Quantum Pinball

Quantum Key Exchange allows a safe code transmission between Sender and Receiver. Data can be encoded with as qBit with a Spin as Value and a random base (sort of polarisation). A receiver uses a random base and measure the qBit (which destroys it). If guessed correct, he got the correct value, otherwise a random number. This is true both for the intended receiver as well as an attacker in between. The attacker has to therefore send a new qBit (the old one is destroyed) with the guessed (therefore maybe wrong) base to the receiver. After receiving a number of values, sender and receiver exchange public the used bases - and throw away the values where both used different ones. If they used the same one, the recieved and send values should be the same, unless an attacker was in the middle and guessed a different base. To detect this, they compare parts of the values public - and take the rest as code, if no attacker was detected.