1. A primitiva criptografia bit-commitment e transferência oblívia podem ser reduzidas uma à outra?

2. A primitiva criptográfica bit commitment pode ser implementada usando apenas one-way functions?

3. A primitiva criptográfica oblívios transfer pode ser implementada usando apenas one-way functions?

4. É impossível ler a informação armazenada num estado quântico sem a destruir?

5. Conjugated coding permite codificar duas mensagens de tal modo que lendo uma se destrói a outra?

6. Conjugated coding usa bases ortogonais?

7. Um gerador quântico de números aleatórios usa uma seed inviolável?

8. Um gerador de números quânticos pode ser usado como seed para um gerador pseudo-aleatório?

9. Os sistemas de distribuição de chaves quânticos usam sempre detetores de fotões únicos?

10. Os sistemas de distribuição de chaves quânticos usam dois canais quânticos?

11. Os sistemas de distribuição de chaves quânticos usam um canal quântico autenticado?

12. Os sistemas de distribuição de chaves quânticos usam um canal clássico secreto?

13. Os sistemas de distribuição de chaves quânticas distribuem pares de chaves simétricas?

14. Os sistemas de distribuição de chaves quânticas permitem substituir os sistemas de criptografia simétricos?

15. Os sistemas de distribuição de chaves quânticas permitem substituir os sistemas de criptografia publica?

16. A reconciliação inversa é usada em sistemas CV-QKD?

17. Os sistemas CV-QKD usam dois detetores de fotões únicos no recetor?

18. Dois fotões entrelaçados não podem ser separados espacialmente, i.e. viajam sempre pelo mesmo caminho?

19. O entrelaçamento nunca pode ser destruído?

20. O entrelaçamento permite aumentar o alcance dos sistemas de distribuição de chaves quânticas?

21. Os sistemas de distribuição de chaves quânticas device independent sem implementados apenas em software?

22. A polarização de um fotão é uma característica do fotão que permanece imutável ao longo do tempo?

23. O AES pode ser atacado em tempo polinomial por um computador quântico?

24. O RSA pode ser atacado em tempo polinomial por um computador quântico?

25. Com tecnologia quântica é possível prescindir da criptografia pública?

26. A criptografia pública é mais eficiente que a criptografia simétrica?

27. Num sistema de reconciliação inversa os erros são corrigidos pelo transmissor?

28. Os sistemas de computação segura multiagentes são baseados em computação quântica?

29. Os sistemas de computação segura multiagentes só usam criptografia pública?

30. Num sistema de computação segura baseado em tecnologia quântica a transferência oblívia é baseada no protocolo RSA?