Receipt-Freeness as a Special Case of Anonymity in Epistemic Logic*

Hugo Jonker[1] and Wolter Pieters[2]

[1] Department of Mathematics and Computer Science
Eindhoven University of Technology
Den Dolech 2, 5600 MB Eindhoven, The Netherlands
h.l.jonker@tue.nl
[2] Institute for Computing and Information Sciences
Radboud University Nijmegen
P.O. Box 9010, 6500 GL Nijmegen, The Netherlands
wolterp@cs.ru.nl

Abstract. Formal methods have provided us with tools to check both anonymity of protocols and – more specifically – receipt-freeness of voting protocols. One of the frameworks used for proving anonymity is epistemic logic. However, to the best of our knowledge, epistemic logic has never been used to prove receipt-freeness of voting protocols. Still, the concept of indistinguishability used in formalizing anonymity seems to apply to receipt-freeness as well: a vote for one party should be indistinguishable from a vote for another party, *even if the voter supplies additional information outside the scope of the protocol*. In this paper, we formalize this aspect of anonymity relations, in order to provide an alternative formalization of receipt-freeness in voting protocols, based on epistemic logic.

1 Introduction

In the field of peer-to-peer (P2P) networks, much effort has been put into formalizing the concept of anonymity of messages (e.g. [10]). Intuitively, anonymity means that it is impossible to determine who sent which message to whom. Depending on the context, different formalizations of the notion of anonymity seem to be necessary [5].

The concept of anonymity is also of importance in electronic voting – often, voters should have the ability to vote without anybody else knowing which option they voted for (although in some countries, such as the United Kingdom and New Zealand, this is ultimately not the case). In the electronic voting community, the property expressing precisely that is usually called "privacy" instead of anonymity [3]. As noted in [1], it is not sufficient for voting systems to allow privacy, they must require it – voters must not be able to reveal their votes,

* This work is partly supported by a Pionier grant from NWO, the Netherlands Organisation for Scientific Research.

even if they attempt to. This property, which is stronger than privacy, is called "receipt-freeness".

The concept of receipt-freeness expresses that a voter cannot convince any other party of how she voted by creating a receipt. The notion has been introduced by [1], after which various receipt-free voting protocols were proposed, such as [7, 13]. Delaune et al. [2] provide a definition of receipt-freeness based on observational equivalence. Independently, Jonker and De Vink [8] provide an alternate definition that allows identification of receipts. Juels et al. note in [9] that receipt-freeness is not sufficient to prevent coercion in electronic elections, and they introduced the notion of coercion-resistance. This broader notion is again formalized by Delaune et al. in [3].

Receipt-freeness and privacy in voting on the one hand, and anonymity in P2P networks on the other, seem to have much in common: they both are information hiding properties. However, there is little overlap in their formalizations. A likely reason for this is that the two properties are seldomly expressed in the same framework. The main difference between the two approaches seems to be the difference in accent between anonymity of *people* (in the case of P2P networks) and anonymity (or privacy) of *messages* (in the case of voting).

In this paper, we aim at bringing the two approaches closer together, by investigating the value of an approach from the anonymity community for expressing properties of electronic voting systems. We are particularly interested in formalizing the concept of receipt-freeness from the perspective of a peer-to-peer anonymity approach. A useful notion from the anonymity community that can be used here is *unlinkability*.

As receipt-freeness expresses that a party cannot be convinced of something, it seems natural to examine this property in the context of logics such as epistemic logic [4]. However, to the best of our knowledge such an approach has not been investigated yet. In the anonymity community, frameworks based on epistemic logic do exist [6, 5]. The approach to defining receipt-freeness of Jonker and De Vink indicates that receipt-freeness can be translated into anonymity of the cast vote. Thus, it should be possible to formalize receipt-freeness in epistemic logic as well. This paper builds on the anonymity framework by Garcia, Hasuo, Pieters and Van Rossum [5] to show that this is indeed the case – receipt-freeness is expressed in that framework.

2 Preliminaries

Throughout this paper, we use the message algebra from Garcia et al. [5], which is defined in a straightforward way, and similar to e.g. [11]. We also adopt their network model, which is summarized below. All definitions in this section are due to Garcia et al., except for minor modifications.

2.1 Runs and observational equivalence

Definition 1. *(Agents, events) We denote by* AG *a non-empty set of agents, which has a special element* spy *for the intruder. An agent which is not* spy *is*

called a regular *agent. An* event *is a quadruple* $(A, B, m, type)$ *of the* sender A*, the* recipient B*, the* delivered message m *and the* channel type $type \in \{public, private\}$*. To make the intention clear we denote the above event by* $(A \to B : m)$ *for type* $= public$ *and with* $(A \to^* B : m)$ *for type* $= private$*. The set of all events (public and private) is denoted by* Event*.*

The reason for introducing private events is that receipt-freeness is often achieved in voting protocols by requiring seclusion of the voter, e.g. by using a voting booth (as in [1]) or secret, untappable channels (as in [13]). For our abstraction, it suffices that the intruder either can observe an event or that he cannot observe an event.

Definition 2. *(Runs) A* run *is a finite list of events, i.e. an element of the set* $\mathsf{Run} := \mathsf{Event}^*$*. A run describes all the events that have occurred in a network. The function* $\mathsf{msg}\colon \mathsf{Run} \to \mathcal{P}(\mathsf{MSG})$ *extracts all public and private messages occurring in a run. The function* msg_{pub} *similarly extracts all public messages from the run.*

Definition 3. *(Visible part of runs) Let* r *be a run. For a regular agent* $A \in \mathsf{AG} \setminus \{\mathsf{spy}\}$ *the* A-visible part *of* r*, denoted by* $r|_A$*, is the sublist of* r *consisting of all the events that have* A *in either sender or receiver field. The* spy-visible part *of* r*, denoted by* $r|_{\mathsf{spy}}$*, is the list of all public events.*

Definition 4. *A run* $r \in \mathsf{Run}$ *is said to be* legitimate *with respect to an initial possession function* $\mathsf{IPo}\colon \mathsf{AG} \to \mathcal{P}(\mathsf{MSG})$ *if, for every* $i \in [0, |r| - 1]$*,* $m_i \in \mathsf{Poss}_{\mathsf{IPo}}(r, A, i)$*, where* $(A_i, B_i, m_i, type_i) = r_i$*.*

$\mathsf{Poss}_{\mathsf{IPo}}(r, A, i)$ is the set of all messages that A can construct in stage i of the run. For formal definitions, see [5].

Definition 5. *(Protocols and runs of protocol) A* protocol *is a pair* $(\mathsf{cr}, \mathsf{IPo})$ *consisting of a set of candidate runs* cr *and an initial possession function* IPo*. A run* $r \in \mathsf{Run}$ *is said to be a* run of a protocol $(\mathsf{cr}, \mathsf{IPo})$ *if* $r \in \mathsf{cr}$ *and* r *is legitimate with respect to the initial possession function* IPo*. The set of runs of a protocol* $(\mathsf{cr}, \mathsf{IPo})$ *is denoted by* $\mathsf{Run}_{\mathsf{cr},\mathsf{IPo}}$*.*

Informally, a reinterpretation π of a run under a set of messages U is a second run which cannot be distinguished from the first based on the possession of the messages in U. For a formal definition, see [5].

Definition 6. *(Observational equivalence of runs) Let* $r, r' \in \mathsf{Run}_{\mathsf{cr},\mathsf{IPo}}$ *be two runs of a protocol* $(\mathsf{cr}, \mathsf{IPo})$ *and let* $A \in \mathsf{AG}$ *be an agent. Two runs* r *and* r' *are said to be* observationally equivalent for an agent A*, denoted by* $r \cong_A r'$*, if there exists a reinterpretation* π *under* $\mathsf{Poss}_{\mathsf{IPo}}(r, A, |r| - 1)$ *such that* $\pi(r|_A) = r'|_A$ *. Such a reinterpretation will be called a* reinterpretation for A*.*

2.2 Formulas and epistemic operators

With a formula, we wish to express not only a fact about a run, but also that an agent knows/does not know a certain fact about a run.

Definition 7. *(Formulas) A* formula φ *is a function which takes as its arguments a protocol* $(\mathsf{cr}, \mathsf{IPo})$ *and a run* $r \in \mathsf{Run}_{\mathsf{cr},\mathsf{IPo}}$ *of that protocol, and returns either* $\mathbf{T}$ *or* $\mathbf{F}$*. The set of all the formulas is denoted by* Form*. We follow the tradition of logic to denote the fact* $\varphi(\mathsf{cr}, \mathsf{IPo}, r) = \mathbf{T}$*, where* $r \in \mathsf{Run}_{\mathsf{cr},\mathsf{IPo}}$*, by* $\mathsf{cr}, \mathsf{IPo}, r \models \varphi$*. Often the protocol* $(\mathsf{cr}, \mathsf{IPo})$ *under consideration is clear from the context, in which case we abbreviate* $\mathsf{cr}, \mathsf{IPo}, r \models \varphi$ *to* $r \models \varphi$*. Logical connectives on formulas such as* $\wedge$*,* $\vee$*,* $\rightarrow$ *and* $\neg$ *are defined in an obvious way. A formula* φ *is said to be* valid *if* $\mathsf{cr}, \mathsf{IPo}, r \models \varphi$ *for all* cr*,* IPo *and* r*.*

Definition 8. *The formula* A Sends m to B *means: at some stage in the run,* A *sends a message to* B *which* contains m as a subterm *(the subterm relation* $\preceq$ *is defined formally in [5]).*

$$r \models A \ \mathsf{Sends}\ m \ \mathsf{to}\ B \quad \stackrel{def}{\Longleftrightarrow}$$
$$\exists i \in [0, |r| - 1].\ \big(m \preceq m' \text{ where } (A, B, m', type) = r_i\big).$$

We will also use A Sends m *to mean that* A *sends the message* m *to someone.*

$$r \models A \ \mathsf{Sends}\ m \quad \stackrel{def}{\Longleftrightarrow} \quad \exists B.\ A \ \mathsf{Sends}\ m \ \mathsf{to}\ B.$$

The formula A $\mathsf{Possesses}$ m at i *means:* at stage i of the protocol*,* A *is capable of constructing the message* m*.*

$$r \models A \ \mathsf{Possesses}\ m \ \mathsf{at}\ i \quad \stackrel{def}{\Longleftrightarrow} \quad m \in \mathsf{Poss}_{\mathsf{IPo}}(r, A, i).$$

The formula A $\mathsf{Possesses}$ m *means:* after the run has finished*,* A *is capable of constructing the message* m*.*

$$r \models A \ \mathsf{Possesses}\ m \quad \stackrel{def}{\Longleftrightarrow} \quad m \in \mathsf{Poss}_{\mathsf{IPo}}(r, A, |r| - 1).$$

The formula A $\mathsf{Originates}$ m *means that:* A Sends m*, but* A *is not relaying. More precisely,* m *does not appear as a subterm of a message which* A *has received before.*

$$r \models A \ \mathsf{Originates}\ m \quad \stackrel{def}{\Longleftrightarrow}$$
$$\exists i \in [0, |r| - 1].\ \exists B.\ \Big(m \preceq m' \text{ where } (A, B, m', type) = r_i$$
$$\wedge\, \forall j \in [0, i - 1].\ \big(m \not\preceq \hat{m} \text{ where } (A', A, \hat{m}, type) = r_j\big)\Big).$$

Definition 9. *(Epistemic operators) Let* $(\mathsf{cr},\ \mathsf{IPo})$ *be a protocol. For an agent* $A \in \mathsf{AG}$*, the epistemic operator* $\Box A : \mathsf{Form} \rightarrow \mathsf{Form}$ *is defined by:*

$$\mathsf{cr}, \mathsf{IPo}, r \models \Box A \varphi \quad \stackrel{def}{\Longleftrightarrow}$$
$$\forall r' \in \mathsf{Run}_{\mathsf{cr},\mathsf{IPo}}.\ \big(r' \cong_A r \implies \mathsf{cr}, \mathsf{IPo}, r' \models \varphi\big).$$

The formula $\Box A\varphi$ is read as "after the run is completed, the agent A knows *that φ is true". The formula $\Diamond A\varphi$ is short for $\neg\Box A\neg\varphi$ and read as "after the run is completed, the agent A* suspects *that φ is true".*

3 Expressing information hiding properties

Using the notion of an *anonymity set* – a collection of agents among which a given agent is not identifiable – Garcia et al. define the information hiding properties of sender anonymity, unlinkability and plausible deniability in epistemic logic:

Definition 10. *(Sender anonymity) Suppose that r is a run of a protocol in which an agent B receives a message m. We say that r provides* sender anonymity *with anonymity set* AS *if it satisfies*

$$r \models \bigwedge_{X \in \mathsf{AS}} \Diamond B(X \ \mathsf{Originates}\ m).$$

This means that, as far as B is concerned, every agent in the anonymity set could have sent the message.

Definition 11. *(Unlinkability) A run r provides* unlinkability *for users A and B with anonymity set* AS *iff*

$$r \models \big(\neg\Box\mathsf{spy}\varphi_0(A,B)\big) \wedge \bigwedge_{X \in \mathsf{AS}} \Diamond\mathsf{spy}\varphi_0(X,B)\ ,$$

where $\varphi_0(X,Y) = \exists n.\ \big(X\ \mathsf{Sends}\ n \wedge Y\ \mathsf{Possesses}\ n\big)$.

Intuitively, the left side of the conjunction means that the adversary is not certain that A sent something to B. The right side means that every other user could have sent something to B. Similarly, unlinkability between a user A and a message m could be defined as $\models \neg\Box\mathsf{spy}(A\ \mathsf{Sends}\ m) \wedge \bigwedge_{X \in \mathsf{AS}} \Diamond\mathsf{spy}(X\ \mathsf{Sends}\ m)$.

In certain circumstances (e.g., relays), agents might be interested in showing that they did not know that they had some sensitive information m. This might be modeled by the following epistemic formula:

Definition 12. *(Plausible deniability) Agent A can* plausibly deny *message m in run r iff*

$$r \models \Box\mathsf{spy}\neg(\Box A(A\ \mathsf{Possesses}\ m))\ .$$

This formula is read as: the spy knows that A does not know that she possesses m.

We extend this set of definitions by providing the additional property of *receipt-freeness*. Receipt-freeness of an agent A with respect to a message m (e.g. a vote) intuitively means that A cannot send a message m' to the spy that proves that she sent m in the past. For this purpose, the definition of plausible deniability

is too strong, since A *does* know that she possesses m. Sender anonymity is particularly useful for providing anonymity of the voter with respect to the election authorities, but in receipt-freeness, A herself tries to communicate with the spy. Instead, it should not be possible to link A to her vote. Thus, unlinkability seems the most natural property to base our definition of receipt-freeness upon.

In the anonymity framework, the concept of anonymity set is used to define the set of entities between which an observer should not be able to distinguish. To apply the framework to votes, we need to adapt the concept of anonymity set. In voting, we are sure that each (actual) voter submits a vote. Therefore, the point is not whether any other user in an anonymity set could have sent the message, but *whether the voter could have submitted any other vote*. Therefore, we define an anonymity set of *messages*, AMS , instead of an anonymity set of agents. This set typically consists of all possible votes.

To be able to define receipt-freeness, we need to have a way to extend a given run with one message: the receipt. We write this as $r.(A \rightarrow B : m))$ for a given run r, message m (the receipt), sender A and receiver B. For A to be able to send the receipt, she needs to have the message in her possessions at the end of the original run. The new run does *not* need to be a run of the protocol. It *does* need to be legitimate with respect to the initial possession function.

Definition 13. *(Weak receipt-freeness) A run of a protocol is* weakly receipt-free *for agent A with respect to message m iff for all $m' \in \mathsf{Poss}_{\mathsf{IPo}}(r, A, |r| - 1)$,*

$$r.(A \rightarrow \mathsf{spy} : m') \models \neg\Box\mathsf{spy}(A \ \mathsf{Sends}\ m)$$

Weak receipt-freeness implies that the voter cannot prove to the spy that she sent message m during the protocol, where m is the part of a message representing the vote. However, this notion is still fairly limited. For example, suppose that the spy wants the voter to vote for party X. Suppose, furthermore, that the voter instead chooses to vote Y, which is represented by message m in the above definition. Now, if the voter cannot show that she voted Y, this protocol is receipt-free with respect to the definition above. However, if the spy can acquire information which proves that the voter did *not* vote X, the spy will not be satisfied. Therefore, we introduce a stronger notion of receipt-freeness as well.

Definition 14. *(Strong receipt-freeness) A run of a protocol is* strongly receipt-free *for agent A with respect to a message m in anonymity set AMS iff for all $m' \in \mathsf{Poss}_{\mathsf{IPo}}(r, A, |r| - 1)$,*

$$r.(A \rightarrow \mathsf{spy} : m') \models (\neg\Box\mathsf{spy}(A \ \mathsf{Sends}\ m)) \wedge \bigwedge_{m'' \in \mathsf{AMS}} \Diamond\mathsf{spy}(A \ \mathsf{Sends}\ m'')$$

Here, no matter what information the voter supplies to the spy, *any* vote in the anonymity set is still possible. This is represented by the "suspects" symbol $\Diamond\mathsf{spy}$. In other words, for all possible votes, the spy still suspects that the voter cast this particular vote; or: the spy is not certain she did *not* cast this vote.

This requires that at least one message has been received (i.e. at least one vote has been cast) for every message (vote) $m'' \in \mathsf{AMS}$. Otherwise, the spy could observe from the results that no-one, in particular not voter A, cast a certain vote. Thus, for votes, $\mathsf{AMS} \subseteq$ the set of candidates who received votes.

Notice that this definition is analogous to the definition of unlinkability of Garcia et al.

Theorem 1. *If a run of a protocol is strongly receipt-free for agent A with respect to message m in anonymity set* AMS *, then it is also weakly receipt-free for agent A with respect to message m.*

Proof. This follows directly from the definitions.

These definitions of receipt-freeness justify the need for the limited reading ability of the spy in Definition 3. If the spy can read all the messages, the voter only needs to supply the secret keys in order to provide a receipt. This is not what is commonly understood by analyzing receipt-freeness. Instead, there are certain messages in the protocol that the spy is not assumed to have access to (when the voter is in a "voting booth").

In our definition, we deviate from the approach by Delaune et al. [3]. Intuitively, receipt-freeness is achieved if a voter does not possess convincing, exclusive evidence of how she voted. The approach by Delaune et al. defines receipt-freeness using two voters (to preserve indistinguishability of the result). By focusing on the actual receipt, our definition only relies on one voter, and thus remains closer to the intuition. The indistinguishability is made explicit in our definition by AMS , and needs not be extended to all candidates (but can be confined e.g. to all candidates for whom at least one vote was cast).

4 Conclusions and future work

In this paper, we introduced an approach to formally verify receipt-freeness in epistemic logic. To the best of our knowledge, we are the first to do so. The approach has not been tested on real protocols thus far.

One of the main benefits of our approach is the intuitive definition that can be provided for receipt-freeness. As opposed to other approaches, especially [3], the "receipt" can easily be distinguished in our model as a separate message that the voter sends to the spy. Instead of investigating whether the spy can recover the vote from forwarded messages, we judge whether the spy really *knows* what the voter's choice was, based on any possible receipt. This notion of *knows* is characteristic for the epistemic logic approach, and this justifies our choice for the anonymity framework of [5] as a basis.

One of the main differences between P2P anonymity and our approach is that we are not in the first place interested in who communicated with whom. Although the fact *that* a voter voted may also be of interest to the spy, the major security risk lies in the content of the message. In this sense, the notion of

anonymity or privacy in voting is closer to confidentiality. In the definitions, this leads to an anonymity set of *messages* instead of an anonymity set of *agents*.

In future work, we aim at providing an alternative definition of receipt-freeness in our model, based on the knowledge of the spy instead of on extension of a run. We hope to prove that the two definitions are equivalent. Moreover, we wish to apply the definitions to existing voting protocols, in order to prove (or disprove) receipt-freeness. It may also be interesting to investigate the relation between verifiability [12] and receipt-freeness in epistemic logic, since both receipt-freeness and verifiability are based on an agent's knowledge instead of its possessions.

References

1. J.C. Benaloh and D. Tuinstra. Receipt-free secret ballot elections (extended abstract). In *Proc. 26th ACM Symposium on the Theory of Computing (STOC)*, pages 544–553. ACM, 1994.
2. S. Delaune, S. Kremer, and M.D. Ryan. Receipt-freeness: Formal definition and fault attacks (extended abstract). In *Proceedings of the Workshop Frontiers in Electronic Elections (FEE 2005)*, Milan, Italy, September 2005.
3. S. Delaune, S. Kremer, and M.D. Ryan. Coercion-resistance and receipt-freeness in electronic voting. In *Proceedings of the 19th IEEE Computer Security Foundations Workshop (CSFW'06)*, Venice, Italy, July 2006. IEEE Computer Society Press.
4. Ronald Fagin, Joseph Y. Halpern, Yoram Moses, and Moshe Y. Vardi. *Reasoning About Knowledge*. MIT Press, Cambridge, MA, USA, 2003.
5. F. D. Garcia, I. Hasuo, W. Pieters, and P. van Rossum. Provable anonymity. In Ralf Küsters and John Mitchell, editors, *3rd ACM Workshop on Formal Methods in Security Engineering (FMSE 2005)*, pages 63–72. ACM Press, 2005.
6. J. Halpern and K. O'Neill. Anonymity and information hiding in multiagent systems. In *16th IEEE Computer Security Foundations Workshop (CSFW '03)*, pages 75–88, 2003.
7. M. Hirt and K. Sako. Efficient receipt-free voting based on homomorphic encryption. In B Preneel, editor, *Proc. EUROCRYPT 2000*, number 1807 in LNCS, pages 539–556, 2000.
8. H.L. Jonker and E.P. de Vink. Formalising receipt-freeness. In Michael Backes, Stefanos Gritzalis, and Bart Preneel, editors, *ISC'06*. To appear, 2006.
9. A. Juels, D. Catalano, and M. Jakobsson. Coercion-resistant electronic elections. In *Proc. WPES'05*. ACM, 2005.
10. S. Mauw, J. Verschuren, and E.P. de Vink. A formalization of anonymity and onion routing. In P. Samarati, P. Ryan, D. Gollmann, and R. Molva, editors, *Proc. esorics 2004*, pages 109–124, Sophia Antipolis. LNCS 3193.
11. L.C. Paulson. The inductive approach to verifying cryptographic protocols. *Journal of Computer Security*, 6:85–128, 1998.
12. W. Pieters. What proof do we prefer? variants of verifiability in voting. In *Proceedings of the Workshop on Electronic Voting and e-Government in the UK*, Edinburgh, UK, February 27-28, 2006.
13. K. Sako and J. Kilian. Receipt-free mix-type voting scheme – a practical solution to the implementation of a voting booth. In L.C. Guillou and J.-J. Quisquater, editors, *EUROCRYPT'95*, volume 921 of *LNCS*, pages 393–403. Springer, 1995.