Übung zur Vorlesung „Sicherheit“
Übung 6

Thomas Agrikola
Thomas.Agrikola@kit.edu

20.07.2017

Chinese-Wall-Definition

Definition (Simple-Security-/ss-Eigenschaft)

Eine (Lese- oder Schreib-)Anfrage (s, o) hat die ss-Eigenschaft, wenn für alle $o' \in \mathcal{O}$, auf die s **schon Zugriff hatte**, gilt: $y(o) = y(o')$ oder $y(o) \notin x(o')$.

Definition ($\star$-Eigenschaft)

Eine `write`-Anfrage (s, o) hat die $\star$-Eigenschaft, falls für alle Objekte o', auf die s schon lesend zugreift, gilt: $y(o') = y(o)$ oder $x(o') = \emptyset$.

Sicherheit – Übungsblatt 6 – Aufgabe 1

- $\mathcal{C} = \{c_1, c_2, c_3\}$, $\mathcal{O} = \{o_1, o_2, o_3\}$, wobei die Firmenzugehörigkeit mit $y(o_i) = c_i$ definiert ist und die Konflikte mit Firmen wie folgt festgelegt sind:

  $$x(o_1) = \emptyset \qquad x(o_2) = \{c_1, c_3\} \qquad x(o_3) = \{c_1\}$$

- Abfolge von Zugriffen:

Anfrage	ss	$\star$	Bemerkung
(s_3, o_3) (`read`)	✓	✓	
(s_3, o_1) (`read`)	X	✓	s_3 liest schon o_3 und $y(o_1) \in x(o_3)$
(s_3, o_2) (`write`)	✓	X	s_3 liest schon o_3 und $x(o_3) \neq \emptyset$
(s_2, o_1) (`read`)	✓	✓	
(s_1, o_2) (`write`)	✓	✓	
(s_1, o_1) (`read`)	X	✓	s_1 hat schon Zugriff auf o_2 und $y(o_1) \in x(o_2)$
(s_2, o_2) (`write`)	✓	✓	(s_2 liest schon o_1, aber $x(o_1) = \emptyset$)
(s_3, o_3) (`write`)	✓	✓	
(s_2, o_3) (`read`)	X	✓	s_2 hat schon Zugriff auf o_2 und $y(o_3) \in x(o_2)$
(s_1, o_1) (`write`)	X	✓	s_1 hat schon Zugriff auf o_2 und $y(o_1) \in x(o_2)$

- Zugegriffene Objekte: s_1: o_2 $\quad$ s_2: o_1, o_2 $\quad$ s_3: o_3
  Verbotene Firmen: s_1: c_1, c_3 $\quad$ s_2: c_1, c_3 $\quad$ s_3: c_1

Bell-LaPadula-Modell

Definition (ds-Eigenschaft)

Eine Anfrage (s, o, a) erfüllt die ds-Eigenschaft wenn $a \in M_{s,o}$ gilt.

Definition (Simple-Security-/ss-Eigenschaft)

Eine Anfrage (s, o, a) mit $a \in \{\texttt{read}, \texttt{write}\}$ erfüllt die ss-Eigenschaft, wenn $f_s(s) \geq f_o(o)$ gilt.

Definition (Star Property/$\star$-Eigenschaft)

Eine Anfrage (s, o, a) mit $a \in \{\texttt{append}, \texttt{write}\}$ erfüllt die $\star$-Eigenschaft, wenn $f_c(s) \leq f_o(o)$ gilt.

Sicherheit – Übungsblatt 6 – Aufgabe 2

Gegeben sei das folgende System im Bell–LaPadula-Modell:

- Subjektmenge $\mathcal{S} = \{\text{Alice}, \text{Bob}, \text{Carol}\}$
- Objektmenge $\mathcal{O} = \{D_1, D_2, D_3, D_4\}$
- Menge der Zugriffsoperationen
  $\mathcal{A} = \{\texttt{read}, \texttt{write}, \texttt{append}, \texttt{execute}\}$
- Zugriffskontrollmatrix M gegeben durch

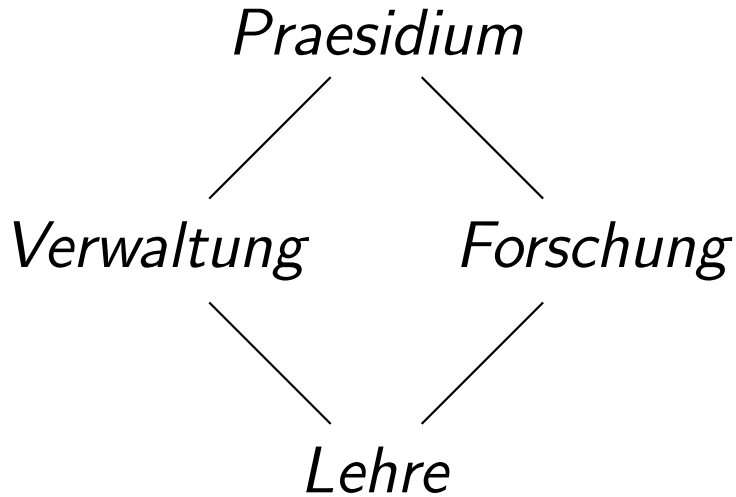
	D_1	D_2	D_3	D_4
Alice	r,w,a	r	r,w,a	r,x
Bob	r,w,a	r,w,a	r,w,a	r,x
Carol	r	r	r,w,a	r,w,a,x

Sicherheit – Übungsblatt 6 – Aufgabe 2

Zuordnung der Sicherheitsstufen $F = (f_s, f_c, f_o)$ gegeben durch

	f_s	f_c
Alice	*Verwaltung*	*Verwaltung*
Bob	*Forschung*	*Lehre*
Carol	*Praesidium*	*Forschung*

	f_o
D_1	*Verwaltung*
D_2	*Lehre*
D_3	*Forschung*
D_4	*Praesidium*



$Lehre \leq Verwaltung \leq Praesidium$; $Lehre \leq Forschung \leq Praesidium$

Sicherheit – Übungsblatt 6 – Aufgabe 2

	D_1	D_2	D_3	D_4
A	r,w,a	r	r,w,a	r,x
B	r,w,a	r,w,a	r,w,a	r,x
C	r	r	r,w,a	r,w,a,x

	f_s	f_c
A	*Verw.*	*Verw.*
B	*For.*	*Lehre*
C	*Prae.*	*For.*

	f_o
D_1	*Verw.*
D_2	*Lehre*
D_3	*For.*
D_4	*Prae.*

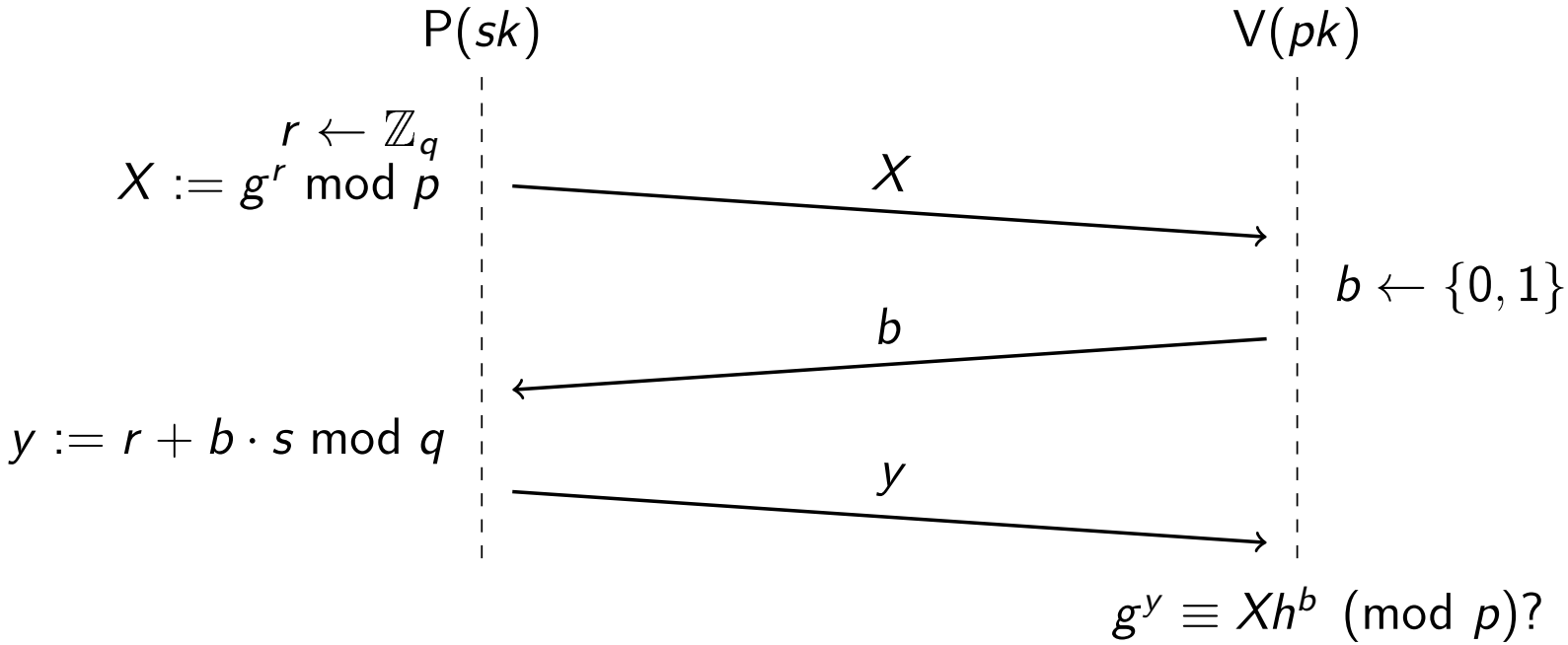
Lehre $\leq$ *Verw.* $\leq$ *Prae.* und *Lehre* $\leq$ *For.* $\leq$ *Prae.*

- Abfolge von Zugriffen (in Reihenfolge):

Anfrage	ds	ss	$\star$	Bemerkung
(Alice, D_1, a)	✓	✓	✓	
(Bob, D_2, w)	✓	✓	✓	
(Bob, D_3, r)	✓	✓	✓	$f_c(\text{Bob}) := f_o(D_3) = \textit{Forschung}$
(Carol, D_3, r)	✓	✓	✓	
(Carol, D_2, w)	X	✓	X	$\texttt{w} \notin M_{\text{Carol},D_2}$, $\neg(f_c(\text{Carol}) \leq f_o(D_2))$
(Alice, D_2, r)	✓	✓	✓	
(Bob, D_4, r)	✓	X	✓	$\neg(f_s(\text{Bob}) \geq f_o(D_4))$
(Bob, D_2, a)	✓	✓	X	$\neg(f_c(\text{Bob}) \leq f_o(D_2))$

Sicherheit – Übungsblatt 6 – Aufgabe 3

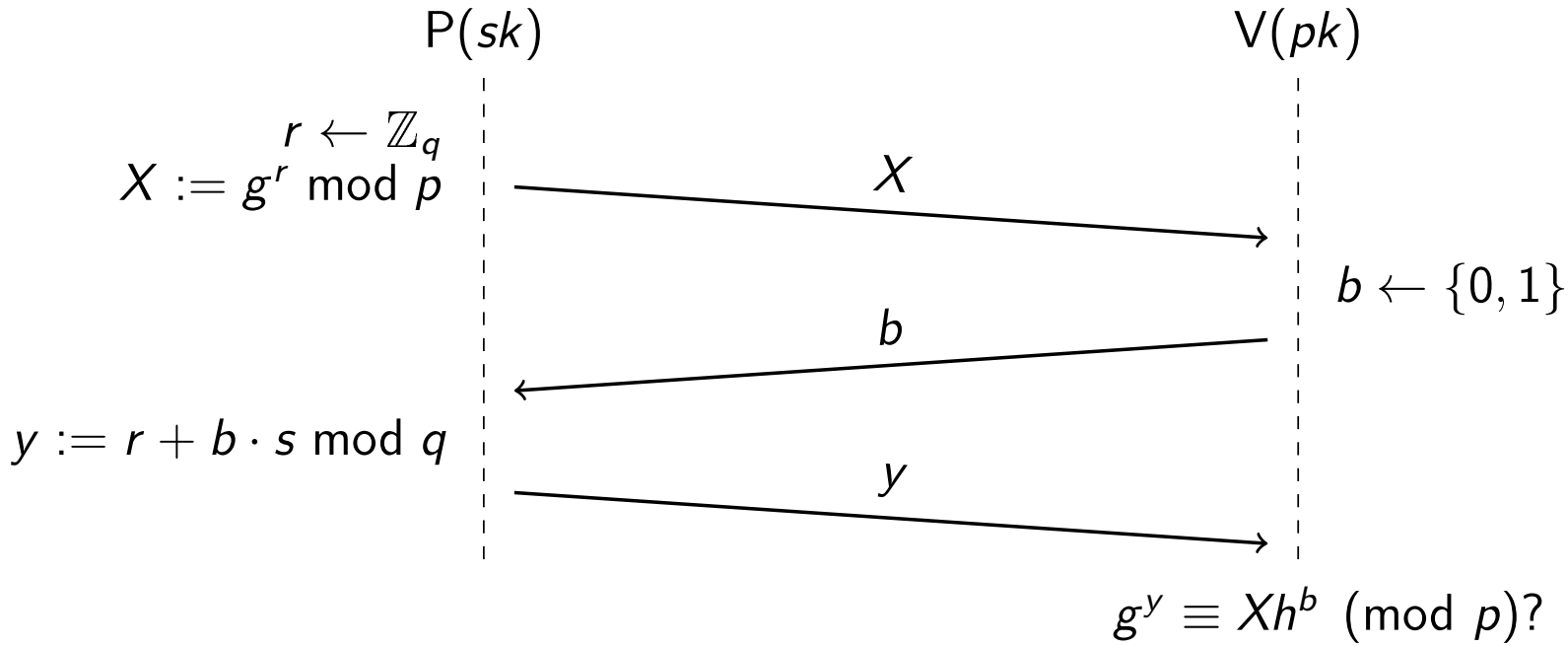
Public-Key-Identifikationsprotokoll $(\mathrm{Gen}, \mathrm{P}, \mathrm{V})$:
$\mathrm{Gen}(1^k)$: ziehe ungerades primes $l \in \mathbb{N}$, sodass $p := 2l + 1$ prim. Sei $g \in \mathbb{Z}_p^\times$ Element der Ordnung $q := \mathrm{ord}(g)$. Ziehe $s \leftarrow \mathbb{Z}_q$, setze $h := g^s \bmod p$. $pk := (\mathbb{Z}_p^\times, g, h)$, $sk := (\mathbb{Z}_p^\times, g, s)$.



P beweist V, dass er diskr. Logarithmus s von $g^s \bmod p$ kennt.

Sicherheit – Übungsblatt 6 – Aufgabe 3a

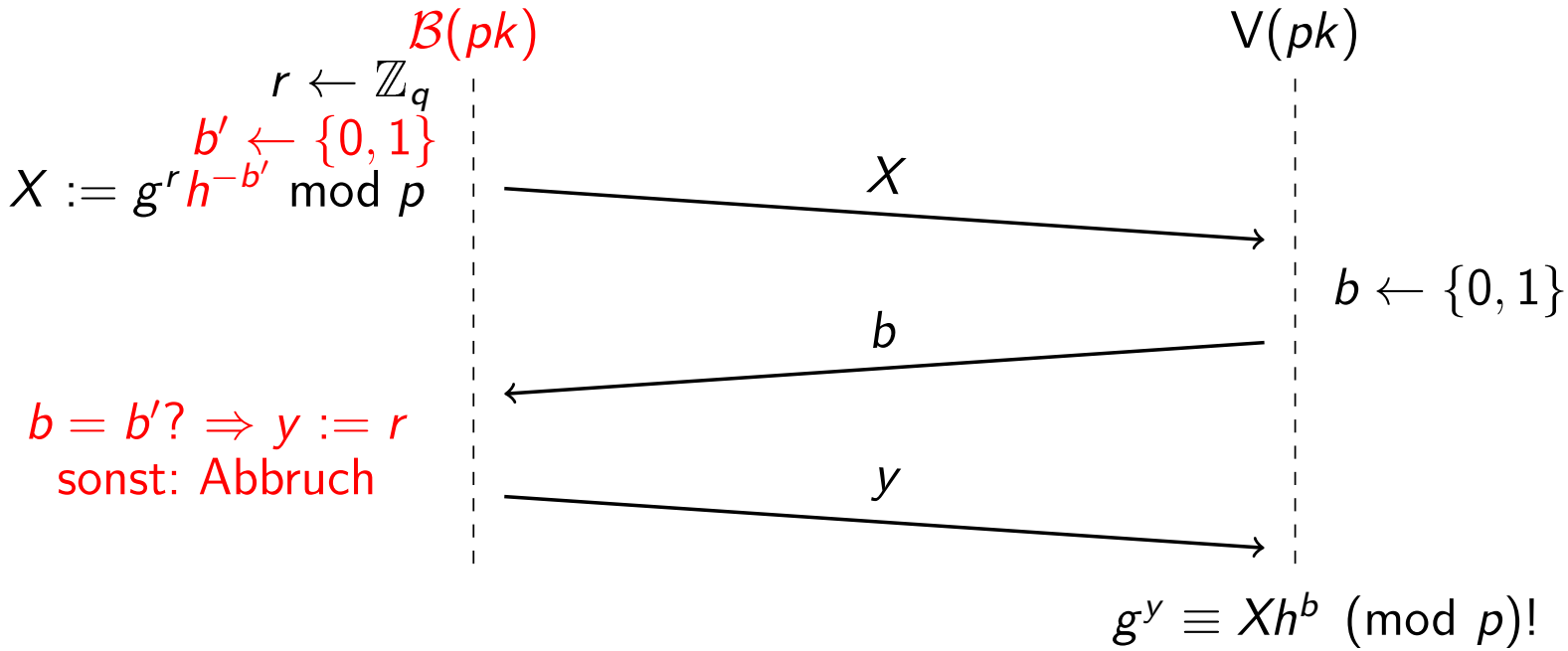
Aufgabe 3a: Zeigen Sie die Korrektheit von $(\mathsf{Gen}, \mathsf{P}, \mathsf{V})$.



Korrektheit: $g^y \equiv g^{r+b\cdot s} \equiv g^r (g^s)^b \equiv X h^b \pmod{p}$. ✓

Sicherheit – Übungsblatt 6 – Aufgabe 3b

Aufgabe 3b: Wie könnte jemand, der sk nicht kennt ehrlichen V trotzdem überzeugen? Wie wahrscheinlich ist das?



Da $g^r \bmod p$ ein zufälliges Element in $\mathbb{Z}_p^\times$ ist, ist auch $g^r h^{-b'} \bmod p$ ein zufälliges Element in $\mathbb{Z}_p^\times$. X sieht zufällig für V aus, V kann das abweichende Verhalten nicht erkennen. V wählt also b zufällig und insbes. unabhängig von b'. Mit Wahrscheinlichkeit $1/2$ haben wir $b' = b$ gezogen und überzeugen V.

Sicherheit – Übungsblatt 6 – Aufgabe 3c

Aufgabe 3c: Geben Sie einen Simulator $\mathcal{S}$ i. d. Rolle von P an.

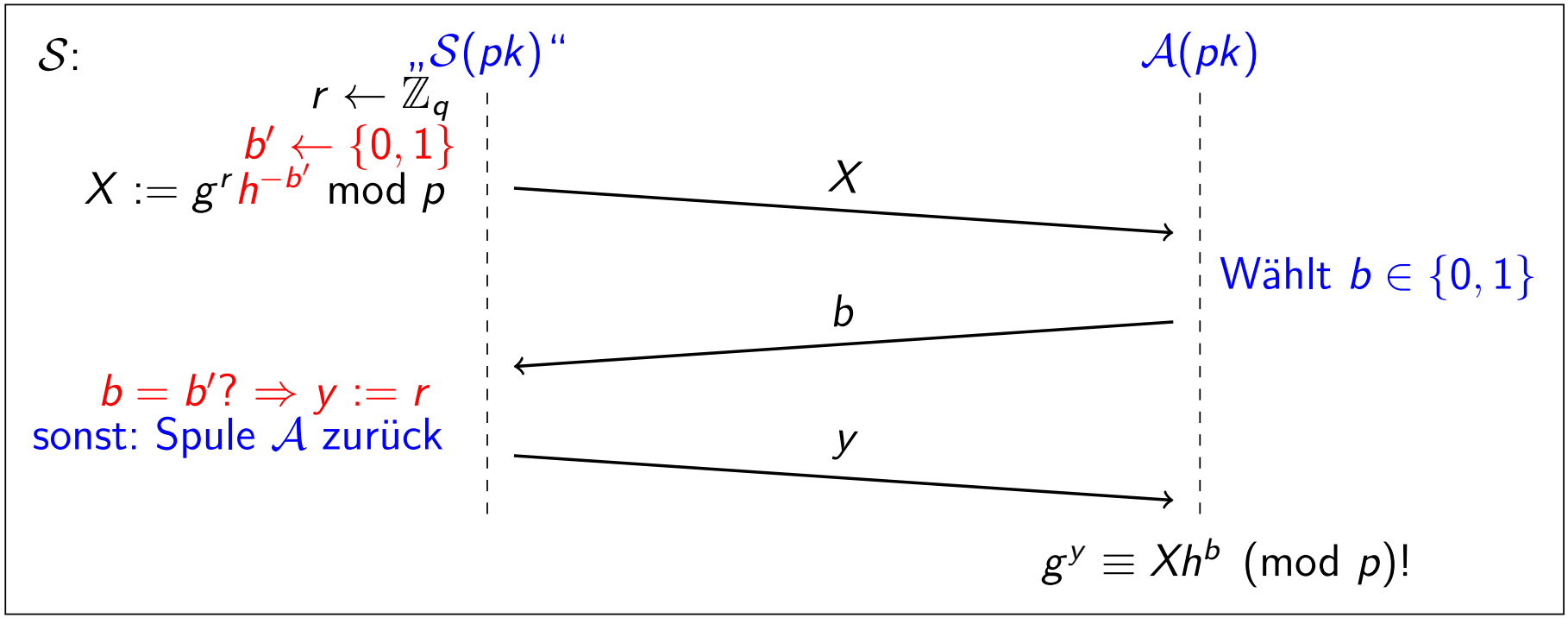
Definition (Zero-Knowledge)

Ein PK-Identifikationsprotokoll $(\mathsf{Gen}, \mathsf{P}, \mathsf{V})$ ist *Zero-Knowledge*, falls für jeden PPT-Algorithmus $\mathcal{A}$ ein PPT-Algorithmus $\mathcal{S}$ (der Simulator) existiert, so dass die folgenden Verteilungen ununterscheidbar sind (wobei $(pk, sk) \leftarrow \mathsf{Gen}(1^k)$):

$$\left(pk, \langle \mathsf{P}(sk), \mathcal{A}(1^k, pk) \rangle\right) \qquad \text{und} \qquad \left(pk, \mathcal{S}(1^k, pk)\right).$$

Sicherheit – Übungsblatt 6 – Aufgabe 3c

Aufgabe 3c: Geben Sie einen Simulator $\mathcal{S}$ i. d. Rolle von P an.



$\mathcal{S}$ gibt Transskript (X, b, y) aus. Wie in 4b): X sieht zufällig aus. Damit wählt $\mathcal{A}$ Challenge b unabhängig von b'. Jeder Durchlauf hat Erfolgswahrscheinlichkeit $1/2$. Nach k-maligem Zurückspulen terminiert $\mathcal{S}$ mit Wahrscheinlichkeit $1 - 2^{-(k+1)}$. $\mathcal{S}$ hat also im Erwartungswert polynomielle Laufzeit.

Sicherheit – Übungsblatt 6 – Aufgabe 3c

Wir zeigen: Die Ausgabeverteilungen

$$\left(pk, \langle \mathrm{P}(sk), \mathcal{A}(1^k, pk)\rangle\right) \qquad \text{und} \qquad \left(pk, \mathcal{S}(1^k, pk)\right)$$

sind ununterscheidbar.

Schon gesehen: X ist, gegeben pk, für $b' = 0$ und $b' = 1$ zufällig verteilt. Sei b die Challenge von $\mathcal{A}$, konditioniert auf $b' = b$. Es ist $\Pr[b' = b] = {}^1\!/_2$.
In diesem Fall ist für einen ehrlichen Beweiser P sowie für einen Simulator $\mathcal{S}$ für $b = 0$ und für $b = 1$ der Wert y ein zufälliger Wert aus $\mathbb{Z}_q$.

Sicherheit – Übungsblatt 6 – Aufgabe 4

Wir betrachten im Folgenden das Jacobi-Symobol $\left(\frac{a}{n}\right)$ für zwei natürliche Zahlen $a, n \in \mathbb{N}$. Dabei gilt, falls $n = p \in \mathbb{P}$ eine Primzahl ist, folgendes:

$$\left(\frac{a}{p}\right) := a^{\frac{p-1}{2}} \bmod p = \begin{cases} 1 & \text{wenn } a \text{ quadratischer Rest in } \mathbb{Z}_p^\times \\ -1 & \text{wenn } a \text{ quadratischer Nichtrest in } \mathbb{Z}_p^\times \\ 0 & \text{wenn } a \equiv 0 \bmod p \end{cases}$$

Desweiteren gelten folgende Rechenregeln für ungerades $n \in \mathbb{N}$:

* $\left(\frac{a}{n}\right) = \left(\frac{a \bmod n}{n}\right), \left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$
* $\left(\frac{a_1 a_2}{n}\right) = \left(\frac{a_1}{n}\right)\left(\frac{a_2}{n}\right), \left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$

Sicherheit – Übungsblatt 6 – Aufgabe 4a

Rechenregeln für ungerades $n \in \mathbb{N}$:

* $\left(\frac{a}{n}\right) = \left(\frac{a \bmod n}{n}\right), \left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$
* $\left(\frac{a_1 a_2}{n}\right) = \left(\frac{a_1}{n}\right)\left(\frac{a_2}{n}\right), \left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$

Berechnen Sie die Jacobi-Symbole von $\left(\frac{15}{35}\right)$, $\left(\frac{32}{33}\right)$, $\left(\frac{17}{39}\right)$

- $\left(\frac{15}{35}\right) = \left(\frac{5}{35}\right)\left(\frac{3}{35}\right) = \left(\frac{5}{7}\right)\left(\frac{5}{5}\right)\left(\frac{3}{7}\right)\left(\frac{3}{5}\right) = 0$
- $\left(\frac{32}{33}\right) = \left(\frac{-1}{33}\right) = (-1)^{\frac{33-1}{2}} = (-1)^{16} = 1$
- $\left(\frac{17}{143}\right) = \left(\frac{17}{13}\right)\left(\frac{17}{11}\right) = \left(\frac{4}{13}\right)\left(\frac{6}{11}\right) = \left(\frac{2}{13}\right)\left(\frac{2}{13}\right)\left(\frac{2}{11}\right)\left(\frac{3}{11}\right) = 1 \cdot (2^5 \bmod 11)(3^5 \bmod 11) = 1 \cdot (-1) \cdot 1 = -1$

Sicherheit – Übungsblatt 6 – Aufgabe 4b

Zeigen Sie, dass -1 für $n = pq$ mit Primzahlen p und q für die $p \equiv q \equiv 3 \bmod 4$ gilt, kein quadratischer Rest mod n ist, jedoch das Jacobi-Symbol 1 ergibt. (Solche Zahlen n nennt man Blum-Integer.)

Es gilt:

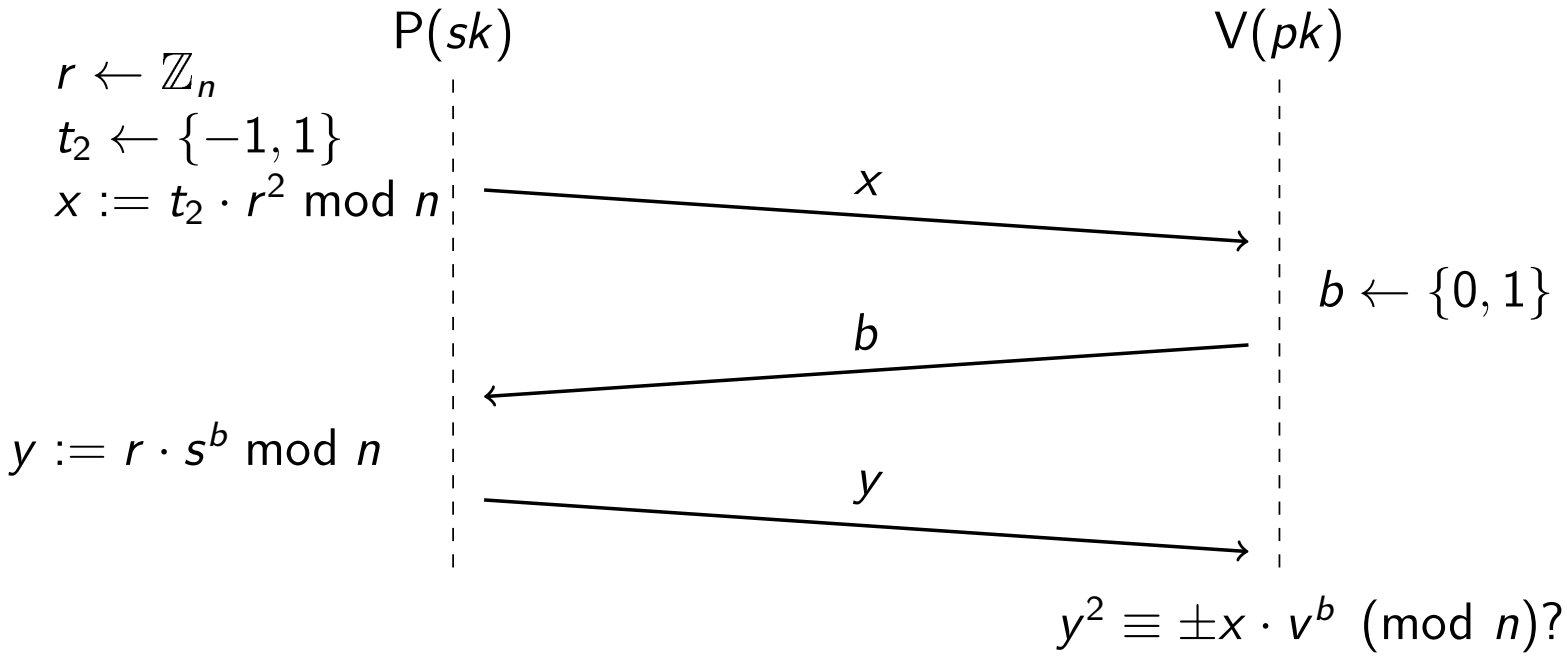
$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}(-1) = -1,$$

da $\frac{p-1}{2}$ ungerade ist ($p \equiv q \equiv 3 \bmod 4$). Für q analog, d.h. -1 ist kein quadratischer Rest in $\mathbb{Z}_p^\times$ und $\mathbb{Z}_q^\times$. Also auch nicht in $\mathbb{Z}_n$ (chinesischer Restsatz).
Allerdings gilt:

$$\left(\frac{-1}{n}\right) = \left(\frac{-1}{p}\right)\left(\frac{-1}{q}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{q-1}{2}} = (-1)(-1) = 1.$$

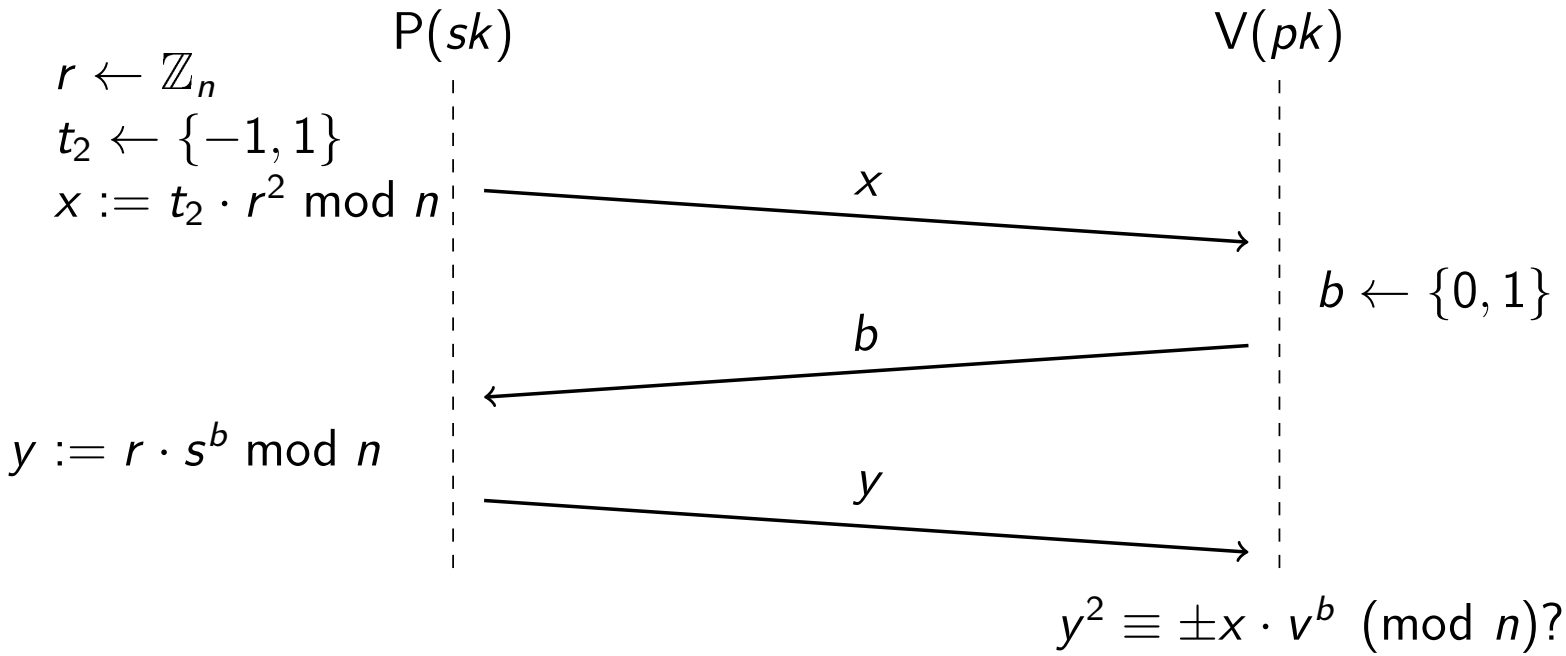
Sicherheit – Übungsblatt 6 – Aufgabe 4c

Eine vertrauenswürdige Instanz veröffentlicht einen RSA-Modulus $n = pq$, wobei n ein Blum-Integer ist. Ein Prover P möchte einem Verifier V gegenüber beweisen, dass er in Besitz eines Geheimnisses ist. Dazu wählt P geheime $s \leftarrow \mathbb{Z}_n$, $t_1 \leftarrow \{-1, 1\}$ und veröffentlicht $v = t_1 \cdot s^2 \bmod n$.



Sicherheit – Übungsblatt 6 – Aufgabe 4c(i)

Erinnerung: $v = t_1 \cdot s^2 \bmod n$

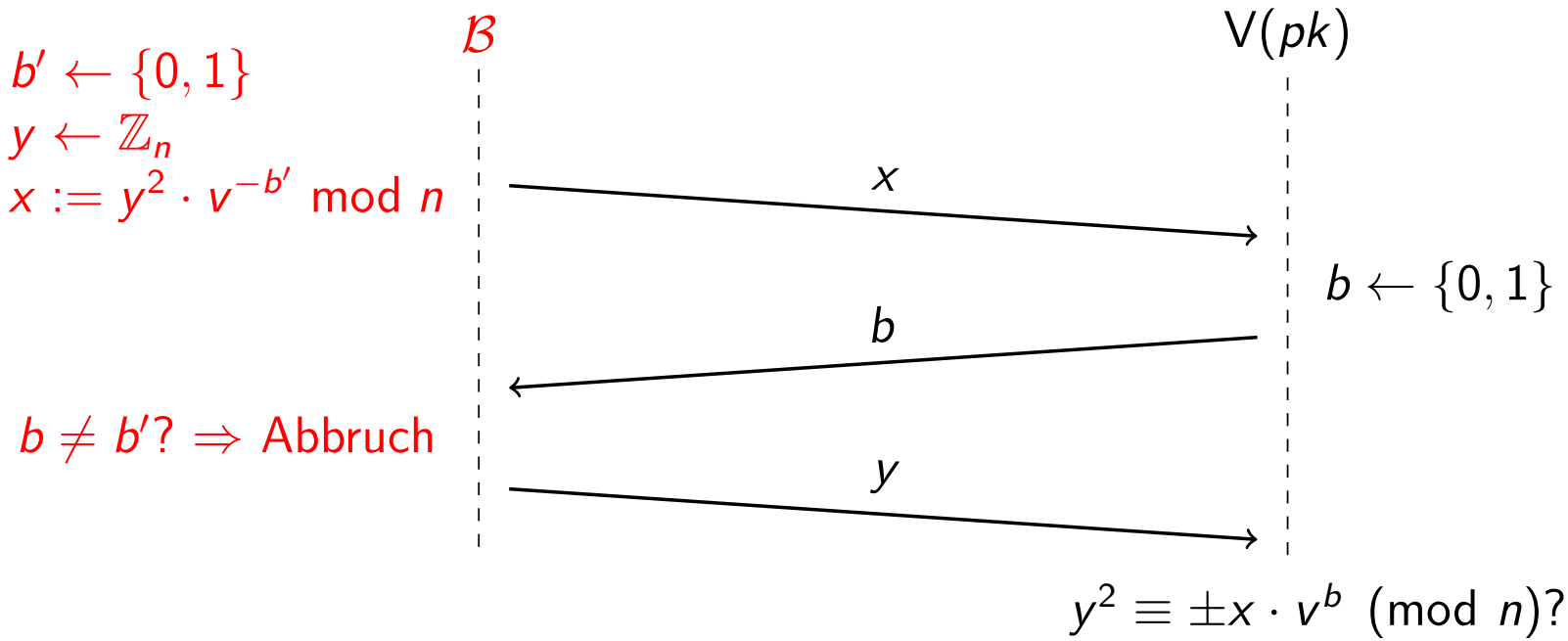


Korrektheit: Wenn P das Geheimnis s kennt, wird er V davon überzeugen können, da

$$y^2 = (rs^b)^2 = r^2 s^{2b} = t_2 x \cdot t_1 v^b = \pm x v^b \bmod n$$

Sicherheit – Übungsblatt 6 – Aufgabe 4c(ii)

Wie könnte ein Angreifer, der sk nicht kennt, V zum Akzeptieren bringen.

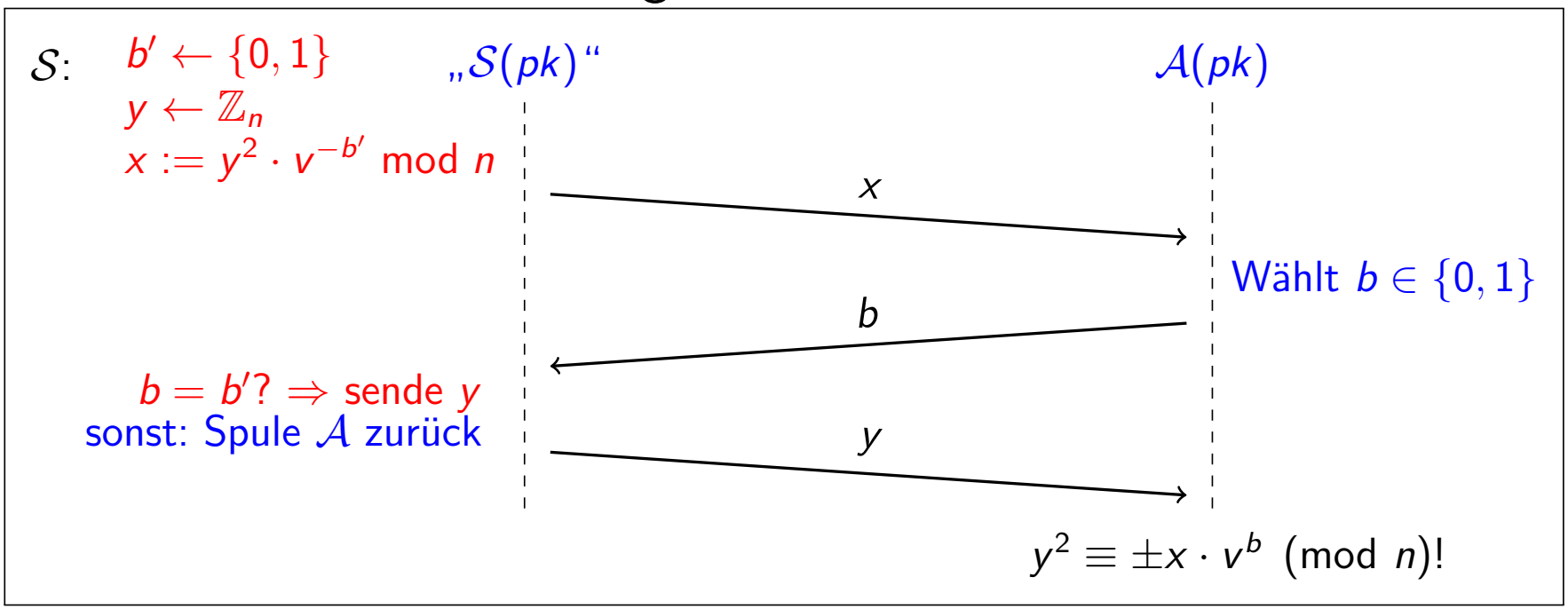


Falls b' richtig geraten wurde, akzeptiert V, denn

$$y^2 \equiv \pm x \cdot v^b \equiv y^2 \cdot v^{-b'} \cdot v^b \bmod n.$$

Sicherheit – Übungsblatt 6 – Aufgabe 4c(iii)

Geben Sie einen Simulator an, um die Zero-Knowledge Eigenschaft des Protokolls zu zeigen.



V gibt schließlich $(x, b, y, 1)$

Sicherheit – Übungsblatt 6 – Aufgabe 4c(iv)

Welche Information würde V über v lernen, falls wir das Protokoll ohne die zufälligen Vorzeichen t_1, t_2 durchführen würden?

- $t_1 = 1 \Rightarrow v := t_1 \cdot s^2 \bmod n$ ist quadratischer Rest modulo n
- $t_1 = -1 \Rightarrow v := t_1 \cdot s^2 \bmod n$ ist quadratischer Nicht-Rest modulo n
- ohne t_1 würde P beweisen, dass v zur Menge der quadratischen Reste gehört
- t_2 verschleiert dies auch bei der Überprüfung von V