

АТАКА ПАСИВНОГО ПЕРЕХОПЛЕННЯ ДЕКІЛЬКОХ ЗЛОВМИСНИКІВ НА ПІНГ-ПОНГ ПРОТОКОЛ З ПАРАМИ ПЕРЕПЛУТАНИХ КУБІТІВ

¹Державний університет інтелектуальних технологій і зв'язку

mail@suitt.edu.ua

Анотація. Виконано аналіз атаки пасивного перехоплення двох і більшого числа зловмисників на пінг-понг протокол з парами переплутаних кубітів та без квантового надцільного кодування. Отримано загальний рекурсивний вираз для ймовірності d виявлення атаки довільної кількості n зловмисників, що дозволяє обчислити цю ймовірність через відповідну ймовірність при атаці $n - 1$ зловмисників. ...

Ключові слова: квантова криптографія, пінг-понг протокол, ...

Захист інформації є однією з найважливіших проблем сучасного інформаційного суспільства. В останні десятиріччя активно розвивається новий напрямок захисту інформації – квантова криптографія, що є найбільш зрілою технологією в новітній області квантової інформатики. Одним з напрямків квантової криптографії є протоколи квантового прямого безпечного зв'язку (КПБЗ). ...

Висновки. ...

Література

1. Boström K., Felbinger T. Deterministic secure direct communication using entanglement // *Physical Review Letters*. 2002. Vol. 89, Issue 18. Art. 187902.
2. Cai Q.-Y., Li B.-W. Improving the capacity of the Boström–Felbinger protocol // *Physical Review A*. 2004. Vol. 69, Issue 5. Art. 054301.
3. Vasiliu E. V. Non-coherent attack on the ping-pong protocol with completely entangled pairs of qutrits // *Quantum Information Processing*. 2011. Vol. 10, No. 2. P. 189–202.