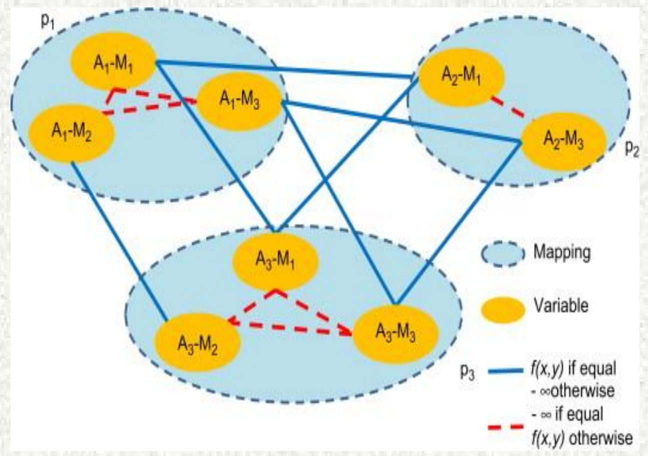
Differentially Private Multi-Agent Constraint Optimization

Sankarshan Damle, Aleksei Triastcyn, Boi Faltings and Sujit Gujar

The 2nd AAAI Workshop on Privacy-Preserving Artificial Intelligence
(PPAI-21)

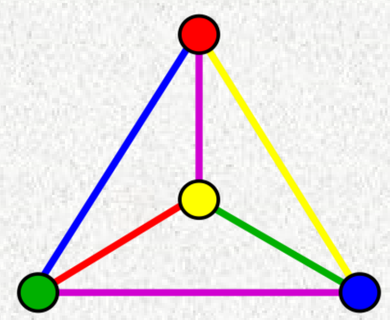
Goal

Designing a scalable DCOP algorithm that preserves constraint privacy from unrelated participants through distributed computation; and from related participants through differential privacy techniques

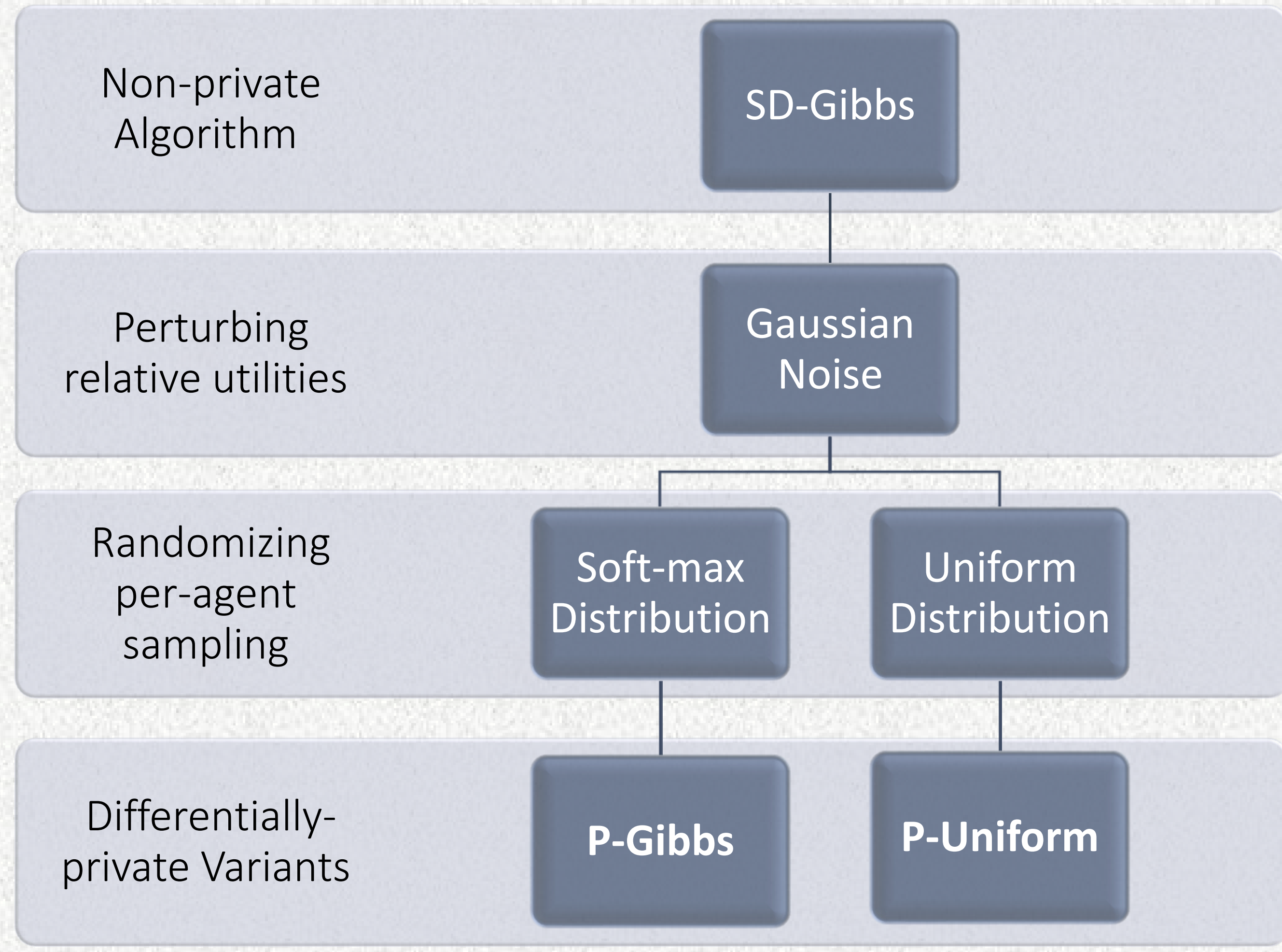


Challenges

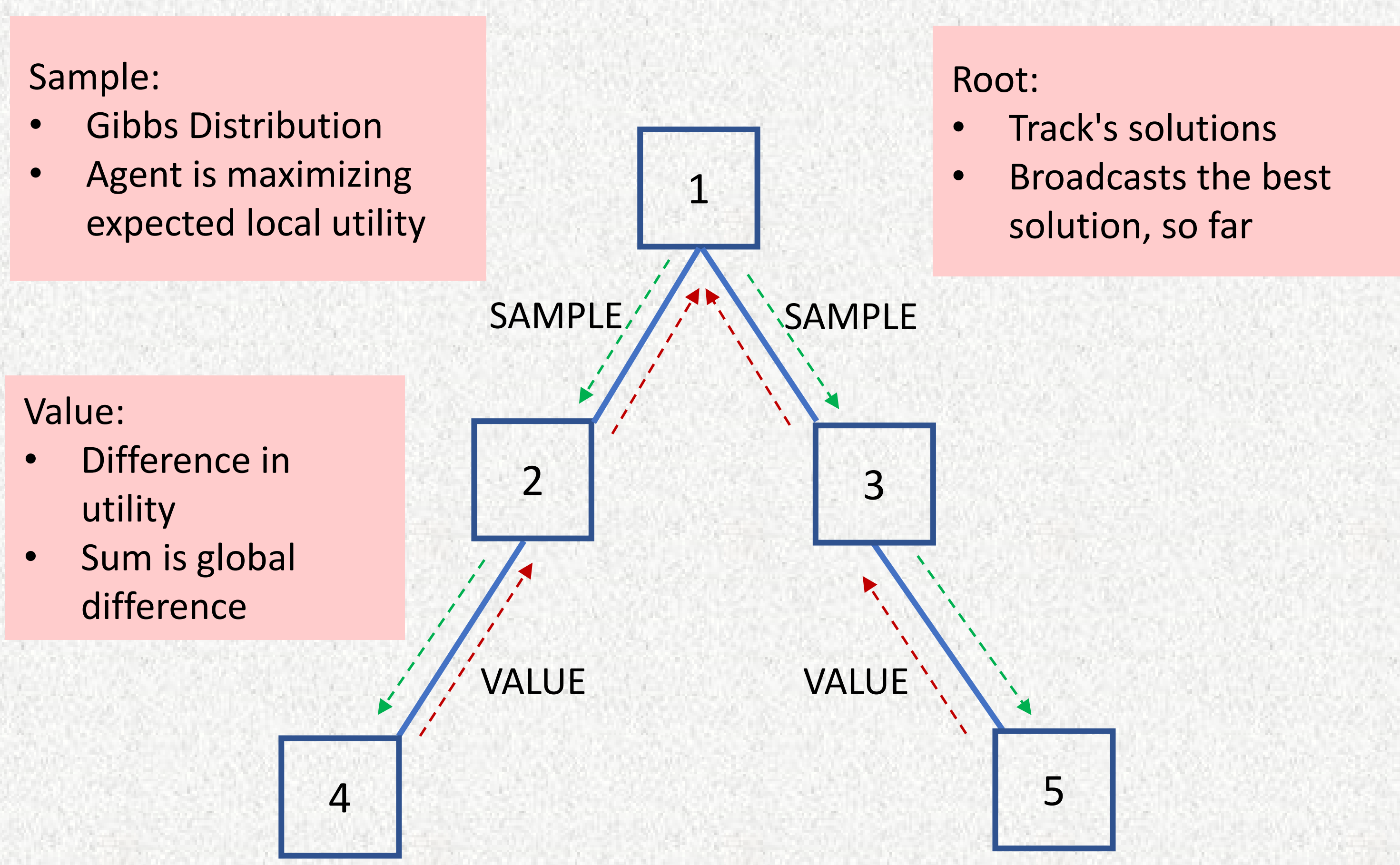
- Protecting information leak
    - during information exchange
    - from the final assignment
- Ensuring Scalability



Benchmark Problems in DCOP

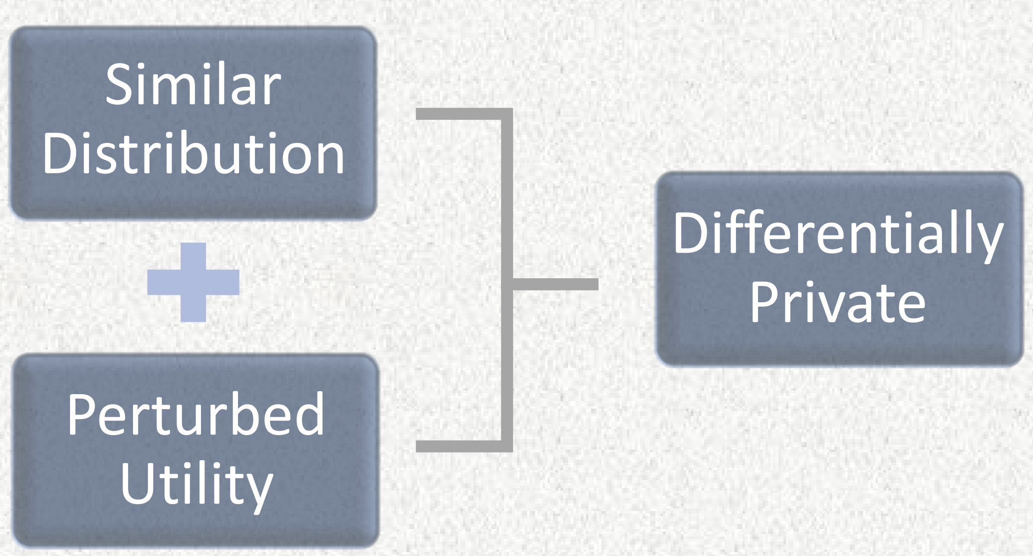


SD-Gibbs: Algorithm Framework [1]



Constraint Privacy loss due to,

1. Sampling
2. Difference in utility



(Assumption) Bounded Sampling Divergence. We assume that the *max-divergence* between the SD-Gibbs sampling distributions is bounded by Γ_∞, i.e.,

$$D_\infty(P_i || P_j) \le \Gamma_\infty$$

Applying the soft-max function with temperature γ, over P_i, we get,

$$\Gamma_\infty = 2/\gamma$$

Sensitivity. We define *sensitivity* as the maximum absolute difference between any two-relative utility, i.e.,

$$\tau = \max_{\{\Delta,\Delta'\}} |\Delta - \Delta'|$$

From sampling divergence assumption, we get,

$$\tau = 2\Gamma_\infty$$

P-Gibbs. The information leak due to sampling is bounded by Γ_∞

P-Uniform. As each agent samples uniformly, the information leak due to sampling is 0

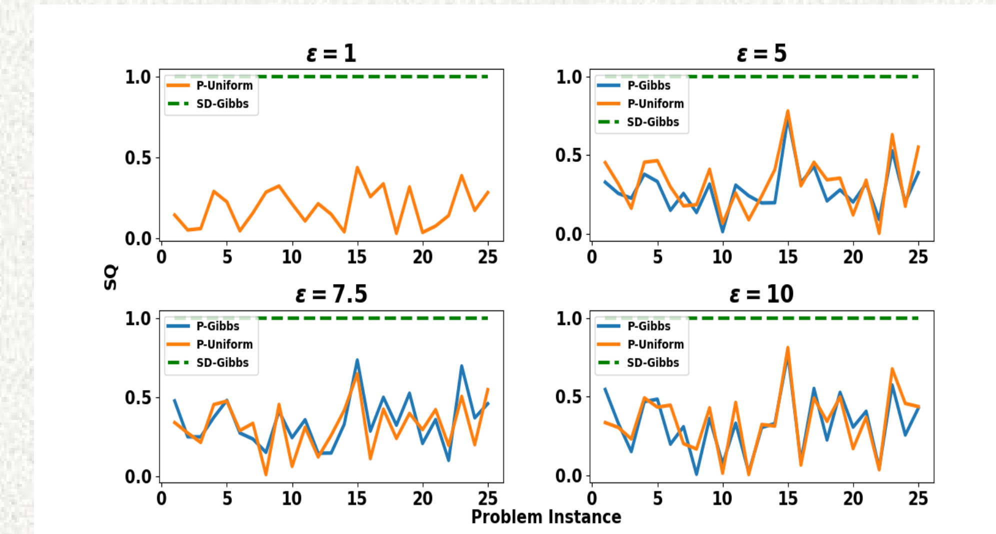
The (ϵ, δ) parameters for the Gaussian noise mechanism can be computed using either basic composition along with [2] or the moments accountant [3]

Summarizing the (ϵ, δ)-DP Bounds

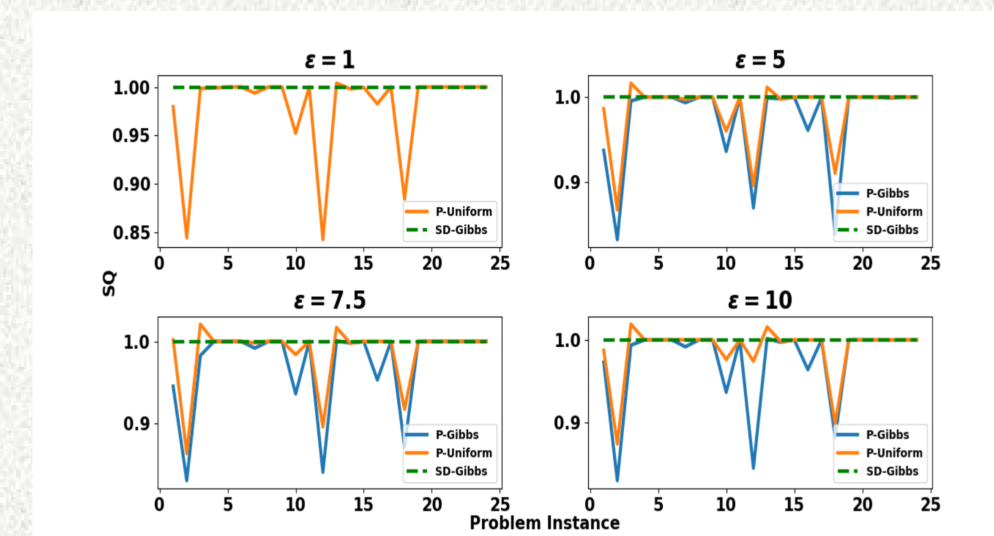
Algorithm	(ϵ_s, δ)	(ϵ_n, δ)	$(\epsilon = \epsilon_s + \epsilon_n, \delta)$ for T iterations
P-Gibbs	$(\Gamma_\infty, 0)$	$(\frac{\tau}{\sigma}\sqrt{2\ln\frac{1.25}{\delta}}, \delta)$	$\left(\frac{T}{\lambda}c_t^{(s)}(\lambda) + \frac{T}{\lambda}c_t^{(n)}(\lambda) - \frac{1}{\lambda}\ln\delta,\ \delta\right)$
P-Uniform	$(0, 0)$	$(\frac{\tau}{\sigma}\sqrt{2\ln\frac{1.25}{\delta}}, \delta)$	$\left(\frac{T}{\lambda}c_t^{(n)}(\lambda) - \frac{1}{\lambda}\ln\delta,\ \delta\right)$

Results

SQ for Graph-coloring



SQ for Meeting-schedule



Average SQ for Graph-coloring

Algorithm	ϵ	SQ (mean ± std)
P-Gibbs	5	0.281 ± 0.143
	7.5	0.348 ± 0.159
	10	0.324 ± 0.192
P-Uniform	1	0.190 ± 0.119
	5	0.322 ± 0.180
	7.5	0.321 ± 0.153
	10	0.341 ± 0.195

Average SQ for Meeting-schedule

Algorithm	ϵ	SQ (mean ± std)
P-Gibbs	5	0.973 ± 0.0513
	7.5	0.973 ± 0.051
	10	0.975 ± 0.0498
P-Uniform	1	0.979 ± 0.0475
	5	0.985 ± 0.0372
	7.5	0.987 ± 0.0373
	10	0.990 ± 0.0328

References

1. Nguyen, Duc Thien, William Yeoh, Hoong Chuin Lau, and Roie Zivan. "Distributed gibbs: A linear-space sampling-based dcop algorithm." Journal of Artificial Intelligence Research 64 (2019): 705-748.
2. Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science, 9(3-4), 211-407.
3. 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).
4. Triastcyn, Aleksei, and Boi Faltings. "Bayesian differential privacy for machine learning." In International Conference on Machine Learning, pp. 9583-9592. PMLR, 2020.