RWTH AACHEN UNIVERSITY Lehrstuhl für Theoretische Informationstechnik

Exercise 13 in Advanced Methods of Cryptography
- Proposed Solution -

Prof. Dr. Rudolf Mathar, Henning Maier, Markus Rothe
2015-02-06

Solution of Problem 40

a) The one-time pad has 16 bits. It is

$$0011100111001001\,.$$

Bob sends a message to Alice saying which are the useful bits. There are various ways he can do this. Qubit numbers of useful bits:

$$3, 4, 7, 10, 11, 16, 17, 18, 19, 24, 25, 26, 27, 28, 29, 30\,.$$

Alternatively, send a complete list of measurement types:

$$+ + \times \times + \times \times + + + \times + \times + + \times + + + \times + + \times \times + + \times + + \times\ .$$

b) Eight useful qubits were sacrificed for interception checking. Suppose they were all intercepted, so there would be a probability of 25% for each qubit that it gave the wrong measurement for Bob. Hence the probability of no discrepancies, i.e. the probability that Eve was lucky, is $\left(\frac{3}{4}\right)^8 \approx 0.1$. In practice Alice and Bob would want to use more qubits to get a better estimate of the risk, but if they went ahead with these their eight non-sacrifice qubits (the even numbered ones) would give a one-time pad of

$$01011001\,.$$

c) If Eve is intercepting every qubit, then on average 25% of the qubits will show a discrepancy if Alice and Bob compare values. For n check qubits, the probability that Eve will not be detected for any of them is $\left(\frac{3}{4}\right)^n$. For the 99.9% certainty we are looking for n large enough that $\left(\frac{3}{4}\right)^n < 0.001$. With a calculator we find we need $n \geq 25$.

It follows that Alice and Bob need 45 *useful* qubits: 20 for the pad and 25 sacrificed for detecting interceptions. Since on average only half the qubits are useful, they need 90 qubits altogether.

d) If Eve intercepts more than 10%, then on average at least 2.5% of the qubits will show a discrepancy. The probability of no discrepancy in n check qubits is 0.975^n, so for 95% certainty we want $0.975^n < 0.05$. By a calculator, $n > \frac{\log 0.05}{\log 0.975} \approx 120$.

For 140 useful qubits (20 for the pad, 120 to check), Alice and Bob need 280 qubits.