Übung Kryptographie

Iryna Karpenko, Gerald Teschl

SS2023

Weitere Details finden Sie in den Unterlagen zur Vorlesung.

1. Man nennt $\varphi(m) = \textit{Anzahl der Elemente von } \mathbb{Z}_m^*$ die **Euler'sche Phi-Funktion**.
   Geben Sie an: $\varphi(4)$, $\varphi(5)$, $\varphi(9)$, $\varphi(26)$, $\varphi(29)$, $\varphi(37)$.

2. Der **Kleine Satz von Fermat** besagt:
   Für jede ganze Zahl a und jede Primzahl p, die teilerfremd zu a ist, gilt:

   $$a^{p-1} = 1 \mod p.$$

   Berechnen Sie mithilfe des Kleinen Satzes von Fermat:
   a) $9^{20} \mod 11$ b) $23^{80} \mod 11$ c) $57^{372} \mod 11$

3. Berechnen Sie mithilfe des erweiterten Euklid'schen Algorithmus das multiplikative Inverse von a in $\mathbb{Z}_m$:
   a) $a = 7$ und $m = 26$ b) $a = 19$ und $m = 999$

4. **Beschleunigung mithilfe des Chinesischen Restsatzes:** Angenommen, ein Computer kann nur zweistellige ganze Zahlen *effizient* verarbeiten. Sie möchten aber auch dreistellige Zahlen effizient darstellen, addieren und multiplizieren. Verwenden Sie dazu die drei (paarweise teilerfremden) Module $m_1 = 97$, $m_2 = 98$ und $m_3 = 99$ und den Chinesischen Restsatz. Gesucht ist zum Beispiel Summe und Produkt von 203 und 125.
   a) Stellen Sie 203 und 125 durch ihre Reste bezüglich der Module dar („Transformation").
   b) Berechnen Sie in dieser Darstellung die Summe und das Produkt von 203 und 125 (effiziente Berechnung).
   c) Stellen Sie Summe bzw. Produkt mithilfe des Chinesischen Restsatzes wieder in Dezimaldarstellung dar („Rücktransformation").

5. Zeigen Sie: (i) Wenn p eine Primzahl ist, so hat die Gleichung $x^2 = 1 \pmod p$ nur die Lösungen $x = 1 \pmod p$ und $x = -1 \pmod p$ (Tipp: $x^2 - 1 = (x-1)(x+1)$).

   (ii) Wenn p eine Primzahl ist, so gilt $(p-1)! = -1 \pmod p$. (Tipp: (i) bedeutet, dass in $\mathbb{Z}_p$ nur 1 und $p-1$ gleich ihrem multiplikativen Inversen sind.)

6. **Affine Doppelverschlüsselung**: Wird die Sicherheit durch Hintereinanderausführung (Verkettung) $(E_2 \circ E_1)(x)$ zweier affiner Chiffren $E_1(x) = (a \cdot x + b) \mod n$ und $E_2(x) = (c \cdot x + d) \mod n$ erhöht?

   a) Zeigen Sie, dass dies *nicht* so ist, indem Sie eine affine Einfachverschlüsselung $E_3(x) = (e \cdot x + f) \mod n$ angeben, die *dieselbe* Ver- und

Entschlüsselung durchführt wie die Doppelverschlüsselung $(E_2 \circ E_1)(x)$.

b) Geben Sie e und f an für $a = 3$, $b = 5$, $c = 11$, $d = 7$ und $n = 26$.

c) Verschlüsseln Sie den Buchstaben F zunächst mit $(E_2 \circ E_1)(x)$ und danach mit $E_3(x)$ und überzeugen Sie sich von der Gleichwertigkeit.

d) Wie groß ist der Schlüsselraum, den ein Angreifer bei einem Brute-Force Angriff durchsuchen muss, wenn er weiß, dass eine affine Doppelverschlüsselung angewendet wurde?

7. **Hill-Chiffre**: Ein Klartext $x_1, x_2, x_3, \ldots$ über dem Alphabet $\mathbb{Z}_n$ wird in Blöcke von je zwei Buchstaben zerlegt, also (x_1, x_2), (x_3, x_4), $\ldots$, und mithilfe Matrixmultiplikation blockweise verschlüsselt:

$$\begin{pmatrix} y_i \\ y_{i+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_i \\ x_{i+1} \end{pmatrix}, \quad i = 1, 3, 5, \ldots$$

Dabei sind $a, b, c, d \in \mathbb{Z}_n$ die Bestandteile des geheimen Schlüssels.
a) Verwenden Sie das Alphabet $\mathbb{Z}_n = \mathbb{Z}_{27}$ und verschlüsseln Sie die Nachricht $x_1, x_2, x_3, x_4 = 11, 5, 24, 2$ mit dem Schlüssel $(a, b, c, d) = (4, 2, 3, 5)$.
b) Berechnen Sie über $\mathbb{Z}_{27}$ die inverse Matrix zu

$$A = \begin{pmatrix} 4 & 2 \\ 3 & 5 \end{pmatrix}$$

und geben Sie dann die Entschlüsselungsvorschrift zu a) an.
c) Können Alice und Bob grundsätzlich bei der Vereinbarung eines geheimen Schlüssels beliebige Zahlen $a, b, c, d \in \mathbb{Z}_n$ wählen?

8. **Known Plaintext Angriff**: Gegeben ist eine Hill Chiffre über dem Alphabet $\mathbb{Z}_{27} = \{0, \ldots, 26\}$ bzw. {`A, B, ..., Z, :`} (d.h., es wird zu den 26 Buchstaben als 27. Zeichen der Doppelpunkt „:“ hinzugefügt):

$$\begin{pmatrix} y_i \\ y_{i+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_i \\ x_{i+1} \end{pmatrix}, \quad i = 1, 3, 5, \ldots,$$

mit $a, b, c, d \in \mathbb{Z}_{27}$. Sie als Angreifer wissen, dass der Geheimtext

`WM:LJTZPJIGURIQDLDXWFJMYLXDCIX`

mit diesem Algorithmus verschlüsselt wurde und außerdem, dass die ersten vier Zeichen `FROM` bedeuten.
a) Wie können Sie mit diesem Wissen a, b, c, d berechnen?
b) Von wem stammt der Funkspruch?

9. **Ciphertext Only Attack**: Gegeben ist folgender Geheimtext.

```
IMDGYWAQZZQZUZRADYMFUWQDNQEEQDDQOTZQZMXEYMFTQYMFUWQDIQUXEUQY
UFUTDQZLQTZRUZSQDZNUEFMGEQZPHUQDGZPLIMZLUSLMQTXQZWAQZZQZ
```

Sie wissen, dass er aus einem deutschen Klartext durch eine Cäsarverschiebung $y = (x + e) \mod 26$ entstand.
a) Finden Sie den geheimen Schlüssel e.
b) Was erfahren wir hier über InformatikerInnen?

10. **Known plaintext Angriff**: Der Geheimtext

$$\{111, 66, 75, 75, 72, 7, 80, 72, 85, 75, 67, 6\}$$

entstand durch xor-Verschlüsselung $y = x \oplus e$ eines englischen Textes über dem Alphabet $\mathbb{Z}_{256}$. Sie wissen, dass 111 zu H (= 72 im ASCII Code) entschlüsselt wird. Entschlüsseln Sie den gesamten Geheimtext.

11. Beweisen Sie die Komplementeigenschaft eines Feistelnetzwerks E_k:

$$\overline{E_k(x)} = E_{\overline{k}}(\overline{x}),$$

wobei $\overline{x}$ das bitweise Komplement von x bezeichnet ($\overline{010} = 101$, etc.). Die Schlüssellänge von Feistel-Netzwerken (DES, S-DES) ist also effektiv um 1 reduziert. (Hinweis: Was passiert beim bitweisen Komplement einer XOR-Verknüpfung?)

12. Schreiben Sie die klassischen Logikfunktionen $NOT(x_1)$, $OR(x_1, x_2)$, $AND(x_1, x_2)$, $XOR(x_1, x_2)$ als Polynome in $\mathbb{Z}_2$. Welche dieser Funktionen sind linear?

13. Betrachten Sie die S-Box $\mathbb{Z}_2^3 \to \mathbb{Z}_2^3$ die durch folgende Vorschrift gegeben ist:

$$\begin{aligned} y_1 &= x_1x_2 + x_1x_3 + x_2x_3 + x_2 + x_3 + 1 \\ y_2 &= x_1x_2 + x_1x_3 + x_2x_3 + x_1 + x_3 + 1 \\ y_3 &= x_1x_2 + x_1x_3 + x_2x_3 + x_1 + x_2 + 1 \end{aligned}$$

Diese S-Box ist offensichtlich nichtlinear und jedes Eingangsbit x_j beeinflusst jedes Ausgangsbit x_k. Würden Sie diese S-Box in einer Verschlüsselungsvorschrift verwenden?

14. Berechnen Sie die Abhängigkeitsmatrix von

$$\begin{aligned} y_1 &= x_1x_2 + x_1x_3 + x_2x_3 + x_2 + x_3 + 1 \\ y_2 &= x_1x_2 + x_1x_3 + x_2x_3 + x_1 + x_3 + 1 \\ y_3 &= x_1x_2 + x_1x_3 + x_2x_3 + x_1 + x_2 + 1 \end{aligned}$$

15. **SubBytes-Transformation bei AES:** Gegeben ist der Zustand

$$\begin{pmatrix} 00 & 00 & 00 & C3 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \end{pmatrix}.$$

Berechnen Sie das Ergebnis der SubBytes-Transformation und kontrollieren Sie am Ende mithilfe der Tabelle (Figure 7) in der AES Dokumentation FIPS197. Hinweis: $(x^7 + x^6 + x + 1)(x^7 + x^5 + x + 1) = 1$ modulo $m(x) = x^8 + x^4 + x^3 + x + 1$.

16. Berechnen Sie die Biastabelle der nichtlinearen Funktion

$$\begin{aligned} y_1 &= x_1 + x_2 + x_1x_2 \\ y_2 &= x_2 + x_1x_2 \end{aligned}$$

Gibt es lineare Beziehungen zwischen den Variablen?

17. Gibt es eine nichtaffine invertierbare S-Box $\mathbb{Z}_2^2 \to \mathbb{Z}_2^2$?
Hinweis: Wie viele invertierbare affine Funktionen gibt es?

18. Verwenden Sie die Beziehung

$$x_1 + x_3 + x_4 + y_2 = 0,$$

für den zweiten Teil der S-Box $S^2 : x_1x_2x_3x_4 \mapsto y_1y_2$ beim S-DES um eine affine Beziehung für den S-DES zu finden.

19. Wie viel Speicher wird für einen Meet-in-the-Middle-Angriff auf 3DES benötigt?

20. Betrachten Sie folgendes einfache Verfahren mit einer großen S-Box und einer Runde:

$$E_k(x) = (X_k \circ S)(x)$$

Hier ist $X_k(x) = x \oplus k$ die Schlüsseladdition (per XOR) und S die (invertierbare) S-Box.

Ist dieses Verfahren sicher, wenn die Block-/Schlüssellänge genügend groß und die (nichtlineare) S-Box gut gewählt ist? Wenn nicht, wie könnte es angegriffen werden? Wäre es besser die Operationen zu vertauschen (also $E_k(x) = (S \circ X_k)(x)$) oder überhaupt gleich zwei S-Boxen zu verwenden (also $E_k(x) = (S_2 \circ X_k \circ S_1)(x)$)? Wie sieht es aus, wenn Key-Whitening verwendet wird (also $E_k(x) = (X_k \circ S \circ X_k)(x)$)?

21. Für die Diffie–Hellmann Schlüsselvereinbarung sei $g = 4$ (also kein Generator in $\mathbb{Z}_{11}^*$) und $p = 11$: Homer und Bart erzeugen einen gemeinsamen Schlüssel, Lisa belauscht die Kommunikation und erfährt dadurch $\alpha = 9$ und $\beta = 5$. Wie kommt sie (durch einen Brute Force Angriff) nun besonders leicht an den geheimen Schlüssel von Homer und Bart und wie lautet dieser geheime Schlüssel?

22. Für die Elgamal-Verschlüsselung sei $g = 7$, $p = 11$. Alice gibt als öffentlichen Schlüssel $\alpha = 2$ bekannt.

a) Bob möchte die Nachricht $x = 8$ verschlüsselt an Alice schicken. Wie geht er vor? (Gehen Sie davon aus, dass er als geheimen Schlüssel $b = 6$ wählt.)

b) Alice erhält die verschlüsselte Nachricht $(c, \beta) = (6, 4)$ von Bob. Wie entschlüsselt sie (ihr geheimer Schlüssel ist $a = 3$)?

23. Beweisen Sie, dass für $a, b \in G$ die Gleichung

$$\log_a(b) \log_b(a) = 1 \pmod{\operatorname{ord}(a)}$$

gilt, sofern beide Logarithmen existieren.

24. Für das Elgamal-Verfahren sei $g = 7$, $p = 11$: Bart gibt als öffentlichen Schlüssel $\alpha = 3$ bekannt. Homer schickt an Bart $(\beta, c_1) = (8, 2)$ und $(\beta, c_2) = (8, 9)$ (er hat also offensichtlich den Fehler begangen und für beide Nachrichten dieselbe Zufallszahl verwendet). Lisa erfährt nun irgendwie, dass $c_1 = 2$ den Klartext $x_1 = 6$ bedeutet. Wie kann sie mithilfe eines Klartextangriffes den Schlüssel k (oder gleich den inversen Schlüssel k^{-1}) ermitteln und somit auch c_2 entschlüsseln? Wie lautet x_2?

25. Beweisen Sie, dass die Schwierigkeit des DLP in $\mathbb{Z}_p^*$ unabhängig vom verwendeten Generator ist. (Hinweis Beispiel 5.22)

26. Zeigen Sie: Jede Sophie-Germain-Primzahl $q > 3$ erfüllt $q = 5 \pmod 6$ und jede Safe-Prime $p > 7$ erfüllt $p = 11 \pmod{12}$.

27. Berechnen Sie $\log_2(12)$ in $\mathbb{Z}_{13}^*$ mit der Pohlig-Hellman Reduktion.

28. Alice besitzt den privaten RSA-Schlüssel $(n, d) = (187, 107)$ (mit Primzahlen $p = 11, q = 17$). Sie erhält von Bob den Geheimtext $y = 126$. Wie entschlüsselt Sie, beschleunigt mithilfe des Chinesischen Restsatzes?

29. Homer und Bart haben die öffentlichen Schlüssel $(2021027, 17)$ und $(2021027, 23)$. Wie kann Bart aus seinem geheimen Schlüssel $(2021027, 135665)$ den von Homer berechnen (ohne Faktorisieren)?

30. Der öffentliche Schlüssel von Homer ist $(2029039, 1350683)$ und den privaten hat er verloren. Kann ihm (ohne Faktorisieren) geholfen werden? (Hinweis: Er kennt den Wiener-Angriff nicht.)

31. Alice besitzt den privaten RSA-Schlüssel $(n, d) = (1147, 149)$. Sie erhält von Bob den Geheimtext:

    233, 286, 815, 24, 187, 94, 992, 992, 187, 844, 919, 711, 103, 573, 418, 286, 307, 187, 1067, 103, 591

    Dieser wurde mittels RSA und OAEP verschlüsselt. Dazu wurde die originale Nachricht zuerst in ASCII codiert (8 Bit Blöcke) und mittels OAEP zu 10 Bit Blöcken verschlüsselt. Die Umwandlung zwischen 10 Bit Blöcken und Zahlen erfolgt, indem man die 10 Bit als Stellen im Dualsystem betrachtet. Als Hashfunktion wurde $G(x) = (x^2 \mod n) \mod 2^8$ und $H(x) = (x^2 \mod n) \mod 2^2$ verwendet. (Hinweis: Falls Sie von Hand rechnen reicht es, den ersten Buchstaben zu entschlüsseln. Sie können aber auch ein kleines Programm schreiben.)

32. Der RAS-Modul sei $n = 14351 = 113 \cdot 127$ und der öffentliche Schlüssel $e = 5$.

    a) Was ist der Wiederherstellungsexponent von $x = 2$?
    b) Was ist der größtmögliche Wiederherstellungsexponent und gibt es ein x, das diesen realisiert?

33. a) Es sei $n = p \cdot q$ das Produkt zweier Primzahlen $p > q$. Wie viele Möglichkeiten gibt es n in der Form $n = a^2 - b^2$ mit $a, b > 0$ zu schreiben?
    b) Faktorisieren Sie $n = 1363$ mit der Methode von Fermat.

34. Faktorisieren Sie $n = 3473$ mit der $p - 1$ Methode.

35. Testen Sie mithilfe des Fermat-Tests, ob n eine Primzahl ist.
    a) $n = 2821$ b) $n = 809$
    Wählen Sie jeweils: $a = 2, 3, 5, 7$. Wie entscheidet der Test?

36. Die Systemparamter für die Schnorr-Signatur seien $(p, g, m) = (167, 4, 83)$ und die Hashfunktion sei die Buchstabensumme modulo 128. Ihr geheimer Schnorr-Schlüssel sei $a = 33$, Ihr öffentlicher Schlüssel ist $\alpha = 29$.
    a) Signieren Sie die Nachricht „FAD“.
    b) Wie überprüft Bob, ob die Signatur echt ist?

37. Die Systemparamter für Elgamal seien $(p, g) = (167, 4)$ und die Hashfunktion sei die Buchstabensumme modulo 128. Homer hat den öffentlichen Schlüssel $\alpha = 62$ und die Nachricht „Nuclear“ mit $(54, 110)$ und die „Doughnut“ mit $(54, 78)$ signiert. Was hat Homer falsch gemacht? Wie lautet sein geheimer Schlüssel? Ist er eindeutig?

38. a) Finden Sie heraus, welche CAs Ihr Webbrowser akzeptiert.
b) Welche CA hat das Zertifikat des Webservers der Uni Wien unterschrieben? Wann läuft es ab?

39. a) Finden Sie heraus welche elliptischen Kurven openssl unterstützt.
b) Erzeugen Sie einen privaten Schlüssel (aus Kompatibilitätsgründen mit secp256k1 oder secp384r1).
c) Erzeugen Sie einen Certificate Signing Request (CSR).
d) Welche Möglichkeiten gibt es ein Gratis-Zertifikat zu bekommen? Berichten Sie über Ihre Erfahrungen.
d) (optional) Führen Sie mit openssl den privaten Schlüssel und das Zertifikat zusammen und importieren sie diese in ihren Email-Client.

40. Erzeugen Sie mit gpg eine signierte Textnachricht
a) im default gpg-Format
b) klartextsigniert (zum Versenden als Email)
c) mit extra Signaturfile (detached signature).
Überprüfen Sie diese Signaturen.

41. Berechnen Sie (wenn möglich) die Wurzeln von:
a) $a = 3$ in $\mathbb{Z}_{11}$ b) $a = -1$ in $\mathbb{Z}_{13}$

42. Betrachten Sie das Rabin-Kryptosystem mit n einer Blum-Zahl, also ein Produkt aus zwei Primzahlen die Rest 3 bei Division mit 4 ergeben. Zeigen Sie: Ist x eine Quadratzahl bezüglich n, dann kann man leicht mit $y^{((p-1)(q-1)+4)/8} = x$ entschlüsseln und x ist die einzige Wurzel von $y = x^2$ mit dieser Eigenschaft. (Hinweis: Verwenden Sie das Legendresymbol in $\mathbb{Z}_p$ und $\mathbb{Z}_q$.)

43. Gegeben ist die elliptische Kurve $E : y^2 = x^3 + 3x + 6$ über $\mathbb{Z}_7$, die aus folgenden vier Punkten besteht: $E = \{\mathcal{O}, (3, 0), (6, 3), (6, 4)\}$.
a) Geben Sie zu jedem Punkt dessen Ordnung an.
b) Geben Sie zu jedem Punkt die von ihm erzeugte Untergruppe an.

44. **ECDH:** Gegeben ist die elliptischen Kurve $E : y^2 = x^3 + x + 6 \mod 11$ und der Punkt $G = (2, 4)$. Alice wählt $a = 6$ und Bob wählt $b = 3$. Wie gehen Alice und Bob beim Diffie Hellman Schlüsselaustausch vor (geben Sie die einzelnen Schritte an) und welchen gemeinsamen geheimen Punkt C vereinbaren sie?

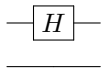
    (Tipp: Sobald Sie die Punktaddition mit der Hand beherrschen, können Sie die Rechenarbeit auslagern z.B. mithilfe `http://www.christelbach.com/eccalculator.aspx`).

45. **Doublespending bei Bitcoin** Da gültige Hashwerte für einen Block durch zufälliges Probieren gefunden werden, kann man davon ausgehen, dass die Zeit bis zu deren Auffinden exponentialverteilt ist:

$$T_1 \sim \mathcal{E}(\alpha).$$

Hierbei ist α die durchschnittliche Zeit, die zum Auffinden benötigt wird.
a) Wie ist die Zeit T_n zum Auffinden von n-Blöcken verteilt?
b) Wenn Mallory mit einer Rate β Hashwerte finden kann, was ist die Wahrscheinlichkeit, dass Mallory n-Blöcke schneller findet, als der Rest?
(Hinweis: Integrale dürfen gerne mit CAS/Tabellen berechnet werden.)

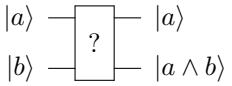
46. Berechnen Sie den Zustand von $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ nach Durchlaufen des Schaltkreises,



der durch die Matrix $H \otimes \mathbb{I}_2$ beschrieben wird.

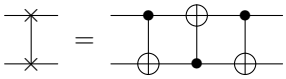
47. a) Geben Sie alle unitären Transformationen U an, die den Zustand $|1\rangle$ auf $\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle$ abbilden.
b) Wie lauten speziell alle *reellen* Transformationen, die $|1\rangle$ wie gewünscht abbilden?

48. Kann man mit einem Quantengatter eine logische UND Verknüpfung in der folgenden Form realisieren?

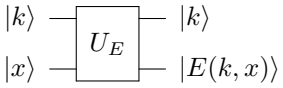


Wenn nein, wie könnte man das machen?

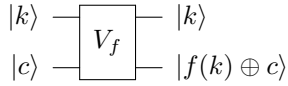
49. Zeigen Sie, dass das SWAP-Gatter mit zwei CNOT- und einem umgedrehten CNOT-Gatter realisieren werden kann:



50. Angenommen Sie haben bereits den Verschlüsselungsalgorithms $y = E(k, x)$ als Quantenorakel



implementiert (etwaige Ancilla-Qubits sind hier nicht mehr explizit angeführt). Nun hat ihre Auslandsabteilung das Klar-/Geheimtextpaar $x = 0$, $y = 1$ ausgespäht. Implementieren Sie ein Quantenorakel von der Form



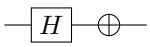
mit $f(k) = 1$ für $1 = E(k, 0)$ und $f(k) = 0$ sonst. Wie erhalten Sie daraus ein Phasenorakel

$$U_f|k\rangle = (-1)^{f(k)}|k\rangle,$$

wie sie es für den Grover-Algorithmus brauchen? Sie sollten mit CNOT, X und H auskommen.

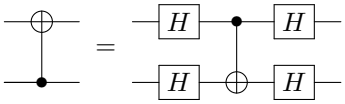
Optional: Testen Sie ihren Code mit einem Simulator (z.B. `https://qiskit.org`).

51. Durch welche Matrix wird der folgende Schaltkreis beschrieben?



52. Zeigen Sie, dass zwei antipodale Zustände auf der Blochkugel orthogonal sind. (Zwei Punkte auf einer Kugel sind antipodal, wenn sie auf einer Geraden durch den Mittelpunkt liegen. Die Kugelkoordinaten zweier antipodaler Punkte sind (φ, θ) und $(\varphi + \pi, \pi - \theta)$.)

53. Zeigen Sie dass das umgedrehte CNOT-Gatter wie folgt realisiert werden kann:



54. Zeigen Sie, dass für die Pauli-Matrizen

$$\sigma_a \sigma_b = \mathrm{i}\sigma_c$$

für $abc \in \{xyz, zxy, yzx\}$ gilt. Zeigen Sie weiter

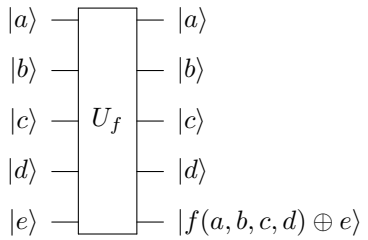
$$\sigma_a \sigma_b = \begin{cases} \mathbb{I}_2, & a = b, \\ -\sigma_b \sigma_a, & a \neq b. \end{cases}$$

Die 16 Matrizen

$$\{\pm\mathbb{I}_2, \pm\mathrm{i}\mathbb{I}_2, \pm\sigma_x, \pm\mathrm{i}\sigma_x, \pm\sigma_y, \pm\mathrm{i}\sigma_y, \pm\sigma_z, \pm\mathrm{i}\sigma_z\}$$

bilden also eine Gruppe, die **Pauli-Gruppe**.

55. Entwerfen Sie ein Quantenorakel



mit $f(a, b, c, d) = 1$ falls $a = b$, $c = d$ und $f(a, b, c, d) = 0$ sonst.

56. Ist die Menge $\mathcal{L} = \{\mathbf{a} \in \mathbb{Z}^2 | a_1 + a_2 = 0 \mod 2\}$ ein Gitter? Wenn ja, geben Sie eine Basis an.

57. Lösen Sie das CVP für $\mathbf{x} = (29.2, 3.4)$ näherungsweise mit dem Rundungsalgorithmus bezüglich beider Basen aus Beispiel 9.5 aus dem Skriptum.

58. Lösen Sie das CVP aus der letzten Aufgabe mit der Basis V näherungsweise mit dem Babai-Näheste-Ebene-Algorithmus.

59. Zeigen Sie, dass die Gitterbasis

$$U = \begin{pmatrix} 1 & 1 \\ \sqrt{3} & -\sqrt{3} \end{pmatrix}$$

längenreduziert ist und Gleichheit in der Ungleichung in Satz 9.10 aus dem Skriptum annimmt.

60. Zeigen Sie: Gilt für $\mathbf{x} \in \mathbb{R}^n$ und $\mathbf{a} \in \mathcal{L}$

$$\|\mathbf{x} - \mathbf{a}\| \leq \frac{\lambda_1(\mathcal{L})}{2},$$

dann kann es keinen näheren Gittervektor geben und wir haben das CVP gelöst.