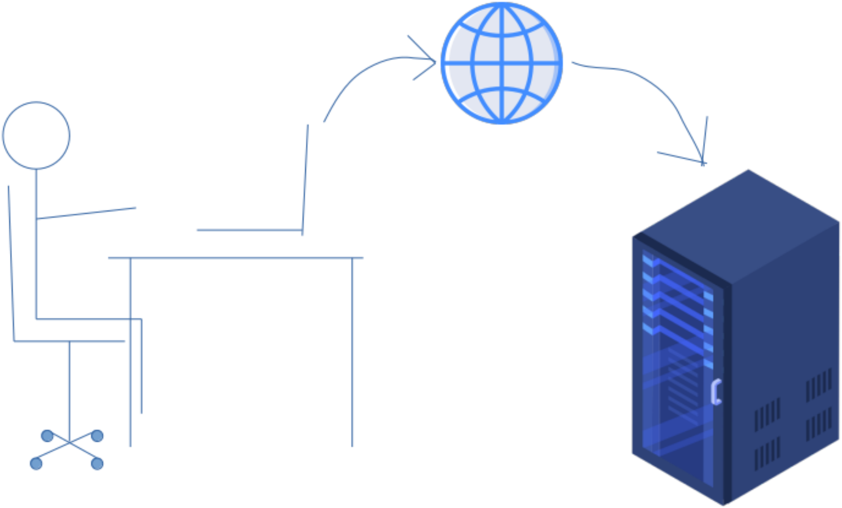
Is the JCJ voting system really coercion-resistant?

Quentin Yang
supervised by
Véronique Cortier and Pierrick Gaudry

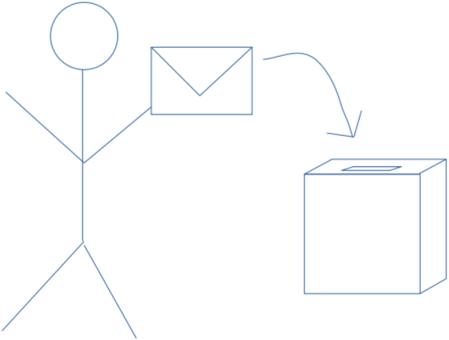
Université de Lorraine, CNRS, Inria

E-Vote-ID PhD colloquium, October 2022

What is electronic voting?

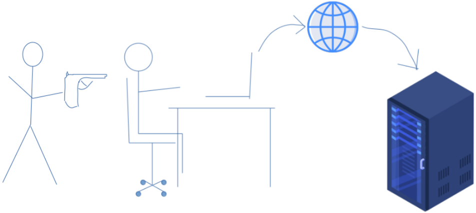


The security goals in electronic voting



Security properties
✓Eligibility ✓Cast-as-intended ✓Vote secrecy ✓Confidence in the result

Coercion-resistance



voteselling.com

Sell your vote!
Easy money!

Fast and secure!

Offer ends in 23 : 58 : 37!!!

Coercion-resistance

Articolo pubblicato il 15 Marzo 2014

La nostra libertà di voto oggi costa appena 50€

Se in Italia, e soprattutto in terra di mafia, i cittadini fossero effettivamente liberi di votare per chi vogliono, la qualità degli eletti sarebbe certamente migliore.

Da tempo denunciamo questa vergognosa realtà ma nessuno prende provvedimenti; evidentemente il controllo del voto torna utile a molti. Abbiamo anche scritto al Presidente Napolitano nel marzo del 2012 ma non abbiamo ricevuto risposta. Ascolta lo SPOT AUDIO _il VOTO quel segreto che la mafia conosce_(1) della campasgna

L'Art. 48 della Costituzione fra l'altro stabilisce che: Il voto è personale ed eguale, libero e

Petition to stop vote buying in Italia (Libero Futuro)

Le Monde

Consulter le journal

Se connecter S'abonner

ACTUALITÉS PRÉSIDENTIELLE 2022 ÉCONOMIE VIDÉOS DÉBATS CULTURE M LE MAG SERVICES

INTERNATIONAL · LETTRES DE

Partage

« Beaucoup d'électeurs sont prêts à vendre leur voix » : l'achat de votes, un fléau bulgare

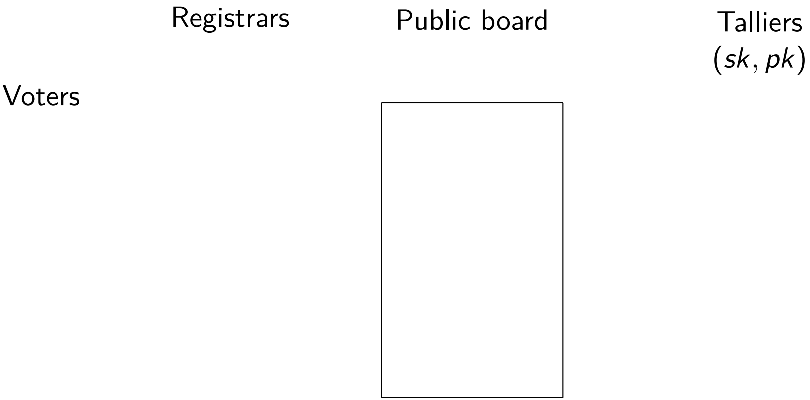
A la veille des élections législatives en Bulgarie du 4 avril, une étude confirme une pratique endémique et partagée par tous les partis du pays : payer les électeurs pour s'assurer leur voix.

Par Jean-Baptiste Chastand (Vienne, correspondant régional)

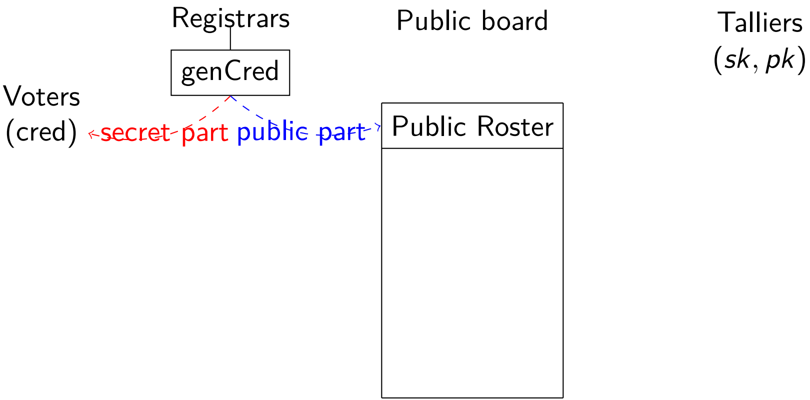
Publié le 02 avril 2021 à 00h14 - Mis à jour le 02 avril 2021 à 12h18 · Lecture 4 min.

Article about vote buying in Bulgaria (Le Monde)

Coercion-resistance in the literature: The JCJ scheme

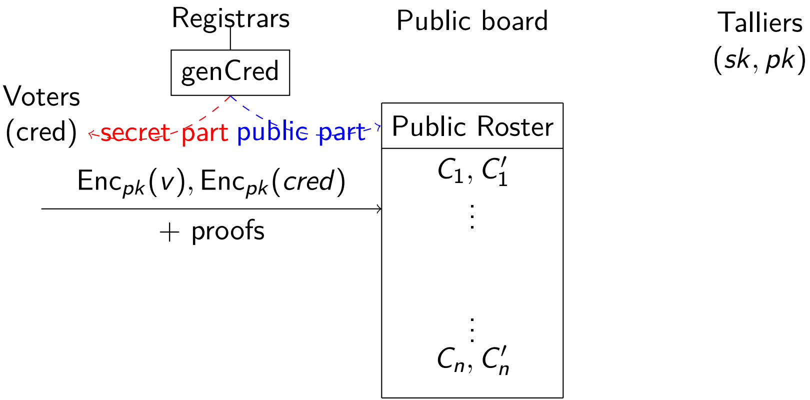


Scheme by Juels, Catalano and Jakobsson, in Coercion-Resistant Electronic Elections, WPES 2005.



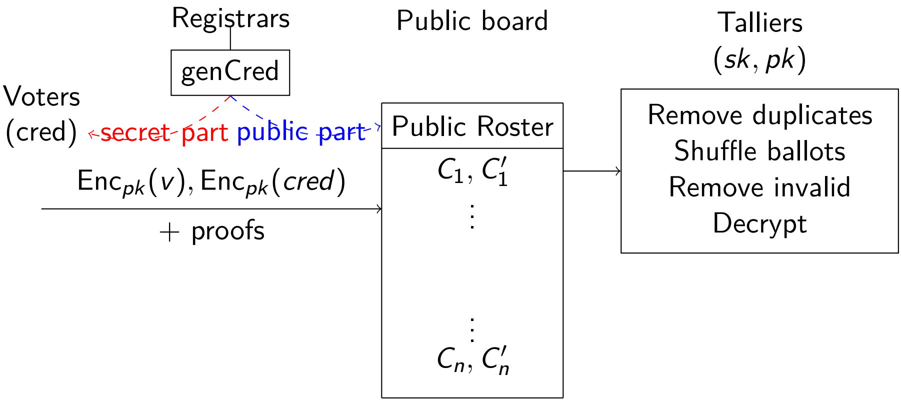
Scheme by Juels, Catalano and Jakobsson, in Coercion-Resistant Electronic Elections, WPES 2005.

Coercion-resistance in the literature: The JCJ scheme



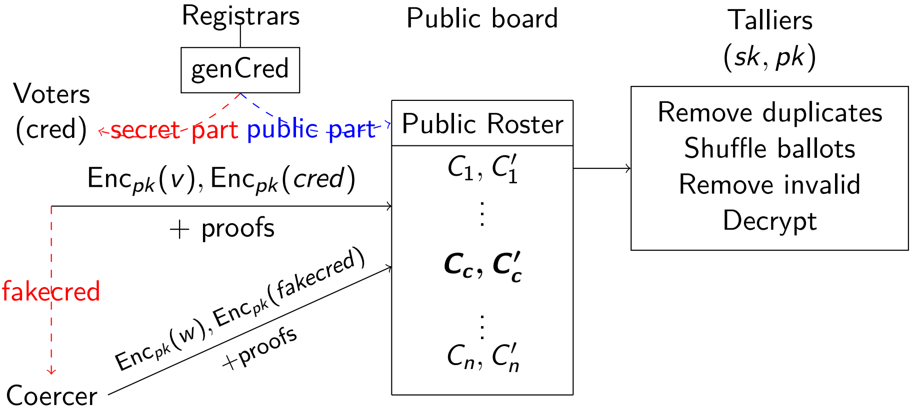
Scheme by Juels, Catalano and Jakobsson, in Coercion-Resistant Electronic Elections, WPES 2005.

Coercion-resistance in the literature: The JCJ scheme



Scheme by Juels, Catalano and Jakobsson, in Coercion-Resistant Electronic Elections, WPES 2005.

Coercion-resistance in the literature: The JCJ scheme



Scheme by Juels, Catalano and Jakobsson, in Coercion-Resistant Electronic Elections, WPES 2005.

Analysis of JCJ - Where does the security come from?

Intuitively:

- Indistinguishability of fake and real credentials.
- Untraceability of the shuffle.

Formally:

- We need a definition of coercion-resistance.

Analysis of JCJ - Defining coercion-resistance

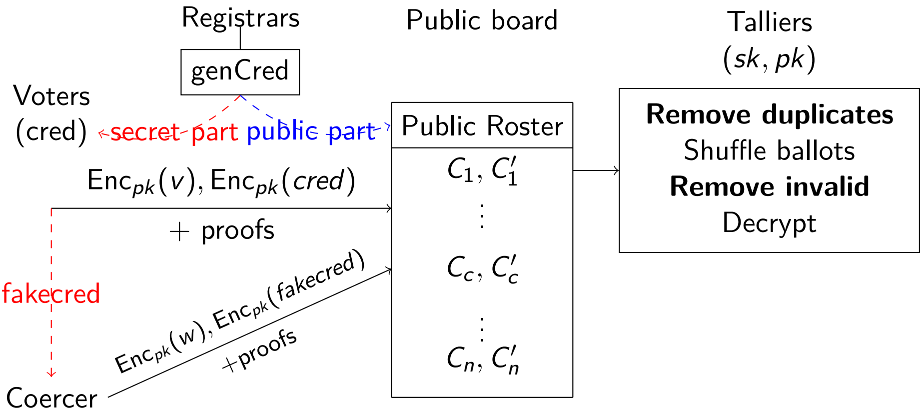
The voter either obeys or evades coercion.

	Real Game	Ideal game
Adversary	Takes part in the protocol	Learns the size of the board
	Learns any public information	Learns the result
	Guesses the behavior of the voter	

Definition (Informal)

A scheme is **coercion-resistant** if the adversary cannot guess the voter's behavior with a better probability in the real game than in the ideal game.

Analysis of JCJ - Is it really coercion-resistant?



Analysis of JCJ - Is it really coercion-resistant?

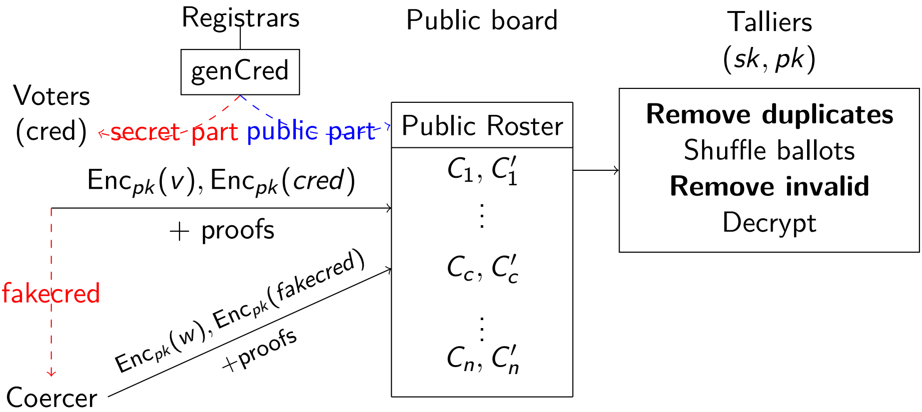
	Real Game	Ideal game
Adversary	Learns the #duplicates Learns the #invalid ballots	Learns the size of the board Learns the (size of the) result
	Guesses the behavior of the voter	

$$size(board) - size(result) = \#duplicates + \#invalid$$

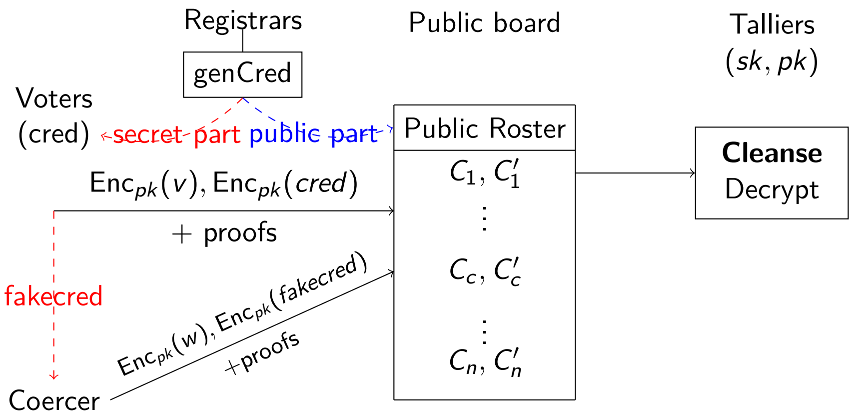
Conclusion:

- The adversary has more information in the real game.
- JCJ is **not** coercion-resistant!

Design of a coercion-resistant protocol

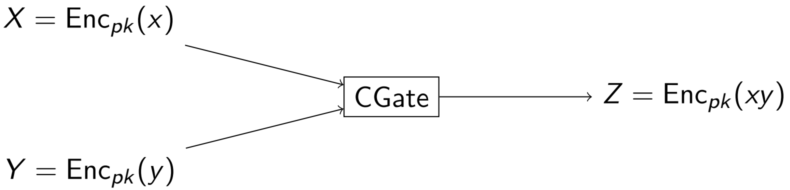


Design a coercion-resistant protocol



Design a cleansing-hiding protocol

We use the CGate primitive to build an MPC protocol:



It allows logical operations on encrypted bits.

Design a cleansing-hiding protocol

We use the framework and security proof from a previous work:

A toolbox for verifiable tally-hiding e-voting systems

Véronique Cortier, Pierrick Gaudry, Quentin Yang
Université de Lorraine, Inria, CNRS

March 2022

ABSTRACT

In most verifiable electronic voting schemes, one key step is the tally phase, where the election result is computed from the encrypted ballots. A generic technique consists in first applying (verifiable) mixnets to the ballots and then revealing all the votes in the clear. This however discloses much more information than the result of the election itself (that is, the winners) and may offer the possibility to coerce voters.

In this paper, we present a collection of building blocks for designing tally-hiding schemes based on multi-party computations. As an application, we propose the first tally-hiding schemes with no leakage for three important counting functions: D'Hondt, STV, and Majority Judgment. We prove that they can be used to design a private and verifiable voting scheme. We also unveil unknown flaws or leakage in several previously proposed tally-hiding schemes.

individual votes. For verifiability, each trustee produces a zero-knowledge proof of correct (partial) decryption so that anyone can check that the result indeed corresponds to the encrypted ballots. The second main approach is based on *verifiable mixnets*. The encrypted ballots are shuffled and re-randomized such that the resulting ballots cannot be linked to the original ones [24, 47]. A zero-knowledge proof of correct mixing is produced to guarantee that no ballot has been removed nor added. Several mixers are successively used and then each (rerandomized) ballot is decrypted, yielding the original votes in clear, in a random order.

Homomorphic tally can only be applied to simple vote counting functions, where voters select one or several candidates among a list and the result of the election is the sum of the votes, for each candidate. We note that even in this simple case, the tally reveals more information than just the winner(s) of the election. Mixnet-based tally can be used for any vote counting function since it

(ESORICS 2022)

Analysis of our cleansing-hiding protocol

Algorithm 3: Real

Require: $\mathbb{A}, \kappa, n_T, t, n_V, n_A, n_C, \mathcal{B}$

$BB \longleftarrow \varnothing$

$\mathsf{pk}, s_1, h_1, \cdots, s_{n_T}, h_{n_T} \longleftarrow P^{\mathbb{A}}_{\texttt{Setup}}(\kappa, n_T, t)$

$V \longleftarrow \mathbb{A}()$

$\{c_i; i \in [1, n_V]\}, \boldsymbol{R} \longleftarrow \texttt{Register}(\kappa, \mathsf{pk}, n_V)$

$(j, \beta) \longleftarrow \mathbb{A}(\{c_i; i \in V\}, \boldsymbol{R})$

if $|V| \neq n_A \vee j \notin [1, n_V] \backslash V \vee \beta \notin [1, n_C] \bigcup \{\phi\}$ **then**

  Return 0

$B \longleftarrow \mathcal{B}(n_V - n_A, n_C)$

for $(i, *) \in B,\ i \notin [1, n_V]$ **do**

  $c_i \longleftarrow \texttt{Fakecred}(c_1)$

$b \xleftarrow{\$} \{0, 1\}$

$\tilde{c} \longleftarrow c_j$

if $b == 1$ **then**

  Remove all $(j, *) \in B$

else

  Remove all $(j, *) \in B$ but the last, which is replaced by (j, β)

  $\tilde{c} \longleftarrow \texttt{Fakecred}(c_j)$

$\mathbb{A}(\tilde{c})$

for $(i, \alpha) \in B$ *(in this order)* **do**

  $\boldsymbol{M} \longleftarrow \mathbb{A}(BB)$

  $BB \longleftarrow BB \bigcup \{m \in \boldsymbol{M} \mid m \texttt{ is valid}\}$

  $BB \longleftarrow \{\texttt{Vote}(c_i, \alpha, \mathsf{pk})\}$

$\boldsymbol{M} \longleftarrow \mathbb{A}(BB)$

$BB \longleftarrow BB \bigcup \{m \in \boldsymbol{M} \mid m \texttt{ is valid}\}$

$\boldsymbol{X}, \Pi \longleftarrow P^{\mathbb{A}}_{\texttt{tally}}(BB, \boldsymbol{R}, \mathsf{pk}, \{h_i, s_i\}, t)$

$b' \longleftarrow \mathbb{A}()$

Return 1 **if** $b' == b$ **else** 0

Algorithm 4: Ideal

Require: $\mathbb{A}, \kappa, n_V, n_A, n_C, \mathcal{B}$

$V \longleftarrow \mathbb{A}(\kappa)$

$(j, \beta) \longleftarrow \mathbb{A}()$

if $|V| \neq n_A \vee j \notin [1, n_V] \backslash V \vee \beta \notin [1, n_C] \bigcup \{\phi\}$ **then**

  Return 0

$B \longleftarrow \mathcal{B}(n_V - n_A, n_C)$

$b \xleftarrow{\$} \{0, 1\}$

if $b == 1$ **then**

  Remove all $(j, *) \in B$

else

  Remove all $(j, *) \in B$ but the last, which is replaced by (j, β)

$(\nu_i)_{i \in V}, \beta' \longleftarrow \mathbb{A}(|B|)$

if $(b == 1) \wedge (\beta' \neq \phi)$ **then**

  $B \longleftarrow B \bigcup \{(j, \beta')\}$

$B \longleftarrow B \bigcup \{(i, \nu_i); i \in V, \nu_i \in [1, n_C]\}$

$\boldsymbol{X} \longleftarrow \texttt{result}(\texttt{cleanse}(B))$

$b' \longleftarrow \mathbb{A}(\boldsymbol{X})$

Return 1 **if** $b' == b$ **else** 0

Fig. 3. Definition of coercion-resistance. κ is the security parameter, n_T the number of talliers, t the threshold, n_V the number of voters, n_A the number of corrupted voters, n_C the number of voting options and $\mathcal{B}$ the distribution of the sequence of votes.

Summary of our contributions

- Detect a shortcoming in the JCJ scheme
- Present a cleansing-hiding protocol which does not have this flaw
- Propose a new definition for coercion-resistance
- Prove that our protocol is coercion-resistant
- Described the exact leakage in JCJ
- Explain how to adapt our methodology to other schemes

Our work is available on eprint: https://eprint.iacr.org/2022/430