RSA Verfahren (Korrektheit, Laufzeiten, Sicherheit)

Übersicht noch mal

1. 2 große Primzahlen p, q $p \neq q$ $n = p \cdot q$

   wählen/bestimmen — modulo n rechnen

   $\varphi(n) = (p-1)(q-1)$

2. Wähle/bestimme $e \in \mathbb{N}$ mit $ggT(e, \varphi(n)) = 1$ (n, e) public-key

3. Berechne $d \in \mathbb{N}$ mit $e \cdot d \equiv 1 \bmod \varphi(n)$ (n, d) privat-key

   (mult. Inverses in $\mathbb{Z}_{\varphi(n)}^*$)

Verschlüsseln: $N' = \{0, 1, 2, \ldots, n-1\}$ Nachrichten mengen

$E : N' \to N'$ $E(x) = x^e \bmod n$

Entschlüsseln: $D : N' \to N'$ $D(y) = y^d \bmod n$

$D(E(m)) = m \; (= E(D(m)))$

$\forall m \in N'$

Korrektheit

Laufzeiten / Sicherheit $n = p \cdot q$ $\varphi(n) = (p-1)(q-1)$

1. Primzahlen $< n$, $\sim \frac{n}{\ln n}$ $\log_2 n$ Eingabegröße

$\ln n$ viele Primzahltests.

Polynomiell in Eingabegröße

AKS-Test

Miller-Rabin Monte-Carlo

2. $ggT(e, \varphi(n)) = 1$

Diese Zahlen $< n$

$\sim \frac{n}{\log(\log n)}$

$\log(\log n)$ viele Euklid-Alg. Ausführungen

3. $ggT(e, \varphi(n)) = 1$ d bereits ausgerechnet

Polynomielle Laufzeit? $C \cdot \log_2(n)^k$ k fest evtl. groß

Primfaktorzerlegung

läßt sich zumindest nur exponentiell in $\log_2(n)$ lösen.

Kap 5. Mathematische Logik

- + Formalisieren von Beweisen
- + Verifikation von Programmen
- + Repräsentieren von Wissen
- + Artificial Intelligence

Automatisieren!

Bedeutung

"Aus A folgt B" A, B Aussagen

$A \Rightarrow B$ Notation

5.1 Aussagenlogik

- + Atomare Axiome wahr/falsch
- + Verknüpfungen
- + Klass Konzept!
- + Korrektheit / Vollständigkeit

5.2 Prädikatenlogik

- + Quantoren $\forall, \exists$
- + starres Modell, Universen
- + komplexere Aussagen
- + Vollständigkeit / Korrektheit ?

Syntax $\leftrightarrow$ Semantik

5.1.1 Syntax

($A, B, C, D, X, Y, Z, W, \ldots$)

Definition 5.1 Menge $AV = \{x_1, x_2, x_3, x_4, \ldots\}$
abzählbar unendlich viele Aussagenvariablen

Die Menge AL der aussagenlogischen Formeln ist die kleinste Sprache über dem Alphabet $AV \cup \{0, 1, \wedge, \vee, \neg, \rightarrow, \leftrightarrow, (,)\}$
mit folgenden Eigenschaften

a) $0 \in AL$, $1 \in AL$ $\quad \forall x \in AV : x \in AL$

b) $\forall \varphi_1 \in AL : \neg \varphi_1 \in AL$ (Negation)

$\forall \varphi_1, \varphi_2 \in AL : (\varphi_1 \wedge \varphi_2) \in AL$ (Konjunktion)

$(\varphi_1 \vee \varphi_2) \in AL$ (Disjunktion)

$(\varphi_1 \to \varphi_2) \in AL$ (Implikation)

$(\varphi_1 \leftrightarrow \varphi_2) \in AL$ (Äquivalenz)

"Lösung"

Bezüglich Schritt: $\Sigma = AV \cup \{0, 1, \overset{\neg}{\wedge}, \vee, \to, \leftrightarrow, (,)\}$

AL rekursiv konstruiert über die Vorschriften!

$$\bigcap L = AL$$

(L Sprache über Σ und die die Bedingungen a) und b) erfüllt)

BSP $\neg(x_1) \notin AL$ $((x_1 \vee \neg x_2)) \notin AL$ $(x_1) \notin AL$

Vorsicht, Automatismen, nichts vergessen!

$$\big((x_1 \to x_2) \leftrightarrow (\neg x_2 \to \neg x_1)\big) \in AL$$

Aufbau / Syntax festgelegt

↓

→ , ⇒

Strukturelle Induktion

Bsp: Eigenschaft E (Aussage) über AL-Formeln gilt:

Ind. Anfang: $0, 1$ und $x \in AV$ erfüllen E

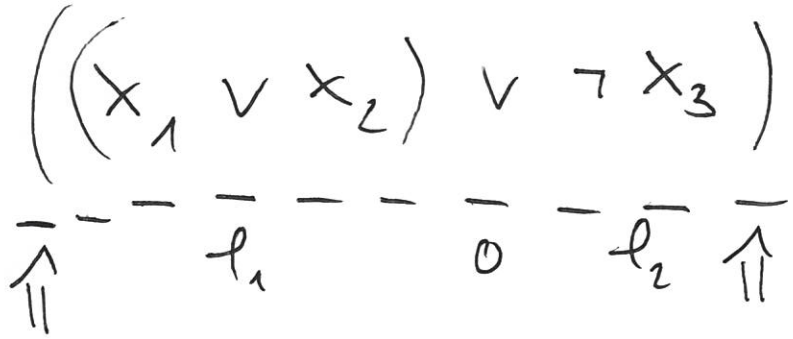
Ind. Ann: Die Aussage gilt schon für $\varphi_1, \varphi_2 \in AL$

Ind. Schritt: Zeige, dass E auch für $\neg\varphi_1$ und für $(\varphi_1 \wedge \varphi_2)$, $(\varphi_1 \vee \varphi_2)$, $(\varphi_1 \to \varphi_2)$ und $(\varphi_1 \leftrightarrow \varphi_2)$ gilt. (Unter der Ann.)

$\neg(\varphi_1 \circ \varphi_2)$ $\quad \circ \in \{\wedge, \vee, \to, \leftrightarrow\}$

Abkürzen ?!

Aussage: Kein echtes Präfix (Anfangswort) (ungleich ε) einer AL-Formel ist selbst eine AL-Formel.



Strukturelle Induktion

Ind. Anfang: $0, 1, X \in AV$

ε einziges Präfix, Aussage gilt

Ind. Annahme: Aussage gilt für $\ell_1 \in AL$, $\ell_2 \in AL$

Ind. Schritt: $\neg \ell_1$ Betrachte

als Zwischenteile $\neg \ell' \ell = \neg \ell_1$

Ann. $\neg \ell'$ echtes Präfix von $\neg \ell_1$ und $\neg \ell' \in AL$

$\Rightarrow \ell_1 = \ell' \ell$, $\ell' \in AL$, ℓ' echtes Präfix von ℓ_1 $\lightning$ Ind. Ann.

Analog:

$(\ell_1 \circ \ell_2)$

wie sieht ein echtes Präfix aus?

Konsequenz $\rightsquigarrow$ Endentje Zerlegung,
Endentje Lesbarkeit

$$\varphi = (\varphi_1 \circ \varphi_2) \quad \circ \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$$

$$\varphi = (\varphi_1' \circ' \varphi_2') \quad \circ' \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$$

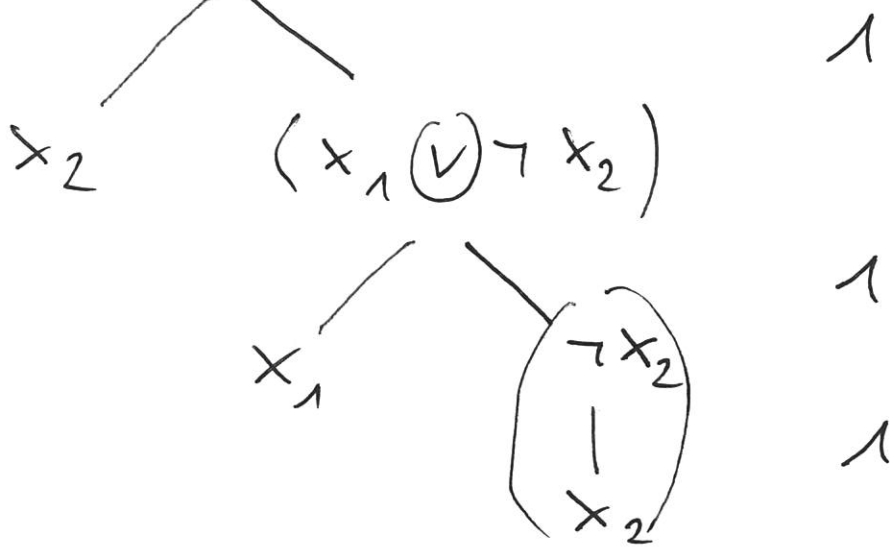
$$\Rightarrow \quad \circ' = \circ \qquad \varphi_1' = \varphi_1 \qquad \varphi_2' = \varphi_2$$

„so kurz wie zwei Zerlegungen"

Syntaxbaum

endentje

$$\overline{\varphi} = \left(x_2 \,\textcircled{\wedge}\, (x_1 \vee \neg x_2)\right)$$



Induktive / Rekursive Tiefe $d(\varphi)$ PAL-Formel

I. $d(0) = d(1) = d(x) = 0 \quad \forall x \in AV$

II. $\varphi \in AL \Rightarrow d(\neg\varphi) = d(\varphi) + 1$

III. $\varphi_1, \varphi_2 \in AL \quad \circ \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$

$$d(\varphi_1 \circ \varphi_2) = \max\{d(\varphi_1), d(\varphi_2)\} + 1$$

$$\begin{aligned} d(\overline{\varphi}) &= \max\{d(x_2), d((x_1 \vee \neg x_2))\} \\ &= d((x_1 \vee \neg x_2)) + 1 \\ &\vdots \\ &= 3 \end{aligned}$$

Andere Definition auch so möglich!

z.B. $VAR(\varphi)$ Variablenmenge

5.1.2 Semantik

Menge der Variablen von AL-Formel φ (induktiv / rekursiv)

$VAR(0) := VAR(1) := \emptyset$

$VAR(x) := \{x\} \quad x \in AV$

$\forall \varphi_1, \varphi_2 \in AL \quad \circ \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$

$VAR(\neg\varphi_1) := VAR(\varphi_1) \qquad VAR((\varphi_1 \circ \varphi_2)) := VAR(\varphi_1) \cup VAR(\varphi_2)$

(BSP) $VAR((x_2 \wedge (x_1 \vee \neg x_2)))$

$= VAR(x_2) \cup VAR((x_1 \vee \neg x_2))$

$\vdots$

$= \{x_1, x_2\}$

Motivation "Klausurteilnahme"

Modellierung

x_1 " StudentIn erfüllt > 50 % Übungsaufgaben "

x_2 " StudentIn erfüllt < 40 % Übungsaufgaben "

x_3 " StudentIn hat 18 vorgerechnet "

x_4 " StudentIn hat Zulassung zur Klausur "

x_5 " StudentIn hat die Klausur erfolgreich bestanden "

$$W = \{((x_1 \wedge x_3) \overset{?}{\Leftrightarrow} x_4), (x_2 \Rightarrow \neg x_1), (\neg x_4 \Rightarrow \neg x_5)\}$$

Aus W folgern dass $(x_2 \Rightarrow \neg x_5)$ ist "gültig"!

Formel gilt

Definition 5.2 Belegung / Interpretation für $X \subseteq AV$

ist Abbildung $\beta : X \to \{0,1\}$

β heißt passend für $\varphi \in AL$ $VAR(\varphi) \subseteq X$

$\varphi \in AL$ φ' "Teilformel" (kommt im Aufbau vor)

$\Rightarrow VAR(\varphi') \subseteq VAR(\varphi)$

$\Rightarrow$ β passend für φ ist auch passend für φ'

Definition 5.3

Sei $\beta : X \to \{0,1\}$ eine $f \in AL$

(passende) Belegung.

Dann besitzt f einen eindeutigen Wahrheitswert

$$\llbracket f \rrbracket_\beta \in \{0,1\}$$

induktiv wie folgt definiert:

a) $\llbracket 0 \rrbracket_\beta := 0 \quad \llbracket 1 \rrbracket_\beta := 1 \quad \llbracket x \rrbracket_\beta := \beta(x) \ \forall x \in X.$

b) $f = \neg f_1 \quad f_1 \in AL \quad \llbracket \neg f \rrbracket_\beta := 1 - \llbracket f_1 \rrbracket_\beta$

c) $f = (f_1 \circ f_2) \quad f_1, f_2 \in AL \quad \circ \in \{\wedge, \vee, \to, \leftrightarrow\}$

$$\|\varphi_1 \wedge \varphi_2\|_{\mathcal{B}} := \min\{\|\varphi_1\|_{\mathcal{B}}, \|\varphi_2\|_{\mathcal{B}}\}$$

$$\|\varphi_1 \vee \varphi_2\|_{\mathcal{B}} := \max\{\|\varphi_1\|_{\mathcal{B}}, \|\varphi_2\|_{\mathcal{B}}\}$$

$$\|(\varphi_1 \to \varphi_2)\|_{\mathcal{B}} := \|(\neg\varphi_1 \vee \varphi_2)\|_{\mathcal{B}}$$

$$\|(\varphi_1 \leftrightarrow \varphi_2)\|_{\mathcal{B}} := \begin{cases} 1 & : \text{falls } \|\varphi_1\|_{\mathcal{B}} = \|\varphi_2\|_{\mathcal{B}} \\ 0 & : \text{sonst} \end{cases}$$

Gilt $\|\varphi\|_{\mathcal{B}} = 1$ so ist φ wahr bezüglich $\mathcal{B}$

$\|\varphi\|_{\mathcal{B}} = 0$ so ist φ falsch bezüglich $\mathcal{B}$

(BSP) $(\neg x_1 \vee (x_2 \wedge \neg x_3)) = \varphi$

$\mathcal{B}(x_1) = 1 \quad \mathcal{B}(x_2) = 1 \quad \mathcal{B}(x_3) = 0$

$$\|\varphi\|_{\mathcal{B}} = \max\{\|\neg x_1\|_{\mathcal{B}}, \|x_2 \wedge \neg x_3\|_{\mathcal{B}}\}$$

$$= \max\{1 - [\![x_1]\!]_B, \min\{[\![x_2]\!]_B, [\![\neg x_3]\!]_B\}\} \quad (18)$$

$$= \max\{0, \min\{1, 1 - [\![x_3]\!]_B\}\}$$

$$= \max\{0, \min\{1, 1\}\} = 1$$

Wahrheitstabelle

	x_1	x_2	x_3	$\neg x_1$	$(x_2 \wedge \neg x_3)$	$(\neg x_1 \vee (x_2 \wedge \neg x_3))$
B_2:	1	1	0	0	1	1

Wahr bezüglich einer Belegung!

Modell, Erfüllbarkeit, Gültigkeit!