



**HAL**  
open science

# Evolving privacy: drift parameter estimation for discretely observed i.i.d. diffusion processes under LDP

Chiara Amorino, Arnaud Gloter, H el ene Halconruy

## ► To cite this version:

Chiara Amorino, Arnaud Gloter, H el ene Halconruy. Evolving privacy: drift parameter estimation for discretely observed i.i.d. diffusion processes under LDP. 2024. hal-04428663

**HAL Id: hal-04428663**

**<https://hal.science/hal-04428663>**

Preprint submitted on 31 Jan 2024

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destin ee au d ep ot et  a la diffusion de documents scientifiques de niveau recherche, publi es ou non,  emanant des  tablissements d'enseignement et de recherche fran ais ou  trangers, des laboratoires publics ou priv es.

# Evolving privacy: drift parameter estimation for discretely observed i.i.d. diffusion processes under LDP

Chiara Amorino\*    Arnaud Gloter †    H el ene Halconruy ‡

January 31, 2024

## Abstract

The problem of estimating a parameter in the drift coefficient is addressed for  $N$  discretely observed independent and identically distributed stochastic differential equations (SDEs). This is done considering additional constraints, wherein only public data can be published and used for inference. The concept of local differential privacy (LDP) is formally introduced for a system of stochastic differential equations. The objective is to estimate the drift parameter by proposing a contrast function based on a pseudo-likelihood approach. A suitably scaled Laplace noise is incorporated to meet the privacy requirements. Our key findings encompass the derivation of explicit conditions tied to the privacy level. Under these conditions, we establish the consistency and asymptotic normality of the associated estimator. Notably, the convergence rate is intricately linked to the privacy level, and in some situations may be completely different from the case where privacy constraints are ignored. Our results hold true as the discretization step approaches zero and the number of processes  $N$  tends to infinity.

*Keywords:* local differential privacy, parameter drift estimation, high frequency data, convergence rate, privacy for processes

*AMS 2010 subject classifications:* 62F12, 62E20, 62M05, 60G07, 60H10

## Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Mathematical framework</b>	<b>5</b>
2.1	Setting and assumptions . . . . .	5
2.2	Problem formulation . . . . .	6
<b>3</b>	<b>Statistical procedure and main results</b>	<b>8</b>
3.1	Privatization mechanism and estimation procedure . . . . .	8
3.2	Main results: consistency and asymptotic normality . . . . .	11
3.3	Effective privacy . . . . .	13
<b>4</b>	<b>Concluding remarks</b>	<b>14</b>

---

\*Universit e du Luxembourg, L-4364 Esch-Sur-Alzette, Luxembourg. The author gratefully acknowledges financial support of ERC Consolidator Grant 815703 ‘‘STAMFORD: Statistical Methods for High Dimensional Diffusions’’.

†Laboratoire de Math ematiques et Mod elisation d’Evry, CNRS, Univ Evry, Universit e Paris-Saclay, 91037, Evry, France.

‡T el ecom SudParis, Institut polytechnique de Paris, 91120, Palaiseau, France.

<b>5</b>	<b>Preliminary results</b>	<b>16</b>
5.1	Splines, some tools . . . . .	16
5.2	Technical results . . . . .	20
<b>6</b>	<b>Proof of main results</b>	<b>21</b>
6.1	Consistency . . . . .	21
6.2	Asymptotic normality . . . . .	29
6.2.1	Proof of Proposition 4 . . . . .	30
6.2.2	Proof of Proposition 5 . . . . .	31
6.2.3	Proof of Corollary 1 . . . . .	36
6.2.4	Proof of Proposition 6 . . . . .	37
<b>7</b>	<b>Proof of preliminary results</b>	<b>37</b>
7.1	Proof of Lemma 2 . . . . .	37
7.2	Proof of Proposition 2 . . . . .	37
7.3	Proof of Lemma 5 . . . . .	38
7.4	Proof of Lemma 7 . . . . .	39
7.5	Proof of Lemma 8 . . . . .	40
7.6	Proof of Lemma 9 . . . . .	41

## 1 Introduction

In recent years, the rapid accumulation of large-scale data, including medical records, cellphone location information, and internet browsing history, underscores the critical need for a nuanced understanding of the tradeoffs between privacy and the utility derived from collected data. Traditional privacy-preserving mechanisms like permutation or basic anonymization have proven inadequate, leading to notable privacy breaches with genomic and movie rating data (see [37]). These incidents, such as Netflix canceling a competition, highlight the urgency of finding a balance between utility and safeguarding sensitive information.

To address these challenges, researchers in statistics, databases, and computer science started studying differential privacy as a formalization of disclosure risk limitation (for example in [20, 22, 21]). Differential privacy has evolved from a theoretical paradigm to a widely deployed technology in various applications over the last decade [18, 23, 25]. It addresses the need for protecting individual data while allowing statistical analysis of aggregate databases. This is achieved through a trusted curator holding individual data, and the protection is ensured by injecting noise into released information. The challenge is to optimize statistical performance while preserving privacy in a remote access query system.

The first attempt to design a private methodology traces back to Dwork et al.’s work [21], that formalized global differential privacy. Research in this field now encompasses central or global privacy models, where a curator collects and privatizes data before releasing only the output, and local privacy models, involving randomized data collection. Major technology companies like Apple [5, 48] and Google [1, 23] have adopted local differential privacy protections, reflecting the broader impact of privacy measures in billions of devices. Understanding the fundamental limitations and possibilities of learning with local privacy notions is crucial in this context.

Historically, methods for locally private analysis were primarily focused on estimating parameters within a binomial distribution [50]. However, recent advancements in research have introduced mechanisms that extend to a broader array of statistical challenges. These encompass hypothesis testing [8, 33], M-estimators [6], robustness [35], change point analysis [9], mean and median estimation [20], and nonparametric estimation [12, 11, 31], among others. With the escalating importance of data protection, striking the right balance between statistical utility and privacy becomes crucial. It is imperative to safeguard data against privacy breaches while

still facilitating the extraction of valuable insights. Consequently, determining the optimal equilibrium between these two considerations has acquired heightened significance.

To the best of our understanding, the exploration of statistical inference under privacy constraints has traditionally centered on  $N$  random variables. The consideration of variables having a historical context, involving  $N$  stochastic processes across a time horizon  $[0, T]$ , has been noticeably absent from prior investigations. This paper aims to address this gap by examining the drift parameter estimation from i.i.d. paths of diffusion processes while adhering to local differential privacy constraints.

Note that the literature on statistical estimation for stochastic differential equations is extensive, owing to the model’s versatility and its applicability across various domains. Examples abound, spanning biology [44], neurology [28], finance [29], and economics [7]. Classical applications extend to physics [38] and mechanics [32]. The framework mentioned can also be employed to model the inherent variability of biomedical experiments, with a specific emphasis on pharmacology (refer to [49, 13, 41, 42] and [19] for an overview of stochastic differential equation estimation for pharmacodynamic models). This is why focusing on diffusion processes becomes interesting when dealing with sensitive data that requires privacy guarantees. However, a significant challenge arises when applying privacy in this context due to the dependency structure of the process. Indeed, it becomes possible to recover information about the private process at a particular time instant through observations about its past or future.

In this work we consider  $N$  i.i.d. diffusion processes  $(X_t^i)_{t \in [0, T]}$  for  $i \in \{1, \dots, N\}$ , with a fixed time horizon  $T > 0$ . They follow the dynamics

$$X_t^{\theta, i} = X_0^{\theta, i} + \int_0^t b(\theta, X_s^{\theta, i}) ds + \int_0^t \sigma(X_s^{\theta, i}) dW_s^i,$$

where the processes  $(W_t^i)_{t \in [0, T]}$  are independent standard Brownian motions. We aim to estimate the parameter  $\theta^* \in \Theta$  based on the discrete observations  $(X_{t_j}^{\theta, i})_{i=1, \dots, N, j=1, \dots, n}$  under  $\alpha$  local differential privacy constraints, for  $N, n \rightarrow \infty$ . In our context, the discrete observations of the private processes  $(X_t^1)_t, \dots, (X_t^N)_t$  are not directly available. Instead, our estimator relies on a public sample derived from the original discrete observations, subject to  $\alpha$  local differential privacy. To achieve this, we begin by adapting the concept of local differential privacy to a context that accommodates the presence of processes, leveraging the definition of *componentwise local differential privacy* (CLDP) proposed in [2] (refer to Section 2.2 for comprehensive details). In our interpretation, the  $N$  processes represent  $N$  independent individuals evolving over time. Each individual contributes  $n$  observations, subject to componentwise local differential privacy, ensuring that the information at different time points is privatized in a different way. This approach enables us to make public each observation corresponding to the same individual separately, using a distinct privacy channel with a privacy level  $\alpha_j$ , for  $j \in \{1, \dots, n\}$ . This strategy is advantageous as it allows for tailoring the level of privacy protection based on the specific context, recognizing that different observations corresponding to various moments in an individual’s life may warrant varying degrees of privacy safeguards.

The rationale behind this choice lies in the recognition that disclosing information about the distant past may have different implications than disclosing information about the present. By treating each observation independently, we can tailor the level of privacy protection based on the specific circumstances.

In our study, we examine a privacy mechanism where the data holder can observe two consecutive realizations of  $X^i$  each time. This scenario models situations such as when a patient’s vitals are taken, and the doctor (data holder) has access not only to the current data but also to the data from the previous check-up (control data).

Given the correlated nature of the observations, it becomes crucial to operate within a framework that acknowledges this dependency. A pertinent question arises: Is it possible to extract sensitive information about the present by exploiting the fact that some extra information is carried by

another observation from the past?

To answer this question, it is important to understand the constraints on the privacy levels  $\alpha_1, \dots, \alpha_n$  necessary to obtain well-performing estimators. Specifically, we will explore how the behavior of  $\alpha_1, \dots, \alpha_n$  as functions of  $N$  and  $n$  leads to two distinct asymptotic regimes, which we will refer to as the "significant contribution of privacy" and "negligible contribution of privacy".

Without the presence of privacy constraints, a natural approach to estimating unknown parameters from the continuous observation of a SDE would be to use maximum likelihood estimation. However, the likelihood function based on the discrete sample is not tractable, as it depends on the transition densities of the process, which are not explicitly known. To overcome this difficulty, several methods have been developed for high-frequency estimation of discretely observed classical SDEs. A widely-used method involves considering a pseudo-likelihood function, often based on the high-frequency approximation of the process dynamics using the Euler scheme, as seen in [24, 30, 52].

This statistical analysis relies on the minimization of a contrast function, akin to methods proposed for classical SDEs, extended to Lévy-driven SDEs [47, 3] and interacting particle systems [46, 4].

Even in our context, with the presence of local differential privacy constraints, it seems natural to leverage the minimization of a contrast function technique, incorporating this quantity into the definition of the privacy mechanism employed in our estimation procedure. Furthermore, introducing centered Laplace-distributed noise to bounded random variables is known to ensure  $\alpha$ -differential privacy (see [2], [20], [31]). This motivates our choice of the anonymization procedure. Specifically, we adopt a Laplace mechanism to construct the public counterpart of the raw samples, as illustrated in (3) below. Some technical challenges arise from such a definition, mainly due to the fact that Laplace random variables are defined only for some values of  $\theta$  on a grid, whose size  $L_n$  goes to  $\infty$  for  $n \rightarrow \infty$ . Consequently, our definition of the public sample  $(Z_j^i(\theta))_{i=1, \dots, N, j=1, \dots, n}$  holds true only on the grid as well. However, to define our estimator, we need to extend the definition of the public sample to  $\theta$  belonging to the whole parameter space  $\Theta$ . To address this, we rely on a spline approximation method, detailed in Section 5.1. Then, with access to the public data  $Z_j^i(\theta)$  for  $i = 1, \dots, N$  and  $j = 1, \dots, n$ , the statistician can propose an estimator obtained by minimizing the contrast function, which is the spline approximation of the private version of the contrast function in the case of classical SDEs (see Section 3 for details).

The main result of the paper is the consistency and asymptotic normality of the resulting estimator, demonstrated using a central limit theorem for martingale difference triangular arrays. Let us introduce

$$r_{n,N} := \frac{L_n^2 \log(n)}{\sqrt{\bar{\alpha}^2}}, \quad (1)$$

where  $\bar{\alpha}^2$  is the harmonic mean over different privacy levels, defined as  $1/\bar{\alpha}^2 := n^{-1} \sum_{j=1}^n 1/\alpha_j^2$  and that may be dependent on  $N$ . We establish the consistency of the proposed estimator under the assumption that

$$\frac{1}{L_n} \sqrt{\frac{\log(L_n)}{N}} r_{n,N} \rightarrow 0 \quad \text{as } n, N, L_n \rightarrow \infty.$$

This requirement implies that the case of perfect privacy ( $\bar{\alpha} = 0$ ) is not allowed and informs us about the price to pay for the privacy guarantee in obtaining reasonable statistical results.

Moreover, as anticipated earlier, we prove the asymptotic normality of our estimator under the two regimes delineated by different values of  $\bar{\alpha}$ . In particular, we find that if the privacy parameters  $\alpha_1, \dots, \alpha_n$  are large enough to guarantee  $r_{n,N} \sqrt{\log(L_n)} \rightarrow 0$ , with some technical conditions, we essentially obtain the same result as in the case without privacy:

$$\sqrt{N}(\hat{\theta}_n^N - \theta^*) \xrightarrow{\mathcal{L}} \mathcal{N}\left(0, 2\left(\int_0^T \mathbb{E}\left[\left(\frac{\partial_\theta b(\theta^*, X_s)}{\sigma(X_s)}\right)^2\right] ds\right)^{-1}\right) =: \mathcal{N}(0, 2(\Sigma_0)^{-1}) \quad \text{as } n, N \rightarrow \infty.$$

Indeed, the convergence above asserts the asymptotic Gaussianity of our estimator with a convergence rate and a variance that resemble the classic scenario without any privacy constraints.

When the contribution of privacy is instead the dominant one (i.e.  $r_{n,N} \rightarrow \infty$ , with  $r_{n,N}$  defined by (1)), we still recover the asymptotic normality of our estimator, but with a different convergence rate, depending on the average amount of privacy  $\bar{\alpha}^2$ . In this context, some extra challenges appear, leading us to replace the previous grid with a random one, depending on a uniform random variable  $S$  (see Equation (13)). Then, subject to some technical conditions we are able to prove the following:

$$\frac{\sqrt{N\bar{\alpha}^2}}{4(a+1)L_n^2 \log(n)\sqrt{T}}(\hat{\theta}_n^N - \theta^*) \xrightarrow{\mathcal{L}} \sqrt{\hat{v}(S)}(\Sigma_0)^{-1}\mathcal{N},$$

where  $\mathcal{N}$  is a gaussian  $\mathcal{N}(0,1)$  random variable independent of  $S$ ,  $a$  and  $\hat{v}$  are respectively a tuning parameter and an auxiliary function properly defined in (14); both depending on the spline functions under consideration.

It is noteworthy that our results distinctly reveal  $L_n^2 \log(n)$  as the threshold for  $\bar{\alpha}$ , thereby delineating whether the newly introduced term arising from the privacy constraints is a primary contributing factor. The significance of this threshold becomes apparent through our findings. Theorem 2 indicates that the case of 'negligible' privacy corresponds to the constraint  $r_{n,N}\sqrt{\log(L_n)} \rightarrow 0$ , while Theorem 3 establishes the condition  $r_{n,N} \rightarrow \infty$  for achieving 'significant' privacy. In Corollary 1, we investigate the scenario where  $r_{n,N}$  converges to a constant. In this case, we are able to demonstrate the convergence in law of our estimator to the sum of the two Gaussian random variables obtained in Theorems 3 and 2, respectively.

This emphasizes that the threshold demarcating the two asymptotic regimes of 'significant' and 'negligible' privacy is dictated by the asymptotic behavior of  $r_{n,N}$ . The additional  $\log(L_n)$  in the condition outlined in Theorem 2 is introduced for technical reasons associated with the grid, representing a non-optimal condition necessary to mitigate the impact of privacy constraints. Additionally, we provide a discussion about effective privacy.

The paper unfolds as follows. In Section 2, we introduce the model and its underlying assumptions. Notably, we formulate the definition of local differential privacy tailored to stochastic processes in Section 2.2. Section 3 is dedicated to presenting the contrast function pivotal for our estimator's definition, alongside articulating our main results, whose strengths and weaknesses we discuss in Section 4. Turning to Section 5, we furnish essential tools essential for proving our main results. This includes an exploration of spline functions in Section 5.1, followed by technical results outlined in Section 5.2. In summary, the proofs of our main and technical results find their place in Sections 6 and 7, respectively.

## 2 Mathematical framework

### 2.1 Setting and assumptions

Let  $T > 0$ . Let  $W^1, \dots, W^N$  be  $N \in \mathbb{N}^* = \{1, 2, 3, \dots\}$  independent standard Brownian motions. For any  $i \in \{1, \dots, N\}$ , we consider the diffusion process  $(X_t^i)_{t \in [0, T]}$  defined by

$$X_t^{\theta, i} = X_0^{\theta, i} + \int_0^t b(\theta, X_s^{\theta, i}) ds + \int_0^t \sigma(X_s^{\theta, i}) dW_s^i, \quad (2)$$

where  $b : \Theta \times \mathbb{R} \rightarrow \mathbb{R}$ ,  $\sigma : \mathbb{R} \rightarrow \mathbb{R}$  and  $\theta \in \Theta$ . We fix  $\Theta := [0, 1]$  to simplify the notation. Assume that for any  $i \in \{1, \dots, N\}$ , the processes  $(W_t^i)_{t \in [0, T]}$  are independent of the initial value  $(X_0^{\theta, 1}, \dots, X_0^{\theta, N})$ . We also assume that  $(X_0^{\theta, i})_i$  are i.i.d with  $X_0^{\theta, i} \in \cap_{p \geq 1} L^p$ .

As anticipated in the introduction, we aim at estimating the parameter  $\theta^* \in \overset{\circ}{\Theta} = (0, 1)$  given the observations  $(X_{t_j}^{\theta, i})_{i=1, \dots, N, j=1, \dots, n}$  subject to local differential privacy constraints, see next section for a formal definition and a rigorous introduction of the problem.

We introduce the discretization step as  $\Delta_n := T/n$ , so that  $t_{j,n} = jT/n = j\Delta_n$ . The asymptotic framework here considered is such that both  $N, n \rightarrow \infty$  while the time horizon  $T$  is fixed. Moreover,  $N$  goes to  $\infty$  as a polynomial of  $n$ , i.e. there exists  $r > 0$  such that  $N = O(n^r)$ . In the sequel we will write simply  $X_{t_j}^i$  when the process is computed in the true value of the parameter  $\theta^*$ , that is  $X_{t_j}^{\theta^*, i}$ .

Let us consider the assumptions :

**Assumption 1.** *For all  $\theta \in \Theta$  the function  $b(\theta, \cdot)$  is bounded. Moreover,  $b(\theta, \cdot)$  and  $\sigma$  are globally Lipschitz, i.e there exists  $c > 0$  such that, for all  $x, y \in \mathbb{R}$ ,*

$$|b(\theta, x) - b(\theta, y)| + |\sigma(x) - \sigma(y)| \leq c|x - y|.$$

**Assumption 2.** *We assume that the diffusion coefficient is bounded away from 0: for some  $\sigma_{\min} > 0$ ,*

$$\sigma_{\min}^2 \leq \sigma^2(x).$$

Under assumptions 1 and 2, Equation (2) has a unique strong solution  $(X_t^{\theta, i})_{t \in [0, T]}$  taking its values in  $(\mathbb{R}, \mathcal{B}(\mathbb{R}))$ .

**Assumption 3.** *For all  $k \in \mathbb{N} = \{0, 1, 2, \dots\}$ , the function  $\frac{\partial^k}{\partial \theta^k} b$  is bounded uniformly in  $\theta$ :  $\sup_{x, \theta} |\frac{\partial^k}{\partial \theta^k} b(\theta, x)| < \infty$ .*

**Assumption 4.** *[Identifiability]*

*For all  $\theta \in \Theta$  such that  $\theta \neq \theta^*$ , it is*

$$\int_0^T \mathbb{E} \left[ \frac{(b(\theta, X_s) - b(\theta^*, X_s))^2}{\sigma^2(X_s)} \right] ds > 0.$$

One can easily check that Assumption 4 is equivalent to ask that, for any  $\theta \in \Theta$  such that  $\theta \neq \theta^*$ , it is  $b(\theta, \cdot) \neq b(\theta^*, \cdot)$ . This will be crucial in order to prove the consistency of the estimator we will propose.

Observe that, in the sequel, we will often shorten the notation  $\partial_{\theta}^k g$  for  $\frac{\partial^k}{\partial \theta^k} g$ , for any derivable function  $g$ .

**Assumption 5.** *[Invertibility]*

*Define the asymptotic Fisher information as  $I(\theta) := \int_0^T \mathbb{E} [(\frac{\partial_{\theta} b(\theta, X_s)}{\sigma(X_s)})^2] ds$ . We assume that, for any  $\theta \in \Theta$ ,  $I(\theta) > 0$ .*

We will see that Assumption 5 will be essential to prove the asymptotic normality of our estimator.

## 2.2 Problem formulation

Let  $(X_t^1), \dots, (X_t^N)$  be solutions of the stochastic differential equation (2). Since they are driven by independent Brownian motions, we can regard them as  $N$  independent realizations of the same diffusion process. It is important to note that, for classical SDEs, it is generally not feasible to estimate the drift over a finite time horizon. However, in this context, the number of copies  $N$  will serve a similar purpose as the time horizon  $T$  does in parameter estimation for classical SDEs. As  $N$  tends to infinity, the sample size will effectively increase, allowing for our estimation procedure. The  $N$  copies follow the law of the same stochastic process  $(X_t)_{t \in [0, T]}$ ,

and we observe each of them in  $n + 1$  different instants of time  $0 = t_0 \leq t_1 \leq \dots \leq t_n = T$ . They can represent the information coming from  $N$  different individuals, that evolves in time.

In our approach, we adopt componentwise local differential privacy as introduced in [2]. It means that we do not release the public data pertaining to each individual based on the whole vector of its private data, but instead release data relying on componentwise observation of this private vector. As shown in [2], this constraint usually makes harder to infer the joint law of the private data, but it might be more suitable in practice when dealing with temporal series.

Let us now formalize the framework discussed earlier. We introduce  $\mathbf{X}^i := (X_{t_0}^i, \dots, X_{t_n}^i)$  for any  $i \in \{1, \dots, N\}$ . The process of privatizing the raw samples  $(\mathbf{X}^i)_{i=1, \dots, N}$  and transforming them into the public set of samples  $(\mathbf{Z}^i)_{i=1, \dots, N}$  is captured by a conditional distribution, known as privacy mechanism or channel distribution. We make the assumption that each component of a disclosed observation, denoted by  $Z_j^i$ , is privatized independently and belongs to a specific space  $\mathcal{Z}^i$ , which may vary for each  $i$ . This implies that the observation  $\mathbf{Z}^i$  belongs to the product space  $\mathcal{Z} := \prod_{j=1}^n \mathcal{Z}_j$ . Additionally, we assume that the spaces  $\mathcal{Z}_j$  are separable complete metric spaces. Their corresponding Borel sigma-fields define measurable spaces  $(\mathcal{Z}_j, \Xi_{\mathcal{Z}_j})$  for all  $j \in \{0, \dots, n\}$ .

Let us now discuss the properties and structure of the privacy mechanism in our framework. For simplicity, the privacy mechanism is designed to be non interactive between the  $N$  individuals. This gives rise to the the following conditional independence structure : for  $j \in \{1, \dots, n\}$ ,

$$\{X_{t_j}^i, X_{t_{j-1}}^i\} \rightarrow Z_j^i, \quad Z_j^i \perp\!\!\!\perp X_{t_l}^k \mid \{X_{t_j}^i, X_{t_{j-1}}^i\} \text{ for } k \neq i, \forall l \in \{0, \dots, n\}.$$

More precisely, for  $j = 1, \dots, n$  and  $i = 1, \dots, N$ , given  $X_{t_j}^i = x_j^i \in \mathbb{R}$  and  $X_{t_{j-1}}^i = x_{j-1}^i \in \mathbb{R}$ , the public output  $Z_j^i \in \mathcal{Z}_j$  is drawn as

$$Z_j^i \sim Q_j(\cdot \mid X_{t_j}^i = x_j^i, X_{t_{j-1}}^i = x_{j-1}^i) \quad (3)$$

for Markov kernels  $Q_j : \Xi_{\mathcal{Z}_j} \times (\mathbb{R} \times \mathbb{R}) \rightarrow [0, 1]$ . The notation  $(\mathcal{Z}, \Xi_{\mathcal{Z}}) = (\prod_{j=1}^n \mathcal{Z}_j, \otimes_{j=1}^n \Xi_{\mathcal{Z}_j})$  refers to the measurable space of non-private (or public) data. The space of public data, denoted by  $\mathcal{Z}$ , can be quite general, as it is selected by the statistician based on a specific privatization mechanism. Nonetheless, in the parameter estimation discussed below, it will be valued in  $\mathcal{Z} = \mathbb{R}^{d_Z \times n}$  for some dimension  $d_Z$  given in Section 3.

This privatization structure highlights a major difference compared to the definition of componentwise local differential privacy (CLDP) introduced in [2]. In our case, the variable  $Z_j^i$  is derived not only from the private value of  $X_{t_j}^i$ , but also from the previous observation at time  $t_{j-1}$ . This allows for incorporating additional temporal information in the privatization process. Such privacy mechanism is in practice more flexible than a usual privatization based on the whole vector  $\mathbf{X}^i$ . It enables for instance a physician accessing to the record of just two consecutive private values of an individual to output the public data. However, it excludes the situation where the private data can be accessed only for a single date before releasing the public value. This would be the case if the collected private data is immediately destroyed after the public view is sent. However, by [2], we know that this situation increases the error of estimation for the joint law of the diffusion process  $X$ , and in turn certainly would deteriorate the estimation of the drift parameter. For this reason, we exclude it from our analysis.

Let us mention that a more general concept of interactive privacy mechanism could be considered. In that case, the output  $Z_j^i$  would be constructed on the basis of some private data and all the public data already available. Although it is typically easier to work with non-interactive algorithms, as they yield independent and identically distributed privatized samples, there are situations where it is advantageous for the channel's output to depend on previous computations. Stochastic approximation schemes, for instance, require this kind of dependency (see [40]). In our framework the temporal aspect of the private data  $X_j^i$  is along the index  $j$ ,



whereas the usual situation of interactive mechanism is to construct  $Z^i$  inductively on the index  $i$  corresponding to the individuals. Thus, to cope with real situation the definition of interactive mechanism should be modified accordingly in our case. For this reason, we do not pursue the discussion here about interactive mechanism.

The notion of privacy can be quantified using the concept of local differential privacy. Let  $\alpha = (\alpha_1, \dots, \alpha_n)$  be a given parameter, where  $\alpha_j \geq 0$  for each  $j \in \{1, \dots, n\}$ . We say that the random variable  $Z_j^i$  is an  $\alpha_j$ -differentially locally privatized view of  $X_{t_j}^i$  and  $X_{t_{j-1}}^i$  if, for all  $x_j, x'_j \in \mathbb{R}$ , and  $x_{j-1}, x'_{j-1} \in \mathbb{R}$ , the following condition holds:

$$\sup_{A \in \Xi_{Z_j}} \frac{Q_j(A | X_{t_j}^i = x_j, X_{t_{j-1}}^i = x_{j-1})}{Q_j(A | X_{t_j}^i = x'_j, X_{t_{j-1}}^i = x'_{j-1})} \leq \exp(\alpha_j). \quad (4)$$

We define the privacy mechanism  $\mathbf{Q} = (Q_1, \dots, Q_n)$  to be  $\alpha$ -differentially locally private if each variable  $Z_j^i$  satisfies the condition of being an  $\alpha_j$ -differentially locally privatized view of  $X_{t_j}^i$  and  $X_{t_{j-1}}^i$ .

The parameter  $\alpha_j$  serves as a measure of the level of privacy guaranteed to the variables  $X_{t_j}^i$  and  $X_{t_{j-1}}^i$ . By setting  $\alpha_j = 0$ , we ensure perfect privacy, meaning that it is impossible to recover these variables from the perspective of  $Z_j^i$ . On the other hand, as  $\alpha_j$  tends to infinity, the privacy restrictions become less stringent.

In the upcoming section, we will introduce a privacy mechanism that serves as the foundation for our estimation procedure. Firstly, we will establish its adherence to the  $\alpha$ -local differential privacy condition, as outlined in Equation (4). Subsequently, we will demonstrate that the estimator we propose, based solely on observations of the privatized views  $Z_j^i$  for  $i = 1, \dots, N$  and  $j = 1, \dots, n$ , is consistent and asymptotically normal, with the convergence rate depending on the privacy level  $\alpha$ , in the case of significant privacy.

### 3 Statistical procedure and main results

#### 3.1 Privatization mechanism and estimation procedure

We assume that the functions  $b$  and  $\sigma$  are known and we aim at estimating the unknown parameter  $\theta^*$  under  $\alpha$ -local differential privacy, as properly formalized in previous section. Hence, we need to define a public sample  $(Z_j^i)_{1 \leq i \leq N, 1 \leq j \leq n}$  obtained from observations  $(X_{t_j}^{\theta, i})_{1 \leq i \leq N, 0 \leq j \leq n}$  of the initial data via a privatization mechanism that satisfies the condition in (4).

Consider the classical scenario in statistics, where the goal is to estimate the parameter  $\theta^*$  based on continuous observations of the stochastic differential equation given in (2). It is well-known that the maximum likelihood estimator (MLE) performs optimally in this case, being consistent and asymptotically Gaussian with an optimal variance. However, when privacy is not a concern and only discrete observations of the equation are available, the transition density (and hence the likelihood) of the process is no longer accessible. To address this challenge, a commonly used approach in the literature is to employ a contrast function that serves as a substitute for the likelihood. This contrast function approximates the likelihood based on the Euler approximation scheme. Specifically, for any  $\theta \in \Theta$ , it takes the form :

$$\sum_{i=1}^N \sum_{j=1}^n \frac{(X_{t_j}^i - X_{t_{j-1}}^i - \Delta_n b(\theta, X_{t_{j-1}}^i))^2}{\sigma^2(X_{t_{j-1}}^i)}.$$

The proposed estimator, denoted as  $\hat{\theta}_n^N$ , minimizes the above quantity over the parameter set  $\Theta$ . It can be verified that minimizing the aforementioned quantity is equivalent to maximizing

the following expression:

$$\sum_{i=1}^N \sum_{j=1}^n \frac{2b(\theta, X_{t_{j-1}}^i)(X_{t_j}^i - X_{t_{j-1}}^i) - \Delta_n b^2(\theta, X_{t_{j-1}}^i)}{\sigma^2(X_{t_{j-1}}^i)} =: \sum_{i=1}^N \sum_{j=1}^n f(\theta; X_{t_{j-1}}^i, X_{t_j}^i). \quad (5)$$

Hence, it is natural to incorporate the above quantity into the definition of the privacy mechanism employed in our estimation procedure.

Furthermore, as said in the introduction, it is widely recognized that introducing centered Laplace-distributed noise to bounded random variables ensures  $\alpha$ -differential privacy. Laplace random variables will therefore play a role in defining the privacy mechanism.

We commence by establishing a grid of the parameter space  $\Theta = [0, 1]$  upon which we will construct the Laplace random variables. Let us denote by  $\Xi = \{0 \leq \theta_0 < \dots < \theta_{L_n-1} \leq 1\}$  this grid. It has cardinality  $L_n \in \mathbb{N}^*$ . For  $n \rightarrow \infty$ , we assume  $L_n$  to go to  $\infty$  with the restriction that there exists  $r > 0$  such that  $L_n = O(n^r)$ .

In order to define the privatized views of our data we need to introduce a smooth version of the indicator function, that we denote as  $\varphi$ . It is such that  $\varphi(\xi) = 0$  for  $|\xi| \geq 2$ ,  $\varphi(\xi) = 1$  for  $|\xi| \leq 1$  and, for  $1 < |\xi| < 2$ ,  $\varphi \in C^\infty(\mathbb{R})$ .

We fix  $a \in \mathbb{N}^*$  and, for  $(i, j, k, \ell) \in \{1, \dots, N\} \times \{1, \dots, n\} \times \{0, \dots, a\} \times \{0, \dots, L_n - 1\}$ , let us denote by  $\mathcal{E}_j^{i, \ell, (k)}$  a random variable, such that  $(\mathcal{E}_j^{i, \ell, (k)})_{i, j, k, \ell}$  are independent variables with law

$$\mathcal{E}_j^{i, \ell, (k)} \sim \mathcal{L}(2\tau_n L_n (a + 1)/\alpha_j), \quad (6)$$

where  $\tau_n := \sqrt{\Delta_n} \log(n)$  and  $L_n$  is the cardinality of  $\Xi$  as above. We assume that the variables  $\mathcal{E}_j^{i, \ell, (k)}$  are independent from the data  $X_{t_{j'}}^{i'}$  for  $i' = 1, \dots, N$  and  $j' = 0, \dots, n$ . Then, we set for any  $i \in \{1, \dots, N\}$ ,  $j \in \{1, \dots, n\}$ ,  $k \in \{0, \dots, a\}$ ,  $\ell \in \{0, \dots, L_n - 1\}$

$$\begin{aligned} Z_j^{i, (k)}(\theta_\ell) &:= f^{(k)}(\theta_\ell; X_{t_{j-1}}^i, X_{t_j}^i) \varphi\left(f^{(k)}(\theta_\ell; X_{t_{j-1}}^i, X_{t_j}^i)/\tau_n\right) + \mathcal{E}_j^{i, \ell, (k)} \\ &= f_j^{i, \ell, (k)} \times \varphi_{\tau_n}\left(f_j^{i, \ell, (k)}\right) + \mathcal{E}_j^{i, \ell, (k)}, \end{aligned} \quad (7)$$

where

$$f_j^{i, \ell, (k)} := f^{(k)}(\theta_\ell; X_{t_{j-1}}^i, X_{t_j}^i) = \frac{\partial^k}{\partial \theta^k} f(\theta_\ell, X_{t_{j-1}}^i, X_{t_j}^i) \quad (8)$$

and  $\varphi_{\tau_n}(\cdot) := \varphi(\cdot/\tau_n)$ . Remark that the dependence on  $k$  in  $\mathcal{E}_j^{i, \ell, (k)}$  does not stand for the derivatives of the Laplace itself but it is a reminder of the fact we are adding some noise to the derivatives of  $f$ . An analogous comment applies to  $Z_j^{i, (k)}$ .

The public data is then defined by

$$Z_j^i := (Z_j^{i, (k)}(\theta))_{\theta \in \Xi, 0 \leq k \leq a} \in \mathbb{R}^{L_n \times (a+1)}. \quad (9)$$

It is easy to check that the local differential privacy control holds true, as proven in the following lemma.

**Lemma 1.** *The public variables described in (9) are  $\alpha$ -local differential private views of the original  $(X_{t_{j-1}}^i, X_{t_j}^i)$ .*

*Proof.* Let us denote by  $(z_j^{\theta, k})_{\theta \in \Xi, 0 \leq k \leq a} \mapsto q_j((z_j^{\theta, k})_{\theta \in \Xi, 0 \leq k \leq a} \mid X_{t_j}^i = x_j, X_{t_{j-1}}^i = x_{j-1})$  the density of the public data  $Z_j^i = (Z_j^{i, (k)}(\theta))_{\theta \in \Xi, 0 \leq k \leq a} \in \mathbb{R}^{L_n \times (a+1)}$  conditional to  $X_{t_j}^i = x_j$ ,  $X_{t_{j-1}}^i = x_{j-1}$  for  $j \in \{1, \dots, n\}$  and  $i \in \{1, \dots, N\}$ .

As  $\mathcal{E}_j^{i,\ell,(k)}$  is distributed as a centered Laplace random variable with scale parameter  $2\tau_n L_n(a+1)/\alpha_j$ , its density at the point  $x \in \mathbb{R}$  is given by  $\frac{1}{2\tau_n L_n(a+1)}\alpha_j \exp(-\frac{1}{2\tau_n L_n(a+1)}\alpha_j|x|)$ . Then, using the independence of the variables  $(Z_j^{i,(k)}(\theta))_{\theta \in \Xi, 0 \leq k \leq a}$  and denoting  $\varphi_{f^{(k)}, \tau_n}^\theta(x, y) := \varphi(f^{(k)}(\theta; x, y)/\tau_n)$  for  $\theta \in \Xi$ , we have

$$\begin{aligned} & \frac{q_j((z_j^{\theta,k})_{\theta \in \Xi, 0 \leq k \leq a} \mid X_{t_j}^i = x_j, X_{t_{j-1}}^i = x_{j-1})}{q_j((z_j^{\theta,k})_{\theta \in \Xi, 0 \leq k \leq a} \mid X_{t_j}^i = x'_j, X_{t_{j-1}}^i = x'_{j-1})} \\ &= \prod_{\theta \in \Xi} \prod_{k=0}^a \exp \left[ \frac{\alpha_j}{2\tau_n L_n(a+1)} (z - f^{(k)}(\theta; x_j, x_{j-1})) \varphi_{f^{(k)}, \tau_n}^\theta(x_{j-1}, x_j) \right. \\ & \quad \left. - \frac{\alpha_j}{2\tau_n L_n(a+1)} (z - f^{(k)}(\theta; x'_j, x'_{j-1})) \varphi_{f^{(k)}, \tau_n}^\theta(x'_{j-1}, x'_j) \right] \\ &= \prod_{\theta \in \Xi} \prod_{k=0}^a \exp \left[ \frac{\alpha_j}{2\tau_n L_n(a+1)} (f^{(k)}(\theta; x_j, x_{j-1}) \varphi_{f^{(k)}, \tau_n}^\theta(x_{j-1}, x_j) \right. \\ & \quad \left. - f^{(k)}(\theta; x'_j, x'_{j-1}) \varphi_{f^{(k)}, \tau_n}^\theta(x'_{j-1}, x'_j) \right] \\ &\leq \prod_{\theta \in \Xi} \prod_{k=0}^a \exp \left( \frac{\alpha_j}{L_n(a+1)} \right) = \exp(\alpha_j), \end{aligned}$$

where we have used the fact that  $f^{(k)}(\theta; X_{t_{j-1}}^i, X_{t_j}^i) \varphi_{f^{(k)}, \tau_n}^\theta(X_{t_{j-1}}^i, X_{t_j}^i)$  is bounded by  $\tau_n$  from the construction of  $\varphi_{f^{(k)}, \tau_n}^\theta$ , together with  $\text{card}(\Xi) = L_n$ . It gives the wanted result.  $\square$

In order to define our estimator and derive the convergence results, we must smoothly extend the definition of  $Z_j^{i,(0)}(\theta_\ell) = f(\theta_\ell; X_{t_{j-1}}^i, X_{t_j}^i) \varphi(f(\theta_\ell; X_{t_{j-1}}^i, X_{t_j}^i)/\tau_n) + \mathcal{E}_j^{i,\ell,(0)}$  from the grid  $\Xi$  to the entire space  $\Theta$ . Indeed, recalling the contrast function without privacy is as in (5), one can easily see it will enable us to define a smooth contrast function by summing these extensions on  $i, j$ .

The extension is achieved through the application of a spline approximation method, which is comprehensively discussed in Section 5.1. More specifically, starting with the initial definition of  $Z_j^i(\theta)$ , valid for all  $\theta \in \Xi$ , we will construct its spline approximation of order  $a$ , denoted as  $H_{\Xi} Z_j^i(\theta)$ . The extended function is well-defined for any  $\theta$  and coincides with  $Z_j^{i,(0)}(\theta)$  within the confines of  $\Xi$ . More formally, the spline extension  $H_{\Xi}$  is given by a linear operator

$$H_{\Xi} : \begin{cases} \mathbb{R}^{L_n \times (a+1)} \rightarrow \mathcal{C}^a([\theta_0, \theta_{L_n-1}]) \\ (g_\ell^k)_{0 \leq \ell \leq L_n-1, 0 \leq k \leq a} \mapsto (g(\theta))_{\theta \in [\theta_0, \theta_{L_n-1}]} \end{cases} \quad (10)$$

where the function  $g$  is such that  $g^{(k)}(\theta_\ell) = g_\ell^k$  for all  $\theta_\ell \in \Xi$ . A thorough elucidation of the process involved in creating such a function can be found in Section 5.1.

The natural contrast function in this context, defined for  $\theta \in \Xi$ , is  $S_n^N(\theta) := \sum_{i=1}^N \sum_{j=1}^n Z_j^{i,(0)}(\theta)$ . Its extension to  $[\theta_0, \theta_{L_n-1}]$  is given by

$$S_n^{N,\text{pub}}(\theta) := \sum_{i=1}^N \sum_{j=1}^n H_{\Xi} \left( Z_j^i \right) (\theta) = \sum_{i=1}^N \sum_{j=1}^n H_{\Xi} \left( (Z_j^{i,(k)}(\theta_\ell))_{\ell,k} \right) (\theta), \quad \theta \in [\theta_0, \theta_{L_n-1}]. \quad (11)$$

With access to public data  $(Z_j^i(\theta))_{1 \leq i \leq N, 1 \leq j \leq n}$ , the statistician considers the estimator

$$\hat{\theta}_n^N = \underset{\theta \in [\theta_0, \theta_{L_n-1}]}{\text{argmax}} S_n^{N,\text{pub}}(\theta). \quad (12)$$

To complete the construction of the private estimator it remains to choose the grid  $\Xi$ . Let us start considering the deterministic uniform grid

$$\Xi := \left\{ \theta_\ell = \frac{\ell}{L_n}, \quad \ell \in \{0, \dots, L_n - 1\} \right\}.$$

We will see it will be crucial for the analysis of the variance of the estimator to determine in certain occasions whether the true value of the parameter, denoted as  $\theta^*$ , resides within this grid. To address this, it will be useful in the sequel to introduce a random grid in which the probability of  $\theta^*$  coinciding with any point is zero. Let us remark that the extension of the contrast function is from the grid  $\Xi$  to  $[\theta_0, \theta_{L_n-1}] = [0, 1 - 1/L_n]$  rather than on the whole parameter set  $\Theta = [0, 1]$ . It is convenient to leave out some space on the the rightmost part of parameter space as we will introduce a random shift of size smaller than  $1/L_n$  of the grid in this sequel, to create the randomization. That is why we have assumed  $\theta^* \in \overset{\circ}{\Theta} = (0, 1)$ .

### 3.2 Main results: consistency and asymptotic normality

It is feasible to demonstrate that the estimator in (12), introduced as a natural extension of the Maximum Likelihood Estimator (MLE) in cases of discrete observations and under local differential privacy constraints, exhibits several desirable properties. Notably, it is consistent, as stated in the following theorem and proved in Section 6.

Let us recall that  $\bar{\alpha}^2$  is the harmonic mean over the different privacy levels. It is such that  $1/\bar{\alpha}^2 = n^{-1} \sum_{j=1}^n 1/\alpha_j^2$ .

**Theorem 1** (Consistency). *Assume that A1- A4 hold and that  $\frac{L_n \log(n)}{\sqrt{N}} \sqrt{\frac{\log(L_n)}{\bar{\alpha}^2}} \rightarrow 0$  for  $n, N, L_n \rightarrow \infty$ . Then, the estimator  $\hat{\theta}_n^N$  defined in (12) is consistent:*

$$\hat{\theta}_n^N \xrightarrow{\mathbb{P}} \theta^*.$$

Furthermore, if  $\bar{\alpha}^2$  is chosen to be sufficiently large to ensure that the impact of privacy constraints is negligible, it becomes viable to regain the asymptotic normality of the estimator with a convergence rate and a variance reminiscent of the classical scenario where no privacy constraints are imposed (see for example [4, 15, 16]). In this case the privacy-related influence becomes negligible. This assertion is formally established in the subsequent theorem whose proof is postponed to Section 6. To establish this, we introduce the following assumptions regarding the spline approximation and the discretization step.

**Assumption 6.** [Condition spline approximation]

1. Assume that  $a > 3$  and that  $\frac{\sqrt{N}}{L_n^{a-2}} \rightarrow 0$ .
2. Assume that  $a > 3$  and that  $\frac{\sqrt{N\bar{\alpha}^2}}{L_n^a \log(n)} \rightarrow 0$ .

**Assumption 7.** [Condition discretization step]

1. Assume that  $\sqrt{N\Delta_n} \rightarrow 0$ .
2. Assume that  $\frac{\sqrt{N\Delta_n\bar{\alpha}^2}}{L_n^2 \log(n)} \rightarrow 0$ .

Note that Conditions A6.1 and A7.1 are essential for demonstrating asymptotic normality in scenarios where the contribution of privacy is negligible. On the other hand, A6.2 and A7.2 are required for cases where the contribution of privacy is significant.

Recall that  $r_{n,N} = \frac{L_n^2 \log(n)}{\sqrt{\bar{\alpha}^2}}$ , as introduced in (1).

Remark that of A6.2 can be seen as  $\frac{\sqrt{N}}{L_n^{a-2}} \frac{1}{r_{n,N}} \rightarrow 0$  and, similarly, the second point of A7 translates to  $\sqrt{N} \Delta_n \frac{1}{r_{n,N}} \rightarrow 0$ . We highlight that, in case of significant privacy,  $r_{n,N}$  goes to  $\infty$ . It implies that Points 1 of both the Assumptions above would be enough to obtain the wanted result. We decided to require the conditions gathered in A6.2 and A7.2 as they are weaker.

**Theorem 2** (Asymptotic normality with negligible contribution of privacy). *Assume that A1-A5, A6.1 and A7.1 hold. Assume moreover that  $\sqrt{\log(L_n)} r_{n,N} \rightarrow 0$  and  $\frac{L_n^3 \log(n)}{\sqrt{N}} \sqrt{\frac{\log(L_n)}{\bar{\alpha}^2}} \rightarrow 0$  for  $N, n, L_n \rightarrow \infty$ . Then*

$$\sqrt{N}(\hat{\theta}_n^N - \theta^*) \xrightarrow{\mathcal{L}} \mathcal{N}\left(0, 2\left(\int_0^T \mathbb{E}\left[\left(\frac{\partial_\theta b(\theta^*, X_s)}{\sigma(X_s)}\right)^2\right] ds\right)^{-1}\right) =: \mathcal{N}(0, 2(\Sigma_0)^{-1}) =: \mathcal{Z}_1.$$

One might question the efficiency of the proposed estimator, in the scenario of 'negligible' privacy contribution. A recent paper [17] establishes the *local asymptotic normality (LAN) property* for drift estimation in  $d$ -dimensional McKean-Vlasov models under continuous observations. If we narrow down their result to dimension 1, with a single-dimensional parameter  $\theta$ , the Fisher information derived by the authors can be expressed as follows

$$\int_0^T \int_{\mathbb{R}} \left(\frac{\partial_\theta b}{\sigma}\right)^2(\theta^*, t, x, \bar{\mu}_t) \bar{\mu}_t(dx) dt,$$

where  $\bar{\mu}_t = \bar{\mu}_t^{\theta^*}$  is the law of the McKean-Vlasov SDE under the true value  $\theta^*$  of the parameter. In the case of i.i.d. diffusion processes under consideration, the above quantity simplifies to  $\int_0^T \mathbb{E}\left[\left(\frac{\partial_\theta b(\theta^*, X_s)}{\sigma(X_s)}\right)^2\right] ds$ . It suggests that our estimator is asymptotically efficient when the privacy contribution is 'negligible'.

We can establish the asymptotic normality of our proposed estimator in the case where the contribution of the privacy is the dominant one as well. However, as evident from Theorem 3 below, the issue of privacy significantly affects the estimation of the parameter we intend to estimate. This is demonstrated by the degradation of the convergence rate, which now becomes dependent on the privacy levels  $\alpha_1, \dots, \alpha_n$ . In this case, it is important to observe that we need to ensure that the various levels of privacy do not differ significantly from each other, as elaborated further below.

**Assumption 8.** [*Privacy ratio*] Assume that  $\frac{\max_j \alpha_j}{\min_j \alpha_j} = O(1)$ .

Moreover, in this context we need to introduce a random grid, as anticipated before. Let us introduce a random variable, denoted as  $S$ , that is uniformly drawn in the interval  $(0, 1)$ . The concept is that the statistician initiates the process by generating the uniform random variable  $S$  and subsequently calculates and assigns the value  $\theta_\ell$  as  $\theta_\ell := (\ell + S)/L_n$  for each  $\ell$  in the range from 0 to  $L_n - 1$ . This procedure leads to the establishment of the following random grid:

$$\Xi_S := \left\{ \theta_\ell = \frac{\ell + S}{L_n}, \quad \ell \in \{0, \dots, L_n - 1\} \right\}. \quad (13)$$

We define for  $s \in [0, 1]$ ,

$$\hat{v}(s) := (2a + 1)^2 \left(\frac{2a}{a}\right)^2 s^{2a} (1 - s)^{2a}. \quad (14)$$

Let  $\ell_n^* \in \{0, \dots, L_n - 1\}$  be such that  $\theta^* \in [\theta_{\ell_n^*}, \theta_{\ell_n^*+1})$ . We set

$$v_n(\theta^*) := \hat{v}(L_n(\theta^* - \theta_{\ell_n^*})). \quad (15)$$

Remark that  $v_n(\theta^*)$  is zero if and only if  $\theta^*$  belongs to the grid  $(\theta_\ell)_{0 \leq \ell \leq L_n - 1} = ((\ell + S)/L_n)_{0 \leq \ell \leq L_n - 1}$ . As the shift variable  $S$  has a continuous law, the probability that  $\theta^*$  lies in the grid for some

$n \geq 1$  is zero. Thus, we have that, almost surely,  $v_n(\theta^*) > 0$  for all  $n \geq 1$ . Moreover, the law of  $v_n(\theta^*)$  is independent of  $\theta^*$  and  $n$ , as stated in next lemma, whose proof can be found in Section 7.

**Lemma 2.** *For all  $n \geq 1$ ,  $v_n(\theta^*)$  has the same law as  $\hat{v}(S)$ .*

This allows us to obtain the following asymptotic result.

**Theorem 3** (Asymptotic normality with significant contribution of privacy). *Assume that A1-A5, A6.2, A7.2 and A8 hold. Assume moreover that  $L_n^3 \log(n) \sqrt{\frac{\log(L_n)}{N\bar{\alpha}^2}} \rightarrow 0$  and  $r_{n,N} \rightarrow \infty$  for  $N, n, L_n \rightarrow \infty$ . Then*

$$\frac{\sqrt{N\bar{\alpha}^2}}{4(a+1)L_n^2 \log(n) \sqrt{T}} (\hat{\theta}_n^N - \theta^*) \xrightarrow{\mathcal{L}} \mathcal{N}(0, \hat{v}(S)(\Sigma_0)^{-2}) =: \mathcal{Z}_2$$

where  $\mathcal{Z}_2$  has a mixed normal distribution, with mean 0 and conditional variance  $\hat{v}(S)(\Sigma_0)^{-2}$ . Moreover, this convergence holds jointly with  $v_n(\theta^*) \xrightarrow{\mathcal{L}} \hat{v}(S)$ .

Theorems 2 and 3 provide insights into how the proposed estimator behaves with varying contributions of privacy, particularly concerning the convergence of  $\sqrt{\log(L_n)}r_{n,N}$  towards 0 or those of  $r_{n,N}$  towards  $\infty$ . As already mentioned in the introduction, the asymptotic behaviour of  $r_{n,N}$  dictates the privacy regime. In the corollary below we explore the scenario where privacy levels  $(\alpha_1, \dots, \alpha_n)$  satisfy  $r_{n,N} \sim 1/c_p > 0$ . Its proof is presented in Section 6.

**Corollary 1.** *Assume that A1- A5, A6.2, A7.2 and A8 hold. Assume moreover that  $L_n^3 \log(n) \sqrt{\frac{\log(L_n)}{N\bar{\alpha}^2}} \rightarrow 0$  and there exists  $c_p > 0$  such that  $r_{n,N} \rightarrow 1/c_p$  for  $N, n, L_n \rightarrow \infty$ . Then*

$$\frac{\sqrt{N\bar{\alpha}^2}}{L_n^2 \log(n)} (\hat{\theta}_n^N - \theta^*) \xrightarrow{\mathcal{L}} c_p \mathcal{Z}_1 + 4(a+1)\sqrt{T} \mathcal{Z}_2 = \mathcal{N}(0, (2c_p^2 \Sigma_0 + 16(a+1)^2 T \hat{v}(S))(\Sigma_0)^{-2})$$

and this convergence holds jointly with  $v_n(\theta^*) \xrightarrow{\mathcal{L}} \hat{v}(S)$ .

Corollary 1 emphasizes the crucial roles played by both  $\mathcal{Z}_1$  and  $\mathcal{Z}_2$  in our analysis. The convergence rate of the proposed estimator towards the sum reveals that, in the scenario of negligible privacy, the convergence is towards  $\mathcal{Z}_1$ , whereas in the case of a significant contribution of privacy, the convergence is towards  $\mathcal{Z}_2$ .

An intriguing question emerges: How can one thoughtfully choose the parameter  $L_n$  while ensuring its compliance with the aforementioned conditions? It is noteworthy that  $L_n = O(n^r)$ , and  $r$  arbitrarily small is a feasible choice. In this case, the choice of the order of the spline approximation  $a$  becomes pivotal, requiring it to be sufficiently large to ensure that  $ar$  satisfies the assumptions outlined in A6.

### 3.3 Effective privacy

When considering local differential privacy, a natural question arises regarding the likelihood of recovering private data from the observation of public data. Specifically, the definition of  $\alpha_j$ -LDP provided in (4) informs us about how well the values of  $X_{t_j}^i$  and  $X_{t_{j-1}}^i$  are covered when the value of  $Z_j^i$  is available. However, some information about  $X_{t_j}^i$  and  $X_{t_{j-1}}^i$  could be conveyed by  $Z_k^i$ , for  $k \neq j$ . Therefore, it is worth understanding how precisely the values of  $X_{t_j}^i$  and  $X_{t_{j-1}}^i$  could be revealed by the observations of  $Z_1^i, \dots, Z_n^i$ , which are publicly available. Similar questions have been explored, for example, in [51] and in Section 4.1 in [2]. In particular, it is well understood that if a vector is privatized with an independent channel for each component and the components are independent, then no information on a private component

is carried by the public views of the others.

The situation becomes more intricate if the components of the vector  $(X_{t_0}^i, \dots, X_{t_n}^i)$  are dependent, as the observation of  $Z_1^i, \dots, Z_n^i$  imparts extra information on  $X_{t_j}^i$  and  $X_{t_{j-1}}^i$ . This is evident in the case under consideration, as the observations  $X_{t_0}^i, \dots, X_{t_n}^i$  represent the evolution of one individual, and they are therefore dependent.

For simplicity, assume that  $\alpha_j = \alpha$  for all  $j \in \{1, \dots, n\}$ . Let us denote by  $q((z_h^{\theta,k})_{\theta \in \Xi, 0 \leq k \leq a, 0 \leq h \leq n} | X_{t_j}^i = x_j, X_{t_{j-1}}^i = x_{j-1})$  the density of the public data  $Z_1^i = (Z_1^{i,(k)}(\theta))_{\theta \in \Xi, 0 \leq k \leq a} \in \mathbb{R}^{L_n \times (a+1)}, \dots, Z_n^i = (Z_n^{i,(k)}(\theta))_{\theta \in \Xi, 0 \leq k \leq a} \in \mathbb{R}^{L_n \times (a+1)}$  conditional to  $X_{t_j}^i = x_j, X_{t_{j-1}}^i = x_{j-1}$  for  $j \in \{1, \dots, n\}$  and  $i \in \{1, \dots, N\}$ . We apply Proposition 4.1 in [2] to the privacy mechanism introduced in Section 3.1 and obtain

$$\frac{q((z_h^{\theta,k})_{\theta \in \Xi, 0 \leq k \leq a, 0 \leq h \leq n} | X_{t_j}^i = x_j, X_{t_{j-1}}^i = x_{j-1})}{q((z_h^{\theta,k})_{\theta \in \Xi, 0 \leq k \leq a, 0 \leq h \leq n} | X_{t_j}^i = x'_j, X_{t_{j-1}}^i = x'_{j-1})} \leq \exp(\alpha + 2(n-1)\alpha) = \exp((2n-1)\alpha), \quad (16)$$

where in the application of Proposition 4.1 in [2] we use the crude bound  $\Delta_{\text{ind}} \leq 2$ . This means that we neglect any possible decorrelation arising in the different components of  $(X_{t_j}^i)_{j=1, \dots, n}$ . Equation (16) evaluates how the privacy of  $X_{t_j}^i$  and  $X_{t_{j-1}}^i$  is deteriorated by the observation of the side-channels  $Z_1^i, \dots, Z_n^i$ .

It is important to note that, according to [51], if someone accesses some private values  $x_j, x'_j, x_{j-1}$ , and  $x'_{j-1}$ , it will be impossible for them to determine with a high level of certainty which of the values corresponds to a specific public observation, denoted as  $(Z_j^i)_{1 \leq j \leq n}$ . Any attempt to make a decision in this regard would result in an error, with a probability of at least  $\frac{1}{1+e^{(2n-1)\alpha}}$ , as  $(2n-1)\alpha$  is the privacy level appearing in (16). Hence, one would like the effective privacy level  $\alpha_f$  to be fixed, implying the choice  $\alpha =: \frac{\alpha_f}{2n-1}$ , where  $f$  stands for 'fixed'.

Observe that, in such a case, the condition  $\frac{N^{-1/2}}{L_n} r_{n,N} \rightarrow 0$  needed for consistency translates to  $\frac{1}{\log(L_n)(L_n \log(n))^2} N \frac{\alpha_f^2}{n^2} \rightarrow \infty$ . If we stick to the policy where the grid size  $L_n$  tends slowly to infinity and neglect its contribution, as the one of the log-terms, it implies  $N \gg n^2$ . One might wonder if that is compatible with the condition on the discretization step that puts  $N$  and  $n$  in a relationship, as required for the asymptotic normality of our estimator. The case of 'negligible' privacy is not compatible with the choice  $\alpha = \frac{\alpha_f}{2n-1}$ . Hence, we turn to the study of the regime of 'significant' privacy only. In such a case, condition A7.2 is implied by  $N \Delta_n \frac{\alpha_f^2}{n^2} \leq c$  for some  $c > 0$ . Hence, we are asking  $N \lesssim n^3$ .

In summary, this section helps us understand that, to achieve an effective level of privacy as performant as possible, the number of individuals  $N$  providing data and the number of data per person  $n$  should be linked in a way ensuring that  $n^2 \ll N \lesssim n^3$ . We also see that the choice  $\alpha \sim \alpha_f/(2n)$  impacts the rate of estimation as  $\sqrt{N \bar{\alpha}^2} \sim c \sqrt{N/n^2}$ . In the best situation, corresponding to  $N \sim n^3$ , this rate is of magnitude at most  $\sqrt{n^3/n^2} \sim N^{1/6}$ , showing a slow rate of estimation, as a function of the number of individuals.

## 4 Concluding remarks

This section proposes a discussions arising from the insights gained through this paper. As highlighted earlier, we introduced the concept of local differential privacy (LDP) for diffusion processes and proposed an estimator for parameter estimation of the drift coefficient of i.i.d. diffusion under LDP constraints. Our main findings include the consistency and asymptotic normality of the proposed estimator. The asymptotic normality is achieved at two distinct convergence rates, dependent on whether the term due to the privacy constraint is the primary

contribution or not, leading to a dichotomy (up to a logarithmic term). Specifically, when  $r_{n,N}$  (defined as in (1)) tends to  $\infty$ , the contribution of privacy constraints is significant. On the other hand, if  $r_{n,N}\sqrt{\log(L_n)} \rightarrow 0$ , privacy is negligible, and results align with those in the case without privacy. In the threshold case, where  $r_{n,N}$  converges towards a constant, the proposed estimator converges to the sum of the two random variables obtained in the two previous cases. This implies that the general limit of the estimator depends on whether 'significant' or 'negligible' privacy dominates.

In the following table, we compare the conditions and results in the case of negligible or significant contributions of privacy, recalling that  $r_{n,N} = \frac{L_n^2 \log(n)}{\sqrt{\alpha^2}}$ .

	<i>Negligible Privacy</i>	<i>Significant Privacy</i>
<b>Consistency</b>		
Assumptions		A1- A4
Perfect privacy not allowed		$\frac{N^{-1/2}}{L_n} r_{n,N} \rightarrow 0$
<b>Asymptotic normality</b>		
Dichotomy privacy	$\sqrt{\log(L_n)} r_{n,N} \rightarrow 0$	$r_{n,N} \rightarrow \infty$
Spline approximation A6	$a > 3, \frac{\sqrt{N}}{L_n^{a-2}} \rightarrow 0$	$a > 3, \frac{\sqrt{N\bar{\alpha}^2}}{L_n^a \log(n)} \rightarrow 0$
Discretization A7	$\sqrt{N\Delta_n} \rightarrow 0$	$\frac{\sqrt{N\Delta_n\bar{\alpha}^2}}{L_n^2 \log(n)} \rightarrow 0$
Privacy ratio A8	Not needed	Needed
Result for $n, N \rightarrow \infty$	$\sqrt{N}(\hat{\theta}_n^N - \theta^*) \xrightarrow{\mathcal{L}} \mathcal{N}(0, 2\Sigma_0^{-1})$	$\frac{\sqrt{N\bar{\alpha}^2}}{4L_n^2(a+1)\log(n)\sqrt{T}}(\hat{\theta}_n^N - \theta^*) \xrightarrow{\mathcal{L}} \mathcal{N}(0, \hat{v}(S)\Sigma_0^{-2})$

Here, we address potential extensions and limitations of our main results. Firstly, it is important to note that in the presence of privacy constraints, the levels of privacy  $\alpha_j$  are commonly assumed to be smaller than 1. Consequently, the condition of negligible privacy (i.e.  $\sqrt{\log(L_n)} r_{n,N} \rightarrow 0$ ) is quite stringent and rarely met in practice. Therefore, the case of 'significant' privacy emerges as potentially the most interesting. In such case, we obtain a convergence rate slower than  $\sqrt{N\bar{\alpha}^2}$  mainly due to the necessity of introducing a grid with size  $L_n$  and the subsequent need for spline approximation. It may be possible to enhance the convergence rate by adopting a different approach, at least in certain models, and the rate optimality of the estimators is an unsolved problem. For instance, in the case where  $b$  is polynomial in  $\theta$ , the spline approximation is exact, and it is possible to show that the conditions as in A6 are no longer necessary. This would enable us to prove our results even without the condition  $L_n \rightarrow \infty$ , allowing us the flexibility to choose  $L_n$  as a constant.

Another remark stems from the dependence among data related to the same individual, impacting the effective privacy. This deviation from the privacy level introduced in Section 2.2 results from the extra information carried by side channels, as detailed in Section 3.3. This discrepancy leads to a connection between  $N$  and  $n$ , prompting us to ponder what would happen in the case where the time horizon  $T$  approaches infinity. While studying the fixed time horizon seems natural from a practical standpoint as it aligns with the model that better fits reality, from a mathematical perspective, understanding the behavior as  $T$  approaches infinity in the ergodic case becomes intriguing. In this scenario, allowing for more distant (and less dependent) observations, such as in the case where the discretization step is fixed, would reduce the amount of retrievable information from the side channel, ensuring better effective privacy.

In conclusion, from our current knowledge this project is a first instance of local differential privacy for continuous time stochastic processes. We believe that it can be an informative starting point, aiding statisticians in comprehending some challenges associated with local differential privacy for evolving time-based data. Additionally, it offers some insights into potential directions for future research.



## 5 Preliminary results

Before proving our main results, let us introduce some notation and provide some tools that will be useful in the sequel.

In particular, we will start by providing a detailed introduction about spline functions.

### 5.1 Splines, some tools

Here are some basic refreshments on B-splines. For a more detailed exposé, the reader can refer to the work of Lyche *et al.* [36] from which our presentation is widely inspired.

#### Definition and properties of B-splines

B-splines are piecewise polynomial functions characterized by :

- A knot vector  $\mathbf{t} = (t_1, \dots, t_M)$  that is a nondecreasing sequence of  $M$  elements of some interval  $I \subset \mathbb{R}$ ,
- An integer  $p$  called the degree of the spline.

In our frame, we exclusively consider B-splines whose associated knot sequence  $\mathbf{t}$  satisfies  $M = (a+1)(\Lambda+3)$  for some  $\Lambda, a \in \mathbb{N}^*$  and such that the knots are repeated as follows:

$$t_1 = \dots = t_{2a+2}, \quad t_{(\ell+1)(a+1)+1} = \dots = t_{(\ell+2)(a+1)}, \quad \ell \in \{1, \dots, \Lambda-1\}, \quad \text{and} \quad t_{(a+1)(\Lambda+1)+1} = \dots = t_M.$$

For the sake of convenience we introduce an auxiliary sequence, i.e. the sequence of interpolation points  $\boldsymbol{\xi} = (\xi_\ell, \ell \in \{-1, \dots, \Lambda+1\})$  built from  $\mathbf{t}$  as

$$\xi_\ell =: t_{(a+1)(\ell+1)+1} = \dots = t_{(a+1)(\ell+2)}, \quad \ell \in \{-1, \dots, \Lambda+1\}. \quad (17)$$

Note that  $\xi_{-1} = \xi_0$  and  $\xi_\Lambda = \xi_{\Lambda+1}$ : the points  $\xi_{-1}$  and  $\xi_{\Lambda+1}$  have only been introduced for convenience. To sum up,

$$\mathbf{t} = \underbrace{(\xi_{-1}, \dots, \xi_{-1})}_{a+1 \text{ times}}, \underbrace{(\xi_0, \dots, \xi_0)}_{a+1 \text{ times}}, \dots, \underbrace{(\xi_{\Lambda+1}, \dots, \xi_{\Lambda+1})}_{a+1 \text{ times}}. \quad (18)$$

From now on, we assume that the knots are equally spaced, i.e. for all  $\ell \in \{0, \dots, \Lambda-1\}$

$$\xi_{\ell+1} - \xi_\ell = 1/\Lambda.$$

We recall the definition of B-splines given in Lyche *et al.* [36]:

**Definition 1.** *Let  $h \in \{1, \dots, (a+1)(\Lambda+1)\}$ . The  $h$ -th B-spline  $B_{h,p,\mathbf{t}} : I \rightarrow \mathbb{R}$  with degree  $p \leq 2a+1$  is identically zero if  $t_{h+p+1} = t_h$  and is otherwise defined recursively by*

$$B_{h,p,\mathbf{t}} := \frac{\cdot - t_h}{t_{h+p} - t_h} B_{h,p-1,\mathbf{t}} + \frac{t_{h+p+1} - \cdot}{t_{h+p+1} - t_{h+1}} B_{h+1,p-1,\mathbf{t}}, \quad (19)$$

starting with

$$B_{h,0,\mathbf{t}} := \begin{cases} 1 & \text{on } [t_h, t_{h+1}) \\ 0 & \text{otherwise.} \end{cases}$$

Note that the definition of the spline  $B_{h,p,\mathbf{t}}$  relies only on the sequence of  $p+2$  knots  $t_h \leq t_{h+1} \leq \dots \leq t_{h+p+1}$  and that the support of  $B_{h,p,\mathbf{t}}$  is  $[t_h, t_{h+p+1}]$ . In the sequel, unless stated otherwise, we consider B-spline of order  $p = 2a+1$ . For the sake of readability, we will simply

denote  $B_h$  for  $B_{h,2a+1,t}$ ; i.e. the B-spline with order  $p = 2a + 1$  and underlying knot sequence  $\mathbf{t}$  defined in Equation (18). It will be helpful to use the notation:

$$B_i^k := B_{h,2a+1,t}, \text{ with } h = (i + 1)(a + 1) + k + 1 \quad (20)$$

where  $k \in \{0, \dots, a\}$  and  $i \in \{-1, \dots, \Lambda - 1\}$ . Note that the support of  $B_i^k$  is  $[\xi_i, \xi_{i+2}]$ . We will refer to  $B_i^k$  as the  $p$ -order B-splines which *starts at position*  $i$  and whose *shape* is  $k$ . For  $i \in \{0, \dots, \Lambda - 2\}$  the functions  $B_i^k$  are  $a$ -differentiable, recalling that the smoothness of a spline function  $B_{h,p,t}$  is equal to the order  $p$  minus the maximal multiplicity of a knot appearing in the sequence  $t_h, \dots, t_{h+p+2}$ . The spline functions  $B_{-1}^k$  are right continuous at  $\xi_0$  and  $a$ -differentiable on  $(\xi_0, \xi_1]$ . Following the convention in [36], to avoid the asymmetry of splines decomposition on the closed interval  $[\xi_0, \xi_\Lambda]$ , we set  $B_{\Lambda-1}^k(\xi_\Lambda) = \lim_{x \rightarrow \xi_\Lambda^-} B_{\Lambda-1}^k(x)$ . With this modification, the functions  $B_{\Lambda-1}^k$  are  $a$ -differentiable on  $[\xi_{\Lambda-1}, \xi_\Lambda)$  and left continuous at  $\xi_\Lambda$ . The spline functions  $(B_i^k)_{i,k}$  restricted to  $[\xi_0, \xi_\Lambda]$  generate a linear space of piecewise polynomial functions with degree  $2a + 1$ , regularity of class  $\mathcal{C}^a$  on  $(\xi_0, \xi_\Lambda)$ , and admitting one-sided derivatives at the boundaries of this interval.

**Remark.** As knots are equally spaced, i.e.  $\xi_{\ell+1} - \xi_\ell = 1/\Lambda$ , it is easy to see from (19) that the spline functions are sharing a common scaling factor  $\Lambda$ . Applying Proposition 11 in [36], we also get

$$\sup_{x \in [\xi_0, \xi_\Lambda]} \left| \frac{\partial^m}{\partial x^m} B_i^k(x) \right| \leq c\Lambda^m \quad (21)$$

for  $m \in \{0, \dots, a\}$ ,  $i \in \{-1, \dots, \Lambda - 1\}$ ,  $k \in \{0, \dots, a\}$ .

### Hermite interpolation

We denote  $I^{\neq, \Lambda+1}$  the set consisting of  $(\Lambda+1)$ -tuples  $\boldsymbol{\xi} = (\xi_0, \dots, \xi_\Lambda)$  of  $I$  with  $\xi_0 < \xi_1 < \dots < \xi_\Lambda$ .

**Definition 2** (Hermite interpolation). Let  $a \in \mathbb{N}^*$ ,  $\boldsymbol{\xi} = (\xi_\ell, \ell \in \{0, \dots, \Lambda\}) \in I^{\neq, \Lambda+1}$ ,  $\mathbf{a}_\ell^{(k)} \in \mathbb{R}$  for  $\ell \in \{0, \dots, \Lambda\}$ ,  $k \in \{0, \dots, a\}$  and  $\mathbf{a} = (\mathbf{a}_\ell^{(k)}, \ell \in \{0, \dots, \Lambda\}, k \in \{0, \dots, a\})$ . If it exists, a function  $H_{\boldsymbol{\xi}}(\mathbf{a}) : [\xi_0, \xi_\Lambda] \rightarrow \mathbb{R}$  of class  $\mathcal{C}^a$  such that

$$H_{\boldsymbol{\xi}}(\mathbf{a})(\xi_\ell) = \mathbf{a}_\ell^{(k)}; \forall k = 0, \dots, a, \ell = 0, \dots, \Lambda,$$

is called a Hermite interpolation of  $\mathbf{a} = (\mathbf{a}_\ell^{(k)}, \ell \in \{0, \dots, \Lambda\}, k \in \{0, \dots, a\})$  at  $\boldsymbol{\xi} = (\xi_\ell, \ell \in \{0, \dots, \Lambda\})$  with order  $a$ .

By Mummy [34], it is possible to relate Hermite interpolation with the B-splines functions defined in (20). We set  $\xi_{-1} = \xi_0$ ,  $\xi_{\Lambda+1} = \xi_\Lambda$  and define for  $-1 \leq i \leq \Lambda - 1$  and  $0 \leq k \leq a$ ,

$$g_i^k(x) = \frac{1}{(2a + 1)!} (x - \xi_i)^{\beta_1^k} (x - \xi_{i+1})^{\beta_2^k} (x - \xi_{i+2})^{\beta_3^k} \quad (22)$$

with

$$\beta_1^k = (a + 1) - k - 1 = a - k, \beta_2^k = a + 1, \beta_3^k = k.$$

The following result can be found in [34].

**Proposition 1.** Let  $\mathbf{a} = (\mathbf{a}_\ell^{(k)}, \ell \in \{0, \dots, \Lambda\}, k \in \{0, \dots, a\})$ . The function  $H_{\boldsymbol{\xi}}(\mathbf{a}) : [\xi_0, \xi_\Lambda] \rightarrow \mathbb{R}$  such that

$$H_{\boldsymbol{\xi}}(\mathbf{a}) = \sum_{i=-1}^{\Lambda-1} \sum_{k=0}^a c_i^k B_i^k, \quad (23)$$

where

$$c_i^k(\mathbf{a}) = \sum_{v=0}^a \frac{(-1)^v}{v!} (g_i^k)^{(p-v)}(\xi_{i+1}) \mathbf{a}_{i+1}^v, \quad (24)$$

$p = 2a + 1$  and the  $g_i^k$  are given by (22), is a Hermite interpolation of  $\mathbf{a}$  with order  $a$ .

Remark that although the formula (23) defines a function on the real line, the function  $H_\xi(\mathbf{a})$  is equal to zero outside of  $[\xi_0, \xi_\Lambda]$ , and it is thus generally  $C^a$  only on the interval  $[\xi_0, \xi_\Lambda]$ .

For any function  $f \in C^a$ , we define its projection  $H_\xi f$  on the spline space by setting

$$H_\xi f = H_\xi(\mathbf{a}) \quad \text{with } \mathbf{a}_i^k = f^{(k)}(\xi_i) \text{ for } 0 \leq i \leq \Lambda \text{ and } 0 \leq k \leq a. \quad (25)$$

When a function  $f$  is already an element of the space generated by the splines functions, then (23)–(24) is the usual representation of splines given for instance in Section 1.2.4 of [36].

**Remark.** *Hermite interpolation preserves polynomial functions with order not larger than  $a$ , i.e. for any polynomial function with degree  $k \leq a$ ,*

$$H_\xi P(x) = P(x) \quad \text{for } x \in [\xi_0, \xi_\Lambda].$$

The map  $H_\xi$  is linear as stated in the following lemma:

**Lemma 3.** *Let  $\phi, \psi : I \rightarrow \mathbb{R}$  and their B-spline interpolating functions at  $\xi$  respectively denoted by  $H_\xi \phi$  and  $H_\xi \psi$ . The B-spline interpolating function of  $(f + g)$  denoted by  $H_\xi(f + g)$  satisfies*

$$H_\xi(\phi + \psi) = H_\xi \phi + H_\xi \psi.$$

*Proof.* By the characterization (23)–(25) of  $H_\xi$ , we have

$$H_\xi(\phi + \psi) = \sum_{i=-1}^{\Lambda-1} \sum_{k=0}^a c_i^k(\phi + \psi) B_i^k,$$

where

$$\begin{aligned} c_i^k(\phi + \psi) &= \sum_{m=0}^a \frac{(-1)^m}{m!} (g_i^k)^{(p-m)}(\xi_{i+1}) (\phi + \psi)^{(m)}(\xi_{i+1}) \\ &= \sum_{m=0}^a \frac{(-1)^m}{m!} (g_i^k)^{(p-m)}(\xi_{i+1}) \phi^{(m)}(\xi_{i+1}) + \sum_{m=0}^a \frac{(-1)^m}{m!} (g_i^k)^{(p-m)}(\xi_{i+1}) \psi^{(m)}(\xi_{i+1}) \\ &= c_i^k(\phi) + c_i^k(\psi). \end{aligned}$$

Then,

$$H_\xi(\phi + \psi) = \sum_{i=-1}^{\Lambda-1} \sum_{k=0}^a c_i^k(\phi + \psi) B_i^k = \sum_{i=-1}^{\Lambda-1} \sum_{k=0}^a c_i^k(\phi) B_i^k + \sum_{i=-1}^{\Lambda-1} \sum_{k=0}^a c_i^k(\psi) B_i^k = H_\xi(\phi) + H_\xi(\psi).$$

Hence the result.  $\square$

The following results provide insights on the interpolation  $H_\xi$ .

**Lemma 4.** *For all collections  $\xi \in I^{\neq, \Lambda+1}$ , with  $\xi_{\ell+1} - \xi_\ell = 1/\Lambda$  for  $\ell = 0, \dots, \Lambda - 1$ , and  $\mathbf{a} := (\mathbf{a}_\ell^{(k)}, \ell \in \{0, \dots, \Lambda\}, k \in \{0, \dots, a\})$ , the following holds true:*

$$\sup_{x \in [\xi_0, \xi_\Lambda]} \left| \frac{\partial^u}{\partial x^u} H_\xi(\mathbf{a})(x) \right| \leq c \Lambda^u \sup_{\ell, k} |\mathbf{a}_\ell^{(k)}|,$$

where  $H_\xi(\mathbf{a})$  is Hermite interpolant to the data  $\mathbf{a}$  at  $\xi$ .

*Proof.* From Proposition 1, the function  $H_{\xi}(\mathbf{a})$  is defined by

$$H_{\xi}(\mathbf{a}) = \sum_{i=-1}^{\Lambda-1} \sum_{k=0}^a \sum_{v=0}^a \frac{(-1)^v}{v!} (g_i^k)^{(p-v)} (\xi_{i+1}) \mathbf{a}_{i+1}^{(v)} B_i^k.$$

We recall that  $p = 2a + 1$ . Using (21) and noting that  $|(g_i^k)^{(p-v)} (\xi_{i+1})|$  is bounded by 1, we get

$$\begin{aligned} \sup_{x \in [\xi_0, \xi_{\Lambda}]} \left| \frac{\partial^u}{\partial x^u} H_{\xi}(\mathbf{a})(x) \right| &\leq \sum_{i=-1}^{\Lambda-1} \sum_{k=0}^a \sum_{v=0}^a \frac{1}{v!} |\mathbf{a}_{i+1}^{(v)}| \sup_{x \in [\xi_0, \xi_{\Lambda}]} \left| \frac{\partial^u}{\partial x^u} B_i^k(x) \right| \\ &\leq c \Lambda^u \sup_{\ell, k} |\mathbf{a}_{\ell}^{(k)}| \end{aligned}$$

for some constant  $c > 0$  that does not depend on  $\Lambda$ . □

**Proposition 2.** *Let  $\xi = (\xi_{\ell}, \ell \in \{0, \dots, \Lambda\}) \in I^{\neq, \Lambda+1}$  such that  $\xi_{\ell+1} - \xi_{\ell} = 1/\Lambda$  for  $\ell = 0, \dots, \Lambda - 1$ , and let  $f : I \rightarrow \mathbb{R}$  a function of class  $C^{a+1}$ . We denote its Hermite interpolation  $H_{\xi}f$  at  $\xi$  defined as (25). For all  $k \in \{0, \dots, a\}$ , there exists a constant  $c > 0$  independent of  $f$  such that*

$$\sup_{x \in [\xi_0, \xi_{\Lambda}]} \left| \frac{\partial^k}{\partial x^k} f(x) - \frac{\partial^k}{\partial x^k} H_{\xi}f(x) \right| \leq \frac{c}{\Lambda^{a+1-k}} \sup_{x \in [\xi_0, \xi_{\Lambda}]} \left| \frac{\partial^{a+1}}{\partial x^{a+1}} f(x) \right|. \quad (26)$$

*Proof.* The proof is postponed to Subsection 7.2 □

**Remark.** *If the function  $f$  in the previous proposition is a polynomial function of order at most  $a$ , then we see that the right hand side in (26) is zero. This is not surprising as we know that the Hermite approximation preserves polynomial functions.*

In our asymptotics, we will see that the number of point  $\Lambda$  will be asymptotically equivalent to  $L_n$ . Hence, it will tend to infinity and so it will be convenient to use the scaling and translation properties (see Section 1.1.1 in [36]) of the spline functions to represent  $B_{\ell}^k$ . Assuming that  $\xi_{\ell+1} - \xi_{\ell} = 1/\Lambda$  for  $\ell \in \{0, \dots, \Lambda - 1\}$ , we can represent, for  $k \in \{0, \dots, a\}$ ,  $\ell \in \{0, \dots, \Lambda - 1\}$ ,

$$B_{\ell}^k(x) = \bar{B}_k(\Lambda(x - \xi_{\ell})),$$

where  $\bar{B}_k$  is the spline function of order  $p = 2a + 1$  constructed on the knots  $0, 1, 2$  where the knot  $0$  is repeated  $a + 1 - k$  times, while the knot  $1$  is repeated  $a + 1$  times and the knot  $2$  is repeated  $k + 1$  times. We have the following result:

**Lemma 5.** *With previous notation, for all  $x \in \mathbb{R}$ ,*

$$\sum_{k=0}^a \bar{B}'_k(x) = (2a + 1) \binom{2a}{a} \left[ x^a (1 - x)^a \mathbf{1}_{[0,1]}(x) - (x - 1)^a (2 - x)^a \mathbf{1}_{[1,2]}(x) \right].$$

*Proof.* The proof is postponed to Subsection 7.3. □

## Public data extension by B-splines

Starting from the notation introduced in the previous subsection on B-splines, we consider the case where  $I = \Theta = [0, 1]$ ,  $\Lambda = L_n - 1$  and  $\xi_{\ell} = \theta_{\ell}$  for all  $\ell \in \{0, \dots, \Lambda\}$ , i.e. the sequence of interpolation points (17) is here the sequence of grid points  $(\theta_{\ell}, \ell \in \{0, \dots, L_n - 1\})$ . Now, the operator  $H_{\Xi}$  given in (10) is the operator  $H_{\xi}$  detailed in the previous subsection. We recall that for any  $(i, j) \in \{1, \dots, N\} \times \{1, \dots, n\}$ , the public data  $Z_j^i = (Z_j^{i,(k)}(\theta))_{\theta \in \Xi, 0 \leq k \leq a} \in \mathbb{R}^{L_n \times (a+1)}$

is available. It encapsulates some proxy for the values of  $f(\theta; X_{t_{j-1}}^i, X_{t_j}^i)$ , where  $\theta$  is an element of the grid, as well as for its derivatives up to order  $a$ . Applying for any  $(i, j) \in \{1, \dots, N\} \times \{1, \dots, n\}$  the Proposition 1 to the data  $Z_j^i$  we define  $H_{\Xi} Z_j^i := H_{\xi} Z_j^i$  the Hermite interpolation of  $Z_j^i$  on the grid  $\Xi$ , i.e. such that for all  $k \in \{0, \dots, a\}$ ,  $\theta \in \Xi = \{\theta_0, \dots, \theta_{L_n-1}\}$ ,

$$(H_{\Xi} Z_j^i)^{(k)}(\theta) = Z_j^{i,(k)}(\theta).$$

To lighten the notation we will write  $H$  for  $H_{\Xi}$ .

## 5.2 Technical results

In the following, it will be particularly convenient to keep track of the size of the different terms we will be working with. The definition of the function  $R_{t,n}^N$  as below will help us in such sense. Define  $\mathcal{F}_t^N = \sigma(X_s^i, s \leq t, i \in \{1, \dots, N\}) \vee \sigma(\mathcal{E}_u^{i,\ell,(k)}, t_u \leq t, i \in \{1, \dots, N\}, \ell \in \{0, \dots, L_n - 1\}, k \in \{0, \dots, a\})$  and  $\mathbb{E}_t[\cdot] := \mathbb{E}[\cdot | \mathcal{F}_t^N]$ . For a set of random variables  $(R_{t,n}^N)$  and  $\tilde{k} \geq 0$ , the notation  $R_{t,n}^N = R_t(\Delta_n^{\tilde{k}})$  means that  $R_{t,n}^N$  is  $\mathcal{F}_t^N$ -measurable and the set  $(R_{t,n}^N / \Delta_n^{\tilde{k}})$  is bounded in  $L^q$  for all  $q \geq 1$ , uniformly in  $t, n, N$ . Hence, it exists a constant  $C_q > 0$  such that

$$\mathbb{E} \left[ \left| \frac{R_{t,n}^N}{\Delta_n^{\tilde{k}}} \right|^q \right] \leq C_q \quad (27)$$

for any  $t, n, N, q \geq 1$ . If this remainder term also depends on the individual  $i \in \{0, \dots, N\}$ , we assume that the control is uniform in  $i$ . Thanks to the definition just provided, the function  $R$  has the following useful property

$$R_t(\Delta_n^{\tilde{k}}) = \Delta_n^{\tilde{k}} R_t(1).$$

We underline that the equation above does not entail the linearity of  $R$ , as in the left and the right hand side above the two functions  $R$  are not necessarily the same but just two functions on which the control in (27) is satisfied.

Let us state a technical lemma that gathers some moment inequalities we will use several times in the sequel. For the interested reader, its proof can be found for example in Lemma 5.1 of [4].

In the sequel the notation  $c$  refers to a general constant and its value may change from line to line.

**Lemma 6.** *Assume that Assumption 1 is satisfied. Then, for all  $p \geq 1$ ,  $0 \leq s < t \leq T$  such that  $t - s \leq 1$  and  $i \in \{1, \dots, N\}$ , the following holds true.*

- $\sup_{t \in [0, T]} \mathbb{E}[|X_t^i|^p] < c.$
- $\mathbb{E}[|X_t^i - X_s^i|^p] \leq c(t - s)^{\frac{p}{2}}.$
- $\mathbb{E}_s[|X_t^i - X_s^i|^p] \leq c(t - s)^{\frac{p}{2}} R_s(1).$

The following lemma will be useful in studying the asymptotic behavior of the elements that will come into play. Its proof is provided in Section 7.

**Lemma 7.** *Suppose that Assumption 1 is in hold. Let  $g : \mathbb{R} \rightarrow \mathbb{R}$  satisfy, for some  $c > 0$ ,  $k \in \mathbb{N}$ ,  $x, y \in \mathbb{R}$*

$$|g(x) - g(y)| \leq c|x - y|(1 + |x| + |y|)^k.$$

*Then, the following convergence in probability holds true*

$$\frac{\Delta_n}{N} \sum_{i=1}^N \sum_{j=1}^n g(X_{t_{j-1}}^i) \rightarrow \int_0^T \mathbb{E}[g(X_s)] ds.$$

In the main body of our paper, we will frequently rely on the fact that  $\varphi_{\tau_n}(f_j^{i,\ell,(k)})$  can be approximated as 1. To establish this, the following lemma will be of utmost importance. Its proof is deferred to Section 7.

**Lemma 8.** *Assume that Assumptions 1- 3 are in order. Recall that  $f(\theta; X_{t_{j-1}}^i, X_{t_j}^i)$  has been given in (5) and  $\tau_n$  has been chosen as  $\sqrt{\Delta_n} \log(n)$ . Then, for any  $r \geq 2$  and any  $k \geq 0$ , there exist constants  $c_1, c_2 > 0$  such that,*

$$\mathbb{P}_{t_{j-1}}(|f^{(k)}(\theta; X_{t_{j-1}}^i, X_{t_j}^i)| > \tau_n) \leq \frac{\Delta_n^{r/2}}{(\log(n))^r} R_{t_{j-1}}(1) + c_1 \exp\left(-c_2(\log(n))^2\right).$$

## 6 Proof of main results

### 6.1 Consistency

Let us start by providing the proof of the consistency as gathered in Theorem 1. This heavily relies on the fact that we can move from the contrast  $S_n^{N,\text{pub}}$  as defined in (11) to the contrast  $S_n^{N,0}(\theta)$  we would have had in absence of privacy constraints and the latter is given by

$$S_n^{N,0}(\theta) := \sum_{i=1}^N \sum_{j=1}^n f(\theta; X_{t_{j-1}}^i, X_{t_j}^i), \quad (28)$$

where we recall

$$f(\theta; X_{t_{j-1}}^i, X_{t_j}^i) = \frac{2b(\theta, X_{t_{j-1}}^i)(X_{t_j}^i - X_{t_{j-1}}^i) - \Delta_n b^2(\theta, X_{t_{j-1}}^i)}{\sigma^2(X_{t_{j-1}}^i)}. \quad (29)$$

Then, the following proposition provides a bound, for any  $u \in \{0, \dots, a\}$ , on the quantity

$$E_{n,N}^{(u)} := \sup_{\theta \in [\theta_0, \theta_{L_n-1}]} \left| \frac{\partial^u}{\partial \theta^u} (S_n^{N,\text{pub}}(\theta) - S_n^{N,0}(\theta)) \right|.$$

**Proposition 3.** *Assume that Assumptions 1- 3 are in order. Then, for any  $p \geq 2$  and for any  $u \in \{0, \dots, a\}$ ,*

$$\|E_{n,N}^{(u)}\|_p = O\left(N \left(\frac{1}{L_n}\right)^{a-u-1}\right) + O\left(L_n^{u+1} \sqrt{N} \log(n) \sqrt{\frac{\log(L_n)}{\bar{\alpha}^2}}\right) + O\left(\frac{L_n^u N}{n^r}\right),$$

where the constant  $r > 0$  can be chosen arbitrarily large, and where we recall that  $\bar{\alpha}^2$  is such that  $1/\bar{\alpha}^2 = n^{-1} \sum_{j=1}^n 1/\alpha_j^2$ .

*Proof.* Recall that, according to Section 3.1, the contrast function  $S_n^{N,\text{pub}}$  is defined by

$$S_n^{N,\text{pub}}(\theta) = \sum_{i=1}^n \sum_{j=1}^N H((Z_j^{i,(k)}(\theta_\ell))_{\ell,k})(\theta),$$

where  $H$  is the interpolation operator (10), fully described in Section 5.1. The private contrast function

$$S_n^{N,0}(\theta) = \sum_{i=1}^n \sum_{j=1}^N f(\theta; X_{t_{j-1}}^i, X_{t_j}^i)$$

admits the spline projection

$$H S_n^{N,0}(\theta) = H\left(\sum_{i=1}^n \sum_{j=1}^N f(\cdot; X_{t_{j-1}}^i, X_{t_j}^i)\right)(\theta) = \sum_{i=1}^n \sum_{j=1}^N H((f_j^{i,\ell,(k)})_{\ell,k})(\theta),$$

where we recall  $f_j^{i,\ell,(k)}$  is as in (8).

The proof is now divided in two steps. In the first we evaluate the error committed by approximating  $S_n^{N,0}(\theta)$  with  $HS_n^{N,0}(\theta)$ , while in the second we move from  $HS_n^{N,0}(\theta)$  to  $S_n^{N,\text{pub}}(\theta)$ , the contrast we propose in presence of privacy constraints. More formally, the proposition is a consequence of (30) and (38) below.

**Step 1:**

In this part of the proof, we show that, for any  $u \in \{0, \dots, a\}$ ,

$$\mathbb{E} \left[ \sup_{\theta \in [\theta_0, \theta_{L_n-1}]} \left| \frac{\partial^u}{\partial \theta^u} (HS_n^{N,0}(\theta) - S_n^{N,0}(\theta)) \right|^p \right] \leq c \left( \frac{1}{L_n} \right)^{(a-u-1)p} N^p. \quad (30)$$

We apply Proposition 2 to the function  $HS_n^{N,0}$  with  $\Lambda = L_n - 1$ . Note that here and in the subsequent discussions, for the sake of simplicity in notation, we will replace  $L_n - 1$  with  $L_n$ , as they are asymptotically equivalent. It follows

$$\sup_{\theta} \left| \frac{\partial^u}{\partial \theta^u} (HS_n^{N,0}(\theta) - S_n^{N,0}(\theta)) \right| \leq c \left( \frac{1}{L_n} \right)^{a-u-1} \times \sup_{\theta} \left| \frac{\partial^{a+1}}{\partial \theta^{a+1}} S_n^{N,0}(\theta) \right|,$$

where the supremum on  $\theta$ , here and below, is on  $\theta \in [\theta_0, \theta_{L_n-1}]$ . Then,

$$\mathbb{E} \left[ \sup_{\theta} \left| \frac{\partial^u}{\partial \theta^u} (HS_n^{N,0}(\theta) - S_n^{N,0}(\theta)) \right|^p \right] \leq c \left( \frac{1}{L_n} \right)^{(a-u-1)p} \mathbb{E} \left[ \sup_{\theta} \left| \frac{\partial^{a+1}}{\partial \theta^{a+1}} S_n^{N,0}(\theta) \right|^p \right]. \quad (31)$$

We now aim to demonstrate that, for some constant  $c > 0$ ,

$$\mathbb{E} \left[ \sup_{\theta} \left| \frac{\partial^{a+1}}{\partial \theta^{a+1}} S_n^{N,0}(\theta) \right|^p \right] \leq cN^p. \quad (32)$$

Once established, it will yield the desired result for the approximation of  $S_n^{N,0}$  with its spline function, thereby concluding the proof of Step 1. To achieve this, we begin by analyzing  $\partial^{a+1} S_n^{N,0}(\theta) / \partial \theta^{a+1}$ . Using the definitions of  $S_n^{N,0}$  as given in (28) and the function  $f$  in (29), one obtains

$$\begin{aligned} \left| \frac{\partial^{a+1}}{\partial \theta^{a+1}} S_n^{N,0}(\theta) \right| &= \left| \sum_{i=1}^N \sum_{j=1}^n \frac{\partial^{a+1}}{\partial \theta^{a+1}} f(\theta; X_{t_j}^i, X_{t_{j-1}}^i) \right| \\ &\leq \left| \sum_{i=1}^N \sum_{j=1}^n \frac{\partial^{a+1}}{\partial \theta^{a+1}} \frac{2b(\theta, X_{t_{j-1}}^i)(X_{t_j}^i - X_{t_{j-1}}^i)}{\sigma^2(X_{t_{j-1}}^i)} \right| + \left| \sum_{i=1}^N \sum_{j=1}^n \frac{\partial^{a+1}}{\partial \theta^{a+1}} \frac{\Delta_n b^2(\theta, X_{t_{j-1}}^i)}{\sigma^2(X_{t_{j-1}}^i)} \right| \\ &=: \left| S_n^{N,(a+1,1)}(\theta) \right| + \left| S_n^{N,(a+1,2)}(\theta) \right|. \end{aligned}$$

From Assumption 2,  $\sigma^2$  is lower bounded by  $\sigma_{\min}^2$ . Moreover, Assumption 3 implies that  $\sup_{\theta, i, j} \left| \frac{\partial^{a+1}}{\partial \theta^{a+1}} b^2(\theta, X_{t_{j-1}}^i) \right|^p$  is bounded by some constant  $c$ . Then,

$$\begin{aligned} \sup_{\theta} \left| S_n^{N,(a+1,2)}(\theta) \right|^p &\leq c(\Delta_n n N)^p \sup_{\theta, i, j} \left| \frac{\partial^{a+1}}{\partial \theta^{a+1}} b^2(\theta, X_{t_{j-1}}^i) \right|^p \\ &\leq cN^p. \end{aligned} \quad (33)$$

Let us now move to the analysis of  $S_n^{N,(a+1,1)}(\theta)$ . We want to control  $\mathbb{E}[\sup_{\theta} |S_n^{N,(a+1,1)}(\theta)|^p]$  and so, in order to deal with the sup inside the expectation, we use a Kolmogorov-type argument. Observe we can write  $S_n^{N,(a+1,1)}$  in an integral way by introducing the function  $\psi_s(n) := \sup\{j \in \{0, \dots, n\} : t_j \leq s\}$ . Then,

$$S_n^{N,(a+1,1)}(\theta) = \sum_{i=1}^N \int_0^T \frac{\partial^{a+1}}{\partial \theta^{a+1}} \frac{b^2(\theta, X_{\psi_n(s)}^i)}{\sigma^2(X_{\psi_n(s)}^i)} dX_s^i. \quad (34)$$

Let us set  $g(\theta, \theta', x) = \frac{\partial^{a+1}}{\partial \theta^{a+1}} \left( \frac{2b}{\sigma^2} \right) (\theta, x) - \frac{\partial^{a+1}}{\partial \theta^{a+1}} \left( \frac{2b}{\sigma^2} \right) (\theta', x)$ . Thanks to Rosenthal inequality for centered i.i.d. variables (see Theorem 3 in [45]), it follows that, for all  $\theta, \theta' \in \Theta$ ,

$$\begin{aligned}
& \mathbb{E} \left[ \left| S_n^{N,(u,1)}(\theta) - S_n^{N,(u,1)}(\theta') - \left( \mathbb{E} \left[ S_n^{N,(u,1)}(\theta) - S_n^{N,(u,1)}(\theta') \right] \right) \right|^p \right] \\
&= \mathbb{E} \left[ \left| \sum_{i=1}^N \int_0^T g(\theta, \theta', X_{\psi_n(s)}^i) dX_s^i - \sum_{i=1}^N \mathbb{E} \left[ \int_0^T g(\theta, \theta', X_{\psi_n(s)}^i) dX_s^i \right] \right|^p \right] \\
&\leq \left( \sum_{i=1}^N \mathbb{E} \left[ \left| \int_0^T g(\theta, \theta', X_{\psi_n(s)}^i) dX_s^i - \mathbb{E} \left[ \int_0^T g(\theta, \theta', X_{\psi_n(s)}^i) dX_s^i \right] \right|^2 \right] \right)^{p/2} \\
&\quad + \sum_{i=1}^N \mathbb{E} \left[ \left| \int_0^T g(\theta, \theta', X_{\psi_n(s)}^i) dX_s^i - \mathbb{E} \left[ \int_0^T g(\theta, \theta', X_{\psi_n(s)}^i) dX_s^i \right] \right|^p \right] \\
&\leq cN^{p/2-1} \sum_{i=1}^N \mathbb{E} \left[ \left| \int_0^T g(\theta, \theta', X_{\psi_n(s)}^i) dX_s^i - \mathbb{E} \left[ \int_0^T g(\theta, \theta', X_{\psi_n(s)}^i) dX_s^i \right] \right|^2 \right]^{p/2} \\
&\quad + \sum_{i=1}^N \mathbb{E} \left[ \left| \int_0^T g(\theta, \theta', X_{\psi_n(s)}^i) dX_s^i - \mathbb{E} \left[ \int_0^T g(\theta, \theta', X_{\psi_n(s)}^i) dX_s^i \right] \right|^p \right],
\end{aligned}$$

having used Jensen's inequality on the first sum, as  $p \geq 2$ . Then, it is upper bounded by

$$\begin{aligned}
& c(N^{p/2-1} + 1) \sum_{i=1}^N \mathbb{E} \left[ \left| \int_0^T g(\theta, \theta', X_{\psi_n(s)}^i) dX_s^i - \mathbb{E} \left[ \int_0^T g(\theta, \theta', X_{\psi_n(s)}^i) dX_s^i \right] \right|^p \right] \\
&\leq c(N^{p/2-1} + 1) \sum_{i=1}^N \mathbb{E} \left[ \left| \int_0^T g(\theta, \theta', X_{\psi_n(s)}^i) dX_s^i \right|^p \right], \tag{35}
\end{aligned}$$

where we used again Jensen inequality in the two last lines, with  $p > 1$ . Observe that, by the dynamics of  $X_s^i$ , we have

$$\begin{aligned}
\mathbb{E} \left[ \left| \int_0^T \left( g(\theta, \theta', X_{\psi_n(s)}^i) \right) dX_s^i \right|^p \right] &\leq c \mathbb{E} \left[ \left| \int_0^T \left( g(\theta, \theta', X_{\psi_n(s)}^i) \right) b(X_s^i, \theta^*) ds \right|^p \right] \\
&\quad + c \mathbb{E} \left[ \left| \int_0^T \left( g(\theta, \theta', X_{\psi_n(s)}^i) \right) \sigma(X_s^i) dW_s^i \right|^p \right] \\
&\leq cT^{p-1} \int_0^T \mathbb{E} [ |g(\theta, \theta', X_{\psi_n(s)}^i)|^p ] ds \\
&\quad + cT^{\frac{p}{2}-1} \int_0^T \mathbb{E} [ |g(\theta, \theta', X_{\psi_n(s)}^i)|^p |\sigma(X_s^i)|^p ] ds, \tag{36}
\end{aligned}$$

where we have used Burkholder-Davis-Gundy and Jensen inequalities as well as the boundedness of the drift. Remark now that

$$\begin{aligned}
|g(\theta, \theta', X_{\psi_n(s)}^i)|^p &= \left| \frac{\partial^{a+1}}{\partial \theta^{a+1}} \left( \frac{2b}{\sigma^2} \right) (\theta, X_{\psi_n(s)}^i) - \frac{\partial^{a+1}}{\partial \theta^{a+1}} \left( \frac{2b}{\sigma^2} \right) (\theta', X_{\psi_n(s)}^i) \right|^p \\
&= |\theta - \theta'|^p \left| \frac{\partial^{a+2}}{\partial \theta^{a+2}} \left( \frac{2b}{\sigma^2} \right) (\tau\theta + (1-\tau)\theta', X_{\psi_n(s)}^i) \right|^p
\end{aligned}$$

for some  $\tau \in [0, 1]$ . Replacing this in (36) and recalling that  $T$  is a fixed constant, it is easy to check that (36) is upper bounded by

$$\begin{aligned}
& c|\theta - \theta'|^p \int_0^T \left( \mathbb{E} [R_{\psi_n(s)}(1)] + \mathbb{E} [R_{\psi_n(s)}(1)R_s(1)] \right) ds \\
&\leq c|\theta - \theta'|^p,
\end{aligned}$$



where the last follows from the definition of function  $R_t$ , as in (27). Then, going back to (35), we obtain

$$\begin{aligned} \mathbb{E} \left[ \left| S_n^{N,(a+1,1)}(\theta) - S_n^{N,(a+1,1)}(\theta') - \left( \mathbb{E} \left[ S_n^{N,(a+1,1)}(\theta) - S_n^{N,(a+1,1)}(\theta') \right] \right) \right|^p \right] \\ \leq c|\theta - \theta'|^p (N^{\frac{p}{2}} + N) \leq c|\theta - \theta'|^p N^{\frac{p}{2}}, \end{aligned}$$

as  $p \geq 2$  and  $N > 1$ . Moreover, thanks to (34) it is

$$\left| \mathbb{E} \left[ S_n^{N,(u,1)}(\theta) - S_n^{N,(u,1)}(\theta') \right] \right| \leq c \sum_{i=1}^N \left| \mathbb{E} \left[ \int_0^T (g(\theta, \theta', X_{\psi_n(s)}^i)) dX_s^i \right] \right| \leq cN|\theta - \theta'|,$$

the validity of the last inequality can be easily confirmed by closely following the reasoning presented above. It follows

$$\mathbb{E} \left[ \left| S_n^{N,(u,1)}(\theta) - S_n^{N,(u,1)}(\theta') \right|^p \right] \leq c|\theta - \theta'|^p N^p.$$

Let us introduce the continuity modulus  $\omega_h$  i.e.

$$\omega_h(f) = \sup_{|\theta - \theta'| \leq h} |f(\theta) - f(\theta')|.$$

We apply Kolmogorov's criterion as given by Theorem 2.1 in Chapter 1 in [43], to get for all  $|h| \leq 1$ ,

$$E[\omega_h(S_n^{N,(a+1,1)})] \leq ch^{1-\varepsilon}N,$$

where  $\varepsilon > 0$  is any fixed constant. Recall now that the interval  $[\theta_0, \theta_{L_n} - 1] \subset \Theta = [0, 1]$  has a radius smaller than 1,

$$\begin{aligned} \mathbb{E} \left[ \sup_{\theta} |S_n^{N,(a+1,1)}(\theta)|^p \right] &\leq c\mathbb{E} \left[ \sup_{\theta} |S_n^{N,(a+1,1)}(\theta) - S_n^{N,(a+1,1)}(\theta^*)|^p \right] + c\mathbb{E} \left[ |S_n^{N,(a+1,1)}(\theta^*)|^p \right] \\ &\leq c\omega_1(S_n^{N,(a+1,1)})^p + cN^p \leq cN^p, \end{aligned} \quad (37)$$

as we wanted. The bounds gathered in (33) and (37) yield (32) and therefore conclude the proof of Step 1, as (30) is then a consequence of (31).

## Step 2:

From now on, let us compare  $HS_n^{N,0}$  with  $S_n^{N,\text{pub}}$ , and we aim to show that for all  $u \in \{0, \dots, a\}$ ,

$$\left\| \sup_{\theta \in [\theta_0, \theta_{L_n} - 1]} \left| \frac{\partial^u}{\partial \theta^u} (HS_n^{N,0}(\theta) - S_n^{N,\text{pub}}(\theta)) \right| \right\|_p = O \left( L_n^{u+1} \sqrt{N} \log(n) \sqrt{\frac{\log(L_n)}{\bar{\alpha}^2}} \right) + O \left( \frac{L_n^u N}{n^r} \right). \quad (38)$$

From the definitions of  $HS_n^{N,0}$  and  $S_n^{N,\text{pub}}$  with the linearity of the operator  $H$ ,

$$\begin{aligned} HS_n^{N,0} - S_n^{N,\text{pub}} &= H \left( \left( \sum_{i=1}^N \sum_{j=1}^n f_j^{i,\ell,(k)} \right)_{k,\ell} \right) - H \left( \left( \sum_{i=1}^N \sum_{j=1}^n Z_j^{i,(k)}(\theta_\ell) \right)_{k,\ell} \right) \\ &= H \left( \left( \sum_{i=1}^N \sum_{j=1}^n \beta_j^{i,(k)}(\theta_\ell) \right)_{k,\ell} \right) - H \left( \left( \sum_{i=1}^N \sum_{j=1}^n \mathcal{E}_j^{i,\ell,(k)} \right)_{k,\ell} \right) =: H(\beta) - H(\mathcal{E}) \end{aligned} \quad (39)$$

where

$$\beta_j^{i,(k)}(\theta_\ell) = f_j^{i,\ell,(k)} [1 - \varphi_{\tau_n}(f_j^{i,\ell,(k)})],$$

and we used (7)–(8) and recall that  $\mathcal{E}_j^{i,\ell,(k)}$  are the Laplace random variables introduced in Section 3.1. Let

$$\Omega^n := \left\{ \omega \in \Omega : \varphi_{\tau_n}(f_j^{i,\ell,(k)})(\omega) = 1, \forall k \leq a, \forall i \in \{1, \dots, N\}, \forall j \in \{1, \dots, n\}, \forall \ell \in \{0, \dots, L_n - 1\} \right\}. \quad (40)$$

Note that on  $\Omega^n$  we have  $HS_n^{N,0} - S_n^{N,\text{pub}} = -H(\mathcal{E})$ , whereas on  $(\Omega^n)^c$ ,  $HS_n^{N,0} - S_n^{N,\text{pub}} = H(\beta) - H(\mathcal{E})$ . Then, our goal consists in finding a bound on

$$\begin{aligned} \left\| \sup_{\theta} \left| \frac{\partial^u}{\partial \theta^u} (HS_n^{N,0}(\theta) - S_n^{N,\text{pub}}(\theta)) \right| \right\|_p &= \left\| \sup_{\theta} \left| \frac{\partial^u}{\partial \theta^u} (HS_n^{N,0}(\theta) - S_n^{N,\text{pub}}(\theta)) \right| 1_{\Omega^n} \right\|_p \\ &\quad + \left\| \sup_{\theta} \left| \frac{\partial^u}{\partial \theta^u} (HS_n^{N,0}(\theta) - S_n^{N,\text{pub}}(\theta)) \right| 1_{(\Omega^n)^c} \right\|_p \\ &\leq \left\| \sup_{\theta} \left| \frac{\partial^u}{\partial \theta^u} H(\mathcal{E})(\theta) \right| \right\|_p + \left\| \sup_{\theta} \left| \frac{\partial^u}{\partial \theta^u} (H(\beta)(\theta) - H(\mathcal{E})(\theta)) \right| 1_{(\Omega^n)^c} \right\|_p. \end{aligned} \quad (41)$$

Let us start considering an upper bound on  $H(\beta)$ . Lemma 4 provides

$$\left\| \frac{\partial^u}{\partial \theta^u} H(\beta) \right\|_{\infty} = \left\| \frac{\partial^u}{\partial \theta^u} H \left( \left( \sum_{i=1}^N \sum_{j=1}^n \beta_j^{i,(k)}(\theta_{\ell}) \right)_{\ell,k} \right) \right\|_{\infty} \leq cL_n^u \sup_{\ell,k} \left| \sum_{i=1}^N \sum_{j=1}^n \beta_j^{i,(k)}(\theta_{\ell}) \right|. \quad (42)$$

Observe that, according to the definition of  $\beta_j^{i,(k)}$  and  $f_j^{i,\ell,(k)}$  it is

$$\begin{aligned} \sup_{\ell,k} \left| \sum_{i=1}^N \sum_{j=1}^n \beta_j^{i,(k)}(\theta_{\ell}) \right| &\leq \sum_{i=1}^N \sum_{j=1}^n 2 \sup_{\ell,k} |f^{(k)}(\theta_{\ell}, X_{t_{j-1}}^i, X_{t_j}^i)| \\ &\leq c \sum_{i=1}^N \sum_{j=1}^n \left[ |X_{t_j}^i - X_{t_{j-1}}^i| + \Delta_n \right], \end{aligned}$$

where we used the definition of  $f$  recalled in (29) and the fact that  $\sigma^2$  is lower bounded thanks to Assumption 2 and that the derivatives of  $b$  with respect of  $\theta$  are bounded because of Assumption 3. Then, second point of Lemma 6 ensures that

$$\begin{aligned} \left\| \sup_{\ell,k} \left| \sum_{i=1}^N \sum_{j=1}^n \beta_j^{i,(k)}(\theta_{\ell}) \right| \right\|_p &\leq c \sum_{i=1}^N \sum_{j=1}^n \| |X_{t_j}^i - X_{t_{j-1}}^i| + \Delta_n \|_p \\ &\leq c \sum_{i=1}^N \sum_{j=1}^n (\Delta_n^{1/2} + \Delta_n) \leq cN\sqrt{n}, \end{aligned} \quad (43)$$

having also used that  $n = T/\Delta_n$  and  $T$  is a fixed constant. From (42) and (43) follows

$$\mathbb{E} \left[ \sup_{\theta} \left| \frac{\partial^u}{\partial \theta^u} |H(\beta)(\theta)| \right|^p \right] \leq cL_n^{up} \mathbb{E} \left[ \sup_{\ell,k} \left| \sum_{i=1}^N \sum_{j=1}^n \beta_j^{i,(k)}(\theta_{\ell}) \right|^p \right] \leq cL_n^{up} N^p n^{p/2}, \quad (44)$$

that concludes the analysis of  $H(\beta)$ .

Let us now study  $H(\mathcal{E})$ . Lemma 4 with the definition of  $H(\mathcal{E})$  through (39) provides

$$\left\| \frac{\partial^u}{\partial \theta^u} H(\mathcal{E}) \right\|_{\infty} \leq cL_n^u \sup_{\ell,k} \left| \sum_{i=1}^N \sum_{j=1}^n \mathcal{E}_j^{i,\ell,(k)} \right|, \quad (45)$$

where we recall that  $\mathcal{E}_j^{i,\ell,(k)} \sim [2\tau_n L_n(a+1)/\alpha_j] \mathcal{L}(1)$  and  $\tau_n = \sqrt{\Delta_n} \log(n)$ . Let us now introduce  $\mathcal{E}_j^{\circ i,\ell,(k)}$ , i.i.d. random variables whose law is  $\mathcal{L}(1/\alpha_j)$ . It is

$$\mathcal{E}_j^{i,\ell,(k)} = 2\tau_n L_n(a+1) \mathcal{E}_j^{\circ i,\ell,(k)} = 2\sqrt{\Delta_n} \log(n) L_n(a+1) \mathcal{E}_j^{\circ i,\ell,(k)}, \quad (46)$$

where we have also replaced the definition of  $\tau_n = \sqrt{\Delta_n} \log(n) = \sqrt{T/n} \log(n)$ . Then, for any fixed  $k, \ell$  we have

$$\sum_{i=1}^N \sum_{j=1}^n \mathcal{E}_j^{i,\ell,(k)} = 2\sqrt{T}(a+1) \log(n) L_n \sqrt{N} \frac{1}{\sqrt{N}} \frac{1}{\sqrt{n}} \sum_{i=1}^N \sum_{j=1}^n \overset{\circ}{\mathcal{E}}_j^{i,\ell,(k)}. \quad (47)$$

Let us now state a control on the sum of Laplace random variables. Its proof can be found in Section 7.

**Lemma 9.** *Let  $U \in \mathbb{N}^*$  and let us introduce a collection of independent random variables  $\mathcal{U} = (\mathcal{U}_h)_{1 \leq h \leq U}$  such that for  $h \in \{1, \dots, U\}$ ,  $\mathcal{U}_h \sim \mathcal{L}(1/\gamma_h)$ . The harmonic mean of  $\gamma_1, \dots, \gamma_U$  is denoted by  $\bar{\gamma}^2$  and satisfies  $1/\bar{\gamma}^2 := U^{-1} \sum_{h=1}^U 1/\gamma_h^2$ , and we set  $S_U := \sum_{h=1}^U \mathcal{U}_h$ . Then,*

$$\mathbb{P}\left(\frac{|S_U|}{\sqrt{U}} \geq \lambda\right) \leq \begin{cases} 2e^{-\lambda^2 \bar{\gamma}^2/8} & \text{if } 0 \leq \lambda \leq 2\gamma_{\max} \sqrt{U}/\bar{\gamma}^2 \\ 2e^{-\gamma_{\max} \lambda \sqrt{U}/4} & \text{if } \lambda \geq 2\gamma_{\max} \sqrt{U}/\bar{\gamma}^2, \end{cases}$$

where we have also introduced  $\gamma_{\max} := \max_{h=1, \dots, U} \gamma_h$ .

We apply this lemma to (47). To this end, we define the sequence  $(\gamma_h)_{h=1, \dots, nN}$  such that for all  $h \in \{1, \dots, nN\}$  that writes  $h = j + kN$  with  $j \in \{1, \dots, n\}$  and  $k \in \{0, \dots, N-1\}$ , we have  $\gamma_h = \alpha_j$  and also set  $\mathcal{U}_h = \overset{\circ}{\mathcal{E}}_j^{i,\ell,(k)}$ . Then, for any fixed  $k \in \{0, \dots, a\}, \ell \in \{0, \dots, L_n-1\}$ , we have

$$\sum_{i=1}^N \sum_{j=1}^n \mathcal{E}_j^{i,\ell,(k)} = 2\sqrt{T}(a+1) \log(n) L_n \sqrt{N} \frac{1}{\sqrt{U}} \sum_{h=1}^U \mathcal{U}_h^{\ell,(k)},$$

where we have introduced  $U := Nn$ . Using the definition of the  $\gamma_h$ 's, we get

$$\frac{1}{\bar{\alpha}^2} = \frac{1}{n} \sum_{j=1}^n \frac{1}{\alpha_j^2} = \frac{1}{Nn} \sum_{i=1}^N \sum_{j=1}^n \frac{1}{\alpha_j^2} = \frac{1}{U} \sum_{h=1}^U \frac{1}{\gamma_h^2} = \frac{1}{\bar{\gamma}^2}.$$

Noting that we also have  $\alpha_{\max} = \gamma_{\max}$ , the application of Lemma 9 directly provides

$$\begin{aligned} \mathbb{P}\left(\frac{1}{\sqrt{Nn}} \sum_{i=1}^N \sum_{j=1}^n \overset{\circ}{\mathcal{E}}_j^{i,\ell,(k)} \geq \lambda\right) &= \mathbb{P}\left(\frac{1}{\sqrt{U}} \sum_{h=1}^U \mathcal{U}_h^{\ell,(k)} \geq \lambda\right) \\ &\leq \begin{cases} 2e^{-\lambda^2 \bar{\alpha}^2/8} & \text{if } 0 \leq \lambda \leq \frac{2\alpha_{\max} \sqrt{Nn}}{\bar{\alpha}^2} \\ 2e^{-\alpha_{\max} \lambda \sqrt{Nn}/4} & \text{if } \lambda \geq \frac{2\alpha_{\max} \sqrt{Nn}}{\bar{\alpha}^2}. \end{cases} \end{aligned} \quad (48)$$

Let us now introduce a threshold  $M_n$  that will be better specified later and satisfies  $\bar{\alpha} M_n \rightarrow \infty$ . Then,

$$\begin{aligned} &\mathbb{E}\left[\sup_{\ell,k} \left| \frac{1}{\sqrt{Nn}} \sum_{i=1}^N \sum_{j=1}^n \overset{\circ}{\mathcal{E}}_j^{i,\ell,(k)} \right|^p\right] \\ &= \mathbb{E}\left[\sup_{\ell,k} \left| \frac{1}{\sqrt{Nn}} \sum_{i=1}^N \sum_{j=1}^n \overset{\circ}{\mathcal{E}}_j^{i,\ell,(k)} \right|^p \mathbf{1}_{\left\{ \sup_{\ell,k} \left| \frac{1}{\sqrt{Nn}} \sum_{i=1}^N \sum_{j=1}^n \overset{\circ}{\mathcal{E}}_j^{i,\ell,(k)} \right| < M_n \right\}}\right] \\ &\quad + \mathbb{E}\left[\sup_{\ell,k} \left| \frac{1}{\sqrt{Nn}} \sum_{i=1}^N \sum_{j=1}^n \overset{\circ}{\mathcal{E}}_j^{i,\ell,(k)} \right|^p \mathbf{1}_{\left\{ \sup_{\ell,k} \left| \frac{1}{\sqrt{Nn}} \sum_{i=1}^N \sum_{j=1}^n \overset{\circ}{\mathcal{E}}_j^{i,\ell,(k)} \right| \geq M_n \right\}}\right] \\ &\leq M_n^p + \mathbb{E}\left[\sup_{\ell,k} \left| \frac{1}{\sup_{\ell,k} \sqrt{Nn}} \sum_{i=1}^N \sum_{j=1}^n \overset{\circ}{\mathcal{E}}_j^{i,\ell,(k)} \right|^p \mathbf{1}_{\left\{ \left| \frac{1}{\sqrt{Nn}} \sum_{i=1}^N \sum_{j=1}^n \overset{\circ}{\mathcal{E}}_j^{i,\ell,(k)} \right| \geq M_n \right\}}\right] \\ &\leq M_n^p + p \int_{M_n}^{\infty} \lambda^{p-1} \mathbb{P}\left(\sup_{\ell,k} \left| \frac{1}{\sqrt{Nn}} \sum_{i=1}^N \sum_{j=1}^n \overset{\circ}{\mathcal{E}}_j^{i,\ell,(k)} \right| \geq \lambda\right) d\lambda. \end{aligned}$$

We now use that

$$\mathbb{P}\left(\sup_{\ell \in \{0, \dots, L_n-1\}, k \in \{0, \dots, a\}} \left| \frac{1}{\sqrt{Nn}} \sum_{i=1}^N \sum_{j=1}^n \mathring{\mathcal{E}}_j^{i, \ell, (k)} \right| \geq \lambda\right) \leq \sum_{\ell=0}^{L_n-1} \sum_{k=0}^a \mathbb{P}\left(\left| \frac{1}{\sqrt{Nn}} \sum_{i=1}^N \sum_{j=1}^n \mathring{\mathcal{E}}_j^{i, \ell, (k)} \right| \geq \lambda\right).$$

From (48) follows

$$\begin{aligned} \mathbb{E}\left[\sup_{\ell, k} \left| \frac{1}{\sqrt{Nn}} \sum_{i=1}^N \sum_{j=1}^n \mathring{\mathcal{E}}_j^{i, \ell, (k)} \right|^p\right] &\leq M_n^p + \sum_{\ell=0}^{L_n-1} \sum_{k=0}^a \int_{M_n}^{\infty} p\lambda^{p-1} \mathbb{P}\left(\frac{1}{\sqrt{Nn}} \sum_{i=1}^N \sum_{j=1}^n \mathring{\mathcal{E}}_j^{i, \ell, (k)} \geq \lambda\right) d\lambda \\ &\leq M_n^p + pL_n(a+1) \int_{M_n}^{\frac{2\alpha_{\max}\sqrt{Nn}}{\bar{\alpha}^2}} 2\lambda^{p-1} e^{-\lambda^2 \bar{\alpha}^2/8} d\lambda \\ &\quad + pL_n(a+1) \int_{\frac{2\alpha_{\max}\sqrt{Nn}}{\bar{\alpha}^2}}^{\infty} 2\lambda^{p-1} e^{-(\lambda\alpha_{\max}\sqrt{Nn})/4} d\lambda, \end{aligned}$$

where the first integral is zero if  $M_n > \frac{2\alpha_{\max}\sqrt{Nn}}{\bar{\alpha}^2}$ . Now remark that this first integral is bounded by

$$\int_{M_n}^{\infty} 2\lambda^{p-1} e^{-\lambda^2 \bar{\alpha}^2/8} d\lambda = O(M_n^p e^{-M_n^2 \bar{\alpha}^2/8}).$$

Regarding the second integral, we apply the change of variable  $\lambda' := \lambda\alpha_{\max}\sqrt{Nn}$ , that provides it is equal to

$$(\alpha_{\max}\sqrt{Nn})^{-p} \int_{\frac{2\alpha_{\max}^2 Nn}{\bar{\alpha}^2}}^{\infty} 2(\lambda')^{p-1} e^{-\lambda'/4} d\lambda' = O\left((\alpha_{\max}\sqrt{Nn})^{-p} \left(\frac{\alpha_{\max}^2 Nn}{\bar{\alpha}^2}\right)^{p-1} e^{-\frac{\alpha_{\max}^2 Nn}{4\bar{\alpha}^2}}\right).$$

It yields

$$\mathbb{E}\left[\sup_{\ell, k} \left| \frac{1}{\sqrt{Nn}} \sum_{i=1}^N \sum_{j=1}^n \mathring{\mathcal{E}}_j^{i, \ell, (k)} \right|^p\right] \leq M_n^p + cL_n M_n^p e^{-\frac{M_n^2 \bar{\alpha}^2}{8}} + c \frac{L_n}{(\alpha_{\max}^2 Nn)^{p/2}} \left(\frac{\alpha_{\max} Nn}{\bar{\alpha}^2}\right)^{p-1} e^{-\frac{\alpha_{\max}^2 Nn}{4\bar{\alpha}^2}}.$$

Comparing the first two terms in the right hand side of the equation above leads us to the choice  $M_n^2 = \kappa \log(L_n)/\bar{\alpha}^2$ , for a constant  $\kappa$  arbitrarily large. It implies

$$\mathbb{E}\left[\sup_{\ell, k} \left| \frac{1}{\sqrt{Nn}} \sum_{i=1}^N \sum_{j=1}^n \mathring{\mathcal{E}}_j^{i, \ell, (k)} \right|^p\right] \leq c \left(\frac{\log(L_n)}{\bar{\alpha}^2}\right)^{\frac{p}{2}}, \quad (49)$$

as the the second and third terms are negligible compared to the first using  $L_n = o(n^r)$  for some  $r > 0$ . Combining (45) and (49) and recalling the definition (46) of the variables  $\mathring{\mathcal{E}}_j^{i, \ell, (k)}$ , we deduce

$$\mathbb{E}\left[\sup_{\theta} \left| \frac{\partial^u}{\partial \theta^u} |H(\mathcal{E})(\theta)| \right|^p\right] \leq cL_n^{up} (\sqrt{N} \log(n) L_n)^p \left(\frac{\log(L_n)}{\bar{\alpha}^2}\right)^{\frac{p}{2}}. \quad (50)$$

Replacing (44) and (50) in (41) we obtain

$$\begin{aligned} &\left\| \sup_{\theta} \left| \frac{\partial^u}{\partial \theta^u} (HS_n^{N,0}(\theta) - S_n^{N,\text{pub}}(\theta)) \right| \right\|_p \\ &\leq cL_n^{u+1} \sqrt{N} \log(n) \sqrt{\frac{\log(L_n)}{\bar{\alpha}^2}} + cn^{-r_0/2} \left[ L_n^{u+1} \sqrt{N} \log(n) \sqrt{\frac{\log(L_n)}{\bar{\alpha}^2}} + L_n^u n^{\frac{1}{2}} N \right], \end{aligned} \quad (51)$$

having used Cauchy-Schwarz inequality and the fact that

$$\mathbb{P}(\Omega_n^c) \leq cn^{-r_0} \quad (52)$$

for any  $r_0 \geq 2$ . Indeed, thanks to Lemma 8,

$$\begin{aligned}\mathbb{P}(\Omega_n^c) &= \mathbb{P}(\exists \bar{k}, \bar{i}, \bar{\ell}, \bar{j} : |f_{\bar{j}}^{\bar{i}, \bar{\ell}, (\bar{k})}| > \tau_n) \\ &= \mathbb{E} \left[ \mathbb{E}_{t_{\bar{j}-1}} \left[ \mathbf{1}_{|f_{\bar{j}}^{\bar{i}, \bar{\ell}, (\bar{k})}| > \tau_n} \right] \right] \\ &\leq c \mathbb{E} \left[ \frac{\Delta_n^{\frac{r_0}{2}}}{(\log(n))} R_{t_{\bar{j}-1}}(1) + \exp(-c(\log(n))^2) \right],\end{aligned}$$

that goes to zero at a rate given by any arbitrarily large exponent of  $1/n$ , recalling that  $\Delta_n = T/n$ , with fixed  $T$ .

It concludes the proof of Step 2, as (38) is an immediate consequence of (51). The proposition is therefore proven.  $\square$

We are now ready to prove the consistency of the proposed estimator based on its analogous result in the privacy-free context and on the approximation argument presented in Proposition 3.

*Proof of Theorem 1.* In order to show the consistency we will prove that

$$\frac{1}{N}(S_n^{N,\text{pub}}(\theta) - S_n^{N,\text{pub}}(\theta^*)) \xrightarrow{\mathbb{P}} - \int_0^T \mathbb{E} \left[ \frac{(b(\theta, X_s) - b(\theta^*, X_s))^2}{a^2(X_s)} \right] ds =: C_\infty(\theta) \quad (53)$$

uniformly in  $\theta \in [\theta_0, \theta_{L_n-1}] = [0, 1 - 1/L_n]$ . Let us stress that, as  $\theta^* \in (0, 1)$ , we have  $\theta^* \in [0, 1 - 1/L_n]$  for  $n$  large enough.

Observe that one can write

$$\begin{aligned}\frac{1}{N}(S_n^{N,\text{pub}}(\theta) - S_n^{N,\text{pub}}(\theta^*)) &= \frac{1}{N}(S_n^{N,\text{pub}}(\theta) - S_n^{N,0}(\theta)) - \frac{1}{N}(S_n^{N,\text{pub}}(\theta^*) - S_n^{N,0}(\theta^*)) \\ &\quad + \frac{1}{N}(S_n^{N,0}(\theta) - S_n^{N,0}(\theta^*)).\end{aligned}$$

Proposition 3 with  $u = 0$  ensures that the  $L^p$  norm of the first two terms here above is upper bounded, uniformly in  $\theta$ , by  $c(\frac{1}{L_n})^{a-1} + c\frac{L_n \log(n)}{\sqrt{N}} \sqrt{\frac{\log(L_n)}{\alpha^2}} + c\frac{N}{n^{r_0}}$ , for any fixed  $r_0 > 0$ . This term goes to 0 under our hypothesis. It follows they converge to 0 in probability as well. Then, it is enough to prove

$$\frac{1}{N}(S_n^{N,0}(\theta) - S_n^{N,0}(\theta^*)) \xrightarrow{\mathbb{P}} C_\infty(\theta) \quad (54)$$

uniformly in  $\theta$  to obtain (53). The derivation of (54) closely mirrors the argumentation found in Steps 3 and 4 of Lemma 6.1 in [4]. It is worth noting that our contrast function  $S_n^{N,0}$  differs slightly from  $S_n^N$  in [4]. In that paper, indeed, the authors aim to jointly estimate both the drift and the diffusion coefficient in a parametric manner, whereas our focus here is solely on estimating the drift. However, similarly as in Step 3 of Lemma 6.1 in [4], and using (28)–(29), the following decomposition holds:

$$\frac{1}{N}(S_n^{N,0}(\theta) - S_n^{N,0}(\theta^*)) = I_n^N(\theta) + 2\rho_n^N(\theta),$$

where

$$\begin{aligned}I_n^N(\theta) &= -\frac{\Delta_n}{N} \sum_{i=1}^N \sum_{j=1}^n \frac{(b(\theta, X_{t_j}^i) - b(\theta^*, X_{t_j}^i))^2}{\sigma^2(X_{t_j}^i)}, \\ \rho_n^N(\theta) &= \frac{1}{N} \sum_{i=1}^N \sum_{j=1}^n (X_{t_j}^i - X_{t_{j-1}}^i - \Delta_n b(\theta^*, X_{t_{j-1}}^i)) \frac{b(\theta, X_{t_j}^i) - b(\theta^*, X_{t_{j-1}}^i)}{\sigma^2(X_{t_{j-1}}^i)}.\end{aligned}$$

Then,  $I_n^N(\theta) \xrightarrow{\mathbb{P}} C_\infty(\theta)$  because of Lemma 7 while  $\rho_n^N(\theta) \xrightarrow{\mathbb{P}} 0$  uniformly in  $\theta$  as in the proof of Lemma 6.1 in [4]. Moreover, Step 4 of Lemma 6.1 in [4] ensures the tightness of the two sequences  $\theta \mapsto I_n^N(\theta)$  and  $\theta \mapsto \rho_n^N(\theta)$ , which concludes the proof of (53) and implies in particular that

$$\sup_{\theta \in [\theta_0, \theta_{L_n-1}]} \left| \frac{1}{N} (S_n^{N,\text{pub}}(\theta) - S_n^{N,\text{pub}}(\theta^*)) - C_\infty(\theta) \right| \xrightarrow{\mathbb{P}} 0. \quad (55)$$

Such equation implies the consistency of  $\hat{\theta}_n^N$ . Indeed, the identifiability condition stated in Assumption 4 implies that, for every  $\epsilon > 0$ , there exists  $\eta > 0$  such that  $C_\infty(\theta) < -\eta$  for every  $\theta$  such that  $|\theta - \theta^*| \geq \epsilon$ . Then,

$$\{|\hat{\theta}_n^N - \theta^*| \geq \epsilon\} \subset \{C_\infty(\hat{\theta}_n^N) < -\eta\}.$$

Observe that we can write

$$C_\infty(\hat{\theta}_n^N) = \left( C_\infty(\hat{\theta}_n^N) - \frac{1}{N} (S_n^{N,\text{pub}}(\hat{\theta}_n^N) - S_n^{N,\text{pub}}(\theta^*)) \right) + \frac{1}{N} (S_n^{N,\text{pub}}(\hat{\theta}_n^N) - S_n^{N,\text{pub}}(\theta^*)).$$

Now, the first converges to 0 in probability because of (55), while the second is non-negative because of the definition of  $\hat{\theta}_n^N$ . We derive that the probability of the event  $\{C_\infty(\hat{\theta}_n^N) < -\eta\}$  converges to 0, which concludes the proof of the consistency.  $\square$

## 6.2 Asymptotic normality

In this section, we establish the asymptotic normality of the proposed estimator. The proof follows a classical path, relying on the asymptotic behavior of  $\partial_\theta S_n^{N,\text{pub}}(\theta)$  and  $\partial_\theta^2 S_n^{N,\text{pub}}(\theta)$  (refer, for instance, to [26], Section 5a).

Particularly noteworthy is the observation that the behavior of the first derivative of the contrast function varies depending on whether the contribution of privacy is negligible in our estimation procedure (see Propositions 4 and 5 below). Conversely, the behavior of the second derivative remains consistent, irrespective of the privacy's contribution, as elucidated in Proposition 6 below. The proofs of Propositions 4, 5, and 6 can be found in the subsequent subsections.

### Proposition 4. [Negligible contribution of privacy]

Assume that A1- A3, A6.1 and A7.1 hold. Assume moreover that  $\sqrt{\log(L_n)} r_{n,N} \rightarrow 0$  for  $N, n, L_n \rightarrow \infty$ . Then,

$$\frac{1}{\sqrt{N}} \partial_\theta S_n^{N,\text{pub}}(\theta^*) \xrightarrow{\mathcal{L}} \mathcal{N}\left(0, 2 \int_0^T \mathbb{E} \left[ \left( \frac{\partial_\theta b(\theta^*, X_s)}{\sigma(X_s)} \right)^2 \right] ds \right) =: \mathcal{N}(0, 2\Sigma_0).$$

When the contribution of the privacy is significant, instead, the following proposition is in hold.

### Proposition 5. [Significant contribution of privacy]

Assume that A1- A3, A6.2, A7.2 and A8 hold. Assume moreover that  $r_{n,N} \rightarrow \infty$  for  $N, n, L_n \rightarrow \infty$ . Define

$$N_{n,N} := \frac{\sqrt{\bar{\alpha}^2}}{\sqrt{N} L_n^2 \log(n)} \frac{1}{4(a+1)\sqrt{T} \sqrt{v_n(\theta^*)}} \frac{\partial}{\partial \theta} S_n^{N,\text{pub}}(\theta^*).$$

Then, we have

$$(N_{n,N}, v_n(\theta^*)) \xrightarrow{\mathcal{L}} (\mathcal{N}, \hat{v}(S)),$$

where  $\mathcal{N}$  is a Gaussian  $\mathcal{N}(0, 1)$  variable independent of  $S$ . We recall that  $\bar{\alpha}^2$  is such that  $1/\bar{\alpha}^2 = n^{-1} \sum_{j=1}^n 1/\alpha_j^2$ ,  $v_n(\theta^*)$  and  $\hat{v}$  have respectively been introduced in (15) and (14).

One can remark that the definition of the estimator guarantees that  $\partial_\theta S_n^{N,\text{pub}}(\hat{\theta}_n^N) = 0$ . Thanks to Taylor's formula, it implies

$$(\hat{\theta}_n^N - \theta^\star) \int_0^1 \partial_\theta^2 S_n^{N,\text{pub}}(\theta^\star + s(\hat{\theta}_n^N - \theta^\star)) ds = -\partial_\theta S_n^{N,\text{pub}}(\theta^\star). \quad (56)$$

The asymptotic behaviour of the second derivative of  $S_n^{N,\text{pub}}$  is gathered in the following proposition.

**Proposition 6.** *Suppose that Assumptions A1- A4 are in hold. Assume moreover that  $a > 3$  and  $L_n^3 \log(n) \sqrt{\frac{\log(L_n)}{N\bar{\alpha}^2}} \rightarrow 0$ . Then, for any  $N, n \rightarrow \infty$  we have*

1.  $\frac{\partial_\theta^2 S_n^{N,\text{pub}}(\theta^\star)}{N} \xrightarrow{\mathbb{P}} \Sigma_0$ ,
2.  $\frac{1}{N} \sup_{s \leq 1} |\partial_\theta^2 S_n^{N,\text{pub}}(\theta^\star + s(\hat{\theta}_n^N - \theta^\star)) - \partial_\theta^2 S_n^{N,\text{pub}}(\theta^\star)| \xrightarrow{\mathbb{P}} 0$ .

From the propositions stated above we easily deduce the asymptotic normality as in Theorems 2 and 3.

*Proof of Theorem 2.* In the case of negligible privacy contribution it looks convenient to write (56) as

$$(\hat{\theta}_n^N - \theta^\star) = -\frac{\sqrt{\frac{1}{N}} \partial_\theta S_n^{N,\text{pub}}(\theta^\star)}{\frac{1}{N} \int_0^1 \partial_\theta^2 S_n^{N,\text{pub}}(\theta^\star + s(\hat{\theta}_n^N - \theta^\star)) ds} \frac{1}{\sqrt{N}}.$$

Then, Propositions 4 and 6 yield

$$\sqrt{N}(\hat{\theta}_n^N - \theta^\star) \xrightarrow{\mathcal{L}} \mathcal{N}(0, 2(\Sigma_0)^{-1}),$$

as in the statement of Theorem 2. □

*Proof of Theorem 3.* In the case of significant privacy contribution we can write (56) as

$$(\hat{\theta}_n^N - \theta^\star) = -\frac{\sqrt{\frac{\bar{\alpha}^2}{N}} \frac{1}{L_n^2 \log(n) 4(a+1) \sqrt{T} \sqrt{v_n(\theta^\star)}} \partial_\theta S_n^{N,\text{pub}}(\theta^\star)}{\frac{1}{N} \int_0^1 \partial_\theta^2 S_n^{N,\text{pub}}(\theta^\star + s(\hat{\theta}_n^N - \theta^\star)) ds} \frac{1}{\sqrt{N\bar{\alpha}^2}} L_n^2 \log(n) 4(a+1) \sqrt{T} \sqrt{v_n(\theta^\star)}.$$

From here we can deduce, thanks to Propositions 5 and 6 and the continuous mapping theorem

$$\frac{\sqrt{N\bar{\alpha}^2}}{L_n^2 \log(n) 4(a+1) \sqrt{T} \sqrt{v_n(\theta^\star)}} (\hat{\theta}_n^N - \theta^\star) \xrightarrow{\mathcal{L}} \mathcal{N}(0, (\Sigma_0)^{-2})$$

jointly with the convergence  $v_n(\theta^\star) \xrightarrow{\mathcal{L}} \hat{v}(S)$ . It concludes the proof of Theorem 3. □

The proof of asymptotic normality is concluded by establishing the validity of the propositions stated above. We will begin with the case where privacy is negligible, as this will serve as a foundation for the more intricate proof of the significant privacy case.

### 6.2.1 Proof of Proposition 4

*Proof.* The proof of Proposition 4 heavily relies on the approximation gathered in Proposition 3. We have indeed

$$\frac{1}{\sqrt{N}} \partial_\theta S_n^{N,\text{pub}}(\theta^\star) = \frac{1}{\sqrt{N}} (\partial_\theta S_n^{N,\text{pub}}(\theta^\star) - \partial_\theta S_n^{N,0}(\theta^\star)) + \frac{1}{\sqrt{N}} \partial_\theta S_n^{N,0}(\theta^\star).$$

Proposition 3 ensures that

$$\left\| \frac{1}{\sqrt{N}} (\partial_\theta S_n^{N,\text{pub}}(\theta^*) - \partial_\theta S_n^{N,0}(\theta^*)) \right\|_p \leq c \frac{\sqrt{N}}{L_n^{a-2}} + c L_n^2 \log(n) \sqrt{\frac{\log(L_n)}{\bar{\alpha}^2}} + c \frac{L_n \sqrt{N}}{n^r},$$

where  $r > 0$  can be chosen arbitrarily large. It goes to zero under the hypothesis A6.1,  $r_{n,N} \sqrt{\log(L_n)} \rightarrow 0$  and the fact that both  $L_n$  and  $N$  go to  $\infty$  at a polynomial rate in  $n$ .

Then, Proposition 4 is proven once we show that  $\frac{1}{\sqrt{N}} \partial_\theta S_n^{N,0}(\theta^*) \xrightarrow{\mathcal{L}} \mathcal{N}(0, 2\Sigma_0)$ . One can easily check this is implied by Proposition 6.2 in [4]. Indeed, similarly as in [4], we can write  $\frac{1}{\sqrt{N}} \partial_\theta S_n^{N,0}(\theta) = \sum_{j=1}^n \xi_j^{(1)}(\theta)$ , with

$$\xi_j^{(1)}(\theta) := \frac{1}{\sqrt{N}} \sum_{i=1}^N \frac{2\partial_\theta b(\theta, X_{t_{j-1}}^i)}{\sigma^2(X_{t_{j-1}}^i)} (X_{t_j}^i - X_{t_{j-1}}^i - \Delta_n b(\theta, X_{t_{j-1}}^i)). \quad (57)$$

Remark that the main differences compared to  $\xi_{j,h}^{(1)}(\theta)$  in Proposition 6.2 in [4] is that in our case the diffusion coefficient  $\sigma$  does not depend on a second parameter  $\theta_2$  and the drift parameter is no longer in  $\mathbb{R}^{p_1}$ , but simply in  $\mathbb{R}$ . Moreover, the convergence gathered in (37) in Proposition 6.2 of [4] is now replaced by

$$\sum_{j=1}^n \mathbb{E}_{t_{j-1}} [(\xi_j^{(1)}(\theta^*))^2] \xrightarrow{\mathbb{P}} 4 \int_0^T \mathbb{E} \left[ \left( \frac{\partial_\theta b(\theta^*, X_s)}{\sigma(X_s)} \right)^2 \right] ds,$$

that can be obtained using Lemma 7 and  $N\Delta_n \rightarrow 0$  by Assumption A7.1. Then, (36) and (40) in Proposition 6.2 of [4] provide, for some  $\tilde{r} > 0$ ,

$$\sum_{j=1}^n \mathbb{E}_{t_{j-1}} [\xi_j^{(1)}(\theta^*)] \xrightarrow{\mathbb{P}} 0, \quad \sum_{j=1}^n \mathbb{E}_{t_{j-1}} [(\xi_j^{(1)}(\theta^*))^{2+\tilde{r}}] \xrightarrow{\mathbb{P}} 0.$$

The proof of Proposition 4 is therefore concluded by application of Theorem 3.2 in [27].  $\square$

## 6.2.2 Proof of Proposition 5

*Proof.* We start by observing that, as a consequence of Lemma 3, for any  $i \in \{1, \dots, N\}$  and  $j \in \{1, \dots, n\}$  it is

$$H(Z_j^i) = H \left( (f_j^{i,\ell,(k)} \varphi_{\tau_n}(f_j^{i,\ell,(k)}))_{\ell,k} \right) + H \left( (\mathcal{E}_j^{i,\ell,(k)})_{\ell,k} \right)$$

where, as a reminder,  $\mathcal{E}_j^{i,\ell,(k)}$  and  $f_j^{i,\ell,(k)}$  are defined as in (6) and (8). Then, from (11) one has

$$\begin{aligned} S_n^{N,\text{pub}}(\theta^*) &= \sum_{i=1}^N \sum_{j=1}^n H \left( (f_j^{i,\ell,(k)} \varphi_{\tau_n}(f_j^{i,\ell,(k)}))_{\ell,k} \right) (\theta^*) + \sum_{i=1}^N \sum_{j=1}^n H \left( (\mathcal{E}_j^{i,\ell,(k)})_{\ell,k} \right) (\theta^*) \\ &=: H(\gamma)(\theta^*) + H(\mathcal{E})(\theta^*), \end{aligned}$$

where  $\gamma = (\gamma^{\ell,(k)})_{\ell,k}$  and  $\mathcal{E} = (\mathcal{E}^{\ell,(k)})_{\ell,k}$  are given by

$$\gamma^{\ell,(k)} := \sum_{i=1}^N \sum_{j=1}^n f_j^{i,\ell,(k)} \varphi_{\tau_n}(f_j^{i,\ell,(k)}), \quad (58)$$

$$\mathcal{E}^{\ell,(k)} := \sum_{i=1}^N \sum_{j=1}^n \mathcal{E}_i^{j,\ell,(k)}. \quad (59)$$



We will see that the main contribution in  $\partial_\theta S_n^{N,\text{pub}}(\theta^*)$  comes from  $\partial_\theta H(\mathcal{E})(\theta^*)$ . By Proposition 1, the Hermite interpolation of the Laplace noise term is given by

$$H(\mathcal{E})(\theta) = \sum_{\ell=-1}^{L_n-2} \sum_{m=0}^a c_\ell^m(\mathcal{E}) B_\ell^m(\theta),$$

where the coefficients in the spline decomposition are given by

$$c_\ell^m(\mathcal{E}) = \sum_{\nu=0}^a (-1)^\nu (g_\ell^m)^{(2a+1-\nu)}(\theta_{\ell+1}) \mathcal{E}^{\ell+1,(\nu)}, \quad (60)$$

with the polynomial function  $g_\ell^m(\theta) = \frac{1}{(2a+1)!} (\theta - \theta_\ell)^{a-m} (\theta - \theta_{\ell+1})^{a+1} (\theta - \theta_{\ell+2})^m$ . The spline function  $B_j^m$  is supported on  $[\theta_j, \theta_{j+2}]$ , where we recall that we have set  $\theta_{-1} = \theta_0$  and  $\theta_{L_n} = \theta_{L_n-1}$ , by repeating the two endpoints.

As the spline expansion is constructed upon a high frequency grid, the dominating term in the expression of the coefficients (60) is the one corresponding to  $\nu = 0$ . Hence, we isolate such contribution. Remarking that the term corresponding to  $\nu = 0$  in the sum (60) is equal to  $\mathcal{E}^{\ell+1,(0)}$ , as  $(g_\ell^m)^{(2a+1)} \equiv 1$ , this leads us to split  $H(\mathcal{E})$  into the sum  $H(\mathcal{E}) = H^0(\mathcal{E}) + \bar{H}(\mathcal{E})$  where the two functions  $H^0(\mathcal{E})$  and  $\bar{H}(\mathcal{E})$  are defined by

$$H^0(\mathcal{E}) = \sum_{\ell=-1}^{L_n-2} \sum_{m=0}^a \mathcal{E}^{\ell+1,(0)} B_\ell^m$$

$$\bar{H}(\mathcal{E}) = \sum_{\ell=-1}^{L_n-2} \sum_{m=0}^a \bar{c}_\ell^m(\mathcal{E}) B_\ell^m,$$

where

$$\bar{c}_\ell^m(\mathcal{E}) = \sum_{\nu=1}^a (-1)^\nu (g_\ell^m)^{(2a+1-\nu)}(\theta_{\ell+1}) \mathcal{E}^{\ell+1,(\nu)}. \quad (61)$$

The proposition will be proved if we show

$$\left( \frac{\sqrt{\bar{\alpha}^2}}{\sqrt{N} L_n^2 \log(n)} \frac{1}{4(a+1)\sqrt{T}\sqrt{v_n(\theta^*)}} \frac{\partial}{\partial \theta} H^0(\mathcal{E})(\theta^*), v_n(\theta^*) \right) \xrightarrow{\mathcal{L}} (\mathcal{N}, \hat{v}(S)), \quad (62)$$

$$\frac{\sqrt{\bar{\alpha}^2}}{\sqrt{N} L_n^2 \log(n)} \frac{1}{\sqrt{v_n(\theta^*)}} \frac{\partial}{\partial \theta} \bar{H}(\mathcal{E})(\theta^*) \xrightarrow{\mathbb{P}} 0, \quad (63)$$

$$\frac{\sqrt{\bar{\alpha}^2}}{\sqrt{N} L_n^2 \log(n)} \frac{1}{\sqrt{v_n(\theta^*)}} \frac{\partial}{\partial \theta} H(\gamma)(\theta^*) \xrightarrow{\mathbb{P}} 0. \quad (64)$$

We now study the asymptotic behaviour of  $\frac{\partial}{\partial \theta} H^0(\mathcal{E})(\theta^*)$ . We recall that  $\ell_n^* \in \{0, \dots, L_n - 2\}$  denotes the value of the index such that  $\theta^* \in [\theta_{\ell_n^*}, \theta_{\ell_n^*+1})$ . Since  $\theta^* \in (0, 1)$ , it is possible to exclude the case  $\ell_n^* = 0$  or  $\ell_n^* = L_n - 2$  for  $n$  large enough. Using that the support of  $B_j^m$  is  $[\theta_j, \theta_{j+2}]$  we deduce, for  $\theta \in [\theta_{\ell_n^*}, \theta_{\ell_n^*+1})$ ,

$$H^0(\mathcal{E})(\theta) = \sum_{\ell \in \{\ell_n^*-1, \ell_n^*\}} \sum_{m=0}^a \mathcal{E}^{\ell+1,(0)} B_\ell^m(\theta). \quad (65)$$

We use the scaling properties of the spline functions, to represent  $B_\ell^m(\theta)$  for  $\ell \in \{1, \dots, L_n - 3\}$ , in the following way

$$B_\ell^m(\theta) = \bar{B}^m(L_n(\theta - \theta_\ell)), \quad (66)$$

where, for  $m \in \{0, \dots, a\}$ ,  $\bar{B}^m$  is the spline function of order  $2a + 1$  constructed on the knots  $0, 1, 2$  where the knot  $0$  is repeated  $a + 1 - m$  times, while the knot  $1$  is repeated  $a + 1$  times and

knot 2 is repeated  $m + 1$  times. The spline function  $\overline{B}^m$  is supported on  $[0, 2]$ . By differentiating (65) and using the representation (66), we deduce

$$\begin{aligned} \frac{\partial}{\partial \theta} H^0(\mathcal{E})(\theta^*) &= \sum_{\ell \in \{\ell_n^* - 1, \ell_n^*\}} \sum_{m=0}^a \mathcal{E}^{\ell+1, (0)} L_n \frac{\partial}{\partial \theta} (\overline{B}^m)(L_n(\theta^* - \theta_\ell)) \\ &= L_n \mathcal{E}^{\ell_n^*, (0)} \sum_{m=0}^a \frac{\partial}{\partial \theta} (\overline{B}^m)(L_n(\theta^* - \theta_{\ell_n^* - 1})) + L_n \mathcal{E}^{\ell_n^* + 1, (0)} \sum_{m=0}^a \frac{\partial}{\partial \theta} (\overline{B}^m)(L_n(\theta^* - \theta_{\ell_n^*})) \\ &= L_n \mathcal{E}^{\ell_n^*, (0)} g\left(L_n\left(\theta^* - \theta_{\ell_n^*} + \frac{1}{L_n}\right)\right) + L_n \mathcal{E}^{\ell_n^* + 1, (0)} g(L_n(\theta^* - \theta_{\ell_n^*})), \end{aligned}$$

where we have set  $g(u) = \sum_{m=0}^a \frac{\partial}{\partial u} \overline{B}^m(u)$  for  $u \in [0, 2]$  and used  $\theta_{\ell_n^* - 1} = \theta_{\ell_n^*} - 1/L_n$ . From Lemma 5, we know that  $g(u) = (2a + 1) \binom{2a}{a} \left[ u^a (1 - u)^a \mathbf{1}_{[0, 1]}(u) - (u - 1)^a (2 - u)^a \mathbf{1}_{[1, 2]}(u) \right]$ . From the definition of  $\widehat{v}$ , given in (14), we deduce that

$$\frac{\partial}{\partial \theta} H^0(\mathcal{E})(\theta^*) = L_n \widehat{v}(L_n(\theta^* - \theta_{\ell_n^*}))^{1/2} \times \left[ \mathcal{E}^{\ell_n^* + 1, (0)} - \mathcal{E}^{\ell_n^*, (0)} \right]. \quad (67)$$

Now we prove,

$$\forall \ell \in \{1, \dots, L_n - 3\}, \quad N_{n, N}^\ell := \frac{\sqrt{\alpha^2}}{\sqrt{N} L_n \log(n)} \frac{1}{4(a + 1) \sqrt{T}} \left[ \mathcal{E}^{\ell+1, (0)} - \mathcal{E}^{\ell, (0)} \right] \xrightarrow{\mathcal{L}} \mathcal{N}(0, 1). \quad (68)$$

We write

$$\mathcal{E}^{\ell+1, (0)} - \mathcal{E}^{\ell, (0)} = \sum_{j=1}^N \sum_{i=1}^n \left( \mathcal{E}_j^{i, \ell+1, (0)} - \mathcal{E}_j^{i, \ell, (0)} \right) = \frac{2\sqrt{T}(a + 1) \log(n) L_n}{\sqrt{n}} \sum_{j=1}^N \sum_{i=1}^n \left( \overset{\circ}{\mathcal{E}}_j^{i, \ell+1, (0)} - \overset{\circ}{\mathcal{E}}_j^{i, \ell, (0)} \right)$$

where we used (46) and  $\tau_n = \sqrt{\Delta_n} \log(n) = \frac{\sqrt{T}}{\sqrt{n}} \log(n)$ . It yields,

$$\frac{\sqrt{\alpha^2}}{\sqrt{N} L_n \log(n) 4(a + 1) \sqrt{T}} \left[ \mathcal{E}^{\ell+1, (0)} - \mathcal{E}^{\ell, (0)} \right] = \sum_{j=1}^N \sum_{i=1}^n \frac{\sqrt{\alpha^2}}{2\sqrt{Nn}} \left( \overset{\circ}{\mathcal{E}}_j^{i, \ell+1, (0)} - \overset{\circ}{\mathcal{E}}_j^{i, \ell, (0)} \right). \quad (69)$$

For each fixed value of  $\ell$ , the sequence  $\left( \overset{\circ}{\mathcal{E}}_j^{i, \ell+1, (0)} - \overset{\circ}{\mathcal{E}}_j^{i, \ell, (0)} \right)_{1 \leq i \leq N, 1 \leq j \leq n}$  is constituted of independent centered variables with variance depending on the index  $j$  and equal to  $4/\alpha_j^2$ . We deduce from  $\sum_{j=1}^n 1/\alpha_j^2 = n/\alpha^2$  that the R.H.S of (69) has a unit variance. We apply a Central Limit Theorem for triangular array, as Theorem 18.1 of [10], to deduce that the R.H.S. of (69) converges in law to a  $\mathcal{N}(0, 1)$ . To apply this Central Limit Theorem, it is necessary that the sequence satisfies a Lindeberg condition as given by equation (18.2) in [10]. Here, the Lindeberg condition follows from the fact that the variances of all terms in the sum (69) are comparable up to a constant, using  $1 \leq \frac{\sup_j \alpha_j}{\inf_j \alpha_j} = O(1)$ . Consequently, the convergence (68) is proved.

Recalling the definition of  $N_{n, N}^\ell$  in (68), the family of random variables  $(N_{n, N}^\ell)_{n \geq 1, 1 \leq \ell \leq L_n - 3}$  is such that for all fixed  $\ell$ , the convergence  $N_{n, N}^\ell \xrightarrow[n \rightarrow \infty]{\mathcal{L}} \mathcal{N}(0, 1)$  holds true. Remark also that from the expression of  $N_{n, N}^\ell$  as sum of independent Laplace variables, we see that the law of  $N_{n, N}^\ell$  does not depend upon the index  $\ell \in \{1, \dots, L_n - 3\}$ . The sequence of Laplace variables  $(\overset{\circ}{\mathcal{E}}_j^{i, \ell, (0)})_{i, \ell, j}$  is independent of the shift variable  $S$  and thus is also independent of the random index  $\ell_n^* = \lfloor L_n \theta^* - S \rfloor$ . It entails the independence of the random index  $\ell_n^*$  with the family  $(N_{n, N}^\ell)_{\ell, n, N}$ . From these descriptions, we deduce the equality in law

$$(N_{n, N}^{\ell_n^*}, S) \stackrel{\mathcal{L}}{=} (N_{n, N}^1, S).$$

Consequently, using the convergence in law of  $N_n^1$ , we deduce

$$(N_{n,N}^{\ell_n^*}, S) \xrightarrow{\mathcal{L}} (\mathcal{N}, S), \quad (70)$$

where  $\mathcal{N} \sim \mathcal{N}(0, 1)$  is a random variable independent of  $S$ . Comparing the expression (67) with the left hand side of (68), we have

$$\frac{\sqrt{\alpha^2}}{\sqrt{N}L_n^2 \log(n)} \frac{1}{4(a+1)\sqrt{T}\sqrt{v_n(\theta^*)}} \frac{\partial}{\partial \theta} H^0(\mathcal{E})(\theta^*) = N_{n,N}^{\ell_n^*}.$$

Since  $v_n(\theta^*) = \hat{v}(L_n(\theta^* - \theta_{\ell_n^*}))$  is measurable with respect to the random variable  $S$ , and with law  $\hat{v}(S)$  by Lemma 2, we deduce from (70) that the convergence (62) holds true.

Now, we prove (63). We write

$$\begin{aligned} \frac{\partial}{\partial \theta} \bar{H}(\mathcal{E})(\theta^*) &= \sum_{\ell=-1}^{L_n-1} \sum_{m=0}^a \bar{c}_\ell^m(\mathcal{E}) \frac{\partial}{\partial \theta} B_\ell^m(\theta^*) \\ &= \sum_{\ell \in \{\ell_n^*-1, \ell_n^*\}} \sum_{m=0}^a \bar{c}_\ell^m(\mathcal{E}) \frac{\partial}{\partial \theta} B_\ell^m(\theta^*), \end{aligned}$$

where we used that the support of  $B_j^m$  is  $[\theta_j, \theta_{j+2})$  and  $\theta^* \in [\theta_{\ell_n^*}, \theta_{\ell_n^*+1})$ . For  $n$  large enough we have  $\ell_n^* \in \{1, \dots, L_n - 3\}$ , and thus using (66), we deduce  $\left\| \frac{\partial}{\partial \theta} B_\ell^m \right\|_\infty \leq cL_n$  for some constant  $c$  and  $\ell \in \{\ell_n^* - 1, \ell_n^*\}$ . It yields,

$$\left| \frac{\partial}{\partial \theta} \bar{H}(\mathcal{E})(\theta^*) \right| \leq cL_n(a+1) \sup_{\ell \in \{\ell_n^*-1, \ell_n^*\}} \sup_{m \in \{0, \dots, a\}} |\bar{c}_\ell^m(\mathcal{E})|.$$

For  $\nu \geq 1$ , we have  $|(g_\ell^m)^{(2a+1-\nu)}(\theta_{\ell+1})| \leq c/L_n$ , and recalling (61), it implies  $|\bar{c}_\ell^m(\mathcal{E})| \leq c(L_n)^{-1} \sup_{\nu \in \{1, \dots, a\}} |\mathcal{E}^{\ell+1, (\nu)}|$  for all  $\ell \in \{-1, \dots, L_n - 2\}$  and  $m \in \{0, \dots, a\}$ . We deduce,

$$\begin{aligned} \left| \frac{\partial}{\partial \theta} \bar{H}(\mathcal{E})(\theta^*) \right| &\leq c \sup_{\ell \in \{\ell_n^*-1, \ell_n^*\}} \sup_{\nu \in \{1, \dots, a\}} |\mathcal{E}^{\ell+1, (\nu)}| \\ &\leq c \sup_{\ell \in \{0, \dots, L_n-1\}} \sup_{\nu \in \{1, \dots, a\}} \left| \sum_{i=1}^N \sum_{j=1}^n \mathcal{E}_j^{i, \ell, (\nu)} \right|, \end{aligned}$$

where in the last line we used the definition (59) of  $\mathcal{E}^{\ell+1, (\nu)}$ . From this, we derive an upper bound for the  $L^2$  norm of  $|\frac{\partial}{\partial \theta} \bar{H}(\mathcal{E})(\theta^*)|$ :

$$\begin{aligned} \mathbb{E} \left[ \left| \frac{\partial}{\partial \theta} \bar{H}(\mathcal{E})(\theta^*) \right|^2 \right] &\leq \mathbb{E} \left[ \sup_{\ell \in \{0, \dots, L_n-1\}} \sup_{\nu \in \{1, \dots, a\}} \left| \sum_{i=1}^N \sum_{j=1}^n \mathcal{E}_j^{i, \ell, (\nu)} \right|^2 \right] \\ &\leq c \log(n)^2 N L_n^2 \mathbb{E} \left[ \sup_{\ell \in \{0, \dots, L_n-1\}} \sup_{\nu \in \{1, \dots, a\}} \left| \frac{1}{\sqrt{nN}} \sum_{i=1}^N \sum_{j=1}^n \mathcal{E}_j^{i, \ell, (\nu)} \right|^2 \right], \end{aligned}$$

where we used (47). Then, (49) with  $p = 2$ , gives,

$$\mathbb{E} \left[ \left| \frac{\partial}{\partial \theta} \bar{H}(\mathcal{E})(\theta^*) \right|^2 \right] \leq c \log(n)^2 N L_n^2 \frac{\log(L_n)}{\alpha^2}.$$

We deduce from  $1/L_n \rightarrow 0$ , that  $\frac{\sqrt{\alpha^2}}{\sqrt{N}L_n^2 \log(n)} \frac{\partial}{\partial \theta} \bar{H}(\mathcal{E})(\theta^*)$  converges to zero in  $L^2$ -norm and thus in probability. Since, using Lemma 2, the law of  $v_n(\theta^*)$  does not depend on  $n$  and

$\mathbb{P}(v_n(\theta^*) > 0) = 1$ , we obtain (63).

Last step is devoted to the proof of (64). Applying Lemma 4, and recalling (58) we have

$$\begin{aligned} \left| \frac{\partial}{\partial \theta} H(\gamma)(\theta^*) \right| &\leq cL_n \sup_{\ell, k} \left| \sum_{i=1}^N \sum_{j=1}^n f_j^{i, \ell, (k)} \varphi_{\tau_n}(f_j^{i, \ell, (k)}) \right| \\ &\leq cL_n n N \sup_{i, j, \ell, k} |f_j^{i, \ell, (k)} \varphi_{\tau_n}(f_j^{i, \ell, (k)})| \\ &\leq cL_n n N \tau_n \leq cL_n \sqrt{n} \log(n) N, \end{aligned}$$

where we have used  $\tau_n = \sqrt{\Delta_n} \log(n) \leq cn^{-1/2} \log(n)$ . Recall we have introduced the set  $\Omega^n$  in (40), in the proof of Proposition 3. The bound above implies

$$\mathbb{E} \left[ \left| \frac{\partial}{\partial \theta} H(\gamma)(\theta^*) \right| \mathbf{1}_{(\Omega^n)^c} \right] \leq cL_n \sqrt{n} \log(n) N \mathbb{P}((\Omega^n)^c) \leq cL_n \sqrt{n} \log(n) N n^{-r_0},$$

for any  $r_0$  arbitrarily large, recalling (52). It entails,

$$\frac{\sqrt{\bar{\alpha}^2}}{\sqrt{N} L_n^2 \log(n)} \left| \frac{\partial}{\partial \theta} H(\gamma)(\theta^*) \right| \mathbf{1}_{(\Omega^n)^c} \xrightarrow{L^1} 0, \quad (71)$$

using that both  $L_n$  and  $N$  are polynomial in  $n$ , together with the fact that  $r_0$  can be as large as needed.

On the set  $\Omega^n$  we have for  $k \in \{0, \dots, a\}$  and  $\ell \in \{0, \dots, L_n - 1\}$ ,

$$\gamma^{\ell, (k)} = \sum_{i=1}^N \sum_{j=1}^n f_j^{i, \ell, (k)} \varphi_{\tau_n}(f_j^{i, \ell, (k)}) = \sum_{i=1}^N \sum_{j=1}^n f_j^{i, \ell, (k)} = \frac{\partial^k}{\partial \theta^k} S_n^{N, 0}(\theta_\ell)$$

by (8) and (28). Thus, on  $\Omega^n$ , we have  $H(\gamma) = HS_n^{N, 0}$  and we can write

$$\begin{aligned} \frac{\partial}{\partial \theta} H(\gamma)(\theta^*) &= \frac{\partial}{\partial \theta} HS_n^{N, 0}(\theta^*) = \frac{\partial}{\partial \theta} (HS_n^{N, 0} - S_n^{N, 0})(\theta^*) + \frac{\partial}{\partial \theta} S_n^{N, 0}(\theta^*) \\ &= I_1(\theta^*) + I_2(\theta^*). \end{aligned}$$

From (30) with  $u = p = 1$ , we get  $\mathbb{E}[|I_1(\theta^*)| \mathbf{1}_{\Omega^n}] \leq \mathbb{E}[|I_1(\theta^*)|] \leq L_n^{2-a} N$ . We deduce from A6.2

$$\frac{\sqrt{\bar{\alpha}^2}}{\sqrt{N} L_n^2 \log(n)} I_1(\theta^*) \rightarrow 0 \quad (72)$$

in  $L^1$  and thus in probability.

To conclude, let us analyze  $I_2(\theta^*)$ . Using the notation (57) introduced in the proof of Proposition 4, we have

$$\sqrt{\bar{\alpha}^2} \frac{1}{L_n^2 \log(n)} \frac{1}{\sqrt{N}} \frac{\partial}{\partial \theta} S_n^{N, 0}(\theta^*) = \sqrt{\bar{\alpha}^2} \frac{1}{L_n^2 \log(n)} \sum_{j=1}^n \xi_j^{(1)}(\theta^*) =: \sum_{j=1}^n \tilde{\xi}_j(\theta^*).$$

Then,

$$\sum_{j=1}^n |\mathbb{E}_{t_{j-1}}[\tilde{\xi}_j(\theta^*)]| = \sqrt{\bar{\alpha}^2} \frac{1}{L_n^2 \log(n)} \sum_{j=1}^n |\mathbb{E}_{t_{j-1}}[\xi_j^{(1)}(\theta^*)]| \xrightarrow{\mathbb{P}} 0,$$

where we used that, from the proof of (36) in Proposition 6.2 of [4], we have  $\mathbb{E}_{t_{j-1}}[\xi_j^{(1)}(\theta^*)] = R_{t_{j-1}}(\sqrt{N} \Delta_n^{3/2})$  and  $\sqrt{\bar{\alpha}^2} \frac{1}{L_n^2 \log(n)} \sqrt{N \Delta_n} \rightarrow 0$  from A7.2.

Moreover, let us consider

$$\sum_{j=1}^n \mathbb{E}_{t_{j-1}}[(\tilde{\xi}_j(\theta^*))^2] = \bar{\alpha}^2 \frac{1}{L_n^4 (\log(n))^2} \sum_{j=1}^n \mathbb{E}_{t_{j-1}}[(\xi_j^{(1)}(\theta^*))^2].$$

Following the proof of (37) in Proposition 6.2 of [4], we have

$$\begin{aligned}\mathbb{E}_{t_{j-1}}[(\xi_j^{(1)}(\theta^*))^2] &\leq \frac{1}{N} \sum_{i_1, i_2=1}^N (R_{t_{j-1}}(\Delta_n) \mathbf{1}_{i_1=i_2} + R_{t_{j-1}}(\Delta_n^2) \mathbf{1}_{i_1 \neq i_2}) \\ &\leq R_{t_{j-1}}(\Delta_n + N\Delta_n^2).\end{aligned}$$

Hence,  $\sum_{j=1}^n \mathbb{E}_{t_{j-1}}[(\tilde{\xi}_j(\theta^*))^2]$  converges to 0 in  $L^1$  as  $\bar{\alpha}^2 \frac{1}{L_n^2 \log(n)^2} (1 + N\Delta_n) \rightarrow 0$  because of  $r_{n,N} \rightarrow \infty$  and the hypothesis A7.2. Then, Lemma 9 in [26] guarantees that

$$\sqrt{\frac{\bar{\alpha}^2}{N L_n^2 \log(n)}} I_2(\theta^*) = \sum_{j=1}^n \tilde{\xi}_j(\theta^*) \xrightarrow{\mathbb{P}} 0. \quad (73)$$

From (71), (72) and (73), we obtain the convergence to zero of  $\frac{\sqrt{\bar{\alpha}^2}}{\sqrt{N L_n^2 \log(n)}} \frac{\partial}{\partial \theta} H(\gamma)(\theta^*)$ . It yields (64) remarking that, because of Lemma 2, the law of  $v_n(\theta^*)$  does not depend on  $n$  and  $\mathbb{P}(v_n(\theta^*) > 0) = 1$ . Then, the proof of the proposition is concluded.  $\square$

### 6.2.3 Proof of Corollary 1

*Proof.* Observe that the proof of Corollary 1 heavily relies on the results obtained until this point. Indeed, its proof follows the same route of Theorems 2 and 3 above. Nevertheless, in this instance, the terms associated with significant and negligible privacy each play a contributory role. We start by writing (56) as

$$(\hat{\theta}_n^N - \theta^*) = -\frac{\sqrt{\frac{\bar{\alpha}^2}{N L_n^2 \log(n)}} \frac{1}{\partial_\theta S_n^{N,\text{pub}}(\theta^*)} \partial_\theta S_n^{N,\text{pub}}(\theta^*)}{\frac{1}{N} \int_0^1 \partial_\theta^2 S_n^{N,\text{pub}}(\theta^* + s(\hat{\theta}_n^N - \theta^*)) ds} \frac{L_n^2 \log(n)}{\sqrt{\bar{\alpha}^2 N}}.$$

Following the proof of Proposition 5 above, one has

$$\sqrt{\frac{\bar{\alpha}^2}{N L_n^2 \log(n)}} \frac{1}{\partial_\theta} S_n^{N,\text{pub}}(\theta^*) = \sqrt{\frac{\bar{\alpha}^2}{N L_n^2 \log(n)}} \left[ \frac{\partial}{\partial \theta} H^0(\boldsymbol{\mathcal{E}})(\theta^*) + \frac{\partial}{\partial \theta} \bar{H}(\boldsymbol{\mathcal{E}})(\theta^*) + \frac{\partial}{\partial \theta} H(\gamma)(\theta^*) \right].$$

The main modification with the proof Proposition 5 is that, under the hypothesis of Corollary 1, the convergence result (64) does not hold. Indeed,  $\sqrt{\frac{\bar{\alpha}^2}{N L_n^2 \log(n)}} I_2(\theta^*)$  no longer converges to 0. Instead, as  $\sqrt{\bar{\alpha}^2} \frac{1}{L_n^2 \log(n)} \rightarrow c_p$  for  $n, N \rightarrow \infty$ , Proposition 6.2 of [4] directly provides

$$\sqrt{\frac{\bar{\alpha}^2}{N L_n^2 \log(n)}} I_2(\theta^*) \underset{n, N \rightarrow \infty}{\rightsquigarrow} \frac{c_p}{\sqrt{N}} I_2(\theta^*) \xrightarrow{\mathcal{L}} \mathcal{N}(0, 2c_p^2 \Sigma_0) = c_p \mathcal{Z}_1.$$

Let us remark that the condition  $N\Delta_n \rightarrow 0$  necessary to apply Proposition 6.2 of [4] holds from Assumption A7.2 with  $\sqrt{\bar{\alpha}^2} \frac{1}{L_n^2 \log(n)} \rightarrow c_p > 0$ . Then, we deduce, relying on (71)–(72),

$$\sqrt{\frac{\bar{\alpha}^2}{N}} \frac{\partial}{\partial \theta} H(\gamma)(\theta^*) \xrightarrow{\mathcal{L}} c_p \mathcal{Z}_1.$$

Now, (62)–(63) together with the independence of the variables  $(\mathcal{E}_j^{i,\ell,(k)})_{i,j,\ell,k}$  from the processes  $(X^i)_i$  yields

$$\sqrt{\frac{\bar{\alpha}^2}{N L_n^2 \log(n)}} \frac{1}{\partial_\theta} S_n^{N,\text{pub}}(\theta^*) \xrightarrow{\mathcal{L}} \mathcal{N}\left(0, 2c_p^2 \Sigma_0 + 16(a+1)^2 T \hat{v}(S)\right).$$

The analysis of the second derivatives of the contrast function is due once again to Proposition 6 that, in the same way as in the proof of Theorems 2 and 3 above, implies the wanted result on  $\frac{\sqrt{N\bar{\alpha}^2}}{L_n^2 \log(n)} (\hat{\theta}_n^N - \theta^*)$ .  $\square$

### 6.2.4 Proof of Proposition 6

*Proof.* The main tool consists in the approximation argument gathered in Proposition 3, this time for  $u = 2$ . Indeed,

$$\frac{1}{N} \partial_{\theta}^2 S_n^{N,\text{pub}}(\theta) = \frac{1}{N} (\partial_{\theta}^2 S_n^{N,\text{pub}}(\theta) - \partial_{\theta}^2 S_n^{N,0}(\theta)) + \frac{1}{N} \partial_{\theta}^2 S_n^{N,0}(\theta).$$

Proposition 3 implies

$$\left\| \sup_{\theta \in [\theta_0, \theta_{L_n-1}]} \frac{1}{N} (\partial_{\theta}^2 S_n^{N,\text{pub}}(\theta) - \partial_{\theta}^2 S_n^{N,0}(\theta)) \right\|_p \leq c \frac{1}{L_n^{a-3}} + c L_n^3 \log(n) \sqrt{\frac{\log(L_n)}{N \bar{\alpha}^2}} + c \frac{L_n \sqrt{N}}{n^r},$$

where  $r > 0$  can be chosen arbitrarily large. Hence, such  $L^p$ -norm goes to 0 as we have chosen  $a > 3$  and  $L_n^3 \log(n) \sqrt{\frac{\log(L_n)}{N \bar{\alpha}^2}} \rightarrow 0$  for  $N, n \rightarrow \infty$ . Then, following the proof of Proposition 6.3 in [4] (see in particular Equation (54)), it is straightforward to check that

$$\frac{1}{N} \partial_{\theta}^2 S_n^{N,0}(\theta) \xrightarrow{\mathbb{P}} 2 \int_0^T \mathbb{E} \left[ \left( \frac{\partial_{\theta} b(\theta, X_s)}{\sigma(X_s)} \right)^2 - \frac{\partial_{\theta}^2 b(\theta, X_s)}{\sigma^2(X_s)} (b(\theta^*, X_s) - b(\theta, X_s)) \right] ds =: 2\Sigma(\theta)$$

uniformly in  $\theta \in \Theta$ . It concludes the proof of the first point.

The second point follows from the continuity of  $\Sigma(\theta)$  at  $\theta = \theta^*$  and the consistency of  $\hat{\theta}_n^N$  as proved in Theorem 1.  $\square$

## 7 Proof of preliminary results

### 7.1 Proof of Lemma 2

*Proof.* From the definition of  $\ell_n^*$ , we have  $\theta_{\ell_n^*} = \frac{\ell_n^* + S}{L_n} \leq \theta^* < \frac{\ell_n^* + 1 + S}{L_n}$ . We deduce that  $\ell_n^* = \lfloor L_n \theta^* - S \rfloor$  and  $\theta_{\ell_n^*} = \frac{\lfloor L_n \theta^* - S \rfloor + S}{L_n}$ . Consequently,  $v_n(\theta^*) = \hat{v}(L_n(\theta^* - \theta_{\ell_n^*})) = \hat{v}(L_n \theta^* - \lfloor L_n \theta^* - S \rfloor - S)$ . Let us denote by  $\vartheta_n^* = L_n \theta^* - \lfloor L_n \theta^* \rfloor \in [0, 1)$  the fractional part of  $L_n \theta^*$ . We have  $L_n \theta^* - \lfloor L_n \theta^* - S \rfloor = \vartheta_n^* - \lfloor \vartheta_n^* - S \rfloor$  and we deduce that  $v_n(\theta^*) = \hat{v}(\vartheta_n^* - S - \lfloor \vartheta_n^* - S \rfloor)$ . Now, if we check that

$$\vartheta_n^* - S - \lfloor \vartheta_n^* - S \rfloor \stackrel{\mathcal{L}}{=} S, \quad (74)$$

the lemma will be proved. Let us recall that the random variable  $S$  is uniformly distributed on  $(0, 1)$ , and therefore we need to show that the L.H.S. of (74) shares the same law. For  $g$  a non negative measurable real function, we write  $\mathbb{E}[g(\vartheta_n^* - S - \lfloor \vartheta_n^* - S \rfloor)] = \mathbb{E}[g(\vartheta_n^* - S) \mathbf{1}_{S \leq \vartheta_n^*}] + \mathbb{E}[g(\vartheta_n^* - S + 1) \mathbf{1}_{S > \vartheta_n^*}]$  where we used that  $\vartheta_n^* \in [0, 1)$ . Since  $S$  is uniform, this gives  $\mathbb{E}[g(\vartheta_n^* - S - \lfloor \vartheta_n^* - S \rfloor)] = \int_0^{\vartheta_n^*} g(\vartheta_n^* - s) ds + \int_{\vartheta_n^*}^1 g(\vartheta_n^* - s + 1) ds = \int_0^{\vartheta_n^*} g(s) ds + \int_{\vartheta_n^*}^1 g(s) ds = \int_0^1 g(s) ds$ , by change of variables. We deduce (74) and the lemma follows.  $\square$

### 7.2 Proof of Proposition 2

*Proof.* Let  $x_0 \in [\xi_0, \xi_{\Lambda}]$  and let  $P_{x_0}$  be the Taylor approximation of  $f$  at the point  $x_0$  with order  $a$ , defined by  $P_{x_0}(x) = \sum_{k=0}^a f^{(k)}(x_0)(x - x_0)^k/k!$ . We know that the spline approximation of the polynomial function  $P_{x_0}$  of degree at most  $a$  is exact, yielding to  $HP_{x_0} = P_{x_0}$ . Hence, using that for  $k \leq a$  the  $k$ -th derivative of  $f$  and  $P_{x_0}$  are the same at the point  $x_0$ , we can write for  $k \in \{0, \dots, a\}$ ,

$$\begin{aligned} \frac{\partial^k}{\partial x^k} Hf(x_0) - \frac{\partial^k}{\partial x^k} f(x_0) &= \frac{\partial^k}{\partial x^k} Hf(x_0) - \frac{\partial^k}{\partial x^k} P_{x_0}(x_0) \\ &= \frac{\partial^k}{\partial x^k} Hf(x_0) - \frac{\partial^k}{\partial x^k} HP_{x_0}(x_0), \end{aligned} \quad (75)$$

where in the second line we used  $HP_{x_0} = P_{x_0}$ . We write

$$\begin{aligned} \left| \frac{\partial^k}{\partial x^k} (Hf - HP_{x_0})(x_0) \right| &= \left| \frac{\partial^k}{\partial x^k} \left[ \sum_{i=-1}^{\Lambda-1} \sum_{r=0}^a [c_i^r(f) - c_i^r(P_{x_0})] B_i^r(x) \right] \Big|_{x=x_0} \right| \\ &\leq c(a+1)\Lambda^k \sup_{i \in \{i_0-1, i_0\}, r \in \{0, \dots, a\}} |c_i^r(f) - c_i^r(P_{x_0})|, \end{aligned} \quad (76)$$

where  $i_0 \in \{0, \dots, \Lambda-1\}$  is such that  $x_0 \in [\xi_{i_0}, \xi_{i_0+1})$  and we used  $\left\| \frac{\partial^k}{\partial x^k} B_i^r \right\|_{\infty} \leq c\Lambda^k$ . From (24),

$$\begin{aligned} |c_i^r(f) - c_i^r(P_{x_0})| &= \left| \sum_{m=0}^a \frac{(-1)^m}{m!} (g_i^r)^{(2a+1-m)}(\xi_{i+1}) [f^{(m)}(\xi_{i+1}) - P_{x_0}^{(m)}(\xi_{i+1})] \right| \\ &\leq c \sum_{m=0}^a \frac{1}{\Lambda^m} |f^{(m)}(\xi_i) - P_{x_0}^{(m)}(\xi_i)|, \end{aligned} \quad (77)$$

since  $(g_i^r)^{(2a+1-m)}$  is the  $(2a+1-m)$ -derivative of a  $(2a+1)$ -degree polynomial function, and so it is an  $m$ -degree polynomial function computed by differentiation of (22).

Collecting (75), (76) and (77) we deduce

$$\left| \frac{\partial^k}{\partial x^k} Hf(x_0) - \frac{\partial^k}{\partial x^k} f(x_0) \right| \leq c \sup_{i \in \{i_0-1, i_0\}} \sum_{m=0}^a \Lambda^{k-m} |f^{(m)}(\xi_i) - P_{x_0}^{(m)}(\xi_i)|.$$

Then, using a Taylor expansion of order  $a-m$  around  $x_0$  for  $f^{(m)}(\xi_i) - P_{x_0}^{(m)}(\xi_i)$ , and recalling that  $f^{(k)}(x_0) - P_{x_0}^{(k)}(x_0) = 0$  for  $k \in \{0, \dots, a\}$ , we deduce that  $|f^{(m)}(\xi_i) - P_{x_0}^{(m)}(\xi_i)| \leq |\xi_i - x_0|^{(a+1-m)} \left\| f^{(a+1)} - P_{x_0}^{(a+1)} \right\|_{\infty} = |\xi_i - x_0|^{(a+1-m)} \left\| f^{(a+1)} \right\|_{\infty} \leq c\Lambda^{m-a-1} \left\| f^{(a+1)} \right\|_{\infty}$ . It yields

$$\left| \frac{\partial^k}{\partial x^k} Hf(x_0) - \frac{\partial^k}{\partial x^k} f(x_0) \right| \leq c \sum_{m=0}^a L_n^{k-m} \Lambda^{m-a-1} \left\| f^{(a+1)} \right\|_{\infty} \leq c\Lambda^{k-a-1} \left\| f^{(a+1)} \right\|_{\infty}.$$

As  $x_0 \in [\xi_0, \xi_{\Lambda}]$  is arbitrary, we get the result.  $\square$

### 7.3 Proof of Lemma 5

*Proof.* We start with the introduction of some useful notation for the proof. First, we define  $\bar{\mathbf{t}} = \{\bar{t}_0, \dots, \bar{t}_{3a+2}\}$  a sequence of knots where  $\bar{t}_l = 0$  for  $0 \leq l \leq a$ ,  $\bar{t}_l = 1$  for  $a+1 \leq l \leq 2a+1$  and  $\bar{t}_l = 2$  for  $2a+2 \leq l \leq 3a+2$ . Recalling Definition 1, we have that, for  $0 \leq k \leq a$ ,  $\bar{B}_k = B_{h, 2a+1, \bar{\mathbf{t}}}$  is the B-spline of degree  $2a+1$  relying on the  $2a+3$  knots  $\{\bar{t}_k, \dots, \bar{t}_{k+2a+2}\} = \underbrace{\bar{t}_k, \dots, \bar{t}_a}_{=0}, \underbrace{\bar{t}_{a+1}, \dots, \bar{t}_{2a+1}}_{=1}, \underbrace{\bar{t}_{2a+2}, \dots, \bar{t}_{2a+2+k}}_{=2}$ . This leads us to denote by  $\bar{B}_{(\beta_1, \beta_2, \beta_3)}$  the B-spline of order  $\beta_1 + \beta_2 + \beta_3 - 2$  where  $(\beta_1, \beta_2, \beta_3)$  stands for the number of repetitions of each knots : 0 is repeated  $\beta_1 = a+1-k$  times, 1 is repeated  $\beta_2 = a+1$  times, and 2 is repeated  $\beta_3 = k+1$  times. Using this notation, we have  $\bar{B}_k := \bar{B}_{k, 2a+1, \bar{\mathbf{t}}} = \bar{B}_{(a+1-k, a+1, k+1)}$ , for  $0 \leq k \leq a$ . For example,  $\bar{B}_0$  is a B-spline based on points  $\{\bar{t}_0, \dots, \bar{t}_{2a+2}\} = \underbrace{\bar{t}_0, \dots, \bar{t}_a}_{=0}, \underbrace{\bar{t}_{a+1}, \dots, \bar{t}_{2a+1}}_{=1}, \underbrace{\bar{t}_{2a+2}}_{=2}$ , that we sum up through the notation

$$\bar{B}_0 = \bar{B}_{(a+1, a+1, 1)}.$$

Recall that by Theorem 9 in [36],  $\bar{B}_{j,p,\bar{\mathbf{t}}}$  satisfies

$$\bar{B}'_{j,p,\bar{\mathbf{t}}} = p \left[ \frac{\bar{B}_{j,p-1,\bar{\mathbf{t}}}}{(\bar{t}_{j+p} - \bar{t}_j)} - \frac{\bar{B}_{j+1,p-1,\bar{\mathbf{t}}}}{(\bar{t}_{j+p+1} - \bar{t}_{j+1})} \right].$$

Noting that  $\bar{B}_k = \bar{B}_{k,2a+1,\bar{t}} = \bar{B}_{(a+1-k,a+1,k+1)}$ , we have for  $0 < k < a$ ,

$$\bar{B}'_k = \frac{2a+1}{2} [\bar{B}_{k,2a,\bar{t}} - \bar{B}_{k+1,2a,\bar{t}}] = \frac{2a+1}{2} [\bar{B}_{(a+1-k,a+1,k)} - \bar{B}_{(a-k,a+1,k+1)}],$$

as well as

$$\bar{B}'_0 = (2a+1)\bar{B}_{(a+1,a+1,0)} - \frac{2a+1}{2}\bar{B}_{(a,a+1,1)} \quad \text{and} \quad \bar{B}'_a = \frac{(2a+1)}{2}\bar{B}_{(1,a+1,a)} - (2a+1)\bar{B}_{(0,a+1,a+1)}.$$

Then,

$$\begin{aligned} \sum_{k=0}^a \bar{B}'_k &= \sum_{k=1}^{a-1} \frac{2a+1}{2} [\bar{B}_{(a+1-k,a+1,k)} - \bar{B}_{(a-k,a+1,k+1)}] + (2a+1) [\bar{B}_{(a+1,a+1,0)} - \frac{1}{2}\bar{B}_{(a,a+1,1)}] \\ &\quad + (2a+1) [\frac{1}{2}\bar{B}_{(1,a+1,a)} - \bar{B}_{(0,a+1,a+1)}] \\ &= \frac{2a+1}{2} [\bar{B}_{(a,a+1,1)} - \bar{B}_{(1,a+1,a)}] + (2a+1) [\bar{B}_{(a+1,a+1,0)} - \frac{1}{2}\bar{B}_{(a,a+1,1)} + \frac{1}{2}\bar{B}_{(1,a+1,a)} - \bar{B}_{(0,a+1,a+1)}] \\ &= (2a+1) [\bar{B}_{(a+1,a+1,0)} - \bar{B}_{(0,a+1,a+1)}]. \end{aligned}$$

We can show (see for instance [14], Section 3) that

$$\bar{B}_{(a+1,a+1,0)}(x) = \binom{2a}{a} x^a (1-x)^a \mathbf{1}_{[0,1]}(x) \quad \text{and} \quad \bar{B}_{(0,a+1,a+1)}(x) = \binom{2a}{a} (x-1)^a (2-x)^a \mathbf{1}_{[1,2]}(x).$$

We deduce that, for  $x \in \mathbb{R}$ ,

$$\sum_{k=0}^a \bar{B}'_k(x) = (2a+1) \binom{2a}{a} [x^a (1-x)^a \mathbf{1}_{[0,1]}(x) - (x-1)^a (2-x)^a \mathbf{1}_{[1,2]}(x)].$$

Hence, the result.  $\square$

## 7.4 Proof of Lemma 7

*Proof.* We start by proving that

$$\frac{\Delta_n}{N} \sum_{i=1}^N \sum_{j=1}^n f(X_{t_{j-1}}^i) - \frac{1}{N} \sum_{i=1}^N \int_0^T f(X_s^i) ds \xrightarrow{L^1} 0.$$

Indeed, one can write  $\int_0^T f(X_s^i) ds$  as  $\sum_{j=1}^n \int_{t_{j-1}}^{t_j} f(X_s^i) ds$ . Recall moreover that  $\Delta_n = t_j - t_{j-1} = \int_{t_{j-1}}^{t_j} ds$ . Hence, the norm 1 of the difference above is bounded by

$$\begin{aligned} &\frac{1}{N} \sum_{i=1}^N \sum_{j=1}^n \int_{t_{j-1}}^{t_j} \mathbb{E}[|f(X_{t_{j-1}}^i) - f(X_s^i)|] ds \\ &\leq \frac{c}{N} \sum_{i=1}^N \sum_{j=1}^n \int_{t_{j-1}}^{t_j} \mathbb{E}[|X_{t_{j-1}}^i - X_s^i| (1 + |X_{t_{j-1}}^i| + |X_s^i|)^k] ds \\ &\leq \frac{c}{N} \sum_{i=1}^N \sum_{j=1}^n \int_{t_{j-1}}^{t_j} |t_{j-1} - s|^{\frac{1}{2}} ds \leq c \Delta_n^{\frac{1}{2}}, \end{aligned}$$

having used Cauchy-Schwarz inequality and Points 1 and 2 of Lemma 6. Then, it clearly goes to 0 as we wanted. To conclude the proof remark that the law of large number provides

$$\frac{1}{N} \sum_{i=1}^N \int_0^T f(X_s^i) ds \xrightarrow{\mathbb{P}} \int_0^T \mathbb{E}[f(X_s)] ds,$$

as  $\{(X_s^i)_{s \in [0,T]}, i \in \{1, \dots, N\}\}$  are i.i.d. processes.  $\square$



## 7.5 Proof of Lemma 8

*Proof.* Recall that, for all  $i \in \{1, \dots, N\}$ ,  $j \in \{1, \dots, n\}$  and  $k \in \mathbb{N}$  it is

$$f^{(k)}(\theta; X_{t_{j-1}}^i, X_{t_j}^i) = 2 \frac{\partial_\theta^k b(\theta, X_{t_{j-1}}^i)(X_{t_j}^i - X_{t_{j-1}}^i)}{\sigma^2(X_{t_{j-1}}^i)} + \Delta_n \frac{\partial_\theta^k (b^2(\theta, X_{t_{j-1}}^i))}{\sigma^2(X_{t_{j-1}}^i)}.$$

Then, we have

$$\begin{aligned} \mathbb{P}_{t_{j-1}}(|f^{(k)}(\theta; X_{t_{j-1}}^i, X_{t_j}^i)| > \tau_n) &\leq \mathbb{P}_{t_{j-1}}\left(\frac{2\partial_\theta^k b(\theta, X_{t_{j-1}}^i)(X_{t_j}^i - X_{t_{j-1}}^i)}{\sigma^2(X_{t_{j-1}}^i)} > \frac{\sqrt{\Delta_n} \log(n)}{2}\right) \\ &\quad + \mathbb{P}_{t_{j-1}}\left(\frac{\Delta_n \partial_\theta^k (b^2(\theta, X_{t_{j-1}}^i))}{\sigma^2(X_{t_{j-1}}^i)} > \frac{\sqrt{\Delta_n} \log(n)}{2}\right) \\ &=: P_1 + P_2. \end{aligned}$$

Since  $\sigma$  and the derivatives of  $b$  are lower and upper bounded by Assumptions 2 and 3 respectively, and  $X_{t_{j-1}}^i$  is  $\mathcal{F}_{t_{j-1}}^N$ -measurable, the second term can be controlled as

$$P_2 \leq \frac{c\Delta_n^{r/2}}{(\log(n))^r} \mathbb{E}_{t_{j-1}} \left[ \left| \frac{\partial_\theta^k (b^2(\theta, X_{t_{j-1}}^i))}{\sigma^2(X_{t_{j-1}}^i)} \right|^r \right] \leq c \left( \frac{\sqrt{\Delta_n}}{\log(n)} \right)^r,$$

for all  $r \geq 1$ . In the first term, replacing the increments of  $X$  by its dynamics, we get

$$\begin{aligned} P_1 &\leq \mathbb{P}_{t_{j-1}}\left(\frac{2|\partial_\theta^k b(\theta, X_{t_{j-1}}^i)|}{\sigma^2(X_{t_{j-1}}^i)} \left| \int_{t_{j-1}}^{t_j} b(\theta, X_{t_{j-1}}^i) ds \right| > \frac{\sqrt{\Delta_n} \log(n)}{6}\right) \\ &\quad + \mathbb{P}_{t_{j-1}}\left(\frac{2|\partial_\theta^k b(\theta, X_{t_{j-1}}^i)|}{\sigma^2(X_{t_{j-1}}^i)} \left| \int_{t_{j-1}}^{t_j} (\sigma(X_s^i) - \sigma(X_{t_{j-1}}^i)) dW_s^i \right| > \frac{\sqrt{\Delta_n} \log(n)}{6}\right) \\ &\quad + \mathbb{P}_{t_{j-1}}\left(\frac{2|\partial_\theta^k b(\theta, X_{t_{j-1}}^i)|}{\sigma(X_{t_{j-1}}^i)} |W_{t_j}^i - W_{t_{j-1}}^i| > \frac{\sqrt{\Delta_n} \log(n)}{6}\right) \\ &=: P_{11} + P_{12} + P_{13}. \end{aligned}$$

From Markov inequality, we get for any  $r \geq 1$ ,

$$P_{11} \leq \frac{\Delta_n^{r/2}}{(\log(n))^r} \mathbb{E}_{t_{j-1}} \left[ \left| \frac{2\partial_\theta^k b(\theta, X_{t_{j-1}}^i)}{\sigma^2(X_{t_{j-1}}^i)} \int_{t_{j-1}}^{t_j} b(\theta, X_{t_{j-1}}^i) ds \right|^r \right] \leq c \left( \frac{\sqrt{\Delta_n}}{\log(n)} \right)^r,$$

where we have used that  $b$  and  $\partial_\theta^k b$  are bounded and  $\sigma$  is lower bounded as given in Assumptions 2 and 3.

Successively applying Markov and Burkholder-Davis-Gundy inequalities, before using the

Lipschitzness of  $\sigma$ , we get for any  $r \geq 2$

$$\begin{aligned}
P_{12} &\leq \frac{c}{(\sqrt{\Delta_n} \log(n))^r} \mathbb{E}_{t_{j-1}} \left[ \left| \frac{2\partial_\theta^k b(\theta, X_{t_{j-1}}^i)}{\sigma^2(X_{t_{j-1}}^i)} \right|^r \left| \int_{t_{j-1}}^{t_j} (\sigma(X_s^i) - \sigma(X_{t_{j-1}}^i)) dW_s^i \right|^r \right] \\
&\leq \frac{c}{(\sqrt{\Delta_n} \log(n))^r} \mathbb{E}_{t_{j-1}} \left[ \left| \int_{t_{j-1}}^{t_j} |\sigma(X_s^i) - \sigma(X_{t_{j-1}}^i)|^2 ds \right|^{r/2} \right] \\
&\leq \frac{c}{(\sqrt{\Delta_n} \log(n))^r} \mathbb{E}_{t_{j-1}} \left[ \left| \int_{t_{j-1}}^{t_j} |X_s^i - X_{t_{j-1}}^i|^2 ds \right|^{r/2} \right] \\
&\leq \frac{c\Delta_n^{r/2-1}}{(\sqrt{\Delta_n} \log(n))^r} \mathbb{E}_{t_{j-1}} \left[ \int_{t_{j-1}}^{t_j} |X_s^i - X_{t_{j-1}}^i|^r ds \right] \\
&\leq \frac{c\Delta_n^{r/2-1} \Delta_n^{r/2+1}}{(\sqrt{\Delta_n} \log(n))^r} R_{t_{j-1}}(1) = \frac{c\Delta_n^r}{(\sqrt{\Delta_n} \log(n))^r} R_{t_{j-1}}(1),
\end{aligned}$$

where we have also used Jensen's inequality in the fourth line and Point 3 of Lemma 6 to get the last one. Last,

$$\begin{aligned}
P_{13} &= \mathbb{P}_{t_{j-1}} \left( \left| W_{t_j}^i - W_{t_{j-1}}^i \right| > \frac{\sqrt{\Delta_n} \log(n)}{12} \frac{|\sigma(X_{t_{j-1}}^i)|}{\sqrt{|\partial_\theta^k b^2(\theta, X_{t_{j-1}}^i)|}} \right) \\
&= \mathbb{P} \left( |Y| > \frac{\log(n)}{12} \frac{|\sigma(x)|}{\sqrt{|\partial_\theta^k b^2(\theta, x)|}} \right) \Big|_{x=X_{t_{j-1}}^i} = 2\mathbb{P} \left( Y > \frac{\log(n)}{12} \frac{|\sigma(x)|}{\sqrt{|\partial_\theta^k b^2(\theta, x)|}} \right) \Big|_{x=X_{t_{j-1}}^i}
\end{aligned}$$

where  $Y$  is a standard Gaussian random variable. Recalling that for all  $z > 0$ ,

$$e^{z^2/2} \mathbb{P}(Y > z) = \frac{1}{\sqrt{2\pi}} \int_z^{+\infty} e^{-(y^2-z^2)/2} dy \leq \frac{1}{\sqrt{2\pi}} \int_0^{+\infty} e^{-(y-z)^2/2} dy = \frac{1}{2},$$

we get

$$P_{13} \leq \exp \left( -\frac{1}{2} \left( \frac{\log(n)}{12} \frac{|\sigma(X_{t_{j-1}}^i)|}{\sqrt{|\partial_\theta^k b^2(\theta, X_{t_{j-1}}^i)|}} \right)^2 \right)$$

Combining all previous bounds, there exist constants  $c_1$  and  $c_2$  such that

$$\mathbb{P}_{t_{j-1}}(|f(\theta; X_{t_{j-1}}^i, X_{t_j}^i)| > \tau_n) \leq \frac{\Delta_n^{r/2}}{(\log(n))^r} R_{t_{j-1}}(1) + c_1 \exp \left( -c_2 (\log(n))^2 \frac{\sigma^2(X_{t_{j-1}}^i)}{\partial_\theta^k b^2(\theta, X_{t_{j-1}}^i)} \right).$$

Hence, the result.  $\square$

## 7.6 Proof of Lemma 9

*Proof.* Our lemma is based on Theorem 15, p.52 of [39]. In order to apply it we need a control on the exponential moments of the Laplace. Recalling that the moment generating function of a Laplace random variable with mean 0 and scale parameter  $b$  is  $t \mapsto 1/(1 - b^2 t^2)$  we have  $\mathbb{E}[e^{t\mathcal{L}(1/\gamma_h)}] = 1/(1 - (t/\gamma_h)^2)$ . Remark that, for  $u \leq 1/4$  it is  $1/(1 - u) < e^{2u}$ . Then, for  $t \leq \gamma_h/2$ , we have  $1/(1 - (t/\gamma_h)^2) \leq \exp(2(t/\gamma_h)^2)$ . From here we conclude

$$\mathbb{E}[e^{t\mathcal{L}(1/\gamma_h)}] \leq e^{2t^2/\gamma_h^2} \text{ for } t \leq \frac{1}{2}\gamma_{\max}.$$

According to Petrov's notation we therefore have  $T := \gamma_{\max}/2$ ,  $g_h := 4/\gamma_h^2$ ,  $G := 4 \sum_{h=1}^U 1/\gamma_h^2$ . Then, from Theorem 15, p.52 of [39] it follows

$$\mathbb{P}(S_U \geq x) \leq \begin{cases} e^{-\frac{x^2}{2G}} & \text{if } 0 \leq x \leq \frac{\gamma_{\max} G}{2} \\ e^{-\frac{\gamma_{\max} x}{4}} & \text{if } x \geq \frac{\gamma_{\max} G}{2} \end{cases}$$

Hence, by symmetry,

$$\mathbb{P}\left(\frac{|S_U|}{\sqrt{U}} \geq \lambda\right) = \mathbb{P}(|S_U| \geq \lambda\sqrt{U}) \leq \begin{cases} 2e^{-\frac{\lambda^2 U}{2G}} & \text{if } 0 \leq \lambda\sqrt{U} \leq \frac{\gamma_{\max} G}{2} \\ 2e^{-\frac{\gamma_{\max} \lambda \sqrt{U}}{4}} & \text{if } \lambda\sqrt{U} \geq \frac{\gamma_{\max} G}{2}. \end{cases} \quad (78)$$

Observe now that, from the definition of  $G$  it is

$$G = 4U \frac{1}{U} \sum_{h=1}^U \frac{1}{\gamma_h^2} = 4U \frac{1}{\bar{\gamma}^2}.$$

Then,  $\lambda\sqrt{U} \leq \gamma_{\max} G/2$  if and only if  $\lambda\sqrt{U} \leq 2U\gamma_{\max}/\bar{\gamma}^2$ , i.e.  $\lambda \leq 2\sqrt{U}\gamma_{\max}/\bar{\gamma}^2$ . Replacing such observation in (78) we obtain

$$\mathbb{P}\left(\frac{|S_U|}{\sqrt{U}} \geq \lambda\right) \leq \begin{cases} 2e^{-\frac{\lambda^2 \bar{\gamma}^2}{8}} & \text{if } 0 \leq \lambda \leq 2\sqrt{U}\gamma_{\max}/\bar{\gamma}^2 \\ 2e^{-\frac{\gamma_{\max} \lambda \sqrt{U}}{4}} & \text{if } \lambda \geq 2\sqrt{U}\gamma_{\max}/\bar{\gamma}^2, \end{cases}$$

as we wanted. □

## References

- [1] Abadi, M., Chu, A., Goodfellow, I., McMahan, H. B., Mironov, I., Talwar, K., & Zhang, L. (2016, October). Deep learning with differential privacy. In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security (pp. 308-318).
- [2] Amorino, C., & Gloter, A. (2023). Minimax rate for multivariate data under componentwise local differential privacy constraints. arXiv preprint arXiv:2305.10416.
- [3] Amorino, C., & Gloter, A. (2020). Contrast function estimation for the drift parameter of ergodic jump diffusion process. *Scandinavian Journal of Statistics*, 47(2), 279-346.
- [4] Amorino, C., Heidari, A., Pilipauskaitė, V., & Podolskij, M. (2023). Parameter estimation of discretely observed interacting particle systems. *Stochastic Processes and their Applications*.
- [5] Apple Differential Privacy Team. (2017). Learning with privacy at scale. *Apple Mach. Learn. J*, 1(8), 1-25. Available at <https://machinelearning.apple.com/2017/12/06/learning-with-privacy-at-scale.html>.
- [6] Avella-Medina, M., Bradshaw, C., & Loh, P. L. (2021). Differentially private inference via noisy optimization. arXiv preprint arXiv:2103.11003.
- [7] Bergstrom, A.R. (1990) *Continuous Time Econometric Modeling*, Oxford University Press, Oxford.
- [8] Berrett, T., & Butucea, C. (2020). Locally private non-asymptotic testing of discrete distributions is faster using interactive mechanisms. *Advances in Neural Information Processing Systems*, 33, 3164-3173.
- [9] Berrett, T., & Yu, Y. (2021). Locally private online change point detection. *Advances in Neural Information Processing Systems*, 34, 3425-3437.
- [10] Billingsley, P. (2013). *Convergence of probability measures*. John Wiley & Sons.
- [11] Butucea, C., Dubois, A., Kroll, M., & Saumard, A. (2020). Local differential privacy: Elbow effect in optimal density estimation and adaptation over Besov ellipsoids.

- [12] Butucea, C., Rohde, A., & Steinberger, L. (2023). Interactive versus noninteractive locally differentially private estimation: Two elbows for the quadratic functional. *The Annals of Statistics*, 51(2), 464-486.
- [13] D’Argenio, D. Z., & Park, K. (1997). Uncertain pharmacokinetic/pharmacodynamic systems: design, estimation and control. *Control Engineering Practice*, 5(12), 1707-1716.
- [14] De Boor, C. (1986). *B (asic)-spline basics*. University of Wisconsin-Madison. Mathematics Research Center.
- [15] Denis, C., Dion, C., & Martinez, M. (2020). Consistent procedures for multiclass classification of discrete diffusion paths. *Scandinavian Journal of Statistics*.
- [16] Delattre, M., Genon-Catalot, V., & Larédo, C. (2018). Parametric inference for discrete observations of diffusion processes with mixed effects. *Stochastic Processes and their Applications*, 128(6), 1929-1957.
- [17] Della Maestra, L., & Hoffmann, M. (2023). The LAN property for McKean–Vlasov models in a mean-field regime. *Stochastic Processes and their Applications*, 155, 109-146.
- [18] Ding, B., Kulkarni, J., & Yekhanin, S. (2017). Collecting telemetry data privately. *Advances in Neural Information Processing Systems*, 30.
- [19] Donnet, S., & Samson, A. (2013). A review on estimation of stochastic differential equations for pharmacokinetic/pharmacodynamic models. *Advanced drug delivery reviews*, 65(7), 929-939.
- [20] Duchi, J. C., Jordan, M. I., & Wainwright, M. J. (2018). Minimax optimal procedures for locally private estimation. *Journal of the American Statistical Association*, 113(521), 182-201.
- [21] Dwork, C., McSherry, F., Nissim, K., & Smith, A. (2006). Calibrating noise to sensitivity in private data analysis. In *Theory of Cryptography: Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4-7, 2006. Proceedings 3* (pp. 265-284). Springer Berlin Heidelberg
- [22] Dwork, C., & Smith, A. (2010). Differential privacy for statistics: What we know and what we want to learn. *Journal of Privacy and Confidentiality*, 1(2).
- [23] Erlingsson, Ú., Pihur, V., & Korolova, A. (2014, November). Rappor: Randomized aggregatable privacy-preserving ordinal response. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security* (pp. 1054-1067).
- [24] Florens-Zmirou, D. (1989). Approximate discrete-time schemes for statistics of diffusion processes. *Statistics: A Journal of Theoretical and Applied Statistics*, 20(4), 547-557.
- [25] Garfinkel, S., Abowd, J. M., & Martindale, C. (2019). Understanding database reconstruction attacks on public data. *Communications of the ACM*, 62(3), 46-53.
- [26] V. Genon-Catalot and J. Jacod. On the estimation of the diffusion coefficient for multi-dimensional diffusion processes. In *Annales de l’IHP Probabilités et statistiques*, volume 29, pages 119–151, 1993.
- [27] Hall, P. and Heyde, C. C. (1980). *Martingale limit theory and its application*. Probability and Mathematical Statistics. New York etc.: Academic Press, A Subsidiary of Harcourt Brace Jovanovich, Publishers. XII, 308 p.

- [28] Holden, A.V. (1976) Models for Stochastic Activity of Neurones, Springer-Verlag, New York. Berlin/Boston.
- [29] Hull, J. (2000) Options, Futures and Other Derivatives, Prentice-Hall, Englewood Cliffs, NJ.
- [30] Kessler, M. (1997). Estimation of an ergodic diffusion from discrete observations. Scandinavian Journal of Statistics, 24(2), 211-229.
- [31] Kroll, M. (2020). Adaptive spectral density estimation by model selection under local differential privacy. arXiv preprint arXiv:2010.04218.
- [32] Kushner, H.J. (1967) Stochastic Stability and Control, Academic Press, New York.
- [33] Lam-Weil, J., Laurent, B., & Loubes, J. M. (2022). Minimax optimal goodness-of-fit testing for densities and multinomials under a local differential privacy constraint. Bernoulli, 28(1), 579-600.
- [34] Mummy, M.S. (1989). Hermite interpolation with B-splines. Computer Aided Geometric Design, 6(2), 177-179.
- [35] Li, M., Berrett, T. B., & Yu, Y. (2023). On robustness and local differential privacy. The Annals of Statistics, 51(2), 717-737.
- [36] Lyche, T. and Manni, C. and Speleers, H. B-Splines and Spline Approximation, 2017.
- [37] Narayanan, A., & Shmatikov, V. (2008, May). Robust de-anonymization of large sparse datasets. In 2008 IEEE Symposium on Security and Privacy (sp 2008) (pp. 111-125). IEEE.
- [38] Papanicolaou, G. C. (1995) Diffusion in random media, Surveys in applied mathematics. 201-253.
- [39] Petrov, V. V. (2012). Sums of independent random variables (Vol. 82). Springer Science & Business Media.
- [40] Polyak, B. T., & Juditsky, A. B. (1992). Acceleration of stochastic approximation by averaging. SIAM journal on control and optimization, 30(4), 838-855.
- [41] Ramanathan, M. (1999). An application of Ito's lemma in population pharmacokinetics and pharmacodynamics. Pharmaceutical research, 16(4), 584.
- [42] Ramanathan, M. (1999). A method for estimating pharmacokinetic risks of concentration-dependent drug interactions from preclinical data. Drug Metabolism and disposition, 27(12), 1479-1487.
- [43] Revuz, D. and Yor, M. (2005). Continuous martingales and Brownian motion. Berlin: Springer, Grundlehr en Math. Wiss., 293.
- [44] Ricciardi, L.M. (1977) Diffusion Processes and Related Topics in Biology, Lecture Notes in Biomathematics, Springer, New York.
- [45] Rosenthal, H.P. (1970). On the subspaces of  $L^p$  ( $p > 2$ ) spanned by sequences of independent random variables. Israel J. Math. 8, 273-303.
- [46] Sharrock, L., Kantas, N., Parpas, P., & Pavliotis, G. A. (2021). Parameter estimation for the McKean-Vlasov stochastic differential equation. arXiv preprint arXiv:2106.13751.
- [47] Shimizu, Y. (2006). M-estimation for discretely observed ergodic diffusion processes with infinitely many jumps. Statistical Inference for Stochastic Processes, 9, 179-225.

- [48] Tang, J., Korolova, A., Bai, X., Wang, X., & Wang, X. (2017). Privacy loss in apple's implementation of differential privacy on macos 10.12. arXiv preprint arXiv:1709.02753.
- [49] Wang, Z., Luo, J., Fu, G., Wang, Z., & Wu, R. (2013). Stochastic modeling of systems mapping in pharmacogenomics. *Advanced drug delivery reviews*, 65(7), 912-917.
- [50] Warner, S. L. (1965). Randomized response: A survey technique for eliminating evasive answer bias. *Journal of the American Statistical Association*, 60(309), 63-69.
- [51] Wasserman, L., & Zhou, S. (2010). A statistical framework for differential privacy. *Journal of the American Statistical Association*, 105(489), 375-389.
- [52] Yoshida, N. (1992). Estimation for diffusion processes from discrete observation. *Journal of Multivariate Analysis*, 41(2), 220-242.