Execution-time opacity control for timed automata

Abstract. Timing leaks in timed automata (TA) can occur whenever an attacker is able to deduce a secret by observing some timed behavior. In execution-time opacity, the attacker aims at deducing whether a private location was visited, by observing only the execution time. It can be decided whether a TA is opaque in this setting. In this work, we tackle control, and show that we are able to decide whether a TA can be controlled at runtime to ensure opacity. Our method is constructive, in the sense that we can exhibit such a controller. We also address the case when the attacker cannot have an infinite precision in its observations.

1 Introduction

In order to infer sensitive information, side-channels attacks [26] exploit various observable aspects of a system rather than directly exploiting its computational processes, such as power consumption, electromagnetic emissions, or time. In particular, by observing subtle differences in timing, attackers can infer valuable information about the internal state of the system. For example, in [20], a timing attack vulnerability is identified in the Chinese public key cryptography standard; the authors show how the most significant zero bits leakage obtained from the execution time allows to extract the secret key.

Timed automata (TAs) [1] are a powerful formalism to reason about real-time systems mixing timing constraints and concurrency. Timing leaks occur when an attacker is able to deduce a secret by observing some behavior of a TA.

Franck Cassez proposed in [19] a first definition of *timed* opacity for TAs: the system is opaque when an attacker can never deduce whether some secret sequence of actions (possibly with timestamps) was performed, by only observing a given set of observable actions together with their timestamp. It is then proved in [19] that it is undecidable whether a TA is opaque. The undecidability holds even for the restricted class of *event-recording automata* [2] (a subclass of TAs). The aforementioned negative result leaves hope only if the definition or the setting is changed, which was done in three main lines of works.

First, in [27,28], the input model is simplified to *real-time automata* [22], a restricted formalism compared to TAs considering a single clock, reset at each transition. In this setting, (initial-state) opacity becomes decidable.

Second, in [4], the authors consider a time-bounded notion of the opacity of [19], where the attacker has to disclose the secret before an upper bound, using a partial observability. Deciding opacity in this setting is shown to be decidable for TAs.

Third, in [7], an alternative definition to Cassez' opacity is proposed, by studying execution-time opacity (ET-opacity): the attacker has only access to the *execution time* of the system, as opposed to Cassez' partial observations where some events (with their timestamps) are observable. In that case, most problems for TAs become decidable.

Orthogonal directions of research include non-interference for TAs. Different notions of equivalence (e.g., bisimulation) can be considered for this property. Several papers [12,13,6] present some decidability results, while control is considered in [14]. General security problems for TAs are surveyed in [9].

Note that a preliminary version of control is considered in [5] for ET-opacity, but only untimed, i.e., the actions could only be enabled or disabled once and for all, thus severely diminishing the possibilities to render the system ET-opaque. Finally note that [7] considers also *parametric* versions of the opacity problems, in which timing parameters [3] can be used in order to make the system ET-opaque. Our notion of control is orthogonal to parameter synthesis, as another way to ensure the system becomes ET-opaque.

Controller synthesis can be described and solved thanks to game theory; finding a strategy for a controller can be equivalent to computing a winning strategy in a corresponding game. Several game models have been considered, as timed games that can be used to solve synthesis problem on timed automata. In this context, [11] aims to restrict the transition relation in order to satisfy certain properties, while [25] completes this result, minimizing the execution time, and [15] studies the reachability with robust strategies only.

Different variants of opacity are also studied for other types of systems, such as stochastic systems [18]. In particular, opacity can be related to the bandwidth of a language [24,10].

Contributions In this work, we aim at tuning a system to make it ET-opaque, by *controling* it at runtime. As usual, we consider that the system actions are partitioned between controllable and uncontrollable. Our controller relies on the following notion of strategy: at each timestamp, the strategy enables only a subset of the controllable actions. Depending of the system, various degrees of opacity can be interesting, and we therefore consider several variants (*existential*, *weak*, *full*). Our technique relies on an *ad-hoc* construction inspired by the region automata for TAs. We show that the existence of a controller to make the system ET-opaque is decidable, and our approach is constructive. We also address the case when the attacker cannot have an infinite precision in its observations.

Outline Section 2 recalls the necessary material. Section 3 defines the control problem for ET-opacity. Sections 4 and 5 define the core of our approach. Section 6 extends our method when the attacker cannot have an infinite precision in observing the execution time. Section 7 highlights future works.

2 Preliminaries

Clocks are real-valued variables that all evolve over time at the same rate. Throughout this paper, we assume a set $\mathbb{X} = \{x_1, \ldots, x_H\}$ of *clocks*. A *clock valuation* is a function $\mu : \mathbb{X} \to \mathbb{R}_{\geq 0}$, assigning a non-negative value to each clock. Given $R \subseteq \mathbb{X}$, we define the reset of a valuation μ with respect to R, denoted by $[\mu]_R$, as follows: $[\mu]_R(x) = 0$ if $x \in R$, and $[\mu]_R(x) = \mu(x)$ otherwise. We write $\mathbf{0}$ for the clock valuation assigning 0 to all clocks. Given a constant $d \in \mathbb{R}_{\geq 0}$, $\mu + d$ denotes the valuation s.t. $(\mu + d)(x) = \mu(x) + d$, for all $x \in \mathbb{X}$.

We assume $\bowtie \in \{<, \leq, =, \geq, >\}$. A *constraint* C is a conjunction of inequalities over $\mathbb{X}$ of the form $x \bowtie d$, with $d \in \mathbb{Z}$. A table of notations is available in Appendix A.

2.1 Timed automata

We define timed automata as in [1], with an extra private location, which encodes the secret that shall not be leaked.

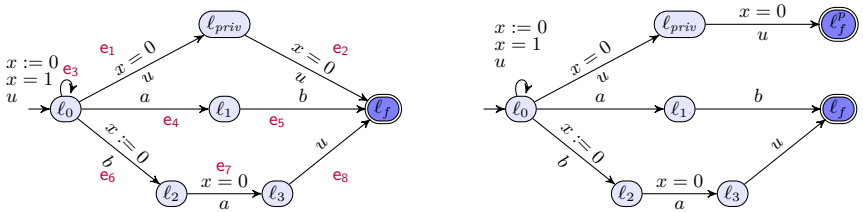
Definition 1 (Timed automaton). *A* timed automaton *(TA) $\mathcal{A}$ is a tuple $\mathcal{A} = (\Sigma, L, \ell_0, \ell_{priv}, F, \mathbb{X}, I, E)$ where: 1) Σ is a finite set of actions, 2) L is a finite set of locations, 3) $\ell_0 \in L$ is the initial location, 4) $\ell_{priv} \in L$ is the private location, 5) $F \subseteq L$ is the set of final locations, 6) $\mathbb{X} = \{x_1, \ldots, x_H\}$ is a finite set of clocks, 7) I is the invariant, assigning to every $\ell \in L$ a constraint $I(\ell)$, 8) E is a finite set of edges $\mathsf{e} = (\ell, g, a, R, \ell')$ where $\ell, \ell' \in L$ are the source and target locations, $a \in \Sigma \cup \{\varepsilon\}$, where ε denotes the silent action, $R \subseteq \mathbb{X}$ is a set of clocks to be reset, and g is a constraint over $\mathbb{X}$ (called* guard*).*

Example 1. Fig. 1a depicts a TA $\mathcal{A}_1$ with a single clock x, where $\Sigma = \{a, b, u\}$. The edge e_1 between ℓ_0 and the private location ℓ_{priv} is available only when the valuation of x is equal to 0. The edge e_6 between ℓ_0 and ℓ_2 resets x.

Since we are only interested in the (first) arrival time in a final location, the following assumption does not restrict our framework, but simplifies the subsequent definitions and results.

Assumption 1 *We consider every final location as* urgent *(where time cannot elapse): formally, there exists $x \in \mathbb{X}$ such that, for all $(\ell, g, a, R, \ell') \in E, \ell' \in F$, we have $x \in R$ and "$x = 0$" $\in I(\ell')$. Moreover, final locations cannot have outgoing transitions: formally, there is no $(\ell, g, a, R, \ell') \in E$ s.t. $\ell \in F$.*

Definition 2 (Semantics of a TA). *Let $\mathcal{A} = (\Sigma, L, \ell_0, \ell_{priv}, F, \mathbb{X}, I, E)$ be a TA, the semantics of $\mathcal{A}$ is given by the timed transition system $TTS_{\mathcal{A}} = (S, s_0, \Sigma \cup \mathbb{R}_{\geq 0}, \delta)$, with 1) $S = \{(\ell, \mu) \in L \times \mathbb{R}^H_{\geq 0} \mid \mu \models I(\ell)\}$, 2) $s_0 = (\ell_0, \mathbf{0})$, 3) δ consists of the discrete and (continuous) delay transition relations: i) discrete transitions: $(\ell, \mu) \overset{\mathsf{e}}{\mapsto} (\ell', \mu')$, if $(\ell, \mu), (\ell', \mu') \in S$, and there exists $\mathsf{e} = (\ell, g, a, R, \ell') \in E$, such that $\mu' = [\mu]_R$, and $\mu \models g$. ii) delay transitions: $(\ell, \mu) \overset{d}{\mapsto} (\ell, \mu + d)$, with $d \in \mathbb{R}_{\geq 0}$, if $\forall d' \in [0, d], (\ell, \mu + d') \in S$.*



(a) TA $\mathcal{A}_1$ (b) Duplicated version of $\mathcal{A}_1$

Fig. 1: A TA and its duplicated version (introduced in Section 4)

We write $(\ell, \mu) \xrightarrow{d,\mathsf{e}} (\ell', \mu + d)$ for a combination of a delay and a discrete transitions when $\exists \mu'' : (\ell, \mu) \overset{d}{\mapsto} (\ell, \mu'') \overset{\mathsf{e}}{\mapsto} (\ell', \mu')$.

Given a TA $\mathcal{A}$ with semantics $(S, s_0, \Sigma \cup \mathbb{R}_{\geq 0}, \delta)$, a *run* of $\mathcal{A}$ is a finite alternating sequence of states of $TTS_{\mathcal{A}}$ and pairs of delays and edges starting from s_0 of the form $s_0, (d_0, \mathsf{e}_0), s_1, \ldots, s_n$ where for all $i < n, \mathsf{e}_i \in E, d_i \in \mathbb{R}_{\geq 0}$ and $s_i \xrightarrow{d_i,\mathsf{e}_i} s_{i+1}$. The duration of a run $\rho = s_0, (d_0, \mathsf{e}_0), s_1, \ldots, (d_{n-1}, \mathsf{e}_{n-1}), s_n$ is $dur(\rho) = \sum_{0 \leq i \leq n-1} d_i$. We define $last(\rho) = s_n$.

Extra clock We will need an extra clock z that will help us later keep track of the elapsed absolute time. This clock is reset exactly every 1 time unit, and therefore each reset corresponds to a "tick" of the absolute time. (Note that its actual value remains in $[0, 1]$ and therefore always matches the fractional part of the absolute time.) In all subsequent region constructions, we assume the existence of $z \in \mathbb{X}$. For each location ℓ, we add the constraint "$z \leq 1$" to $I(\ell)$, and we add a self-loop edge $(\ell, z = 1, \varepsilon, \{z\}, \ell)$.

2.2 Regions

Given $\mathcal{A}$, for a clock x_i, we denote by c_i the largest constant to which x_i is compared within the guards and invariants of $\mathcal{A}$: formally, $c_i = \max_j\{d_j \mid x_i \bowtie d_j$ appears in a guard or invariant of $\mathcal{A}\}$. Given μ and a clock x_i, let $\lfloor \mu(x_i) \rfloor$ (resp. $\mathrm{fr}(\mu(x_i))$) denotes the integral (resp. fractional) part of $\mu(x_i)$.

Definition 3 (Region equivalence [1]). *Two clocks valuations μ, μ' are* equivalent*, denoted by $\mu \approx \mu'$, when the following three conditions hold for any clocks $x_i, x_j \in \mathbb{X}$:*

1. $\lfloor \mu(x_i) \rfloor = \lfloor \mu'(x_i) \rfloor$ *or* $\mu(x_i) > c_i$ *and* $\mu'(x_i) > c_i$*;*
2. *if* $\mu(x_i) \leq c_i$ *and* $\mu(x_j) \leq c_j$*:* $\mathrm{fr}(\mu(x_i)) \leq \mathrm{fr}(\mu(x_j))$ *iff* $\mathrm{fr}(\mu'(x_i)) \leq \mathrm{fr}(\mu'(x_j))$*;*
3. *if* $\mu(x_i) \leq c_i$ *:* $\mathrm{fr}(\mu(x_i)) = 0$ *iff* $\mathrm{fr}(\mu'(x_i)) = 0$.

The equivalence relation $\approx$ is extended to the states of $TTS_{\mathcal{A}}$: given two states $s = (\ell, \mu), s' = (\ell', \mu')$ of $TTS_{\mathcal{A}}$, we write $s \approx s'$ iff $\ell = \ell'$ and $\mu \approx \mu'$. We denote by $[s]$ and call *region* the equivalence class of a state s for $\approx$. The set of

all regions of $\mathcal{A}$ is denoted $\mathsf{R}_\mathcal{A}$. A region $r = [(\ell, \mu)]$ is *final* whenever $\ell \in F$. The set of final regions is denoted by $\mathsf{R}_\mathcal{A}^F$. A region r is *reachable* when there exists a run ρ such that $last(\rho) \in r$.

Region automaton We now define a region automaton based on [17, Proposition 5.3] with two changes on the transition labels : the first component indicates whether z has been reset to 0 (symbol "1") or not (symbols 0 or 0^+ according to whether time has elapsed or not). We also add as a second component the action that allows to move from a region to another (or ε when no action is involved).

Given a state $s = (\ell, \mu)$, and $d \in \mathbb{R}_{\geq 0}$, we write $s + d$ to denote $(\ell, \mu + d)$. We write $r \cup r'$ for $\{s \mid s \in r \text{ or } s \in r'\}$.

Definition 4 (Labeled Region Automaton). *For a given TA $\mathcal{A}$, the region automaton $\mathcal{R}_\mathcal{A}$ is given by the tuple $(\mathsf{R}_\mathcal{A}, \Sigma^\mathsf{R}, \delta^\mathsf{R})$ where:*

1. *$\mathsf{R}_\mathcal{A}$ is the set of states*
2. *$\Sigma^\mathsf{R} = \{0, 0^+, 1\} \times (\Sigma \cup \varepsilon)$,*
3. *given two regions $r, r' \in \mathsf{R}_\mathcal{A}$ and $\zeta \in \Sigma^\mathsf{R}$, we have $(r, \zeta, r') \in \delta^\mathsf{R}$ if one of the following holds:*
   - *(a) $\zeta = (0, a)$ and $\exists (\ell, \mu) \in r, (\ell', \mu') \in r'$ such that $(\ell, \mu) \overset{\mathsf{e}}{\mapsto} (\ell', \mu') \in \delta$ in $TTS_\mathcal{A}$ with $\mathsf{e} = (\ell, g, a, R, \ell')$ for some g and R;*
   - *(b) $\zeta = (0^+, \varepsilon)$ and $\exists s = (\ell, \mu) \in r, s' = (\mu + d) \in r'$ and $d \in \mathbb{R}_{>0}$ such that 1) $s \overset{d}{\mapsto} s'$, 2) $\forall 0 < d' \leq d$ $s + d' \in r \cup r'$ and 3) $\mathrm{fr}(\mu(z)) \neq 0$ and $\mathrm{fr}(\mu + d(z)) \neq 0$;*[1]
   - *(c) $\zeta = (1, \varepsilon)$ and $\exists s \in r$ such that $\exists d \in \mathbb{R}_{>0}$ such that 1) $s + d \in r'$, 2) either $\lfloor \mu(z) \rfloor \neq \lfloor \mu'(z) \rfloor$ or $0 \in \{\mathrm{fr}(\mu(z)), \mathrm{fr}(\mu'(z))\}$ but $\mathrm{fr}(\mu(z)) \neq \mathrm{fr}(\mu'(z))$, and 3) $\forall d' \in \mathbb{R}_{>0}$ such that $d' < d$, $s + d' \in r \cup r'$.*

We write $r \xrightarrow{\zeta}_\mathsf{R} r'$ for $(r, \zeta, r') \in \delta^\mathsf{R}$.

2.3 Execution-time opacity of a TA

Let us now recall from [7] the notions of private and public runs.

Given a TA $\mathcal{A}$ and a run ρ, we say that ℓ_{priv} is *visited on the way to a final location in* ρ when ρ is of the form $(\ell_0, \mu_0), (d_0, \mathsf{e}_0), (\ell_1, \mu_1), \ldots, (\ell_m, \mu_m), (d_m, \mathsf{e}_m), \ldots, (\ell_n, \mu_n)$ for some $m, n \in \mathbb{N}$ such that $\ell_m = \ell_{priv}$ and $\ell_n \in F$. We denote by $Visit^{priv}(\mathcal{A})$ the set of those runs, and refer to them as *private* runs. We denote by $DVisit^{priv}(\mathcal{A})$ the set of all the durations of these runs.

Conversely, we say that ℓ_{priv} is *avoided on the way to a final location in* ρ when ρ is of the form $(\ell_0, \mu_0), (d_0, \mathsf{e}_0), (\ell_1, \mu_1), \ldots, (\ell_n, \mu_n)$ with $\ell_n \in F$ and $\forall 0 \leq i < n, \ell_i \notin \{\ell_{priv}\}$. We denote the set of those runs by $Visit^{\overline{priv}}(\mathcal{A})$, referring

[1] Condition 2) ensures that we only move from one region to the "next" one (no intermediate region), and condition 3) adds that we stay in the same region for z (otherwise one of the two regions would have an integer value for z).

to them as *public* runs, and by $DVisit^{\overline{priv}}(\mathcal{A})$ the set of all the durations of these public runs.

These concepts can be seen as the set of execution times from the initial location ℓ_0 to a final location while visiting (resp. not visiting) ℓ_{priv}.

Example 2. Consider the following two runs of the TA $\mathcal{A}_1$ in Fig. 1a. Note that we use (ℓ_0, v) as a shortcut for (ℓ_0, μ) such that $\mu(x) = v$.

$$\rho_1 = (\ell_0, 0), (1, \mathsf{e}_3), (\ell_0, 0), (0, \mathsf{e}_1), (\ell_{priv}, 0), (0, \mathsf{e}_2), (\ell_f, 0)$$
$$\rho_2 = (\ell_0, 0), (0.1, \mathsf{e}_6), (\ell_2, 0), (0, \mathsf{e}_7), (\ell_3, 0), (0.7, \mathsf{e}_8), (\ell_f, 0.8)$$

Run $\rho_1 \in Visit^{priv}(\mathcal{A}_1)$ is a private run, and $dur(\rho_1) = 1 \in DVisit^{priv}(\mathcal{A}_1)$ and run $\rho_2 \in Visit^{\overline{priv}}(\mathcal{A}_1)$ is a public run with $dur(\rho_2) = 0.8 \in DVisit^{\overline{priv}}(\mathcal{A}_1)$.

ET-opacity We now recall from [7] the concept of "ET-opacity for a set of durations (or execution times) D": a system is *ET-opaque for execution times D* whenever, for any duration in D, it is not possible to deduce whether the system visited ℓ_{priv} or not.

Definition 5 (Execution-time opacity (ET-opacity) for D). *Given a TA $\mathcal{A}$ and a set of execution times D, we say that $\mathcal{A}$ is* execution-time opaque (ET-opaque) for execution times D *when* $D \subseteq (DVisit^{priv}(\mathcal{A}) \cap DVisit^{\overline{priv}}(\mathcal{A}))$.

Definition 6 (Full, weak and existential ET-opacity). *A TA $\mathcal{A}$ is*

- fully ET-opaque *when* $DVisit^{priv}(\mathcal{A}) = DVisit^{\overline{priv}}(\mathcal{A})$,
- weakly ET-opaque *when* $DVisit^{priv}(\mathcal{A}) \subseteq DVisit^{\overline{priv}}(\mathcal{A})$,
- existentially ET-opaque *when* $DVisit^{priv}(\mathcal{A}) \cap DVisit^{\overline{priv}}(\mathcal{A}) \neq \emptyset$.

That is, if for any run of duration d reaching a final location after visiting ℓ_{priv}, there exists another run of the same duration reaching a final location but not visiting the private location, the system is weakly ET-opaque. If, in addition, the converse holds, the system is fully ET-opaque. Finally, when there is at least one private run such that there exists a public run of the same duration, the system is existentially ET-opaque, denoted ∃-ET-opaque in the following.

Example 3. Consider again $\mathcal{A}_1$ in Fig. 1a. Each time x is equal to 1, we can reset it via e_3, and take edges e_1 and e_2 instantaneously. It results that $DVisit^{priv}(\mathcal{A}_1) = \mathbb{N}$. We have seen that $0.8 \in DVisit^{\overline{priv}}(\mathcal{A}_1)$ in Example 2. So $DVisit^{priv}(\mathcal{A}_1) \neq DVisit^{\overline{priv}}(\mathcal{A}_1)$ and $\mathcal{A}_1$ is not fully ET-opaque. However, since we can reach ℓ_f at any time without visiting ℓ_{priv}, clearly $DVisit^{priv}(\mathcal{A}_1) \subseteq DVisit^{\overline{priv}}(\mathcal{A}_1)$ and $\mathcal{A}_1$ is weakly ET-opaque (and ∃-ET-opaque too).

3 Problem: Controling TA to achieve ET-opacity

Let us formally define the main problem addressed in this work. We assume $\Sigma = \Sigma_c \uplus \Sigma_u$ where Σ_c (resp. Σ_u) denotes controllable (resp. uncontrollable) actions. The uncontrollable actions are always available, whereas the controllable actions can be enabled and disabled at runtime.

The controller has a *strategy*, i.e., a function $\sigma : \mathbb{R}_{\geq 0} \to 2^{\Sigma_c}$ which associates to each time a subset of Σ_c, these actions are enabled, while others are disabled.

We define the semantics of a controlled TA as follows.

Definition 7 (Semantics of a controlled TA). *Given a TA* $\mathcal{A} = (\Sigma, L, \ell_0, \ell_{priv}, F, \mathbb{X}, I, E)$ *and a strategy* $\sigma : \mathbb{R}_{\geq 0} \to 2^{\Sigma_c}$*, the semantics of the controlled TA* $\mathcal{A}^\sigma$ *is given by the TTS* $TTS_{\mathcal{A}^\sigma} = (S, s_0, \Sigma \cup \mathbb{R}_{\geq 0}, \delta^\sigma)$ *with*

1. $S = \{(\ell, \mu, t) \in L \times \mathbb{R}^H_{\geq 0} \times \mathbb{R}_{\geq 0} \mid \mu \models I(\ell)\}$,
2. $s_0 = (\ell_0, \mathbf{0}, 0)$,
3. δ^σ *consists of the discrete and (continuous) delay transition relation:*
   (a) *discrete transitions:* $(\ell, \mu, t) \overset{\mathsf{e}}{\mapsto}_\sigma (\ell', \mu', t)$*, if* $(\ell, \mu, t), (\ell', \mu', t) \in S$ *and there exists* $\mathsf{e} = (\ell, g, a, R, \ell') \in E$ *such that* $\mu' = [\mu]_R$*,* $\mu \models g$*, and* $a \in \sigma(t) \cup \Sigma_u$.
   (b) *delay transitions:* $(\ell, \mu, t) \overset{d}{\mapsto}_\sigma (\ell, \mu + d, t + d)$*, with* $d \in \mathbb{R}_{\geq 0}$*, if* $\forall d' \in [0, d]$*,* $(\ell, \mu + d', t + d') \in S$.

We write $(\ell, \mu, t) \xrightarrow{d,e}_\sigma (\ell', \mu', t')$ for a combination of a delay and discrete transitions when $\exists \mu''$ such that $(\ell, \mu, t) \overset{d}{\mapsto}_\sigma (\ell, \mu'', t') \overset{\mathsf{e}}{\mapsto}_\sigma (\ell', \mu', t')$.

A run $\rho = (\ell_0, \mu_0), (d_0, \mathsf{e}_0), \ldots, (\ell_n, \mu_n)$ is σ*-compatible* when, $\forall 0 \leq i < n$, it holds that $(\ell_i, \mu_i, \sum_{j<i} d_j) \xrightarrow{d_i, \mathsf{e}_i}_\sigma (\ell_{i+1}, \mu_{i+1}, \sum_{j \leq i} d_j)$.

We let

- $Visit^{priv}_\sigma(\mathcal{A}) = \{\rho \mid \rho \text{ is private and } \sigma\text{-compatible}\}$,
- $Visit^{\overline{priv}}_\sigma(\mathcal{A}) = \{\rho \mid \rho \text{ is public and } \sigma\text{-compatible}\}$,
- $DVisit^{priv}_\sigma(\mathcal{A}) = \{dur(\rho) \mid \rho \text{ is private and } \sigma\text{-compatible}\}$,
- $DVisit^{\overline{priv}}_\sigma(\mathcal{A}) = \{dur(\rho) \mid run \text{ is public and } \sigma\text{-compatible}\}$.

Definition 8 (Full, weak and existential ET-opacity with strategy). *For a strategy* σ*, a TA* $\mathcal{A}$ *is*

1. fully ET-opaque with σ *when* $DVisit^{priv}_\sigma(\mathcal{A}) = DVisit^{\overline{priv}}_\sigma(\mathcal{A})$
2. weakly ET-opaque with σ *when* $DVisit^{priv}_\sigma(\mathcal{A}) \subseteq DVisit^{\overline{priv}}_\sigma(\mathcal{A})$
3. $\exists$-ET-opaque with σ *when* $DVisit^{priv}_\sigma(\mathcal{A}) \cap DVisit^{\overline{priv}}_\sigma(\mathcal{A}) \neq \emptyset$.

Finitely-varying strategies To be able to manage strategies in the following constructions, we expect them to behave in a "reasonable" way. We only consider *finitely-varying strategies* where the number of changes are finite for any closed time interval. Indeed, we can assume that a controller cannot change infinitely frequently its strategy in a finite time: it is unrealistic to consider, in a bounded

interval, neither a system that can perform an infinite number of actions, nor a controller that can make an infinite number of choices. More formally, a strategy σ is *finitely-varying* when, for any closed time interval I, there is a finite partition $p_1, \ldots, p_n$ of I such that each p_i is an interval and for all $\tau_1, \tau_2 \in p_i$, $1 \leq i \leq n$, $\sigma(\tau_1) = \sigma(\tau_2)$. (See Example 10 in Appendix D for an example of non-finitely-varying strategy.)

In this paper, we are interested in several ET-opacity control problems i.e., related to a strategy σ making the TA $\mathcal{A}^\sigma$ ET-opaque. Those problems differ on the type of ET-opacity (full, weak or existential) we want to enforce, and whether we want to prove the existence of a finitely-varying strategy enforcing the ET-opacity or synthesize this strategy.

Full ET-opacity finitely-varying controller emptiness problem:
INPUT: A TA $\mathcal{A}$
PROBLEM: Decide whether the set of finitely-varying strategies σ such that $\mathcal{A}^\sigma$ is fully ET-opaque is empty.

Full ET-opacity finitely-varying controller synthesis problem:
INPUT: A TA $\mathcal{A}$
PROBLEM: Synthesize a finitely-varying strategy σ such that $\mathcal{A}^\sigma$ is fully ET-opaque.

Example 4 (Non-ET-opaque TA). There is no strategy such that TA $\mathcal{A}_1$ in Fig. 1a is fully ET-opaque. Indeed, as $\Sigma_u = \{u\}$ and $\Sigma_c = \{a, b\}$, the transitions e_1 and e_2 are uncontrollable, so we can reach ℓ_f at any integer time along a run visiting ℓ_{priv}. However, even if we can allow transitions a and b at integer times too, the last transition e_8 is uncontrollable and can be taken at any time. Then, location ℓ_f can be reached at any time along a run not visiting ℓ_{priv}.

4 The belief automaton

In this section, we build an automaton called the "belief automaton", that will allow us to determine in which regions the system can be after a given execution time. This automaton considers a duplicated TA instead of the original TA in order to distinguish the final state reached by a private or a public run.[2]

4.1 Separating private and public runs

We define a duplicated version of a TA $\mathcal{A}$, denoted by $\mathcal{A}^{dup}$, making it possible to decide if a given run avoids ℓ_{priv} or not just looking at the final reached location. Note that any run of $\mathcal{A}$ has an equivalent one in $\mathcal{A}^{dup}$ where each location is replaced by its duplicated version if a previous visited location is ℓ_{priv}. In particular, $D\mathit{Visit}^{\overline{priv}}(\mathcal{A}) = D\mathit{Visit}^{\overline{priv}}(\mathcal{A}^{dup})$ and $D\mathit{Visit}^{priv}(\mathcal{A}) = D\mathit{Visit}^{priv}(\mathcal{A}^{dup})$.

[2] This could equally have been encoded using a Boolean variable remembering whether ℓ_{priv} was visited, as in [8].

Definition 9 (Duplicated TA). *Let $\mathcal{A} = (\Sigma, L, \ell_0, \ell_{priv}, F, \mathbb{X}, I, E)$ be a TA. The associated* duplicated TA *is $\mathcal{A}^{dup} = (\Sigma', L', \ell'_0, \ell'_{priv}, F', \mathbb{X}', I', E')$ where: 1) $\Sigma' = \Sigma$, 2) $L' = L_{pub} \uplus L_{priv}$ with $L_{pub} = L \setminus \ell_{priv}$ and $L_{priv} = \{\ell^p \mid \ell \in L\} \cup \{\ell_{priv}\}$, 3) $\ell'_0 = \ell_0$, 4) $\ell'_{priv} = \ell_{priv}$, 5) $F' = \{\ell_f^p \mid \ell_f \in F\} \cup F$, 6) $\mathbb{X}' = \mathbb{X}$, 7) I' is the invariant such that $\forall \ell \in L, I'(\ell) = I'(\ell^p) = I(\ell)$, 8) $E' = \big\{(\ell_1, g, a, R, \ell_2) \mid (\ell_1, g, a, R, \ell_2) \in E \text{ and } \ell_1 \neq \ell_{priv}\big\} \cup \big\{(\ell_1^p, g, a, R, \ell_2^p) \mid (\ell_1, g, a, R, \ell_2) \in E\big\} \cup \big\{(\ell_{priv}, g, a, R, \ell^p) \mid (\ell_{priv}, g, a, R, \ell) \in E\big\}$*

Example 5. Fig. 1b depicts $\mathcal{A}_1^{dup}$, the duplicated version of $\mathcal{A}_1$ in Fig. 1a. We do not depict unreachable locations. Observe that each run avoiding ℓ_{priv} ends in ℓ_f, and that the only outgoing transition of ℓ_{priv} is modified to go to ℓ_f^p.

4.2 Beliefs

For a given time $t \in \mathbb{R}_{\geq 0}$, we define a *belief* $\mathfrak{b}_t$ as the set of regions that can be reached at time t, i.e., for a TA $\mathcal{A}$ and $r \in \mathsf{R}_{\mathcal{A}^{dup}}$, $r \in \mathfrak{b}_t$ when $\exists \rho$ in $\mathcal{A}^{dup}$ such that $last(\rho) \in r$ and $dur(\rho) = t$. We denote the set of beliefs of $\mathcal{A}$ by $\mathbb{B}_{\mathcal{A}} = \{\mathfrak{b}_t \mid t \in \mathbb{R}_{\geq 0}\}$.

Definition 10 (Belief automaton). *For $\mathcal{A}$ a TA with $\Sigma = \Sigma_c \uplus \Sigma_u$, we define the* belief automaton *as the tuple $\mathcal{B}_{\mathcal{A}} = (\mathfrak{S}^{\mathcal{B}_{\mathcal{A}}}, \mathfrak{A}^{\mathcal{B}_{\mathcal{A}}}, \bot, \mathfrak{d}^{\mathcal{B}_{\mathcal{A}}})$ where:*

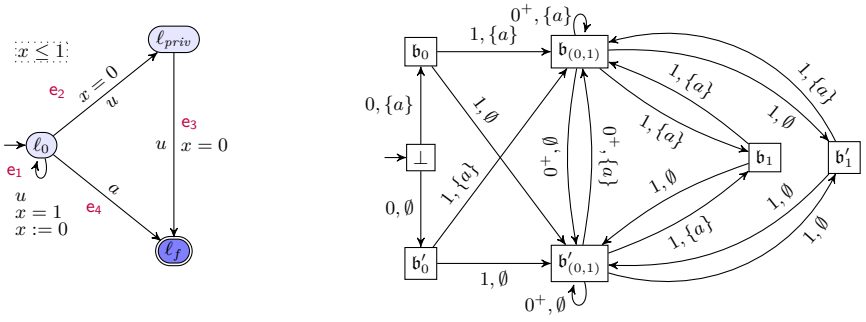
1. $\mathfrak{S}^{\mathcal{B}_{\mathcal{A}}} = 2^{\mathsf{R}_{\mathcal{A}^{dup}}} \cup \{\bot\}$ *is the set of states,*
2. $\mathfrak{A}^{\mathcal{B}_{\mathcal{A}}} = \{0, 0^+, 1\} \times 2^{\Sigma_c}$,
3. $\bot$ *is the initial state,*
4. $\mathfrak{d}^{\mathcal{B}_{\mathcal{A}}} \subseteq (\mathfrak{S}^{\mathcal{B}_{\mathcal{A}}} \times \mathfrak{A}^{\mathcal{B}_{\mathcal{A}}} \times \mathfrak{S}^{\mathcal{B}_{\mathcal{A}}})$ *and*
   (a) $(\bot, (0, \mathfrak{C}), \mathfrak{b}) \in \mathfrak{d}^{\mathcal{B}_{\mathcal{A}}}$ *iff* $\mathfrak{b}$ *is the largest set such that* $\forall r \in \mathfrak{b}$, $\exists n \geq 0$, $[s_0] \xrightarrow{(0,a_1)}_{\mathsf{R}} \cdots \xrightarrow{(0,a_n)}_{\mathsf{R}} r$ *in* $\mathcal{R}_{\mathcal{A}^{dup}}$ *with* $\forall 1 \leq i \leq n$, $a_i \in (\mathfrak{C} \cup \Sigma_u)$,
   (b) $(\mathfrak{b}, (\dagger_1, \mathfrak{C}), \mathfrak{b}') \in \mathfrak{d}^{\mathcal{B}_{\mathcal{A}}}$ *iff* $\mathfrak{b} \neq \bot$, $\mathfrak{b}'$ *is the largest set such that* $\forall r' \in \mathfrak{b}'$, $\exists r \in \mathfrak{b}$, $\exists n \geq 1$, $r \xrightarrow{(\dagger_1,a_1)}_{\mathsf{R}} \cdots \xrightarrow{(\dagger_n,a_n)}_{\mathsf{R}} r'$ *in* $\mathcal{R}_{\mathcal{A}^{dup}}$ *with* $\forall 1 \leq i \leq n, a_i \in (\mathfrak{C} \cup \Sigma_u \cup \{\varepsilon\})$ *and* $\dagger_1 \in \{0^+, 1\}$ *and* $\forall 1 < i \leq n, \dagger_i \in \{0, 0^+\}$.

Bad and good beliefs Intuitively, a bad belief allows to discriminate private and public runs. For a given TA $\mathcal{A}$, we denote $\mathsf{Secret}_{\mathcal{A}} = \big\{[(\ell, \mu)] \mid \ell \in L_{priv}, \mu \in \mathbb{R}^H_{\geq 0}\big\}$ the set of regions reachable on a run visiting ℓ_{priv} in $\mathcal{A}^{dup}$, and $\overline{\mathsf{Secret}_{\mathcal{A}}} = \big\{[(\ell, \mu)] \mid \ell \in L_{pub}, \mu \in \mathbb{R}^H_{\geq 0}\big\}$ the set of regions reachable on a run not visiting ℓ_{priv} in $\mathcal{A}^{dup}$.

For a given TA $\mathcal{A}$, a belief $\mathfrak{b}$ is said to be *bad for full ET-opacity* when exactly one of the following two conditions is satisfied: 1) $(\mathfrak{b} \cap \mathsf{R}^F_{\mathcal{A}} \cap \mathsf{Secret}_{\mathcal{A}} \neq \emptyset)$, or 2) $(\mathfrak{b} \cap \mathsf{R}^F_{\mathcal{A}} \cap \overline{\mathsf{Secret}_{\mathcal{A}}} \neq \emptyset)$.

For a given TA $\mathcal{A}$, a belief $\mathfrak{b}$ is said to be *bad for weak ET-opacity* when $(\mathfrak{b} \cap \mathsf{R}^F_{\mathcal{A}} \cap \mathsf{Secret}_{\mathcal{A}} \neq \emptyset)$ and $(\mathfrak{b} \cap \mathsf{R}^F_{\mathcal{A}} \cap \overline{\mathsf{Secret}_{\mathcal{A}}} = \emptyset)$.

There is no bad belief for $\exists$-ET-opacity, but here we want to verify that at least one duration corresponds to both a private and a public run. We are then looking for a good belief. For a given TA $\mathcal{A}$, a belief $\mathfrak{b}$ is said to be *good for* $\exists$*-ET-opacity* when $(\mathfrak{b} \cap \mathsf{R}^F_{\mathcal{A}} \cap \mathsf{Secret}_{\mathcal{A}} \neq \emptyset)$ and $(\mathfrak{b} \cap \mathsf{R}^F_{\mathcal{A}} \cap \overline{\mathsf{Secret}_{\mathcal{A}}} \neq \emptyset)$.



(a) TA $\mathcal{A}_2$ (b) Belief automaton $\mathcal{B}_{\mathcal{A}_2}$

Fig. 2: $\mathcal{A}_2$ and the corresponding belief automaton

Example 6. In this example and the following ones, we associate each belief either to an open interval or to an integer, and, by abuse of notation, since the automaton has only one clock, we write $(\ell, (\tau, \tau'))$ for the region containing the state $(\ell, \mu(x_1))$ with $\mu(x_1) \in (\tau, \tau'), \tau \in \mathbb{N}, \tau' = +\infty$ if $\tau = c_1$, $\tau' = \tau + 1$ otherwise. Similarly, we write (ℓ, τ) for the region containing the state $(\ell, \mu(x_1)), \mu(x_1) = \tau \in \mathbb{N}$.

Let $\mathcal{A}_2$ be the TA in Fig. 2a. With the global invariant $x \leq 1$, we have the following beliefs. Here, the value of clock z is not given as, in this example, it is equivalent to the value of x. (See Example 9 in Appendix D for an example with z.)

The corresponding belief automaton is depicted in Fig. 2b.

$$
\begin{aligned}
\mathfrak{b}_0 &= \big\{(\ell_0, 0), (\ell_{priv}, 0), (\ell_f^p, 0), (\ell_f, 0)\big\} \\
\mathfrak{b}'_0 &= \big\{(\ell_0, 0), (\ell_{priv}, 0), (\ell_f^p, 0)\big\} \\
\mathfrak{b}_{(0,1)} &= \big\{(\ell_0, (0,1)), (\ell_{priv}, (0,1)), (\ell_f, (0,1))\big\} \\
\mathfrak{b}'_{(0,1)} &= \big\{(\ell_0, (0,1)), (\ell_{priv}, (0,1))\big\} \\
\mathfrak{b}_1 &= \big\{(\ell_0, 1), (\ell_0, 0), (\ell_{priv}, 0), (\ell_f^p, 0), (\ell_f, 0)\big\} \\
\mathfrak{b}'_1 &= \big\{(\ell_0, 1), (\ell_0, 0), (\ell_{priv}, 0), (\ell_f^p, 0)\big\}
\end{aligned}
$$

Beliefs and strategy For a TA $\mathcal{A}$ and a strategy σ, we denote by $\mathfrak{b}_t^\sigma$ the set of regions in which we can be after a time t while following a strategy σ, i.e., $r \in \mathfrak{b}_t^\sigma$ when there exists ρ in $\mathcal{A}^{dup}$ such that ρ is σ-compatible, $last(\rho) \in r, r \in \mathsf{R}_{\mathcal{A}^{dup}}$ and $dur(\rho) = t$.

We define $\mathbb{B}_{\mathcal{A}}^\sigma$ as the set of beliefs reachable by a strategy σ. Formally, for a given strategy σ: $\mathbb{B}_{\mathcal{A}}^\sigma = \{\mathfrak{b}_t^\sigma \mid t \in \mathbb{R}_{\geq 0}\}$.

A strategy for a belief automaton, called a $\mathfrak{b}$-*strategy*, is a function which associates to a sequence of actions the next available action. Formally, a $\mathfrak{b}$-strategy is a function $\alpha : (\mathfrak{A}^{\mathcal{B}_\mathcal{A}})^* \to \mathfrak{A}^{\mathcal{B}_\mathcal{A}}$. A *state* in a belief automaton controlled by a $\mathfrak{b}$-strategy is made of the sequence of actions performed until that state is reached, and the current belief.

Definition 11 (Controlled belief automaton). *For a belief automaton $\mathcal{B}_\mathcal{A}$ and a $\mathfrak{b}$-strategy α, we define $\mathcal{B}^\alpha_\mathcal{A} = (\mathfrak{S}^{\mathcal{B}^\alpha_\mathcal{A}}, \mathfrak{A}^{\mathcal{B}^\alpha_\mathcal{A}}, (\varepsilon, \bot), \mathfrak{d}^{\mathcal{B}^\alpha_\mathcal{A}})$ the belief automaton controlled by α as follows:*

1. $\mathfrak{S}^{\mathcal{B}^\alpha_\mathcal{A}} = (\mathfrak{A}^{\mathcal{B}_\mathcal{A}})^* \times \mathfrak{S}^{\mathcal{B}_\mathcal{A}}$ *is the set of states,*
2. $\mathfrak{A}^{\mathcal{B}^\alpha_\mathcal{A}} = \mathfrak{A}^{\mathcal{B}_\mathcal{A}} = \{0, 0^+, 1\} \times 2^{\Sigma_c}$ *is the alphabet,*
3. $(\varepsilon, \bot)$ *is the initial state,*
4. $\mathfrak{d}^{\mathcal{B}^\alpha_\mathcal{A}} \subseteq (\mathfrak{S}^{\mathcal{B}^\alpha_\mathcal{A}} \times \mathfrak{A}^{\mathcal{B}^\alpha_\mathcal{A}} \times \mathfrak{S}^{\mathcal{B}^\alpha_\mathcal{A}})$ *and* $((v, \mathfrak{b}), (\dagger, \mathfrak{C}), (v \cdot (\dagger, \mathfrak{C}), \mathfrak{b}')) \in \mathfrak{d}^{\mathcal{B}^\alpha_\mathcal{A}}$ *if* $(\mathfrak{b}, (\dagger, \mathfrak{C}), \mathfrak{b}') \in \mathfrak{d}^{\mathcal{B}_\mathcal{A}}$, *and* $\alpha(v) = (\dagger, \mathfrak{C})$ *with* $\dagger \in \{0, 0^+, 1\}$.

We define a *finitely-varying* $\mathfrak{b}$-*strategy* α in such a way that it corresponds to a finitely-varying strategy for a TA: for all $k \in \mathbb{N}$ such that $\alpha^{(k)}(\varepsilon) = (0^+, \mathfrak{C})$ for some $\mathfrak{C}$, there exists a $k' > k \in \mathbb{N}$ such that $\alpha^{(k')}(\varepsilon) = (1, \mathfrak{C}')$ for some $\mathfrak{C}'$, with $\alpha^{(i)}(\varepsilon) = \alpha(\ldots(\alpha(\varepsilon)))$ where α is applied i times.

In order to define the correspondence between a strategy for a TA and a $\mathfrak{b}$-strategy for the corresponding belief automaton, we need to associate an interval of time $t(v)$ to a sequence of transitions $v = (\dagger_1, \mathfrak{C}_1) \cdots (\dagger_n, \mathfrak{C}_n)$. Let $\#_\dagger(v)$ be the number of indices $i, 0 < i \leq n$, such that $\dagger_i = 1$; then

$$t(v) = \begin{cases} \{\#_\dagger(v)/2\} & \text{if } \#_\dagger(v) \equiv 0 \pmod 2 \\ (\lfloor \#_\dagger(v)/2 \rfloor, \lfloor \#_\dagger(v)/2 \rfloor + 1) & \text{otherwise} \end{cases}$$

Definition 12 (Strategy correspondence).

Let $\mathcal{A}$ be a TA. We say that σ, a finitely-varying strategy of $\mathcal{A}$, corresponds *to α, a finitely-varying $\mathfrak{b}$-strategy of $\mathcal{B}_\mathcal{A}$, denoted by $\sigma \vdash \alpha$, when:*

1. $\alpha(\varepsilon) = (0, \sigma(0))$,
2. $\alpha(v) = (1, \mathfrak{C})$ *if* $\exists \tau \in t(v \cdot (1, \mathfrak{C})), \sigma(\tau) = \mathfrak{C}$ *and there is no* $\tau' < \tau$ *such that* $\tau' \in t(v \cdot (1, \mathfrak{C}))$ *and* $\sigma(\tau') \neq \sigma(\tau)$,
3. *for* $n \geq 0$, $\alpha(v \cdot (1, \mathfrak{C}_0) \cdot (0^+, \mathfrak{C}_1) \cdot \ldots \cdot (0^+, \mathfrak{C}_n)) = (0^+, \mathfrak{C}_{n+1})$ *if there exist* $\tau_0 < \ldots < \tau_{n+1}$ *such that for all* $0 \leq i \leq n+1$, $\tau_i \in t(v \cdot (1, \mathfrak{C}_0))$, $\sigma(\tau_i) = \mathfrak{C}_i$ *and, for all* $0 \leq i \leq n$, *there is no* τ'_i, $\tau_i < \tau'_i < \tau_{i+1}$ *such that* $\sigma(\tau_i) \neq \sigma(\tau'_i) \neq \sigma(\tau_{i+1})$.

In other words, within a time interval of the form $(t, t+1)$ with $t \in \mathbb{N}$, the $\mathfrak{b}$-strategy α does not keep track of the precise timestamps of stragegy changes in σ but makes the same changes in the same order.A belief $\mathfrak{b}$ is *reachable in* $\mathcal{B}^\alpha_\mathcal{A}$ when there exists a word $v \in (\mathfrak{A}^{\mathcal{B}_\mathcal{A}})^*$ such that the state $(v, \mathfrak{b})$ is reachable. We define a run that follows a $\mathfrak{b}$-strategy as follows.

Definition 13 (Feasible run). *Let $\mathcal{A}$ be a TA, ρ be a run of $\mathcal{A}$ and $v \in (\mathfrak{A}^{\mathcal{B}_\mathcal{A}})^*$. We say that ρ admits v, denoted $\rho \models v$ when one of the following holds*

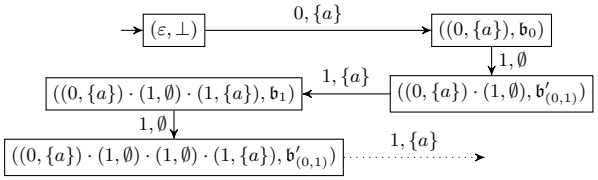


Fig. 3: $\mathcal{B}^{\alpha}_{\mathcal{A}_2}$: First states of the controlled belief automaton for TA $\mathcal{A}_2$ and $\mathfrak{b}$-strategy α

1. $\rho = (\ell_0, \mathbf{0}), (0, \mathsf{e}_0), (\ell_1, \mathbf{0}), \ldots, (0, \mathsf{e}_{n-1}), (\ell_n, \mathbf{0})$, $v = (0, \mathfrak{C}_0)$ *and for all* $0 \leq i < n$, $\mathsf{e}_i = (\ell_i, g_i, a_i, R_i, \ell'_i)$ *with* $a_i \in \mathfrak{C}_0 \cup \Sigma_u$.
2. $\rho = (\ell_0, \mathbf{0}), (d_0, \mathsf{e}_0), (\ell_1, \mu_1), \ldots, (d_{n-1}, \mathsf{e}_{n-1}), (\ell_n, \mu_n)$ *and* $v = v' \cdot (\dagger, \mathfrak{C})$, *with* $\mathsf{e}_{n-1} = (\ell, g, a, R, \ell')$ *where* $a \in \mathfrak{C} \cup \Sigma_u$, $\sum_{i=0}^{n-1} d_i \in t(v)$ *and for* $\rho' = (\ell_0, \mathbf{0}), (d_0, \mathsf{e}_0), (\ell_1, \mu_1), \ldots, (d_{n-2}, \mathsf{e}_{n-2}), (\ell_{n-1}, \mu_{n-1})$ *either* $\rho' \models v$, *or* $\rho' \models v'$, $d_{n-1} > 0$ *and* $\dagger = 1$.

Given a $\mathfrak{b}$*-strategy* α, ρ *is feasible in* $\mathcal{B}^{\alpha}_{\mathcal{A}}$ *when there exist* $v \in (\mathfrak{A}^{\mathcal{B}_{\mathcal{A}}})^*$ *and a belief* $\mathfrak{b} \in \mathfrak{S}^{\mathcal{B}_{\mathcal{A}}}$ *such that* $\rho \models v$ *and* $(v, \mathfrak{b})$ *is reachable in* $\mathcal{B}^{\alpha}_{\mathcal{A}}$.

Example 7. Let $\mathcal{A}_2$ be the TA in Fig. 2. Let σ be a strategy such that $\mathcal{A}_2$ is fully ET-opaque defined as follows:

$$\sigma(\tau) = \begin{cases} \{a\} & \text{if } \tau \in \mathbb{N} \\ \emptyset & \text{otherwise} \end{cases}$$

Let α be a $\mathfrak{b}$-strategy for $\mathcal{B}_{\mathcal{A}_2}$ such that $\sigma \vdash\!\dashv \alpha$:

$$\alpha(v) = \begin{cases} (0, \{a\}) & \text{if } v = \varepsilon \\ (1, \emptyset) & \text{if } v \in (0, \{a\}) \cdot ((1, \emptyset) \cdot (1, \{a\}))^* \\ (1, \{a\}) & \text{if } v \in (0, \{a\}) \cdot (1, \emptyset) \cdot ((1, \{a\}) \cdot (1, \emptyset))^* \end{cases}$$

Then, the first states of the automaton $\mathcal{B}^{\alpha}_{\mathcal{A}_2}$ are depicted in Fig. 3.
Runs ρ_1 and ρ_2 are feasible in $\mathcal{B}^{\alpha}_{\mathcal{A}_2}$:

$$\rho_1 = (\ell_0, 0), (1, \mathsf{e}_1), (\ell_0, 0), (0, \mathsf{e}_2), (\ell_{priv}, 0), (0, \mathsf{e}_3), (\ell_f, 0)$$
$$\rho_2 = (\ell_0, 0), (1, \mathsf{e}_1), (\ell_0, 0), (0, \mathsf{e}_4), (\ell_f, 0)$$

For $v = (0, \{a\}) \cdot (1, \emptyset) \cdot (1, \{a\})$ a sequence of actions in the automaton $\mathcal{B}^{\alpha}_{\mathcal{A}_2}$, we have $\rho_1 \models v$ and $\rho_2 \models v$.

5 Solving ET-opacity problems through the belief automaton

We first characterize the different notions of ET-opacity of a TA with beliefs.

Lemma 1 (Beliefs characterization for full ET-opacity). *A TA $\mathcal{A}$ is fully ET-opaque with a strategy σ iff, for all $\mathfrak{b} \in \mathbb{B}^{\sigma}_{\mathcal{A}}$, $\mathfrak{b}$ is not bad for full ET-opacity.*

Proof.

$\Rightarrow$ Let $\mathcal{A}$ be a TA that is fully ET-opaque with strategy σ. Let $\mathfrak{b} \in \mathbb{B}^{\sigma}_{\mathcal{A}}$. Suppose w.l.o.g. that $\mathfrak{b} \cap \mathsf{R}^{F}_{\mathcal{A}} \cap \mathsf{Secret}_{\mathcal{A}} \neq \emptyset$. Let $r \in \mathfrak{b} \cap \mathsf{R}^{F}_{\mathcal{A}} \cap \mathsf{Secret}_{\mathcal{A}}$. Then there is a σ-compatible run $\rho \in \mathit{Visit}^{priv}_{\sigma}(\mathcal{A})$ such that $\mathit{last}(\rho) \in r$. $\mathcal{A}$ being fully ET-opaque with strategy σ, $\mathit{DVisit}^{priv}_{\sigma}(\mathcal{A}) = \mathit{DVisit}^{\overline{priv}}_{\sigma}(\mathcal{A})$. Thus, there exists $\rho' \in \mathit{Visit}^{\overline{priv}}_{\sigma}(\mathcal{A})$ such that $\mathit{dur}(\rho') = \mathit{dur}(\rho)$. Denoting $r' = [\mathit{last}(\rho')]$, we have by definition that $r' \in \mathfrak{b} \cap \mathsf{R}^{F}_{\mathcal{A}} \cap \overline{\mathsf{Secret}_{\mathcal{A}}}$. Therefore $\mathfrak{b} \cap \mathsf{R}^{F}_{\mathcal{A}} \cap \overline{\mathsf{Secret}_{\mathcal{A}}} \neq \emptyset$.

$\Leftarrow$ If $\mathit{DVisit}^{priv}_{\sigma}(\mathcal{A}) \cup \mathit{DVisit}^{\overline{priv}}_{\sigma}(\mathcal{A}) = \emptyset$, $\mathcal{A}$ is fully ET-opaque with σ by definition. We thus assume otherwise and select $t \in \mathit{DVisit}^{priv}_{\sigma}(\mathcal{A}) \cup \mathit{DVisit}^{\overline{priv}}_{\sigma}(\mathcal{A})$. W.l.o.g. we can assume that $t \in \mathit{DVisit}^{priv}_{\sigma}(\mathcal{A})$. There thus exists a private σ-compatible run ρ of duration t. In particular, $[\mathit{last}(\rho)] \in \mathfrak{b}_t$. By hypothesis, as $\mathfrak{b}_t \cap \mathsf{R}^{F}_{\mathcal{A}} \neq \emptyset$ (because of ρ), we have that $\mathfrak{b}_t \cap \mathsf{R}^{F}_{\mathcal{A}} \cap \overline{\mathsf{Secret}_{\mathcal{A}}} \neq \emptyset$. Thus, there exists a σ-compatible run ρ' such that $\mathit{dur}(\rho') = t$ and $[\mathit{last}(\rho')] \in \mathfrak{b}_t \cap \mathsf{R}^{F}_{\mathcal{A}} \cap \overline{\mathsf{Secret}_{\mathcal{A}}}$. By definition of these sets, this implies that $t \in \mathit{DVisit}^{\overline{priv}}_{\sigma}(\mathcal{A})$. Hence, $\mathit{DVisit}^{priv}_{\sigma}(\mathcal{A}) = \mathit{DVisit}^{\overline{priv}}_{\sigma}(\mathcal{A})$ and $\mathcal{A}$ is fully ET-opaque with σ. □

Lemma 2 (Beliefs characterization for weak ET-opacity). *A TA $\mathcal{A}$ is weakly ET-opaque with a strategy σ iff, for all $\mathfrak{b} \in \mathbb{B}^{\sigma}_{\mathcal{A}}$, $\mathfrak{b}$ is not bad for weak ET-opacity.*

Proof. This proof can be achieved similarly to the proof of Lemma 1. □

Lemma 3 (Beliefs characterization for $\exists$-ET-opacity). *A TA $\mathcal{A}$ is $\exists$-ET-opaque with a strategy σ iff there exists $\mathfrak{b} \in \mathbb{B}^{\sigma}_{\mathcal{A}}$ such that $\mathfrak{b}$ is good for $\exists$-ET-opacity.*

Proof.

$\Rightarrow$ Let $\mathcal{A}$ be a TA $\exists$-ET-opaque with strategy σ. Since $\mathit{DVisit}^{priv}_{\sigma}(\mathcal{A}) \cap \mathit{DVisit}^{\overline{priv}}_{\sigma}(\mathcal{A}) \neq \emptyset$, there exist ρ, ρ' σ-compatible such that $\rho \in \mathit{Visit}^{priv}_{\sigma}(\mathcal{A})$, $\rho' \in \mathit{DVisit}^{\overline{priv}}_{\sigma}(\mathcal{A})$ and $\mathit{dur}(\rho) = \mathit{dur}(\rho')$. Then $[\mathit{last}(\rho)] \in \mathfrak{b}_{\mathit{dur}(\rho)} \cap \mathsf{R}^{F}_{\mathcal{A}} \cap \mathsf{Secret}_{\mathcal{A}}$ and $[\mathit{last}(\rho')] \in \mathfrak{b}_{\mathit{dur}(\rho)} \cap \mathsf{R}^{F}_{\mathcal{A}} \cap \overline{\mathsf{Secret}_{\mathcal{A}}}$, and so $\mathfrak{b}_{\mathit{dur}(\rho)}$ is a good belief for $\exists$-ET-opacity.

$\Leftarrow$ Let $\mathfrak{b}_t \in \mathbb{B}^{\sigma}_{\mathcal{A}}$ such that $\mathfrak{b}_t \cap \mathsf{R}^{F}_{\mathcal{A}} \cap \mathsf{Secret}_{\mathcal{A}} \neq \emptyset$ and $\mathfrak{b}_t \cap \mathsf{R}^{F}_{\mathcal{A}} \cap \overline{\mathsf{Secret}_{\mathcal{A}}} \neq \emptyset$. Then, there exist ρ, ρ' σ-compatible with $\mathit{dur}(\rho) = \mathit{dur}(\rho') = t$ such that $[\mathit{last}(\rho)] \in \mathfrak{b}_t \cap \mathsf{R}^{F}_{\mathcal{A}} \cap \mathsf{Secret}_{\mathcal{A}}$ and $[\mathit{last}(\rho')] \in \mathfrak{b}_t \cap \mathsf{R}^{F}_{\mathcal{A}} \cap \overline{\mathsf{Secret}_{\mathcal{A}}}$. Finally, $t \in \mathit{DVisit}^{priv}_{\sigma}(\mathcal{A}) \cap \mathit{DVisit}^{\overline{priv}}_{\sigma}(\mathcal{A})$ and $\mathcal{A}$ is $\exists$-ET-opaque with σ. □

We prove in the following that a strategy in the TA matches a $\mathfrak{b}$-strategy in the belief automaton as do the runs and sequences of actions in belief automaton.

Lemma 4 (Strategy correspondence). *Let $\mathcal{A}$ be a TA. Given a finitely-varying strategy σ of $\mathcal{A}$, there is a finitely-varying $\mathfrak{b}$-strategy α of $\mathcal{B}_\mathcal{A}$ such that $\sigma \vdash\!\dashv \alpha$. Reciprocally, given a finitely-varying $\mathfrak{b}$-strategy α of $\mathcal{B}_\mathcal{A}$, there is a finitely-varying strategy σ of $\mathcal{A}$ such that $\sigma \vdash\!\dashv \alpha$.*

Proof. Let σ be a finitely-varying strategy for $\mathcal{A}$. For any interval $[i, i+1)$, $i \in \mathbb{N}$, let $p_{i_0}, p_{i_1}, \ldots, p_{i_{n_i}}$ be a finite partition into intervals such that σ makes the same choice within each p_{i_j}. We can assume w.l.o.g. that integers appear as singleton within this partition.

We build the $\mathfrak{b}$-strategy α by imitating the structure of Definition 12:

- $\alpha(\varepsilon) = (0, \sigma(0))$,
- for all $v \in (\mathfrak{A}^{\mathcal{B}_\mathcal{A}})^+$, with $|v|$ denoting the length of the word v,
  - if $t(v) = \{\iota\}$ is a singleton then by assumption, $p_{\iota_0} = t(v)$ and we set $\alpha(v) = (1, \sigma(\tau))$ for some $\tau \in p_{\iota_1}$,
  - otherwise, $v = v' \cdot (1, \mathfrak{C}_1) \cdot v''$ such that $v'' = (0^+, \mathfrak{C}_2) \cdot \ldots \cdot (0^+, \mathfrak{C}_k)$ and as σ is finitely-varying, there exist ι, n_ι such that $\bigcup_{j=1}^{n_\iota} p_{\iota_j} = t(v)$ and we can assume w.l.o.g. that for all $1 \leq j < n$, for any $\tau \in p_{\iota_j}$, $\tau' \in p_{\iota_{j+1}}$, $\sigma(\tau) \neq \sigma(\tau')$. Then,

$$\alpha(v) = \begin{cases} (0^+, \sigma(\tau)), \text{ for some } \tau \in p_{\iota_{2+|v''|}} & \text{if } |v''| < n_\iota - 1 \\ (1, \sigma(\tau)), \text{ for some } \tau \in p_{\iota'_0}, \iota' = \iota + 1 & \text{otherwise} \end{cases}$$

By construction, α is finitely-varying and $\sigma \vdash\!\dashv \alpha$.

Conversely, let α be a finitely-varying $\mathfrak{b}$-strategy, let us build σ such that $\sigma \vdash\!\dashv \alpha$. Let $\tau \in \mathbb{R}_{\geq 0}$ be a time instant and $v = (\dagger_0, \mathfrak{C}_0) \cdot \ldots \cdot (\dagger_k, \mathfrak{C}_k) = (\alpha)^{(1)}(\varepsilon) \cdot \ldots \cdot (\alpha)^{(k)}(\varepsilon)$ be the smallest sequence such that $t(v) = \{\iota\}$ is a singleton and $\iota \geq \tau$. As the strategy is finitely-varying this sequence is finite, and we have $\dagger_k = 1$, then:

- either τ is an integer, then we fix $\sigma(\tau) = \mathfrak{C}_k$;
- otherwise, let $j < k$ be the greatest integer such that $\dagger_j = 1$. Consider then the sequence $(\alpha)^{(j)}(\varepsilon) \cdot \ldots \cdot (\alpha)^{(k)}(\varepsilon) = (1, \mathfrak{C}_j) \cdot (0^+, \mathfrak{C}_{j+1}) \cdot \ldots \cdot (0^+, \mathfrak{C}_{k-1}) \cdot (1, \mathfrak{C}_k)$ and denote $m = k - j$, we define $\sigma(\tau) = \mathfrak{C}_i$ where $i = j + \lfloor \mathrm{fr}(\tau) * m \rfloor$.

By construction, σ is finitely-varying and $\sigma \vdash\!\dashv \alpha$. □

Lemma 5 (Strategies and runs acceptance). *Let $\mathcal{A}$ be a TA, ρ a run of $\mathcal{A}$, σ a finitely-varying strategy and α a finitely-varying $\mathfrak{b}$-strategy such that $\sigma \vdash\!\dashv \alpha$. ρ is σ-compatible iff ρ is feasible in $\mathcal{B}^\alpha_\mathcal{A}$.*

Proof.

⇒ Let $\rho = (\ell_0, \mathbf{0}), (d_0, \mathsf{e}_0), \ldots, (d_{n-1}, \mathsf{e}_{n-1}), (\ell_m, \mu_m)$ be a σ-compatible run. By definition of a run, for all $0 \leq i < n$, there exists a sequence of transitions $(\ell_i, \mu_i) \xmapsto{d_i} (\ell_i, \mu'_i) \xmapsto{\mathsf{e}_i} (\ell_{i+1}, \mu_{i+1})$ in $TTS_\mathcal{A}$ with $\mathsf{e}_i = (\ell_i, g, a, R, \ell_{i+1})$ s.t. $a \in \sigma\left(\sum_{j \leq i} d_j\right) \cup \Sigma_u$.

For all transitions in the $TTS_{\mathcal{A}}$, there exist $\mathfrak{b}, \mathfrak{b}'$ such that the initial state of the transition belongs to $\mathfrak{b}$ and the target state belongs to $\mathfrak{b}'$, and such that either $\mathfrak{b} = \mathfrak{b}'$ or there is a transition between them in the belief automaton. More exactly, there is $(\mathfrak{b}, (\dagger, \mathfrak{C}), \mathfrak{b}') \in \delta^{\mathcal{B}_{\mathcal{A}}}$ such that $[(\ell_{i+1}, \mu_{i+1})] \in \mathfrak{b}', \mathsf{e}_i \in (\mathfrak{C} \cup \Sigma_u)$ and *i)* if $\lfloor \mu_i(z) \rfloor = \lfloor \mu_{i+1}(z) \rfloor$, and $\mathrm{fr}(\mu_i(z)) = 0$ iff $\mathrm{fr}(\mu_{i+1}(z)) = 0$. then $[(\ell_i, \mu_i)] \in \mathfrak{b}$ and $\dagger \in \{0, 0^+\}$, *ii)* otherwise, $\dagger = 1$ and $\exists \mathfrak{b}_{i_1}, \ldots, \mathfrak{b}_{i_{m-1}}$ s.t. $[(\ell_i, \mu_i)] \in \mathfrak{b}_{i_1}$ and $(\mathfrak{b}_{i_1}, (1, \mathfrak{C}_1), \mathfrak{b}_{i_2}), \ldots, (\mathfrak{b}_{i_{m-1}}, (1, \mathfrak{C}_{m-1}), \mathfrak{b}) \in \delta^{\mathcal{B}_{\mathcal{A}}}$.
Finally, as $a \in \sigma\left(\sum_{j \leq i} d_j\right) \cup \Sigma_u$, for all $0 \leq i < n$, and $\sigma \vdash \alpha$, the transition associated to each action will be available in $\mathcal{B}^{\alpha}_{\mathcal{A}}$ and ρ is feasible in $\mathcal{B}^{\alpha}_{\mathcal{A}}$.

$\Leftarrow$ Let $\rho = (\ell_0, \mathbf{0}), (d_0, \mathsf{e}_0), \ldots, (d_{n-1}, \mathsf{e}_{n-1}), (\ell_n, \mu_n)$ feasible in $\mathcal{B}^{\alpha}_{\mathcal{A}}$. Then, for all $0 \leq i < n$, there is $\mathfrak{b}_{i_1}, \ldots, \mathfrak{b}_{i_m}$ with $\mathfrak{b}_{i_1}$ reachable with $(\dagger_1, \mathfrak{C}_1), \ldots, (\dagger_k, \mathfrak{C}_k)$ and such that $[(\ell_i, \mu_i)] \in \mathfrak{b}_{i_1}$ and:

- if $d_i = 0$, $\sum_{j \leq i} d_j \in t((\dagger_1, \mathfrak{C}_1) \cdot \ldots \cdot (\dagger_k, \mathfrak{C}_k))$ and the action a_i of the edge e_i belongs to $\mathfrak{C}_k \cup \Sigma_u$,
- otherwise, $\sum_{j \leq i} d_j \in t((\dagger_1, \mathfrak{C}_1) \cdot \ldots \cdot (\dagger_k, \mathfrak{C}_k)(\dagger_{i_1}, \mathfrak{C}_{i_1}) \cdot \ldots \cdot (\dagger_{i_{m-1}}, \mathfrak{C}_{i_{m-1}}))$ and the action a_i of the edge e_i belongs to $\mathfrak{C}_{i_{m-1}} \cup \Sigma_u$.

In both cases, as $\sigma \vdash \alpha$, $a_i \in \sigma(\sum_{j \leq i} d_j)$ and then ρ is σ-compatible. □

Finally, we can prove that reasoning on the TA is equivalent to reasoning on the belief automaton.

Theorem 1. *Let $\mathcal{A}$ be a TA. Given a finitely-varying strategy σ such that $\mathcal{A}$ is fully (resp. weakly) ET-opaque with σ, there exists $\sigma \vdash \alpha$ such that there is no belief that is bad for full (resp. weak) ET-opacity reachable in $\mathcal{B}^{\alpha}_{\mathcal{A}}$. Reciprocally, given a $\mathfrak{b}$-strategy α such that there is no belief that is bad for full (resp. weak) ET-opacity reachable in $\mathcal{B}^{\alpha}_{\mathcal{A}}$, there exists $\sigma \vdash \alpha$ such that $\mathcal{A}$ is fully (resp. weakly) ET-opaque with σ.*

Proof. Let $\mathcal{A}$ be a TA and σ a finitely-varying strategy such that $\mathcal{A}$ is fully ET-opaque (resp. weakly ET-opaque) with σ. By Lemma 4, the existence of the finitely-varying strategy σ is equivalent to the existence of α a $\mathfrak{b}$-strategy with $\sigma \vdash \alpha$. By Lemma 5, we know that it is equivalent for a run ρ to be σ-compatible or feasible in $\mathcal{B}^{\alpha}_{\mathcal{A}}$. By Definition 13, this means that there is a sequence v of actions of $\mathcal{B}^{\alpha}_{\mathcal{A}}$ such that $\rho \models v$ and there is a belief $\mathfrak{b} = \mathfrak{b}^{\sigma}_{dur(\rho)} \in \mathbb{B}^{\sigma}_{\mathcal{A}}$ such that $(v \cdot \mathfrak{b})$ is reachable in $\mathcal{B}^{\alpha}_{\mathcal{A}}$. This results that the set of reachable beliefs in $\mathcal{B}^{\alpha}_{\mathcal{A}}$ is equal to the set $\mathbb{B}_{\mathcal{A}}$. Finally, by Lemma 1 (resp. Lemma 2), there is no belief bad for full ET-opacity (resp. for weak ET-opacity) reachable in $\mathbb{B}^{\sigma}_{\mathcal{A}}$, and therefore, as the two sets are equal, neither in $\mathcal{B}^{\alpha}_{\mathcal{A}}$. □

Theorem 2. *Let $\mathcal{A}$ be a TA, and σ a finitely-varying strategy, $\mathcal{A}$ is $\exists$-ET-opaque with σ iff there exists $\sigma \vdash \alpha$ such that there is a belief that is good for $\exists$-ET-opacity reachable in $\mathcal{B}^{\alpha}_{\mathcal{A}}$.*

Proof. The proof is closed to the one of Theorem 1. By Lemma 3, as $\mathcal{A}$ is $\exists$-ET-opaque, there is a good belief for $\exists$-ET-opacity reachable in $\mathbb{B}^{\sigma}_{\mathcal{A}}$, and therefore, as the set of reachable beliefs in $\mathcal{B}^{\alpha}_{\mathcal{A}}$ being equal to the one of $\mathbb{B}^{\sigma}_{\mathcal{A}}$, there is a good belief for $\exists$-ET-opacity in $\mathcal{B}^{\alpha}_{\mathcal{A}}$, and vice versa. □

Finding a $\mathfrak{b}$-strategy to avoid bad beliefs within $\mathcal{B}_{\mathcal{A}}$ amounts to solving a one-player safety game on a finite arena. More precisely, a one-player safety game can be defined by a tuple $\mathcal{G} = (Q, q_0, \delta^{\mathcal{G}}, Bad)$ where Q is a set of states, $q_0 \in Q$ is the initial state, $\delta^{\mathcal{G}} \subseteq Q \times Q$, and $Bad \subseteq Q$. Starting from q_0, at each step, the player selects an edge from $\delta^{\mathcal{G}}$ to reach a new state. The player wins if no state from Bad is ever reached. As the belief automaton is deterministic, the interpretation of the belief automaton as a one-player safety game consists simply in removing the labels. Deciding the existence of a winning strategy in one-player safety games, and computing it if it exists, can be done in PTIME using a fixed-point algorithm [23]. In the following lemma, we show that deciding the existence of a winning strategy can even be done in NLOGSPACE.

Lemma 6. *Deciding the existence of a winning strategy in a one-player safety game can be decided in* NLOGSPACE *and its computation is solvable.*

Proof. Let $\mathcal{G} = (Q, q_0, \delta^{\mathcal{G}}, Bad)$ be a one-player safety game. For $n = |Q| + 1$, there exists a sequence $q_0, \dots, q_n$ of states such that, for all $i < n, (q_i, q_{i+1}) \in \delta^{\mathcal{G}}$ and for all $i \leq n$, $q_i \notin Bad$ iff there exists a winning strategy for the player in the game.

Indeed, if no such sequence exists, then Bad is reached in at most n steps, ensuring that the player has no winning strategy. Conversely, if such a sequence exists, then there exist i, j such that $i < j$ and $q_i = q_j$. Thus a winning strategy consists in following the sequence until q_i is reached, and then to repeat the choices made from q_i to q_{j-1}.

The existence of this sequence can be tested in NLOGSPACE by starting from q_0 and guessing n times the next state within $Q \setminus Bad$. Finally, this sequence is the winning strategy which is therefore computable. □

Theorem 3. *The full (resp. weak) ET-opacity finitely-varying controller emptiness problem is decidable; and the full (resp. weak) ET-opacity finitely-varying controller synthesis problem is solvable.*

Proof. First, for a TA $\mathcal{A}$, we know by Theorem 1 that if there is a strategy σ such that $\mathcal{A}$ is fully ET-opaque with σ then there is a $\mathfrak{b}$-strategy α such that no bad belief is reachable in $\mathcal{B}^{\alpha}_{\mathcal{A}}$. In other words, there is a winning strategy in the one-player safety game $\mathcal{G} = (\mathfrak{S}^{\mathcal{B}^{\alpha}_{\mathcal{A}}}, (\varepsilon, \bot), \mathfrak{d}^{\mathcal{B}^{\alpha}_{\mathcal{A}}}, Bad)$ where $Bad = \{\mathfrak{b} \mid \mathfrak{b} \text{ is bad for full ET-opacity}\}$. By Lemma 6, the existence of a winning strategy in this game is decidable. Then, the full ET-opacity finitely-varying controller emptiness problem is decidable. Moreover, by Lemma 6 a winning strategy in this game is computable if it exists. Then, the full ET-opacity finitely-varying controller synthesis problem is solvable. The same reasoning can be done for weak ET-opacity. □

6 Extensions: robust definitions of ET-opacity

So far, the attacker needed to measure the execution time with an infinite precision—this is often unrealistic in practice [21,16]. We therefore consider

variants of opacity where intervals of non-opaque execution times can be considered acceptable as long as they are of size 0, i.e., reduced to a point (note that there can be an infinite number of them). We introduce two new notions of opacity: 1) *almost full ET-opacity*, where every punctual opacity violation is ignored, and 2) *closed full ET-opacity*, where a punctual violation is ignored only if it is followed or preceded by an opaque interval.

In order to formally define these two new notions, we introduce new notations: given a set S, then let $[\![S]\!]$ denote the *closure* of S (i.e., the smallest closed set containing S) and let $(\!|S|\!)$ denote the *interior* of S (i.e., the largest open set contained in S). Let $\oplus$ denotes the exclusive `OR` operator such that, for two sets A and B, $A \oplus B = \{v \mid v \in (A \cup B) \setminus (A \cap B)\}$.

Definition 14 (Almost full ET-opacity). *A TA $\mathcal{A}$ is almost fully ET-opaque when* $(\!|DVisit^{priv}(\mathcal{A}) \oplus \overline{DVisit^{priv}}(\mathcal{A})|\!) = \emptyset$.

Definition 15 (Closed full ET-opacity). *A TA $\mathcal{A}$ is closed fully ET-opaque when* $[\![DVisit^{priv}(\mathcal{A})]\!] = [\![\overline{DVisit^{priv}}(\mathcal{A})]\!]$.

Example 8. Let $\mathcal{A}_3$ be a TA such that $DVisit^{priv}(\mathcal{A}_3) = [0,2]$ and $\overline{DVisit^{priv}}(\mathcal{A}_3) = (0,1) \cup (1,2)$. $\mathcal{A}_3$ is not fully ET-opaque (but it is weakly ET-opaque). Note that $(\!|DVisit^{priv}(\mathcal{A}_3)|\!) \neq (\!|\overline{DVisit^{priv}}(\mathcal{A}_3)|\!)$ as $(0,2) \neq ((0,1) \cup (1,2))$ but $(\!|DVisit^{priv}(\mathcal{A}_3) \oplus \overline{DVisit^{priv}}(\mathcal{A}_3)|\!) = (\!|\{0\} \cup \{1\} \cup \{2\}|\!) = \emptyset$, so $\mathcal{A}_3$ is almost fully ET-opaque. Moreover, $[\![DVisit^{priv}(\mathcal{A}_3)]\!] = [\![\overline{DVisit^{priv}}(\mathcal{A}_3)]\!] = [0,2]$ so $\mathcal{A}_3$ is closed fully ET-opaque.

Now, let $\mathcal{A}_4$ be a TA such that $DVisit^{priv}(\mathcal{A}_4) = (0,1) \cup \{2\}$ and $\overline{DVisit^{priv}}(\mathcal{A}_4) = (0,1)$. $\mathcal{A}_4$ is not fully ET-opaque. $(\!|DVisit^{priv}(\mathcal{A}_4) \oplus \overline{DVisit^{priv}}(\mathcal{A}_4)|\!) = \emptyset$ so $\mathcal{A}_4$ is almost fully ET-opaque. $[\![DVisit^{priv}(\mathcal{A}_4)]\!] = [0,1] \cup \{2\} \neq [\![\overline{DVisit^{priv}}(\mathcal{A}_4)]\!] = [0,1]$ so $\mathcal{A}_4$ is not closed fully ET-opaque.

We define similarly *almost weak ET-opacity* and *closed weak ET-opacity* (Definition 20 and Definition 22 in Appendix B).

If we ignore punctual violations in closed ET-opacity and almost ET-opacity, the same idea applied to $\exists$-ET-opacity leads to looking for an interval where all times are opaque. We therefore consider the *existential-interval ET-opacity* (noted $\exists$-interval ET-opacity in the following).

Definition 16 ($\exists$-interval ET-opacity). *A TA $\mathcal{A}$ is $\exists$-interval ET-opaque when* $(\!|DVisit^{priv}(\mathcal{A})|\!) \cap (\!|\overline{DVisit^{priv}}(\mathcal{A})|\!) \neq \emptyset$.

We are interested in the same problems as before for almost ET-opacity, closed ET-opacity and $\exists$-interval ET-opacity. In particular, our aim is to build a controller to make a TA almost ET-opaque (resp. closed ET-opaque, or $\exists$-interval ET-opaque) with a finitely-varying strategy.

Characterization A single belief is not sufficient to characterize a TA that is not almost ET-opaque (resp. closed). Indeed, suppose a time t such that $\mathfrak{b}_t$ is bad for full ET-opacity. This means that a punctual violation of opacity exists. This kind of violation can be allowed in the context of almost and closed full ET-opacity. It is problematic if the times around it are also a violation of opacity.

More specifically, a violation to almost full ET-opacity corresponds to a succession of bad beliefs, i.e., every punctual violation is ignored. On the other hand, a violation of closed full ET-opacity corresponds either to a succession of bad beliefs, or to a unique bad belief surrounded by beliefs that do not contain any final region. Intuitively, a punctual violation is ignored if it belongs to an interval where private and public final states can be reached.

Finally, we can certify the $\exists$-interval ET-opacity of a TA with the reachability of a succession of beliefs containing private and public final states.

The formal definitions of bad belief for almost ET-opacity (Definition 17) and closed ET-opacity (Definition 18), and good belief for $\exists$-interval ET-opacity (Definition 19), can be found in Appendix B.

Theorem 4. *The closed full ET-opacity (resp. weak) finitely-varying controller emptiness problem is decidable; the closed full ET-opacity (resp. weak) finitely-varying controller synthesis problem is solvable.*

As for full ET-opacity, this result is due to the equivalence between finding a strategy for a TA and finding a strategy in the corresponding belief automaton, and to the fact that such a strategy corresponds to a winning strategy in a one-player safety game. All the intermediate results and proofs are available in Appendix C.2. Similar results for closed weak ET-opacity, almost full ET-opacity, almost weak ET-opacity and $\exists$-interval ET-opacity are presented in Appendix C.2.

7 Conclusion

We addressed here the control of a system modeled by a TA to make it $\exists$-ET-opaque, weakly ET-opaque or fully ET-opaque. We showed that the controller synthesis problem can be effectively solvable for these three definitions. We also addressed three extensions ($\exists$-interval ET-opacity, closed full ET-opacity and almost full ET-opacity, with their variants) which can relate to a *robust* setting where the attacker cannot have an infinite precision.

Future works A natural next step will be to introduce timing parameters *à la* [7], and address control in that setting. Addressing the control for the definition of opacity (based on languages) as in [19] would be interesting in two settings: 1) the general setting, where the controller synthesis will be undecidable but may terminate for some semi-algorithms, and 2) decidable subclasses that remain to be exhibited, presumably one-clock TAs.

References

[1] Alur, R., Dill, D.L.: A theory of timed automata. TCS **126**(2), 183–235 (Apr 1994). https://doi.org/10.1016/0304-3975(94)90010-8

[2] Alur, R., Fix, L., Henzinger, T.A.: Event-clock automata: A determinizable class of timed automata. TCS **211**(1-2), 253–273 (1999). https://doi.org/10.1016/S0304-3975(97)00173-4

[3] Alur, R., Henzinger, T.A., Vardi, M.Y.: Parametric real-time reasoning. In: Kosaraju, S.R., Johnson, D.S., Aggarwal, A. (eds.) STOC. pp. 592–601. ACM, New York, NY, USA (1993). https://doi.org/10.1145/167088.167242

[4] Ammar, I., El Touati, Y., Yeddes, M., Mullins, J.: Bounded opacity for timed systems. Journal of Information Security and Applications **61**, 1–13 (Sep 2021). https://doi.org/10.1016/j.jisa.2021.102926

[5] André, É., Bolat, S., Lefaucheux, E., Marinho, D.: strategFTO: Untimed control for timed opacity. In: Artho, C., Ölveczky, P. (eds.) FTSCS. pp. 27–33. ACM (2022). https://doi.org/10.1145/3563822.3568013

[6] André, É., Kryukov, A.: Parametric non-interference in timed automata. In: Li, Y., Liew, A. (eds.) ICECCS. pp. 37–42 (2020). https://doi.org/10.1109/ICECCS51672.2020.00012

[7] André, É., Lefaucheux, E., Lime, D., Marinho, D., Sun, J.: Configuring timing parameters to ensure execution-time opacity in timed automata. In: ter Beek, M.H., Dubslaff, C. (eds.) TiCSA. Electronic Proceedings in Theoretical Computer Science, vol. 392, pp. 1–26 (2023). https://doi.org/10.4204/EPTCS.392.1, invited paper.

[8] André, É., Lime, D., Marinho, D., Sun, J.: Guaranteeing timed opacity using parametric timed model checking. ACM Transactions on Software Engineering and Methodology **31**(4), 1–36 (Oct 2022). https://doi.org/10.1145/3502851

[9] Arcile, J., André, É.: Timed automata as a formalism for expressing security: A survey on theory and practice. ACM Computing Surveys **55**(6), 1–36 (Jul 2023). https://doi.org/10.1145/3534967

[10] Asarin, E., Degorre, A., Dima, C., Inclán, B.J.: Bandwidth of timed automata: 3 classes. In: Bouyer, P., Srinivasan, S. (eds.) FSTTCS. LIPIcs, vol. 284, pp. 10:1–10:17. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2023). https://doi.org/10.4230/LIPICS.FSTTCS.2023.10

[11] Asarin, E., Maler, O., Pnueli, A., Sifakis, J.: Controller synthesis for timed automata. IFAC Proceedings Volumes **31**(18), 447–452 (1998)

[12] Barbuti, R., Francesco, N.D., Santone, A., Tesei, L.: A notion of non-interference for timed automata. FI **51**(1-2), 1–11 (2002)

[13] Barbuti, R., Tesei, L.: A decidable notion of timed non-interference. FI **54**(2-3), 137–150 (2003)

[14] Benattar, G., Cassez, F., Lime, D., Roux, O.H.: Control and synthesis of non-interferent timed systems. International Journal of Control **88**(2), 217–236 (2015). https://doi.org/10.1080/00207179.2014.944356

[15] Bouyer, P., Fang, E., Markey, N.: Permissive strategies in timed automata and games. Electronic Communication of the European Association of Software Science and Technology **72** (2015). https://doi.org/10.14279/tuj.eceasst.72.1015

[16] Bouyer, P., Markey, N., Sankur, O.: Robustness in timed automata. In: Abdulla, P.A., Potapov, I. (eds.) RP. LNCS, vol. 8169, pp. 1–18. Springer (9 2013). https://doi.org/10.1007/978-3-642-41036-9_1, invited paper

[17] Bruyère, V., Dall'Olio, E., Raskin, J.F.: Durations and parametric model-checking in timed automata. ACM Transactions on Computational Logic **9**(2), 12:1–12:23 (2008). https://doi.org/10.1145/1342991.1342996
[18] Bérard, B., Mullins, J., Sassolas, M.: Quantifying opacity. Mathematical Structures in Computer Science **25**(2), 361–403 (2015). https://doi.org/10.1017/S0960129513000637
[19] Cassez, F.: The dark side of timed opacity. In: Park, J.H., Chen, H.H., Atiquzzaman, M., Lee, C., Kim, T.H., Yeo, S.S. (eds.) ISA. LNCS, vol. 5576, pp. 21–30. Springer (2009). https://doi.org/10.1007/978-3-642-02617-1_3
[20] Chen, A., Hong, C., Shang, X., Jing, H., Xu, S.: Timing leakage to break SM2 signature algorithm. Journal of Information Security and Applications **67**, 103210 (2022). https://doi.org/10.1016/J.JISA.2022.103210
[21] De Wulf, M., Doyen, L., Markey, N., Raskin, J.F.: Robustness and implementability of timed automata. In: Lakhnech, Y., Yovine, S. (eds.) FORMATS and FTRTFT. LNCS, vol. 3253, pp. 118–133. Springer (2004). https://doi.org/10.1007/978-3-540-30206-3_10
[22] Dima, C.: Real-time automata. Journal of Automata, Languages and Combinatorics **6**(1), 3–23 (2001). https://doi.org/10.25596/jalc-2001-003
[23] Grädel, E., Thomas, W., Wilke, T. (eds.): Automata, Logics, and Infinite Games: A Guide to Current Research, LNCS, vol. 2500. Springer (2002). https://doi.org/10.1007/3-540-36387-4, outcome of a Dagstuhl seminar (February 2001)
[24] Inclán, B.J., Degorre, A., Asarin, E.: Bounded delay timed channel coding. In: Bogomolov, S., Parker, D. (eds.) FORMATS. LNCS, vol. 13465, pp. 65–79. Springer (2022). https://doi.org/10.1007/978-3-031-15839-1_4
[25] Jurdzinski, M., Trivedi, A.: Reachability-time games on timed automata. In: Arge, L., Cachin, C., Jurdzinski, T., Tarlecki, A. (eds.) ICALP. LNCS, vol. 4596, pp. 838–849. Springer (2007). https://doi.org/10.1007/978-3-540-73420-8_72
[26] Standaert, F.: Introduction to side-channel attacks. In: Verbauwhede, I.M.R. (ed.) Secure Integrated Circuits and Systems, pp. 27–42. Integrated Circuits and Systems, Springer (2010). https://doi.org/10.1007/978-0-387-71829-3_2
[27] Wang, L., Zhan, N.: Decidability of the initial-state opacity of real-time automata. In: Jones, C.B., Wang, J., Zhan, N. (eds.) Symposium on Real-Time and Hybrid Systems - Essays Dedicated to Professor Chaochen Zhou on the Occasion of His 80th Birthday, LNCS, vol. 11180, pp. 44–60. Springer (2018). https://doi.org/10.1007/978-3-030-01461-2_3
[28] Wang, L., Zhan, N., An, J.: The opacity of real-time automata. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems **37**(11), 2845–2856 (2018). https://doi.org/10.1109/TCAD.2018.2857363

A Notation table

Timed automaton	
$\mathcal{A}$	a timed automaton
Σ	a finite set of actions of a TA
L	a finite set of locations of a TA
ℓ_0	the initial location of a TA
ℓ_{priv}	the private location of a TA
F	the set of final locations of a TA
$\mathbb{X}$	a finite set of clocks
x_i	the i^{th} clock
H	the number of clocks
$I(\ell)$	the invariant of location ℓ
E	the finite set of edges of a TA
e	an edge
R	a set of clocks to be reset
g	a guard
μ	a clock valuation
d	a delay
z	extra clock
c_i	largest constant for clock x_i

Semantics	
$TTS_{\mathcal{A}}$	the semantics of TA $\mathcal{A}$
S	the set of states in $TTS_{\mathcal{A}}$
s_0	the initial state in $TTS_{\mathcal{A}}$
s	a state in $TTS_{\mathcal{A}}$
δ	transition function of $TTS_{\mathcal{A}}$
$\overset{\mathsf{e}}{\mapsto}$	a discrete transition with edge e
$\overset{d}{\mapsto}$	a delay transition with delay d
ρ	a run
$last(\rho)$	last state of run ρ

Regions	
r	a region
$[s]$	equivalence class of s
$\mathsf{R}_{\mathcal{A}}$	regions set of $\mathcal{A}$
$\mathsf{R}_{\mathcal{A}}^{F}$	set of final regions of $\mathcal{A}$
$\mathcal{R}_{\mathcal{A}}$	region automaton of $\mathcal{A}$
Σ^{R}	set of actions of $\mathcal{R}_{\mathcal{A}}$
δ^{R}	transition function of $\mathcal{R}_{\mathcal{A}}$
$\rightarrow_{\mathsf{R}}$	a transition in $\mathcal{R}_{\mathcal{A}}$

Opacity	
$Visit^{priv}(\mathcal{A})$	set of private runs of $\mathcal{A}$
$Visit^{\overline{priv}}(\mathcal{A})$	set of public runs of $\mathcal{A}$
$DVisit^{priv}(\mathcal{A})$	set of durations of private runs of $\mathcal{A}$
$DVisit^{\overline{priv}}(\mathcal{A})$	set of durations of public runs of $\mathcal{A}$

Strategy	
Σ_c	controllable actions
Σ_u	uncontrollable actions
σ	a strategy
α	a $\mathfrak{b}$-strategy
$\mathcal{A}^\sigma$	$\mathcal{A}$ controlled by strategy σ
δ^σ	transition function of $TTS_{\mathcal{A}^\sigma}$
$\mapsto_\sigma$	a discrete or delay transition in $TTS_{\mathcal{A}^\sigma}$
$\xrightarrow{d,e}_\sigma$	a transition with delay d and edge e in $TTS_{\mathcal{A}^\sigma}$
$\mathfrak{C}$	set of activated controllable actions

Duplicated TA	
$\mathcal{A}^{dup}$	a duplicated TA
L_{priv}	set of private states
L_{pub}	set of public states
ℓ_{priv}	a private state

Beliefs	
$\mathfrak{b}_t$	belief for time t
$\mathbb{B}_\mathcal{A}$	set of beliefs of $\mathcal{A}$
$\mathcal{B}_\mathcal{A}$	belief automaton of $\mathcal{A}$
$\mathfrak{S}^{\mathcal{B}_\mathcal{A}}$	states of $\mathcal{B}_\mathcal{A}$
$\mathfrak{A}^{\mathcal{B}_\mathcal{A}}$	actions of $\mathcal{B}_\mathcal{A}$
v	a sequence of actions of $\mathcal{B}_\mathcal{A}$
$\mathfrak{d}^{\mathcal{B}_\mathcal{A}}$	transition function of $\mathcal{B}_\mathcal{A}$
$\mathsf{Secret}_\mathcal{A}$	set of regions reachable on a run visiting ℓ_{priv}
$\overline{\mathsf{Secret}_\mathcal{A}}$	set of regions not reachable on a run visiting ℓ_{priv}
$\mathbb{B}^\sigma_\mathcal{A}$	set of beliefs reachable by a strategy σ
$\mathcal{B}^\alpha_\mathcal{A}$	controlled belief automaton of $\mathcal{A}$ and $\mathfrak{b}$-strategy α
$\mathfrak{S}^{\mathcal{B}^\alpha_\mathcal{A}}$	states of controlled belief automaton
$\mathfrak{A}^{\mathcal{B}^\alpha_\mathcal{A}}$	actions of controlled belief automaton
$\mathfrak{d}^{\mathcal{B}^\alpha_\mathcal{A}}$	transition function of controlled belief automaton

B Full definitions

We define formally bad belief for almost full ET-opacity and closed full ET-opacity.

Definition 17 (Bad belief for almost full ET-opacity). *A belief* $\mathfrak{b}_t$ *is* bad for almost full ET-opacity *when*

- *it is bad for full ET-opacity and*
- *there is* $d \in \mathbb{R}_{>0}$ *such that, either*
  - *for all* $\epsilon \in \mathbb{R}_{>0}$, $\epsilon \leq d$, $\mathfrak{b}_{t+\epsilon}$ *is bad for full ET-opacity; or*
  - *for all* $\epsilon \in \mathbb{R}_{<0}, \epsilon \geq -d$, $\mathfrak{b}_{t+\epsilon}$ *is bad for full ET-opacity.*

Definition 18 (Bad belief for closed full ET-opacity). *A belief* $\mathfrak{b}_t$ *is* bad for closed full ET-opacity *when*

- *it is bad for full ET-opacity and*
- *there is* $d \in \mathbb{R}_{>0}$ *such that either*
  - *for all* $\epsilon \in \mathbb{R}_{>0}$, $\epsilon \leq d$, $\mathfrak{b}_{t+\epsilon}$ *is bad for full ET-opacity, or*
  - *for all* $\epsilon \in \mathbb{R}_{<0}, \epsilon \geq -d$, $\mathfrak{b}_{t+\epsilon}$ *is bad for full ET-opacity, or*
  - *for all* $\epsilon \in \mathbb{R}_{\neq 0}$, $-d \leq \epsilon \leq d$, $\mathfrak{b}_{t+\epsilon} \cap \mathsf{R}^F_{\mathcal{A}} = \emptyset$.

Definition 19 (Good belief for $\exists$-interval ET-opacity). *A belief* $\mathfrak{b}_t$ *is* good for almost full ET-opacity *when*

- *it is good for* $\exists$*-ET-opacity and*
- *there is* $d \in \mathbb{R}_{>0}$ *such that, either*
  - *for all* $\epsilon \in \mathbb{R}_{>0}$, $\epsilon \leq d$, $\mathfrak{b}_{t+\epsilon}$ *is good for* $\exists$*-ET-opacity; or*
  - *for all* $\epsilon \in \mathbb{R}_{<0}$, $\epsilon \geq -d$, $\mathfrak{b}_{t+\epsilon}$ *is good for* $\exists$*-ET-opacity.*

Now, we formally define weak variants of almost and closed opacity. We give also the corresponding definition of bad beliefs for each notion.

Definition 20 (Almost weak ET-opacity). *A TA* $\mathcal{A}$ *is almost weakly ET-opaque when* $(\!|DVisit^{priv}(\mathcal{A})|\!) \setminus (\!|D\,\overline{Visit^{priv}}(\mathcal{A})|\!) = \emptyset$.

Definition 21 (Bad belief for almost weak ET-opacity). *A belief* $\mathfrak{b}_t$ *is* bad for almost weak ET-opacity *when*

- *it is bad for weak ET-opacity and*
- *there is* $d \in \mathbb{R}_{>0}$ *such that, either*
  - *for all* $\epsilon \in \mathbb{R}_{>0}$, $\epsilon \leq d$, $\mathfrak{b}_{t+\epsilon}$ *is bad for weak ET-opacity; or*
  - *for all* $\epsilon \in \mathbb{R}_{<0}, \epsilon \geq -d$, $\mathfrak{b}_{t+\epsilon}$ *is bad for weak ET-opacity.*

Definition 22 (Closed weak ET-opacity). *A TA* $\mathcal{A}$ *is closed weakly ET-opaque when* $[\![DVisit^{priv}(\mathcal{A})]\!] \subseteq [\![D\,\overline{Visit^{priv}}(\mathcal{A})]\!]$.

Definition 23 (Bad belief for closed weak ET-opacity). *A belief* $\mathfrak{b}_t$ *is* bad for closed weak ET-opacity *when*

- *it is bad for weak ET-opacity and*
- *there is* $d \in \mathbb{R}_{>0}$ *such that either*
  - *for all* $\epsilon \in \mathbb{R}_{>0}$, $\epsilon \leq d$, $\mathfrak{b}_{t+\epsilon}$ *is bad for weak ET-opacity; or*
  - *for all* $\epsilon \in \mathbb{R}_{<0}, \epsilon \geq -d$, $\mathfrak{b}_{t+\epsilon}$ *is bad for weak ET-opacity; or*
  - *for all* $\epsilon \in \mathbb{R}_{\neq 0}$, $-d \leq \epsilon \leq d$, $\mathfrak{b}_{t+\epsilon} \cap \mathsf{R}^F_{\mathcal{A}} = \emptyset$.

C Detailed proofs for Section 6

C.1 Beliefs characterizations

Lemma 7 (Beliefs characterization for closed full ET-opacity). *A TA $\mathcal{A}$ is closed fully ET-opaque with a strategy σ iff, for all $\mathfrak{b} \in \mathbb{B}^{\sigma}_{\mathcal{A}}$, $\mathfrak{b}$ is not bad for closed full ET-opacity.*

Proof.

$\Rightarrow$ Let $\mathcal{A}$ be a TA closed fully ET-opaque with strategy σ. Let $\mathfrak{b}_t \in \mathbb{B}^{\sigma}_{\mathcal{A}}$.

- Either $t \in DVisit^{priv}_{\sigma}(\mathcal{A}) \cap \overline{DVisit^{priv}_{\sigma}}(\mathcal{A})$ then $\mathfrak{b}_t$ is not bad for full ET-opacity, and thus cannot be bad for closed full ET-opacity,
- or, similarly, $t \notin DVisit^{priv}_{\sigma}(\mathcal{A}) \cup \overline{DVisit^{priv}_{\sigma}}(\mathcal{A})$ and is not bad for closed full ET-opacity,
- or finally, suppose w.l.o.g. that $t \in DVisit^{priv}_{\sigma}(\mathcal{A}) \setminus \overline{DVisit^{priv}_{\sigma}}(\mathcal{A})$. As $\mathcal{A}$ is closed fully ET-opaque with σ, $[\![DVisit^{priv}_{\sigma}(\mathcal{A})]\!] = [\![\overline{DVisit^{priv}_{\sigma}}(\mathcal{A})]\!]$, and so this means that there exists $d \in \mathbb{R}_{>0}$ such that either
  1. for all $\epsilon \in \mathbb{R}_{>0}, \epsilon \leq d$, $t + \epsilon \in DVisit^{priv}_{\sigma}(\mathcal{A}) \cap \overline{DVisit^{priv}_{\sigma}}(\mathcal{A})$, or
  2. for all $\epsilon \in \mathbb{R}_{<0}, \epsilon \geq -d$, $t + \epsilon \in DVisit^{priv}_{\sigma}(\mathcal{A}) \cap \overline{DVisit^{priv}_{\sigma}}(\mathcal{A})$, or
  3. for all $\epsilon \in \mathbb{R}_{\neq 0}$, $-d \leq \epsilon \leq d$, $\mathfrak{b}_{t+\epsilon} \cap \mathsf{R}^{F}_{\mathcal{A}} = \emptyset$.

  In other words, for Items 1 and 2, for all ϵ there are σ-compatible runs $\rho_\epsilon, \rho'_\epsilon$ such that $dur(\rho_\epsilon) = dur(\rho'_\epsilon) = t + \epsilon$ and $\rho_\epsilon \in DVisit^{priv}_{\sigma}(\mathcal{A}), \rho'_\epsilon \in \overline{DVisit^{priv}_{\sigma}}(\mathcal{A})$. Then, $\{[last(\rho_\epsilon)], [last(\rho'_\epsilon)]\} \subseteq \mathfrak{b}_{t+\epsilon}$ and so $\mathfrak{b}_{t+\epsilon}$ is not bad for full ET-opacity. For Item 3, for all ϵ, there are no run ρ_ϵ such that $dur(\rho_\epsilon) = t$. So $\mathfrak{b}_{t+\epsilon} \cap \mathsf{R}^{F}_{\mathcal{A}} \neq \emptyset$. As a consequence, $\mathfrak{b}_t$ is not a bad belief for closed full ET-opacity.

Therefore, no bad belief for closed full ET-opacity belongs to $\mathbb{B}^{\sigma}_{\mathcal{A}}$.

$\Leftarrow$ Let $\mathcal{A}$ be a TA such that there is no bad belief for closed full ET-opacity in $\mathbb{B}^{\sigma}_{\mathcal{A}}$. For every time $t \in \mathbb{R}_{\geq 0}$, let $\mathfrak{b}_t$ be the associated belief. $\mathfrak{b}_t$ is not bad for closed full ET-opacity, thus one of the following holds:

- $\mathfrak{b}_t$ is not bad for full ET-opacity so no violation of opacity occurs at time t,
- $\mathfrak{b}_t$ is bad for full ET-opacity and there exists $d \in \mathbb{R}_{>0}$ such that either
  1. for all $\epsilon \in \mathbb{R}_{>0}$, $-d \leq \epsilon \leq d$, $\mathfrak{b}_{t+\epsilon}$ is not bad for full ET-opacity, and
  2. for all $\epsilon \in \mathbb{R}_{\neq 0}$, $-d \leq \epsilon \leq d$, $\mathfrak{b}_{t+\epsilon} \cap \mathsf{R}^{F}_{\mathcal{A}} \neq \emptyset$.

  Thus, for all ϵ, there are σ-compatible runs $\rho_\epsilon, \rho'_\epsilon$ such that $\rho_\epsilon \in Visit^{priv}_{\sigma}(\mathcal{A}), \rho'_\epsilon \in \overline{Visit^{priv}_{\sigma}}(\mathcal{A})$ with $t + \epsilon = dur(\rho_\epsilon) = dur(\rho'_\epsilon)$. This means that $t + \epsilon \in DVisit^{priv}_{\sigma}(\mathcal{A}) \cap \overline{DVisit^{priv}_{\sigma}}(\mathcal{A})$ and $[\![DVisit^{priv}_{\sigma}(\mathcal{A})]\!] = [\![\overline{DVisit^{priv}_{\sigma}}(\mathcal{A})]\!]$.

Therefore, $\mathcal{A}$ is closed fully ET-opaque with strategy σ. □

Lemma 8 (Beliefs characterization for closed weak ET-opacity). *A TA $\mathcal{A}$ is closed weakly ET-opaque with a strategy σ iff, for all $\mathfrak{b} \in \mathbb{B}^{\sigma}_{\mathcal{A}}$, $\mathfrak{b}$ is not bad for closed weak ET-opacity.*

Proof. This proof can be achieved similarly to the proof of Lemma 7. □

Lemma 9 (Beliefs characterization for almost full ET-opacity). *A TA $\mathcal{A}$ is almost fully ET-opaque with a strategy σ iff, for all $\mathfrak{b} \in \mathbb{B}^{\sigma}_{\mathcal{A}}$, $\mathfrak{b}$ is not bad for almost full ET-opacity.*

Proof.

$\Rightarrow$ Let $\mathcal{A}$ be a TA almost fully ET-opaque with strategy σ. Let $\mathfrak{b}_t \in \mathbb{B}^{\sigma}_{\mathcal{A}}$.

- Either $t \in DVisit^{priv}_{\sigma}(\mathcal{A}) \cap \overline{DVisit^{priv}_{\sigma}}(\mathcal{A})$, then $\mathfrak{b}_t$ is not bad for full ET-opacity, and thus cannot be bad for almost full ET-opacity,
- or, similarly, $t \notin DVisit^{priv}_{\sigma}(\mathcal{A}) \cup \overline{DVisit^{priv}_{\sigma}}(\mathcal{A})$ and is not bad for almost full ET-opacity,
- or finally, suppose w.l.o.g. that $t \in DVisit^{priv}_{\sigma}(\mathcal{A}) \setminus \overline{DVisit^{priv}_{\sigma}}(\mathcal{A})$. As $\mathcal{A}$ is almost fully ET-opaque with σ, $(\!|DVisit^{priv}_{\sigma}(\mathcal{A}) \oplus \overline{DVisit^{priv}_{\sigma}}(\mathcal{A})|\!) = \emptyset$, and so this means that there exists $d \in \mathbb{R}_{>0}$ such that either
  - for all $\epsilon \in \mathbb{R}_{>0}, \epsilon \leq d$, $t + \epsilon \in DVisit^{priv}_{\sigma}(\mathcal{A}) \cap \overline{DVisit^{priv}_{\sigma}}(\mathcal{A})$, or
  - for all $\epsilon \in \mathbb{R}_{<0}, \epsilon \geq -d$, $t + \epsilon \in DVisit^{priv}_{\sigma}(\mathcal{A}) \cap \overline{DVisit^{priv}_{\sigma}}(\mathcal{A})$.

  In other words, for all ϵ there are σ-compatible runs $\rho_\epsilon, \rho'_\epsilon$ such that $dur(\rho_\epsilon) = dur(\rho'_\epsilon) = t + \epsilon$ and $\rho_\epsilon \in DVisit^{priv}_{\sigma}(\mathcal{A}), \rho'_\epsilon \in \overline{DVisit^{priv}_{\sigma}}(\mathcal{A})$. Then, $\{[last(\rho_\epsilon)], [last(\rho'_\epsilon)]\} \subseteq \mathfrak{b}_{t+\epsilon}$. In both case, $\mathfrak{b}_{t+\epsilon}$ is not bad for full ET-opacity. As a consequence, $\mathfrak{b}_t$ is not a bad belief for almost full ET-opacity.

Therefore, no bad belief for almost full ET-opacity belongs to $\mathbb{B}^{\sigma}_{\mathcal{A}}$.

$\Leftarrow$ Let $\mathcal{A}$ be a TA such that there is no bad belief for almost full ET-opacity in $\mathbb{B}^{\sigma}_{\mathcal{A}}$. For every time $t \in \mathbb{R}_{\geq 0}$, let $\mathfrak{b}_t$ be the associated belief. $\mathfrak{b}_t$ is not bad for almost full ET-opacity, thus one of the following holds:

- $\mathfrak{b}_t$ is not bad for full ET-opacity so no violation of opacity occurs at time t,
- $\mathfrak{b}_t$ is bad for full ET-opacity and there exists $d \in \mathbb{R}_{>0}$ such that for all $\epsilon \in \mathbb{R}_{>0}$, $-d \leq \epsilon \leq d$, $\mathfrak{b}_{t+\epsilon}$ is not bad for full ET-opacity. Thus, for all ϵ, either
  - there are σ-compatible runs $\rho_\epsilon, \rho'_\epsilon$ such that $\rho_\epsilon \in Visit^{priv}_{\sigma}(\mathcal{A}), \rho'_\epsilon \in \overline{Visit^{priv}_{\sigma}}(\mathcal{A})$ with $t + \epsilon = dur(\rho_\epsilon) = dur(\rho'_\epsilon)$. This means that $t + \epsilon \in DVisit^{priv}_{\sigma}(\mathcal{A}) \cap \overline{DVisit^{priv}_{\sigma}}(\mathcal{A})$, or
  - there are no run ρ_ϵ such that $dur(\rho_\epsilon) = t + \epsilon$. This means that $t + \epsilon \notin DVisit^{priv}_{\sigma}(\mathcal{A}) \cup \overline{DVisit^{priv}_{\sigma}}(\mathcal{A})$.

  Finally, $(\!|DVisit^{priv}_{\sigma}(\mathcal{A}) \oplus \overline{DVisit^{priv}_{\sigma}}(\mathcal{A})|\!)$.

Therefore, $\mathcal{A}$ is almost fully ET-opaque with strategy σ. □

Lemma 10 (Beliefs characterization for almost weak ET-opacity). *A TA $\mathcal{A}$ is almost weakly ET-opaque with a strategy σ iff, for all $\mathfrak{b} \in \mathbb{B}^{\sigma}_{\mathcal{A}}$, $\mathfrak{b}$ is not bad for almost weak ET-opacity.*

Proof. This proof can be achieved similarly to the proof of Lemma 9. □

Lemma 11 (Beliefs characterization for ∃-interval ET-opacity). *A TA $\mathcal{A}$ is ∃-interval ET-opacity with a strategy σ iff there exists $\mathfrak{b} \in \mathbb{B}^{\sigma}_{\mathcal{A}}$ such that $\mathfrak{b}$ is good for ∃-interval ET-opacity.*

Proof.

⇒ Let $\mathcal{A}$ be a TA ∃-interval ET-opaque with strategy σ. There is a time t such that $t \in DVisit^{priv}_{\sigma}(\mathcal{A}) \cap D\,\overline{Visit^{priv}_{\sigma}}(\mathcal{A})$ and a delay $d \in \mathbb{R}_{>0}$ such that either
- for all $\epsilon \in \mathbb{R}_{>0}$, $\epsilon \leq d$, $t + \epsilon \in DVisit^{priv}_{\sigma}(\mathcal{A}) \cap D\,\overline{Visit^{priv}_{\sigma}}(\mathcal{A})$, or
- for all $\epsilon \in \mathbb{R}_{<0}, \epsilon \geq -d$, $t + \epsilon \in DVisit^{priv}_{\sigma}(\mathcal{A}) \cap D\,\overline{Visit^{priv}_{\sigma}}(\mathcal{A})$.

Then, there is $\rho \in Visit^{priv}_{\sigma}(\mathcal{A})$ and $\rho' \in \overline{Visit^{priv}_{\sigma}}(\mathcal{A})$, both σ-compatible, with $dur(\rho) = dur(\rho') = t$ and, for all ϵ, there is $\rho_\epsilon \in Visit^{priv}_{\sigma}(\mathcal{A})$ and $\rho'_\epsilon \in \overline{Visit^{priv}_{\sigma}}(\mathcal{A})$, σ-compatible, with $dur(\rho_\epsilon) = dur(\rho'_\epsilon) = t + \epsilon$. Thus, we have that $\{[last(\rho)], [last(\rho')]\} \subseteq \mathfrak{b}_t$ and, for all ϵ, $\{[last(\rho_\epsilon)], [last(\rho'_\epsilon)]\} \subseteq \mathfrak{b}_{t+\epsilon}$. Then, $\mathfrak{b}_t$ is good for ∃-interval ET-opacity.

⇐ Let $\mathcal{A}$ be a TA with a good belief for ∃-interval ET-opacity $\mathfrak{b}_t \in \mathbb{B}^{\sigma}_{\mathcal{A}}$. Then, there exists $d \in \mathbb{R}_{>0}$ such that, either
- for all $\epsilon \in \mathbb{R}_{>0}$, $\epsilon \leq d$, $\mathfrak{b}_{t+\epsilon}$ is good for ∃-ET-opacity, or
- for all $\epsilon \in \mathbb{R}_{<0}, \epsilon \geq -d$, $\mathfrak{b}_{t+\epsilon}$ is good for ∃-ET-opacity.

There is so $\rho \in Visit^{priv}_{\sigma}(\mathcal{A})$, $\rho' \in \overline{Visit^{priv}_{\sigma}}(\mathcal{A})$ such that $dur(\rho) = dur(\rho') = t$, but also, for all ϵ, $\rho_\epsilon \in Visit^{priv}_{\sigma}(\mathcal{A})$, $\rho'_\epsilon \in \overline{Visit^{priv}_{\sigma}}(\mathcal{A})$ with $dur(\rho_\epsilon) = dur(\rho_{\epsilon'}) = t + \epsilon$. Therefore, $\mathcal{A}$ is ∃-interval ET-opaque with strategy σ. □

C.2 Proof of Theorem 4 and additional results

Proof of Theorem 4. First, as for full ET-opacity with Theorem 1, we can prove that, for a given TA $\mathcal{A}$ and a strategy σ, $\mathcal{A}^{\sigma}$ is closed fully ET-opaque (resp. closed weakly ET-opaque) iff there exists α, $\sigma \vdash\!\dashv \alpha$ such that there is no bad belief for closed full ET-opacity (resp. for closed weak ET-opacity) reachable in $\mathcal{B}^{\alpha}_{\mathcal{A}}$. The proof is similar to the one of Theorem 1.

Then, as within the proof of Theorem 3, based on Lemma 6 and the relation between our problems and their correspondence with a safety game, we can conclude that closed full ET-opacity finitely-varying controller emptiness problem is decidable and the closed full ET-opacity finitely-varying controller synthesis problem is solvable. □

Theorem 5. *The almost full (resp. weak) ET-opacity finitely-varying controller emptiness problem is decidable; the almost full (resp. weak) ET-opacity finitely-varying controller synthesis problem is solvable.*

Proof. This proof can be achieved similarly to the proof of Theorem 4. □

Theorem 6. *The ∃-interval ET-opacity finitely-varying controller emptiness problem is decidable; the ∃-interval ET-opacity finitely-varying controller synthesis problem is solvable.*

Proof. This proof can be achieved similarly to the proof of Theorem 4. □

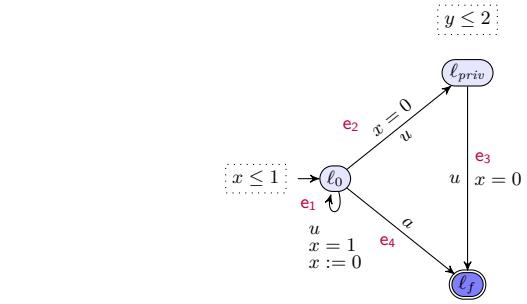
D Additional examples

If there is more than one clock, we extend our abuse of notation for regions to $(\ell, \tau_1, \dots, \tau_H)$, where each τ_i is either an interval or an integer. Note that this notation does not take into account the comparaison between clocks but this is acceptable in the following example as the clocks always have the same fractionnal part.

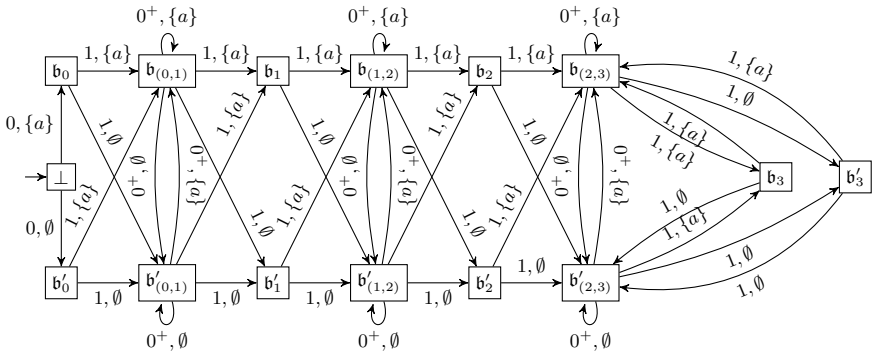
Example 9. Let $\mathcal{A}_3$ the TA depicted in Fig. 4a. With the invariant $x \leq 1$ for ℓ_0 and $y \leq 2$ for ℓ_{priv}, we have the following beliefs. Each region is written $(\ell, \tau_1, \tau_2, \tau_3)$ with τ_1 for x, τ_2 for y and τ_3 for z. The corresponding belief automaton is depicted in Fig. 4b.

$$
\begin{aligned}
\mathfrak{b}_0 &= \big\{(\ell_0,0,0,0),(\ell_{priv},0,0,0),(\ell_f,0,0,0)\big\}\\
\mathfrak{b}'_0 &= \big\{(\ell_0,0,0,0),(\ell_{priv},0,0,0)\big\}\\
\mathfrak{b}_{(0,1)} &= \big\{(\ell_0,(0,1),(0,1),(0,1)),(\ell_{priv},(0,1),(0,1),(0,1)),(\ell_f,(0,1),(0,1),(0,1))\big\}\\
\mathfrak{b}'_{(0,1)} &= \big\{(\ell_0,(0,1),(0,1),(0,1)),(\ell_{priv},(0,1),(0,1),(0,1))\big\}\\
\mathfrak{b}_1 &= \big\{(\ell_0,1,1,1),(\ell_0,1,1,0),(\ell_0,0,1,1),(\ell_0,0,1,0),(\ell_{priv},1,1,1),(\ell_{priv},1,1,0),\\
&\quad (\ell_{priv},0,1,1),(\ell_{priv},0,1,0),(\ell_f,1,1,1),(\ell_f,1,1,0),(\ell_f,0,1,1),(\ell_f,0,1,0)\big\}\\
\mathfrak{b}'_1 &= \big\{(\ell_0,1,1,1),(\ell_0,1,1,0),(\ell_0,0,1,1),(\ell_0,0,1,0),(\ell_{priv},0,1,1),(\ell_{priv},0,1,0),\\
&\quad (\ell_{priv},1,1,1),(\ell_{priv},1,1,0)\big\}\\
\mathfrak{b}_{(1,2)} &= \big\{(\ell_0,(0,1),(1,2),(0,1)),(\ell_f,(0,1),(1,2),(0,1)),(\ell_{priv},(0,1),(1,2),(0,1)),\\
&\quad (\ell_{priv},(1,+\infty),(1,2),(0,1))\big\}\\
\mathfrak{b}'_{(1,2)} &= \big\{(\ell_0,(0,1),(1,2),(0,1)),(\ell_{priv},(0,1),(1,2),(0,1)),(\ell_{priv},(1,+\infty),(1,2),(0,1))\big\}\\
\mathfrak{b}_2 &= \big\{(\ell_0,0,2,1),(\ell_0,0,2,0),(\ell_0,1,2,1),(\ell_0,1,2,0),(\ell_{priv},0,2,1),(\ell_{priv},0,2,0),\\
&\quad (\ell_{priv},1,2,1),(\ell_{priv},1,2,0),(\ell_{priv},(1,+\infty),2,1),(\ell_{priv},(1,+\infty),2,0),\\
&\quad (\ell_f,1,2,1),(\ell_f,1,2,0),(\ell_f^p,0,2,1),(\ell_f^p,0,20)\big\}\\
\mathfrak{b}'_2 &= \big\{(\ell_0,1,2,1),(\ell_0,1,2,0),(\ell_0,0,2,1),(\ell_0,0,2,0),(\ell_{priv},0,2,1),(\ell_{priv},0,2,0),\\
&\quad (\ell_{priv},(1,+\infty),2,1),(\ell_{priv},(1,+\infty),2,0),(\ell_{priv},1,2,1),(\ell_{priv},1,2,0),\\
&\quad (\ell_f^p,0,2,1),(\ell_f^p,0,2,0)\big\}\\
\mathfrak{b}_{(2,3)} &= \big\{(\ell_0,(0,1),(2,+\infty),(0,1)),(\ell_f,(0,1),(2,+\infty),(0,1))\big\}\\
\mathfrak{b}'_{(2,3)} &= \big\{(\ell_0,(0,1),(2,+\infty),(0,1))\big\}\\
\mathfrak{b}_3 &= \big\{(\ell_0,1,(2,+\infty),1),(\ell_0,1,(2,+\infty),0),(\ell_0,0,(2,+\infty),1),(\ell_0,0,(2,+\infty),0),\\
&\quad (\ell_f,0,(2,+\infty),1),(\ell_f,0,(2,+\infty),0),(\ell_f,1,(2,+\infty),1)(\ell_f,1,(2,+\infty),0)\big\}\\
\mathfrak{b}'_3 &= \big\{(\ell_0,1,(2,+\infty),1),(\ell_0,1,(2,+\infty),0),(\ell_0,0,(2,+\infty),1),(\ell_0,0,(2,+\infty),0)\big\}
\end{aligned}
$$

The following example show a TA opaque with a non-finitely-varying strategy and why we cannot manage it with our beliefs construction.



(a) TA $\mathcal{A}_3$



(b) Belief automaton $\mathcal{B}_{\mathcal{A}_3}$

Fig. 4: $\mathcal{A}_3$ and the corresponding belief automaton

Example 10 (A non-finitely-varying strategy). Let $\mathcal{A}_4$ be the automaton in Fig. 5, with a global invariant $x, y \leq 1$. Let $\Sigma_u = \{u\}$ and $\Sigma_c = \{a, b\}$, we can build a strategy σ (depicted in red boxes) to make it opaque where

- $\forall \tau \in \mathbb{Q}$, $\sigma(\tau) = \{a\}$
- $\forall \tau \notin \mathbb{Q}$, $\sigma(\tau) = \{b\}$.

Let us see if we can find an corresponding $\mathfrak{b}$-strategy α for the belief automaton. In the belief automaton, whatever the subset of controllable actions chosen in $\bot$, $\mathfrak{b}_0$ contains the region with location ℓ_0 and $x = 0$. Different beliefs are then reachable from $\mathfrak{b}_0$ according to the chosen (finitely-varying) strategy:

- $\forall \tau \in (0, 1)$, if $\alpha(\tau) = \{a, b\}$, then we can reach the final location by the edge e_3 (private way) and by e_4 (public way). However, we can also reach location ℓ_3, which will allow us to reach the final location by e_7 when $x = 1$. As we cannot reach ℓ_f by a private way when $x = 1$, we do not want a and b are available at the same time when $x \leq 1$ to prevent to take edge e_7. So this strategy is not good.
- $\forall \tau \in (0, 1)$, if $\alpha(\tau) = \{a\}$, $\alpha(\tau) = \{b\}$, or $\alpha(\tau) = \emptyset$ then we can reach the final location by e_4, but not by e_3. None of these strategies makes $\mathcal{A}_3$ opaque.

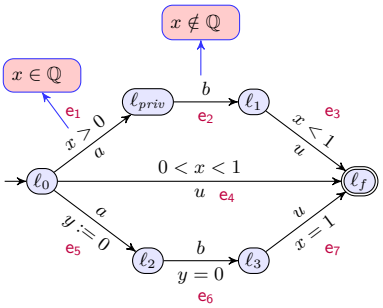


Fig. 5: Automaton $\mathcal{A}_4$

As σ is not finitely-varying and there is no other finitely-varying strategy such that $\mathcal{A}_3$ is opaque, we cannot find a $\mathfrak{b}$-strategy in the belief automaton.