Adaptation of an i-voting scheme to Italian Elections for Citizens Abroad

Riccardo Longo[2][0000−0002−8739−3091], Umberto Morelli[1][0000−0003−2899−2227], Chiara Spadafora[2][0000−0003−3352−9210], and Alessandro Tomasi[1][0000−0002−3518−9400]

[1] Fondazione Bruno Kessler {umorelli,altomasi}@fbk.eu
[2] Università degli Studi di Trento {riccardo.longo,chiara.spadafora}@unitn.it

Abstract. We adapt the Araújo-Traoré protocol to Italian elections, with emphasis on anti-coercion measures. In this short paper we focus on a new method for managing anti-coercion credentials for each voter.

Keywords: i-voting · Coercion Resistance · e-Democracy · Verifiability.

1 Introduction

We report on work in progress of an adaptation of the ABRTY protocol [1,2] intended to address specific requirements of the Italian scenario.

First, the Italian Constitution allows voting from abroad - currently by postal vote, with an official experimentation of internet voting run in 2021 [4]. However, it has more stringent requirements than others, e.g., it does not allow early voting as in the U.S. [3]. Second, to access public digital services, Italian citizens are already widely using two eIDAS-notified [7] electronic identification schemes, reaching a High Level of Assurance. Third, vote selling and coercion due to organised crime are historically well-documented threats [5].

Our proposal is intended to guarantee the properties of *coercion-resistance* via the established mechanism of anti-coercion credentials (ACC) as in JCJ [10]; *end-to-end verifiability* and *ballot secrecy*, by encryption with a threshold modified ElGamal scheme [6], zero-knowledge proofs of ballot correctness, and verifiable shuffling and re-encryption [8].

In [2], a forged and a real ACC are distinguished by their private piece, x; this should be delivered over an untappable channel, memorized, and then typed by the voter, but being 20-30 ASCII characters long, it is impractical to remember [9]. To achieve a compromise between security and usability, a short PIN unmasking the ACC would be preferable; Neumann and Volkamer [11] therefore propose allowing voters to set their choice of PIN during the registration phase by being physically present in a controlled environment.

The physical presence of voters is difficult to reconcile with voters residing abroad. However, enabling voters to set their choice of PIN remotely would enable a coercion strategy. We therefore need to deliver a PIN threshold-generated by Registration Tellers (RT) to remote voters without interception by a coercer.

We assume that on a large scale it is very difficult to maintain active surveillance on sufficiently many voters to sway the results of an election, while it is more practical to indirectly monitor them by requesting proofs of the voter's actions and the RTs' responses, e.g. a video. Therefore, we relax the untappable channel assumption assuming instead that gaps exist in the surveillance of the coercer, so a randomization of the response times makes it possible for a coerced voter to conceal communications and pass a forged response as the real one.

Our strategy is the following. During the Registration phase, the RTs send the ACC masked by a random value, of which the κ least significant digits are the PIN. After a first random time, the RTs send the mask to reveal the ACC; after a second, subsequent random time, the RTs send a Designated-Verifier Non-Interactive Zero-Knowledge Proof (DVNIZKP) to prove the correctness of the unmasked ACC. During the waiting periods, a coerced voter can exploit the surveillance gap to request a *forged* mask share from a trusted RT. Since a forged mask reveals a forged ACC, the voter can use it to evade coercion: if the voter received the real mask when not under active surveillance, they can feign to have never received it and pretend that the forged mask is the real one. The waiting period before receiving the DVNIZKP allows a coerced voter to exploit the DV secret key to construct a DVNIZKP that validates the forged mask.

2 Anti Coercion Credential (ACC)

Let $n_{\mathtt{RT}}$ be the number of RT that collaborate to generate and distribute the ACCs so that no single entity may generate a valid ACC, and only the voter may know the whole ACC, assuming that at least $n_{\mathtt{RT}} - t_{\mathtt{RT}}$ do not collude.

Let $\mathbb{G}$ be a cyclic group with prime order p where the q-SDH and SDDHI [1] problems are assumed to be hard. Let g_1, g_2, g_3, o be four generators of $\mathbb{G}$. The ACC for a voter $\mathcal{V}$ is the tuple $(A_{\mathcal{V}}, r_{\mathcal{V}}, x_{\mathcal{V}})$, with $A_{\mathcal{V}} = (g_1 g_3^{x_{\mathcal{V}}})^{\frac{1}{y+r_{\mathcal{V}}}}$, where $(A_{\mathcal{V}}, r_{\mathcal{V}})$ is public and y is the registration secret key, shared among the RTs and common for all ACCs in an election, associated to a public key $R = g_3^y$ that is used to verify the credentials with a DVNIZKP or during the tallying. Given a shared secret value z, z_i will identify the share of z owned by RT$_i$.

We now describe the ACC generation procedure [13,2][3]:

1. The RTs cooperatively generate the public key $V = g_1^{\xi_1} g_2^{\xi_2}$ for the Modified ElGamal Cryptosystem [10] with threshold $t_{\mathtt{RT}}$.
2. Using the same approach as [13], the RTs generate the secrets x, σ, r, y so that each RT$_i$ owns only a share, but they can compute $E_V[(g_1 \cdot g_3^x)^{\frac{1}{y+r}}]$.
3. The value A is retrieved from $E_V[(g_1 \cdot g_3^x)^{\frac{1}{y+r}}]$ by threshold decryption, then every RT$_i$ broadcasts the encryption $E_T^{\tilde{r}_i}[A]$ (where T is the public key of the TTs), so that they can be interpolated to obtain $E_T^{\tilde{r}}[A]$.
4. Each RT_i privately stores the tuple $\mathcal{T}_i = \big(r, x_i, \sigma_i, \tilde{r}_i, E_T^{\tilde{r}_i}[A]\big)$.
5. The tuple $\big(A, r, E_T^{\tilde{r}}[A], E_V^{\hat{r}}[g_1 \cdot g_3^x]\big)$ is called *public ACC* and is published on a Web Bulletin Board (WBB), associated to a pseudonymous identifier of $\mathcal{V}$.

To issue an ACC, to a voter $\mathcal{V}$ the following procedure is followed:

[3] The subscript $\mathcal{V}$ may be omitted when clear from context.

1. $\mathcal{V}$ generates uniformly at random the Designated Verifier private key $e_\mathcal{V} \in \mathbb{Z}_p$ and computes the corresponding public key $D_\mathcal{V} = g_2^{e_\mathcal{V}}$.
2. $\mathcal{V}$ uses an official electronic identification scheme to authenticate and request a pseudonymous credential associated to $D_\mathcal{V}$ that demonstrates $\mathcal{V}$'s right to vote (checked against the appropriate institutional registry).
3. Upon registration, $D_\mathcal{V}$ is linked to a public ACC and published on the WBB, so the tuple $\left(D_\mathcal{V}, A_\mathcal{V}, r_\mathcal{V}, E_T^{\tilde{r}_\mathcal{V}}[A_\mathcal{V}], E_\mathcal{V}^{\hat{r}_\mathcal{V}}[g_1 \cdot g_3^{x_\mathcal{V}}]\right)$ is publicly available.
4. Each RT$_i$ uses $\tilde{r}_{i,\mathcal{V}}$ to compute a NIZKP $\mathit{\Pi}_{i,\mathcal{V}}$ that proves that $E_T^{\tilde{r}_{i,\mathcal{V}}}[A_\mathcal{V}]$ encrypts $A_\mathcal{V}$ and sends to $\mathcal{V}$ the tuple $(i, x_{i,\mathcal{V}} + \sigma_{i,\mathcal{V}}, E_T^{\tilde{r}_{i,\mathcal{V}}}[A_\mathcal{V}], \mathit{\Pi}_{i,\mathcal{V}})$.
5. With $t_{\texttt{RT}}$ tuples, $\mathcal{V}$ can compute $x_\mathcal{V} + \sigma_\mathcal{V}$, and $E_T^{\tilde{r}_\mathcal{V}}[A_\mathcal{V}]$. Then $\mathcal{V}$ recovers from the WBB $r_\mathcal{V}, A_\mathcal{V}$, $E_T^{\tilde{r}_\mathcal{V}}[A_\mathcal{V}]$, verifies the proofs $\mathit{\Pi}_{i,\mathcal{V}}$ and the correctness of the ciphertext interpolation. $\mathcal{V}$ stores $(A_\mathcal{V}, r_\mathcal{V}, x_\mathcal{V} + \sigma_\mathcal{V})$ on the voting device.
6. Each RT$_i$ waits for a randomized time interval then sends the share $(i, \sigma_{i,\mathcal{V}})$.
7. With $t_{\texttt{RT}}$ tuples, $\mathcal{V}$ can compute $\sigma_\mathcal{V}$ which is split as: $\sigma_\mathcal{V} = \hat{\sigma}_\mathcal{V} \cdot 10^\kappa + \texttt{PIN}_\mathcal{V}$. Then $\mathcal{V}$ memorizes $\texttt{PIN}_\mathcal{V}$ and saves $\hat{\sigma}_\mathcal{V} \cdot 10^\kappa$ on the voting device.
8. $\mathcal{V}$ can request multiple times to receive again the shares $(i, \sigma_{i,\mathcal{V}})$, this allows to re-compute $\texttt{PIN}_\mathcal{V}$ if it was forgotten.
9. To request a forged mask (to legitimize a forged PIN) $\mathcal{V}$ chooses $\texttt{PIN}'_\mathcal{V} \neq \texttt{PIN}_\mathcal{V}$, and computes $\sigma'_\mathcal{V} = \hat{\sigma}_\mathcal{V} \cdot 10^\kappa + \texttt{PIN}'_\mathcal{V}$. $\mathcal{V}$ then selects a set I of size at least $n_{\texttt{RT}} - t_{\texttt{RT}} + 1$: the RT$_i$ for $i \in I$ are trusted to collaborate with the evasion strategy. $\mathcal{V}$ uses the points $(0, \sigma'_\mathcal{V})$, $\{(j, \sigma_{j,\mathcal{V}})\}_{j \notin I}$ to interpolate a polynomial $p_{\sigma'_\mathcal{V}}$ of degree $t_{\texttt{RT}}$ and computes the forged shares $\sigma'_{i,\mathcal{V}} = p_{\sigma'_\mathcal{V}}(i)$. Finally a request to receive again the shares is made, but each RT$_i$ for $i \in I$ is privately instructed to respond with the forged share $(i, \sigma'_{i,\mathcal{V}})$, while the untrusted RTs respond normally. Note that once the forged shares have been computed, $\mathcal{V}$ can safely delete $\hat{\sigma}_\mathcal{V} \cdot 10^\kappa$ from the voting device (since the same value will be reconstructed from the forged shares) and pretend to not have received the mask yet (legitimizing the reception of the forged shares).

Once the mask has been sent to $\mathcal{V}$, the voter may verify the correctness of the ACC. After a randomized time, each RT$_i$ sends to $\mathcal{V}$ a share of a DVNIZKP which, once reconstructed through interpolation, proves either the knowledge of $e_\mathcal{V} = \log_{g_2}(D_\mathcal{V})$ or the knowledge of $y = \log_{g_1 \cdot g_3^{x_\mathcal{V}} \cdot A_\mathcal{V}^{-r_\mathcal{V}}}(A_\mathcal{V}) = \log_{g_3}(R)$. The RTs can compute the shares of the proofs because they know the shares y_i of y, and $\mathcal{V}$ is convinced by the proof because $e_\mathcal{V}$ is kept private. On the other hand $\mathcal{V}$ can forge the proof for any PIN to fool a coercer using $e_\mathcal{V}$. We underline that the proof can be also used to verify that the PIN the voter remembers is correct: with a wrong PIN $\mathcal{V}$ retrieves the wrong $x_\mathcal{V}$ and the proof will not be verified.

To prevent RTs from *ballot stuffing* [12] by generating illegitimate credentials - i.e., valid credentials not associated to eligible voters - the values $E_T^{\tilde{r}_\mathcal{V}}[A_\mathcal{V}]$ published on the WBB are used to compute fingerprints [2] that identify legitimate ones. This procedure can be used to revoke credentials by marking the public ACC on the WBB as invalid; any corresponding vote will not be tallied. For other elections, the RTs can issue new credentials to eligible voters by changing only the public ACCs, not the private value $x_\mathcal{V}$, so voters may use the same PIN. This approach is particularly convenient for multiple concurrent elections.

3 Final Remarks

ACCs are interactively generated between RTs, therefore ACC are likely generated in advance rather than on the fly, and a certain number of spare ACCs may be pre-generated in case of revocation e.g., due to compromised voter devices. Voters may find it hard to trust a system in which more voting credentials are generated than actual eligible voters, in the name of service availability. One option could be to post the public ACCs on the WBB in advance, marked as un-assigned until associated with an authenticated voter.

Ideally, the masked ACC should be stored safely enough to guard against malicious exfiltration, but exportable without trace to allow a victim of coercion to vote from a separate device, recalling only their PIN. We leave considerations on PIN length and brute force countermeasures as implementation choices.

References

1. Araújo, R., Ben Rajeb, N., Robbana, R., Traoré, J., Youssfi, S.: Towards practical and secure coercion-resistant electronic elections. In: Cryptology and Network Security. Springer (2010). https://doi.org/10.1007/978-3-642-17619-7_20
2. Araújo, R., Traoré, J.: A practical coercion resistant voting scheme revisited. In: International Conference on E-Voting and Identity. pp. 193–209. Springer Berlin Heidelberg (2013). https://doi.org/10.1007/978-3-642-39185-9_12
3. Bifulco, R., Celotto, A., Olivetti, M.: Commentario alla Costituzione, vol. 1. UTET giuridica (2006)
4. Camera dei deputati: Comitato permanente sugli italiani nel mondo, audizione del dottor Vignali, https://webtv.camera.it/evento/21102
5. Desantis, V.: Il voto degli italiani all'estero: nuove criticità e vecchi problemi nella prospettiva del superamento del voto per corrispondenza. Federalismi.it (22) (2022)
6. Desmedt, Y., Frankel, Y.: Threshold cryptosystems. In: Conference on the Theory and Application of Cryptology. pp. 307–315. Springer (1989). https://doi.org/10.1007/0-387-34805-0_28
7. Overview of pre-notified and notified eID schemes under eIDAS, https://ec.europa.eu/digital-building-blocks/wikis/x/iw3oAg
8. Groth, J.: A verifiable secret shuffle of homomorphic encryptions. Journal of Cryptology **23**(4), 546–579 (2010). https://doi.org/10.1007/s00145-010-9067-9
9. Huh, J.H., Kim, H., Bobba, R.B., Bashir, M.N., Beznosov, K.: On the memorability of system-generated PINs: Can chunking help? In: SOUPS 2015. pp. 197–209
10. Juels, A., Catalano, D., Jakobsson, M.: Coercion-resistant electronic elections. In: Towards Trustworthy Elections, LNCS, vol. 6000, pp. 37–63. Springer (2010). https://doi.org/10.1007/978-3-642-12980-3_2
11. Neumann, S., Volkamer, M.: Civitas and the real world: problems and solutions from a practical point of view. In: Seventh International Conference on Availability, Reliability and Security. IEEE (2012). https://doi.org/10.1109/ARES.2012.75
12. Puiggali, J., Chóliz, J., Guasch, S.: Best practices in internet voting. In: NIST: Workshop on UOCAVA Remote Voting Systems. Washington DC (2010)
13. Wang, H., Zhang, Y., Feng, D.: Short threshold signature schemes without random oracles. In: Progress in Cryptology - INDOCRYPT 2005. pp. 297–310. Springer Berlin Heidelberg (2005). https://doi.org/10.1007/11596219_24