Exercise 13 in Advanced Methods of Cryptography

Prof. Dr. Rudolf Mathar, Henning Maier, Markus Rothe

2015-02-06

Problem 40. *(using qubits to agree on a one time pad)* Alice and Bob wish to use 30 qubits in order to agree a one-time pad. Bob receives 30 qubits from Alice, and for each one he randomly applies + or × before measuring it. Subsequently Alice tells him what type she used for preparing each qubit. The results are as follows. The four rows in each block show the qubit number, Bob's measurement type, Bob's result and Alice's preparation type.

qubit	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Bob's type	+	+	×	×	+	×	×	+	+	+	×	+	×	+	+
result	1	1	0	0	1	0	1	0	0	1	1	0	1	1	1
Alice' type	×	×	×	×	×	+	×	×	×	+	×	×	+	×	×
qubit	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Bob's type	×	+	+	+	×	+	+	×	×	+	+	×	+	+	×
result	0	0	1	1	0	0	1	0	1	0	0	1	0	0	1
Alice' type	×	+	+	+	+	×	×	+	×	+	+	×	+	+	×

a) How long is their one-time pad, and what is it? What message does Bob send back to Alice?

Before they use their pad, they remember they should have checked to see if the qubits were intercepted. They decide they will sacrifice half of their useful qubits: the first, third, fifth and so on. When Alice tells Bob how she prepared them, it turns out that they were indeed just as Bob measured them.

b) What can they deduce about interception? What one-time pad do they end up with?

c) Suppose they want 20 bits in their one-time pad, and 99.9% certainty that Eve is not intercepting every qubit. How many qubits do they need to use?

d) Suppose they still want 20 bits for the one-time pad, but this time they want 95% certainty that Eve is intercepting no more than 10% of the qubits. How many qubits do they need?

Note: Exercise kindly adopted from *Quantum Computing and Cryptography* of *The University of Birmingham* (Spring Semester 2011, Exercises 4).