Expressing Receipt-Freeness and Coercion-Resistance in Logics of Strategic Ability: Preliminary Attempt

Masoud Tabatabaei
Interdisciplinary Centre for Security, Reliability and Trust
University of Luxembourg
masoud.tabatabaei@uni.lu

Wojciech Jamroga
Institute of Computer Science
Polish Academy of Sciences
w.jamroga@ipipan.waw.pl

Peter Y. A. Ryan
Interdisciplinary Centre for Security, Reliability and Trust
University of Luxembourg
peter.ryan@uni.lu

ABSTRACT

Voting is a mechanism of utmost importance to social processes. In this paper, we focus on the strategic aspect of information security in voting procedures. We argue that the notions of receipt-freeness and coercion resistance are underpinned by existence (or nonexistence) of a suitable strategy for some participants of the voting process. In order to back the argument formally, we provide logical "transcriptions" of the informal intuitions behind coercion-related properties that can be found in the existing literature. The transcriptions are formulated in the modal game logic **ATL***, well known in the area of multi-agent systems.

CCS Concepts

•**Security and privacy** → *Logic and verification;* Privacy-preserving protocols; Privacy protections; •**Theory of computation** → *Modal and temporal logics;* •**Applied computing** → Voting / election technologies;

Keywords

receipt freeness, coercion resistance

1. INTRODUCTION

Voting is a mechanism of utmost importance to social processes, as many important decisions for the society are made by means of elections and referenda. Digital technology holds out the promise of greater citizen engagement in decision making. Throughout the history of democracy elections have been the target of attempts to manipulate the outcome. In order to counter threats of coercion or vote buying, *ballot confidentiality* was recognised an important property of voting systems. More recently, cryptographers and security experts have been looking at using cryptographic mechanisms to provide *voter-verifiability*, i.e., the ability of voters to confirm that their votes are correctly registered and counted. Voter-verifiability strengthens the integrity of the voting procedure, but, if it is not done carefully, it can introduce new threats to confidentiality. This leads to the introduction of more sophisticated notions: *receipt-freeness* and *coercion-resistance*. Receipt-freeness focuses on the resources needed to construct a coercion attack, and requires that the voter can obtain no certified information (a receipt) which could be used to prove to a coercer that she voted in a certain way. Coercion-resistance, on the other hand, is intended to capture broader security concerns, guided by the following intuition: whatever strategy the coercer adopts, the voter always has a strategy to vote as they intend while appearing to comply with all the coercer's requirements.

In this paper, we focus on the strategic aspect of information security in voting procedures. We argue that coercion-related properties are underpinned by existence (or nonexistence) of a suitable strategy for some participants: typically for the voter, the coercer, or both. Such strategic behaviour has been studied in game theory, social choice theory, and theory of multi-agent systems. In particular, a number of *game logics* have been proposed that can be used to specify properties related to strategic ability. Here, we use formulae of the game logic **ATL*** to encode and disambiguate different flavours of receipt-freeness and coercion resistance.

In the existing literature, coercion-related properties are typically formulated on two levels of abstraction. On one hand, the *informal intuition* usually builds upon abilities of participants in the interaction between the voter and the potential coercer. That is, it refers to the existence or nonexistence of suitable strategies for players in the *real* game between the voter and the coercer.

On the other hand, the *formal definition* specifies a mathematical structure to which the property is related, and defines how to evaluate the property based on the structure. Some of the formal definitions are game-based, but the games used there are primarily mathematical devices to define the concept, much like in case of the game semantics for first-order predicate logic, or the game semantics of programming languages. It is *not* the real game between participants of the voting process, but rather an abstract game between the "verifier" trying to prove the property true, and the "falsifier" that attempts the opposite. Thus, strategy-based definitions of coercion resistance and receipt-freeness are either informal, or use strategies that have no obvious relation to the real behavior of actual participants in the voting process. The closest work we know of, that has formalized the coercion resistance property as strategic abilities of the participants, is the the work of Kusters et al. [34]. They have formalized the property as a quantitative measure showing how well a coercer can distinguish between

PrAISe '16, August 29 - 30, 2016, The Hague, Netherlands

ISBN 978-1-4503-4304-6/16/08...$15.00

DOI: http://dx.doi.org/10.1145/2970030.2970039

the strategy he has prescribed to the coerced voter, and a counter-strategy used by the voter. However for formalizing the property they have also used a cryptographic model, rather than a model oriented for specifying strategic abilities of players.

The aim of this paper is to provide logical "transcriptions" of the informal intuitions that can be found in the literature. The work is still very preliminary. Nevertheless, the transcriptions formally expose the strategic nature of coercion-related properties, and allow to demonstrate some differences between the existing approaches.

2. RELATED WORK

The related work can be divided into two strands. On one hand, the concepts of receipt-freeness and coercion resistance have been defined and discussed in multiple variants. On the other hand, some authors have attempted to capture several security properties in modal logics of time, knowledge, and/or strategies. We briefly discuss both strands below.

Receipt-freeness and coercion resistance. In 1994, Benolah and Tuinstra [9] introduced receipt freeness as a required property for avoiding coercion in e-voting systems. Later Michels et al. [40] extended the concept by considering different levels of voter-control for the coercers, and different levels of collusion between coercer and other parties in the election. Okamoto and Tatsuaki [45] developed the formal definition of [9] to make it more appropriate for large scale elections. In 2005, Juels et al. [29] introduced coercion resistance as the property of being receipt freeness, plus resisting against randomization, forced abstention and simulation attacks.

Delaune et al. have a series of works [21, 19, 20] in which they have formalized receipt freeness and coercion resistance properties in applied pi calculus. Moran and Naor [44] introduced a simulation based definition for coercion resistance. Backes et al. [6] introduced a definition of coercion resistance in symbolic model which was more suitable for automation than previous works. Meng [39] provided a state of the art survey on the definitions of receipt-freeness and coercion-resistance and on what technologies are used at the time to implement these property in voting schemes.

Kuesters et al. [34] introduced a formalisation of coercion resistance which could provide a probabilistic measure of the amount of coercion resistance in a voting scheme. Dreier et al. [22] provided formal definitions of various privacy notions in applied pi calculus, and showed how they are related to each other.

Several works such as [38, 36, 1, 35, 32, 51, 5, 48], without introducing new definitions of receipt freeness and coercion resistance properties, have developed weaker, more practical, or more efficient ways to realize the needed assumptions for achieving these properties (assumptions such as existence of untappable channels, anonymous channels, etc.).

Also some works, such as [28, 7, 33] have used formal logic to express coercion resistance property in elections. Junker and Pieters [28] and Baskar et al. [7] defined the receipt freeness property in terms of knowledge of the agents. Also Kusters and Truderung [33] used an epistemic approach for defining the coercion resistance property in elections. The main difference between our approach and these works is that neither of them have incorporated strategic abilities of the participants as a parameter in defining the security properties.

Specification of security in modal logics of time, knowledge, and/or strategies. There has been some research on specification of security properties in combinations of temporal, epistemic, and strategic logics, especially in the context of model checking. Temporal-epistemic logic **CTLK**, together with the modeling methodology of *interpreted systems*, has been used to specify and verify properties of cryptographic protocols, including authentication protocols [37, 10], and authentication as well as key-establishment protocols [13]. **CTLK** was also used to disambiguate and construct a taxonomy of specifications for detectability of attacks on information security [11].

An extension of **CTLK** with reasoning modulo *equational theories* was used in [12] to construct and verify multi-agent models of electronic voting protocols automatically extracted from high-level descriptions. The following properties were considered: vote privacy, voter-vote unlinkability, receipt-freeness, and coercion-resistance. Thus, the agenda of [12] comes very close to what we address in this paper. However, their specifications of the security properties are completely different from ours – in particular, they leave the strategic aspects implicit and buried deep in the detailed structure of their models.

Modal logics with explicit modalities for strategic play have been, to the best of our knowledge, only used to specify and verify correctness of contract signing protocols [30], to specify and analysis of multiparty contract-signing protocols [16], and specify a taxonomy of security properties for non-repudiation and fair exchange protocols [31, 26].

3. LOGICS OF STRATEGIC ABILITY

The idea behind this paper is to capture the intuitive meaning of coercion-related properties by formal specifications that explicitly refer to the strategic interaction between the voter(s) and the coercer(s). We will show a number of logical formulae that refer to the existence (or nonexistence) of strategies to coerce (resp. to defend from coercion). To this end, we will use *modal logics of strategic ability*, or *modal game logics* [8, 4, 50, 17, 43], that have gained much popularity within Artificial Intelligence in the last 20 years.

There are many syntactic and semantic variants of game logics. In this paper, we use *alternating-time temporal logic* **ATL** whose formulae allow for expressing statements about the existence of a surely winning strategy to achieve a given temporal goal.

3.1 What Agents Can Achieve: ATL and ATL*

Alternating-time temporal logic [3, 4] generalizes branching-time temporal logic **CTL*** [23] by replacing path quantifiers E, A with *strategic modalities* $\langle\langle A\rangle\rangle$. Informally, $\langle\langle A\rangle\rangle\gamma$ says that a group of agents A has a collective strategy to enforce temporal property γ. **ATL*** formulas can include temporal operators: "X" ("in the next state"), "G" ("always from now on"), "F" ("now or sometime in the future"), and U (strong "until"). Similarly to **CTL*** and **CTL**, we consider two syntactic variants of the alternating-time logic, namely **ATL*** and **ATL**.

Syntax. Formally, let $\mathbb{A}\mathrm{gt}$ be a finite set of agents, and PV a countable set of atomic propositions. The language of **ATL*** is defined as follows:

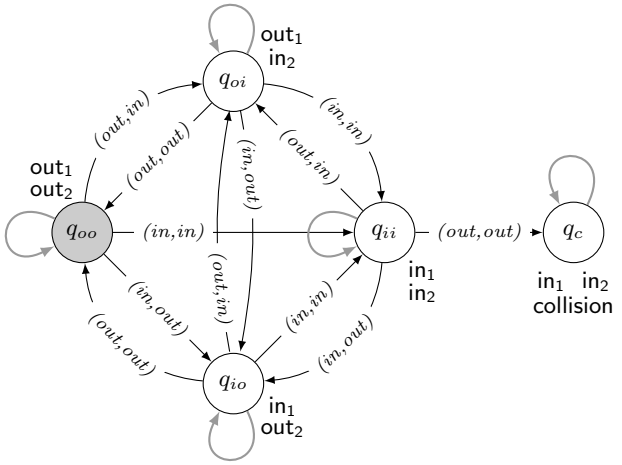

Figure 1: Autonomous vehicles at the intersection: model M_1

$$\varphi ::= \mathsf{p} \mid \neg\varphi \mid \varphi \wedge \varphi \mid \langle\langle A\rangle\rangle\gamma,$$
$$\gamma ::= \varphi \mid \neg\gamma \mid \gamma \wedge \gamma \mid \mathrm{X}\gamma \mid \gamma\,\mathrm{U}\,\gamma.$$

where $A \subseteq \mathbb{A}\mathrm{gt}$ and $\mathsf{p} \in PV$. Derived boolean connectives and constants $(\vee, \top, \bot)$ are defined as usual. "Sometime", "weak until", and "always from now on" are defined as $\mathrm{F}\gamma \equiv \top\,\mathrm{U}\,\gamma$, $\gamma_1\,\mathrm{W}\,\gamma_2 \equiv \neg((\neg\gamma_2)\,\mathrm{U}\,(\neg\gamma_1 \wedge \neg\gamma_2))$, and $\mathrm{G}\gamma \equiv \gamma\,\mathrm{W}\,\bot$.

ATL (without "star") is the syntactic variant in which strategic and temporal operators are combined into compound modalities:

$$\varphi ::= \mathsf{p} \mid \neg\varphi \mid \varphi \wedge \varphi \mid \langle\langle A\rangle\rangle\mathrm{X}\varphi \mid \langle\langle A\rangle\rangle\varphi\,\mathrm{U}\,\varphi \mid \langle\langle A\rangle\rangle\varphi\,\mathrm{W}\,\varphi.$$

Models. The semantics of **ATL*** is defined over a variant of synchronous multi-agent transition systems.

Definition 3.1 (CGS). *A* concurrent game structure (CGS) *is a tuple $M = \langle \mathbb{A}\mathrm{gt}, St, Act, d, o, PV, V\rangle$ which includes nonempty finite sets of: agents $\mathbb{A}\mathrm{gt} = \{1, \ldots, k\}$, states St, actions Act, atomic propositions PV, and a propositional valuation $V : St \to 2^{PV}$. The function $d : \mathbb{A}\mathrm{gt} \times St \to 2^{Act}$ defines availability of actions. The (deterministic) transition function o assigns a successor state $q' = o(q, \alpha_1, \ldots, \alpha_k)$ to each state $q \in St$ and any tuple of actions $\alpha_i \in d(i, q)$ that can be executed by $\mathbb{A}\mathrm{gt}$ in q.*

A pointed CGS *is a pair (M, q_0) consisting of a concurrent game structure M and an initial state q_0 in M.*

Example 3.1 (Driving agents). *Consider an intersection with two autonomous vehicles around it. Each vehicle i is modeled as a separate agent, whose local state is characterized by either the proposition* out_i *(when the vehicle is outside the intersection) or* in_i *(when the vehicle is inside it). The available actions are: in ("drive in" or "stay in", depending on the current state) and out ("drive out" or "stay out"). Transitions update the state accordingly, except for one case: when both agents are in and decide to leave at the same time, a collision occurs (*$\mathsf{collision}$*).*

Figure 1 presents a pointed CGS modeling this scenario. The combinations of actions that are not displayed in the graph do not change the state of the system.

Strategies and their outcomes. Given a CGS, we define the strategies and their outcomes as follows. A *strategy* for a is a function $s_a : St \to Act$ such that $s_a(q) \in d(a, q)$.[1] The set of such strategies is sometimes denoted by Σ_a^{Ir}, with the capital "I" referring to perfect **I**nformation, and the lowercase "r" for possibly imperfect **r**ecall. A *collective strategy* for a group of agents $A = \{a_1, \ldots, a_r\}$ is a tuple of individual strategies $s_A = \langle s_{a_1}, \ldots, s_{a_r}\rangle$. The set of such strategies is denoted by Σ_A^{Ir}.

A *path* $\lambda = q_0 q_1 q_2 \ldots$ in a CGS is an infinite sequence of states such that there is a transition between each q_i, q_{i+1}. $\lambda[i]$ denotes the ith position on λ (starting from $i = 0$) and $\lambda[i, \infty]$ the suffix of λ starting with i. The "outcome" function $out(q, s_A)$ returns the set of all paths that can occur when agents A execute strategy s_A from state q onward. Function $out(q, s_A)$ returns the set of all paths $\lambda \in St^\omega$ that may occur when agents A execute strategy s_A from state q onward, defined as follows:

$out(q, s_A) = \{\lambda = q_0, q_1, q_2 \ldots \mid q_0 = q$ and for each $i = 0, 1, \ldots$ there exists $\langle \alpha^i_{a_1}, \ldots, \alpha^i_{a_k}\rangle$ such that $\alpha^i_a \in d_a(q_i)$ for every $a \in \mathbb{A}\mathrm{gt}$, and $\alpha^i_a = s_A[a](q_i)$ for every $a \in A$, and $q_{i+1} = o(q_i, \alpha^i_{a_1}, \ldots, \alpha^i_{a_k})\}$.

Semantics. The semantics of **ATL*** is defined by the following clauses:

$M, q \models \mathsf{p}$ iff $q \in V(\mathsf{p})$, for $\mathsf{p} \in PV$;

$M, q \models \neg\varphi$ iff $M, q \not\models \varphi$;

$M, q \models \varphi_1 \wedge \varphi_2$ iff $M, q \models \varphi_1$ and $M, q \models \varphi_2$;

$M, q \models \langle\langle A\rangle\rangle\gamma$ iff there is a strategy $s_A \in \Sigma_A^{\mathrm{Ir}}$ such that, for each path $\lambda \in out(q, s_A)$, we have $M, \lambda \models \gamma$.

$M, \lambda \models \varphi$ iff $M, \lambda[0] \models \varphi$;

$M, \lambda \models \neg\gamma$ iff $M, \lambda \not\models \gamma$;

$M, \lambda \models \gamma_1 \wedge \gamma_2$ iff $M, \lambda \models \gamma_1$ and $M, \lambda \models \gamma_2$;

$M, \lambda \models \mathrm{X}\gamma$ iff $M, \lambda[1, \infty] \models \gamma$; and

$M, \lambda \models \gamma_1\,\mathrm{U}\,\gamma_2$ iff there is an $i \in \mathbb{N}_0$ such that $M, \lambda[i, \infty] \models \gamma_2$ and $M, \lambda[j, \infty] \models \gamma_1$ for all $0 \le j < i$.

Example 3.2 (Driving agents, ctd.). *For model M_1, we have $M_1, q_{oo} \models \langle\langle 1\rangle\rangle\mathrm{G}\neg\mathsf{collision}$: agent 1 can avoid the collision forever (the obvious strategy is to never enter the crossroads). On the other hand, the agent cannot ensure the collision even if it wants to: $M_1, q_{oo} \models \neg\langle\langle 1\rangle\rangle\mathrm{F}\mathsf{collision}$. This can only be guaranteed if the agents cooperate: $M_1, q_{oo} \models \langle\langle 1, 2\rangle\rangle\mathrm{F}\mathsf{collision}$. Moreover, $M_1, q_{oo} \models \langle\langle 1\rangle\rangle\mathrm{F}\mathsf{in}_1 \wedge \langle\langle 2\rangle\rangle\mathrm{F}\mathsf{in}_2$: each agent is able to enter the intersection. Still, it cannot successfully drive through the crossroads on its own (e.g., $M_1, q_{oo} \not\models \langle\langle 1\rangle\rangle\mathrm{F}(\mathsf{in}_1 \wedge \mathsf{out}_1)$). Finally, if the agents cooperate, they can make sure that they successfully drive through the crossroads: $M_1, q_{oo} \models \langle\langle 1, 2\rangle\rangle\mathrm{F}(\mathsf{in}_1 \wedge \mathrm{F}\mathsf{out}_1)$.*

3.2 Abilities under Imperfect Information

ATL* was originally proposed for reasoning about agents in perfect information scenarios. However, realistic multi-agent interaction always includes some degree of limited observability [50, 27, 2, 24, 25, 49]. Here, we use the classical

[1] This corresponds to the notion of *memoryless* or *positional* strategies. In other words, we assume that the memory of agents is explicitly defined by the states of the model.

variant of "**ATL*** with imperfect information" from [50], defined as follows.

First, we extend concurrent game structures with indistinguishability relations $\sim_1, \ldots, \sim_k$, one per agent in $\mathbb{A}$gt. Now, strategies must specify identical choices in indistinguishable situations. That is, strategies with imperfect information (ir strategies, for short) are functions $s_a : St \to Act$ such that (1) $s_a(q) \in d(a,q)$, and (2) if $q \sim_a q'$ then $s_a(q) = s_a(q')$.[2] As before, collective strategies for $A \subseteq \mathbb{A}$gt are tuples of individual strategies for $a \in A$. We denote the set of A's imperfect information strategies by Σ_A^{ir}.

The semantics of "**ATL*** with imperfect information" differs from the one presented in Section 3.1 only in the clause for strategic modality:

$M, q \models \langle\langle A\rangle\rangle\gamma$ iff there is a strategy $s_A \in \Sigma_A^{\mathrm{ir}}$ such that, for every agent $a \in A$, state q' such that $q \sim_a q'$, and path $\lambda \in out(q', s_A)$, we have that $M, \lambda \models \gamma$.

In other words, the agents in A should have an executable strategy which enforces γ from all the states that at least one member of the coalition considers possible.

Example 3.3 (Intersection with limited visibility). *Take model M_1 from Example 3.1, and assume that no agent sees the location of the other vehicle. This can be modeled by the following indistinguishability relations: $q_{oo} \sim_1 q_{oi}$ and $q_{ii} \sim_1 q_{io}$; $q_{oo} \sim_2 q_{io}$ and $q_{oi} \sim_2 q_{ii}$. Now, we still have e.g. that $M_2, q_{oo} \models \langle\langle 1\rangle\rangle \mathrm{G}\neg\mathsf{collision}$ (it suffices that agent 1 executes action "out" regardless of anything) On the other hand, $M_2, q_{oo} \models \neg\langle\langle 1,2\rangle\rangle \mathrm{F}\mathsf{collision}$ (the agents cannot make sure that a collision will happen, even if they want to). We leave it up to the interested reader to check the latter.*

3.3 Knowledge and Belief Modalities

Coercion resistance and receipt-freeness are privacy-type properties. In this sense, they are related to the *knowledge* and/or *beliefs* of the adversary about a given secret. In case of elections, the secret is usually the value of the voter's vote. Thus, we will need modalities for knowledge (resp. beliefs). The former is formalized by epistemic formulae of type $K_a\varphi$, expressing that agent *a knows that φ holds*, with the following semantics:

$M, q \models K_a\varphi$ iff, for every state q' such that $q \sim_a q'$, we have that $M, q' \models \varphi$.

It is interesting to observe that this modality is in fact superfluous in "**ATL*** with imperfect information," since we can equivalently express $K_a\varphi$ by $\langle\langle a\rangle\rangle\varphi \,\mathrm{U}\, \varphi$.

The modality for beliefs is very similar. $B_a\varphi$ expresses that *a believes* that ϕ holds, and exactly the same semantic clause can be used to interpret $K_a\varphi$ and $B_a\varphi$. The difference lies in the axiomatic properties. For knowledge, the indistinguishability relation is assumed to be an equivalence (i.e., reflexive, symmetric, and transitive), whereas for beliefs it is sufficient to have it serial, symmetric and Euclidean. Thus, whenever the indistinguishability relation $\sim_a$ is an equivalence, one can use K_a to address the subjective view of player a; otherwise B_a should be used.

4. EXPRESSING INFORMAL DEFINITIONS OF COERCION-RELATED PROPERTIES

[2]Again, we consider only positional strategies here.

In order to express security properties of a voting system, we assume that the voting process is modeled as a concurrent game structure where the set of players $\mathbb{A}$gt includes the set of voters V, the coercer c, and possibly some other players. Let *Bal* be the set of possible "ballot values," i.e., ways in which a ballot can be cast by a voter. In a simple majority voting procedure where each voter votes for one of the candidates, *Bal* is the set of candidates. We assume that the states where voter $v \in V$ has already voted are labeled by the atomic proposition $\mathsf{voted}_{\mathsf{v},\mathsf{i}}$, where $i \in Bal$ indicates how v voted.

For this work, we have chosen several important papers on preventing coercion in elections. In each of the papers, an informal intuition is first given, and later followed by a formal definition that typically uses some heavy mathematical machinery. Here, we only look at the informal intuitions, in order to provide their transcriptions in the game logic **ATL***. To make the list easier to read, we label the properties to be transcribed as either **(RFx)** for variants of receipt freeness properties, and **(CRx)** for variants of coercion resistance.

4.1 Benaloh and Tuinstra (1994)

(RF1) For a voting system to be uncoercable, no voter should be able to convince any other participant of the value of its vote. [9]

This paper introduced the notion of receipt freeness. They showed with some examples why giving a "receipt" to the voter can be harmful, as it prevents the voter from being be able to deceive the coercer. Therefore through the paper "uncoercibility" is regarded equivalent to receipt freeness.

For expressing this definition, we need to interpret two terms *to convince'* and *other participants*. We can consider "other participants" to be the set of all voters, or to be the set of all players. The more subtle term to interpret is "to convince". It can both mean to prove to someone about one's vote value, and to make someone believe that the voter has voted in a particular way. In the first case the knowledge modality is the right one to use and in the second case the belief modality. However, because in this definition "being unable to convince" is used only for the actual vote of the voter, we decide to use knowledge modality for expressing the property. Therefore definition **(RF1)**, if we consider "other participants" to be the set of voters, can be expressed as:

$$\bigwedge_{\substack{v,v' \in V \setminus \{c\} \\ v \neq v'}} \bigwedge_{i \in Bal} \neg\langle\langle v\rangle\rangle \mathrm{F}(\mathsf{voted}_{\mathsf{v},\mathsf{i}} \wedge K_{v'}\mathsf{voted}_{\mathsf{v},\mathsf{i}}),$$

or if we consider "other participants" to be any other player in the model:

$$\bigwedge_{v \in V} \bigwedge_{\substack{a \in \mathbb{A}\mathrm{gt} \\ v \neq a}} \bigwedge_{i \in Bal} \neg\langle\langle v\rangle\rangle \mathrm{F}(\mathsf{voted}_{\mathsf{v},\mathsf{i}} \wedge K_a\mathsf{voted}_{\mathsf{v},\mathsf{i}}).$$

Note that $\bigwedge$ is not a first order quantifier but a conjunction of finitely many subformulae. Thus, the above specifications are propositional modal formulae of finite length.

4.2 Juels, Catalano, and Jakobsson (2005)

This paper introduced the notion of coercion resistance property as an improvement over receipt freeness. We start by the definition of receipt freeness as given in this work:

(RF2) Receipt-freeness is the inability of a voter to prove to an attacker that she voted in a particular manner, even if the voter wishes to do so. [29]

This definition is very similar to **(RF1)** The difference is that instead of any other player, we use a coercer player as the adversary. Although one might think the two interpretations imply each other, they can in fact have different nuances. One may define specific abilities for the adversaries in the model that are not different from those accessible to the voters, or other players in the system. Also one might consider some (maybe powerful) players in the model as trustworthy and decide not to include them in the set of coercers. The definition **(RF2)** then can be expressed as follows:

$$\bigwedge_{v\in V\setminus\{c\}} \bigwedge_{i\in Bal} \neg\langle\langle v\rangle\rangle \mathrm{F}(\mathsf{voted}_{\mathsf{v,i}} \wedge K_c \mathsf{voted}_{\mathsf{v,i}}).$$

The definition of the coercion resistance property given in this paper is meant to give extra protection, where receipt freeness fails to protect an election system against several forms of serious, real-world attack, specifically against randomization attacks, forced abstention attacks, and simulation attacks. In randomization attack the coercer asks the voter to use some randomization method for choosing her vote. In forced abstention attack the attacker wants the voter to avoid voting in the election, and in simulation attack the attacker himself simulate the role of the voter (for example by causing her to divulge her private keying material after the registration, but prior to the election process).

(CR1) A coercion-resistant voting system is one in which the user can deceive the adversary into thinking that she has behaved as instructed, when the voter has in fact cast a ballot according to her own intentions. [29]

This definition includes *instructions* of the coercer to the voter. The paper explains that this instructions can be voting for a specific candidate, but also abstaining from voting, randomizing the vote, and in general any specific behavior during the election process. Here, we focus only on instructing to vote for a specific candidate and abstaining from voting, and we discuss the other cases later. Notice that in this definition, the voter intends to deceive the adversary to accept the voter has voted in a way which is not the actual vote of the voter. This means that the knowledge modality cannot be used here, because in classical epistemic logic knowledge about a proposition implies the truth of it in all possible worlds. Hence we use belief modalities in this case. The - narrowly interpreted - expression of definition **(CR1)** then can be as follows:

$$\bigwedge_{v\in V\setminus\{c\}} \bigwedge_{i,j\in Bal} \langle\langle v\rangle\rangle \mathrm{F}(\mathsf{voted}_{\mathsf{v,i}} \wedge B_c \mathsf{voted}_{\mathsf{v,j}}).$$

4.3 Delaune, Kremer, and Ryan (2005)

(RF3) An election protocol is receipt-free if a voter A cannot prove to a potential coercer C that she voted in a particular way. We assume that A wishes to cooperate with C; receipt-freeness guarantees that such cooperation will not be worthwhile, because it will be impossible for C to obtain proof about how A voted. [21]

The paper proposed a formalization of receipt freeness in applied pi calculus. Here, unlike the previous definitions, a cooperation between the coercer and the voter has been mentioned explicitly. Expressing this definition can be as follows:

$$\bigwedge_{v\in V\setminus\{c\}} \bigwedge_{i\in Bal} \neg\langle\langle c, v\rangle\rangle \mathrm{F}(\mathsf{voted}_{\mathsf{v,i}} \wedge K_c \mathsf{voted}_{\mathsf{v,i}}).$$

4.4 Moran and Naor (2006)

(RF4) A voting system is receipt free, if a voter is unable to convince a third party of her vote even if she wants to do so. [44]

This work gives a formal definition for receipt freeness in computation model. The differences between this definition and **(RF3)** is that firstly here the adversary can be any other player, and secondly the term ""to convince" is used instead of "to prove". We can include the latter by replacing the knowledge modality with belief modality. So **(RF4)** can be expressed as follows:

$$\bigwedge_{v\in V} \bigwedge_{\substack{a\in \mathbb{A}\mathrm{gt}\\ v\neq a}} \bigwedge_{i\in Bal} \neg\langle\langle v\rangle\rangle \mathrm{F}(\mathsf{voted}_{\mathsf{v,i}} \wedge B_a \mathsf{voted}_{\mathsf{v,i}}).$$

4.5 Backes, Hritcu, and Maffei (2008)

(RF5) A voting system satisfies receipt freeness, if a coercer cannot force a voter to cast a certain vote and to provide a receipt that would certify her vote. [6]

This paper provided a formalization of coercion resistance and receipt freeness in applied pi calculus. A key term in the informal definition here is "to force". Because there is not a way to exactly express *forcing someone to do something* in ATL, we interpret it as though the coercer has a way to make voter to commit to a mutual strategy. In this way, *forcing the voter* can be interpreted as *having a mutual strategy with the voter*. The other key term here is "the receipt". Again, for being able to express the informal definition in ATL, we replace the concept of *existence of a receipt*' with a more general concept of *existence a strategy to prove the value of the vote*. With these interpretations we can express the definition as follows, which is similar to **(RF3)**:

$$\bigwedge_{v\in V\setminus\{c\}} \bigwedge_{i\in Bal} \neg\langle\langle c, v\rangle\rangle \mathrm{F}(\mathsf{voted}_{\mathsf{v,i}} \wedge K_c \mathsf{voted}_{\mathsf{v,i}}).$$

4.6 Delaune, Kremer, and Ryan (2010)

(RF6) A voting system is receipt free, if the voter does not obtain any artefact (a "receipt") which can be used later to prove to another party how she voted. [20]

Here again similar to definition **(RF5)**, we translate the *having a receipt* to *having a strategy to prove the value of the vote*. Therefore the definition can be expressed as:

$$\bigwedge_{v\in V} \bigwedge_{\substack{a\in \mathbb{A}\mathrm{gt}\\ v\neq a}} \bigwedge_{i\in Bal} \neg\langle\langle v\rangle\rangle \mathrm{F}(\mathsf{voted}_{\mathsf{v,i}} \wedge K_a \mathsf{voted}_{\mathsf{v,i}}).$$

(CR2) A voting system is coercion resistant, if the link between a voter and her vote cannot be established by

an attacker, even if the voter cooperates with the attacker during the election process. We assume that the voter and the attacker can communicate and exchange data at any time during the election process. [20]

If we translate *establishing a link between a voter and her vote* by *knowing the value of the vote of the voter*, then this definition can be expressed similar to definitions **(RF3)** and **(RF5)**:

$$\bigwedge_{v\in V\setminus\{c\}} \bigwedge_{i\in Bal} \neg\langle\!\langle c,v\rangle\!\rangle \mathrm{F}(\mathsf{voted}_{\mathsf{v,i}} \wedge K_c \mathsf{voted}_{\mathsf{v,i}}).$$

On the other hand, if we take it as a more general concept of *finding any correlation between the voter and his vote*, then we can express it as:

$$\bigwedge_{v\in V\setminus\{c\}} \bigwedge_{i\in Bal} \neg\langle\!\langle c,v\rangle\!\rangle \mathrm{F}(\mathsf{voted}_{\mathsf{v,i}} \wedge \bigvee_{j\in Bal\setminus\{i\}} K_c \neg \mathsf{voted}_{\mathsf{v,j}}).$$

4.7 Kusters, Truderung and Vogt (2010)

(CR3) A voting system is coercion resistant, if there exists a counter-strategy for the voter such that the coercer cannot tell whether the coerced voter is in fact following the coercer's instructions or whether she is just running the counter-strategy, and hence, achieves her own goal. [34]

The counter-strategy of the voter in this definition has to satisfy two conditions. Firstly it has to be indistinguishable from the instructed strategy of the coercer, and secondly makes the voter achieves her goal. Here again we focus only on the simple case where the coercer's instruction is basically voting for a certain candidate, and the goal of the voter is voting for her preferred candidate. The definition then can be expressed as follows:

$$\bigwedge_{v\in V\setminus\{c\}} \bigwedge_{\substack{i,j\in Bal\\ i\neq j}} \langle\!\langle v\rangle\!\rangle \mathrm{F}(\mathsf{voted}_{\mathsf{v,i}} \wedge \mathrm{G}\neg K_c \neg \mathsf{voted}_{\mathsf{v,j}}).$$

That is, the voter always has a strategy to eventually vote for her preferred candidate, and be sure that the coercer never finds out that she has disobeyed his instruction.

4.8 Randomization and Forced Abstention Attacks

In several definitions of coercion resistance, like **(CR1)**, the security property is meant to satisfy receipt freeness, but also protect against forced abstention attacks and randomization attack. We have omitted those kinds attacks in the previous subsections. Here, we tentatively suggest how resistance to randomization and forced abstention attacks can be specified.

Randomization attack happens when the coercer wants the voter to cast her vote in a way that the result follows some probability distribution, for example uniform distribution over the set of candidates. However, if the coercer instructs the voter to "vote at random with uniform distribution over the candidates", he will have no way of checking whether the voter followed his instruction. Therefore, in case of election a randomization attack is possible only when there exist a more tangible property (from the point of view of the coercer) for verifying the randomness of a single cast vote. It must be, at least in principle, possible for the coercer to verify the property based on the actual sequence of events (and not the voter's behavior as a whole, which is inaccessible to the coercer). For example in Prêt à Voter [18, 47], the list of candidates are printed in a completely random way on each ballot. Therefore if the coercer asks the voter to "cross the first slot in the ballot", this is potentially verifiable, and indirectly it implies random voting of the voter. In fact, the voter always has the possibility of auditing a ballot and obtaining a new one, so the voter has a counter strategy to obtain a ballot with her candidate in the coercer specified position, but of course this would be tedious to execute for complex ballots.

To make this idea more general, we can represent *feasible* randomization attacks by a state property p, such that the occurrence of p implies random behavior of the voter, in the way intended by the coercer. For example, the above scenario can be represented by $\mathsf{p} \equiv \mathsf{crossed}_{\mathsf{v},1}$, where $\mathsf{crossed}_{\mathsf{v,n}}$ expresses that voter v has crossed the nth slot on the ballot. Then, resistance to randomization attacks can be approximated by the following formula:

$$\bigwedge_{v\in V\setminus\{c\}} \neg\langle\!\langle c,v\rangle\!\rangle \mathrm{F} K_c \mathsf{p}.$$

That is, there is no collective strategy for the coercer and the voter (even assuming that they fully cooperate) such that at some point the coercer will know that p has occurred, and hence conclude that the voter has followed his instruction.

Forced abstention attack happens when the coercer wants the voter to behave such that her vote does not affect the final ballot counting result. It can be simply asking the voter not to cast a vote, but also can be wanting the voter to cast a vote in a way that is considered a spoilt vote. For the case of asking for casting a spoilt vote, the formalization can be similar to the case of randomization attack, where occurrence of a potentially verifiable state property p means that a spoilt vote is cast by the voter. For the case where the coercer asks the voter not to participate in the election(or not to cast a vote) the protection against forced abstention attack can be expressed as follows:

$$\bigwedge_{v\in V\setminus\{c\}} \neg\langle\!\langle c,v\rangle\!\rangle \mathrm{G}\left(\bigwedge_{i\in Bal} \neg\mathsf{voted}_{\mathsf{v,i}} \wedge K_c \bigwedge_{i\in Bal} \neg\mathsf{voted}_{\mathsf{v,i}}\right).$$

That is, there is no collective strategy for the coercer and the voter such that at any time after the end of the election time, the coercer knows that the voter has voted for a candidate (any candidate, even if the coercer cannot figure out which one).

5. CONCLUSIONS AND FUTURE WORK

In this work we have provided logical transcriptions of the informal form of the definitions of the coercion resistance and receipt freeness properties that can can be found in the literature. Our focus in these transcriptions was to show the role of strategic abilities of the participants in an election system in defining coercion related properties. To this end, we used formulae of the game logic **ATL*** for expressing these properties, and demonstrated some differences between the existing approaches.

There are many possible paths for future work. Among other things, we plan to refine our specifications using the

more flexible language of Strategy Logic [43, 41, 42] that allows for explicit quantification over strategies in k-player concurrent games. In particular, this should allow for a more general specification of resistance to randomization and abstention attacks, by directly encoding that the coercer is unable to distinguish between the actual behavior of the voter and the behavior prescribed by the coercer.

Perhaps more importantly, we will try to map the *formal* definitions of receipt-freeness and coercion resistance from [9, 29, 21, 44, 6, 20, 34] to models and formulae of game logics, in order to study the precise relationship between the informal intuitions and their formalizations. Adapting the **ATL** model checking algorithms so that they can be used to verify coercion-related properties is the third line that we envisage for future research.

Finally, we plan to study how *opacity*, as defined by Bryans et al. [14, 15] can be expressed in **ATL**, and more specifically how to to define coercion resistance as a flavour of opacity, similar to the style suggested in [46].

Acknowledgments. Masoud Tabatabaei acknowledges the support of the National Research Fund Luxembourg under project GAIVS (AFR Code:5884506).

6. REFERENCES

[1] R. Aditya, B. Lee, C. Boyd, and E. Dawson. An efficient mixnet-based voting scheme providing receipt-freeness. In *Trust and Privacy in Digital Business*, pages 152–161. Springer, 2004.

[2] T. Ågotnes. Action and knowledge in alternating-time temporal logic. *Synthese*, 149(2):377–409, 2006. Section on Knowledge, Rationality and Action.

[3] R. Alur, T. A. Henzinger, and O. Kupferman. Alternating-time Temporal Logic. In *Proceedings of the 38th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 100–109. IEEE Computer Society Press, 1997.

[4] R. Alur, T. A. Henzinger, and O. Kupferman. Alternating-time Temporal Logic. *Journal of the ACM*, 49:672–713, 2002.

[5] R. Araújo, N. B. Rajeb, R. Robbana, J. Traoré, and S. Youssfi. Towards practical and secure coercion-resistant electronic elections. In *Cryptology and Network Security*, pages 278–297. Springer, 2010.

[6] M. Backes, C. Hritcu, and M. Maffei. Automated verification of remote electronic voting protocols in the applied pi-calculus. In *Computer Security Foundations Symposium, 2008. CSF'08. IEEE 21st*, pages 195–209. IEEE, 2008.

[7] A. Baskar, R. Ramanujam, and S. Suresh. Knowledge-based modelling of voting protocols. In *Proceedings of the 11th conference on Theoretical aspects of rationality and knowledge*, pages 62–71. ACM, 2007.

[8] N. Belnap and M. Perloff. Seeing to it that: a canonical form for agentives. *Theoria*, 54:175–199, 1988.

[9] J. Benaloh and D. Tuinstra. Receipt-free secret-ballot elections. In *Proceedings of the twenty-sixth annual ACM symposium on Theory of computing*, pages 544–553. ACM, 1994.

[10] I. Boureanu, M. Cohen, and A. Lomuscio. Automatic verification of temporal-epistemic properties of cryptographic protocols. *Journal of Applied Non-Classical Logics*, 19(4):463–487, 2009.

[11] I. Boureanu, M. Cohen, and A. Lomuscio. Model checking detectability of attacks in multiagent systems. In *Proceedings of AAMAS*, pages 691–698, 2010.

[12] I. Boureanu, A. V. Jones, and A. Lomuscio. Automatic verification of epistemic specifications under convergent equational theories. In *Proceedings of AAMAS*, pages 1141–1148, 2012.

[13] I. Boureanu, P. Kouvaros, and A. Lomuscio. Verifying security properties in unbounded multiagent systems. In *Proceedings of AAMAS*, pages 1209–1217, 2016.

[14] J. W. Bryans, M. Koutny, L. Mazaré, and P. Y. Ryan. Opacity generalised to transition systems. In *Formal Aspects in Security and Trust*, pages 81–95. Springer, 2005.

[15] J. W. Bryans, M. Koutny, and P. Y. Ryan. Modelling opacity using petri nets. *Electronic Notes in Theoretical Computer Science*, 121:101–115, 2005.

[16] R. Chadha, S. Kremer, and A. Scedrov. Formal analysis of multiparty contract signing. *Journal of Automated Reasoning*, 36(1-2):39–83, 2006.

[17] K. Chatterjee, T. A. Henzinger, and N. Piterman. Strategy logic. In *Proceedings of CONCUR*, pages 59–73, 2007.

[18] D. Chaum, P. Y. A. Ryan, and S. A. Schneider. A practical voter-verifiable election scheme. In *Proceedings of ESORICS*, pages 118–139, 2005.

[19] S. Delaune, S. Kremer, and M. Ryan. Coercion-resistance and receipt-freeness in electronic voting. In *Computer Security Foundations Workshop, 2006. 19th IEEE*, pages 12–pp. IEEE, 2006.

[20] S. Delaune, S. Kremer, and M. Ryan. Verifying privacy-type properties of electronic voting protocols: A taster. In *Towards Trustworthy Elections*, pages 289–309. Springer, 2010.

[21] S. Delaune, S. Kremer, and M. D. Ryan. Receipt-freeness: Formal definition and fault attacks. In *Proceedings of the Workshop Frontiers in Electronic Elections (FEE 2005), Milan, Italy*. Citeseer, 2005.

[22] J. Dreier, P. Lafourcade, and Y. Lakhnech. A formal taxonomy of privacy in voting protocols. In *Communications (ICC), 2012 IEEE International Conference on*, pages 6710–6715. IEEE, 2012.

[23] E. Emerson. Temporal and modal logic. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume B, pages 995–1072. Elsevier Science Publishers, 1990.

[24] A. Herzig and N. Troquard. Knowing how to play: Uniform choices in logics of agency. In *Proceedings of AAMAS'06*, pages 209–216, 2006.

[25] W. Jamroga and T. Ågotnes. Constructive knowledge: What agents can achieve under incomplete information. *Journal of Applied Non-Classical Logics*, 17(4):423–475, 2007.

[26] W. Jamroga, S. Mauw, and M. Melissen. Fairness in non-repudiation protocols. In *Proceedings of STM'11*, volume 7170 of *Lecture Notes in Computer Science*, pages 122–139, 2012.

[27] W. Jamroga and W. van der Hoek. Agents that know

how to play. *Fundamenta Informaticae*, 63(2–3):185–219, 2004.

[28] H. L. Jonker and W. Pieters. Receipt-freeness as a special case of anonymity in epistemic logic. 2006.

[29] A. Juels, D. Catalano, and M. Jakobsson. Coercion-resistant electronic elections. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, pages 61–70. ACM, 2005.

[30] S. Kremer and J. Raskin. Game analysis of abuse-free contract signing. In *Proceedings of the 15th IEEE Computer Security Foundations Workshop (CSFW'02)*, pages 206–220. IEEE Computer Society Press, 2002.

[31] S. Kremer and J.-F. Raskin. A game-based verification of non-repudiation and fair exchange protocols. *Journal of Computer Security*, 11(3), 2003.

[32] W.-C. Ku and C.-M. Ho. An e-voting scheme against bribe and coercion. In *e-Technology, e-Commerce and e-Service, 2004. EEE'04. 2004 IEEE International Conference on*, pages 113–116. IEEE, 2004.

[33] R. Kusters and T. Truderung. An epistemic approach to coercion-resistance for electronic voting protocols. In *Security and Privacy, 2009 30th IEEE Symposium on*, pages 251–266. IEEE, 2009.

[34] R. Küsters, T. Truderung, and A. Vogt. A game-based definition of coercion-resistance and its applications. In *2010 23rd IEEE Computer Security Foundations Symposium*, pages 122–136. IEEE, 2010.

[35] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang, and S. Yoo. Providing receipt-freeness in mixnet-based voting protocols. In *Information Security and Cryptology-ICISC 2003*, pages 245–258. Springer, 2004.

[36] B. Lee and K. Kim. Receipt-free electronic voting scheme with a tamper-resistant randomizer. In *Information Security and Cryptology-ICISC 2002*, pages 389–406. Springer, 2003.

[37] A. Lomuscio and W. Penczek. LDYIS: a framework for model checking security protocols. *Fundamenta Informaticae*, 85(1-4):359–375, 2008.

[38] E. Magkos, M. Burmester, and V. Chrissikopoulos. Receipt-freeness in large-scale elections without untappable channels. In *Towards The E-Society*, pages 683–693. Springer, 2001.

[39] B. Meng. A critical review of receipt-freeness and coercion-resistance. *Information Technology Journal*, 8(7):934–964, 2009.

[40] M. Michels and P. Horster. Some remarks on a receipt-free and universally verifiable mix-type voting scheme. In *Advances in Cryptology-ASIACRYPT'96*, pages 125–132. Springer, 1996.

[41] F. Mogavero, A. Murano, G. Perelli, , and M. Vardi. What makes ATL* decidable? a decidable fragment of strategy logic. In *Proceedings of CONCUR*, pages 193–208, 2012.

[42] F. Mogavero, A. Murano, G. Perelli, and M. Vardi. Reasoning about strategies: On the model-checking problem. *ACM Transactions on Computational Logic*, 15(4):1–42, 2014.

[43] F. Mogavero, A. Murano, and M. Vardi. Reasoning about strategies. In *Proceedings of FSTTCS*, pages 133–144, 2010.

[44] T. Moran and M. Naor. Receipt-free universally-verifiable voting with everlasting privacy. In *Advances in Cryptology-CRYPTO 2006*, pages 373–392. Springer, 2006.

[45] T. Okamoto. Receipt-free electronic voting schemes for large scale elections. In *Security Protocols*, pages 25–35. Springer, 1998.

[46] T. Peacock and P. Ryan. Coercion-resistance as opacity in voting systems. *Technical Report Series-University Of Newcatle Upon Tyne Computing Science*, 959, 2006.

[47] P. Y. A. Ryan. The computer ate my vote. In *Formal Methods: State of the Art and New Directions*, pages 147–184. Springer, 2010.

[48] M. Schlapfer, R. Haenni, R. Koenig, and O. Spycher. 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*, volume 7187, page 71. Springer, 2012.

[49] H. Schnoor. Strategic planning for probabilistic games with incomplete information. In *Proceedings of AAMAS'10*, pages 1057–1064, 2010.

[50] P. Y. Schobbens. Alternating-time logic with imperfect recall. *Electronic Notes in Theoretical Computer Science*, 85(2):82–93, 2004.

[51] S. G. Weber, R. Araujo, and J. Buchmann. On coercion-resistant electronic elections with linear work. In *Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on*, pages 908–916. IEEE, 2007.