**Open Problem 2.3 (The planted clique problem)** *Let $G$ be a random graph constructed by taking a $G\left(n, \frac{1}{2}\right)$ and planting a clique of size $\omega$.*

1. *Is there a polynomial time algorithm that is able to find the largest clique of $G$ (with high probability) for $\omega \ll \sqrt{n}$. For example, for $\omega \approx \frac{\sqrt{n}}{\log n}$.*
2. *Is there a polynomial time algorithm that is able to distinguish, with high probability, $G$ from a draw of $G\left(n, \frac{1}{2}\right)$ for $\omega \ll \sqrt{n}$. For example, for $\omega \approx \frac{\sqrt{n}}{\log n}$.*
3. *Is there a quasi-linear time algorithm able to find the largest clique of $G$ (with high probability) for $\omega \leq \left(\frac{1}{\sqrt{e}} - \varepsilon\right)\sqrt{n}$, for some $\varepsilon > 0$.*

This open problem is particularly important. In fact, the hypothesis that finding planted cliques for small values of $\omega$ is behind several cryptographic protocols, and hardness results in average case complexity (hardness for Sparse PCA being a great example [BR13]).

# Reference

[BR13] Q. Berthet and P. Rigollet. Complexity theoretic lower bounds for sparse principal component detection. *Conference on Learning Theory (COLT)*, 2013.