dante-Herbsttagung 2008
13. September
in der Universität Tübingen
Wilhelm-Schickard-Institut für Informatik

Eberhard Karls Universität Tübingen

Veranstalter

DANTE e. V.
Postfach 10 18 40
69008 Heidelberg

☎: +49 (6221) 2 97 66
Fax: +49 (6221) 16 79 06

Wilhelm-Schickard-Institut für Informatik
Sand 13
72076 Tübingen

Anmeldung:
`http://cms.dante.de/herbst2008`
`mv39@dante.de`
oder schriftlich an DANTE e. V.

DANTE, Deutschsprachige Anwendervereinigung TEX e.V., wurde am 14. April 1989 in Heidelberg gegründet. Der Zweck des wissenschaftlichen Vereins ist die Betreuung und Beratung von TEX-Benutzern im gesamten deutschsprachigen Raum. Außerdem werden Entwicklungen im Bereich von TEX, LATEX, METAFONT, BIBTEX, ... national und international initiiert, gefördert und koordiniert.

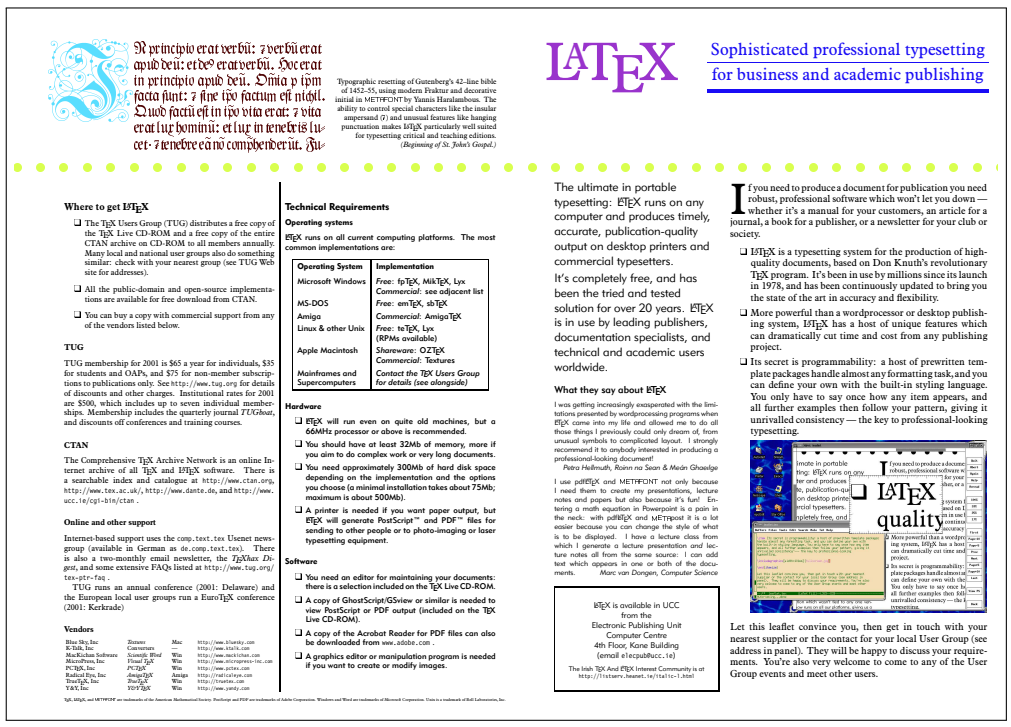
Zeitplan

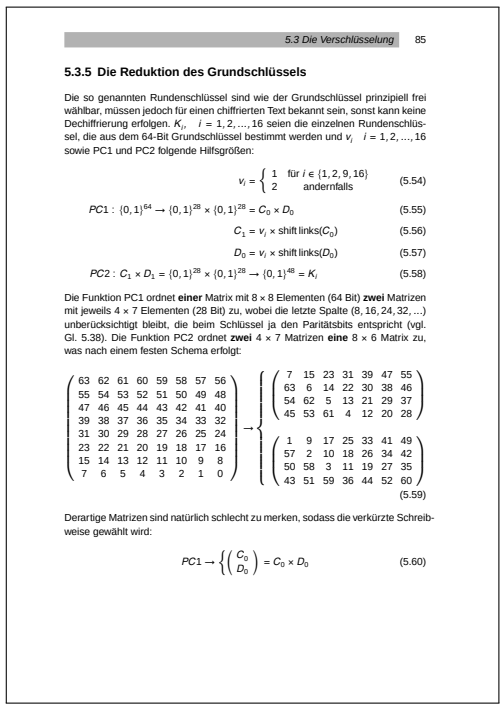
Freitag 12.9. 2008:

19:00 Uhr	Vorabendtreff im Casino, Wöhrdstraße 25

Sonnabend 13.9.:

8:30	Ausgabe Tagungsunterlagen
8:45	Begrüßung
9:00–10.15	39. Mitgliederversammlung von dante e. V.
10:30–12.30	Tutorien und Vorträge
13:00	Mittagspause
14.30–17.00	Tutorien und Vorträge
19:00	Abendtreff im „Ratskeller“, Haaggasse 4





5.3 Die Verschlüsselung 85

5.3.5 Die Reduktion des Grundschlüssels

Die so genannten Rundenschlüssel sind wie der Grundschlüssel prinzipiell frei wählbar, müssen jedoch für einen chiffrierten Text bekannt sein, sonst kann keine Dechiffrierung erfolgen. K_i, $i = 1, 2, ..., 16$ seien die einzelnen Rundenschlüssel, die aus dem 64-Bit Grundschlüssel bestimmt werden und v_i $i = 1, 2, ..., 16$ sowie PC1 und PC2 folgende Hilfsgrößen:

$$v_i = \begin{cases} 1 & \text{für } i \in \{1, 2, 9, 16\} \\ 2 & \text{anderenfalls} \end{cases} \quad (5.54)$$

$$PC1 : \{0,1\}^{64} \rightarrow \{0,1\}^{28} \times \{0,1\}^{28} = C_0 \times D_0 \quad (5.55)$$

$$C_1 = v_i \times \text{shift links}(C_0) \quad (5.56)$$

$$D_0 = v_i \times \text{shift links}(D_0) \quad (5.57)$$

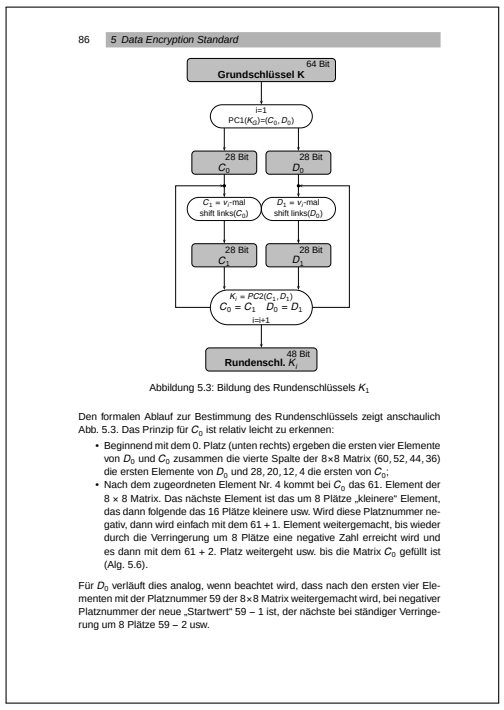
$$PC2 : C_1 \times D_1 = \{0,1\}^{28} \times \{0,1\}^{28} \rightarrow \{0,1\}^{48} = K_i \quad (5.58)$$

Die Funktion PC1 ordnet **einer** Matrix mit 8 × 8 Elementen (64 Bit) **zwei** Matrizen mit jeweils 4 × 7 Elementen (28 Bit) zu, wobei die letzte Spalte (8, 16, 24, 32, ...) unberücksichtigt bleibt, die beim Schlüssel ja den Paritätsbits entspricht (vgl. Gl. 5.38). Die Funktion PC2 ordnet **zwei** 4 × 7 Matrizen **eine** 8 × 6 Matrix zu, was nach einem festen Schema erfolgt:

$$\begin{pmatrix} 63 & 62 & 61 & 60 & 59 & 58 & 57 & 56 \\ 55 & 54 & 53 & 52 & 51 & 50 & 49 & 48 \\ 47 & 46 & 45 & 44 & 43 & 42 & 41 & 40 \\ 39 & 38 & 37 & 36 & 35 & 34 & 33 & 32 \\ 31 & 30 & 29 & 28 & 27 & 26 & 25 & 24 \\ 23 & 22 & 21 & 20 & 19 & 18 & 17 & 16 \\ 15 & 14 & 13 & 12 & 11 & 10 & 9 & 8 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \end{pmatrix} \rightarrow \left\{ \begin{pmatrix} 7 & 15 & 23 & 31 & 39 & 47 & 55 \\ 63 & 6 & 14 & 22 & 30 & 38 & 46 \\ 54 & 62 & 5 & 13 & 21 & 29 & 37 \\ 45 & 53 & 61 & 4 & 12 & 20 & 28 \end{pmatrix} \right. \left. \begin{pmatrix} 1 & 9 & 17 & 25 & 33 & 41 & 49 \\ 57 & 2 & 10 & 18 & 26 & 34 & 42 \\ 50 & 58 & 3 & 11 & 19 & 27 & 35 \\ 43 & 51 & 59 & 36 & 44 & 52 & 60 \end{pmatrix} \right\} \quad (5.59)$$

Derartige Matrizen sind natürlich schlecht zu merken, sodass die verkürzte Schreibweise gewählt wird:

$$PC1 \rightarrow \left\{ \begin{pmatrix} C_0 \\ D_0 \end{pmatrix} = C_0 \times D_0 \right. \quad (5.60)$$



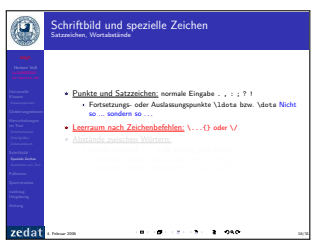
86 5 Data Encryption Standard

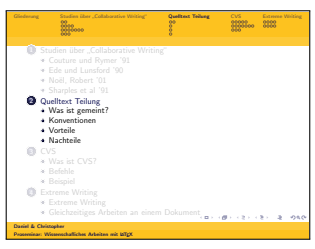
Abbildung 5.3: Bildung des Rundenschlüssels K_1

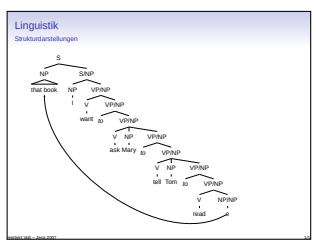
Den formalen Ablauf zur Bestimmung des Rundenschlüssels zeigt anschaulich Abb. 5.3. Das Prinzip für C_0 ist relativ leicht zu erkennen:

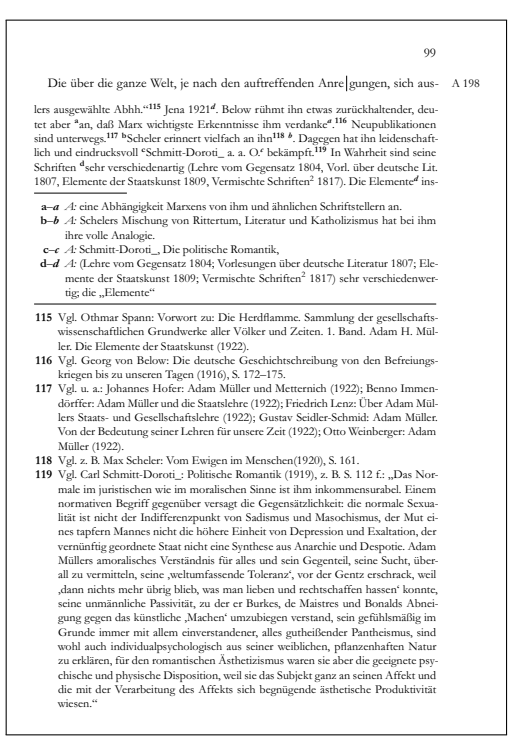
- Beginnend mit dem 0. Platz (unten rechts) ergeben die ersten vier Elemente von D_0 und C_0 zusammen die vierte Spalte der 8×8 Matrix (60, 52, 44, 36) die ersten Elemente von D_0 und 28, 20, 12, 4 die ersten von C_0;
- Nach dem zugeordneten Element Nr. 4 kommt bei C_0 das 61. Element der 8 × 8 Matrix. Das nächste Element ist das um 8 Plätze „kleinere“ Element, das dann folgende das 16 Plätze kleinere usw. Wird diese Platznummer negativ, dann wird einfach mit dem 61 + 1. Element weitergemacht, bis wieder durch die Verringerung um 8 Plätze eine negative Zahl erreicht wird und es dann mit dem 61 + 2. Platz weitergeht usw. bis die Matrix C_0 gefüllt ist (Alg. 5.6).

Für D_0 verläuft dies analog, wenn beachtet wird, dass nach den ersten vier Elementen mit der Platznummer 59 der 8×8 Matrix weitergemacht wird, bei negativer Platznummer der neue „Startwert“ 59 – 1 ist, der nächste bei ständiger Verringerung um 8 Plätze 59 – 2 usw.









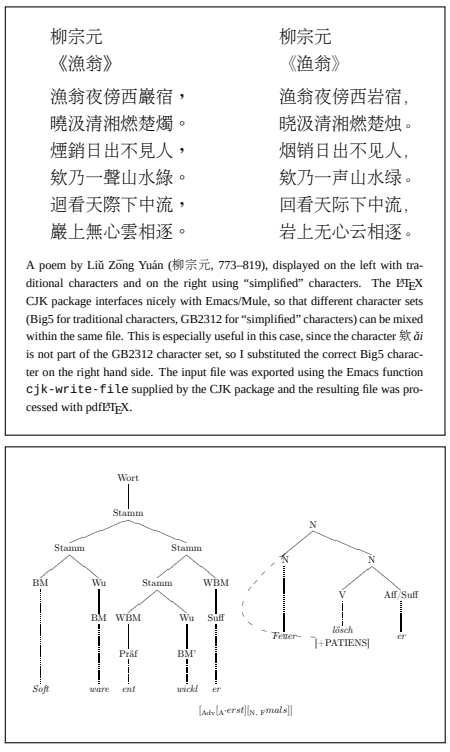
99

Die über die ganze Welt, je nach den auftreffenden Anre|gungen, sich aus- A 198

lers ausgewählte Abhh.“[115] Jena 1921[d]. Below rühmt ihn etwas zurückhaltender, deutet aber [a]an, daß Marx wichtigste Erkenntnisse ihm verdanke“.[116] Neupublikationen sind unterwegs.[117] [b]Scheler erinnert vielfach an ihn[118] [b]. Dagegen hat ihn leidenschaftlich und eindrucksvoll [c]Schmitt-Doroti_ a. a. O.[c] bekämpft.[119] In Wahrheit sind seine Schriften [d]sehr verschiedenartig (Lehre vom Gegensatz 1804, Vorl. über deutsche Lit. 1807, Elemente der Staatskunst 1809, Vermischte Schriften[2] 1817). Die Elemente[d] ins-

a–a *A:* eine Abhängigkeit Marxens von ihm und ähnlichen Schriftstellern an.
b–b *A:* Schelers Mischung von Rittertum, Literatur und Katholizismus hat bei ihm ihre volle Analogie.
c–c *A:* Schmitt-Doroti_, Die politische Romantik,
d–d *A:* (Lehre vom Gegensatz 1804; Vorlesungen über deutsche Literatur 1807; Elemente der Staatskunst 1809; Vermischte Schriften[2] 1817) sehr verschiedenwertig; die „Elemente“

115 Vgl. Othmar Spann: Vorwort zu: Die Herdflamme. Sammlung der gesellschaftswissenschaftlichen Grundwerke aller Völker und Zeiten. 1. Band. Adam H. Müller. Die Elemente der Staatskunst (1922).
116 Vgl. Georg von Below: Die deutsche Geschichtschreibung von den Befreiungskriegen bis zu unseren Tagen (1916), S. 172–175.
117 Vgl. u. a.: Johannes Hofer: Adam Müller und Metternich (1922); Benno Immendörffer: Adam Müller und die Staatslehre (1922); Friedrich Lenz: Über Adam Müllers Staats- und Gesellschaftslehre (1922); Gustav Seidler-Schmid: Adam Müller. Von der Bedeutung seiner Lehren für unsere Zeit (1922); Otto Weinberger: Adam Müller (1922).
118 Vgl. z. B. Max Scheler: Vom Ewigen im Menschen(1920), S. 161.
119 Vgl. Carl Schmitt-Doroti_: Politische Romantik (1919), z. B. S. 112 f.: „Das Normale im juristischen wie im moralischen Sinne ist ihm inkommensurabel. Einem normativen Begriff gegenüber versagt die Gegensätzlichkeit: die normale Sexualität ist nicht der Indifferenzpunkt von Sadismus und Masochismus, der Mut eines tapfern Mannes nicht die höhere Einheit von Depression und Exaltation, der vernünftig geordnete Staat nicht eine Synthese aus Anarchie und Despotie. Adam Müllers amoralisches Verständnis für alles und sein Gegenteil, seine Sucht, überall zu vermitteln, seine ‚weltumfassende Toleranz‘, vor der Gentz erschrack, weil ‚dann nichts mehr übrig blieb, was man lieben und rechtschaffen hassen‘ konnte, seine unmännliche Passivität, zu der er Burkes, de Maistres und Bonalds Abneigung gegen das künstliche ‚Machen‘ umzubiegen verstand, sein gefühlsmäßig im Grunde immer mit allem einverstandener, alles gutheißender Pantheismus, sind wohl auch individualpsychologisch aus seiner weiblichen, pflanzenhaften Natur zu erklären, für den romantischen Ästhetizismus waren sie aber die geeignete psychische und physische Disposition, weil sie das Subjekt ganz an seinen Affekt und die mit der Verarbeitung des Affekts sich begnügende ästhetische Produktivität wiesen.“



柳宗元
《漁翁》

漁翁夜傍西巖宿，
曉汲清湘燃楚燭。
煙銷日出不見人，
欸乃一聲山水綠。
迴看天際下中流，
巖上無心雲相逐。

柳宗元
《渔翁》

渔翁夜傍西岩宿，
晓汲清湘燃楚烛。
烟销日出不见人，
欸乃一声山水绿。
回看天际下中流，
岩上无心云相逐。

A poem by Liǔ Zōng Yuán (柳宗元, 773–819), displayed on the left with traditional characters and on the right using “simplified” characters. The LaTeX CJK package interfaces nicely with Emacs/Mule, so that different character sets (Big5 for traditional characters, GB2312 for “simplified” characters) can be mixed within the same file. This is especially useful in this case, since the character 欸 *ăi* is not part of the GB2312 character set, so I substituted the correct Big5 character on the right hand side. The input file was exported using the Emacs function `cjk-write-file` supplied by the CJK package and the resulting file was processed with pdfLaTeX.

Resultate:[13]

Abbildung 1: Group identification functions from native speakers of standard French for three *côte-cotte* (/o/–/ɔ/) series that differ in vowel duration.

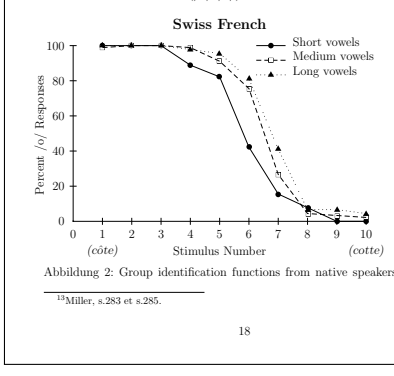


Abbildung 2: Group identification functions from native speakers of Swiss

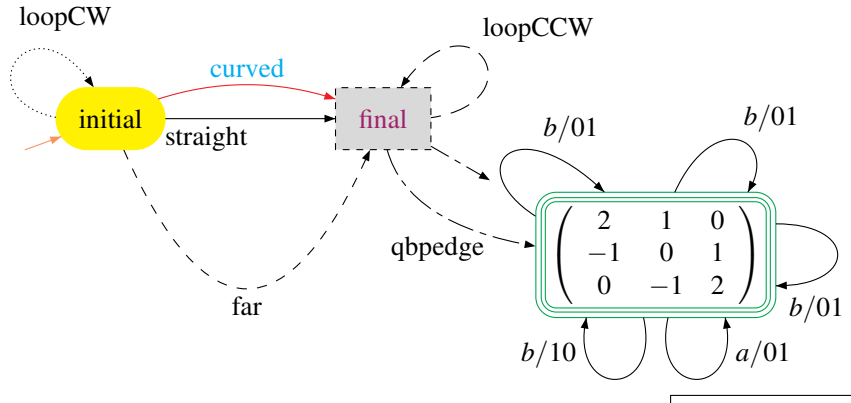
[13] Miller, s.283 et s.285.

18

F Gegenüberstellung ausgewählter Berufsbezeichnungen 109

Maskuline Bezeichnung	Frankreich	Québec	Belgien	Schweiz
magistrat	magistrate	magistrate	magistrate	magistrate
maïeuticien (informatique)	maïeuticienne			
makrobiotisch (medizine)	**sage-femme**	**maïeuse**	**maire / mairesse**	**maïeuse**
maire	maire / mairesse	maire / mairesse	maire / maitre	maître / maîtresse
maître	maître / maîtresse	maître / maîtresse (dans certaines expressions)		
manageur	manageuse	manageuse	manageuse	
manequin	manequin (e)	mannequin	mannequin	mannequin
manucure	manucure	manucure	manucure	manucure
maquilleur	maquilleuse	maquilleur	maquilleuse	maquilleuse
marchand	marchande	marchand	marchande	marchande
maréchal	maréchale	maréchal	maréchale	maréchale
marin	marin	marin	marin	marine
marinier	marinière		marinière	marinière
marqueteur	marqueteuse	marqueteur	marqueteuse	marqueteuse
masseur	masseuse	masseur	masseuse	masseuse
matelot	matelote (e)	matelot	matelote / matelot	matelote
mécanicien	mécanicienne	mécanicien	mécanicienne	mécanicienne
médecin	médecin (e)	médecin	médecin	médecin
menuisier	menuisière	menuisier	menuisière	menuisière
metteur en scène	metteuse en scène	metteur en scène	metteuse en scène	metteuse en scène
minueur	minueuse	minueur	minueuse	minueuse
ministre	ministre	ministre	ministre	ministre

TEX (wym. tech) jest systemem profesjonalnego składu drukarskiego. Wśród systemów służących do podobnych celów wyróżnia się dbałością o jakość wyników. Chðc mwng nåm mši Ο Σύλλογος Ελλήνων Φίλων του TEX, γνωστός και ως ;λληνες Φίλοι του TEX (ΕΦΤ για συντομία) αποτελεί την επίσημη Τοπική Ομάδα του TEX ή το ελληνικό TEX ΛΥΓ. CyrTUG или Ассоциация пользователей кириллического TEX'а была учреждена в мае 1991 г. Учредительная конференция, на которой присутствовали 23 TEXuser'а из Москвы, Санкт-Петербурга, Новосибирска и Протвино, проходила в Москве, в издательстве Мир.



Computer Modern – AvantGarde – Helvetica – Times – Palatino – NewCenturySchoolbook – Bookman – *ZapfChancery* – CharterBT – Concrete – CM Bright – Luximono – PX Roman – Utopia – CM Typewriter - Courier

Poster erstellt mit `article.cls` und pdfTEX von Herbert Voß