# Privacy Preserved Meeting Scheduling

Group 06

September 24, 2024

## 1 Tentative basic definitions

Following finite sets are defined:

- $\mathcal{D}$: The set of all documents.
- $\mathcal{R}$: The set of all roles.
- $\mathcal{I}$: The set of all individuals
- $\mathcal{L}$: The set of all locations.
- $\mathcal{T}$: The set of all time slots.

Following functions are also defined:

$$access : \mathcal{D} \mapsto 2^{\mathcal{R}} (2^{\mathcal{R}} = \text{power set of } \mathcal{R})$$

$$access(d) = \{r \in \mathcal{R} \mid r \text{ has access to } d\}$$

$$transform : \mathcal{I} \times \mathcal{L} \times \mathcal{T} \mapsto \mathcal{R}$$

$$transform(i, l, t) = r : r \text{ is role of } i \text{ at location } l \text{ at time slot } t$$

$$location : \mathcal{I} \times \mathcal{T} \mapsto \mathcal{L}$$

$$location(i, t) = l : i \text{ is at } l \text{ at } t$$

A meeting M is a 4-tupple,

$$M =< D, I, L, t >$$

such that,

$$D \subseteq \mathcal{D}$$

$$L \subseteq \mathcal{L}$$

$$I \subseteq \mathcal{I}$$

$$t \in \mathcal{T}$$

## 2 Access Control List

Consider that following finite sets are defined:

- $\mathcal{D}$: The set of all documents.
- $\mathcal{I}$: The set of all individuals

Based on those 2 sets, we define following 2 relationships.

$$d = \{d \in \mathcal{D} \mid \text{d is a document}\}$$

$$i = \{i \in \mathcal{I} \mid i \text{ is an individual }\}$$

$$g = \{g \subseteq \mathcal{I} \mid g \text{ is a subset of one or more individuals in } \mathcal{I}\}$$

Above relationships mean that $d$ is an element of set $\mathcal{D}$, and $i$ is an element of set $\mathcal{I}$. Further, $g$ is a group of one or more individuals ($i$), where $i \in \mathcal{I}$, such that $g \neq \emptyset$.

Consider that following finite set is also defined:

- $\mathcal{G}$: Set of all possible not-null subsets of $\mathcal{I}$

Based on above all sets, we define following relationship.

$$access(d) = \{g \in \mathcal{G} \mid g \text{ has access to } d\}$$

Above relationship means that $g$ is an element of set $\mathcal{G}$, and that $access(d)$ is the set of groups ($g$) having access permission to document $d$.
Here we note that, $access(d) = \mathcal{G}$ converts $d$ to a **public document**.

By above last two relationships, since any element $g$ of $access(d)$ is also a subset of $\mathcal{I}$, such that $g \subseteq \mathcal{I}$, we obtain the relationship $access(d) \subseteq \mathcal{I}$, when $access(d)$ is defined in form of **singleton subsets** of $\mathcal{I}$, and $\mathcal{I}$ is defined as a collection of singleton subsets, each containing an individual $i$. It implies also that $|access(d)| \leq |\mathcal{I}|$, when $access(d)$ and $\mathcal{I}$ both are defined as sets of singleton subsets of $\mathcal{I}$. Simply, a singleton subset of $\mathcal{I}$ includes an individual ($i$).
Regarding that inequality, $|access(d)| = |\mathcal{I}|$ is the situation when every $i$ in $\mathcal{I}$ is present in at least one group ($g$), such that $g \subseteq access(d)$. Accordingly, at such a situation, by eliminating the singleton subset format used for constructing inequality $|access(d)| = |\mathcal{I}|$, we can obtain $access(d) = \mathcal{G}$, which means that document is **public**.

## 3 Meeting agenda

Agenda of a meeting is the document that defines the set of groups ($g$) required to attend the meeting, where **group** has same meaning as defined above. When we consider agenda as document $d$, those groups ($g$) are elements of set $access(d)$.

Here, we obviously note that, we never need all individuals in set $\mathcal{I}$ to attend a single meeting. It means that, all possible not-null subsets of set $\mathcal{I}$, are never required to participate in a single meeting.

But, there are private meetings and public meetings both. If $access(d) = \mathcal{G}$ is used for meeting agenda of public meetings, it's impossible to distinguish the intended participant groups explicitly. Therefore, in agenda document of public meetings, we include a group defined as **public** group, in addition to the actual intended participant groups of meeting, to state that agenda is **public**. So, on the other hand, absence of group defined as **public** in $access(d)$, where $d = meeting\ agenda$, means that meeting is **private**.

- If there is at least one another document in meeting, such that $access(d) \neq \mathcal{G}$, **public** group shouldn't have access to meeting agenda.
- If every other documents in meeting has $access(d)$ such that $access(d) = \mathcal{G}$, **public** group can have access to meeting agenda.
- If agenda is the only document in meeting, **public** group can be used by meeting organizer to define whether agenda document is **private** or **public**.

Following flow chart depicts the process of identifying whether a document is **private** or **public**.

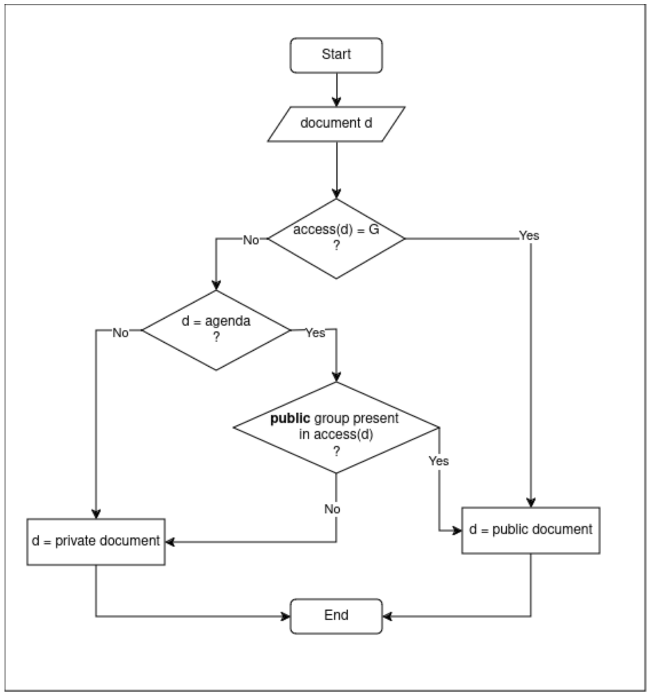


Figure 1: Process to identify whether a document is private or public

In addition to presence or absence of **public** group in $access(d)$, meeting agenda should define the **meeting quorum**, for the meeting. This theme will be discussed later.

# 4 Definition of a meeting

Consider that following finite sets are also defined, other than sets defined above:

- $\mathcal{L}$: The set of all locations.
- $\mathcal{T}$: The set of all time slots.

**We assume that every meeting has an agenda associated with it, to define the set of groups($g$) required to attend the meeting**. Agenda of a particular meeting $M$ is a document, belonging to set $\mathcal{D}$.
When we consider that agenda of meeting $M$ is $d$, for every group $g$ invited to meeting $M$; $g \in access(d)$. Also consider that, $D$ represents set of documents discussed in $M$, including agenda, such that $D \subseteq \mathcal{D}$. Hence, according to the assumption emphasized above, for any meeting $M$; $|D| \geq 1$.

For conducting a meeting, at least 2 individuals are required. Consider that

$I$ represents the set of individuals attending meeting $M$, such that $I \subseteq \mathcal{I}$, when groups ($g$) of $access(d)$ of agenda are converted to corresponding elementary individuals ($i$). Here we note that, for any meeting $M$; $|I| \geq 2$.
Accordingly, when $access(d)$ of agenda is defined in terms of singleton subsets of $\mathcal{G}$, and groups required for meeting are represented by $G$, $|G| \geq 2$.

Consider set of locations of individuals in $M$ as $L$ (in other words, set of locations of indiduals in set $I$, during meeting time), such that $L \subseteq \mathcal{L}$. Every individual attends meeting from a particular location $l$, such that $l \in L$. We note that if meeting is online or hybrid, $|L| > 1$. If meeting is onsite, $|L| = 1$, since every individual is at same location. Every meeting should be in one mode, out of online, hybrid, onsite modes. $\therefore$ For any meeting $M$; $|L| \geq 1$.

Since a **meeting** is a **synchrnous** communication, every individual in meeting $M$ should attend the meeting during the same time slot $t$ (Assuming that all individuals are in same time zone).

Based on these definitions, we define meeting M as a 4-tupple,

$$M =< D, I, L, t >$$

such that,

$$D \subseteq \mathcal{D}$$

$$L \subseteq \mathcal{L}$$

$$I \subseteq \mathcal{I}$$

$$t \in \mathcal{T}$$

# 5 Transformation of individual into role

Consider that same sets defined above will be used in explanations below, in same notations:

Consider $g$ and $g'$ as subsets of $\mathcal{G}$ such that $g, g' \subseteq \mathcal{G}$. And consider $d$ as a **private** document , $l$ as a location and $t$ as a time slot such that $d \in \mathcal{D}$, $l \in \mathcal{L}$ and $t \in \mathcal{T}$. Further consider that $g \in access(d)$ and $g' \notin access(d)$, for restricting access of document $d$, where $|access(d)| = n$ , given that $access(d)$ is defined as a set of singleton subsets of $\mathcal{G}$. A singleton subset of $\mathcal{G}$ means an elementary subset $g$, in which only one element (i.e. only one individual $i$) is present.
Also note that, $i$ and $i'$ are two individuals representing subsets $g$ and $g'$, respectively.

Assume that at scenario 1, $i$ attends a **meeting** at location $l$ during time slot $t$ to discuss document $d$, where $i'$ has no access to location $l$ during same time slot $t$.

Here we state that privacy of meeting discussing document $d$ was preserved at context $l \times t$

Now assume that at scenario 2, $i$ attends a **meeting** at location $l$ during time slot $t$ to discuss document $d$, where $i'$ also has access to location $l$ during same time slot $t$.
Here we state that privacy of meeting discussing document $d$ was violated at context $l \times t$, because $n+1$ individuals including $i'$ have got access to content of document $d$. But actually $|access(d)| = n$, when $access(d)$ is defined as a set of singleton subsets of $\mathcal{G}$, as mentioned above. We observe that $(n+1) \geq |access(d)| = n$

When above 2 scenarios are compared, we observe that role of same individual $i$, representing subset $g$ such that $g \in access(d)$, has experienced a variation. Context of $i$ has changed, depending on location and time.

Therefore we define that presence of $i$ at context $l \times t$ transforms $i$ to role $r$.

$$transform(i, l, t) = r : r \text{ is role of } i \text{ at location } l \text{ at time slot } t$$

If $g \in access(d)$, $g' \notin access(d)$ and $d$ is a **private** document, $i$ representing $g$ should attend a meeting to discuss $d$ at context $l \times t$, only if $i'$ representing $g'$ has no access to $l \times t$. Accordingly, to identify the privacy preserving context for discussing document $d$, combination of i, l, t is required.

# 6 Difference between public and private roles

When we consider a **private** document $d$, we can't exactly predict the time, at which $i'$, representing $g'$, such that $g' \notin access(d)$, will get access to location $l$. Therefore, meeting organizer has the responsibility of defining location $l$ as a **private** location or a **public** location, considering whether access of $i'$ has been strictly restricted, during all potential meeting time slots (represented by set $\mathcal{T}$).

Using this definition and above formula, we can show that, $i$ representing $g$, such that $g \in access(d)$ where $d$ is a **private** document, is transformed to role $g$ itself, at a **private** location. Here, location should be defined as a **private** location, by same entity, that defined the set $access(d)$ for document $d$.

$$transform(i, l, t) = r$$

$$transform(i, (private\_location), t) = r$$

$$transform(i, (private\_location), t) = g$$

On the other hand, any location $l$ is defined as a **public** location, if access of $i'$ has **not** been strictly restricted, during any potential meeting time slot (represented by $t$).

Using this definition and above formula, we can show that, $i$ representing $g$, such that $g \in access(d)$, is transformed to **public** role, at a **public** location. Location should be defined as a **public** location, by same entity, that defined the set $access(d)$ for document $d$.

$$transform(i, l, t) = r$$

$$transform(i, (public\_location), t) = r$$

$$transform(i, (public\_location), t) = public$$

Based on these derivations, we have identified a constraint relevant to $i$, for discussing $d$ in a privacy preserved meeting.

**Constraint**: When $d$ is a **private** document, every $i$ representing $g$, such that $g \in access(d)$, that attends a meeting to discuss document $d$, must represent role $g$ in the meeting.

When $d$ is a **public** document, every $i$ that attends a meeting to discuss document $d$, is allowed to represent **public** role in the meeting.

### 6.1 Roles in meeting agenda

If meeting agenda $d$ doesn't include **public** group in $access(d)$, then $i'$ representing $g'$ such that $g' \notin access(d)$, should be strictly prevented from accessing the meeting, by conducting meeting at a **private** location, defined by relevant entity.

On the other hand, if meeting agenda $d$ includes **public** group in $access(d)$, then it is **not** mandatory to prevent access of $i'$ representing $g'$ such that $g' \notin access(d)$, for the meeting. Therefore, meeting can be conducted at a **private** location or **public** location, based on locations defined by relevant entity.

## 7 Variation of role

Now consider a situation where individual $i$ representing $g$, such that $g \in access(d)$ has $x$ number of locations, out of which any one can be selected for attending a meeting to discuss $d$. And assume that $i$ has $y$ number of time slots, out of which any one can be selected for attending the meeting.

We can depict the possible variations of $transform(i, l, t)$ function as below, for individual $i$, depending on locations defined by the entity, assuming that $i$ doesn't change location during middle of a time slot.

| $(i)$ | $t_1$ | $t_2$ | ... | $t_{y-1}$ | $t_y$ |
|---|---|---|---|---|---|
| $l_1$ | x | x | | x | x |
| $l_2$ | x | x | | x | x |
| ... | | | | | |
| $l_{x-1}$ | x | x | | x | x |
| $l_x$ | x | x | | x | x |

Table 1: Possibilities in variation of $transform(i, l, t)$ for individual $i$

Note that $l_x$ represents the $x^{th}$ location, while $t_y$ represents the $y^{th}$ time slot. Meanwhile x represents the role of $i$ at the corresponding $l$ and $t$ (based on formula $transform(i, l, t) = r$). According to this representation, we observe that $i$ has $x \times y$ number of possibilities at maximum, to attain the role.

Here we emphasize that some x roles can be categorized as **public**, with respect to **public** locations defined by an entity. According to the constraint identified, if $d$ is a **private** document, $i$ should attend the meeting only when $r = g$, such that $g \in access(d)$. When r = **public** role, individual $i$ should strictly avoid discussing **private** documents. By following this constraint, access of $i'$ representing $g'$, such that $g' \notin aceess(d)$, into this meeting can be prevented.

# 8 Meeting quorum

We define **meeting quorum** as the minimum number of individuals ($i$) representing participant groups ($g$), required to attend a meeting, such that $g \in access(d)$ and $d$ is the meeting agenda.

**Now consider that document d is agenda**, for following description regarding the meeting quorum. In *privacy preserved meeting* context, if a specific **meeting quorum** isn't defined in the agenda, other than $access(d)$ set, we assume that every $i$ representing at least one $g$, such that $g \in access(d)$, except $g =$ **public**, is required for the meeting. Therefore, $|meeting\ quorum| \leq |access(d)|$, when $access(d)$ is defined in form of singleton subsets of $\mathcal{G}$.
Because, it's possible that $|meeting\ quorum| < |access(d)|$, if a specific percentage based rule is defined in meeting agenda.

Since at least 2 individuals ($i$) are required for any meeting, $2 \leq |meeting\ quorum|$.

Accordingly, $2 \leq |meeting\ quorum| \leq |access(d)|$.

When $access(d)$ is defined in form of singleton subsets of $\mathcal{G}$, as we have already depicted earlier, $|access(d)| \leq |\mathcal{I}|$. By merging this inequality with above expression, theoretically we obtain following expression.

$2 \leq |meeting\ quorum| \leq |access(d)| \leq |\mathcal{I}|$

But, in real world, since all individuals of set $\mathcal{I}$ are never required for a single meeting, $|meeting\ quorum| < |\mathcal{I}|$. Therefore, we can express a practically valid expression, as mentioned below.

$\therefore 2 \leq |meeting\ quorum| < |\mathcal{I}|$