Enforcing Privacy in the Presence of Others: Notions, Formalisations and Relations

Naipeng Dong*, Hugo Jonker, and Jun Pang

Faculty of Sciences, Technology and Communication,
University of Luxembourg, Luxembourg

Abstract. Protecting privacy against bribery/coercion is a necessary requirement in electronic services, like e-voting, e-auction and e-health. Domain-specific privacy properties have been proposed to capture this. We generalise these properties as *enforced privacy*: a system enforces a user's privacy even when the user collaborates with the adversary. In addition, we account for the influence of third parties on a user's privacy. Third parties can help to break privacy by collaborating with the adversary, or can help to protect privacy by cooperating with the target user. We propose *independency of privacy* to capture the negative privacy impact that third parties can have, and *coalition privacy* to capture their positive privacy impact. We formally define these privacy notions in the applied pi calculus and build a hierarchy showing their relations.

1 Introduction

Privacy is of great importance to electronic services such as e-voting, e-auction, and e-health. A large amount of research has been done in this area, for example, using statistical methods. In the literature, an important focus is privacy in communication protocols, since most electronic services use the Internet. To capture privacy in protocols, a wide variety of privacy properties have been proposed, such as anonymity, untraceability, quantified privacy, etc. (e.g., see [1–5]). We focus on a subset of such properties – non-quantified (binary) data privacy, i.e., properties that are either satisfied or not (as opposed to providing a quantitative answer).

Classical data privacy assumes that users want to keep their privacy [1, 3, 4]. However, a user may want to reveal information to the adversary due to bribery or coercion. Systems providing electronic services need to protect against such threats (e.g., [6–9]). This was first achieved in voting: a system in which a voter could not undo his privacy after voting (preventing vote selling) [6], and later, a system in which a voter, coerced to communicate continuously with the adversary, cannot undo his privacy [8]. These ideas were lifted to an e-auction system [7] and an e-health system [9]. Following this development of stronger systems, domain-specific formalisations of privacy properties against bribery and coercion were proposed in the literature: receipt-freeness and coercion-resistance

* Supported by a grant from the Fonds National de la Recherche (Luxembourg).

in e-voting [10], e-auction [11], and e-health [12]. In order to address these privacy concerns domain-independently, we propose a generic notion of *enforced privacy*: a user's privacy is preserved even if the user collaborates with the adversary by sharing information.

Our notions of (enforced) data privacy focus only on one target user – ignoring the privacy impact of other users. However, a third party may help to break user privacy (*collaboration*), e.g., revealing your vote may enable the adversary to deduce another voter's vote. On the other hand, a third party can help maintain privacy (*coalition*), e.g., a non-coerced voter (who votes as the adversary desires) can swap receipts with a coerced voter, providing the coerced voter "proof" of compliance while being free to vote as he pleases. Accounting for the privacy effect of third parties is particularly necessary in domains where many non-trusted roles are involved. For example, pharmacists in e-health may be able to help reveal prescription behaviour of doctors. In order to ensure doctor prescribing-privacy, an e-health system must prevent this [9, 13]. This requirement has been expressed and formalised in e-health [12] and e-voting [14]. In this paper, we generalise these formalisations as *independency of privacy*: the help of a set of third parties does not enable the adversary to break a target user's privacy. To capture the converse situation – the privacy effect of third parties helping the target user by sharing information with the target user, we propose a new notion of *coalition privacy*: a target user's privacy is preserved with the help of a set of third parties sharing information with the target user. In particular, we use this notion to also capture the situation where third parties are involved but no information is shared between the target user and third parties. In this case, the mere *existence* of the third parties can help to create a situation where privacy is preserved.

In addition to identifying these (new) privacy notions, this paper contributes on formalising them in a new formal framework and formally prove their relations. Cryptographic protocols are well known to be error-prone and formal approaches have shown to be efficient in addressing this problem, e.g., see [15, 16]. Thus, formalising privacy notions is a necessary step to verify the privacy claims of a protocol. Our framework is based on the applied pi calculus as it provides an intuitive way for modelling privacy properties and cryptographic protocols. In addition, it is supported by the ProVerif [17] tool, which allows us to verify many privacy properties automatically [18, 19].

We present a formal framework which allows us to give domain-independent formalisations. We define a standard form of protocols which is able to represent any protocol. To formally define enforced privacy properties and independency of privacy properties, we model *collaboration* between users and the adversary. The collaboration allows us to precisely specify which information is shared and how it is shared, thus provides the necessary flexibility for modelling various types of collaboration. To model coalition privacy properties, we propose the notion of *coalition* in our framework to formally capture the behaviour and shared information among a target user and a set of third parties. In our framework, the foundational property data-privacy, is formalised in a classical way as strong secrecy:

Table 1. Privacy notions

target user collaborates with adversary	**third parties**			
	all neutral	*some attacking*	*some defending*	*some defending some attacking*
no	priv	ipriv	cpriv	cipriv
yes	epriv	iepriv	cepriv	ciepriv

equivalence of two processes where a variable is instantiated differently [20]. Based on this property, we formalise enforced-privacy, independency-of-privacy and independency-of-enforced-privacy using the formalisation of collaboration. Using the formalisation of coalition, four corresponding coalition privacy properties are formalised. Finally, we formally discuss how the formalised privacy properties are related in a privacy hierarchy. In addition, we show that many existing formalisations are instances of properties in our hierarchy.

2 Privacy Notions

With respect to the classical Dolev-Yao adversary [21][1], we distinguish between two classes of privacy-affecting behaviour: the target user (collaborating with the adversary or not), and the behaviour of third parties. Third parties may be *neutral*, collaborating with the adversary (*attacking*), or collaborating with the target user (*defending*) – thus we also consider the situation where some are attacking and some are defending. A target user who collaborates with the adversary is not under the adversary's direct control, contrary to a compromised user who genuinely shares initial private information with the adversary. A *neutral* third party, like an honest user, follows the protocol specification exactly. Thus, such a third party neither actively helps nor actively harms the target user's privacy. A *defending* third party helps the target user to preserve his privacy. An *attacking* third party communicates with the adversary to break the target user's privacy. Note that we do not consider a third party that attacks and defends the target user simultaneously. Given this classification, a target user will find himself one of the following four situations w.r.t. third parties: 1) all are neutral; 2) some are attacking; 3) some are defending; and 4) some are attacking, some are defending. In the latter three cases, the remaining third parties (if any) are considered neutral. Combining the various behaviours of the third parties with those of the target user gives rise to eight privacy properties (see Tab. 1).

Motivation examples for each property are as follows – data-privacy (priv): the adversary cannot link the contents of an encrypted email to the user; enforced-

[1] Note that the Dolev-Yao adversary is not assumed to fully control authenticated users. Bribed or coerced users cannot be modelled as part of the adversary, as they are not trusted by the adversary. In addition, it is necessary to model which information and how users share the information, especially those obtained from channels hidden from the adversary.

privacy (epriv): a voter should not be able to prove to a vote-buyer how he voted; independency-of-privacy (ipriv): in e-health the adversary cannot link a doctor to his prescriptions, despite the help of a pharmacist; independency-of-enforced-privacy (iepriv): the adversary should not be able to link a doctor to his prescriptions (to prevent bribes), even when both the pharmacist and the doctor are helping him; coalition-privacy (cpriv): in location-based services, the user's real location is hidden amongst the locations of the helping users; coalition-enforced-privacy (cepriv): in anonymous routing, a sender remains anonymous if he synchronises with a group of senders, even if he seems to collaborate; coalition-independency-of-privacy (cipriv): the adversary cannot link an RFID chip to its identity, even though some malicious readers are helping the adversary, provided other RFID tags behave exactly as the target one; coalition-independency-of-enforced-privacy (ciepriv): in electronic road pricing, other users may hide a user's route from the adversary, even if the user seems to collaborate and malicious routers relay information on passing cars to the adversary.

The examples above illustrate that similar privacy concerns arise in many different domains – e-voting, e-health, location-based services, RFID, etc. So far, attempts at formalising privacy have usually been domain-specific (e.g., [22, 2, 10, 3, 4, 23, 11, 12, 24]). We advocate a domain-independent approach to privacy, and develop a formal framework to achieve this in Sect. 3.

3 Formal Framework

3.1 The Applied Pi Calculus

The applied pi calculus [25] assumes an infinite set of *names* to model data and communication channels, an infinite set of *variables* and a finite set of *function symbols* each with an associated arity to capture cryptographic primitives. A constant is defined as a function symbol with arity zero. *Terms* are defined as either names, or variables or function symbols applied on other terms to capture communicated messages. We denote the variables in a term N as $\mathsf{Var}(N)$. In addition, the applied pi calculus assumes a set of base types (e.g., the universal type *Data*) and a type system (sort system) for terms generated by the base set. Terms are assumed to be well-typed and syntactic substitutions preserve types. Processes (see Fig. 1) are defined to model protocols. A name is *bound* if it is under restriction. A variable is *bound* by restrictions or inputs. Names and variables are *free* if they are not delimited by restrictions or by inputs. The sets of free names, free variables, bound names and bound variables of a process A are denoted as $\mathsf{fn}(A)$, $\mathsf{fv}(A)$, $\mathsf{bn}(A)$ and $\mathsf{bv}(A)$, respectively. A term is *ground* when it does not contain variables. A process is *closed* if it does not contain free variables. $\{M/x\}$ is a substitution which replaces variable x with term M. A *context* $\mathcal{C}[\_]$ is defined as a process with a hole, which may be filled with any process. An evaluation context is a context whose hole is not under a replication, a conditional, an input or an output. Finally, we use $\nu\widetilde{\mathtt{n}}$ to abbreviate the process generating a list of names (i.e., $\nu\mathtt{n}_1 \cdots \nu\mathtt{n}_n$) and use $\nu\widetilde{\mathtt{n}}/\mathtt{n}_i$ to abbreviate process $\nu\mathtt{n}_1 \cdots \nu\mathtt{n}_{i-1}.\nu\mathtt{n}_{i+1}.\cdots.\nu\mathtt{n}_n$ (erasing $\nu\mathtt{n}_i$ from process $\nu\widetilde{\mathtt{n}}$).

Fig. 1. Applied pi processes

$P, Q, R ::=$	plain processes	$A, B, C ::=$	extended processes
0	null process	P	plain process
$P \mid Q$	parallel composition	$A \mid B$	parallel composition
$!P$	replication	$\nu \mathtt{n}.A$	name restriction
$\nu \mathtt{n}.P$	name restriction	$\nu x.A$	variable restriction
if $M =_E N$ then		$\{M/x\}$	active substitution
P else Q	conditional		
$\mathsf{in}(v, x).P$	message input		
$\mathtt{out}(v, M).P$	message output		

Several equivalence relations on processes are defined in the applied pi calculus. We mainly use labelled bisimilarity $\approx_\ell$ [25]. Two processes are labelled bisimilar if the adversary cannot distinguish them.

3.2 Well-formed Protocols

For the simplicity of formalisation, we define a standard form of a protocol, inspired by Arapinis et al. [3], and any protocol can be written in this form.

Definition 1 (well-formed protocols). *A protocol with p roles is well-formed if it is a closed plain process P_w of the form:*

$$P_w = \nu\widetilde{\mathtt{c}}.(genkey \mid !R_1 \mid \cdots \mid !R_p)$$
$$R_i = \nu \mathtt{id}_i.\nu \mathtt{data}_i.init_i.!(\nu \mathtt{s}_i.\nu \mathtt{sdata}_i.sinit_i.main_i) \quad (\forall i \in \{1, \cdots, p\})$$

1. *P_w is canonical [3]: names and variables in the process never appear both bound and free, and each name and variable is bound at most once;*
2. *data is typed, channels are ground, private channels are never sent on any channel;*
3. *$\nu\widetilde{\mathtt{c}}$, $\nu\mathtt{data}_i$ and $\nu\mathtt{sdata}_i$ may be null;*
4. *$init_i$ and $sinit_i$ are sequential processes;*
5. *genkey, $init_i$, $sinit_i$ and $main_i$ can be any process (possibly null) such that P_w is a closed plain process.*

In process P_w, $\widetilde{\mathtt{c}}$ are channel names; *genkey* is a sub-process in which shared data (e.g., keys shared between two roles) are generated and distributed; R_i ($1 \leq i \leq p$) is a role. To distinguish instances taking the same role R_i, each instance is dynamically associated with a distinct identity $\nu\mathtt{id}_i$; $\mathtt{data}_i$ is private data of an instance; $init_i$ models the initialisation of an instance; $(\nu\mathtt{s}_i.\nu\mathtt{sdata}_i.sinit_i.main_i)$ models a session of an instance. To distinguish sessions of the same instance, each session is dynamically associated to a distinct identity ($\nu\mathtt{s}_i$); $\mathtt{sdata}_i$ is private data of a session; $sinit_i$ models the initialisation of a session; $main_i$ models the behaviour of a session.

Note that this standard form does not limit the type of protocols we consider. A role may include a number of sub-roles so that a user may take more than one part in a protocol. The identities do not have to be used in the process. All of $\nu\widetilde{\mathsf{c}}$, $\nu\mathtt{data}_i$ and $\nu\mathtt{sdata}_i$ may be null and *genkey*, $init_i$, $sinit_i$ and $main_i$ can be any process (possibly null) such that P_w is a closed plain process. Any process can be written in a canonical form by α-conversion [3]. Thus, any protocol can be written as a well-formed protocol.

3.3 Data-privacy

We formally define the property data-privacy that acts as the foundation upon which other properties are built. To do so, we need to make explicit *which data* is protected. Thus, the property data-privacy always specifies the target data. In process P_w, the target data τ can be expressed as a bound name (complicated target data can be reduced to bound names) which belongs to a role (the target role R_i), i.e., $\tau \in \mathsf{bn}(R_i)$. For the sake of simplicity, we (re)write the role R_i in the form of $R_i = \nu\mathtt{id}_i.\nu\tau.\hat{R}_i$, where $\hat{R}_i$ is a plain process which has two variables id_i and τ. By α-conversion we can always transform R_i into the above form.

Intuitively, data-privacy w.r.t. τ of protocol P_w, is the inability of the adversary to link an honest user taking role R_i to his instantiation of the target data τ. An honest user taking role R_i is modelled as process R_i. $\hat{R}_i\{\mathsf{id}/id, t/\tau\}$ denotes an instance of the target user in which the target user instantiates the target data with t where t denotes any data which can be used to replace the target data. The data-privacy can be modelled as strong secrecy [20] of the target data: the adversary cannot distinguish an execution of R_i where $\tau = \mathtt{t}_1$ from an execution where $\tau = \mathtt{t}_2$, for $\mathtt{t}_1 \neq \mathtt{t}_2$.

Definition 2. *A well-formed protocol P_w satisfies data-privacy (priv) w.r.t. data τ ($\tau \in \mathsf{bn}(R_i)$), if $C_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\}] \approx_\ell C_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\}]$.*

In the above definition, id is a constant, $\mathtt{t}_1$ and $\mathtt{t}_2$ are free names. Since $R_i = \nu\mathtt{id}_i.\nu\tau.\hat{R}_i$, process $\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\}$ is an instance of role R_i where the identity is id and the target data is $\mathtt{t}_1$. The evaluation context $C_{P_w}[\_]$ models neutral third parties. Thus, $C_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\}]$ is an instance of the protocol P_w, similarly for $C_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\}]$. The only difference between these two instances is the instantiation of the target data τ. Thus, this definition captures data-privacy by using the relation $\approx_\ell$: the adversary cannot distinguish a user process with different target data.

3.4 Modelling Collaboration with the Adversary

In order to define enforced privacy properties where the target user collaborates with the adversary and independency privacy properties where a set of third parties collaborate with the adversary, we need to model *collaboration* of users (a target user/third parties) with the adversary.

The process of a set of users is modelled as processes of each user in parallel. Since a user process is modelled as a role in a well-formed protocol and each user

process can be any role, the set of users of a protocol P_w is formally defined as a plain process $R_U = R_{u_1} \mid \cdots \mid R_{u_m}, \forall i \in \{1, \ldots, m\}, R_{u_i} \in \{R_1, \ldots, R_p\}$.

Inspired by the formal definition of coercion in [10], the collaboration between a set of users and the adversary is formalised as a transformation of the process of the set of users. Note that a user may not always share *all* his information, e.g., a bribed user in a social network may reveal his relation with another user, but not his password. A way to express partly information sharing is to specify which terms of a process are shared and how they are shared. Since the process of a set of users is canonical in a well-formed protocol, bound names and variables are different in each user process. Thus, we can express information of a set of users as a set of terms appearing in the process of the set of users. Terms appearing in a plain process R_U are $\mathsf{Term}(R_U)$.

$$\begin{array}{ll}
\mathsf{Term}(0) = \emptyset & \mathsf{Term}(P \mid Q) = \mathsf{Term}(P) \cup \mathsf{Term}(Q) \\
\mathsf{Term}(!P) = \mathsf{Term}(P) & \mathsf{Term}(\nu \mathtt{n}.P) = \{\mathtt{n}\} \cup \mathsf{Term}(P) \\
\mathsf{Term}(\mathsf{in}(v, x).P) = \{x\} \cup \mathsf{Term}(P) & \mathsf{Term}(\mathsf{out}(v, M).P) = \{M\} \cup \mathsf{Term}(P) \\
\multicolumn{2}{l}{\mathsf{Term}(\mathit{if}\ M =_E N\ \mathit{then}\ P\ \mathit{else}\ Q) = \mathsf{Term}(P) \cup \mathsf{Term}(Q)}
\end{array}$$

Thus, a collaboration can be specified as a specification defined as follows.

Definition 3 (collaboration specification). *A* collaboration specification *of a process R_U is a tuple $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle$. $\Psi \subseteq \mathsf{Term}(R_U)$ denotes the set of terms sent to the adversary each of which is of base type, $\Phi \subseteq \mathsf{Term}(R_U)$ represents terms to be replaced by information provided by the adversary, c_{out} is a fresh channel for sending information to the adversary, and c_{in} is a fresh channel for reading information from the adversary, i.e., $\mathsf{c}_{out}, \mathsf{c}_{in} \notin \mathsf{fn}(R_U) \cup \mathsf{bn}(R_U)$.*

Given a plain process R_U and a collaboration specification $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle$ of the process, the transformation of R_U is given by $R_U^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}$.

Definition 4 (collaboration behaviour). *Let R_U be a plain process, and $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle$ be a collaboration specification of R_U. Collaboration behaviour of R_U according to $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle$ is defined as:*

- $0^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle} \triangleq 0$,
- $(P \mid Q)^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle} \triangleq P^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle} \mid Q^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}$,
- $(!P)^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle} \triangleq !P^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}$,
- $(\nu \mathtt{n}.P)^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle} \triangleq \begin{cases} \nu \mathtt{n}.\mathsf{out}(\mathsf{c}_{out}, \mathtt{n}).P^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle} & \mathit{if}\ \mathtt{n} \in \Psi, \\ \nu \mathtt{n}.P^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle} & \mathit{otherwise}, \end{cases}$
- $(\mathsf{in}(v, x).P)^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle} \triangleq \begin{cases} \mathsf{in}(v, x).\mathsf{out}(\mathsf{c}_{out}, x).P^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle} & \mathit{if}\ x \in \Psi, \\ \mathsf{in}(v, x).P^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle} & \mathit{otherwise}, \end{cases}$
- $(\mathsf{out}(v, M).P)^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle} \triangleq \begin{cases} \mathsf{in}(\mathsf{c}_{in}, x).\mathsf{out}(v, x).P^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle} & \mathit{if}\ M \in \Phi \\ \qquad \wedge \mathsf{c}_{in} \neq \bot,\ \mathit{where}\ x\ \mathit{is\ a\ fresh\ variable}, & \\ \mathsf{out}(v, M).P^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle} & \mathit{otherwise}, \end{cases}$
- $(\mathit{if}\ M =_E N\ \mathit{then}\ P\ \mathit{else}\ Q)^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle} \triangleq$

$$\begin{cases} \mathsf{in}(\mathsf{c}_{in}, x).\mathit{if}\ x = \mathsf{true}\ \mathit{then}\ P^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\ \mathit{else}\ Q^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle} & \mathit{if}\ \mathsf{c}_{in} \neq \bot, \\ \qquad \mathit{where}\ x\ \mathit{is\ a\ fresh\ variable\ and}\ \mathsf{true}\ \mathit{is\ a\ constant}, & \\ \mathit{if}\ M =_E N\ \mathit{then}\ P^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\ \mathit{else}\ Q^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle} & \mathit{otherwise}. \end{cases}$$

Note that we use $\mathsf{c}_{in} = \bot$ to denote that the adversary neither prepares information for the coerced users nor controls the conditional evaluations of the users. We only specify user behaviour in a collaboration with the adversary. The adversary's behaviour may be omitted, as in the applied pi calculus the adversary is considered as the environment and does not need to be explicitly modelled. Our approach to reasoning about the adversary's behaviour in a collaboration (e.g., enforcing a voter to cast a particular vote) follows the line of the definition of coercion-resistance in [10]. Namely, a context $\mathcal{C}[\_] = \nu \mathsf{c}_{out}.\nu \mathsf{c}_{in}(\_ \mid Q)$ models a specific way of collaboration of the adversary, where Q models the adversary's behaviour in the context. In this way, we separate the adversary's behaviour of distinguishing two processes, which is modelled by the environment, from the behaviour of collaborating with users which is modelled by the context.

3.5 Modelling User Coalitions

To define coalition privacy properties, we need to formally define a *coalition* between a target user and a set of defending third parties. The notion collaboration from the previous section cannot be adopted directly, as it does not specify the adversary's behaviour, whereas a coalition must specify the behaviour of *all* involved users.

Given a set of users $R_U = R_{u_1} \mid \cdots \mid R_{u_m}$, a coalition of the users specifies communication between (potentially) each pair of users. For every communication, a coalition specification needs to make explicit who the sender and receiver are (unlike collaboration). Similar to the specification of collaboration, a coalition specification makes explicit which data is sent on which channel. To make the behaviour of both communicating parties explicit, we need to specify how the term in a communication is referred to in the receiver's process. A communication in a coalition is specified as a tuple $\langle R_{u_i}, R_{u_j}, M, \mathsf{c}, y\rangle$ where $R_{u_i}, R_{u_j} \in \{R_{u_1}, \ldots, R_{u_m}\}$ $(R_{u_i} \neq R_{u_j})$ are the sender and receiver process, respectively; $M \in \mathsf{Term}(R_{u_i})$ is the data sent in the communication; $\mathsf{c} \notin \mathsf{fn}(R_U) \cup \mathsf{bn}(R_U)$ is a fresh channel used in the communication; $y \notin \mathsf{fv}(R_U) \cup \mathsf{bv}(R_U)$ is the variable used by the receiver to refer to the term M. A coalition specifies a set of communications of this type (denoted as Θ). For the simplicity of modelling, we assume that for each communication, the coalition uses a distinct channel and distinct variable, i.e., $\forall\ \langle R_{u_i}, R_{u_j}, M, \mathsf{c}, y\rangle \in \Theta$ and $\langle R'_{u_i}, R'_{u_j}, M', \mathsf{c}', y'\rangle \in \Theta$ we have $\mathsf{c} \neq \mathsf{c}' \wedge y \neq y'$.

A coalition specifies a set of terms which are communicated by the originating user process and are replaced in the coalition. In addition, a coalition needs to define how a term is replaced. In a collaboration, the adversary is assumed to be able to compute and prepare this, but in a coalition, no user can compute and prepare information for other users. Thus, this ability has to be explicitly specified in a coalition as a set of substitutions $\Delta = \{\{N/M\} \mid M \in \mathsf{Term}(R_U)\}$. The new term N are calculated from a set of terms $N_1, \ldots, N_n$ which are generated by the user, read in by the original process, or read in from coalition members. A successful coalition requires that there are no such situations where N cannot be calculated in the user process when M needs to be replaced.

Moreover, in a coalition, we allow the coalition to decide values of conditional evaluations (similar to collaboration, where the adversary decides this). Since no user in a coalition has the ability to specify the values of evaluations, these need to be assigned specifically. In addition, to add more flexibility, we allow a coalition to specify which evaluations are decided by the coalition and which are not. The evaluations of a plain user process R_U is $\mathsf{Eval}(R_U)$. The assignments of evaluations are specified as a set $\Pi \subseteq \{(e, b) \mid e \in \mathsf{Eval}(R_U) \wedge b \in \{\mathsf{true}, \mathsf{false}\}\}$.

$$\begin{array}{ll}
\mathsf{Eval}(0) = \emptyset & \mathsf{Eval}(P \mid Q) = \mathsf{Eval}(P) \cup \mathsf{Eval}(Q) \\
\mathsf{Eval}(!P) = \mathsf{Eval}(P) & \mathsf{Eval}(\nu \mathsf{n}.P) = \mathsf{Eval}(P) \\
\mathsf{Eval}(\mathsf{in}(v, x).P) = \mathsf{Eval}(P) & \mathsf{Eval}(\mathsf{out}(v, M).P) = \mathsf{Eval}(P) \\
\multicolumn{2}{l}{\mathsf{Eval}(\mathit{if}\ M =_E N\ \mathit{then}\ P\ \mathit{else}\ Q) = \{M =_E N\} \cup \mathsf{Eval}(P) \cup \mathsf{Eval}(Q)}
\end{array}$$

Definition 5 (coalition specification). *A coalition*[2] *of a set of users R_U is specified as a tuple $\langle \Theta, \Delta, \Pi \rangle$ where Θ is a set of communication, Δ is a set of substitutions and Π is an assignment for a set of evaluations.*

With the above setting, given a set of users R_U and a coalition specification $\langle \Theta, \Delta, \Pi \rangle$ on users, the behaviour of a user in the coalition is modelled as a coalition transformation of the user's original process, as defined in Def. 6.

In the definition, process $\mathsf{in}(\mathsf{c}_1, y'_1).!\mathsf{out}(\mathsf{c}'_1, y'_1) \mid \cdots \mid \mathsf{in}(\mathsf{c}_\ell, y'_\ell).!\mathsf{out}(\mathsf{c}'_\ell, y'_\ell)$ models the receiving behaviour of process R in the coalition. The coalition specifies which channel is use to receive data. The received data on a channel are referred to as a distinct fresh variable. The received data is sent out over a distinct private channel. The association of channels and variables is modelled in ξ. This sending behaviour is used for the process $R^{\langle \Gamma, \Delta, \Pi \rangle}$ to read the data when it is needed. Process $R^{\langle \Gamma, \Delta, \Pi \rangle}$ models the sending behaviour, substitution of terms, assignments of evaluations. F captures the variables which are in $\{y_1, \ldots, y_\ell\}$ and has not been read in yet.

Definition 6 (coalition behaviour). *Let $R_U = R_{u_1} \mid \cdots \mid R_{u_m}$ be a plain process of a set of users, $\langle \Theta, \Delta, \Pi \rangle$ be a coalition specification of process R_U, $R \in \{R_{u_1}, \cdots, R_{u_m}\}$ be a plain user process, the transformation of the process R in the coalition is given by $R^{\langle \Theta, \Delta, \Pi \rangle}$:*

$$R^{\langle \Theta, \Delta, \Pi \rangle} = \nu \eta.(R^{\langle \Gamma, \Delta, \Pi \rangle} \mid \mathsf{in}(\mathsf{c}_1, y'_1).!\mathsf{out}(\mathsf{c}'_1, y'_1) \mid \cdots \mid \mathsf{in}(\mathsf{c}_\ell, y'_\ell).!\mathsf{out}(\mathsf{c}'_\ell, y'_\ell))$$

where $\Gamma = \{\langle R, R_{u_j}, M, \mathsf{c}, y \rangle \mid \langle R, R_{u_j}, M, \mathsf{c}, y \rangle \in \Theta\}$, $\eta = \{\mathsf{c}'_1, \ldots, \mathsf{c}'_\ell\}$, c'_1, $\ldots$, c'_ℓ are fresh, $\{\mathsf{c}_1, \ldots, \mathsf{c}_\ell\} = \{\mathsf{c} \mid \langle R_{u_i}, R, M, \mathsf{c}, y \rangle \in \Theta\}$, $y'_1, \ldots, y'_\ell$ are fresh variables, $\xi = \{(\mathsf{c}_1, y'_1, \mathsf{c}'_1), \ldots, (\mathsf{c}_\ell, y'_\ell, \mathsf{c}'_\ell)\}$ defines the association of channels and variables in process $\mathsf{in}(\mathsf{c}_1, y'_1).!\mathsf{out}(\mathsf{c}'_1, y'_1) \mid \cdots \mid \mathsf{in}(\mathsf{c}_\ell, y'_\ell).!\mathsf{out}(\mathsf{c}'_\ell, y'_\ell)$, and

[2] This model does not include the coalition strategies in which the target users and defending third parties are able to generate new data, initiate new sessions, establishing new secrets, etc.

$R^{\langle \Gamma,\Delta,\Pi\rangle}$ *is given by:*

- $0_F^{\langle \Gamma,\Delta,\Pi\rangle} \;\hat{=}\; 0,$
- $(P \mid Q)_F^{\langle \Gamma,\Delta,\Pi\rangle} \;\hat{=}\; P_F^{\langle \Gamma,\Delta,\Pi\rangle} \mid Q_F^{\langle \Gamma,\Delta,\Pi\rangle},$
- $(!P)_F^{\langle \Gamma,\Delta,\Pi\rangle} \;\hat{=}\; !P_F^{\langle \Gamma,\Delta,\Pi\rangle},$
- $(\nu \mathtt{n}.P)_F^{\langle \Gamma,\Delta,\Pi\rangle} \;\hat{=}\; \begin{cases} \nu \mathtt{n}.\mathsf{out}(\mathtt{c}_1,\mathtt{n}).\ldots.\mathsf{out}(\mathtt{c}_\ell,\mathtt{n}).P_F^{\langle \Gamma,\Delta,\Pi\rangle} \\ \quad \textit{if } \{\mathtt{c}_1,\ldots,\mathtt{c}_\ell\} = \{\mathtt{c} \mid \langle R, R_{u_j}, \mathtt{n}, \mathtt{c}, y\rangle \in \Gamma\}, \\ \nu \mathtt{n}.P_F^{\langle \Gamma,\Delta,\Pi\rangle} \quad \textit{otherwise,} \end{cases}$
- $(\mathsf{in}(v,x).P)_F^{\langle \Gamma,\Delta,\Pi\rangle} \;\hat{=}\; \begin{cases} \mathsf{in}(v,x).\mathsf{out}(\mathtt{c}_1,x).\ldots.\mathsf{out}(\mathtt{c}_\ell,x).P_F^{\langle \Gamma,\Delta,\Pi\rangle} \\ \quad \textit{if } \{\mathtt{c}_1,\ldots,\mathtt{c}_\ell\} = \{\mathtt{c} \mid \langle R, R_{u_j}, x, \mathtt{c}, y\rangle \in \Gamma\}, \\ \mathsf{in}(v,x).P_F^{\langle \Gamma,\Delta,\Pi\rangle} \quad \textit{otherwise,} \end{cases}$
- $(\mathsf{out}(v,M).P)_F^{\langle \Gamma,\Delta,\Pi\rangle} \;\hat{=}\; \begin{cases} \mathsf{in}(\mathtt{c}'_1,y_1).\cdots.\mathsf{in}(\mathtt{c}'_\ell,y_\ell).\mathsf{out}(v,N).P_{F\setminus\{y_1,\ldots,y_\ell\}}^{\langle \Gamma,\Delta,\Pi\rangle} \\ \quad \textit{if } \{N/M\} \in \Delta, \{y_1,\ldots,y_\ell\} \subseteq F \cup \mathsf{Var}(N), \\ \qquad \forall i \in \{1,\ldots,\ell\}, \\ \qquad \langle R_i, R, \mathtt{c}_i M, y_i\rangle \in \Theta \wedge (\mathtt{c}_i, y'_i, \mathtt{c}'_i) \in \xi, \\ \mathsf{out}(v,M).P_F^{\langle \Gamma,\Delta,\Pi\rangle} \quad \textit{otherwise,} \end{cases}$
- $(\textit{if } M =_E N \textit{ then } P \textit{ else } Q)_F^{\langle \Gamma,\Delta,\Pi\rangle} \;\hat{=}$

$$\begin{cases} P_F^{\langle \Gamma,\Delta,\Pi\rangle} & \textit{if } (M =_E N, \mathsf{true}) \in \Pi, \\ Q_F^{\langle \Gamma,\Delta,\Pi\rangle} & \textit{if } (M =_E N, \mathsf{false}) \in \Pi, \\ \textit{if } M =_E N \textit{ then } P_F^{\langle \Gamma,\Delta,\Pi\rangle} \textit{ else } Q_F^{\langle \Gamma,\Delta,\Pi\rangle} & \textit{otherwise.} \end{cases}$$

with F *initially equals to* $\{y_1,\ldots,y_\ell \mid \langle R_{u_i}, R, M, \mathtt{c}, y\rangle \in \Theta\}$.

Given a set of users R_U and a coalition specification $\langle \Theta, \Delta, \Pi\rangle$ for them, the coalition is now modelled as $R_U^{\langle \Theta,\Delta,\Pi\rangle} = \nu\Omega.(R_{u_1}^{\langle \Theta,\Delta,\Pi\rangle} \mid \cdots \mid R_{u_m}^{\langle \Theta,\Delta,\Pi\rangle})$ where $\Omega = \{\mathtt{c} \mid \langle R_{u_i}, R_{u_j}, M, \mathtt{c}, y\rangle \in \Theta\}$.

4 Formalising the Privacy Notions

4.1 Enforced-privacy

Enforced-privacy is the adversary's unlinkability of a target user to his data even when the user collaborates with the adversary. Different collaborations impact privacy differently, so when we say a protocol satisfies enforced-privacy, it always refers to a specific collaboration specification.

Similar as in receipt-freeness and coercion-resistance [10], when a protocol P_w satisfies enforced-privacy w.r.t. a target data τ (which belongs to role R_i) and a collaboration specification $\langle \Psi, \Phi, \mathtt{c}_{out}, \mathtt{c}_{in}\rangle$ defined on process $\hat{R}_i$ (where $R_i = \nu \mathtt{id}_i.\nu\tau.\hat{R}_i$), there exists a process P_f for the target user to execute, such that the adversary cannot distinguish between real collaboration with $\tau = \mathtt{t}_1$ and fake collaboration (by means of process P_f) with $\tau = \mathtt{t}_2$.[3]

[3] In the epistemic notion of coercion-resistance, enforced-privacy can be defined as the existence of a *counter-strategy* for the target user to achieve his own goal, but the adversary cannot distinguish it from the target user following the adversary's instructions [26].

Definition 7. *A well-formed protocol P_w satisfies enforced-privacy (*epriv*) w.r.t. target data τ and collaboration specification $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle$, if there exists a closed plain process P_f, such that for any context $\mathcal{C}[\_] = \nu \mathsf{c}_{out}.\nu \mathsf{c}_{in}.(\_ \mid Q)$ satisfying $\mathsf{bn}(P_w) \cap \mathsf{fn}(\mathcal{C}[\_]) = \emptyset$ and $C_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}]] \approx_\ell C_{P_w}[\hat{R}_i^{\langle \Psi, \emptyset, \mathsf{c}'_{out}, \perp \rangle}\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\}]$, we have*

1. $\mathcal{C}[P_f]^{\backslash(\mathsf{c}'_{out}, \cdot)} \approx_\ell \hat{R}_i\{\mathsf{id}/id_i, \mathsf{t}_2/\tau\}$,
2. $C_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}]] \approx_\ell C_{P_w}[\mathcal{C}[P_f]]$,

where $\tau \in \mathsf{bn}(R_i)$, $R_i = \nu \mathsf{id}_i.\nu\tau.\hat{R}_i$, $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle$ is defined on $\hat{R}_i$, t is a free name representing a piece of data, and $\mathcal{C}[P_f]^{\backslash(\mathsf{c}'_{out}, \cdot)} = \nu \mathsf{c}'_{out}.(\mathcal{C}[P_f] \mid !\mathsf{in}(\mathsf{c}'_{out}, x))$.

The process $\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}$ models the behaviour of the collaborating target user. The behaviour of the adversary in the collaboration is implicitly modelled as Q in the context $\mathcal{C}[\_] = \nu \mathsf{c}_{out}.\nu \mathsf{c}_{in}.(\_ \mid Q)$. Thus a specific collaboration is modelled as $\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}]$. Note that sometimes the target data in the collaboration is not decided by $\{t/\tau\}$, but by the context $\mathcal{C}[\_]$. The target data is actually instantiated by $C_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}]] \approx_\ell C_{P_w}[\hat{R}_i^{\langle \Psi, \emptyset, \mathsf{c}'_{out}, \perp \rangle}\{\mathsf{id}/id_i, \mathsf{t}_1/\tau\}]$. The first equivalence shows that even if the context $\mathcal{C}[\_]$ is able to decide the target data, the target user can still actually instantiate the target data with t_2 by executing the process P_f. The second equivalence shows that the adversary cannot distinguish the target user following the collaboration in process $\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}$ from executing the process P_f, in the context of the adversary collaboration $\mathcal{C}[\_]$.

4.2 Independency-of-privacy

Next, we account for attacking third parties. As different sets of third parties may differently influence the target user's privacy, and since different collaboration amongst the same third parties leads to different privacy properties, independency-of-privacy is defined with respect to a set of third parties and a collaboration specification between them and the adversary.

Definition 8 (third parties). *Given a well-formed protocol P_w and an instance of the target user $\hat{R}_i\{\mathsf{id}/id, t/\tau\}$, a set of third parties is defined as a set of users $R_U = R_{u_1} \mid \cdots \mid R_{u_m}$ where $\forall i \in \{1, \cdots, m\}, R_{u_i} \neq \hat{R}_i\{\mathsf{id}/id, t/\tau\}$. We use R_T to denote a set of attacking third parties and R_D to denote a set of defending third parties.*

The collaboration between a set of attacking third parties R_T and the adversary is expressed as a collaboration specification $\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in} \rangle$ defined on process R_T. The behaviour of the third parties in the collaboration is modelled as $R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in} \rangle}$. Inspired by the domain-specific formal definitions, vote-independence [14] in e-voting and independency-of-prescribing-privacy [12] in e-health, independency-of-privacy is defined as follows: a well-formed protocol P_w

satisfies independency-of-privacy w.r.t. $(R_T, \langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle)$ and $\tau \in \mathsf{bn}(R_i)$, if the adversary cannot distinguish the honest target user executing role R_i with $\tau = \mathtt{t}_1$ from the same user with $\tau = \mathtt{t}_2$, even when the set of third parties R_T collaborates with the adversary according to collaboration specification $\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle$.

Definition 9. *A well-formed protocol P_w satisfies independency-of-privacy (*ipriv*) w.r.t. data τ and attacking third parties $(R_T, \langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle)$ if*

$$C_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\} \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}] \approx_\ell C_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}],$$

where $\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle$ is a collaboration specification of process R_T.

If the equivalence holds, then despite this collaboration, adversary cannot distinguish $\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\}$ in which the target user uses $\tau = \mathtt{t}_1$ from $\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\}$ in which the target user uses $\tau = \mathtt{t}_2$.

4.3 Independency-of-enforced-privacy

We define independency-of-enforced-privacy (iepriv) based on epriv in a similar fashion as ipriv. More precisely, iepriv of a protocol P_w is defined w.r.t. target data $\tau \in \mathsf{bn}(R_i)$, a collaboration specification $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle$ defined on process $\hat{R}_i$ with $R_i = \nu \mathsf{id}_i.\nu\tau.\hat{R}_i$, and a set of attacking third parties together with a collaboration specification defined on the third parties processes $(R_T, \langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle)$. A well-formed protocol P_w satisfies iepriv w.r.t. τ, $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle$, and $(R_T, \langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle)$, if there exists a closed plain process P_f for the target user to execute, such that, despite the help of third parties R_T according to $\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle$, the adversary cannot distinguish between the target user collaborating with $\tau = \mathtt{t}_1$, and him really using $\tau = \mathtt{t}_2$ but faking collaboration for $\tau = \mathtt{t}_1$ by P_f.

Definition 10. *A well-formed protocol P_w satisfies independency-of-enforced-privacy (*iepriv*) w.r.t. τ, $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle$, and $(R_T, \langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle)$, if there exists a closed plain process P_f, such that for any $\mathcal{C}[\_] = \nu \mathsf{c}_{out}.\nu \mathsf{c}_{in}.(\_ \mid Q)$ satisfying $\mathsf{bn}(P_w) \cap \mathsf{fn}(\mathcal{C}[\_]) = \emptyset$ and $C_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_T] \approx_\ell C_{P_w}[\hat{R}_i^{\langle \Psi, \emptyset, \mathsf{c}'_{out}, \bot\rangle}\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\} \mid R_T]$, we have*

1. $\mathcal{C}[P_f]^{\setminus(\mathsf{c}'_{out}, \cdot)} \approx_\ell \hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\}$,
2. $C_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}] \approx_\ell C_{P_w}[\mathcal{C}[P_f] \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}]$,

where $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in}\rangle$ is a collaboration specification for target user process $\hat{R}_i$, and $\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle$ is a collaboration specification of third party process R_T.

This formalisation adds third parties collaboration $R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in}\rangle}$ to Def. 7.

4.4 Coalition Privacy Properties

Corresponding to each privacy property defined above, we define coalition privacy properties which take into account defending third parties.

Definition 11 (defensive coalition). *Given an instance of the target user* $\hat{R}_i\{\mathsf{id}/id, t/\tau\}$*, a set of defending third parties* R_D*, and a coalition specification* $\langle \Theta, \Delta, \Pi \rangle$ *defined on* $(\hat{R}_i\{\mathsf{id}/id, t/\tau\} \mid R_D)$*, the coalition is modelled as* $\nu\Omega.(\hat{R}_i\{\mathsf{id}/id, t/\tau\} \mid R_D)^{\langle \Theta, \Delta, \Pi \rangle}$*, where* $\Omega = \{\mathsf{c} \mid \langle R_{u_i}, R_{u_j}, M, \mathsf{c}, y \rangle \in \Theta\}$*. The target user's behaviour in the coalition is* $\hat{R}_i\{\mathsf{id}/id, t/\tau\}^{\langle \Theta, \Delta, \Pi \rangle} = \nu\eta.((\hat{R}_i\{\mathsf{id}/id, t/\tau\})^{\langle \Gamma, \Delta, \Pi \rangle} | P_\gamma)$*, where* η *is a set of fresh channels* $\{\mathsf{c}'_i, \ldots, \mathsf{c}'_\ell\}$*,* $\Gamma = \{\langle \hat{R}_i\{\mathsf{id}/id, t/\tau\}, R_{u_j}, M, \mathsf{c}, y \rangle \mid \langle \hat{R}_i\{\mathsf{id}/id, t/\tau\}, R_{u_j}, M, \mathsf{c}, y \rangle \in \Theta\}$*, and* $P_\gamma = \mathsf{in}(\mathsf{c}_1, y'_1).!\mathsf{out}(\mathsf{c}'_1, y'_1) \mid \cdots \mid \mathsf{in}(\mathsf{c}_\ell, y'_\ell).!\mathsf{out}(\mathsf{c}'_\ell, y'_\ell)$ *with* $\{y'_1, \ldots, y'_\ell\}$ *being fresh variables, and* $\{(\mathsf{c}_1, \ldots, \mathsf{c}_\ell\} = \{\mathsf{c} \mid \langle R_{u_i}, \hat{R}_i\{\mathsf{id}/id, t/\tau\}, M, \mathsf{c}, y \rangle \in \Theta\}$*. The third parties' behaviour in the coalition is* $R_D^{\langle \Theta, \Delta, \Pi \rangle}$*.*

Coalition-privacy. Intuitively, coalition-privacy means that a target user's privacy is preserved due to the cooperation of a set of defending third parties. A well-formed protocol P_w satisfies coalition-privacy w.r.t. $\tau \in \mathsf{bn}(R_i)$ and $(R_D, \langle \Theta, \Delta, \Pi \rangle)$ ($\langle \Theta, \Delta, \Pi \rangle$ is defined on $\hat{R}_i \mid R_D$, where $R_i = \nu \mathtt{id}_i.\nu\tau.\hat{R}_i$), if the adversary cannot distinguish an honest user in role R_i using $\tau = \mathtt{t}_1$ from the user actually using $\tau = \mathtt{t}_2$ while helped by a set of defending third parties.

Definition 12. *A well-formed protocol* P_w *satisfies coalition-privacy (*cpriv*) w.r.t. data* τ *and coalition* $(R_D, \langle \Theta, \Delta, \Pi \rangle)$ *if* $C_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\} \mid R_D] \approx_\ell C_{P_w}[\nu\Omega.(\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_D)^{\langle \Theta, \Delta, \Pi \rangle}]$*, where* $\langle \Theta, \Delta, \Pi \rangle$ *is a coalition specification defined on* $\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_D$*.*

In the definition, the coalition is modelled as $\nu\Omega.(\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_D)^{\langle \Theta, \Delta, \Pi \rangle}$, where the target user instantiates the target data with $\mathtt{t}_2$. The equivalence shows that the adversary cannot distinguish the target user instantiating the target data with $\mathtt{t}_2$ in the coalition from the target user instantiating the target data with $\mathtt{t}_1$. In this way, coalition-privacy ensures the target user's privacy when there exists a set of third parties cooperating with him following a pre-defined coalition specification.

Coalition-enforced-privacy. Taking into account defending third parties, we define coalition-enforced-privacy based on enforced-privacy. As before, coalition-enforced-privacy specifies a target data τ and a collaboration specification of the target user $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle$. As in coalition-privacy, coalition-enforced-privacy specifies a set of defending third parties R_D and a coalition specification $\langle \Theta, \Delta, \Pi \rangle$. In coalition-enforced-privacy, the target user both cooperates with the adversary and defending third parties. Similar to enforced-privacy, we assume that the target user lies to the adversary if possible. We do not assume that the target user lies to the defending third parties, as they help the target user maintain privacy.

Intuitively, coalition-enforced-privacy means that a target user is able to lie to the adversary about his target data when helped by defending third parties – the adversary cannot tell whether the user lied. This property is modelled as the combination of coalition-privacy and enforced-privacy: a protocol

P_w satisfies coalition-enforced-privacy w.r.t $\tau \in \mathsf{bn}(R_i), \langle \Psi, \Phi, \mathtt{c}_{out}, \mathtt{c}_{in} \rangle$ and $(R_D, \langle \Theta, \Delta, \Pi \rangle)$, for $\langle \Psi, \Phi, \mathtt{c}_{out}, \mathtt{c}_{in} \rangle$ a collaboration specification defined on $\hat{R}_i$ with $R_i = \nu \mathtt{id}_i.\nu\tau.\hat{R}_i$, and $\langle \Theta, \Delta, \Pi \rangle$ a coalition specification defined on the target user and R_D, if there exists a process P_f, such that the adversary cannot distinguish between genuine collaboration with $\tau = \mathtt{t}_1$ and faking collaboration using P_f with the help of the coalition for $\tau = \mathtt{t}_2$.

Definition 13. *A well-formed protocol P_w satisfies coalition-enforced-privacy (*cepriv*) w.r.t. data τ, $\langle \Psi, \Phi, \mathtt{c}_{out}, \mathtt{c}_{in} \rangle$ and $(R_D, \langle \Theta, \Delta, \Pi \rangle)$, if there exists a closed plain process P_f, such that for any $\mathcal{C}[\_] = \nu \mathtt{c}_{out}.\nu \mathtt{c}_{in}.(\_ \mid Q)$ satisfying $\mathsf{bn}(P_w) \cap \mathsf{fn}(\mathcal{C}[\_]) = \emptyset$ and $C_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathtt{c}_{out}, \mathtt{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_D] \approx_\ell C_{P_w}[\hat{R}_i^{\langle \Psi, \emptyset, \mathtt{c}'_{out}, \bot \rangle}\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\} \mid R_D]$, we have*

1. $\nu\Omega.(\nu\eta.(\mathcal{C}[P_f]^{\setminus(\mathtt{c}'_{out}, \cdot)} \mid P_\gamma) \mid R_D^{\langle \Theta, \Delta, \Pi \rangle}) \approx_\ell \nu\Omega.(\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_D)^{\langle \Theta, \Delta, \Pi \rangle}$,
2. $C_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathtt{c}_{out}, \mathtt{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_D] \approx_\ell C_{P_w}[\nu\Omega.(\nu\eta.(\mathcal{C}[P_f] \mid P_\gamma) \mid R_D^{\langle \Theta, \Delta, \Pi \rangle})]$,

where Ω, η, P_γ are defined in Def. 11, $\langle \Psi, \Phi, \mathtt{c}_{out}, \mathtt{c}_{in} \rangle$ is defined on $\hat{R}_i$, $\langle \Theta, \Delta, \Pi \rangle$ is a coalition specification defined on $\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_D$.

The collaboration between the target user and the adversary instantiating the target data with $\mathtt{t}_1$ is modelled by $C_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathtt{c}_{out}, \mathtt{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_D] \approx_\ell C_{P_w}[\hat{R}_i^{\langle \Psi, \emptyset, \mathtt{c}'_{out}, \bot \rangle}\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\} \mid R_D]$. The target user's actual behaviour of instantiating the target data with $\mathtt{t}_2$ in process P_f is modelled as the first equivalence. The second equivalence shows that the adversary cannot distinguish the target user following the collaboration with the adversary from the target user lying to the adversary with the help of defending third parties.

Coalition-independency-of-privacy. Similarly, we define the privacy notion of coalition-independency-of-privacy with respect to a target data τ, a set of attacking third parties with a collaboration specification $(R_T, \langle \Psi^t, \Phi^t, \mathtt{c}^t_{out}, \mathtt{c}^t_{in} \rangle)$, and a set of defending third parties R_D with a coalition specification $\langle \Theta, \Delta, \Pi \rangle$. Note that we require that there is no intersection between attacking third parties and defending third parties, i.e., $R_T \cap R_D = \emptyset$, as we assume a third party cannot be both attacking and defending at the same time. A well-formed protocol P_w satisfies coalition-independency-of-privacy w.r.t. τ, $(R_T, \langle \Psi^t, \Phi^t, \mathtt{c}^t_{out}, \mathtt{c}^t_{in} \rangle)$ and $(R_D, \langle \Theta, \Delta, \Pi \rangle)$, if the adversary, even with the collaboration of a set of attacking third parties, cannot distinguish the target user instantiating $\tau = \mathtt{t}_1$ from the target user actually instantiating $\tau = \mathtt{t}_2$ in the coalition with the help of defending third parties.

Definition 14. *A well-formed protocol P_w satisfies coalition-independency-of-privacy (*cipriv*) w.r.t. data τ, $(R_T, \langle \Psi^t, \Phi^t, \mathtt{c}^t_{out}, \mathtt{c}^t_{in} \rangle)$, and $(R_D, \langle \Theta, \Delta, \Pi \rangle)$, if*

$$C_{P_w}[\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\} \mid R_D \mid R_T^{\langle \Psi^t, \Phi^t, \mathtt{c}^t_{out}, \mathtt{c}^t_{in} \rangle}] \approx_\ell C_{P_w}[\nu\Omega.((\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_D)^{\langle \Theta, \Delta, \Pi \rangle}) \mid R_T^{\langle \Psi^t, \Phi^t, \mathtt{c}^t_{out}, \mathtt{c}^t_{in} \rangle}],$$

where $\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in} \rangle$ *is a collaboration specification of process* R_T, $\langle \Theta, \Delta, \Pi \rangle$ *is a coalition specification defined on* $\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_D$.

Coalition-independency-of-enforced-privacy. Finally, we consider the case combining all situations together: the target user collaborates with the adversary following $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle$, a set of attacking third parties R_T collaborate with the adversary following $\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in} \rangle$, and a set of defending third parties R_D and a coalition $\langle \Theta, \Delta, \Pi \rangle$). We formally define the property as follows.

Definition 15. *A well-formed protocol* P_w *satisfies coalition-independency-of-enforced-privacy (*ciepriv*) w.r.t.* τ, $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle$, $(R_T, \langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in} \rangle)$, $(R_D, \langle \Theta, \Delta, \Pi \rangle)$, *if there exists a closed plain process* P_f *such that for any context* $\mathcal{C}[\_] = \nu \mathsf{c}_{out}.\nu \mathsf{c}_{in}.(\_ \mid Q)$ *satisfying* $\mathsf{bn}(P_w) \cap \mathsf{fn}(\mathcal{C}[\_]) = \emptyset$ *and* $C_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_T \mid R_D] \approx_\ell C_{P_w}[\hat{R}_i^{\langle \Psi, \emptyset, \mathsf{c}'_{out}, \bot \rangle}\{\mathsf{id}/id_i, \mathtt{t}_1/\tau\} \mid R_T \mid R_D]$, *we have*

1. $\nu\Omega.(\nu\eta.(\mathcal{C}[P_f]^{\setminus(\mathsf{c}'_{out}, \cdot)} \mid P_\gamma) \mid R_D^{\langle \Theta, \Delta, \Pi \rangle}) \approx_\ell \nu\Omega.((\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} | R_D)^{\langle \Theta, \Delta, \Pi \rangle})$,
2. $C_{P_w}[\mathcal{C}[\hat{R}_i^{\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle}\{\mathsf{id}/id_i, t/\tau\}] \mid R_D \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in} \rangle}]$
$\approx_\ell C_{P_w}[\nu\Omega.(\nu\eta.(\mathcal{C}[P_f] \mid P_\gamma) \mid R_D^{\langle \Theta, \Delta, \Pi \rangle}) \mid R_T^{\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in} \rangle}]$,

where Ω, η, P_γ *are defined in Def. 11,* $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle$ *is a collaboration specification defined on* $\hat{R}_i$, $\langle \Psi^t, \Phi^t, \mathsf{c}^t_{out}, \mathsf{c}^t_{in} \rangle$ *is a collaboration specification defined on* R_T, $\langle \Theta, \Delta, \Pi \rangle$ *is a coalition specification defined on* $\hat{R}_i\{\mathsf{id}/id_i, \mathtt{t}_2/\tau\} \mid R_D$.

Remark. As certain coalitions may fail to maintain privacy, the coalition privacy properties can be generalised by requiring the existence of a successful coalition. The general version of coalition privacy properties allows us to reason about the existence of a coalition such that a user's privacy is preserved. How to find such a coalition is an interesting topic for studying coalition privacy properties. Each property defined in the above can be instantiated in many different forms by specifying the parameters of the property (such as target data, collaboration, coalition). Furthermore, only the target user is allowed to lie to the adversary – we do not consider lying third parties. Properties, ipriv, iepriv, cipriv and ciepriv, can be extended by allowing third parties to lie. For details, see [27].

5 Relations between the Privacy Notions

We show the relations between the privacy properties in Fig. 2: ρ specifies a collaboration of the target user with the adversary, θ specifies a set of attacking third parties and their collaboration with the adversary, and δ specifies a set of defending third parties and their coalition with the target user.

The left diamond in Fig. 2 shows the relations between privacy properties which do not consider defending third parties while the right diamond shows the relations between privacy properties which consider defending third parties. In the left diamond, epriv_ρ and ipriv_θ are stronger than priv, meaning that if

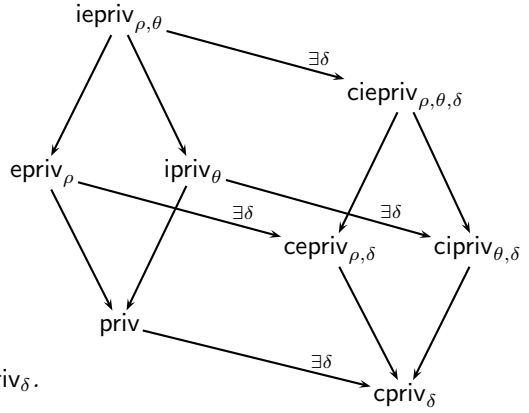
a protocol satisfies epriv_ρ or ipriv_θ, then the protocol satisfies priv. Intuitively, if the adversary cannot break privacy with the help from the target user (in epriv_ρ) or from a set of attacking third parties (in ipriv_θ), the adversary cannot break privacy without any help (in priv). Similarly, if the adversary cannot break privacy with the help from both target user and attacking third parties (in $\mathsf{iepriv}_{\rho,\theta}$), the adversary cannot break privacy with the help from only one of them (in epriv_ρ and ipriv_θ). Thus, $\mathsf{iepriv}_{\rho,\theta}$ is stronger than both enforced-privacy$_\rho$ and ipriv_θ. This is described as Thm. 1. Similar reasoning holds in the right diamond as described in Thm. 2. Each privacy property in the left diamond has a weaker corresponding property in the right diamond, meaning that if a protocol satisfies a privacy property in the left diamond, there exists a coalition such that the property satisfies the corresponding coalition privacy property in the right diamond. Intuitively, if a protocol preserves privacy of a target user without any help from third parties, the protocol can still preserve his privacy with the help from others. This is described as Thm. 3.

Theorem 1. *(1)* $\forall\theta$, $\mathsf{iepriv}_{\rho,\theta} \implies \mathsf{epriv}_\rho$, *(2)* $\forall\rho$, $\mathsf{iepriv}_{\rho,\theta} \implies \mathsf{ipriv}_\theta$, *(3)* $\forall\rho$, $\mathsf{epriv}_\rho \implies \mathsf{priv}$, *and (4)* $\forall\theta$, $\mathsf{ipriv}_\theta \implies \mathsf{priv}$.

Theorem 2. *(1)* $\forall\theta$, $\mathsf{ciepriv}_{\rho,\theta,\delta} \implies \mathsf{cepriv}_{\rho,\delta}$, *(2)* $\forall\rho$, $\mathsf{ciepriv}_{\rho,\theta,\delta} \implies \mathsf{cipriv}_{\theta,\delta}$, *(3)* $\forall\rho$, $\mathsf{cepriv}_{\rho,\delta} \implies \mathsf{cpriv}_\delta$, *and (4)* $\forall\theta$, $\mathsf{cipriv}_{\theta,\delta} \implies \mathsf{cpriv}_\delta$.

Theorem 3. *(1)* $\mathsf{ciepriv}_{\rho,\theta} \implies \exists\delta$, $\mathsf{ciepriv}_{\rho,\theta,\delta}$, *(2)* $\mathsf{epriv}_\rho \implies \exists\delta$,$\mathsf{cepriv}_{\rho,\delta}$, *(3)* $\mathsf{ipriv}_\theta \implies \exists\delta$, $\mathsf{cipriv}_{\theta,\delta}$, *and (4)* $\mathsf{priv} \implies \exists\delta$, cpriv_δ.

Fig. 2. Relations of the privacy notions



6 Discussion

Privacy notions modelled as strong secrecy can be captured by data-privacy. For instance, anonymity [3] is data-privacy where the target data is a user's identity. Various domain-specific properties, which capture privacy in domains where data-privacy is too strong to be satisfied, can be instantiated by cpriv. For instance, bidding-privacy [11] in sealed-bid e-auctions is defined as the adversary cannot determine a bidder's bidding-price, assuming the existence of a winning bid. This can be instantiated as cpriv where the target data is a bid, the defending third party is the winning bidder and the coalition specification is $\langle\emptyset,\emptyset,\emptyset\rangle$. Vote-privacy [22] is defined as the adversary cannot determine a voter's vote with the existence of a counter-balancing voter. This can be instantiated as cpriv where the target data is a vote, the defending third party is the counter-balancing voter

and the coalition specification is $\langle \emptyset, \Delta, \emptyset \rangle$ where Δ specifies how to replace the counter-balancing voter's vote.

Enforced privacy notions like receipt-freeness or coercion-resistance can be captured by either epriv or cepriv. Receipt-freeness [10] in voting can be instantiated by cepriv, where the target data and the coalition are the same as in vote-privacy, and the collaboration specification is $\langle \Psi, \emptyset, \mathsf{c}_{out}, \bot \rangle$ where Ψ contains all private terms generated and read-in in the target voter process. Similarly, coercion-resistance [10] in voting is an instance of coalition-enforced-privacy.

The two independency of privacy properties, independency-of-prescribing-privacy and independence-vote-privacy, are instances of cipriv. For example, the property independence-vote-privacy [14] can be considered as an instance of cipriv, where the target data and the coalition are the same as in vote-privacy, the set of attacking third parties is a third voter, and the collaboration specification of the third voter is $\langle \Psi, \Phi, \mathsf{c}_{out}, \mathsf{c}_{in} \rangle$ where Ψ are all generated and read-in terms and Φ are all communicated terms in the third voter process. For details, see [27].

7 Conclusion and Future Work

In this paper, we have identified (enforced) privacy notions in the presence of third parties. We formalised the collaboration of users, including the target user and attacking third parties, with the adversary and the coalition among users (the target user with defending third parties) in a generic way. The identified privacy notions are formally defined in the applied pi calculus. We presented the relations among the properties as a privacy hierarchy. We also showed that various existing privacy properties in the literature can be instantiated as one of the properties in the hierarchy.

We have already mentioned a few interesting research directions in the paper, for example, how to find a coalition and synthesise strategy for the coalition to satisfy some coalition privacy properties for a protocol, and how to extend our privacy hierarchy to capture situations where a third party is coerced but has a strategy to lie to the adversary. One important future work is to apply our privacy notions to real-world applications such as online social networks.

References

1. Reiter, M.K., Rubin, A.D.: Crowds: Anonymity for web transactions. ACM Transactions on Information and System Security **1**(1) (1998) 66–92
2. van Deursen, T., Mauw, S., Radomirović, S.: Untraceability of RFID protocols. In: Proc. 2nd WISTP. Volume 5019 of LNCS., Springer (2008) 1–15
3. Arapinis, M., Chothia, T., Ritter, E., Ryan, M.D.: Analysing unlinkability and anonymity using the applied pi calculus. In: Proc. 23rd CSF, IEEE (2010) 107–121
4. Bohli, J., Pashalidis, A.: Relations among privacy notions. ACM Transactions on Information and System Security **14**(1) (2011) 4:1–4:24
5. Jonker, H.L., Pang, J.: Bulletin boards in voting systems: Modelling and measuring privacy. In: Proc. 6th ARES, IEEE (2011) 294–300

6. Benaloh, J., Tuinstra, D.: Receipt-free secret-ballot elections (extended abstract). In: Proc. 26th STOC, ACM (1994) 544–553
7. Abe, M., Suzuki, K.: Receipt-free sealed-bid auction. In: Proc. 5th ISC. Volume 2433 of LNCS., Springer (2002) 191–199
8. Juels, A., Catalano, D., Jakobsson, M.: Coercion-resistant electronic elections. In: Proc. 4th WPES, ACM (2005) 61–70
9. De Decker, B., Layouni, M., Vangheluwe, H., Verslype, K.: A privacy-preserving eHealth protocol compliant with the Belgian healthcare system. In: Proc. 5th EuroPKI. Volume 5057 of LNCS., Springer (2008) 118–133
10. Delaune, S., Kremer, S., Ryan, M.D.: Verifying privacy-type properties of electronic voting protocols. Journal of Computer Security **17**(4) (2009) 435–487
11. Dong, N., Jonker, H.L., Pang, J.: Analysis of a receipt-free auction protocol in the applied pi calculus. In: Proc. 7th FAST. Volume 6561 of LNCS., Springer (2011) 223–238
12. Dong, N., Jonker, H.L., Pang, J.: Formal analysis of privacy in an eHealth protocol. In: Proc. 17th ESORICS. Volume 7459 of LNCS., Springer (2012) 325–342
13. Dong, N., Jonker, H.L., Pang, J.: Challenges in eHealth: From enabling to enforcing privacy. In: Proc. 1st FHIES. Volume 7151 of LNCS., Springer (2012) 195–206
14. Dreier, J., Lafourcade, P., Lakhnech, Y.: Vote-independence: A powerful privacy notion for voting protocols. In: Proc. 4th FPS. Volume 6888 of LNCS., Springer (2011) 164–180
15. Lowe, G.: Breaking and fixing the Needham-Schroeder public-key protocol using FDR. In: Proc. 2nd TACAS. Volume 1055 of LNCS., Springer (1996) 147–166
16. Chadha, R., Kremer, S., Scedrov, A.: Formal analysis of multi-party contract signing. In: Proc. 17th CSFW, IEEE (2004) 266–279
17. Blanchet, B.: An efficient cryptographic protocol verifier based on prolog rules. In: Proc. 14th CSFW, IEEE (2001) 82–96
18. Blanchet, B., Abadi, M., Fournet, C.: Automated verification of selected equivalences for security protocols. Journal of Logic and Algebraic Programming **75**(1) (2008) 3–51
19. Cheval, V., Blanchet, B.: Proving more observational equivalences with ProVerif. In: Proc. 2nd POST. Volume 7796 of LNCS., Springer (2013) 226–246
20. Blanchet, B.: Automatic proof of strong secrecy for security protocols. In: Proc. 25th S&P, IEEE (2004) 86–100
21. Dolev, D., Yao, A.C.C.: On the security of public key protocols. IEEE Transactions on Information Theory **29**(2) (1983) 198–207
22. Kremer, S., Ryan, M.D.: Analysis of an electronic voting protocol in the applied pi calculus. In: Proc. 14th ESOP. Volume 3444 of LNCS., Springer (2005) 186–200
23. Dahl, M., Delaune, S., Steel, G.: Formal analysis of privacy for anonymous location based services. In: Proc. TOSCA. Volume 6993 of LNCS., Springer (2011) 98–112
24. Dreier, J., Lafourcade, P., Lakhnech, Y.: Defining privacy for weighted votes, single and multi-voter coercion. In: Proc. 17th ESORICS. Volume 7459 of LNCS., Springer (2012) 451–468
25. Abadi, M., Fournet, C.: Mobile values, new names, and secure communication. In: Proc. 28th POPL, ACM (2001) 104–115
26. Küsters, R., Truderung, T.: An epistemic approach to coercion-resistance for electronic voting protocols. In: Proc. 30th S&P, IEEE (2009) 251–266
27. Dong, N., Jonker, H.L., Pang, J.: Enforcing privacy in the presence of others: Notions, formalisations and relations. Technical report, University of Luxembourg (2013) Available at `http://satoss.uni.lu/projects/epriv/`.