Які основні переваги НШ (направленное шифрование) в кільці зрізаних поліномів та як вони можуть бути застосовані в протоколі «захищені дані»?

Переваги:

* Швидкість
* Безпека може бути доведена без використання евристичної випадкової моделі оракула
* Достатня стійкість від злому квантовим комп’ютером