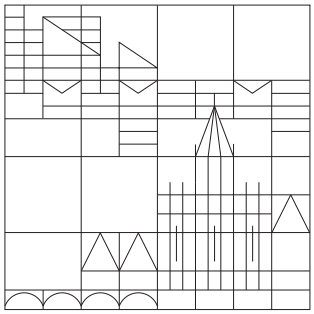
UNIVERSITÄT KONSTANZ
Fachbereich Physik
Prof. Dr. Guido Burkard
Dr. Mónica Benito
https://theorie.physik.uni-konstanz.de/burkard/teaching/19W-QI



Quanteninformationstheorie
Wintersemester 2019/2020 - Übungsblatt 3
Ausgabe: 8.11.2019, Abgabe: 15.11.2019, Übungen: 18/21.11.2019

Aufgabe 10 : Universalität des NAND-Gatters (3 Punkte)

Zeigen Sie, dass die AND, XOR, und NOT Gatter durch NAND-Gatter simuliert werden können, wenn Ancilla-Bits (Hilfsbits) und FANOUT zur Verfügung stehen.

Aufgabe 11 : Boolean functions (3 Punkte)

a) (1 Punkt) Schreiben Sie die Function XOR in disjunktiver Normalform.

b) (2 Punkte) Schreiben Sie die Abbildung

$$(x, y, z) \to (x + y, x + y + z) \bmod 2$$

in disjunktiver Normalform.

Aufgabe 12 : Komplexität der Multiplikation

Zeigen Sie, dass die Komplexität der Multiplikation von zwei n-Bit Zahlen $\mathcal{O}(n^2)$ ist.

Aufgabe 13: RSA-Protokoll (4 Punkte)

Alice würde es gern allen ermöglichen, ihr verschlüsselte Information zu senden, die nur sie entschlüsseln kann. Dafür nimmt sie zwei grosse Primzahlen p und q und berechnet das Produkt $N = p\,q$. Alice wählt ausserdem einen Kodierungsexponenten e, der folgende Bedingung erfüllt:

$$\mathrm{ggT}(e, (p-1)(q-1)) = 1.$$

ggT bezeichnet den grössten gemeinsamen Teiler. Der öffentliche Schlüssel ist damit (N, e). Um den geheimen Schlüssel zu bekommen, findet Alice den Dekodierungsexponenten aus der folgenden Gleichung:

$$e\,d = 1 \mod [(p-1)(q-1)]. \tag{1}$$

Damit ist der geheime Schlüssel (d, p, q). Die verschlüsselte Nachricht ist nun $c = m^e \mod N$, wobei m die Nachricht ist, und $m < N$ erfüllt sein muss. Die Entschlüsselung erfolgt nach der Formel $m = c^d \mod N$.

a) (2 Punkte) Benutzen Sie das Euler-Theorem, zusammen mit der Gleichung (1) und den algebraischen Eigenschaften des Modulus, um sich zu vergewissern, dass $c^d \mod N = m$. Das Euler-Theorem besagt, dass für beliebige Primzahlen p und q und eine natürliche Zahl m gilt

$$m^{(p-1)(q-1)} = 1 \mod p\,q, \quad \text{falls} \quad \mathrm{ggT}(m, p\,q) = 1; \tag{2}$$
$$m^{q-1} = 1 \mod q, \quad \text{falls} \quad \mathrm{ggT}(m, q) = 1. \tag{3}$$

Die folgende Eigenschaft des Modulus ist ebenfalls nützlich:

$$x^s \mod N = (x \mod N)^s \mod N. \tag{4}$$

b) (2 Punkte) Benutzen Sie das in a) beschriebene RSA-Protokoll um eine Nachricht zu verschlüsseln und wieder zu entschlüsseln. Nehmen Sie z.B. $p = 7$, $q = 11$ und $e = 37$. In diesem Fall ist dann $d = 13$. Nehmen Sie $m = 2$ und finden Sie die verschlüsselte Nachricht c und daraus m wieder. Die Rechnung kann man mit einem normalen Taschenrechner durchführen, wenn man die Eigenschaft (4) benutzt.