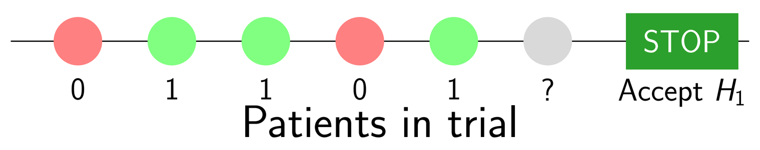
# DP-SPRT: Differentially Private Sequential Probability Ratio Tests

Thomas Michel, Debabrota Basu, Emilie Kaufmann
University of Lille, Inria, CNRS, Centrale Lille, UMR 9189-CRIStAL, France

## Sequential Hypothesis Testing

**The Problem**: We observe samples $X_1, X_2, \ldots$ from distribution $f_\theta$
**Goal**: Test $H_0 : \theta = \theta_0$ vs. $H_1 : \theta = \theta_1$ with as few samples as possible
**Constraints**: False positive probability $\leq \alpha$, false negative probability $\leq \beta$

**Example - Medical Trial:** Consider a clinical trial where patients arrive sequentially. Each patient outcome is observed, and we must decide when to stop the trial.




**Privacy Leak**: Stopping decision reveals information about the last patient's outcome!

- **Clinical Trials**: Patient outcomes confidential
- **A/B Testing**: User behavior sensitive
- **RL/Control**: Model validation, constraints satisfaction

## Sequential Probability Ratio Test (SPRT)

**SPRT Decision Rule (Wald 1945):** Stop when

$$\prod_{i=1}^{t} \frac{f_{\theta_1}(X_i)}{f_{\theta_0}(X_i)} \notin (\beta, 1/\alpha)$$

**For Bernoulli observations:** Stop at $\tau = \min(\tau_0, \tau_1)$ with decision $\hat{d} = i$ if $\tau = \tau_i$ where

$$\tau_0 = \inf\left\{ n : \bar{X}_n \leq \mu_0 + \frac{\mathrm{KL}(\nu_{\theta_0}, \nu_{\theta_1}) - \log(1/\beta)/n}{\theta_1 - \theta_0} \right\}$$

$$\tau_1 = \inf\left\{ n : \bar{X}_n \geq \mu_1 - \frac{\mathrm{KL}(\nu_{\theta_1}, \nu_{\theta_0}) - \log(1/\alpha)/n}{\theta_1 - \theta_0} \right\}$$

- **Optimal**: Minimizes expected sample size among all tests with similar error probabilities
- **Not Private**: Stopping pattern leaks info

## Differential Privacy for Sequential Tests

A randomized algorithm $\mathcal{A}$ is DP (Dwork, Roth, et al. 2014) if for any datasets $D$ and $D'$ differing by a single record and any events $S$:

$$\varepsilon\text{-DP:} \quad \log\left(\frac{\mathbb{P}[\mathcal{A}(D) \in S]}{\mathbb{P}[\mathcal{A}(D') \in S]}\right) \leq \varepsilon$$

$$(\alpha, \varepsilon)\text{-Rényi DP:} \quad D_\alpha(\mathcal{A}(D) \| \mathcal{A}(D')) \leq \varepsilon$$

where $D_\alpha$ is the Rényi divergence of order $\alpha > 1$.

## Main Contributions

1. **First theoretically calibrated** private sequential test with **guaranteed error control**
2. **Near-optimal sample complexity** matching lower bounds up to a constant in some regimes
3. **Practical implementation** with **no empirical tuning** required, **low variance** in stopping times, and **subsampling amplification** in high-privacy regimes

**Privacy is critical for real-world sequential decision-making**

## Our Method: DP-SPRT

**Algorithm 1** DP-SPRT Algorithm

**Require:** Hypotheses $\theta_0, \theta_1$, error probabilities $\alpha, \beta$, noise distributions $\mathcal{D}_Z, \mathcal{D}_Y$, correction function $C(n, x)$, error allocation $\gamma$

Sample threshold noise $Z \sim \mathcal{D}_Z$
**for** $n \leftarrow 1, 2, 3, \ldots$ **do**
  Sample query noise $Y_n \sim \mathcal{D}_Y$
  Compute noisy average $\bar{X}_n = \frac{1}{n}\sum_{i=1}^{n} X_i + \frac{Y_n}{n}$
  Compute noisy threshold $\hat{T}_0^n = \mu_0 + \frac{\mathrm{KL}(\nu_{\theta_0},\nu_{\theta_1}) - \log(1/(\gamma\beta))/n}{\theta_1 - \theta_0} - C(n, (1-\gamma)\beta) - \frac{Z}{n}$
  Compute noisy threshold $\hat{T}_1^n = \mu_1 - \frac{\mathrm{KL}(\nu_{\theta_1},\nu_{\theta_0}) - \log(1/(\gamma\alpha))/n}{\theta_1 - \theta_0} + C(n, (1-\gamma)\alpha) + \frac{Z}{n}$
  **if** noisy average $\bar{X}_n$ is below noisy threshold $\hat{T}_0^n$ **then**
   **Accept** $H_0$ and **stop**
  **else if** noisy average $\bar{X}_n$ is above noisy threshold $\hat{T}_1^n$ **then**
   **Accept** $H_1$ and **stop**
  **end if**
**end for**

**Noise Distributions:**

- **Laplace**: $Y_n \sim \mathrm{Lap}(4/\varepsilon)$, $Z \sim \mathrm{Lap}(2/\varepsilon)$ $C(n, x) = \frac{6\log(n^s\zeta(s)/x)}{n\varepsilon}$ ($\varepsilon$-DP)
- **Gaussian**: $Y_n \sim \mathcal{N}(0, \sigma_Y^2)$, $Z \sim \mathcal{N}(0, \sigma_Z^2)$, $C(n, x) = \frac{\sqrt{2(\sigma_Y^2 + \sigma_Z^2)\log(n^s\zeta(s)/2x)}}{n}$ (RDP)

## Theoretical Guarantees

**Privacy:** DP-SPRT satisfies $\varepsilon$-differential privacy (Laplace) or $(\alpha, \varepsilon(\alpha))$-RDP (Gaussian) where $\epsilon(\alpha) = \frac{\alpha - 1/2}{\alpha - 1} \cdot \frac{\alpha}{\sigma_Z^2} + \frac{\alpha}{2\sigma_Y^2} + \frac{\log\left(2\mathbb{E}_{\mathcal{D}_Z}[\mathbb{E}_{\mathcal{A}(D')}[\tau | Z = z]^2]\right)}{2(\alpha - 1)}$

**Correctness:** DP-SPRT satisfies $\mathbb{P}_{\theta_0}(\hat{d} = 1) \leq \alpha$ and $\mathbb{P}_{\theta_1}(\hat{d} = 0) \leq \beta$ when the correction function $C(n, x)$ satisfies:

$$\sum_{n=1}^{\infty} \mathbb{P}\left(\frac{Y_n}{n} - \frac{Z}{n} > C(n, x)\right) \leq x$$

**Lower Bound** (any $\varepsilon$-DP test):

$$\mathbb{E}[\tau] \geq \frac{\log(1/\beta)}{\min(\mathrm{KL}(\nu_{\theta_0}, \nu_{\theta_1}), \varepsilon \cdot \mathrm{TV}(\nu_{\theta_0}, \nu_{\theta_1}))}$$

**Sample Complexity Upper Bound** (Laplace Noise):

$$\mathbb{E}[\tau] \lesssim \max\left(\frac{\log(1/\beta)}{\mathrm{KL}(\nu_{\theta_0}, \nu_{\theta_1})}, \frac{(\theta_1 - \theta_0)\log(1/\beta)}{\varepsilon \cdot \mathrm{KL}(\nu_{\theta_0}, \nu_{\theta_1})}\right)$$

For Bernoulli distributions:

$$\frac{\mathrm{KL}(\nu_{\theta_0}, \nu_{\theta_1})}{\theta_1 - \theta_0} \xrightarrow[\theta_1 \to \theta_0]{} \mathrm{TV}(\nu_{\theta_0}, \nu_{\theta_1})$$

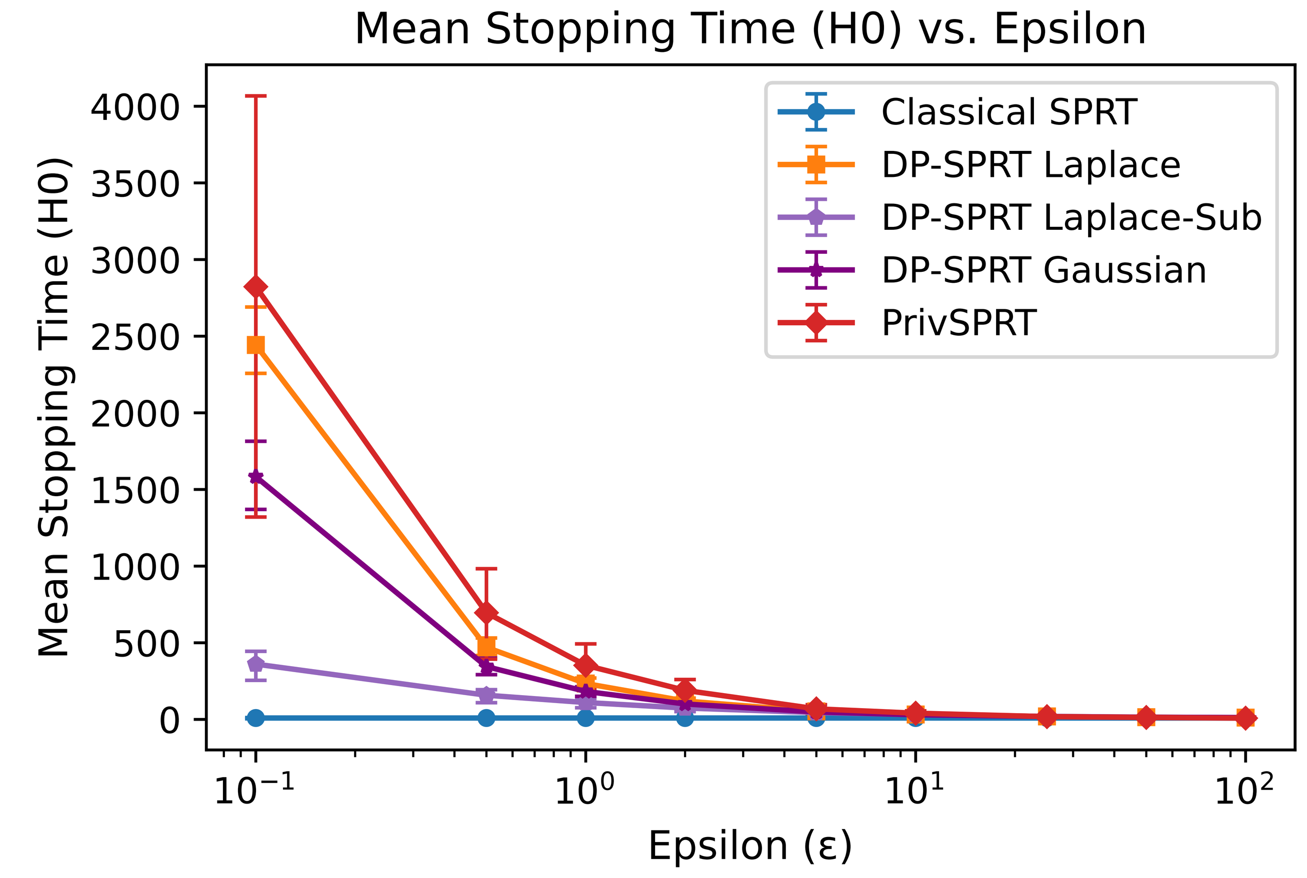
**Near-Optimal:** DP-SPRT matches lower bound up to constants when $\theta_1 \to \theta_0$

## Privacy Amplification via Subsampling

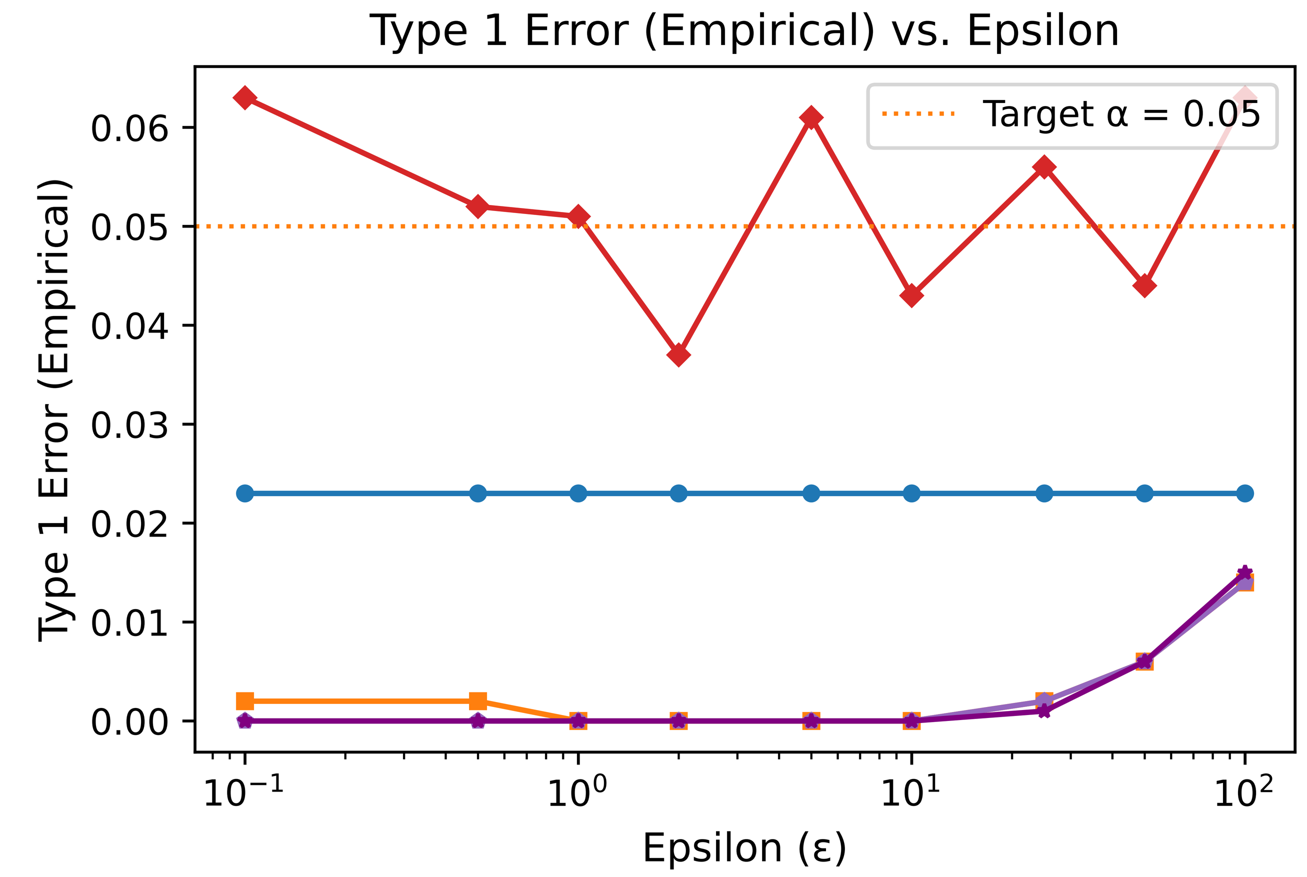
**Mechanism:** Include observations with probability $r$, leading to effective privacy amplification by factor $1/r$.
This practical improvement significantly reduces noise in high privacy contexts and better balances statistical hardness with privacy cost.

## Experimental Results

**Setting:** Bernoulli(0.3) vs Bernoulli(0.7), $\alpha = \beta = 0.05$, 1000 trials




On average, **DP-SPRT variants outperform** PrivSPRT (Zhang, Mei, and Cummings 2022) across privacy levels




**All DP-SPRT variants guarantee error control**, while PrivSPRT can violate error targets due to empirical tuning