"You Shall not Abstain!" A Formal Study of Forced Participation

Wojciech Jamroga[1,2][0000−0001−6340−8845], Yan Kim[1][0000−0001−7523−8783], Peter B. Roenne[1][0000−0002−2785−8301], and Peter Y.A. Ryan[1][0000−0002−1677−9034]

[1] Interdisciplinary Centre for Security, Reliability, and Trust, SnT, University of Luxembourg
[2] Institute of Computer Science, Polish Academy of Science, Warsaw, Poland

Abstract. In this paper we revisit the idea of participation privacy in secure voting, i.e., when public data does not reveal whether a given voter participated in the election. This is an important property, especially when defining coercion-resistance preventing forced abstention attacks, and it is frequently mentioned as one of the main necessary conditions. However, what has been largely overlooked in the secure voting literature, is the idea of preventing forced participation attacks, i.e., where a voter is forced, or more subtly feels forced, to participate in an election. Whereas a high participation rate might seem like a desirable democratic property, there are cases when a part of the society wants to boycott the vote, e.g., in order to express its disapproval, or to prevent the proposed legislation. We logically formalise the idea of resistance to forced participation and, perhaps surprisingly, show that it is to some extent dual to forced abstention resistance. We also give intuitive examples of systems that satisfy one, but not the other.

Keywords: formal methods · voting · coercion-resistance · receipt-freeness · participation privacy

1 Introduction

In this paper, we revisit the notion of participation privacy in elections. This is a property that can be desirable for several reasons. For example, in Germany and Switzerland it is required that the fact of having voted (or not) must be private. This was also a motivation for the design of the participation-private KTV-Helios scheme [41]. In terms of coercion-resistance, this is an important property especially when wanting to guard against forced abstention attacks where the coercer prevents a voter from casting a vote. The point is that *forced abstention resistance* is a quite separate property from being able to equivocate the content of a ballot to a coercer. Several methods have been developed to achieve this. Firstly, the voting scheme can be designed so that public ballots cannot be directly attributed to a voter, e.g. by using anonymous vote casting channels as in the JCJ scheme [35]. Secondly, obfuscating ballots can be used to hide real ballots, see e.g. [41]. Thirdly, some systems even refrain from publishing ballots

– as it is the case in the Estonian voting system. However, the latter solution fails in providing universal verifiability (especially for eligibility verifiability), a security property which is intuitively at odds with the participation privacy.

What we point out in this paper, is that it has been largely overlooked in the secure voting literature that besides forced abstention resistance, it can also be important to guard against *forced participation* attacks, where the coercer forces the voter to participate in the election, or more subtly the voter feels forced to participate.

A high participation rate might at the first glance seem like a desirable democratic property. Some electoral systems even have mandatory election participation to increase the turnout. Others directly flag people who voted, e.g., providing 'I voted' stickers. However, there are important cases where a part of the electorate wants to boycott an election, e.g., in order to express its disapproval, or to prevent the proposed legislation if certain levels of participation are mandatory.

We demonstrate that the methods used to achieve participation privacy, and especially forced *abstention* resistance, do not necessarily imply forced *participation* resistance, and vice versa. We also formally define these properties in the strategic logic **ATL***, which allows us to derive relations between the privacy notions, thus laying a foundation for future work on the topic.

Structure of the Paper. We first present the motivating scenario from the Polish parliamentary election and referendum of 2023 in Section 2. Next, in Section 3, we introduce the structures and the logical formalism used to represent multi-agent systems and reason about agents' strategic abilities. We also provide an example of how certain privacy-type properties (such as coercion-resistance and receipt-freeness) can be formally translated into corresponding logical formulae. Then, in Section 4, we consider several voting protocols and mechanisms that are designed to provide participation privacy and the corresponding variants of coercion-resistance. We determine whether the proposed measures are vulnerable to forced participation attacks (and thus susceptible to coercion), and study their relation with forced abstention- and forced-participation resistance. In Section 5, we discuss the related work. Finally, Section 6 provides a summary, concluding remarks, and plans for future work.

2 Motivating Scenario: Polish Election & Referendum '23

On 15 October 2023, the latest Polish parliamentary election were held. Together with the election, a referendum took place. It asked four questions in the form of yes/no approval of: selling state properties to foreign entities, increasing the retirement age, dismantling of the barrier along Polish-Belarus border, and admission of thousands of illegal immigrants from Middle East and Africa (sic!) [66].

The organization of the referendum gave rise to a number of controversies (e.g., vague questions, lack of clear guidelines for electoral commissions). It was also argued that the questions were designed in a way that guarantees nearly

unanimous outcome, and thus feign an appearance of massive public support for the ruling party. Importantly, the Polish constitution specifies that if the turnout in a referendum exceeds 50% of the eligible voters, its outcome is legally binding (whatever that would actually mean in case of such ambiguous questions). Moreover, invalid votes *are* included in the turnout. Because of that, opposition representatives were concerned that the results of the referendum could be used to undermine the outcome of the parliamentary election in case the opposition wins majority in the parliament [54,24]. Consequently, the opposition leaders encouraged the voters to boycott the referendum, so that the required 50% turnout would not be reached.

Outcome. The referendum ended with a turnout 40.91% with almost unanimous answer "NO" to all four questions: 96.49%, 94.61%, 96.04%, 96.79% respectively [58]. In accordance with the Constitution of Poland, the National Election Commission (NEC) concluded the result to be not binding [56]. The turnout in the parliamentary election was 74,38%, the highest in the Polish post-1989 history [57]. Thus, nearly half of the election participants refused to take and cast their referendum ballots. While the ruling party obtained the highest support, the coalition of center-left opposition parties won a majority in the new parliament.

Privacy and coercion-resistance. According to the legislation [59], the voters checking in at a polling station were issued two election ballots (one for the lower, and one for the upper chamber of the parliament), as well as one referendum ballot. A voter could refuse to collect a ballot (or ballots). In that case, the electoral commission official handling the registration noted the fact in the voters' register [26]. Since the register was open to see by everybody on the local commission (as well as the members of the superior electoral commissions), the voter's participation (or abstention) could be only considered semi-private. This was even more problematic in smaller – especially rural – constituencies, where most families had a friend or a relative on the local commission. Thus, voters who wanted to boycott the referendum were potentially vulnerable to coercion, e.g., by a dominating family member [67].

Interestingly, the Polish story has an additional, subtle twist. Voters who refused to take the referendum ballot could be, with very high probability, assumed to have voted for the centre-left opposition in the parliamentary election. Thus, the voter's active abstention in the referendum leaks information about the same voter's vote in the election. Reportedly, that posed a significant dilemma for many voters in rural areas (where right-wing sympathies prevail). If they wanted to vote without exposing their center/left preferences, they could either vote for the opposition in the election but participate in the referendum against their wish, or abstain from voting in both the election and the referendum [32]. In consequence, the voter was put in a "voting Nelson hold" that combined forced participation (in the referendum) with forced abstention (in the election).

3 Formal Definitions

Intuitively, privacy is about the *ability* of the voter to prevent the exposure of sensitive information about their part in the election. Similarly, coercion resistance is closely related to the voter's ability to avoid coercion and choose the voting behaviour that expresses their preferences best. We will use standard models of multi-agent systems and the strategic logic **ATL*** to formalise the relevant aspects of the interaction.

3.1 Models of Multi-Agent Interaction

Concurrent Game Structures [3,25,65]. An imperfect information *concurrent game structure* (CGS) is a tuple $M = \langle \mathbb{A}\mathrm{gt}, St, PV, L, Act, d, o, \{\sim_a |\ a \in \mathbb{A}\mathrm{gt}\}\rangle$, where:

- $\mathbb{A}\mathrm{gt} = \{1, \ldots, k\}$ is a non-empty finite set of agents,
- St is a finite non-empty set of states,
- PV is a set of atomic propositions,
- $L : St \mapsto \mathcal{P}(PV)$ is a labelling function,
- Act is a non-empty set of actions,
- $d : \mathbb{A}\mathrm{gt} \times St \mapsto \mathcal{P}(Act)$ denotes actions that are available for each agent in each state,
- $o : St \times Act^1 \times \ldots \times Act^k \mapsto St$ is a transition function that assigns the outcome state $q' = o(q, \alpha_1, \ldots, \alpha_k)$ to each state q and tuple of actions $\langle \alpha_1, \ldots, \alpha_k \rangle$, such that $\alpha_i \in d_i(q)$ for $i = 1, \ldots, k$,
- $\sim_a \subseteq St \times St$ is an (epistemic) equivalence relation for each $a \in \mathbb{A}\mathrm{gt}$.

Informally, whenever $q \sim_a q'$, the states q and q' are said to be indistinguishable to an agent a. Here, every CGS is assumed to be *uniform*, that is:

$$\forall_{q,q' \in St} \left(q \sim_a q' \Rightarrow d_a(q) = d_a(q')\right)$$

Strategies [3,65]. A (memoryless) *strategy* for agent $a \in \mathbb{A}\mathrm{gt}$ is function $\sigma_a : St \mapsto Act$ that prescribes every state with some available action, i.e., $\forall_{q \in St} \sigma_a(q) \in d(a, q)$. We assume strategies to be uniform, that is $\forall_{q,q' \in St} \left(q \sim_a q' \Rightarrow \sigma_a(q) = \sigma_a(q')\right)$. The set of all strategies for $a \in \mathbb{A}\mathrm{gt}$ is denoted by Σ_a^{ir}.[3]

A *collective strategy* for $A = \{a_1, \ldots, a_l\} \subseteq \mathbb{A}\mathrm{gt}$ is a tuple of corresponding (individual) strategies $\sigma_A = (\sigma_{a_1}, \ldots, \sigma_{a_l})$. The set of all such strategies is denoted by Σ_A^{ir}.

Paths [19,3]. An infinite sequence of states $\lambda = q_0 q_1 q_2 \ldots$ in CGS, where there is a transition connecting every q_i with q_{i+1}, is called a *path*. For a path λ and $i \geq 0$ by $\lambda[i]$ and $\lambda[i, \infty]$ we denote a state in i-th position and an infinite suffix starting from $\lambda[i]$ respectively.

The outcome $out(q, \sigma_A)$ returns a set of paths that can occur when agents in A execute σ_A starting from state q onward, that is $\lambda \in out(q, \sigma_A)$ iff:

[3] The lowercase letters "i" and "r" refer to imperfect **i**nformation and imperfect **r**ecall respectively [65].

(i) $\lambda[0] = q_0$, and

(ii) $\forall_{i\geq 0}.\, \exists_{\langle \alpha_1^i,\ldots,\alpha_k^i\rangle}.\, \forall_{a_j\in A}\, \Big(\alpha_{a_j}^i = \sigma_{a_j}(\lambda[i]) \wedge \lambda[i+1] = o(\lambda[i], \alpha_1^i, \ldots, \alpha_k^i)\Big)$.

3.2 Alternating-Time Temporal Logic ATL*

To express system requirements and capture properties of interaction between agents, we will use alternating-time temporal logic **ATL*** [2,3,65].

Syntax. Given a finite set of agents $\mathbb{A}\mathrm{gt}$ and a set of atomic propositions PV, the syntax of **ATL*** is defined by the following grammar:

$$\phi ::= p \mid \neg\phi \mid \phi \vee \phi \mid \langle\langle A\rangle\rangle\psi$$
$$\psi ::= \phi \mid \neg\psi \mid \psi \vee \psi \mid \mathrm{X}\psi \mid \psi\,\mathrm{U}\,\psi$$

where $p \in PV$ is an atomic proposition, $A \subseteq \mathbb{A}\mathrm{gt}$ is a subset of agents (called coalition), temporal operators "X" and " U " stand for "*in the next state*" and "*(strong) until*" respectively. Additional Boolean connectives and temporal operators can be derived in a standard way; in particular: $\mathrm{F}\psi \equiv \top\,\mathrm{U}\,\psi$ for "*now or sometime in the future*" and $\mathrm{G}\psi \equiv \neg\mathrm{F}\neg\psi$ for "*now and always in the future*."

Informally, formula $\langle\langle A\rangle\rangle\gamma$ says that the group of agents A can enforce the temporal property γ no matter how the other agents in $\mathbb{A}\mathrm{gt}\backslash A$ proceed.

Semantics. Given a CGS M, a state q and a path λ, the satisfaction relation $\models$ is inductively defined as follows:

$$\begin{array}{ll}
M, q \models p & \text{iff } q \in L(p),\\
M, q \models \neg\phi & \text{iff } M, q \not\models \phi,\\
M, q \models \phi_1 \vee \phi_2 & \text{iff } M, q \models \phi_1 \text{ or } M, q \models \phi_2,\\
M, q \models \langle\langle A\rangle\rangle\psi & \text{iff } \exists\sigma_A \in \Sigma_A^{\mathrm{ir}}\ \forall_{\lambda\in out^{\mathrm{ir}}(q,\sigma_A)}\ M, \lambda \models \psi,\\
M, \lambda \models \phi & \text{iff } M, \lambda[0] \models \phi,\\
M, \lambda \models \neg\psi & \text{iff } M, \lambda \not\models \psi,\\
M, \lambda \models \psi_1 \vee \psi_2 & \text{iff } M, \lambda \models \psi_1 \text{ or } M, \lambda \models \psi_2,\\
M, \lambda \models \mathrm{X}\psi & \text{iff } M, \lambda[1,\infty] \models \psi,\\
M, \lambda \models \psi_1\,\mathrm{U}\,\psi_2 & \text{iff } \exists i \geq 0\ M, \lambda[i,\infty] \models \psi_2 \text{ and } \forall_{0\leq j<i}\ M, \lambda[j,\infty] \models \psi_1.
\end{array}$$

Thus, the semantics of the "sometime" and "always" modalities becomes:

$$\begin{array}{ll}
M, \lambda \models \mathrm{F}\psi & \text{iff } \exists i \geq 0\ M, \lambda[i,\infty] \models \psi,\\
M, \lambda \models \mathrm{G}\psi & \text{iff } \forall i \geq 0\ M, \lambda[i,\infty] \models \psi.
\end{array}$$

The standard **ATL*** can be further extended to support reasoning about agents' knowledge. The epistemic formula $K_a\phi$ says that an agent $a \in \mathbb{A}\mathrm{gt}$ *knows* that ϕ holds. Hence, the following rule is added to semantic:

$$M, q \models K_a\phi \quad \text{iff} \quad \forall_{q'\in St}(q \sim_a q' \Rightarrow M, q' \models \phi)$$

3.3 Expressing Privacy-Related Properties in ATL*

Let $Vot \subseteq \mathbb{A}\mathrm{gt}$ be the set of eligible voter agents, $c \in \mathbb{A}\mathrm{gt}$ a coercer, and Bal set of possible returned ballots, including a special case of "returning nothing". We use the following functions:

- $info : Bal \mapsto Data$ to extract information that was filled on a ballot;
- $vote : Bal \mapsto \mathcal{P}(Choice)$ to extract information on the selection made only, where $\mathcal{P}(Choice) \subsetneq Data$ and $Choice$ corresponds to relevant information (e.g., set of candidates for single choice voting);
- $vb, vv : Bal \mapsto \{\top, \bot\}$ for ballot and vote validity respectively; the intuition is that a *ballot is valid*, if it was not damaged or completely destroyed, and a *vote is valid* if it was cast with a valid ballot that was also duly filled.

There could be many ways of completing the ballot form (including adding some satellite data), and adding extra notes on the ballot will normally lead to invalidation of the vote, i.e. $\forall_{b \in Bal}(info(b) \neq vote(b) \Rightarrow vv(b){=}\bot)$.

In what follows we consider some $v, v' \in Vot \setminus \{c\}$, s.t. $v \neq v'$, $v^* \in Vot$, $a \in \mathbb{A}\mathrm{gt} \setminus \{v^*\}$, $a^* \in \mathbb{A}\mathrm{gt}$, $i, j \in Bal$, s.t. $i \neq j$, and $x, y \in \mathcal{P}(Choice)$, s.t. $x \neq y$.

The atomic proposition $recor_{v^*,i}$ asserts that a ballot $i \in Bal$ was recorded for voter $v^* \in Vot$, $cast_{v^*,i}$ asserts that a voter $v^* \in Vot$ cast a ballot $i \in Bal$, and $voted_{v^*,x}$ asserts that a voter $v^* \in Vot$ cast some ballot with $x \in \mathcal{P}(Choice)$ selected.[4] Depending on the system, a different set of assumptions and corresponding logical implications and equivalences over aforementioned propositions can be made. For example:

- in systems, where voter casts a single vote maximally one vote per voter can be recorded: $\forall_{v^*,i}(recor_{v^*,i} \Rightarrow \bigwedge_j \neg recor_{v^*,j})$,
- in systems, where voters are allowed to re-vote, effectively overwriting the previously cast votes: $\forall_{v^*,i,j}(recor_{v^*,i} \wedge recor_{v^*,j} \Rightarrow \neg vv(i) \vee \neg vv(j))$,
- in traditional paper-based voting system, where cast-as-intended is provided by design: $\forall_{v^*,b}(cast_{v^*,b} \wedge vote(b){=}x \iff voted_{v^*,x})$.

Additionally, we introduce dual abstract propositions $abst_{v^*}$ and prt_{v^*} denoting voter's genuine abstention and participation in the voting itself. Note that prt_{v^*} alone does not necessarily imply the vote from v^* would count towards a turnout. The exact definition and method for computing a turnout will depend on the legislation; moreover, in many cases (e.g., re-voting) it cannot be inferred from a single ballot alone, and the corresponding turnout function must be defined over a multi-set of returned ballots.

[4] The subtle difference between $voted_{v^*,x}$ and $cast_{v^*,i}$ is that $x \in \mathcal{P}(Choice)$ only indicates the relevant selections (e.g., it would not capture the presence of any "hidden" marks), whereas $i \in Bal$ can represent any possible ballot along with all the information that can be derived from it.

Note also that we formalise coercion resistance as the ability of the voter to *effect any election choice*. Thus, we do not need to represent the *intention* of the voter; it suffices to reason solely about the voter's possible choices.

Fig. 1. Naturally derived implications for considered coalitions.

The paper [68] reviews various definitions for receipt-freeness and coercion-resistance properties, and provides their logical transcriptions with a focus on strategic aspects. The relevant properties (excluding those using the belief operator) are presented below with their original labels:

RF1a.	$\bigwedge_{v,v',x}$	$\neg\langle\langle v\rangle\rangle$	$\mathrm{F}\,(voted_{v,x} \wedge K_{v'} voted_{v,x})$
RF1b.	$\bigwedge_{v^*,a,x}$	$\neg\langle\langle v\rangle\rangle$	$\mathrm{F}\,(voted_{v,x} \wedge K_a voted_{v,x})$
RF2.	$\bigwedge_{v,x}$	$\neg\langle\langle v\rangle\rangle$	$\mathrm{F}\,(voted_{v,x} \wedge K_c voted_{v,x})$
RF3.	$\bigwedge_{v,x}$	$\neg\langle\langle c, v\rangle\rangle$	$\mathrm{F}\,(voted_{v,x} \wedge K_c voted_{v,x})$
RF5.	$\bigwedge_{v,x}$	$\neg\langle\langle c, v\rangle\rangle$	$\mathrm{F}\,(voted_{v,x} \wedge K_c voted_{v,x})$
RF6.	$\bigwedge_{v^*,a,x}$	$\neg\langle\langle v\rangle\rangle$	$\mathrm{F}\,(voted_{v,x} \wedge K_a voted_{v,x})$
CR2a.	$\bigwedge_{v,x}$	$\neg\langle\langle c, v\rangle\rangle$	$\mathrm{F}\,(voted_{v,x} \wedge K_c voted_{v,x})$
CR2b.	$\bigwedge_{v,x}$	$\neg\langle\langle c, v\rangle\rangle$	$\mathrm{F}\,(voted_{v,x} \wedge (\bigvee_y K_c \neg voted_{v,y}))$
CR3.	$\bigwedge_{v,x,y}$	$\langle\langle v\rangle\rangle$	$\mathrm{F}\,(voted_{v,x} \wedge \mathrm{G}\neg K_c \neg voted_{v,y})$

For instance, property **RF2** says that the voter v has no strategy such that eventually v has voted for candidate x and the coercer knows that, however we might choose the actual values of v and x.

The transcription of properties **RF5** and **CR2a** is identical with that of **RF3**, and **RF6** with **RF1b**, and thus written in grey.

3.4 Resistance to Forced Participation and Forced Abstention

Following the approach of [68], we formalise the properties of forced participation resistance (**FPR**) and forced abstention resistance (**FAR**) as:

FPR.	$\bigwedge_{v^*,a}$	$\neg\langle\langle v^*, a\rangle\rangle$	$\mathrm{F}\,(prt_{v^*} \wedge K_a \neg abst_{v^*})$
FAR.	$\bigwedge_{v^*,a}$	$\neg\langle\langle v^*, a\rangle\rangle$	$\mathrm{G}\,(abst_{v^*} \wedge K_a \neg prt_{v^*})$

Thus, **FPR** says that there is no collective strategy for the voter v^* and another voter a which ensures that, eventually, v^* has participated in the election and a knows that v^* has not abstained. Similarly, **FAR** says that there is no collective strategy for the voter v^* and another voter a to make sure that v^* consistently abstains and a consistently knows that v^* has not participated.

Remark 1. Note that quantifiers over voters often exclude the coercer, i.e., range over $Vot \setminus \{c\}$. Depending on the context, this might make a significant difference.

A notable example is Selene voting system [62], where the coercer being a voter himself would possess a knowledge of his own tracker, and then it is possible that a voter, who wishes to fake his vote, happens to point to the coercer's tracker.

Furthermore, we formalise the notion of *public participation privacy* by:

$$\textbf{PPP.} \quad \bigwedge_{v^*,a} \neg\langle\langle\varnothing\rangle\rangle \, \mathrm{F}\,(K_a \neg prt_{v^*} \vee K_a \neg abst_{v^*})$$

Theorem 1. *(i)* $\boldsymbol{FPR} \Rightarrow \boldsymbol{PPP}$ *and (ii)* $\boldsymbol{FAR} \Rightarrow \boldsymbol{PPP}$.

Proof. Follows directly from the facts that $K_a\varphi \Rightarrow \varphi$ for any $a \in \mathbb{A}\mathrm{gt}$, and $\langle\langle\varnothing\rangle\rangle\varphi \Rightarrow \langle\langle A\rangle\rangle\varphi$ for any $A \subseteq \mathbb{A}\mathrm{gt}$. □

Thus, **PPP** is a necessary condition for both **FPR** and **FAR**.

4 Protocols and Examples

In this section, we discuss several example protocols that, in varying degrees, provide resistance to forced abstention and/or forced participation coercion.

4.1 Indelible Ink

Applying an indelible ink (usually by dipping the forefinger of a voter) is designed to prevent double-voting. According to [21,42], one of the earliest adoptions of election inking was in India back in 1960–1980s. This method provides abstention-privacy (in the simplest case, one could simply dip their finger into a bottle of writing ink) but lacks participation-privacy, which opens up possibilities to coercion and may sometimes even undermine the voter's safety.

We found reports of ink compound being smuggled [70], disenfranchisement attacks when voters were forced or tricked into having their finger marked by malicious third-party [7,33], disinformation attacks aimed to weaken public confidence in integrity of the results, threats (both to inked and non-inked voters) [33,21], and post-election violence towards those who had their finger marked [37]. We refer the interested reader to [21,22] for more details and an evidence study.

As a counter-measure to potential exposure of the voter's participation, some countries deploy an invisible ink, such that a special UV LED is needed to check the mark [22,49]. While it does not guarantee complete participation-privacy, it might be seen as its weaker variant under certain assumptions. However, it is notable that with different inking methods, the risks of forced abstention and forced participation attacks appear to have inverse relationship.

Interestingly, [33] describes a case of voters refusing to cast a vote immediately after getting an ink-mark. Depending on the legal constraints, this might be a viable response to forced-participation coercion.

4.2 KTV-Helios

The KTV Helios scheme is designed to have participation privacy [41]. Here the voter casts ballots each encrypting a number. The actual chosen candidate will be the sum of all of these numbers. Others can cast ballots too on behalf of the voter, but without knowing the voter's secret key these ballots will have to be encryptions of zero and thus do not affect the overall vote. The point of these obfuscating ballots is to give the voter plausible deniability: Even if the voter casts a ballot together with the coercer, he or she can update the result by casting another corrective vote, but claim it was an obfuscating ballot from another voter. We have here assumed a coercer model where the voter always casts ballots oneself, and thus knows the corresponding number, i.e., an over-the-shoulder coercer model.

In this model, we also have forced abstention resistance because the voter can cast a vote and plausibly claim it was an obfuscating vote. Interestingly, it might also provide forced participation resistance since – even if the voter first casts a valid vote together with the coercer – he or she can later correct the sum back to zero using a corrective ballot, and claim it was an obfuscation ballot from someone else.

Interestingly, there is a small asymmetry between the two notions in this scheme. If a voter should not vote at all, there is a small probability that no obfuscating votes are cast on behalf of that voter, hence making abstention clear. That is, even without interaction between the voter and the coercer, we have a small probability of leaking the abstention, whereas if the voter participated it would never be provable without interaction between the voter and coercer.

4.3 Estonian E-Voting System

The Estonian system allows to verify ballots directly via the random coins used in the ballot construction. However, to achieve a level of coercion-resistance the system allows for the last-vote-counts re-voting. This kind of a voting system enables forced abstention resistance, since the voter might cast a ballot without telling the coercer. On the other hand, the voter can prove participation by casting a ballot and verifying this together with the coercer, thus we do not achieve forced participation resistance.

4.4 S&P 2024

A recent scheme with vote updating [23] from S&P 2024 is also based on the over-the-should coercion model. Here obfuscating votes are cast by the election authority and these will override votes cast together with a coercer, if the voter has already cast a vote on their own. Due to the obfuscation, this does provide forced abstention resistance in the constrained coercer model of [23]. However, if the coercer casts the very first ballot together with the voter, then this will be a valid ballot which can only be overwritten by other valid ballots. Hence, the scheme does not obtain forced participation resistance.

4.5 JCJ

In the JCJ voting protocol [35] a voter uses secret credentials to cast votes. A coercer is simply presented with a fake credential, and could even try to vote on his own, however ballots with invalid credentials will not be counted. Assuming the tally procedure does not leak, this allows us to achieve resistance against both forced abstention and forced participation attacks.

Yet, as pointed out in [20,14], the public deduplication process might leak important information. Let us e.g. say that the coercer knows that all voters vote twice, but the coerced voter does not know this. Thus, if the coercer sees a vote in the deduplication phase only appearing once, he knows it came from the coerced voter. In consequence, the scheme does not have forced abstention resistance. On the other hand, we could still have forced participation resistance because the voter might simply refrain from casting a vote with the real credential.

4.6 Opt-Out Schemes

Depending on the legislation, a general method striving to achieve forced participation resistance is to include an additional (opt-out) checkbox for "do not participate" on ballots.

The point is that if the scheme already provides coercion-resistance including forced abstention resistance then the coerced voter can cast a ballot and choose this option while being able to deny it to the coercer. Thus in this case forced abstention resistance can help to provide forced participation resistance. However, this option might also be used by a coercer to launch a forced abstention attack, so we again see a duality between the two properties here.

5 Related Work

The related work can be divided into two strands. On the one hand, various flavours of privacy and coercion-resistance have been defined and discussed in the literature. On the other hand, some authors have attempted to capture those properties in modal logics of time, knowledge, and/or strategies. The second strand includes also attempts at automated verification by theorem proving or model checking, based on such formalisations.

Receipt-freeness and coercion resistance. Over the years, the properties of *ballot secrecy*, *receipt-freeness*, *coercion resistance*, and *voter-verifiability* were recognized as important for an election to work properly. In particular, [8] introduced receipt freeness as a required property for avoiding coercion in e-voting systems. It was later extended in [52] by considering different levels of voter-control for the coercers, and different levels of collusion between coercer and other parties in the election, and further in [55]. [35] introduced coercion resistance as the property of being receipt free, plus resisting against randomization, forced abstention and simulation attacks. Moreover, significant progress has been made in the development of coercion-resistant voting systems, especially in combination with various forms of vote verifiability [60,13], cf. for instance [12,61,63,62].

Formal definitions of vote privacy, and receipt freeness and coercion resistance in various process calculi were proposed and discussed in [17,15,16,53,5,45,18] introduced a simulation based definition for coercion resistance, see also [51] for a survey. Several works such as [48,46,1,47,40,69,4,64] have developed weaker, more practical, or more efficient ways to realize the assumptions for achieving of receipt freeness and coercion resistance (without introducing new definitions).

Specification of voting properties in modal logics of time, knowledge, and/or strategies. [34,6,44] have used epistemic logic to express the property of coercion resistance in elections. More sophisticated formalisations, based on temporal or temporal-epistemic specifications, were used in [50,10,71], combined with verification through automated theorem proving, and in [9] together with verification by model checking. Formalizations in strategic-epistemic logic were proposed in [68,27,30,31,43,36,29], often with experimental verification of integrity and security requirements for a given voting protocol.

In a related line of work, modal logics of strategies, time, and knowledge were used to specify correctness of contract signing and non-repudiation protocols [38,39,11,28].

6 Conclusions

We have introduced the notion of forced participation attacks and defined formally forced participation resistance and forced abstention resistance, along with public participation privacy.

We highlight the internal strain between the first two properties by demonstrating several protocols which satisfy resistance to forced abstention but not to forced participation or vice versa.

Acknowledgments. This research has been supported by NCBR Poland and FNR Luxembourg under the PolLux/FNR-CORE project SpaceVote (POLLUX-XI/14/SpaceVote/2023 and C22/IS/17232062/ SpaceVote) and the FNR-CORE project PABLO (C21/IS/16326754/PABLO). For the purpose of open access, and in fulfilment of the obligations arising from the grant agreement, the authors have applied CC BY 4.0 license to any Author Accepted Manuscript version arising from this submission.

References

1. Aditya, R., Lee, B., Boyd, C., Dawson, E.: An efficient mixnet-based voting scheme providing receipt-freeness. In: Trust and Privacy in Digital Business, pp. 152–161. Springer (2004)
2. Alur, R., Henzinger, T.A., Kupferman, O.: Alternating-time Temporal Logic. In: Proceedings of the 38th Annual Symposium on Foundations of Computer Science (FOCS). pp. 100–109. IEEE Computer Society Press (1997)
3. Alur, R., Henzinger, T.A., Kupferman, O.: Alternating-time Temporal Logic. Journal of the ACM **49**, 672–713 (2002). https://doi.org/10.1145/585265.585270

4. Ara jo, R., Rajeb, N., Robbana, R., Traor , J., Youssfi, S.: Towards practical and secure coercion-resistant electronic elections. In: Heng, S.H., Wright, R., Goi, B.M. (eds.) Cryptology and Network Security, Lecture Notes in Computer Science, vol. 6467, pp. 278–297. Springer Berlin Heidelberg (2010)
5. Backes, M., Hritcu, C., Maffei, M.: Automated verification of remote electronic voting protocols in the applied pi-calculus. In: Computer Security Foundations Symposium, 2008. CSF'08. IEEE 21st. pp. 195–209. IEEE (2008)
6. Baskar, A., Ramanujam, R., Suresh, S.: Knowledge-based modelling of voting protocols. In: Proceedings of the 11th conference on Theoretical aspects of rationality and knowledge. pp. 62–71. ACM (2007)
7. BBC News: Tsvangirai rejects 'sham' ballot (2008), http://news.bbc.co.uk/2/hi/africa/7478399.stm
8. Benaloh, J., Tuinstra, D.: Receipt-free secret-ballot elections. In: Proceedings of the twenty-sixth annual ACM symposium on Theory of Computing. pp. 544–553. ACM (1994)
9. Boureanu, I., Jones, A.V., Lomuscio, A.: Automatic verification of epistemic specifications under convergent equational theories. In: Proceedings of International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS). pp. 1141–1148 (2012)
10. Bruni, A., Drewsen, E., Schürmann, C.: Towards a mechanized proof of Selene receipt-freeness and vote-privacy. In: Proceedings of E-Vote-ID. Lecture Notes in Computer Science, vol. 10615, pp. 110–126. Springer (2017). https://doi.org/10.1007/978-3-319-68687-5_7
11. Chadha, R., Kremer, S., Scedrov, A.: Formal analysis of multiparty contract signing. Journal of Automated Reasoning **36**(1-2), 39–83 (2006)
12. Chaum, D., Ryan, P.Y.A., Schneider, S.A.: A practical voter-verifiable election scheme. In: Proceedings of ESORICS. pp. 118–139 (2005). https://doi.org/10.1007/11555827_8
13. Cortier, V., Galindo, D., Küsters, R., Müller, J., Truderung, T.: SoK: Verifiability notions for e-voting protocols. In: IEEE Symposium on Security and Privacy. pp. 779–798 (2016). https://doi.org/10.1109/SP.2016.52
14. Cortier, V., Gaudry, P., Yang, Q.: Is the jcj voting system really coercion-resistant? Cryptology ePrint Archive (2022)
15. Delaune, S., Kremer, S., Ryan, M.: Coercion-resistance and receipt-freeness in electronic voting. In: Computer Security Foundations Workshop, 2006. 19th IEEE. pp. 12–pp. IEEE (2006)
16. Delaune, S., Kremer, S., Ryan, M.: Verifying privacy-type properties of electronic voting protocols: A taster. In: Towards Trustworthy Elections, pp. 289–309. Springer (2010)
17. Delaune, S., Kremer, S., Ryan, M.D.: Receipt-freeness: Formal definition and fault attacks. In: Proceedings of the Workshop Frontiers in Electronic Elections (FEE 2005), Milan, Italy. Citeseer (2005)
18. Dreier, J., Lafourcade, P., Lakhnech, Y.: A formal taxonomy of privacy in voting protocols. In: Communications (ICC), 2012 IEEE International Conference on. pp. 6710–6715. IEEE (2012)
19. Emerson, E.: Temporal and modal logic. In: van Leeuwen, J. (ed.) Handbook of Theoretical Computer Science, vol. B, pp. 995–1072. Elsevier (1990)
20. Estaji, E., Haines, T., Gjøsteen, K., Rønne, P.B., Ryan, P.Y., Soroush, N.: Revisiting practical and usable coercion-resistant remote e-voting. In: Electronic Voting: 5th International Joint Conference, E-Vote-ID 2020, Bregenz, Austria, October 6–9, 2020, Proceedings 5. pp. 50–66. Springer (2020)

21. Ferree, K.E., Jung, D.F., Dowd, R.A., Gibson, C.C.: Election ink and turnout in a partial democracy. British Journal of Political Science **50**(3), 1175–1191 (2020)
22. Gerhard, A.S.H., Atic, M., Letic, P., Erben, P.: Indelible Ink in Elections. White paper, IFES (2009), available at: https://web.archive.org/web/20191108205514/https://www.ifes.org/sites/default/files/ifes_gerhard_atic_letic_erben_white_paper_indelible_ink_in_elections_may_2019.pdf
23. Giustolisi, R., Garjan, M.S., Schuermann, C.: Thwarting last-minute voter coercion. Cryptology ePrint Archive (2023)
24. Żaneta Gotowalska-Wróblewska: Jak nie brać udziału w referendum? [how not to take part in the referendum?] (2023), https://wiadomosci.wp.pl/nie-chcesz-wziac-udzialu-w-referendum-oto-co-powinienes-zrobic-6950661018536768a
25. van der Hoek, W., Wooldridge, M.: Cooperation, knowledge and time: Alternating-time Temporal Epistemic Logic and its applications. Studia Logica **75**(1), 125–157 (2003)
26. Horbaczewski, R.: Sąd najwyższy odpowiedział, czy będzie osobny spis wyborców na referendu (2023), https://www.prawo.pl/samorzad/odnotowanie-niepobrania-karty-referendalnej-przez-komisje,523420.html
27. Jamroga, W., Knapik, M., Kurpiewski, D.: Model checking the SELENE e-voting protocol in multi-agent logics. In: Proceedings of the 3rd International Joint Conference on Electronic Voting (E-VOTE-ID). Lecture Notes in Computer Science, vol. 11143, pp. 100–116. Springer (2018)
28. Jamroga, W., Mauw, S., Melissen, M.: Fairness in non-repudiation protocols. In: Proceedings of STM'11. Lecture Notes in Computer Science, vol. 7170, pp. 122–139 (2012)
29. Jamroga, W., Kim, Y.: Practical model reductions for verification of multi-agent systems. In: Proceedings of the Thirty-Second International Joint Conference on Artificial Intelligence, IJCAI. pp. 7135–7139. ijcai.org (2023). https://doi.org/10.24963/IJCAI.2023/834
30. Jamroga, W., Kim, Y., Kurpiewski, D., Ryan, P.Y.A.: Towards model checking of voting protocols in uppaal. In: Proceedings of E-Vote-ID. Lecture Notes in Computer Science, vol. 12455, pp. 129–146. Springer (2020). https://doi.org/10.1007/978-3-030-60347-2_9
31. Jamroga, W., Kurpiewski, D., Malvone, V.: Natural strategic abilities in voting protocols. In: Proceedings of STAST 2020 (2021), to appear
32. Jaros, J.: Wieś boi się bojkotu referendum. To będzie tajemnica poliszynela [The countryside is afraid to boycott the referendum. It will be an open secret] (2023), https://kalisz.wyborcza.pl/kalisz/7,181359,30197487,tajemnica-wyborcza-fikcja-podczas-referendum-kobiety-o-przedwyborczych.html
33. Jha, P.S.: What a Tiny Spot of Ink Can Mean. World Press Review **49**(12) (2002), available at: https://www.worldpress.org/Asia/801.cfm
34. Jonker, H.L., Pieters, W.: Receipt-freeness as a special case of anonymity in epistemic logic (2006)
35. Juels, A., Catalano, D., Jakobsson, M.: Coercion-resistant electronic elections. In: Proceedings of the 2005 ACM workshop on Privacy in the electronic society. pp. 61–70. ACM (2005)
36. Kim, Y., Jamroga, W., Ryan, P.Y.: Verification of the socio-technical aspects of voting: The case of the Polish postal vote 2020. In: Proceedings of STAST (2022), to appear, available at https://arxiv.org/abs/2210.10694
37. King, L.: Taliban cut off Afghan voters' ink-stained fingers, election observers say. Los Angeles Times (2009), https://www.latimes.com/archives/la-xpm-2009-aug-23-fg-afghan-election23-story.html

38. Kremer, S., Raskin, J.: Game analysis of abuse-free contract signing. In: Proceedings of the 15th IEEE Computer Security Foundations Workshop (CSFW'02). pp. 206–220. IEEE Computer Society Press (2002). https://doi.org/10.1109/CSFW.2002.1021817
39. Kremer, S., Raskin, J.F.: A game-based verification of non-repudiation and fair exchange protocols. Journal of Computer Security **11**(3) (2003). https://doi.org/10.1007/3-540-44685-0_37
40. Ku, W.C., Ho, C.M.: An e-voting scheme against bribe and coercion. In: e-Technology, e-Commerce and e-Service, 2004. EEE'04. 2004 IEEE International Conference on. pp. 113–116. IEEE (2004)
41. Kulyk, O., Teague, V., Volkamer, M.: Extending helios towards private eligibility verifiability. In: E-Voting and Identity: 5th International Conference, VoteID 2015, Bern, Switzerland, September 2-4, 2015, Proceedings 5. pp. 57–73. Springer (2015)
42. Kumar, R.K.: The business of 'black-marking' voters. The Hindu (2004), available at: https://web.archive.org/web/20040412223708/http://www.hindu.com/2004/03/17/stories/2004031700571300.htm
43. Kurpiewski, D., Jamroga, W., Masko, L., Mikulski, L., Pazderski, W., Penczek, W., Sidoruk, T.: Verification of multi-agent properties in electronic voting: A case study. In: Advances in Modal Logic. pp. 531–556. College Publications (2022)
44. Kusters, R., Truderung, T.: An epistemic approach to coercion-resistance for electronic voting protocols. In: Security and Privacy, 2009 30th IEEE Symposium on. pp. 251–266. IEEE (2009)
45. Küsters, R., Truderung, T., Vogt, A.: A game-based definition of coercion-resistance and its applications. In: Proceedings of the 2010 23rd IEEE Computer Security Foundations Symposium. pp. 122–136. IEEE Computer Society (2010)
46. Lee, B., Kim, K.: Receipt-free electronic voting scheme with a tamper-resistant randomizer. In: Information Security and Cryptology-ICISC 2002, pp. 389–406. Springer (2003)
47. Lee, B., Boyd, C., Dawson, E., Kim, K., Yang, J., Yoo, S.: Providing receipt-freeness in mixnet-based voting protocols. In: Information Security and Cryptology-ICISC 2003, pp. 245–258. Springer (2004)
48. Magkos, E., Burmester, M., Chrissikopoulos, V.: Receipt-freeness in large-scale elections without untappable channels. In: Towards The E-Society, pp. 683–693. Springer (2001)
49. Mascol Technologies: Invisible election ink, https://www.election-ink.co.uk/
50. Meier, S., Schmidt, B., Cremers, C., Basin, D.: The TAMARIN prover for the symbolic analysis of security protocols. In: Computer Aided Verification, Proceedings of CAV. Lecture Notes in Computer Science, vol. 8044, pp. 696–701. Springer (2013). https://doi.org/10.1007/978-3-642-39799-8_48
51. Meng, B.: A critical review of receipt-freeness and coercion-resistance. Information Technology Journal **8**(7), 934–964 (2009)
52. Michels, M., Horster, P.: Some remarks on a receipt-free and universally verifiable mix-type voting scheme. In: Advances in Cryptology-ASIACRYPT'96. pp. 125–132. Springer (1996)
53. Moran, T., Naor, M.: Receipt-free universally-verifiable voting with everlasting privacy. In: Advances in Cryptology-CRYPTO 2006. pp. 373–392. Springer (2006)
54. Notes from Poland: Exit poll: Polish government's referendum invalidated by low turnout (2023), https://notesfrompoland.com/2023/10/15/exit-poll-polish-governments-referendum-invalidated-by-low-turnout/
55. Okamoto, T.: Receipt-free electronic voting schemes for large scale elections. In: Security Protocols. pp. 25–35. Springer (1998)

56. Państwowa Komisja Wyborcza [National Electoral Commission]: Obwieszczenie państwowej komisji wyborczej z dnia 17 października 2023 r. o wynikach głosowania i wyniku referendum przeprowadzonego w dniu 15 października 2023 r. (2023), https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19970780483
57. Państwowa Komisja Wyborcza [National Electoral Commission]: Turnout in 2023 elections for sejm (2023), https://wybory.gov.pl/sejmsenat2023/en/frekwencja/pl
58. Państwowa Komisja Wyborcza [National Electoral Commission]: Turnout in nationwide referendum 2023 (2023), https://referendum.gov.pl/referendum2023/en/frekwencja/pl
59. Państwowa Komisja Wyborcza [National Electoral Commission]: Uchwała nr 211/2023 pkw z dnia 25 września 2023 r. w sprawie wytycznych dla obwodowych komisji wyborczych dotyczących zadań i trybu przygotowania oraz przeprowadzenia głosowania w obwodach głosowania utworzonych w kraju w wyborach do sejmu rzeczypospolitej polskiej i do senatu rzeczypospolitej polskiej oraz w referendum ogólnokrajowym zarządzonych na dzień 15 października 2023 r. (2023), https://pkw.gov.pl/prawo-wyborcze/uchwaly-pkw/2023-r/uchwala-nr-2112023-pkw-z-dnia-25-wrzesnia-2023-r-w-sprawie-wytycznych-dla-obwodowych-komisji-wyborcz
60. Ryan, P.Y.A., Schneider, S.A., Teague, V.: End-to-end verifiability in voting systems, from theory to practice. IEEE Security & Privacy **13**(3), 59–62 (2015). https://doi.org/10.1109/MSP.2015.54
61. Ryan, P.: The computer ate my vote. In: Formal Methods: State of the Art and New Directions, pp. 147–184. Springer (2010)
62. Ryan, P., Rønne, P., Iovino, V.: Selene: Voting with transparent verifiability and coercion-mitigation. In: Financial Cryptography and Data Security: Proceedings of FC 2016. Revised Selected Papers. Lecture Notes in Computer Science, vol. 9604, pp. 176–192. Springer (2016). https://doi.org/10.1007/978-3-662-53357-4_12
63. Ryan, P., Teague, V.: Pretty good democracy. In: Security Protocols XVII, Lecture Notes in Computer Science, vol. 7028, pp. 111–130. Springer Berlin Heidelberg (2013)
64. Schlapfer, M., Haenni, R., Koenig, R., Spycher, O.: Efficient vote authorization in coercion-resistant internet voting. In: E-Voting and Identity: Third International Conference, VoteID 2011, Tallinn, Estonia, September 28-20, 2011, Revised Selected Papers. vol. 7187, p. 71. Springer (2012)
65. Schobbens, P.Y.: Alternating-time logic with imperfect recall. Electronic Notes in Theoretical Computer Science **85**(2), 82–93 (2004)
66. Sejm Rzeczypospolitej Polskiej [Parliament of the Republic of Poland]: Uchwała sejmu rzeczypospolitej polskiej z dnia 17 sierpnia 2023 r. o zarządzeniu referendum ogólnokrajowego w sprawach o szczególnym znaczeniu dla państwa (2023), https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20230001636/O/D20231636.pdf
67. Sitnicka, D.: Najważniejsze są wybory, referendum jest drugorzędne. podpowiadamy, jak je bezpiecznie zbojkotować (2023), https://oko.press/referendum-bojkot-glosowanie
68. Tabatabaei, M., Jamroga, W., Ryan, P.Y.A.: Expressing receipt-freeness and coercion-resistance in logics of strategic ability: Preliminary attempt. In: Proceedings of the 1st International Workshop on AI for Privacy and Security, PrAISe@ECAI 2016. pp. 1:1–1:8. ACM (2016). https://doi.org/10.1145/2970030.2970039
69. Weber, S.G., Araujo, R., Buchmann, J.: On coercion-resistant electronic elections with linear work. In: Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on. pp. 908–916. IEEE (2007)

70. Wong, R.: Ink washout. The Star (2008), available at: https://web.archive.org/web/20080430202643/http://www.thestar.com.my/election/story.asp?file=%2F2008%2F3%2F5%2Felection2008%2F20540844&sec=Election2008&focus=1
71. Zollinger, M., Roenne, P., Ryan, P.: Mechanized proofs of verifiability and privacy in a paper-based e-voting scheme. In: Proceedings of 5th Workshop on Advances in Secure Electronic Voting (2020)