Prof. Dr.Werner Bley
Eva Brenner

24.10.2023

2. Übungsblatt Quantencomputing

Aufgabe 1 Sei N eine natürliche Zahl und $\omega := e^{2\pi i/N}$. Sei

$$A := \frac{1}{\sqrt{N}} \left(\omega^{jk}\right)_{0\leq j,k\leq N-1} \in \mathbb{C}^{N\times N}.$$

a) Zeige: A ist unitär.
b) Berechne A^{-1}.

Aufgabe 2 Seien X, V und W Vektorräume über dem Körper K von endlicher Dimension und sei $f\colon V \longrightarrow W$ eine lineare Abbildung. Wir nehmen an, dass X nicht der Nullraum ist. Zeigen Sie:
a) f surjektiv $\implies$ $id_X \otimes f\colon X\otimes V \longrightarrow X\otimes W$ surjektiv.
b) f injektiv $\implies$ $id_X \otimes f\colon X\otimes V \longrightarrow X\otimes W$ injektiv.
c) $V \neq 0 \implies X\otimes V \neq 0$.

Aufgabe 3 Die folgende Nachricht

$$[39333, 79897], [41845, 67922], [22349, 41118]$$

wurde mit dem ElGamal-Verfahren verschlüsselt. Dabei wurde in der Gruppe $G = (\mathbb{Z}/p\mathbb{Z})^\times$ mit $p = 101009$ gerechnet. Es wurden die Parameter $g = 3$ und $A = 5153$ verwendet.
Dabei wurde wie folgt vorgegangen: der alphanumerische Klartext wurde zu Gruppen von je 3 Buchstaben zusammengefasst. Jeder solchen Dreiergruppe xyz, $x, y, z \in \{A, B, \ldots, Z\}$ wurde die Zahl $W(xyz) := w(x)\cdot 26^2 + w(y)\cdot 26 + w(z) \bmod N$ zugeordnet, wobei

$$w : \{A, B, \ldots, Z\} \longrightarrow \{0, 1, \ldots, 25\}$$

jedem Buchstaben einen Wert anhand der Tabelle

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

zuordnet. $W(xyz) \in \mathbb{Z}/N\mathbb{Z}$ wurde dann mit ElGamal verschlüsselt.
Wie lautet die Nachricht?

Zu bearbeiten bis: Mi 02.11.2023