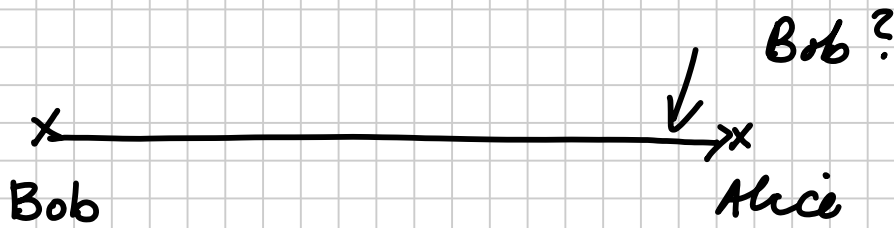


30.1.2006

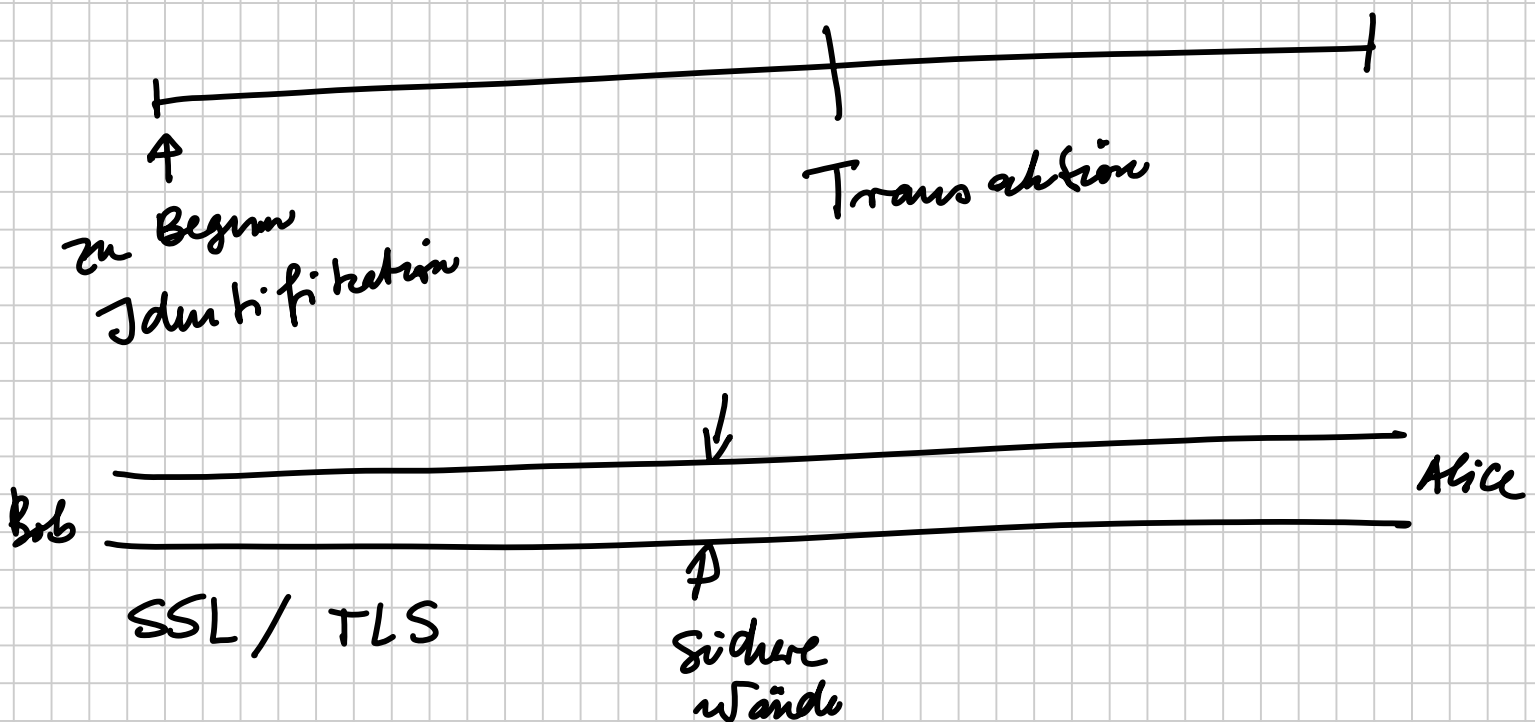
Notiztitel

30.01.2006

Identifikation



häufige Anwendung: home banking
ebay
(Parawörter)



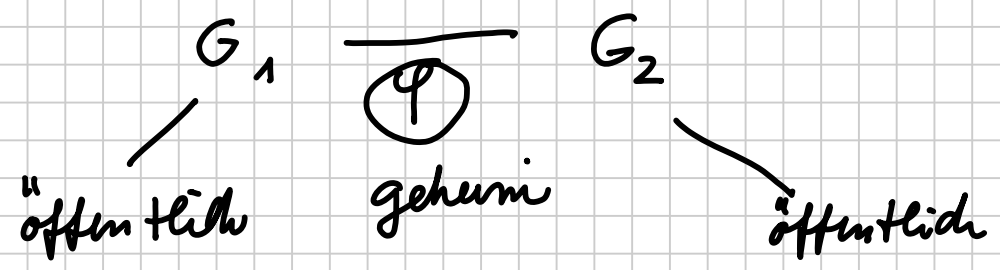
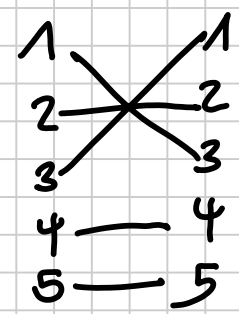
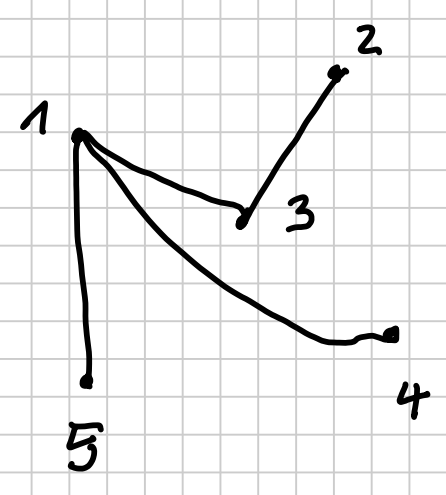
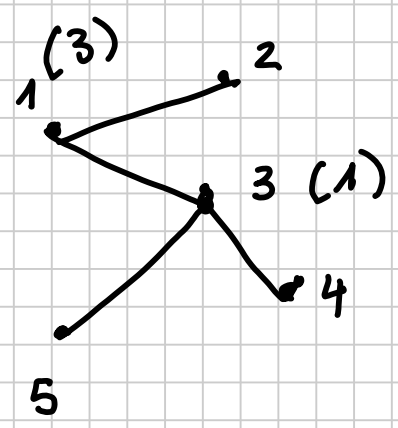
Zero knowledge Protokolle

Ich beweise, dass ich ein Geheimnis kenne.

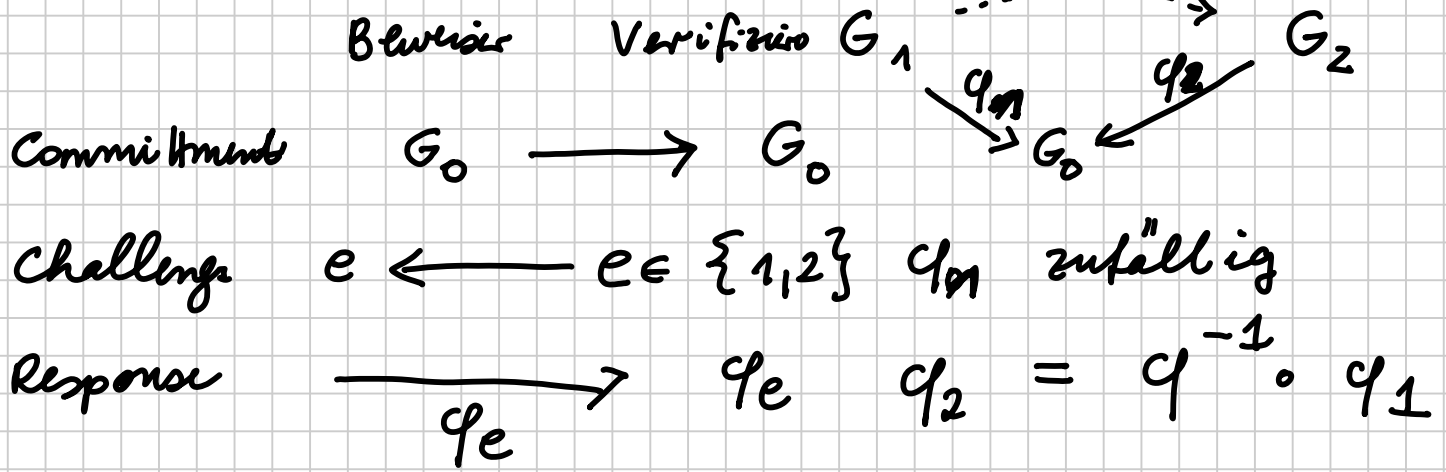
Sie glauben dem Beweis.

Aber Sie lernen nichts aus dem Beweis über das Geheimnis.

Graph-Isomorphismus



Zero knowledge Beweis



"Eine Hälfte des Weges von G_1 nach G_2 ."

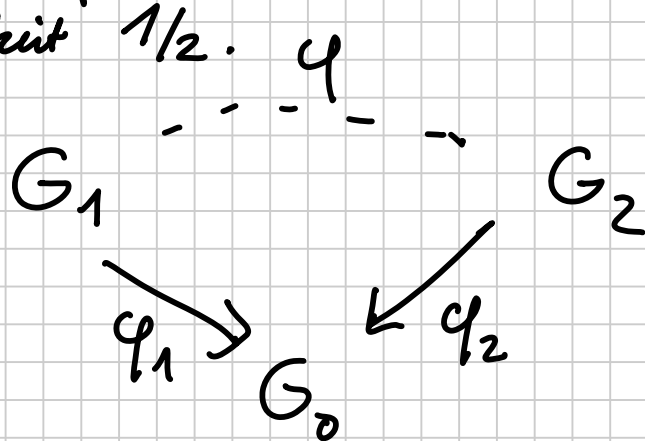
Verifikation

$$\varphi_e(G_e) \stackrel{?}{=} G_0$$

1. Correctness: Wenn beide sich ans Protokoll halten, akzeptiert der Verifizierer.

2. Soundness

Wenn der Beweiser das Geheimnis nicht kennt, fällt er auf mit Wahrscheinlichkeit $1/2$.

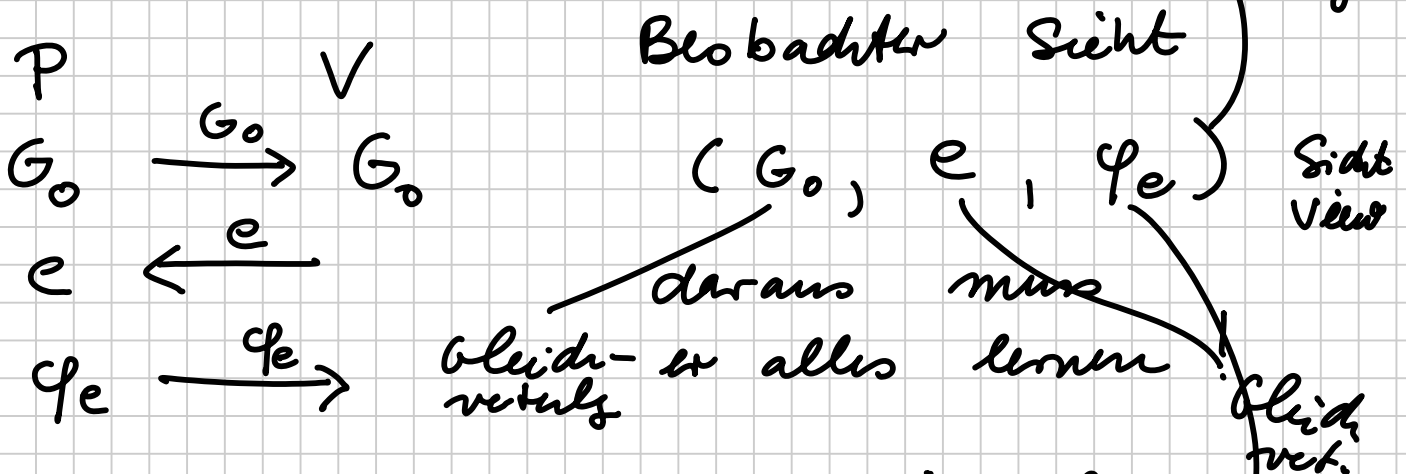


Wer das Geheimnis nicht kennt, kann nicht beide Antworten geben.

Bei 10 Durchgängen: Betrugs w. $1/2^{10}$

Zero knowledge Eigenschaft

unterliegt Wahrscheinlichkeitsverteilung



Zero knowledge: den View kann man ohne Kenntnis des Geheimnisses simulieren.

$$\varphi_e(G_e) = G_0$$

Simulator

wähle e zufällig

wähle φ_e zufällig $G_0 = \varphi_e(G_e)$

Ausgabe (G_0, e, φ_e) .

Problem: Betrügerischer Verifizierer?

polynomialer

Simulator für $(G_0, \mathbb{A}, \varphi_e)$

wähle f zufällig

wähle φ_f zufällig

\mathbb{A} zufällig
nach Wahl
Ver.

$$G_0 = \varphi_f(G_f)$$

Wähle e wie Verifizierer

wenn $e = f$, gib (G_0, e, φ_e) aus

Sonst von vorn.

Variante

Fiat - Shamir

geheim

$$n = p \cdot q, \quad r \in \{0, \dots, n-1\}$$

$$S = r^2 \pmod n$$

öffentlich

\mathbb{P}

\mathbb{V}

Commitment $x, y = x^2 \pmod n$

Challenge e

Response

Verification

$$z = r^e x \pmod n$$

$$\rightarrow y$$

$$\leftarrow e \in \{0, 1\}$$

$$\rightarrow z$$

$$z^2 \stackrel{?}{=} S \cdot y$$

mod n

$$p = 0$$

$$p = 1$$

$$x$$

$$n \cdot x \quad \text{mod } n$$