Advanced Cryptography: Quantum Cryptography

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

12. Exercise sheet
Hand in solutions until Monday, 31 January 2011, 23:59h.

Exercise 12.1 (B92). (9 points)

We will now discuss another protocol for secure key distribution, the so called B92 protocol, named after its inventor C. H. Bennet. There Alice selects randomly a classical bit a and sends to Bob

$$|\psi\rangle = \begin{cases} |0\rangle & \text{, if } a = 0 \\ \frac{|0\rangle+|1\rangle}{\sqrt{2}} & \text{, if } a = 1. \end{cases}$$

Bob in turn also creates randomly a classical bit a' and measures $|\psi\rangle$ either with respect to the Z basis (if $a' = 0$) or with respect to the X basis, obtaining a classical bit b.

(i) Restate the X and the Z basis. 2

Bob now publishes b.

(i) Show that if $b = 0$ then Bob learns nothing about the bit Alice sent. 2

(ii) Show that otherwise $a' = 1 - a$. 2

(iii) Generalize the protocol to multiple bit transmission. 3

Exercise 12.2 (Alternant codes). (19 points)

In the lecture we studied alternant codes. Here you will see such a code running! Any computer aided help might be a big advantage. Take the finite field $\mathbb{F}_{64} = \mathbb{F}_4[s]/(s^3 + s + 1)$ over $\mathbb{F}_4 = \mathbb{F}_2[r]/(r^2 + r + 1)$ that is an extension of degree $m = 3$. We construct an alternant code over $\mathbb{F}_4$ with $n = 9$ and $t = 2$.

(i) Compute which dimensions of the code are possible. 1

(ii) Now select two vectors $x, y \in \mathbb{F}_{64}$ with $x_i \neq x_j$ for $i \neq j$ and $y_i \neq 0$ for all i. Write down the matrix $H_t(x, y)$. 3

(iii) Give a basis of the vector space $\mathbb{F}_{64}$ over $\mathbb{F}_4$. 2

(iv) Now replace every entry in $H_t(x, y)$ as the (column) vector of coefficients when expressed in this basis, obtaining a matrix $\tilde{H}_t(x, y) \in \mathbb{F}_4^{km \times n}$. 3

(v) Compute a basis of the kernel of this matrix. 3

(vi) Now produce a list of all codewords. 3

(vii) Which minimum distance does your code have? 2

(viii) What does the theory say about the minimum disctance? 2

Exercise 12.3 (Dyadic matrices). (7 points)

Given a vector $v \in \mathbb{F}_q^n$ with n being a power of 2, the dyadic matrix $\Delta(v)$ is defined as

$$\Delta(v)_{ij} = v_{i \oplus j}$$

3 (i) Show that for $n > 1$ the matrix $\Delta(v)$ is of the form

$$\begin{bmatrix} A & B \\ B & A \end{bmatrix},$$

where A, B are dyadic matrices.

1 (ii) How much space do you need to store a dyadic matrix?

3 (iii) Give two proofs to show that the set of dyadic $n \times n$ matrices forms a commutative subring of the set of all $n \times n$ matrices over $\mathbb{F}_q$.