

# Informacja Kwantowa 1/2

## Seria 4

do oddania na 22.03.2013

Rozważmy protokół kryptografii kwantowej zwany protokołem sześćo-stanowym (6S). Do czterech stanów  $|\leftrightarrow\rangle$ ,  $|\updownarrow\rangle$ ,  $|\nearrow\rangle$ ,  $|\searrow\rangle$  używanych w BB84, dodajmy jeszcze stany  $|\odot\rangle$ ,  $|\ominus\rangle$  tworzące trzecią bazę. Protokół przebiega analogicznie do BB84 z tym że teraz  $A$  wysyła 6 różnych stanów każdy z prawdopodobieństwem  $1/6$  a  $B$  mierzy qubit przypadkowo w jednej z trzech baz.

- a) Jaka część bitów pozostanie  $A$  i  $B$  po wykonaniu procedury uzgodnienia baz
- b) Przeanalizuj atak typu intercept-resend w którym: atakujący atakuje część fotonów używając przypadkowo wybranej jednej z trzech baz. Poniżej jakiej wartości QBER możemy czuć się bezpieczni względem tego ataku.
- c) Przeanalizuj atak typu intercept-resend w którym: atakujący atakuje część fotonów wykonując pomiar rzutujący zawsze w tej samej bazie. Jaki powinien wybrać pomiar, żeby nie wyróżniał on żadnej z używanych baz (uogólnienie tego co robiliśmy na ćwiczeniach dla protokołu BB84, gdzie robiliśmy pomiar w bazie  $|22.5^\circ\rangle$ ,  $|112.5^\circ\rangle$ ). Poniżej jakiej wartości QBER możemy czuć się bezpieczni względem tego ataku. Który z ataków jest groźniejszy?