Advances in new tächnologies concerning recentness and related research areas

Bachelorarbeit

KIT – Karlsruher Institut für Technologie
Fraunhofer IOSB – Fraunhofer-Institut für Optronik,
Systemtechnik und Bildauswertung

Tim Samorei

September 2019

Verantwortlicher Betreuer:	Prof. S. U. Per
Betreuender Mitarbeiter:	Dr. B. Ester
	B. Löd

Erklärung der Selbstständigkeit

Hiermit versichere ich, dass ich die Arbeit selbständig verfasst habe und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe, die wörtlich oder inhaltlich übernommenen Stellen als solche kenntlich gemacht habe und die Satzung des Karlsruher Instituts für Technologie zur Sicherung guter wissenschaftlicher Praxis in der gültigen Fassung beachtet habe.

Karlsruhe, den September 2019

(Tim Samorei)

Notation

Allgemeine Bezeichner

$\alpha, \ldots, \omega$	Skalare
$a, \ldots, z$	Skalar, Vektor, Funktionssymbol (oder Realisierung einer Zufallsvariablen)
$\boldsymbol{a}, \ldots, \boldsymbol{z}$	Zufallsvariable (skalar bzw. vektoriell)
$\hat{\boldsymbol{a}}, \ldots, \hat{\boldsymbol{z}}$	Schätzer für jeweilige Variable als Zufallsgröße
$\hat{a}, \ldots, \hat{z}$	Realisierter Schätzer für jeweilige Variable
$A, \ldots, Z$	Matrix
$\boldsymbol{A}, \ldots, \boldsymbol{Z}$	Matrix als Zufallsgröße
$\mathcal{A}, \ldots, \mathcal{Z}$	Menge
$\mathfrak{A}, \ldots, \mathfrak{Z}$	Mengensystem

Spezielle Bezeichner

t	Spezielle Bezeichner mit konkreter Bedeutung in dieser Arbeit, z. B. t Zeitindex

Allgemeine Mengen

$\mathbb{C}$	Menge der komplexen Zahlen
$\mathbb{H}$	Poincaré Halbebene
$\mathbb{N}$	Menge der natürliche Zahlen (ohne Null)
$\mathbb{N}_0$	Menge der natürliche Zahlen mit Null
$\mathbb{Q}$	Menge der rationalen Zahlen
$\mathbb{Q}^{>0}$, $\mathbb{Q}^{<0}$	Menge der positiven bzw. negative rationalen Zahlen
$\mathbb{R}$	Menge der reellen Zahlen
$\mathbb{R}^{>0}$, $\mathbb{R}^{<0}$	Menge der positiven bzw. negative reellen Zahlen
$\mathbb{Z}$	Menge der ganzen Zahlen

Spezielle Symbole

$\mathfrak{N}(\mu, \sigma^2)$	Normalverteilung mit Erwartungswert μ und Varianz σ
$\mathfrak{F}_{r,s}$	Fisher-Verteilung mir r Zähler- und s Nennerfreiheitsgraden
$\mathfrak{t}_s$	Student-t-Verteilung mit s Freiheitsgraden
δ_ξ	Ein-Punkt-Maß an der Stelle ξ
χ^2_s	χ^2-Verteilung mit s Freiheitsgraden

Inhaltsverzeichnis

Einleitung

Am Lehrstuhl für Interaktive Echtzeitsysteme (IES) des Karlsruhe Instituts für Technologie (KIT) wurde von Philipp Wook die erste LaTeX-Vorlage zur Erstellung von wissenschaftlichen Arbeiten erstellt. Diese basierte ihrerseits auf der Vorlage von Matthias Pospiech von der Leibniz Universität Hannover. Die von Matthias Pospiech und durch Philipp Wook stark erweitere Vorlage, hatte den Anspruch die „eierlegende Wollmilchsau“ zu sein und möglichst alle Anwendungsfälle abzudecken.

Leider hatte diese Vorlage – da sie ständig um zusätzliche Pakete erweitert wurde – auch zwei meiner Meinung nach entscheidende Nachteile:

- Es setzte auf den alten BibLatexs-Paketen auf anstatt des neueren `biblatex`-Ökosystems. Dadurch war eine durchgängige UTF-8-Unterstützung nicht möglich und die ein oder andere Konstellation von Umlauten hat immer mal wieder „geknallt“.

- Zum Erstellen von Vektorgrafiken mit einer hohen Druck- undTypografiequalität gibt es TikZ. Die alte Vorlage unterstütze zwar grundlegendes TikZ, aber bei vielen TikZ-Zusatzpaketen kam es zu Inkompatibilitäten mit anderen Paketen.

Diese Vorlage ist quasi ein Neudesign der Vorlage von Philipp Wook. Allerdings hat sie intern nicht mehr allzu viele Gemeinsamkeiten. Im Wesentlichen wurde versucht das Layout nachzuahmen, um eine halbwegs konsistentes Erscheinungsbild zwischen Dokumenten mit alter und neuer Vorlage zu erreichen.

Natürlich ist so ein Neustart nicht ohne Nachteile möglich. Gegenwärtig ist diese Vorlage noch sehr „schlank“ und viele Möglichkeiten der alten Vorlage sind noch nicht wieder nachgebaut. Dies wird in Zukunft und bei Bedarf geschehen.

Einige Möglichkeiten der alten Vorlage werden aber nie wieder ihren Weg in diese Vorlage finden. Dies betrifft alle LaTeX-Pakete die in irgendeiner Weise PostScript benötigen. Um das volle Potential von UTF-8, BibLaTex und TikZ ausnutzen zu können, ist die Verarbeitungskette auf

$$\texttt{LaTeX-Quellcode} \xrightarrow{\texttt{pdflatex}} \texttt{PDF}$$

reduziert worden. Umwege wie

$$\texttt{LaTeX-Quellcode} \xrightarrow{\texttt{latex}} \texttt{DVI} \xrightarrow{\texttt{dvi2ps}} \texttt{PS} \xrightarrow{\texttt{ps2pdf}} \texttt{PDF}$$

sind ausgeschlossen. Das bedeutet insbesondere, dass alle Optionen, die das bekannte Paket `pstricks` bietet nicht mehr zur Verfügung stehen. Allerdings bietet hier TikZ immer eine Ersatzlösung an. Das einzige, was definitiv gar nicht mehr funktioniert und auch nicht durch TikZ nachgestellt werden kann, ist das direkte Einbinden von PostScript- bzw. EPS-Abbildungen. Diese müssen nun zunächst durch externe Tools in PDF konvertiert werden.

1 Grundlagen

1.1 Public Key Cryptographie

1.1.1 Formale Definition

Formal besteht ein Public-Key-Verschlüsselungsverfahren aus drei Algorithmen:

- Der Schlüsselerzeugungsalgorithmus erzeugt zu einem gegebenen Sicherheitsparameter ein Schlüsselpaar, das aus einem öffentlichen und dem dazugehörigen geheimen Schlüssel besteht.
- Der Verschlüsselungsalgorithmus erzeugt aus einem Klartext unter Verwendung des öffentlichen Schlüssels einen Geheimtext. Es kann zu einem Klartext mehrere Geheimtexte geben. In diesem Fall ist der Algorithmus probabilistisch.
- Der Entschlüsselungsalgorithmus berechnet zu einem Geheimtext unter Verwendung des geheimen Schlüssels den passenden Klartext.

Es wird nun gefordert, dass jede Nachricht, die mit einem öffentlichen Schlüssel verschlüsselt wurde, mit dem zugehörigen geheimen Schlüssel wieder aus dem Chiffrat gewonnen werden kann.

1.1.2 Sicherheit

Für die Sicherheit asymmetrischer Verfahren ist es notwendig, dass die den verschiedenen Verfahren zugrundeliegenden Einwegfunktionen praktisch unumkehrbar sind, da ansonsten aus dem öffentlichen Schlüssel der private berechnet werden könnte. Die Sicherheit aller asymmetrischen Kryptosysteme beruht also immer auf unbewiesenen Annahmen, insbesondere auf der Annahme, dass P ungleich NP ist. In der Regel wird von diesen Annahmen jedoch stark vermutet, dass sie zutreffen. Die beim symmetrischen One-Time-Pad erreichbare informationstheoretische Sicherheit kann mit einem asymmetrischen Verfahren nicht erreicht werden, weil ein entsprechend mächtiger Angreifer immer das zugrundeliegende mathematische Problem lösen kann.

1.1.3 Anwendung

Diese Verfahren werden heutzutage z. B. im E-Mail-Verkehr (OpenPGP, S/MIME) ebenso wie in kryptografischen Protokollen wie SSH oder SSL/TLS verwendet. SSL/TLS wird in größerem Umfang beispielsweise als Protokoll https zur sicheren Kommunikation eines Web-Browsers mit einem Server eingesetzt.
Zur Verschlüsselung wird der öffentliche Schlüssel auf den zu verschlüsselnden Text angewandt. Der verschlüsselte Text wird dann vom Schlüsselinhaber mit dem privaten Schlüssel wieder entschlüsselt.

1.2 Public Key Infrastructure

https://de.microcosm.com/products/pki-tokens

1.3 Android

https://developer.android.com/about/versions/android-4.3.htmlSecurity
https://books.google.de/books?id=-QcvDwAAQBAJpg=PA298lpg=PA298dq=Broadcom+BCM20793M+NFC+Cont
xysig=ACfU3Uonxf4CRE-c-tLTZJOdHqTIKwU7qQhl=desa=Xved=2ahUKEwivhpuyoMnhAhWEa1AKHSzqAJ8Q6

1.4 Near Field Communication

http://www.icedev.se/proxmark3/docs/ISO-14443-3.pdf
https://cardwerk.com/iso-7816-part-4/

1.5 Android Keystore

https://developer.android.com/training/articles/keystore
https://developer.android.com/reference/java/security/KeyStorepublic-methods
http://www.cs.kun.nl/ erikpoll/publications/AndroidSecureStorage.pdf
https://nelenkov.blogspot.com/2013/08/credential-storage-enhancements-android-43.html
http://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/11252/KASAGIANNIS%20GEORGIOS%201515%20-
%20SECURITY%20EVALUATION%20OF%20ANDROID%20KEYSTORE.pdf?sequence=3isAllowed=y

1.6 Host Card Emulation

http://blog.opendatalab.de/hack/2013/11/07/android-host-card-emulation-with-acr122
https://benjaminerhart.com/2015/07/nfc-android-vs-computer-in-host-based-card-emulation-app/
https://nelenkov.blogspot.com/2012/10/emulating-pki-smart-card-with-cm91.html
http://www.medien.ifi.lmu.de/iwssi2012/papers/iwssi-spmu2012-roland.pdf
https://github.com/championswimmer/NFC-host-card-emulation-Android

1.7 PKCS 11

http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/os/pkcs11-base-v2.40-os.html$_{T}oc416959744$

2 Related Work

2.1 Android Smart Card Emulator

2.2 JCAndroid

2.3 Virtual Keycard

2.4 Hardware-BackedHeist

3 Aufbau

3.1 Klassendiagramm

3.2 Sequenzdiagramm

3.3 Ausschnitte Sourcecode

4 Future Work and Conclusions

4.1 Future Work

4.2 Conclusions

Tabellenverzeichnis

Abbildungsverzeichnis

Theoremverzeichnis

Listings

Glossar

BibLaTex Der Nachfolger von BibTex zum Erzeugen von Literaturverzeichnissen in LaTeX. Es zeichnet sich vor allem durch deutlich bessere Flexibilität bei der Gestaltung des Literaturverzeichnisses und der Art und Weise wie Zitatmarken gesetzt werden aus. Darüber hinaus ist es vollständig UTF-8-kompatibel. 1

BibLatex Der Vorgänger von BibLaTex. 1

EPS Embedded Postscript. 2,

Java Eine von Sun Microsystems 1995 veröffentlichte, objektorientierte Programmiersprache.

LaTeX Eine von Leslie Lamport 1980 entwickelter Satz von Makros zur Erweiterung von TeX.

Paket Ein LaTeX-Paket besteht aus einer oder mehrerer Dateien, die entweder vorhandene Kernfunktionen von LaTeX umdefinieren und so das Verhalten derselbigen bzw. das Erscheinungsbild des fertigen Dokuments verändern oder die zusätzliche Befehle zur Verfügung stellen. 1

PCA Principal Component Analysis.

PDF Portable Document Format. 2,

PGFplots Eine Sammlung von TikZ-Paketen, die ein direktes Erzeugen von Diagrammen aller Art (inkl. 3D-Diagramme) direkt aus LaTeX heraus ermöglicht.

PostScript Eine von Adobe 1984 entwickelte Seitenbeschreibungssprache. 1, 2

TikZ Eine Sammlung von LaTeX-Paketen, die ein direktes Erzeugen von (technischen) Zeichnungen, Diagrammen, etc. in LaTeX erlaubt. 1, 2

Umgebung Ein Bereich im LaTeX-Code der mit `begin` eingeleitet und mit `end` beendet wird. Umgebungen können auch verschachtelt sein.

UTF-8 Ein Schema zur Kodierung von Zeichen in computerverarbeitbarer Form, die Zeichen aus allen Sprachen umfasst. 1

WYSIWYG What you see is what you get.