Identification & Privacy Enhanced Technologies

Jan Arends

Hochschule Bonn-Rhein-Sieg

M.Sc. Computer Science

Sommersemester 2019

Inhalt

Übungsblatt 1 –
Biometrie

1. Was sollen **biometrische Systeme** leisten?
   - Personidentifikation & -Verifikation
   - (Automatisierte Erkennung von Personen anhand ihrer körperlichen Merkmale)

Auf welcher **prinzipiellen Basis** funktionieren diese?
   - Physiologischer/ körperliche/ biologischer/ persönlicher Merkmalen
   - Biometrische Eignungsmerkmale:
     - Beständig
     - Eindeutig
     - Technisch erfassbar
     - Universal
   - Beispiele: Finger, Gesicht, Iris, (Ohr), Venen

2. Begrifflichkeiten Identifikation und Verifikation:
   - Ziel einer biometrischen Erkennung ist stets, die **Identität einer Person zu ermitteln** (Identifikation) oder **die behauptete Identität zu bestätigen oder zu widerlegen** (Verifikation).

     Identifikation = 1: n Vergleich (Identifikation einer Person innerhalb einer Menge)
     Verifikation = 1:1 Vergleich (Referenz-Template ?=? Live-Template)

Verifikation in der Informatik (Programme): Macht die Software/Hardware das was sie soll?
Erfüllt diese die Spezifikation von Software/Hardware - typischerweise mittels Tests.

3. **Statische biometrische Merkmale** für eine Identifikation/-verifikation + ihren Eigenschaften:

Merkmale	Eigenschaften
Gesichtsbild	- Unterschiedliche Ansätze der Gesichtserkennung, wobei alle gewisse Schlüsselelemente verwenden. Meistens charakteristischen Merkmale der Gesichtszüge. Besonders Interessant die Merkmale, die sich aufgrund der Mimik nicht ständig verändern. - Vergleich über klassische Bildanalyseverfahren - Den verschiedenen Gesichtserkennungssysteme liegen unterschiedliche Verfahren aus dem Bereich der Mustererkennung bzw. deren Kombinationen zugrunde: • Template Matching • Elastische Graphen / Landmarks (Markante Stellen werden zu Gittermodel verbunden) • Geometrische Merkmale (Relative Position von markante Stellen bilden mathematischen Vektor) • Eigenfaces
Fingerabdruck	- Graustufenbild des Fingers, Weiterverarbeitung nötig - Die Extrahierung der charakteristischen Kennzeichen kann entweder anhand des gesamten Bildes (Global Pattern Matching), relevante Teile daraus, oder die

	anatomischen Merkmale der Papillarlinien **(Minuzien) nach Art, Lage und Richtung** erfasst werden. - Musterklassifizierung mit Hilfe Henry Klassifikation: Schleife, Wirbel, Bogen. (Manche Fingerabdrücke lassen sich nicht eindeutig in eine konkrete Fingerklasse einordnen). - Merkmalextraktion: Lage der Minuzien wird detektiert und extrahiert - Die häufigsten Minuzien sind 1. das Papillarlinienende und 2. die Gabelung
Iris	Iris-Kodierung nach Daugman in 2048 Bit String: 1. Detektion Iris-Mitte 2. Umwandlung „Iris-Ringe“ in Polardarstellung 3. Berechnung Gabor- Wavelet-Koeffizienten (256 Byte) 4. Zusätzlich 256 „Masken-Bytes“ für Artefakte
Venen	- Keine klar definierten Features – nur Extraktionsverfahren, die bisher auf Skimming hinauslaufen: • Repeated Line Tracking (RLT): „Linienverfolgung“ basierend auf den maximalen Grauwerten • Maximum Curvator (MC): Linienverfolgung“ basierend auf den maximalenKrümmungen der Grauwerten - Beide Verfahren basieren auf der Annahme *kontinuierlicher Venenverläufe.* - Aus den Verfahren können Minutien abgeleitet werden
Ohr	Anchor Point + Ohrabstände

4. Neben statischen biometrischen Verfahren werden auch zunehmend **dynamische (verhaltensbasierte) Verfahren** diskutiert. Welchem grundsätzlichen Sicherheits-Problem scheinen verhaltensbasierte Verfahren zu unterliegen und muss in der Praxis beachtet werden?

- Problem: Leichte Reproduzierbarkeit
- Beispiele: Gangverhalten, Tippverhalten, Bedienung von Software

5. Welche zwei gängigen **Methoden zur Merkmalsextraktion** haben sich in der Gesichtsbiometrie etabliert?

- Elastische Graphen/ Landmarks
- Neuronale Netze

6. Wenn Sie die „typischen“ biometrischen Merkmale wie, 2D-Finger, Iris, Gesicht, Venen betrachten, welche(s) Merkmal(e) sind aus Sicht der Informationssicherheit **besonders geeignet**, weil diese eine unbemerkte Erfassung durch Dritte erschweren?

- Venen, da der Fäschlungs-Aufwand hier am größten ist.

7. Welche Merkmale machen die **Eindeutigkeit eines Fingerabdrucks** aus?

- Die Papillarleisten bilden verschiedene Muster (siehe Henry-Klassifizierung), die in Verbindung mit den Unterbrechungen der Papillarleisten (Minuzien) von Finger zu Finger unterschiedlich sind.

- Anders ausgedrückt: Die wahre Individualität eines Fingerabdruckes wird durch die anatomischen Merkmale der Papillarlinien (Minuzien) und durch ihre gegenseitige Orientierung festgelegt.

8. Mit Hilfe welcher Verfahren kann man die **Umgebungseigenschaften** einer Minuzie eines Fingerabdrucks beschreiben? Welche Verfahren sind Ihnen bekannt und was sagen diese aus?

Deskriptor	Ist ein Maß für…
Orientierungs-	• Die mittlere Orientierung
Frequency-	• Den mittleren Abstand der “Valleys”
	… im Umfeld der Minuzie.

9. Beschreiben Sie eingehend zwei Ihnen aus der Vorlesung bekannte **Verfahren der Venenbiometrie** mit Hilfe derer aus Venen-Graustufenbilder Venenverläufe extrahiert werden.

- Beide Verfahren nehmen an einen kontinuierlichen Venenverlauf zu haben.

Verfahren	„Linenverfolgung“ basierend auf…
Repeated Line Tracking	• Maximalen Grauswerten
Maximum Curvature	• Maximalen Krümmungen der Grauwerten
	… im erfassten Bild.

- Genauen Schritte:
  - Grauwerbild aufzeichnen / Venen erfassen
  - ROI bestimmen
  - Extraktion charakteristischer Merkmale:
    Grauwertverteilung in Schritten über ROI bestimmen
  - Dunkelste Stellen über die ROI-Schritte berechnen/ verfolgen bzw.

10. Welche **Fehlermaße** sind Ihnen bekannt, mit denen biometrische Systeme charakterisiert werden?

Affinität: Zwei biometrische Samples sind affin, gdw. sie vom identischen Körperteil stammen.

Fehlermaße	Abkz.	Erläuterung.
		Häufigkeit/Anteil der jenigen, die
Failure to Enrole Rate	FER	… biometrisch nicht erfassbar sind.
Failure to Acquire	FTA	… wegen nicht erfassbaren Merkmalen bei Verifikation, zurückgiewesen werden müssen.
False Rejection Rate	FRR	…zu unrecht abgelehnt werden. $FRM*(1-FTA)$
False Acceptance Rate	FAR	…zu unrecht akzeptiert werden. $FTA+FNMR*(1-FTA)$
False Match Rate	FMR	Häufigkeit mit der nicht-affine Vergleiche ein „match“ liefern
False Non Match Rate	FNMR	Häufigkeit mit der affine Vergleiche ein "non-match" ergeben

11. Wodurch unterscheidet sich die False Match Rate (**FMR**) von der False Acceptance Rate (**FAR**)?
- FRM ist Obermenge von FAR $FMR \supset FAR$
- FMR = $\frac{\text{Anzahl FM}}{\text{Gesamtanzahl nicht-affiner Vergleiche}}$
- FAR = FMR * (1 – FTA)
- Bei der Berechnung der FAR werden noch zusätzlich Zugangsversuche, die zum Beispiel aufgrund schlechter Bildqualität von vornherein abgewiesen werden (FTA), mit berücksichtigt.

12. Mit welchem Maß bestimmen Sie den **mittleren Informationsgehalt** der Zeichen einer diskreten Nachrichtenquelle? Was ist ein geeignetes Maß zur Bestimmung der Anzahl von Zufallsbits, die aus einer diskreten Quelle mit einer definierten Wahrscheinlichkeitsverteilung erzielt werden können ?
- Shannon Entopie

13. Sie sollen ein biometrisches Erkennungssystem basierend auf der Fingerbiometrie mit einer False Matching Rate (**FMR**) von 0,1 % installieren.
Erläutern Sie, was FMR = 0,1% genau bedeutet.
- Das beudetet, dass jede 1000 Person falsch identifieziet/ verifiziert wird.

14. Ein Angriffspunkt gegenüber biometrischen Systemen sind Nachbildungen biometrischer Merkmale (Fakes). Was können Sie prinzipiell tun, um **Fakes** von echten biometrischen Merkmalen zu unterscheiden?
- Lebendmerkmale überprüfen:
  Plus, Blutfluss im Gewebe, Temperatur, Hautleitfähigkeit, Relexionsspektrum der Haut

15. Was zeichnet ein lebendes menschliches „Organ“ aus und wie kann man diese Eigenschaften für die **Lebenderkennung biometrischer Merkmale** heranziehen? Betrachten sie insbesondere den Spezialfall der Fingerbiometrie.
- Methoden aus (14) und neuere Idee: Optical Kohärenztomographie

16. Eine neue Technologie, deren Einsatz z.Zt. in der Finger-Biometrie erforscht wird, ist die **Optical Kohärenztomographie**. Was ist der Mehrwert dieser Technologie gegenüber allen anderen Sensor-Technologien zur Erfassung der Finger?
- Mehrwert: Erfassung Fingeroberfläche + Hautstrukturen
- --> Zwei Fingerabdrücke + Schweißdrüsen

17. Ein OCT-Scan eines Hautsegmentes (z.B. Finger) liefert ein Frequenzspektrum. Welche mathematische Transformation müssen sie auf das erhaltene Frequenzspektrum anwenden, um ein ortsaufgelöstes **3D-Bild aus** diesem **Spektrum** zu erhalten?
- Fourier-Transformation

18. Ein weiteres Problem in der Biometrie ist Morphing.
a) Was wird darunter verstanden, insbesondere für Gesichter?
   - Verschmelzen von 2 oder mehr Gesichtsbildern (von verschiedenen Personen) zu einem.

b) Was meinen Sie: Ist Morphing nur ein Problem für die Gesichtsbiometrie.
   Erläutern sie ihre Einschätzung.

- Morphing kann dann zum Problem werden, wenn gemorphte Bilder als Referenz verwendet werden.

19. Die Verwendung von **Neuronalen Netzen** anstatt von Landmarks in der Gesichtsbiometrie eröffnet die Möglichkeit von gezielten Falschklassifikationen einer **Person Adversarial Attack**. Beschreiben Sie was darunter verstanden wird und was ein Angreifer tun müsste, um einen derartigen Angriff vorzubereiten und gezielt auszunutzen.

Übungsblatt II - Biometrische Kryptofunktionen

A linear code C over F q is denoted as [n, k, d]-code, following the standard notation in coding literature. This code C encode k-digit data values to n-digit codewords has minimum hamming distance $d_{min} \geq 2t+1$ and can correct up to t errors without regarding list decoding algorithms.

- **d** is the distance, that is the minimum number of positions in which any 2 codewords differ.
- **d_min** die minimale Hammingsdistanz aller gültigen Codewörter
- **n** is the block length or the length of the codeword (**Codewortlänge**)
- **k** is the dimension of the codeword (**Datenwortlänge**)

Normal gilt: $k \leq n-d+1$
Bei MDS: $n=k+d-1$ bzw. $k=n-d+1$

1. Sie haben die Aufgabe aus einer nicht gleichverteilten Zufallsfolge X guten Zufall abzuleiten. Welches Maß gibt Ihnen bei gegebenem X eine Abschätzung über die erreichbare Ableitung zufälliger Bits aus dieser Verteilung?
   - Die **Min-Entopie** $H_\infty(X)$ dient dazu die **Zufälligkeit zu beurteilen**.

2. Beschreiben sie den prinzipiellen Unterschied zwischen Block- und Faltungscodes.
   - **Blockcode**: Kodiert Datenbitblock einer konstanter Länge (vergleichbar Block-Chiffre)
   - **Faltungscode**: Kodiert Kontinurierlichen Bitstrom (vergleichbar Stromchiffre)

3. Für einen spezifischen Code ist die **Code-Rate** R = 0,6 (ein Maß für die Codeeffizienz). Der Code besteht aus einer Menge von Codewörtern mit einer Länge von jeweils 30 Bits. Aus wieviel Bits bestehen die zugehörigen Datenworte?
   - Gegeben:
     - Codewortlänge n: 30 Bit
     - Code-Rate R = 0,6, $R=\frac{k}{n}$
   - Gesucht: Datenwortlänge k
   - Durch umformen: $k=R*n=0,6*30=18$

4. Welche **Gesetzmäßigkeit** gilt für einen **linearen Code**?
   - Gesetzmäßigkeiten einer kommutativen, abelschen Gruppe gelten, also
     - Abgechlossenheit
     - Assoziativität
     - Einselement
     - Inverse

- Kommunikativität

5. Gegeben sind die nachfolgenden Codeworte eines Codes.

```
0000000, 0001011, 0010110, 0011101, 0100111, 0101100, 0110001,
0111010, 1000101, 1001110, 1010011, 1011000, 1100010, 1101001,
1110100, 1111111
```

Prüfen sie exemplarisch, ob es sich dabei um einen linearen Code handelt. Wie gehen sie vor?

- Gruppenaxiome müssen geprüft werden (s.o.)
- Abgeschlossenheit:
  - Das Ergebnis einer Operation muss auch wieder Element der Gruppe sein. Prüfung:

```
          1011000
(mod 2) 1000101
----------------
          0011101 → Element in Gruppe, also Test bestanden
```

- U.s.w.

6. Welches Maß eines Codes müssen sie maximieren, um **gute Fehlerkorrektureigenschaften** zu erhalten? → Minimale Hammingdistanz d_{min}

7. Was macht einen **zyklischen linearen Code** aus?

- Ein linearer Blockcode heißt zyklisch, wenn jede zyklische Verschiebung eines Codewortes wieder ein gültiges Codewort ergibt.
- Zyklische Codes sind eine Unterklasse linearer Blockcodes.

8. Mit Hilfe welcher beiden Berechnungsvorschriften können sie aus gegebenen Datenworten Codeworte berechnen, die einen zyklischen Code ergeben?

- Preamble:
  - $v(x)$ → Codepolynom
  - $g(x)$ → Generatorpolynom
  - $u(x)$ → Datenpolynom
- Multiplikationsverfahren: $v(x)=u(x)*g(x)$
- Divisionsverfahren: $v(x)=u(x)*x^k-r(x)$
  - Multiplikation von $u(x)$ mit x^k bedeutet, dass das Polynom um *k*-Stellen nach links verschoben wird, hin zu höheren Potenzen.

9. Gegeben sind die nachfolgenden Bitfolgen: 0110010111000101 und 0001101000101110.
Wie groß ist das Hamminggewicht und **die Hammingdistanz** der beiden Bitfolgen?

- Hamming-Gewicht: Anzahl der 1-Bits eines Codewortes
  - 0110010111000101 → 8
  - 0001101000101110 → 7
- Hamming Distanz: Anzahl der unterschiedlichen Bits zweier Codewörter:

```
      0110010111000101
(xor) 0001101000101110
----------------------
      0111111111101011 → 14
```

- Je kleiner die Hammingdistanz, desto ähnlicher sind die Wörter.

10. Was wird unter einem **irreduziblen Modularpolynom** verstanden?

- Zyklische Codes können mittels eines Generatorpolynom *g(x)* berechnet werden.
- Grundlage für die Bildung eines Generatorpolynoms ist ein irreduzibel Modularpolynom *M(x)*.

- Irreduzibel bedeutet dass sich das Modularpolynom *M(x)* nicht in ein Produkt von Polynomen zerlegen lässt.
- Modularpolynom bestimmt den Codeparameter *n*, also die Codewortlänge.

11. Berechnen Sie den **Erweiterungskörper** GF(2^n), die zugehörigen **Polynomreste** und die **Koeffizienten** der Polynomreste mittels Modularpolynom $m(x)=x^3+x+1$.

- $\alpha^0 \, mod \, M(x=\alpha)=1 \rightarrow 001$
- $\alpha^1 \, mod \, M(x=\alpha)=\alpha \rightarrow 010$
- $\alpha^2 \, mod \, M(x=\alpha)=\alpha^2 \rightarrow 100$
- $\alpha^3 \, mod \, M(x=\alpha)=\alpha+1 \rightarrow 011$
- $\alpha^4 \, mod \, M(x=\alpha)=\alpha(\alpha+1)=\alpha^2+\alpha \rightarrow 110$
- $\alpha^5 \, mod \, M(x=\alpha)=\alpha(\alpha^4)=\alpha(\alpha^2+\alpha)=\alpha^3+\alpha^2=\alpha+1+\alpha^2=\alpha^2+\alpha+1 \rightarrow 111$
- $\alpha^6 \, mod \, M(x=\alpha)=\alpha(\alpha^5)=\alpha(\alpha^2+\alpha+1)=\alpha^3+\alpha^2+\alpha=\alpha+1+\alpha^2+\alpha=\alpha^2+1 \rightarrow 101$

12. Ein aufgrund seiner Eigenschaften häufig verwendeter Code ist der Reed-Solomon Code.
Er gehört zur Klasse der **MDS-Codes**. Wofür ist MDS die Abkürzung und was bedeutet das inhaltlich?

- MDS= Maximum Distance Separable
- *(n,k,d)*-Code wird als MDS-Code bezeichnet, falls gilt: $n=k+d-1$ (*d* entspricht d_{min})
- Bei fest Codewortlänge *n* gilt:
  - Eine hohe Fehlerkorrektur: Je grösser d_{min} , desto mehr Fehler können korrigiert werden.
  - Eine hohe Informationsrate: Je grösser k, desdo mächtiger ist die Sprache

13. Der **Reed-Solomon Code** ist ein nichtbinärer Code. Was bedeutet das und über welchen Körpern können sie Reed-Solomon Codes praktisch erzeugen?

- Codeberechnung erfolgt über $v(x)=u(x)*g(x)$
- $u(x)$ ist Datenwortpolynom - die Koeffizienten sind Elemente eines Körpers.

14. Sie haben zwei **Klassen biometrischer Kryptosysteme** in der LV Identifikation kennengelernt. Wie heißen diese beiden „Klassen“.

- Fuzzy Commitment Scheme (FCS)
- Fuzzy Vault Schemes (FVS)

Beide setzen **fehlerkorrigierende** Codes ein. Welchen Sinn macht dieser Einsatz?

- Um eine Fehlertoleranz zu erreichen. Diese Fehler treten bei der sensorischen Erfassung/ Digitalisierung auf (Rauschen, Messfehler).
- Das FCS akzeptiert bei der Validierung nur dann, wenn das Haminggewicht nicht größer als die Anzahl an Fehlern, die von dem ECC korrigiert werden können.

15. Erläutern Sie den Begriff des „**Fuzzy Extractor**“ nach Dodis.

- Ein Fuzzy Extractor ermöglicht das Extrahieren von Zufallszahlen (um als krytpographisches Material zu verwenden). Die zufällige Bitfolge kann reproduziert werden, wofür ein auxiliary darta (AD) Bit String dient.
- Ein Fuzzy Extracot besteht aus zwei Algorithmen:
  - Gen → erzeugt Zufallszahl R und AD für biometrisches Enrolment
  - Rep → führt auf R anhand von AD zurück für biometrische Verifikation

16. Wie unterscheiden sich die **Pseudonymen Identifikatoren** (PI) beim FCS und FVS?

- FCS: Hashwert über Zufallszahl = $h(s)$
- FVS: Hashwert über Koeffizenienten des Polynoms = $h(s_0|\ldots|s_{(k-1)})$

17. Stellen Sie die Unterschiede zwischen den **FVS** von **Jules/Sudan** und **Dodis** 2004 dar.
- Preample: Chaff points are additional fake minutiae used to hide the genuine minutiae, so that too many combinations exist for a brute force attack.
- Pseudonymous Identifier (PI) → bei beiden gleich
- Auxiliary Data (AD) unterscheidet sich
  - Bei Jules Sudan: AD = Complete fuzzy vault (Chaff Points + Genuine Points)
  - Dodis: Koeffizenten des Polynoms $p(x)$

18. Das **Fuzzy Vault** ist letztlich eine öffentliche Information. Wodurch wird erreicht, dass ein Angreifer aus Kenntnis eines speziellen Fuzzy Vault **nicht auf** eine **Person schließen** kann?
- Angreifer stehen nur die Auxililary Data (AD) zur Verfügung.
- D.h. bei FVS die Koeffizenten des Polynoms.
- Ziel eines Angreifers: Polynomrekonstruktion – er kennt Polynom grad aber nicht.
- Die gesamte Sicherheit von alles Futty Vault Ansätzen ist basierend auf der Schwieirigkeit der Polynomrekonstruktion.

19. Welche **aktiven Angriffe** können auf **Fuzzy Commitment Verfahren** durchgeführt werden?
- Brute Force Attack
- Crossmatching Attack (requires multiple databases)
- False Accept Attack

20. Über Polynomrekonstruktion können die Koeffizienten des Pseudonymen Identifikators (PI) wieder auf Basis der zugehörigen biometrischen Information aus dem zugehörigen Fuzzy Vault berechnet werden. Angenommen ein Pseudonymer Identifikator wird berechnet über einer Sequenz von 8 Koeffizienten s0 - s7. Im Rahmen einer biometrischen Verifikation soll das Verfahren 2 Fehler tolerieren. **Wieviel Minutien** müssen Sie kodieren, **damit** diese **Fehlerkorrektur möglich** wäre? Welche Arten von Fehlern werden damit toleriert?
- Wieviel Minuitien müssen ins Polynom hineingerechnet werden?
- Grad des Polynoms k: $k-1=n-2t-1$, wobei
  - n = Anzahl an kodierten high-quality Minuitien
  - t = Anzahl korrigierbarerer Fehler (s. Folie 17 – BioCrypt)

  $k-1=n-2*2+1$
  $8-1+2*2+1=n$
  $12=n$
- Somit können Fehler bzw. Uneinheitlichkeiten bei Digitalisierung tolerieret werden.

21. Angenommen, Sie sollen ein **Fuzzy Vault Scheme konzipieren** und haben die Aufgabe, dieses für die Fingerbiometrie zu konzipieren. Es sollen jeweils die besten 30 Minutien im Fuzzy Vault kodiert werden und es sollen im Rahmen der Verifikation 4 Fehler durch den gewählten Code korrigierbar sein. Welchen Polynomgrad müssen sie für den Fall wählen?
- Gegeben: t = 4, n = 30
- $k-1=n-2t-1$
- $k-1=30-2*4-1$
- $k=30-2*4$
- $k=22$

22. Sie wollen einen **brute-force Angriff auf die Koeffizienten eines Pseudonymen Identifikators** von einem FVS machen. Welche Informationen wären für sie als Angreifer sehr hilfreich und welche Berechnungsschritte müssten Sie als Angreifer durchführen?

- Angenommen FVS nach Jules Sudan, also hat Angreifer PI und AD (gesamte Punktemenge)
- Hilfsreiche Infos für den Angreifer:
  - Grad k des Polynoms
    → Falls k irgendwie bekannt, könnte Polynom rekonstruiert werden
    → Lagrange Polynom Interpolation
  - Anzahl der kodierten Minuzien *n*
- Berechnungsschritte:
  - $s_0 - s_{k-1}$ mit allen möglichen Werten belegen → Elemente aus F_q
  - Bzw. Gleichungssystem aufstellen und lösen
    → Calculates the related polynom coefficients
  - Compares the hash value of the calculated coefficients with the PI as long as he find a match, also $h(s_0'|\ldots|s_{(k-1)}') ?= ? h(s_0|\ldots|s_{(k-1)})$

23. Neben dem Brute-Force Angriff werden beim Fuzzy Vault Verfahren drei weitere Angriffe unterschieden: **Smart Polynom Angriff, False Accept Angriff** und **Crossmatch Angriff.** Beschreiben Sie am Beispiel des Fuzzy Vault Verfahrens, was sie für die Durchführung der jeweiligen Angriffe benötigen, wie sie diese durchführen und worauf diese Angriffe abzielen?

- Smart Polynom Angriff
  - Angreifer haz Zusatzwissen womit er Chaff Points identifizieren und somit den Suchrraum verringert kann.
  - Die starke Abhängigkeit zwischen der Orientierung der Minutien, der jeweiligen Lokation der Minutien und der Orientierung der benachbarten minutien, kann die Unterscheidung erleichtern.
  - Gelingt es einem Angriefer alle chaff points von den genuine points in einem Fuzzy Vault zu unterscheiden, kann er die Koeffizienten direkt herraus finden.
- False Accept Angriff
  - Angreifer hat DB mit biometrischen Merkmalen zur Verfügung.
  - Der Angreifer versucht das geschützte Template aus dem Vault offline wiederherzustellen, indem er Authentifizierungs-Versuche simuliert
  - Aufgrund der *FAR*, ist query attempt nach $\log(0,5)/\log(1-FAR)$ Versuchen erfolgreich
  - Angriff ist FVS unspezifisch
- Crossmatch Angriff
  - Angreifer stellt Querbeziehungen von geschützten Templates zwischen Datenbanken her
  - Fuzzy Vault verwendet einheitliche Abbildungsvorschrift:
    Minutien --> Körperelemente (Nicht Y aber X Werte mappen)

24. Mit Hilfe welcher **Gegenmassnahme** verhindern Sie **Crossmatching-Angriffe** beim Fuzzy Vault Verfahren?

- Besser Futty Vault nach Dodoes einsetzen
- Oder: Alle Quanten belegen

25. Für ein gegebenes Fuzzy Vault Verfahren (n=24, k=11, f (Chaff Points)=100) sollen Sie die **Brute-Force Festigkeit berechnen.**

- Number of experiments to reconstruct the polynom with probability 50 % (logarithm law):

$$\log_{(1-B)}(0,5) = \frac{\log(0,5)}{\log(1-B)} \quad \rightarrow \quad B = n * r^{-1}$$

- Number of genuine and chaff points: r = n + f = 24 + 100 = 124
- $B = 24 * 124^{-1} = 0,19$

26. Welchen **Vorteil** bietet das Fuzzy Vault Verfahren **nach Dodis** im Hinblick auf die Brute-Force Festigkeit?
- Dodis hat keine expliziten Chaff Points mehr. Alle Punkte sind gefüllt → großer Suchraum

27. Sie haben die Aufgabe, das Fuzzy Commitment Verfahren auf die Fingerbiometrie anzuwenden. Wie könnten Sie vorgehen?
- Mapping Vorschrift konstruieren
- Die Minutienpositionen in einen reproduzierbaren Bitstring überführt
- oder laut BSI:
  - Feature vector generation
  - Bit string generation
  - FCS
  - Hashing

28. Was sind **Bloomfilter** und wozu werden diese primär eingesetzt?
- Bloom filter are a probabilistic data structure
- Application: proof whether $x \in S$
- Für schnelles Suchen; beschleunigt Suchoperationen
- Eigenschaften von Hash-Funktionen: Schnell, ähnliche Verteilung

29. Welche Fehlererkennungs- und Fehlerkorrektureigenschaft haben **Bloomfilter**?
- Keine

30. Ein Anwendungsfeld für Bloomfilter in der Biometrie ergibt sich im Rahmen einer biometrischen Identifikation zur Performancesteigerung des Fuzzy Vault Verfahren. Nunmehr ist nicht mehr ein 1:N Fuzzy Vault Match erforderlich sondern über die Bloomfilter kann eine mögliche Vorauswahl getroffen werden, welche Einträge einen Match liefern könnten.
D.h. die ursprünglich erforderlichen 1:N Fuzzy Vault Matches reduzieren sich auf notwendige 1:M Fuzzy Vault Matches mit N>>M. Welchem **Seiteneffekten** hat dieser Performancegewinn?
- Der Bloomfilter über den ganzen Fingerabdruck legt alles wieder offen

31. Beschreiben Sie im Detail, wie BioHashing im Rahmen des Enrolements und der Verifikation funktioniert.

Übungsblatt III - Identitätsbasierte Kryptographie und bilineare Paarungen

1. Was wird unter einer **bilinearen Paarung** verstanden?
   - **Grob**: Paarung ist ein Mapping mit bestimmten Eigenschaften, welche zwei Elemente einer Gruppe auf ein Element einer anderen Gruppe überführt.

   - **Ausführlicher**:
     - Seien G1, G2 additive und G3 eine multiplikative zyklische Gruppen mit Ordnung n.
     - Eine (Typ 1) Paarung ist eine Abbildung $e: G_1 \times G_1 \rightarrow G_2$
     - Sie heißt bilineare Abbildung falls gilt
       - $e(A+B,C)=e(A,C)e(A,B)$
       - $e(A,B+C)=e(A,B)e(A,C)$

2. Wie unterscheiden sich die **Bilinear – und die Decisional Bilinear Diffie Hellman Annahme** voneinander? Stellen Sie diese gegenüber, erläutern Sie die Unterschiede und was diese bedeuten.
   - Bilinear Diffie Hellman Annahme (BDH):
     Angreifer weiß (G, aG, bG, cG) und will $e(G,G)^{abc}$ berechnen.
     → Ein Angreifer kann diese Bechnung nicht effizient durchführen.
   - Decisional Bilinear Diffie Hellman Annahme
     Angreifer weiß die Dinge aus BDH-Annahme und zusätzlich $Z \in G_2$
     → Angreifer kann nicht entscheiden, ob $Z = e(G,G)^{abc}$ oder eine zufällige Zahl aus G2 ist.

3. Welche spezielle Eigenschaft macht die **identitätsbezogene Kryptographie** aus?
   - Es eliminiert die Notwendigkeit, den öffentlichen Schlüssel des Empfängers zu beziehen
     → Public Key einer Person ist aus ihrer „Identität“ ableitbar, z.B. aus Email-Adresse
   - Key Generation Center (KGC) notwendig für private Schlüssel

4. Was versteht man unter „Ciphertext Indistinguishability“ (**IND**) bzw. Indistinguishability against adaptive chosen ciphertext (**IND-CCA**) eines Publiy Key Verschlüsselungsverfahrens im Rahmen eines kryptographischen Beweises?
   - Die Sicherheitsidee von IND ist, dass ein Angreifer die Chiffrate zweier gleich langer Klartexte nicht unterscheiden kann.
   - Bei IND-CCA hat der Angreifer Zugrif auf ein encryption oracle welche beliebeige Klartext verschlüsselt. Angreifer stellt queries an das Oracle und passt queries anhand von vorherigen Antworten des Oracles an. An einem Punkt sendet der Angreifer zwei gleich lange Nachrichten M1, M2 an das Oracle, welches zufällig aus M1 und M2 wählt und eine verschlüsselte Version zurück gib – enc(M1) oder enc(M2). Angreifer muss dann bestimmen, ob M1 oder M2 verschlüsselt wurde. Der Vorteil des Angreifers ist dann die hohe Wahrscheinlichkeit eines richtigen Treffers.

5. Welche Berechnungsschritte und welche Kommunikation muss zwischen Alice, Bob und Eve stattfinden, um sich auf einen geheimen **Diffie Hellman Key unter Verwendung bilinearer Paarungen** zu einigen? Stellen Sie die Berechnungsschritte und die Kommunikation eingehend dar.

- Jeder Teilnehmen hat eine zufällige Zahl aus Z_p : Alice: a, Bob: b und Eve: c
- Jeder Teilnehmer multipliziert die Zahl mit dem Generatorpunkt G und verteilt das Ergebnis.
- Daraufhin wendet jeder Teilnehmer die Abbildung für die bilineare Paarung mit den erhaltenen Produkten an. Z.B. berechnet Alice $e(bG,cG)^a$, was durch die bilineare Eigenschaft der Paarung $e(G,G)^{abc}$ ergibt. Da das jeder berechnen kann, kann sich somit auf das gemeinsame Geheimnis geeignigt werden.

6. Stellen Sie den Berechnungsaufwand für Signierer und Verifizierer für eine ID-basierte **Signatur nach Paterson** bzw. einer **klassischen ECDSA-Signatur** dar und diskutieren sie diesen.

7. Stellen Sie beim **Boneh Franklin Verfahren** die konkreten Berechnungsschritte dar, um die Gültigkeit eines Boneh Franklin Kryptogramms zu prüfen. Entschlüsselung: $m = V \; xor \; h_2(e(d_{ID},U))$

- Preamble:
  - First practical identity-based encryption scheme using bilinear pairing → S.49 IBK-Book
  - Während Setup: $P_{Pub} = s \times G$, mit zufälligen $z \in Z_p^*$
  - Während Encryption: Zufälliges $r \in Z_p^*$
  - Pub Key: $Q_{ID} := h_1(ID)$, Privater Schlüssel: $d_{ID} := s \times Q_{ID}$
- $e(Q_{ID},P_{pub})^r$
  $= e(Q_{ID},s \times G)^r = e(Q_{ID},G)^{sr} = e(s \times Q_{ID},r \times G) = e(d_{ID},r \times G) = e(d_{ID},U)$
  $= e(d_{id},U)$

8. Welche Beziehungen müssen für das identitätsbasierte Schlüssel-Paar des Signierer gelten, damit das **Paterson Verfahren** funktioniert?

- Das Signaturschema nach Paterson beasiert auf IBE nach Boneh und Franklin. Die Schlüsselpaar-Beziehungen ist daher dort definiert → siehe also oben.
- (Private) Zufallszahl *s* kommt von KGC.

9. Wie kann sichergestellt werden, dass der Public Key des Signierers beim **Paterson-Verfahren** in ein Gruppenelement der Gruppe G1 abgebildet wird und um welche Art von Gruppenelementen handelt es sich?

- Kryptographische Hashfunktionen $h_1 : \{0,1\}^* \rightarrow G_1$ bildet auf einen Kurvenpunkt in *G1* ab.
- Die Gruppenelemente sind Kurvenpunkte.

10. Der Verifizierer muss beim **Paterson-Verfahren** drei Paarungsoperationen durchführen, um die Signatur zu prüfen. Welchen Einfluss hat der Einbettungsgrad des Generators (Erzeugers) auf die Sicherheit der Paarungsoperation ?

11. Welche Eigenschaft zeichnet ein **Sign-Crypt-Verfahren** aus?

- Neue Klasse asymmetrischer Kryptographischer Verfahren
- Sicherstellung Authentizität und Vertraulichkeit einer Nachricht innerhalb eines Verfahrens
- Heutzutage eher hybrider Ansatz: encryption-then-mac

12. Beim Sign-Crypt Verfahren von Libert und Quisquater müssen im Rahmen der Signaturverifikation *k1* und *k2* berechnet werden. Zeigen Sie die **Korrektheit der Verifikationsgleichung** von $k_2 := h_2(e(S,Q_{IDB})e(Q_{IDA},d_{IDB})^r)$ dadurch, dass Sie diese auf die Berechnungsformel für *k2* im Zuge der Signaturerstellung $k_2 := h_2(e(P_{Pub},Q_{IDB})^x)$ zurück führen.

- Preamble: $S := x \times P_{pub} - r \times d_{IDA}$

$k_2 = h_2(e(s, Q_{id}) * e(Q_{id}, d_{IDb})^r)$
$k_2 = h_2(e(x \times P_{Pub} - r \times d_{IDA}, Q_{id}) e(Q_{ID}, d_{IDB})^r)$

$k_2 = h_2(e(Q_{IDB} * P_{pub} - r \times d_{IDA}, Q_{ID}) e(Q_{ID}, d_{IDB})^r)$
$k_2 = e(P_{Pub}, Q_{IDB})^x * e(Q_{IDB}, -r * d_{IDA})(Q_{IDA}, d_{IDB})^r$
$k_2 = e(P_{Pub}, Q_{IDB})^x * e(Q_{IDB}, r * s * Q_{IDA}) * e(Q_{IDA}, s * Q_{IDB})^r$
$k_2 = e(Q_{IDB}, Q_{IDA})^{-rs} * e(Q_{IDB}, Q_{IDA})^{rs}$
$k_2 = e(Q_{IDB}, -rs Q_{IDA}) * e(Q_{IDB} + r * s * q_{IDA})$
$k_2 = e(Q_{IDB}, r * s * Q_{IDA} - r * s * Q_{IDA})$

$k_2 = h_2(e(P_{Pub}, Q_{IDB})^x)$

13. Ein Problem der identitätsbasierten Kryptographie ist das **Key Escrow**.
Nennen und beschreiben Sie zwei Ansätze, die helfen, ein Key Escrow zu vermeiden.

- A major issue with the deployment of IBE schemes is that the PKG is able to obtain a secret key of any user and hence will be able to decrypt any ciphertext. This is called the problem of inherent key escrow in IBE schemes.
- Gegenmaßnahmen:
  - Nutzung mehrerer, verteilter KGCs für geteilte Generierung der Schlüssel
  - Geteilte Schlüsselgenerierung duch eine KGC und dem Nutzer
  - Nutzung einer Semi-Trusted Authority

14. Es existiert eine KGC – Infrastruktur bestehend aus 4 **unabhängigen KGC**s: (KGC 1 , KGC 2 , KGC 3 , KGC 4). Jedes KGC i hat einen eigenen Secret key s_i und einen zugehörigen Public key K_pub. Für alle Teilnehmer: Alice, Bob ... erzeugt jedes KGC i einen Teilschlüssel d_iID .

a) Wie berechnen sich der secret Master-Key und der zugehörige Public Key für die KGC-Infrastruktur?
   - Master Key $s = \sum_{i=1}^{n} s_i$ also die Summe aller KGC spezifischen privater Schlüssel
   - Pub Master Key: $P_{Pub} = \sum_{i=1}^{n} P_{Pub,i}$, also auch die Summe..

b) Wie berechnet sich nun der private Schlüssel eines Teilnehmers?
   - Nutzer mit Identitär ID erhält von jedem KGC ein Schlüsselteil $d_{ID}^i = s_i * Q_{ID} = s_i \times h(ID)$
   - Nutzer kann dann Schlüssel zusammen rechnen: $d_{ID} = \sum_{i=1}^{n} d_{ID}^i$

c) Ist damit sichergestellt, dass kein KGC Key Escrow für einen Teilnehmer durchführen kann?
   - Ja, da selbst die KGCs nur die Teilschlüssel kennen. Nur der Nutzer hat den vollständigen Schlüssel.

15. Angenommen wir haben das Szenario aus der vorhergehenden Aufgabenstellung mit vier **unabhängigen KGCS** (KGC 1 , KGC 2 , KGC 3 , KGC 4). Nun arbeiten aber die KGCs: KGC 1, KGC 2 und KGC 3 zusammen. Was bedeutet das für die Sicherheit eines Teilnehmerschlüssels?

- Die Sicherheit eines Nutzers ist nicht gefährdet, da sich der private Master-key trotzdem nicht berechnen lässt.

16. Typischerweise werden zeitliche **Gültigkeiten von Schlüsseln** für die asymmetrische Kryptographie in den zugehörigen Zertifikaten ausgedrückt. Bei der ID-basierten Kryptographie gibt es aber keine Schlüsselzertifikate. Wie können Sie trotzdem zeitliche Gültigkeiten bei der ID-basierten Kryptographie definieren/berücksichtigen?

- Vorschalg von Boneh-Frankling:
  Eindeitige ID kann mit weiteren Bestandteilen, wie einer zeitlichen Schlüsselgültigkeit, definiert werden.
- Nachteil: Kein explizites key revocation

17. Bei der ID-basierten Kryptographie gibt es keine Zertifikate, also auch keine Certificate Revocation List (CRL). Was könnten Sie tun, um dieses Problem zu lösen?

- Vorschlag aus vorherigen Aufgabe annehmen und stets auf entsprechenden Bestandteil prüfen

18. **Stellen** Sie funktional die Aufgaben einer Certificate Authority (**CA**) einer klasssichen PKI den Aufgaben eines **KGC** bei der ID-basierten Kryptographie **gegenüber**.

- CA zertifiziert öffentlichen Schlüssel und händelt certificate revocation list (CRL)
- KGC generiert Schlüssel und stell diese zur Verfügung
- Beides sind trusted third paries

Übungsblat IV - Privacy
Identifikationsprotokolle - Blinde Signaturen - Credentialsysteme

1. Was wird unter **Unlinkability** und der **k-Anonymity** verstanden?
   - Unlinkability: Unterschiedliche kryptographische Artifakte (Kryptogramme, Sessions, Signaturen) einer Identität können dieser nicht zugeordnet werden
   - k-Anonymity: Ein Individuum ist von weiteren k − 1 Individuen bezüglich einer Menge von Kriterien nicht unterscheidbar/ identifizierbar.

2. Welche **Bedrohungen** können die Privatsphäre einer „Person“ bei elektronischer Kommunikation teilweise oder vollständig offenlegen?
   - Endsystem des Nutzers (Browser-, Computerfingerprint)
   - Netzwerk (Verlinkbare Adressen wie IP), Mobilefunknummer
   - Nutzung kryptographicher Konzepte, welche Identität preisgeben

3. Was ist eine **blinde Signatur** und welche konkreten **Verfahren** sind ihnen bekannt?
   - Erläuterung
     - Nutzer blindet Nachricht bevor diese zu Signer gereicht wird.
     - Signer signiert Nachricht – kann diese aber nicht einsehen.
     - Resultierende Blindsignatur wird von Nutzer wieder „ungeblindet“, womit man öffentlich gegen die ursprüngliche, nicht geblindete Nachricht in Form einer regulären digitalen Signatur verifiziert kann.
     - Ermöglich *Unlinkability*
   - Verfahren
     - Blind Schnorr Signature
     - Blind Okamoto-Schnorr Signature

4. Wozu können **blinde Signaturen** eingesetzt werden und welche **Rollen/Instanzen** kommen bei der Ausstellung/Einsatz blinder Signaturen vor.
   - In Anwendungen bei denen die Privatsphäre des Senders gewährt werden soll
     - Elektronisches Geld ohne Geldflusseigenschaft
     - Beglaubigung von Willenserklärungen (durch Notar) ohne Kenntnisnahme des Testamentinhaltes
     - Signierung elektronische Wahlzettel (Authentizität) ohne Kenntnisnahme des Wahlvotums
   - Rollen/Instanzen:
     - User, Signer, Verifier

5. Für blinde Signaturen müssen die beiden Eigenschaften **Blindness** und **One-more Forgery** gelten. Erläutern sie präzise, was sich dahinter verbirgt.
   - Blindness:

    - Ausschließelich der Ntuzer kann eine Verbdinung zwischen der blind signatures (m_b, sig_b) und (m, sig) herstellen.
    - A signature is said to be blind if a given message-signature pair and the signer's view are statistically independent.
    - At a later time, the signer is not able to link the output of signature V to the view of the protocol V'
- One-more Forgery:
    - Ein Angreifer kann sich beliebig viele blind Signatures vom Signer ausstellen lassen. Danach darf er nicht in der Lage sein, ein Paar (m_b, sig_b) zu berechen, was als gültige Signatur verifiziert wird.

6. Was wird unter der **Zero-Knowledge-Eigenschaft** verstanden. Erläutern Sie die Grundidee eines Zero-Knowledge Proofs anhand des Beispiels der Höhle von Ali Baba.

- Ein Wissensbeweis ist, bei dem die Existenz eines Geheimnisses bewiesen wird ohne dieses preiszugeben.
- Eine Ausprägung des Zero-Knowledge-Beweissystems für den diskreten Logarithmus ist das Schnorr-Identifikastions-Protokoll.
- Bei

7. Ein häufig verwendetes Konstrukt in der Kryptographie ist die **Fiat Shamir Heuristik**. Beschreiben Sie präzise, was die Fiat Shamir Heuristik aussagt und erläutern sie, wie mit Hilfe der Fiat Shamir Heuristik ein **Schnorr Identifikation Protocol in eine Schnorr Signature** überführt werden kann.

- Die Fiat-Shamir Heuristik ist eine Technik, welche ein beliebiges interactives 3-Schritte Protokoll zwischen Prover und Verifier in ein 1-Schritt Protokoll, also ein non-interaktives, überführt werden kann.
  Dazu muss der Verifier im Rahmen des Protokolls eine Zufallszahl als Challenge senden.
- Der Prover lässt sozusagen das Protokoll bei sich "virtuell" ablaufen. Über das Transcript berechnet er dann eine Hashfunktion.

8. Ein User hat eine message m und sendet diese geblindet an einen Signer, der mittels der **Blind Schnorr Signature** eine dazugehörige Signature V erstellt. Welche Werte muss der User einem Verifizierer zur Verfügung stellen, damit dieser „die Signature" zu m prüfen kann?

- Nachricht m
- und die dazu gehörige unblindet Signature $sig = (e, s)$

9. Welche **Berechnungsschritte** muss ein Verifizierer durchführen, um „ die Signature" zu prüfen? Wie gehen dabei die Blindungswerte α und β der blind Signature ein?

- Preamble
    - α und β sind blinding values, welche der User gewählt hat
    - y ist public Key, x ist private Key
    - g ist zyklische Gruppe mit Ordnung q
    - r wurde mit einer von Signer ausgewählten Zahl k berechnet
    - User berechnet ~r, welches zusammen mit der Nachricht m gehasht wird $e = H(m, \sim r)$

- Verifier bekommt die in Aufg. 8 beschriebenen Werte *(e, s)* und wendet folgende Schitte an
  1. Verifier rekonstruiert ~*r* anhand der öffentlichen und zugeschickten Parameter:
     $\sim r' = g^s * y^{-e}$
  2. Hasht die erhaltene Nachricht mit dem zuvor berechneten Wert: $e' = H(m, \sim r')$
  3. Prüft, ob $e' == e$, falls true dann ist die Verifikation erfolgreich

10. Führen Sie gegenüber einem honest Verifier einen Zero-Knowledge Prove of Knowledge über den Besitz des Geheimnisses z.

11. Welche Eigenschaften hat ein Commitment Verfahren?

12. Warum darf beim verallgemeinerten Pederson Verfahren der Logarithmus von h nicht bekannt sein?

13. Mit einem Commitment bindet sich ein Prover zunächst an einen Wert ‘z‘ und drückt dadurch die Berechnung eines Commitments aus, z.B. in Form eines Peterson Commitments. Normalerweise legt der User zu einem späteren Zeitpunkt das Commitment offen, indem er den Wert ‘z‘ und den Blendungsfaktor ‘r‘ offen legt. Was könnte der Prover alternativ tun, wenn er zwar die Kenntnis von ‘z‘ und ‘r‘ nachweisen will, aber die Werte von ‘z‘ und ‘r‘ nicht offen legen will?

14. Führen sie einen Wissensbeweis des Wissens von v1,v2 ,v3 gegenüber einem honest Verifier V.

15. Das Anonymous Credential Light Verfahren nach Baldimtsi und Lysyanskaya ist eine Erweiterung der blinden Signatur von Abe um Attribute, bei der die Attribute in einen Commitment C kodiert werden.

a) Erläutern sie die Registrierung und Ausstellung eines anonymem Credentials.
b) Woraus besteht ein anonymes Credential.
c) Welche Prüfschritte muss ein Verifier bei der Prüfung eines anonymen Credentials durchführen?

16. Wie unterscheiden sich **Pseudonymous- von Groupe/Gruppen-Signatures**?

- Pseudonymous Signature: Verifier kann Signartur verlinken (Signatur komm von A)
- Verifier kann signatur nur auf eine Gruppe zurückführen, nicht auf Individium

17. Mit welchem ihnen bekanntem Signature Verfahren haben die **Pseudonymous Signatures** große algorithmische Ähnlichkeit?

- Mit Schnorr Signatur/ Identifikationsverfahren
- *c* (das Ergebnis der Hashfunktion) ist ähnlich des Ergebnisses *e* der Schnorr Signatur

18. Warum ist es aus Sicherheitsgesichtspunkten besonders kritisch, wenn bei den **Pseudonymous Signatures** zwei **User Keys** bekannt werden? Begründen Sie dies und stellen Sie dar, welche Möglichkeiten ein Angreifer dann hat, wenn dies unentdeckt bleibt.

- Aus zwei geheimen User-Keys ist der Private Key (*z, x)* des Group-Managers berechenbar.
- Daher dürfen User ihre geheimen Keys (x_1, x_2) nicht kennen.

19. Was wird unter einer Signature of Knowlege verstanden und wie wird diese mit Hilfe einer Nachricht *m* gebildet?

- Darunter wird die Gruppensignatur verstanden, welche mit Hilfe der Nachricht beweist, dass der Signer im Besitz von (α, δ, und x_i) ist.

20. Im **Signature of Knowlege** Verfahren wird eine Hashfunktion benötigt. In der theoretischen Betrachtung der Signature of Knowlege wird die notwendige Hashfunktion als randomoracle idealisiert. Was wird unter dem **Random Oracle Model** verstanden und wie grenzt sich dieses von einer realen Hashfunktion ab?

- Funktion bildet eine Menge jeweils unterschiedlicher Inputs auf voneinander unabhängige und gleichverteilte Outputs ab.
- No actual hash function is a random oracle. Hash functions are deterministic; for a given hash function, $H(x)$ in one problem is equal to $H(x)$ in some other problem. With a random oracle, this is not the case: the function used is *random*.
- Random oracle wird auch bei Non-Interactive-Zero-Knowledge Prove of Knowledge (NIZKPoK) verwendet.

21. Das Boneh-Boyen-Shacham-Gruppensignaturverfahren stellt eine „Open-Operation“ zur Verfügung. Was wird durch die **Open-Prozedur** erreicht und welche Instanz ist womit in der Lage, eine Open-Prozedur erfolgreich durchzuführen?

- Features:
  - „Dieser Algorithmus (ausgeführt vom Group-Manager) liefert die Identität eines Signierers und einen Beweis für diese Behauptung.“
  - Bei einer Signatur eines Gruppenmitglieds ist für den Verifier nämlich nur der Public-Key der Gruppe sichtbar.
  - Also Open-Prozedur erlaubt die Feststellung der Identität des Gruppenmitglieds.
  - Signatur wird einer bestimmten Instanz zugeordnet.
- Instanzen:
  - Nur Opener kann diese Feststellung durchführen.
  - Schlüssel nötig um basierend auf Signatur des Mitglied zu bestimmen.

22. Erläutern sie warum ein Gruppensignaturverfahren **ohne Open-Operation** insgesamt ein **Sicherheitsrisiko** darstellen kann?

- Stellt das Risiko dar, dass ein Mitglied die Gruppensignatur missbraucht, da genauer Signierer nicht ermittelt werden kann.

23. Was ist die wesentliche **Sicherheitseigenschaft von Gruppensignaturverfahren**?

- Signaturen von Gruppenmitglieder kann nur auf die Gruppe zurückgeführt werden
- Signaturen eines Gruppenmitglieds sind nicht einer Person verlinkbar

24. Wozu könnten Sie **Gruppensignaturen einsetzen**? Nennen Sie zwei Szenarien, in denen der Einsatz eines Gruppensignaturverfahrens sehr sinnvoll wäre.

- Aus Übung:
  - Fahrzeug-2-Fahrzeug Kommunikation

    - Zugang nur für Sparkassenkunden

25. Stellen sie sich vor ihnen wird durch den Opener unterstellt eine konkrete Gruppensignatur erstellt zu haben. Mit welchem Algorithmus könnten sie **öffentlich prüfen**, ob die Aussage des Openers stimmt? Steht dieser Algorithmus beim Boneh-Boyen-Shacham- Gruppensignaturverfahren zur Verfügung?

- **Judgement Procedure**: „Mit diesem öffentlichen Algorithmus kann geprüft werden, ob die Identitätsbehauptung und der zugehörige Beweis gültig sind.“

26. Sie haben die Aufgabe ein anonymes, elektronisches Ticketsystem zu bauen. Tickets dürfen nur einmal verwendet werden. Jede Form der Mehrfachnutzung (z.B. Kopien Dritter) soll auf die Identität desjenigen zurückführen, für den das Ticket ausgestellt wurde. a) Mindestens welche Rollen haben Sie in dem System ? b) An welches kryptographische Verfahren könnten Sie sich anlehnen zum Aufbau des Ticketsystems. c) Wodurch wird sichergestellt, dass die Identität des Ticketusers bei regel konformer Nutzung nicht aufgedeckt wird ? d) Aus welchen Bestandteilen besteht ein Ticket ? e) Wie wird einerseits die Authentizität des Tickets sichergestellt und anderseits ausgeschlossen, dass Mehrfachnutzungen des Tickets unentdeckt bleiben.

Sonstiges:
One Time Signature Schemes (OTSS)

- Aus dem Themengebiet *hash-based crypto*, welche für *post-quantum crypto* von Interesse ist.
- Die gesamte Sicherheit beruht exklsuiv auf der zugrunde liegenden Hashfunktion.
- Private- und Public Key dürfen jeweils nur einmal angewendet werden.
- Konsequenz: *Secure key issuing problem.*
  → Key Issuing Improvement: Merkle key authentication (key tree)
- Unterschied Lamport-Diffie - und Winternitz Scheme:
  - Lamport-Diffi signiert iterativ
  - Winternitz signiert mehrer Bits auf einmal (Anzahl bestimmt der Winternitz Parameter)
  - Signaturgröße bei 256 bit Hashfunktion
    - Lamport-Diffi: 256 x 256 Bit
    - Winternitz: t x 256 Bit
  - Privat Key bei 256 Bit Hash Funktion
    - Lamport-Diffi: 2 x 256 x 256 = 131072 Bit = 128 KiBit

- Lamport-Diffi-Scheme im Detail
  - Key Pair Generation für 256 bit Hashfunktion
    - Priv Key: RNG berechnet 2 x 256 Zufallszahlen mit einer jeweiligen Länge von 256 bit
    - Pub Key: Hashwerte über die 2 x 256 Zufallszahlen, also 512 Hashes mit jeweils 256 bit
  - …

- Winternitz Scheme im Detail
  - Priv Key: Wähle x als secret Key und *w.*
  - Pub Key: $h^w(x)$
  - ...