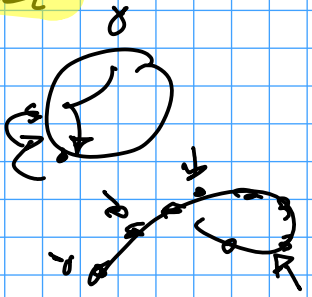
Einführung in die Kryptographie

9.2.2011

Letztes Mal: Diskrete Logarithmen

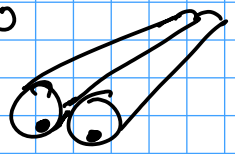
- Babystep-Giantstep
- Pollard Rho



Freiübungen einsicht:

Fr. 11.2.2011, A216

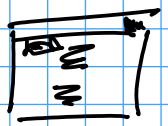
9:50 – 11:20



Dieses Mal: Digitale Signaturen III

- Pollard Rho (Nachtrag)
- Merkle Signaturverfahren
- Bonus: Shamir Secret Sharing

Klausur:

- Anmeldung Diplom
  ⇒ E-Mail 
- Raumaufteilung
  ⇒ Webseite 

Pollard Rho (Nachtrag)

letzte Vorlesung — ab jetzt falsch ✗

$$\beta_{i+1} = f(\beta_i) = \begin{cases} \alpha\,\beta_i & \beta \in G_1 \\ \beta\,\beta_i & \beta \in G_2 \\ \gamma\,\beta_i & \beta \in G_3 \end{cases}$$

$$x_{i+1} = \begin{cases} x_i & \beta_i \in G_1 \\ 2x_i & \beta_i \in G_2 \\ x_i + 1 & \beta_i \in G_3 \end{cases}$$

$$y_{i+1} = \begin{cases} y_i + 1 & \beta_i \in G_1 \\ 2y_i & \beta_i \in G_2 \\ y_i & \beta_i \in G_3 \end{cases}$$

Buch — ab jetzt richtig ✓

$$\beta_{i+1} = f(\beta_i) = \begin{cases} \gamma\,\beta_i & \beta \in G_1 \\ \beta\,\beta_i & \beta \in G_2 \\ \alpha\,\beta_i & \beta \in G_3 \end{cases}$$

$$x_{i+1} = \begin{cases} x_i + 1 & \beta_i \in G_1 \\ 2x_i & \beta_i \in G_2 \\ x_i & \beta_i \in G_3 \end{cases}$$

$$y_{i+1} = \begin{cases} y_i & \beta_i \in G_1 \\ 2y_i & \beta_i \in G_2 \\ y_i + 1 & \beta_i \in G_3 \end{cases}$$

Weitere Signaturverfahren

Was bisher geschah:

Signaturverfahren	Sicherheitsannahme
RSA	RSA Problem: e-te Wurzel modulo n (unbekannte Gruppenordnung)
El Gamal	DL in $(\mathbb{Z}/p\mathbb{Z})^*$ schwer
DSA	DL in $H \leq (\mathbb{Z}/p\mathbb{Z})^*$ $\lvert H\rvert = q$ schwer
Lamport-Diffie Einmalsignatur	Hashfunktion Einweg

Signaturverfahren	Sicherheitsannahme
RSA	RSA Problem: e-te Wurzel modulo n (unbekannte Gruppenordnung)
El Gamal	DL in $(\mathbb{Z}/p\mathbb{Z})^*$ schwer
DSA	DL in $H \leq (\mathbb{Z}/p\mathbb{Z})^*$ $\lvert H\rvert = q$ schwer
Lamport-Diffie Einmalsignatur	Hashfunktion Einweg

- Für Quantencomputer ist RSA und DL einfach! [Shor 1994]
- Viele kryptographische Hashfunktionen

  $\Rightarrow$ Viele LD Sicherheitsannahmen

Wir brauchen mehrfach Signatur auf Basis von Hashfkt!

⇒ Merkle 1979

Hashfkt $h: \{0,1\}^{2n} \to \{0,1\}^n$, Einmalsignatur

Aufgabe: Verfahren für $N = 2^h$ Signaturen

Lösung:

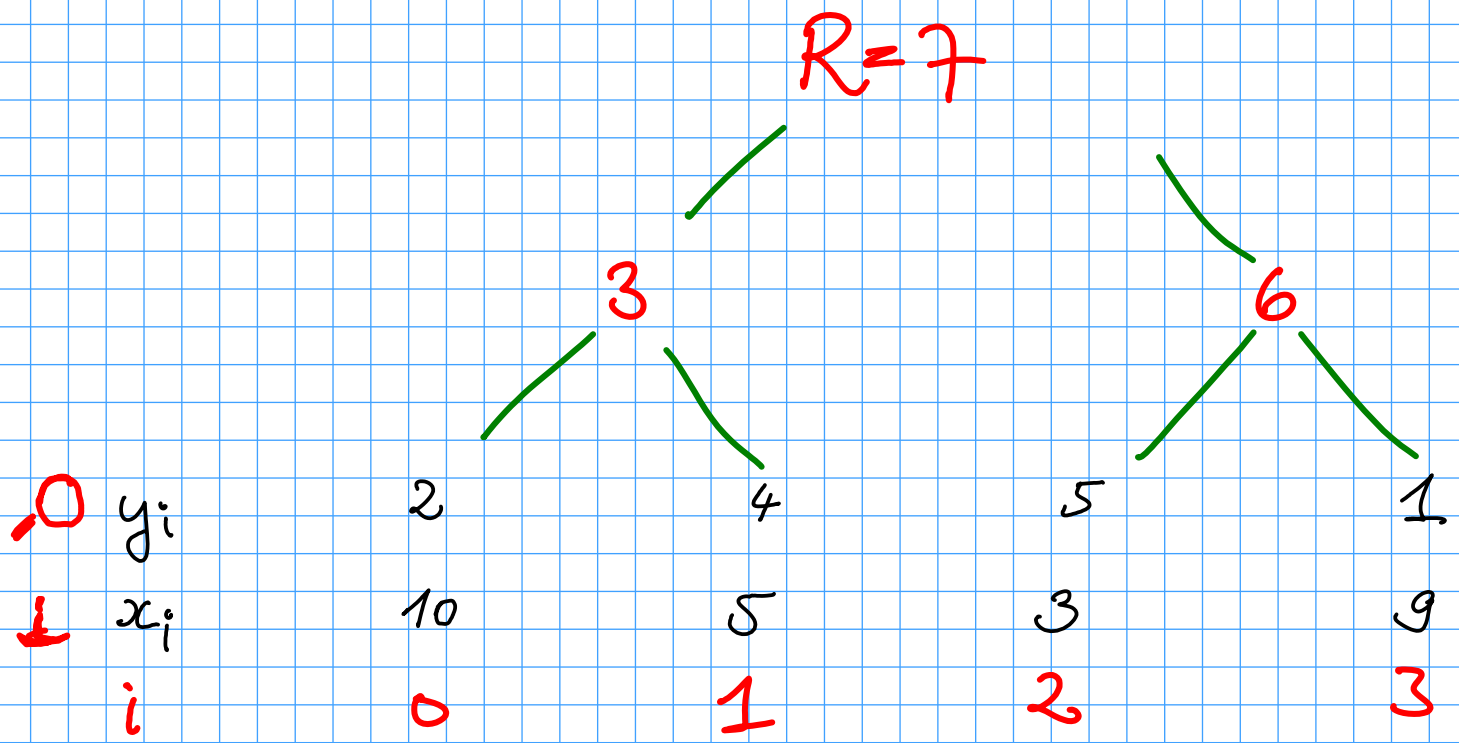
merkle.pptx

in Powerpoint

auf Englisch

Beispiel: $h(a|b) = 2^a 5^b \mod 11$ $\quad N = 2^2$

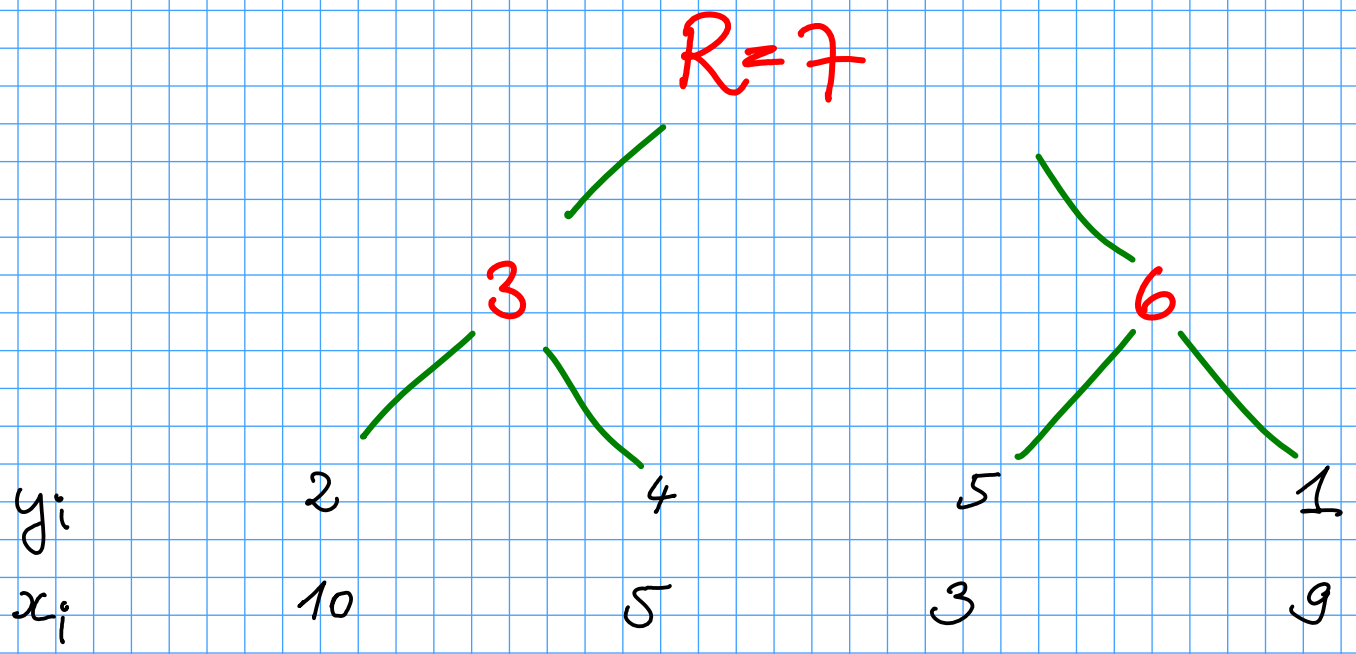
a,b	2^a	5^b
1	2	5
2	4	3
3	8	4
4	5	9
5	10	1
6	9	
7	7	
	3	
	6	
	1	



Einmalsignatur $(m, i=2)$ ist $s=3$

Merklesignatur $(i=2, s=3, y_2=5, 1, 3)$

Beispiel: $h(a|b) = 2^a 5^b \mod 11$ $N = 2^2$



a, b	2^a	5^b
1	2	5
2	4	3
3	8	4
4	5	9
5	10	1
6	9	
7	7	
	3	
	6	
	1	

Einmalsignatur $(m, i=2)$ ist S

Merklesignatur $(i, S, y_i, \text{"Pfad zu R"})$

Woher weiß der Verifizierer ob die Knoten Rechts oder Links sind?

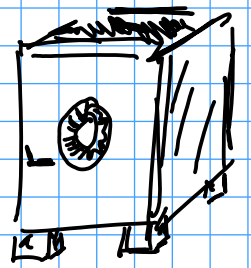
→ Binärdarstellung von i

Fragen?

Bonus: Shamir Secret Sharing

Sei $n, t \in \mathbb{N}$, $t \leq n$, $p \in \mathbb{P}$, $p > n$

Geheime Safe Kombination $s \in \mathbb{Z}/p\mathbb{Z}$



10^7 €

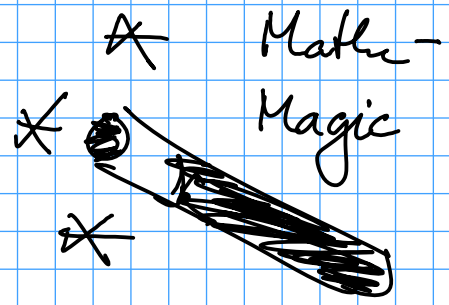
Ziel: Geheimnis aufteilen in $y_1, \ldots, y_n$

So dass

1) Mit t Teilen: s kann exakt berechnet werden

2) Mit $< t$ Teilen: <u>Kein Vorteil</u> beim Raten von s

Mathematischer Hintergrund:



Jedes Polynom $a(x) \in \mathcal{P} = (\mathbb{Z}/p\mathbb{Z})[x]$

mit $\text{Grad}(a) < t$

kann mit t Stützstellen $(x_i, \underbrace{a(x_i)}_{=y_i})$ x_i paarweise versch.

eindeutig bestimmt werden.

$$a(x) = \sum_{i=1}^{t} y_i \prod_{\substack{j=1 \\ j \neq i}}^{t} \frac{x_j - x}{x_j - x_i}$$

Lagrange Interpolation

Beweis: "Übung"

Shamirs Lösung (1979):

- Wähle $a_1, \dots, a_{t-1}$ zufällig in $\mathbb{Z}/p\mathbb{Z}$

$$a(x) = s + a_1 x + a_2 x^2 + \dots + a_{t-1} x^{t-1}$$

- $y_i = a(i)$ für $i = 1, \dots, n$.

Rekonstruktion: Grad$(a) < t$, also kann es mit t Stützstellen (i, y_i) interpoliert werden, $s = a(0)$

Sicherheit: Jedes Konstante Term s' ist Stützstelle $(0, s')$

Mit $(t-1)$ Stützstellen kann man jeweils $a'(x)$ mit Grad$(a') < t$ interpolieren

Beispiel: $n = 4$, $t = 2$, $p = 11$

$s = 4$ $\quad a(x) = 4 + 7x \mod 11$

$y_1 = 8$ $\quad y_2 = 7$ $\quad y_3 = 3$ $\quad y_4 = 10$

$y_1 = 8$ $\quad y_2 = 7$ $\quad y_3 = 3$ $\quad y_4 = 10$

Rekonstruiert mit y_2 y_3:

$$a(x) = 7 \frac{x-3}{-1} + 3 \frac{x-2}{1} \mod 11$$?

$$a(x) = 7 \cdot \frac{3-x}{3-2} + 3 \frac{2-x}{2-3} \mod 11$$

$$a(0) = 10 + (-6) \mod 11 = 4$$

Klausur Theorie Brainstorming

! Kein Gewähr auf Vollst.

Rechnen im AES Körper

Zyklische Gruppen

Permutationschiffren
Affin lineare Chiffren
Chiffren Modi

> Angriffe

Chinesischer Restsatz

El Gamal
DSA
Diffie-Hellman
RSA Verschlüsselung
Signatur

Hashfunktion — Eigenschaften
— Signaturverfahren
— Angriffe

DL — Babystep GS
— Pollard Rho

(kein Common Modulus Angriff)

Perfekte Sicherheit
Shannon

Danke für die Aufmerksamkeit!

Noch Fragen?