## Zero Knowledge Protokolle zur Authentikation (Nachweis der Identität)

Fiat-Shamir-Protokoll → Beispiel: Bankkunde identifiziert sich am Kontenrechner

**Vorbereitung:** Kunde berechnet für sich folgenden Parametersatz (ähnlich wie bei GNUPP):

| | | |
|---|---|---|
| I) | 2 große (z. B. 200-stelligen) geheime Primzahlen: | $p, q$ |
| II) | öffentlicher Modul: | $n = p \cdot q$ |
| III) | geheime, zu n teilerfremde Zufallszahl s: | $s < n,\ ggT(s,n) = 1$ |
| IV) | öffentliche modulare Quadratzahl v: | $v = s^2 \text{ MOD } n$ |

Es gibt kein schnelles Verfahren zur Berechnung der modularen Quadratwurzel s aus den Werten v und n **ohne** Kenntnis von p, q (siehe W. Dankmeier, „Modulare Quadratwurzeln beim Fiat-Shamir-Verfahren zur Authentikation", 10.04.1996, Downloadbereich auf www.vkfco.de ). Die Bank erhält vom Kunden die Werte n und v und versichert sich, dass diese Angaben wirklich von ihrem Kunden stammen (z. B. über die Verifizierungsinformationen zu GNUPP).

**Protokollablauf,** wenn der Kunde am Geldautomaten auf sein Konto zugreifen will:

1) Die Bank bittet den Kunden, eine zu n teilerfremde Zufallszahl $r < n$ zu wählen, diese geheim zu halten und ihr das modulare Quadrat $x = r^2 \text{ MOD } n$ zu nennen.
2) Die Bank bestimmt mit einem zweiwertigen Würfel eine Zufallszahl 0 oder 1.
3) **Wenn Würfelergebnis „1"**, bittet Bank den Kunden, ihr das Ergebnis von $y = (r \cdot s) \text{ MOD } n$ zu senden.

   Die Bank berechnet $x \cdot v \text{ MOD } n$ und $y^2 \text{ MOD } n$. Stimmen beide Ergebnisse überein, nimmt sie an, dass der Kunde „ok" ist, da nur der Kunde selbst den Wert s kennt:

   $$(x \cdot v) \text{ MOD } n = ((r^2 \text{ MOD } n) \cdot (s^2 \text{ MOD } n)) \text{ MOD } n = (r \cdot s)^2 \text{ MOD } n = y^2 \text{ MOD } n$$

4) Diese Annahme ist allerdings unsicher, da ein Betrüger unter Verwendung von v den für den obigen Vergleich passenden Wert von x unter Vorgabe eines beliebigen, teilerfremd zu n gewählten Wertes y berechnen kann, ohne den geheimen Wert s zu kennen. Dazu nimmt der Betrüger **vor** Schritt 1 an, dass die Bank eine „1" würfeln wird und löst die obige lineare modulare Gleichung durch Multiplikation beider Seiten mit der zu v modularen inversen Zahl $v^{-1}$ (Erinnerung: $(v \cdot v^{-1}) \text{ MOD } n = 1$):

   - Betrüger gibt sich einen zu n teilerfremden Zufallswert für y vor, also $y < n$ und $ggT(y,n) = 1$
   - $y^2 \text{ MOD } n \quad = x \cdot v \text{ MOD } n \quad | \leftarrow$ beidseitige Multiplikation mit $v^{-1} \text{ MOD } n$
   - $y^2 \cdot v^{-1} \text{ MOD } n \quad = x \cdot v \cdot v^{-1} \text{ MOD } n$
   - $y^2 \cdot v^{-1} \text{ MOD } n \quad = x$

   Die Bank erbittet gemäß Schritt 1 zunächst den Wert x und – wenn sie „1" würfelt – in Schritt 2 den Wert y. Der Vergleich ergibt

   $$x \cdot v \text{ MOD } n \quad = y^2 \cdot v^{-1} \cdot v \text{ MOD } n \quad = y^2 \text{ MOD } n$$

   und veranlasst zu der falschen Annahme, dass der Betrüger der berechtigte Kunde sei.

5) **Falls Würfelergebnis „0" ist**, bittet Bank den Kunden, ihr den Wert $y = r \text{ MOD } n$ zu senden. Sie berechnet

   $$y^2 \text{ MOD } n \quad = r^2 \text{ MOD } n \quad = x$$

   und ist überzeugt, dass der Kunde tatsächlich einen geheimen Wert r gewählt hatte.

6) Hatte der Betrüger jedoch den Wert für y gemäß Schritt 4 bestimmt, kann er in diesem Fall den zu x passenden Wert $y = r \text{ MOD } n$ nicht senden, da er den Wert r nicht verwendet hatte. Für eine nachträgliche Berechnung der modularen Quadratwurzel zu x gibt es keine heute bekannten schnellen Verfahren. Die Bank wird den Betrüger also in jedem Protokollschritt mit einer Wahrscheinlichkeit von 50% entdecken.

7) Nahm der Betrüger vor Schritt 1 den Würfelwert „0" an, wählt er den Wert r und sendet $x = r^2 \text{ MOD } n$. Die Bank stellt in Schritt 5 dann fälschlicherweise „ok" fest, wenn sie tatsächlich „0" würfelt. Bei einem Wurf „1" kann der Betrüger aber $y = r \cdot s \text{ MOD } n$ nicht senden, da er den Wert von s nicht kennt und wird auch hier entlarvt (50%).