HPImgzn

Hasso-Plattner-Institut

Ausgabe 15 – Wintersemester 2013 / 2014

Konrad Zuse

Überspannter Erfinder und gescheiterter Unternehmer 8

IT-Größen in Deutschland

Studentisches

HPIintern

Blick über den Tellerrand

Jubiläum

Das HPImgzn erscheint zum fünfzehnten Mal! Zur Feier des Tages gibt es diese Ausgabe komplett in bunt!

Einen runden Geburtstag konnte auch unser Institutsgründer feiern. Ihm widmen wir uns mit einem ausführlichen Portrait der etwas anderen Art im Hauptteil dieser Ausgabe. Ebenso stellen wir andere deutsche Branchen-Größen aus Vergangenheit und Gegenwart vor.

Damit auch das Studentische nicht zu kurz kommt, haben wir unsere Studententipps wieder aufgelegt. Ob ihr euch besser in euer soziales Umfeld einfügen wollt oder lieber davor ins Ausland flüchtet – fühlt euch versorgt. Ergebnisse aus den Klubs und der HPI-Forschung runden das Ganze ab.

Auch wagen wir diesmal einen Blick hinaus über den Tellerrand und beschäftigen uns mit so aktuellen wie unterschiedlichen Themen. Bevor ihr sie lest, hat die NSA natürlich schon längst einen Blick auf diese Ausgabe geworfen. Wir haben uns gefragt, was wir Informatiker in Zukunft dafür tun können, derartige Skandale zu vermeiden oder zumindest daran beteiligt zu sein. Außerdem forschen wir dem Mensa-essen hinterher und diskutieren bauliche Änderungen auf dem Campus. Wem das nicht fachlich genug ist, dem sei unsere Einführung in die Verschlüsselungstechnologie ans Herz gelegt.

Ein herzlicher Dank geht wie immer an alle internen und externen Autoren. Eine Zeitung wie diese besteht aus viel mehr als nur Texten. Nicht zu vergessen sind die Interview- und Recherche-Partner, die Fotografen und Korrektoren sowie das fleißige Layout-Team. Einmal mehr freuen wir uns über die großartige Zusammenarbeit mit dem Foto-Klub und dem Alumni-Klub. Nicht zuletzt hat auch der Klub Kulinarisches wieder einige leckere Rezepte, der Kunstklub einige seiner besten Bilder beigesteuert, sodass ihr hier ein echtes Gemeinschaftswerk in Händen haltet.

Damit haben wir uns dann wohl alle die Ferien verdient.

Wir sehen uns im nächsten Semester!
Carolin Fiedler und Franz Liedke

Die Redaktion dieser Ausgabe

Carolin Fiedler
Franz Liedke

Andreas Burmeister
Daniel Dummer
Jasper Schulz
Johannes Wolf
Julia Wachtel
Konstantin Harmuth
Lukas Wagner
Maria Graber
Matthias Barkowsky
Maximilian Götz
Pascal Lange
Suhanyaa Nitkunanantharajah

Happy Birthday, Hasso

Dieses Jahr ist ein besonderes für unseren Stifter. Es ist das Jahr, in dem er seinen 70. Geburtstag feiert. Über seinen beruflichen Werdegang und sein Engagement für den Nachwuchs wissen wir alle einiges – spätestens seit Wikipedia. Wie aber ist Hasso Plattner als Privatperson? Was steckt hinter seinem Erfolg? Und wie sehen ihn Menschen aus seinem Umfeld?
Anlässlich seines Geburtstags haben wir uns mit einigen von Hasso Plattners Freunden und Bekannten unterhalten, um mehr über seine Person und seine Persönlichkeit zu erfahren.

August-Wilhelm Scheer

Langjähriger Wegbegleiter und Mitglied des Stiftungsrats der Hasso-Plattner-Stiftung

Hasso Plattner ist eine sehr imponierende Persönlichkeit. Die Mischung, die er verkörpert, ist sehr selten – in seinen Entscheidungen ist er oft bauchorientiert, hat aber gleichzeitig einen sehr scharfsinnigen Intellekt. Diese Kombination zwischen Intuition und intellektueller Schärfe zeichnet ihn meines Erachtens aus. Sie ist aber auch typisch für andere Erfolgreiche in der IT-Industrie – seien es Steve Jobs oder Bill Gates. Intelligente Leute gibt es schließlich genug; Leute, die nur nach Emotion handeln, auch. Aber diese Kombination ist ein wichtiger Teil von Hasso Plattners Erfolgsmodell.

Er ist ein Kämpfer. Er bringt auch nach so vielen Jahren immer noch einen sehr hohen Einsatz für die SAP AG. Schließlich ist er auch der Letzte der Gründer, der immer noch 100 Prozent Einsatz für die Informationstechnik bringt, während sich die Anderen zurückgezogen haben.

Zu seiner Bauchfähigkeit gehört auch sein Kunstinteresse. Wenn man ihn mal als Schauspieler erlebt hat, wenn er jemanden imitiert – das ist super. Auch die Art, wie er mit Menschen umgeht, ist sehr aufgeschlossen. Vor allem sein Interesse an jungen Leuten und Studenten ist bemerkenswert. Er besitzt eine Kombination von Eigenschaften, die schon außergewöhnlich ist. Auch, dass er sich bei der HANA-Entwicklung quasi mit den jungen Forschern des HPI gegen das Establishment der SAP verbündet hat, zeigt seine innovative Weitsicht. Dieses ist auch etwas, was wir in unserer schnelllebigen Industrie brauchen.

Es genügt nicht, einmal eine tolle Idee gehabt zu haben und zu meinen, dass sie jetzt 50 Jahre hält, sondern, dass man das immer wieder in Frage stellt.

Hasso Plattner stellt sich stets die Frage, was die nächste IT-Welle ist und wie sie seine SAP angreifen könnte. Da zeigt sich wieder das Emotionale, das Angstgesteuerte. Er setzt sich nicht zur Ruhe und sagt sich, es werde schon alles gut gehen, sondern fragt sich

ständig, wie Google oder Oracle das Unternehmen angreifen könnten. Nur so hat er das notwendige Sensorium, um mögliche Gefahren zu wittern. Das ist eine Eigenschaft, die bei ihm sehr ausgeprägt ist.

Hasso Plattner ist extrem fachlich orientiert. Ich habe es erlebt, dass er auch bei gesellschaftlichen Anlässen sich lieber mit dem Mann links von ihm zu fachlichen Themen unterhält als Small Talk mit der rechts von ihm sitzenden attraktiven Dame zu führen.

Die Tatsache, dass er als Kapitän an Bord bleibt, und sich nicht einen ruhigen Hafen gesucht hat, fasziniert mich besonders an seinem Lebenswerk.

Selbst in seiner Freizeit unternimmt er Segeltouren und sonstige sportliche Aktivitäten, die immer den vollen Einsatz verlangen. Ich kann mir nicht vorstellen, dass er in seiner Freizeit die Beine baumeln lässt.

Ich möchte ihm sehr herzlich zu seinem Geburtstag gratulieren und wünsche ihm, dass er auch weiterhin Arbeit als Privileg ansieht.

Das Gespräch führte
Suhanyaa Nitkunanantharajah

Prof. Dr. Dr. h. c. Rolf Emmermann

Mitglied des Stiftungsrats der Hasso-Plattner-Stiftung

Hasso Plattner ist eine sehr beeindruckende, ungewöhnlich vielseitig interessierte und engagierte, wissenschaftlich und wirtschaftlich außerordentlich erfolgreiche und dabei ganz und gar uneitel gebliebene Persönlichkeit.

Ich kenne Herrn Plattner aus meiner Mitwirkung im Stiftungsrat der nach ihm benannten Stiftung für Softwaresystemtechnik; das heißt, so wie man jemanden bei einer Sitzung, aber auch in Gesprächen über ganz andere Themen am Rande derartiger Treffen eben kennenlernen kann.

Herr Plattner finanziert das Institut – sein Institut – aus den Stiftungsmitteln nicht nur zu hundert Prozent privat, sondern er ist auch nach wie vor ein wichtiger Ideengeber und treibende Kraft für dessen erfolgreiche Weiterentwicklung. Er beeindruckt mich immer wieder durch die Art und Weise, wie er auftritt und argumentiert, wie er sich in jedem Detail auskennt und Schwachstellen in fachlichen Berichten oder Finanzplänen sofort identifiziert und dabei gleichzeitig den Blick für das große Ganze nicht verliert. Er ist sehr mitreißend, gerade bei Diskussionen, und vertritt seine Auffassungen zu fachlichen Fragen und Themen mit viel Jugendlichkeit, Dynamik, Energie und Durchsetzungsvermögen.

Dabei wird klar, dass er nach wie vor ein hervorragender Wissenschaftler ist, der auf

seinem Fachgebiet auch im internationalen Vergleich an der Spitze steht. Außerdem gewinnt man den Eindruck, dass er wissenschaftlich immer noch sehr neugierig ist und sich selbst und die Wissenschaft ständig weiterentwickeln möchte. Dies tut er auch, indem er als Leiter des Fachgebiets »Enterprise Platform and Integration Concepts« in seinem eigenen Institut in Forschung und Lehre tätig ist, durch sein Beispiel und durch seine Persönlichkeit junge Menschen für die Wissenschaft begeistert und vor allem zum Querdenken und zum Beschreiten neuer, unkonventioneller Wege anregt.

Es ist zu spüren, wie sehr ihn die Arbeit und der ständige Meinungsaustausch mit jungen, kreativen Studierenden befriedigen und wie groß sein Anliegen ist, berufliche Perspektiven für die jungen Leute zu schaffen und ihnen das notwendige Rüstzeug für eine erfolgreiche Tätigkeit in der Praxis mitzugeben.

Ich gratuliere Hasso Plattner ganz herzlich zu seinem 70. Geburtstag und wünsche ihm, dass er noch viele Jahre so dynamisch und erfolgreich weiterarbeiten kann und dass er immer die Kraft hat, um ganz vorne zu bleiben.

Das Gespräch führte Franz Liedke

Jann Jakobs

Oberbürgermeister von Potsdam

Ich habe Herrn Plattner in Zusammenhang mit der Gründung des Hasso-Plattner-Instituts kennen gelernt.

Herr Plattner ist ein erfrischender, quirliger und kreativer Mensch. Aus meiner Sicht zeichnet er sich durch eine unkonventionelle Herangehensweise aus. Er ist immer am Puls der Zeit und über alle Gesprächsdiskussionen informiert. Dabei verbindet er seine Empfindsamkeit und Emotionalität, wie ich finde, sehr gut mit seiner nüchternen, naturwissenschaftlich ausgerichteten Handlungsweise.

Zu seinem 70. Geburtstag wünsche ich ihm weiterhin viel Schaffenskraft, dass er seinen gesunden Optimismus behält und seine innige Verbundenheit mit Potsdam.

Das Gespräch führte
Suhanyaa Nitkunanantharajah

Auch wir schließen uns den Glückwünschen an und gratulieren ganz herzlich zum 70. Geburtstag. Wir freuen uns auf viele weitere tolle Jahre mit unserem Stifter!

– Franz Liedke, Suhanyaa Nitkunanantharajah

Konrad Zuse

Überspannter Erfinder und gescheiterter Unternehmer

Berlin, 1935. Ein 24-jähriger Uniabsolvent. Unzufrieden mit seiner momentanen Anstellung. Entnervt von der stupiden Rechnerei mit Stift und Papier. Den Kopf voller Visionen und Ideen für eine vollautomatische Rechenmaschine.
Konrad Zuse macht sich selbstständig.

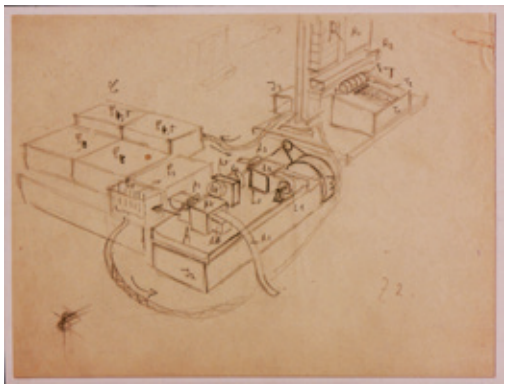
Seine Geschichte ähnelt zu Beginn der anderer Computerpioniere wie Bill Gates oder den HP-Brüdern. Auch sie begannen im Stillen zu tüfteln. Dennoch wurde Zuse nie weltberühmt oder gar reich durch seine Erfindungen. Im Gegenteil, noch zu Lebzeiten musste er alle Anteile seiner Firma verkaufen. Was genau steckt hinter seinen Erfindungen? Woran scheiterte der Deutsche letztlich?

Konrad Zuse beschließt kurz nach seinem Uniabschluss, die Wohnung seiner Eltern in der Methfesselstraße in Kreuzberg zu einer Erfinderwerkstatt umzufunktionieren. Er hat zwar eine sichere Stelle als Statiker bei den Henschel-Flugzeugwerken, kündigt diese jedoch und beginnt damit, seine Idee der ersten vollautomatischen Rechenmaschine umzusetzen. Später sagt er über diese Zeit: »Ich war zu faul zum Rechnen«. Das erste Modell soll komplett mechanisch funktionieren. Die Umsetzung mittels mechanischer Schaltglieder, die durch einen Staubsaugermotor angetrieben werden, scheint dem Erfinder kompakter als die Arbeit mit elektromechanischen Relais. Mithilfe von Freunden und der Unterstützung seiner Familie werkelt er bis 1938 an der Maschine. Das Ergebnis kann sich sehen lassen: 30 000 Bleche, mit der Laubsäge ausgesägt und von Stiften zusammengehalten, bedecken die Fläche eines Wohnzimmerschrankes. 1 408 Bit kann das Gerät speichern. Zuverlässig arbeitet es jedoch nicht, zu oft verhakt die Mechanik. Wenn jedoch alles glatt geht und kein Teil ein anderes blockiert, liefert die Maschine stets das korrekte Ergebnis. Instruktionen werden von einem mit Löchern versehenen Filmstreifen geliefert. Zuse tauft seine Erfindung selbstbewusst die Z1.

Heute befindet sich an der Stelle des Wohnhauses von Zuses Eltern eine Gedenktafel.

Um die Unzuverlässigkeit der Z1 zu überwinden, entwirft der Berliner in den darauffolgenden Jahren die Z2, ein Demonstrations- und Testobjekt. Diese verwendete weiterhin mechanische Speicher. Für das Rechenwerk setzte Zuse jedoch, auf den Rat eines Freundes hin, 800 Telefonrelais ein. Diese erweisen sich als deutlich zuverlässiger.

Die Arbeit von Zuse und seinen Angestellten geht nun jedoch wesentlich langsamer voran, denn es herrscht Krieg in Europa. Der Erfinder kann die Nationalsozialisten von der Wichtigkeit seiner Forschung überzeugen. Er wird von der »Deutschen Versuchsanstalt für Luftfahrt« unterstützt und als kriegswichtig eingestuft. Zuse kann so nach nur einem halben Jahr Wehrdienst an seinen Arbeitsplatz, nun in der Rüstungsindustrie, zurückkeh-



ren. Abends und am Wochenende arbeitet er ununterbrochen an seinen Erfindungen.

Am 12. Mai 1941 ist es dann soweit: Die Z3 wird als die erste funktionsfähige, frei programmierbare und auf dem binären Zahlensystem sowie der binären Schaltungstechnik basierende Rechenmaschine fertiggestellt und vor kleinem Publikum präsentiert. Nur wenige Leute können mit Zuses Forschungsarbeiten etwas anfangen. Die Maschine hat erneut gewaltige Ausmaße: Sie besteht aus etwa 30 000 Kabeln und circa 2 500 Relais. Sie ist in der Lage 64 Zahlen zu speichern, braucht 0,8 Sekunden für eine Addition und etwa drei Sekunden für eine Multiplikation. Die Ausgabe der Ergebnisse erfolgt mittels Glühbirnen. Die Materialien, mit denen Zuse arbeitet, sind zum Großteil Abfallprodukte der Wehrmacht. Geld für neue Technik gibt es nicht. Der Tüftler gründet schließlich das »Zuse Ingenieurbüro und Apperatebau, Berlin«.

In den letzten Kriegsjahren wird bei einem Bombenangriff auf Berlin das Herzstück von Zuses Forschung, die Z3, komplett zerstört und der Erfinder muss aus Berlin flüchten. Es verschlägt ihn in das Allgäu. Dort versucht er sich eine neue Existenz aufzubauen. Er arbeitet kontinuierlich an der Z4, einem verbesserten Modell der Z3. Weiterhin entwickelt er 1942 – 45 das »Plankalkül«, ein Programmiersystem, das komplexe Aufgaben in Programme umsetzen soll. Es enthält komplexe Zahlen, Unterprogrammtechnik, bedingte Abfragen, sieben verschiedene Schleifenarten und viele weitere Sprachkonstrukte.

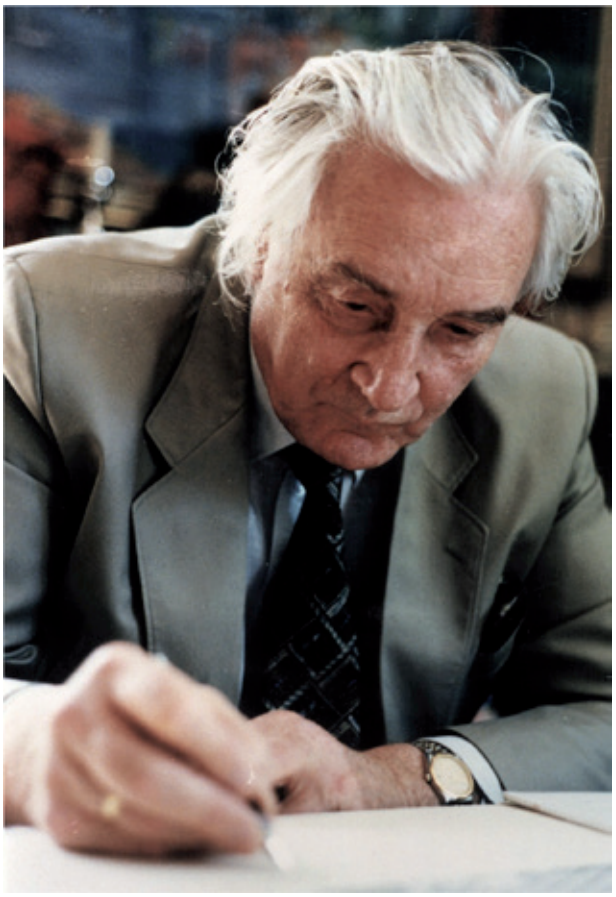
In der Nachkriegszeit hat Zuse sehr zu kämpfen. Als Erfinder in Zeiten des NS-Regimes durfte er nicht publizieren. Der Forscher war isoliert von der weltweiten Wissenschaft. Alle seine Patentanmeldungen blieben

Ein originalgetreuer Nachbau der Z1 befindet sich heute im Deutschen Technikmuseum in Berlin.

Staatsgeheimnis. So weiß niemand von Zuses Errungenschaften der letzten zehn Jahre. 26 Jahre brauchen die deutschen Gerichte, um sein Patent auf die Z3 letztendlich abzulehnen – Grund: »mangelnde Erfindungshöhe«. Er besucht Forscher in Amerika, die drei Jahre nach Zuse den »Mark I«, angeblich den ersten Computer der Welt, entwickelt haben. Dieser ist deutlich größer als Zuses Z3, verwendet das umständlichere Dezimalsystem und keine Gleitkommaarithmetik. Der Deutsche gibt Hinweise zur Verbesserung des Geräts, wird aber ignoriert.

In Deutschland hat er mittlerweile die »Zuse KG« gegründet. Diese entwickelt und produziert weitere programmgesteuerte Rechengeräte. Dank dem Wirtschaftswunder der 50er-Jahre herrscht ein wahrer Computerboom. Die Firma wächst und wächst. Zu Hochzeiten arbeiten hier über 1 000 Mitarbeiter. Das Betriebsklima ist und bleibt sehr familiär. Doch schon in den 60ern läuft es in der Zuse KG nicht mehr gut, der Erfinder scheint nicht das Zeug zum Unternehmer zu haben. Er wollte sein Leben lang seine Vision realisieren, Ingenieuren das stupide Rechnen durch vollautomatische Maschinen abzunehmen. Wirtschaftlich scheint er nicht das richtige Gespür zu haben. Sobald ein fertiges Modell ausgeliefert wird, will Zuse schon eine neue Maschine erfinden, jedoch ist der Markt für solch drängenden Erfindergeist nicht gemacht. Außerdem wird in der Zuse KG gleichzeitig an zwei verschiedenen Modellen von Rechenmaschinen gearbeitet: Einerseits an der speziell für den Einsatz in der Verwaltung und in großen Betrieben angepassten Z31, andererseits an der für die bisherige Stammkundschaft, wissenschaftliche Anwendungen in Forschung und Entwicklung, optimierten Z25. Die Ressourcen werden knapp. Schließlich muss Zuse die Entwicklungskosten komplett durch den Verkauf seiner Rechner finanzieren. Einer Legende zufolge soll ein Rechner, der an die UdSSR geliefert wurde, mit einem Güterzug voll Gemüse bezahlt worden sein. Ein Gegenwert, der sich schlecht in die notwendigen technischen Bauteile umsetzen lässt. Weiterhin wächst beständig die Konkurrenz durch den amerikanischen Markt, allen voran durch IBM. Die Firma macht keine Gewinne. Der Berliner ist, wie er selbst im Nachhinein zugibt, als Vorsitzender nicht hart genug gewesen. 1964 scheidet er als aktiver Teilhaber aus, bereits 1967 schluckt Siemens die letzten Anteile der Zuse KG. Die Firma verkaufte insgesamt 250 Computer. Zuse widmet sich in seinen letzten Lebensjahren der Malerei und soll nie einen modernen Computer angerührt haben.

– Julia Wachtel



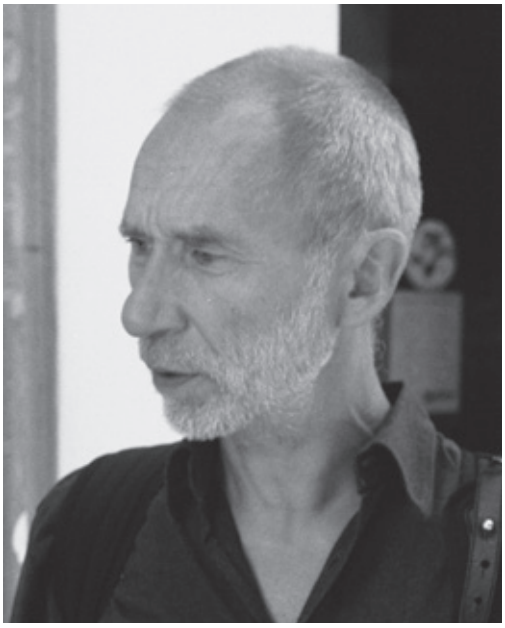
Frieder Nake

Ein Pionier der Computerkunst

»Die Frage, was Kunst ist, ist ebenso dumm wie die Frage, ob Computer jemals intelligent sein werden – Definitionssache.«

Frieder Nake

Frieder Nake ist Mathematiker und Informatiker; er gilt als einer der Pioniere der Computerkunst. Nake wurde 1938 in Stuttgart geboren, wo er nach dem Abitur Mathematik studierte. Während des Studiums arbeitete er 1963 erstmals am Graphomat Zuse Z64.



Die entstandenen Plotterzeichnungen markierten den Beginn der digitalen Kunst. Eine erste Ausstellung computergenerierter Werke fand 1965 statt. Es folgten Teilnahmen unter anderem an der »Cybernetic Serendipity« in London und der Biennale Venedig. Während dieser Zeit promovierte Nake über Wahrscheinlichkeitstheorie und begann anschließend im Bereich Computerkunst weiter zu forschen. Seit 1972 ist er Professor für Grafische Datenverarbeitung und Interaktive Systeme an der Universität Bremen: Er befasst sich mit Informationsästhetik sowie soziokulturellen Aspekten der Informatik. In seinen Publikationen werden vorwiegend Themen wie Computergrafik und Design interaktiver Systeme behandelt. Außerdem beschäftigt er sich mit Begriffen wie Semiotik, Algorithmik und Kreativität. Zu seinen bekanntesten Werken gehört – neben »Polygonzug« und »Geradenscharen« – die Zeichnung »Hommage à Paul Klee«, welche zu einer Ikone der algorithmischen Kunst aufgestiegen ist. Heute entstehen nur noch wenige Werke – Nake konzentriert sich auf die Lehre, mitunter an der Hochschule für Künste in Bremen. Zu sehen ist er aber bei zahlreichen Ausstellungen, kürzlich in Berlin.

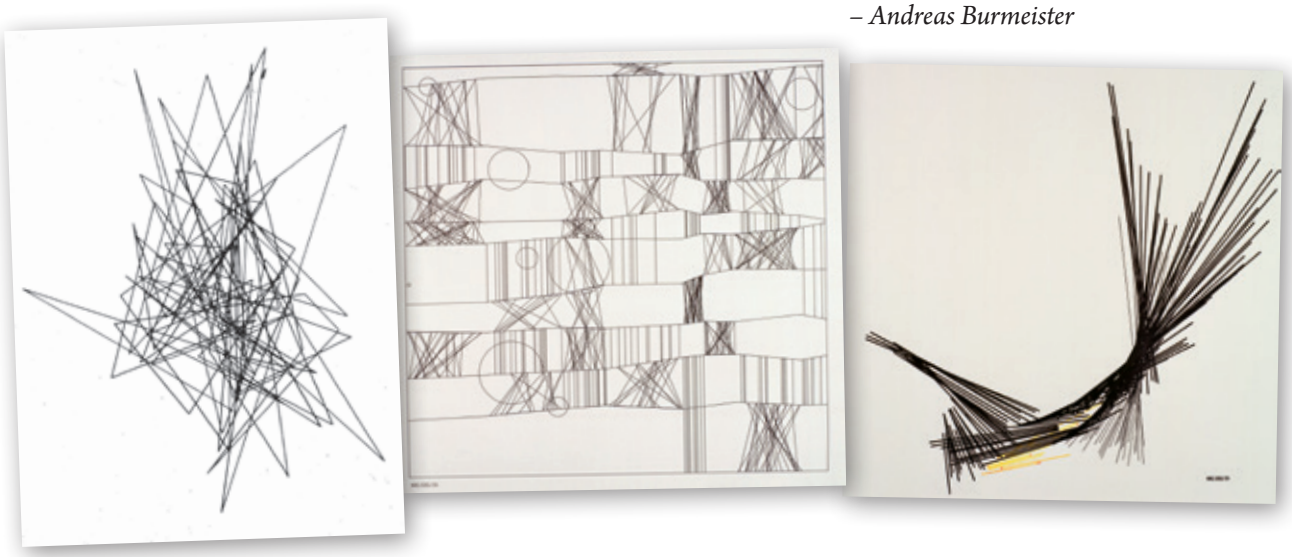
– Andreas Burmeister

Nakes Meisterwerke
(v.l.n.r.)

→ Früher zufälliger Polygonzug (1963)

→ Hommage à Paul Klee(1965)

→ Geradenscharen (1965)



»No message whatsoever«

Eine Retrospektive Frieder Nakes Arbeiten eröffnete am 15. November unter dem Namen »No message whatsoever« in Berlin. Wir haben den Künstler getroffen und so einige Einblicke in sein Schaffen gewinnen können.

Herr Nake, wie würden Sie Ihre Arbeit einordnen? Würden Sie sich jemandem als Künstler, Informatiker, Professor vorstellen?

→ *Frieder Nake:* Das kann ich so eindeutig gar nicht beantworten. Als Künstler würde ich mich nicht bezeichnen. Eher würde ich sagen, ich bin Hochschullehrer und beschäftige mich mit Informatik und digitalen Medien. So ließe ich es meinem Gegenüber offen, weitere Fragen zu stellen. Allerdings verstehe ich mich schon auch als Künstler. *[lacht]* Vor 30 Jahren hätte ich diese Frage so nicht beantwortet, sie abgelehnt. Auf einen Künstler hätte ich mich nicht reduzieren lassen wollen. Heute spielen Kunst, Wissenschaft und Technologie aber immer mehr zusammen und ich habe mich stets gerne irgendwo dazwischen bewegt.

»Was andere Intuition beim Schaffen von Kunst nennen, das ist oft nur Zufall.«

Frieder Nake

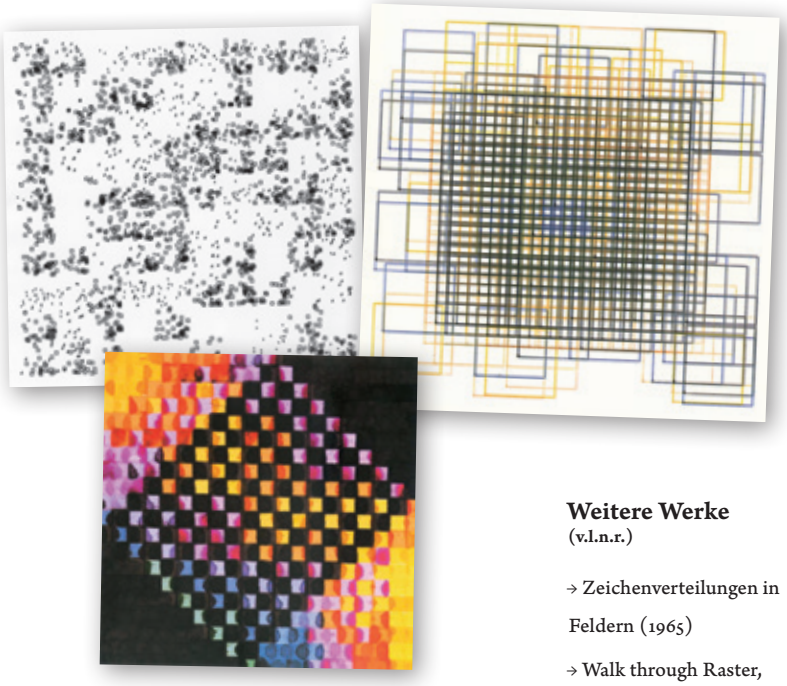
Wie passen für Sie als promoviertem Wahrscheinlichkeitstheoretiker zwei so verschiedene Dinge wie Computer und Kunst überhaupt zusammen?

→ *Frieder Nake:* Das Maschinenhafte ist der Kunst viel näher, als wir das gemeinhin zugeben mögen. In die meisten Kunstwerke fließt eine sorgfältige Planung. Was andere dann Intuition beim Schaffen von Kunst nennen, das ist oft nur Zufall. So manche Künstler haben festgestellt, dass bei ihnen immer wieder bestimmte Muster auftraten. Daraufhin beschlossen einige, gewisse Regeln aufzuschreiben, um sich anschließend ganz bewusst nach diesen zu verhalten. Auch unser tägliches Leben folgt zu großen Teilen definierten Regeln. Es wird dann spannend, wenn man in deren Randbereiche vordringt.

Sie haben allerdings eine Abneigung gegen die Bezeichnung »Computerkunst«. Welcher Begriff sagt Ihnen mehr zu?

→ *Frieder Nake:* »Algorithmische Kunst« oder »Generative Kunst« sind sehr treffend. »Computerkunst« wurde als Wort nur leider sehr früh geprägt. Niemand spricht jedoch von »Bleistiftkunst« oder »Pinselkunst«: Das Instrument zu nehmen, um die Art der künstlerischen Hervorbringung zu bezeichnen, ist also nicht sehr gut gewählt. Kunst mithilfe von Computern umfasst schließlich viel mehr. Denken wir nur an den Bereich Netzkunst. Durch den Computer als Werkzeug hat aber die Verdopplung aller Dinge stattgefunden. Gemeint ist, dass jedes Kunstwerk ein Sichtbares und ein Berechenbares hat. Das kennt die traditionelle Kunst nicht. Das Wirkliche und das Mögliche eines Kunstwerks sind in dieser Weise verbunden. Programme sind Möglichkeitswelten und werden überhaupt erst erkennbar durch ihre Ausgaben. Ich glaube nicht, dass die Kunstgeschichte davon schon irgendeine Ahnung hat.

Ihre ersten Werke entstanden 1963 mittels eines Graphomaten Zuse Z64. Wie sind Sie dazu gekommen und was hat Sie zu dieser Pionierzeit angetrieben?



Weitere Werke
(v.l.n.r.)

→ Zeichenverteilungen in Feldern (1965)

→ Walk through Raster, 7.1-6 (1966)

→ Matrizenmultiplikation Serie 31 (Ausschnitt, 1967)

→ *Frieder Nake:* Eines Tages kam mein Chef und sagte zu mir »Herr Nake, wir kaufen eine Zeichenmaschine, haben dafür aber keine Software.« Dann hat er mich gefragt »Würden Sie das machen?« und ich sagte nur »Ja.« Im Rückblick finde ich das klasse, denn eigentlich hätte ich ehrlich antworten müssen, dass ich keine Ahnung hatte. Jetzt sollte ich plötzlich etwas programmieren, das Bilder hervorbrachte, nicht Zahlen. Ich sollte das Analoge schlechthin – also die Zeichnung – digital machen. Beim Testen meiner Software sind dann die ersten Grafiken entstanden. Das waren einfache Versuche, bestimmte Vektoren zu Papier zu bringen.

Diese Ereignisse sind jetzt 50 Jahre her. Gab es aus Ihrer Sicht Highlights?

→ *Frieder Nake:* Zum einen habe ich zu vielen Bildern später auch interaktive Installationen gemacht. Außerdem ist der Zufall sicherlich häufig ein zentrales Element. Zeigt man einem Betrachter ein Werk, erkennt er vielleicht eine Stadtansicht. Tatsächlich hat aber nur der Computer entschieden, wo bestimmte Rechtecke und Schraffuren wie platziert werden. Überrascht war ich auch, als ich 1968 als einer von 100 Künstlern eingeladen wurde, ein Porträt zu vollenden. Im Anschluss entstand daraus eine sehr schöne Ausstellung. *[lacht]* Das ist für mich deshalb ein Highlight, weil ich dann wusste: Aha, ich bin also Künstler.

Ihre neue Ausstellung trägt den Titel »No message whatsoever« – gibt es aber nicht doch eine Nachricht, die Sie zum Ausdruck bringen wollen?

→ *Frieder Nake:* Das ist zunächst ein Zitat, im französischen Original von Vera Molnár, die einst sagte, in ihrer Arbeit gäbe es überhaupt keine Botschaft. Natürlich ist das Quatsch, aber es ist die Maxime der konkreten Kunst. Das, was da an der Wand hängt, sind Papier und Tusche – fertig. Wenn wir uns fragen, was der Künstler uns sagen will, sagt der gar nichts. Die Botschaft ist also: Der Betrachter schafft die Botschaft. Davon bin ich überzeugt.

Es gibt mit Zeichenprogrammen wie Harold Cohens Aaron oder Sprachen wie Processing – die große Popularität erreichen – eine Vielzahl an Entwicklungen im Bereich algorithmischer Kunst. Welcher Zukunft steuern wir entgegen?

→ *Frieder Nake:* In jedem Fall muss das Bild in Bewegung sein: Ob als dynamische Installation oder durch Interaktion mit der Umwelt, das ist egal. Das statische Bild ist nicht auf der Höhe des Mediums algorithmische Kunst. Es wird dennoch Malerei geben. Cohen hat hoch entwickelte Algorithmen für Farbgebung, malt aber lieber selbst. Vom Computer lässt er sich nur Formen geben. In der weiteren Erforschung dieses Urproblems – Form und Farbe, die nur zusammen auftreten können – da glaube ich, wird die Zukunft liegen.

Vielen Dank für das Interview.
Das Gespräch führten
Andreas Burmeister und Jasper Schulz.

Deutsche IT-Pioniere

Neben Hasso Plattner, Konrad Zuse und Frieder Nake brachte Deutschland einige Pioniere der IT-Branche hervor. Doch die wenigsten von ihnen sind in der breiten Öffentlichkeit bekannt oder werden in der Regel nicht mit IT in Verbindung gebracht. Daher im Folgenden eine kleine Auswahl von deutschen IT-Größen.

Rainer Mallebrein

Der vergessene Pionier, der die Kugel umdrehte

Tag für Tag arbeiten wir mit ihr, der Entdeckung Engelbarts, die er in seiner berühmten »mother of all demos« der Welt offenbarte – die Computermaus. Was aber, wenn Engelbart gar nicht der Erfinder der Maus ist? Bereits zwei Monate im Voraus, im Oktober 1968, entwickelte und publizierte ein deutsches Forschungsteam rund um Rainer Mallebrein bei Telefunken in Konstanz ein Eingabegerät, die sog. Rollkugel, mit der Nutzer »ein Positionssymbol auf dem Schirm […] verschieben, Marken […] setzen und damit die Information […] verändern« konnten. Ursprünglich handelte es sich dabei um eine in Radarschirmen eingelassene Kugel, die die Bundesanstalt für Flugsicherung zum Abruf von Flugzeugdaten nutzte. Als dann 1968 ein neues Eingabegerät für den Telefunken SIG-100 Monitor entwickelt werden sollte, kam das Forschungsteam auf die Idee, die Trackballs aus der Flugsicherung wiederzuverwenden. Da Mallebrein den Nutzern jedoch nicht zumuten wollte, zunächst einmal Löcher in die Tische bohren zu müssen und das Eingabegerät darin zu versenken, bevor sie es nutzen konnten, drehte er den Spieß um. Statt sie in einer Halterung im Tisch zu befestigen, mobilisierte er die Kugel, indem er sie samt der sie umgebenden Halterung aus dem Tisch nahm, umdrehte und mithilfe eines Kabels mit dem Rechner verband.

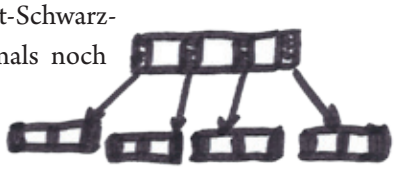
Die deutsche »Rollkugel« eroberte bereits 1972, noch neun Jahre vor der ersten verkauften amerikanischen Computermaus, die deutschen Rechenzentren.

Dennoch sah man bei Telefunken die Erfindung der Rollkugel, die für sie in gewisser Weise lediglich das Umdrehen ihrer schon vorhandenen Rollkugel darstellte, als zu unbedeutend und nichtig an, als dass eine Patentanmeldung lohnenswert gewesen wäre – Glück für Engelbart, Pech für Mallebrein.

Rudolf Bayer

Gemeinsam mit Edward M. McCreight entwickelte Rudolf Bayer bereits in den 70ern eine der in modernen Datenbanksystemen gängigsten Index- / Datenstrukturen, den sog. B-Baum. Die von Bayer entwickelte Baumstruktur speichert Daten sortiert nach den Schlüsseln und ermöglicht durch ihre flache Struktur nicht nur einen möglichst schnellen Zugriff, sondern auch das Einfügen und Löschen von Datensätzen in logarithmischer Zeit.

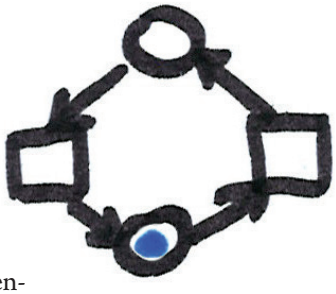
Auch wird Bayer nachgesagt, er sei der Erste gewesen, der den Rot-Schwarz-Baum beschrieb, damals noch unter dem Namen »symmetric binary B-trees«.



Heute ist er emeritierter Professor an der Technischen Universität München.

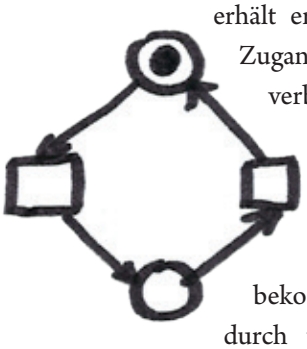
Karl-Adam Petri

Von chemischer Prozessanalyse zur Kommunikation mit Automaten



Wohl kaum ein Informatiker ist nicht schon mindestens einmal in seiner Karriere über Karl-Adam Petris Entwicklung gestolpert – die Petri-Netze. Was jedoch die wenigsten wissen: Petri hatte diese Modellierungstechnik ursprünglich für die Beschreibung von chemischen Prozessen entwickelt und das im zarten Alter von 13 Jahren.

Als Sohn eines Mathematikers war Petri bereits als Kind fasziniert von der Naturwissenschaft. Durch die Kontakte seines Vaters erhält er bereits in jungen Jahren Zugang zu den damals noch verbotenen Werken von Einstein und Heisenberg. Als er zu seinem zwölften Geburtstag zwei dicke Lehrbücher der Chemie bekommt, arbeitet er diese durch und entwickelt basierend darauf das Konzept der Petri-Netze. Später beschäftigt sich der studierte Mathematiker, begeistert von Zuses Arbeit mit Rechenmaschinen, mit physikalischen Gesetzen mit dem Ziel, das Rechnen zu automatisieren. Stets vergleicht er die Informatik mit der Physik und versucht so, neue Erkenntnisse zu gewinnen.

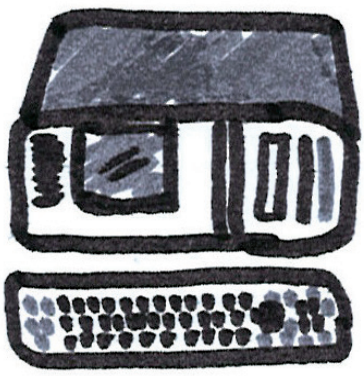


Bis zum heutigen Tage wurde er bereits mehrere hunderttausendmal zitiert und gilt als einer der bedeutendsten deutschen Informatiker. Für sein Lebenswerk wurde Petri mehrfach ausgezeichnet, zuletzt mit der »Academy Gold Medal of Honor« der Academy of Transdisciplinary Learning (ATLAS) und dem Computer Pioneer Award des IEEE.

Gottfried Wilhelm Leibniz

»Es ist unwürdig, die Zeit von hervorragenden Leuten mit knechtischen Rechenarbeiten zu verschwenden, weil mit dem Einsatz einer Maschine auch der Einfältigste die Ergebnisse sicher hinschreiben kann.«

Diesem Grundsatz folgend entwickelte das Universaltalent Gottfried Wilhelm Leibniz im späten 17. Jahrhundert keine Kekse, sondern eine Rechenmaschine, die als erste ihrer Art alle vier Grundrechenarten meisterte. Rechenmaschinen, die seiner vorangegangen waren, beherrschten dagegen nur einen Bruchteil davon. Auch war es Leibniz, der die Bedeutung und die Effizienz der bereits seit Jahrhunderten existierenden binären Codierung von Zahlen für Rechenprozesse erkannte. Seine Rechenmaschine war ein wichtiger, wegbereitender Schritt für die Entwicklung von Computern.



»Diese Aufgaben könnten ohne Besorgnis abgegeben werden, wenn wir Maschinen hätten.«

Gottfried Wilhelm Leibniz

Karlheinz Brandenburg

Der Erfinder des akustischen Gefriertrockners

Begonnen hat alles mit einem engstirnigen Patentprüfer, der der festen Überzeugung war: »Musik über ISDN übertragen – unmöglich, das funktioniert nicht«, und einem ehrgeizigen Professor, der das Gegenteil beweisen wollte. So holte Professor Seitzer den damals noch jungen Karlheinz Brandenburg als Doktoranden in seine Arbeitsgruppe. Sein Ziel sollte es sein, die A-capella-Version von Tom's Diner ohne hörbare Verluste zu komprimieren, verschlüsseln und zu entschlüsseln, um sie als Datei über ISDN-Telefonleitungen übertragen zu können. Gemeinsam mit seinem Forschungsteam an der Universität Erlangen und dem Fraunhofer Institut gelang ihm der Durchbruch.

Die Datenkomprimierung in das heute wohl beliebteste Format für Audiodaten, dem MP3-Format, beschreibt der begeisterte Ingenieur selbst »als eine Art akustisches Gefriertrocknen«. Schließlich bestehe der Kernpunkt in der Digitalisierung darin, die wesentlichen Bestandteile des Ausgangsmaterials so zu komprimieren, dass sie möglichst wenig Platz einnehmen – wie etwa die Gemüsestückchen im Tütensuppenkonzentrat. Dabei werden Frequenzen und Töne, die vom menschlichen Ohr aufgrund seiner beschränkten Wahrnehmung ohnehin nicht gehört werden können, nicht mitcodiert. Wie mit kochend heißem Wasser, das auf das Konzentrat gegossen aus trockenen Bröckchen knackige, scheinbar frische Gemüsestückchen zaubert, müssen bei der Rückwandlung aus den diskreten Bits Töne, Melodien und Klangfarben wieder rekonstruiert und dem Stück damit sein »Biss« wiederverliehen werden.

Heute ist der studierte Elektrotechniker und Mathematiker Leiter des Fraunhofer-Instituts für Digitale Medientechnologie IDMT. Des Weiteren lehrt Karlheinz Brandenburg elektronische Medientechnik an der Technischen Universität Ilmenau.

Andreas von Bechtolsheim

Er stand auf und verließ wortlos den Raum, während Larry Page und Sergej Brin ihm ihre Geschäftsidee vorstellten – sein Scheckbuch lag im Auto, er ging es holen. Bekannt wurde Andreas von Bechtolsheim in der IT-Branche aber nicht als einer der ersten und wichtigsten Investoren von Google, sondern als Mitgründer des IT-Giganten Sun Microsystems. Von einem bayrischen Bauernhof verschlug es ihn zu Studienzeiten nach einem kurzen Zwischenstopp an der Carnegie Mellon University nach Stanford. Dort gründete er zusammen mit einigen Kollegen das »Stanford University Network«, SUN. Auf der Suche nach neuen Herausforderungen hat er das Unternehmen bereits mehrere Male verlassen, denn »passive Tätigkeiten« wie etwa die Arbeit im Aufsichtsrat oder als Venture Capitalist langweilen ihn. Auch nach über 30 Jahren ist es das Umsetzen eigener Ideen, das ihm am meisten Spaß macht.

Joseph Weizenbaum

Vom Meilenstein der künstlichen Intelligenz zum Aufruf nach mehr (tatsächlicher) Intelligenz

Joseph Weizenbaum machte sich mit der Entwicklung seines Sprachanalyseprogramms ELIZA einen Namen in der Informatikbranche. Diese Software analysiert das Gesprochene und formuliert daraus, basierend auf dem gleichen Prinzip, das Chatbots heutzutage nutzen, intelligent erscheinende Fragen. Wissenschaftler konnten mit ELIZA beispielsweise psychotherapeutische Sitzungen so gut simulieren, dass Teilnehmer im Nachhinein der festen Überzeugung waren, sie hätten mit einem Menschen kommuniziert. Was für manch einen wie ein Meilenstein der künstlichen Intelligenz erscheinen mag, erschütterte den Entwickler. Aus dem einstigen Pionier, der die künstliche Intelligenz revolutionierte, wird ein (Gesellschafts-) Kritiker. Er bemängelt die »Leichtsinnigkeit […] und die Unverantwortlichkeit, […] mit der wir mit […] unserer Naturwissenschaft und Technik überhaupt umgehen« und ruft daher zu verantwortungsbewusstem Handeln anstelle der blinden Umsetzung verkaufsträchtiger Ideen auf. Man müsse als Wissenschaftler auch über einen Weitblick für die möglichen Konsequenzen seiner Forschung verfügen. »Wir haben eine künstliche Welt geschaffen«, so Weizenbaum, »in der es kein echtes Erleben mehr gibt.«

– Suhanyaa Nitkunanantharajah

Weitere intressante IT-Größen

Heinz Nixdorf
Der erfolgreiche Gründungsunternehmer der Nixdorf Computer AG entwickelte das Konzept eines Elektronenrechners auf Rundfunkröhrenbasis.

Gottlob Frege
Als Mathematiker und Philosoph revolutionierte er mit der Entwicklung einer formalen Sprache und formaler Beweise das Gebiet der Logik und schuf somit eine Grundlage für die moderne Informatik.

Karl Steinbuch
Im Jahr 1960 revolutionierte der als Mitbegründer der deutschen Informatik geltende Nachrichtentechniker und Informationstheoretiker Karl Steinbuch die Welt der Informatik mit seiner bahnbrechenden Erfindung, der sog. Lernmatrix. Somit entwickelte er das erste künstliche neuronale Netz und wird daher in der Branche als Vater und Pionier der künstlichen Intelligenz gefeiert.

Nikolaus Joachim Lehmann
Als wohl bedeutendster Informatiker der DDR entwickelte er unter anderem den ersten Tischrechner der DDR und bewies die Funktionsfähigkeit der von Leibniz entwickelten mechanischen Rechenmaschine.

Hans-Peter Kriegel
Mit seiner Forschung auf dem Gebiet des Data Mining gilt Hans-Peter Kriegel als einer der bedeutendsten und meistzitierten deutschen Informatiker.

Wege ins Ausland

Viele Wege führen nach Rom. Das hat euch wahrscheinlich schon eure Oma erzählt. Doch mindestens genauso viele Wege führen euch auch raus aus Potsdam und weg vom HPI – hinaus in die bunte Welt und, wenn ihr mögt, auch weit über Rom hinaus. Ob ihr euch auf einen dieser Wege wagen wollt und wenn ja, auf welchen, das müsst ihr selbst entscheiden. Wir haben euch ein paar Möglichkeiten zusammengestellt. Schließlich machen sich Auslandsaufenthalte nicht nur in eurem Lebenslauf bemerkbar, sondern bringen euch auch eine Menge einzigartige, interkulturelle Erfahrungen und stärken eure Selbstsicherheit. Egal, ob ihr im Ausland studiert, arbeitet oder reist. Doch bevor die Koffer gepackt werden können, gibt es einiges zu bedenken und zu planen.

– Julia Wachtel, Suhanyaa Nitkunanantharajah

Studieren

Ihr wollt mal etwas anderes sehen, fremde Länder und Kulturen entdecken, fremde Sprachen erlernen? Und am besten all das noch neben dem Studium? Dann seid ihr die perfekten Kandidaten für ein Studium im Ausland. Ob nur ein Semester oder doch einen gesamten Studienabschnitt, ob bei unseren Nachbarn in Frankreich oder doch am anderen Ende der Welt in Australien oder China – euch sind keine Grenzen gesetzt. Mit einem Studienaufenthalt im Ausland könnt ihr gemeinsam mit den einheimischen Studenten ihre Kultur erleben, das Land entdecken und dabei noch etwas dazulernen.

Vorbereitung

Je nach angestrebter Zieluniversität, Austauschprogramm und Aufenthaltsdauer kann die Vorbereitungszeit zwischen vier und 15 Monaten variieren. Insbesondere wer Stipendien zur Finanzierung in Anspruch nehmen möchte, sollte mindestens ein Jahr im Voraus mit der Planung beginnen.

»Toll studieren können Sie auch am HPI, aber im Ausland erleben Sie eben andere Dinge als in Berlin und Potsdam.«

Professor Naumann

Kosten

Miete und Lebenshaltungskosten sind im Ausland meist nicht billig. Dazu kommen Kosten für den Umzug und oftmals sehr üppige Studiengebühren. Natürlich möchte man dann nicht auch noch in den Bibliotheken oder Poolräumen der ausländischen Universität Wurzeln schlagen, sondern herumreisen und etwas vom Land sehen. All das kann das studentische Portemonnaie stark überstrapazieren. Eine Möglichkeit zur Finanzierung ist dabei das Auslands-BAföG. Eine Bewerbung lohnt sich selbst dann, wenn ihr bisher kein Inlands-BAföG erhalten habt. Auch Stipendien können den Geldbeutel ein wenig entlasten. Neben Stipendien diverser Stiftungen sind vor allem die des Deutschen Akademischen Austauschdienstes (DAAD) sehr begehrt. Sie können neben monatlichen Stipendien auch eine Reisekostenpauschale und Versicherungen enthalten.

Für Studenten mit dem Ziel USA ist das Fulbright-Stipendium sehr zu empfehlen. Dabei lassen Fördersummen von bis zu 34 500 € den etwas mühseligeren Bewerbungsprozess vergessen.

Achtung: Stipendienanträge für Fulbright sollten wegen ihrer Begehrtheit und der geringen Vergabekapazität mit viel Vorlaufzeit (mindestens ein Jahr) eingereicht werden.

Möglichkeiten

Erasmus

Eine Möglichkeit im Ausland zu studieren ist ein Erasmus-Semester im europäischen Ausland. Zwar ist man dabei in der Auswahl stark eingeschränkt, jedoch besteht der Vorteil, dass Studienbeiträge lediglich in der Heimat, nicht aber an der ausländischen Institution fällig werden.

Tipp: Solltet ihr keinen der begehrten Erasmus-Plätze des HPIs erhalten, besteht auch die Möglichkeit, über die Restplatzbörse, in der alle nicht-besetzten Erasmus-Plätze einer Universität gesammelt werden, einen Platz zu ergattern.

Das HPI pflegt derzeit unter anderem Partnerschaften mit Universitäten in Finnland, Schweden, Estland, Italien, Portugal und Frankreich.

Auslandsstudium über Hochschulpartnerschaften

Wem die EU weder aufregend noch fern genug ist, der sollte einen Blick auf die Hochschulpartnerschaften der Universität Potsdam werfen. Unter anderem gibt es derzeit Austauschprogramme mit ausgewählten Universitäten in Australien, Russland, Israel, Brasilien, Kolumbien, Costa Rica und den USA. Dort können Studenten der Universität Potsdam unter günstigeren Umständen studieren, meist sogar ohne Studiengebühren zahlen zu müssen.

Achtung: Die Semesterzeiträume entsprechen nicht an allen Partneruniversitäten den unseren. Ebenso verlangen einige Partnerhochschulen eine sehr frühzeitige Bewerbung (bis zu 1,5 Jahre im Voraus).

Selbst organisierte Auslandssemester

Habt ihr eine ganz bestimmte Universität ausgewählt, zu der weder das HPI noch die Universität Potsdam eine Partnerschaft pflegen, könnt ihr euer Auslandssemester selbstverständlich auch selbst organisieren. Ihr müsst euch dann aber auch darauf einstellen, dass ihr Studiengebühren zu zahlen habt. Auch bei Wohnungssuche und Co ist möglicherweise mit weniger Unterstützung zu rechnen, als es an einem Partner-Institut der Fall wäre. Daher ist eine vorherige Absprache mit dem Auslandskoordinator sehr zu empfehlen.

Sprachkurse

Zwar ist an den meisten Universitäten – vor allem im Master – Englisch die Unterrichtssprache. Dennoch: wer sich mit Einheimischen unterhalten mag und das Land nicht nur als Tourist erleben will, sollte die Landessprache zumindest ansatzweise beherrschen. Um euch den ersten Kontakt mit dem Land und der Sprache zu erleichtern, bieten viele Universitäten für ausländische Studenten kurz vor Beginn des Semesters zwei- bis dreiwöchige Sprachkurse an. Wer bereits früh weiß, wohin er will, kann auch schon einen Blick auf die Sprachkurse in den StudiumPlus-Angeboten der Universität Potsdam werfen.

Learning Agreement

Laufen die Vorbereitungen auf Hochtouren, solltet ihr einen Termin mit dem Auslandskoordinator (derzeit: Prof. Naumann) vereinbaren, um ein Learning Agreement aufzusetzen. Darin legt ihr fest, welche Kurse ihr im Ausland vorausichtlich belegen werdet. So erfahrt ihr bereits im Voraus, welche Kurse angerechnet werden, in welche Module sie eingebracht werden können und wie die Punkte und Noten umgerechnet werden.

Freiwilligendienst

Ihr habt Lust euch ehrenamtlich zu engagieren? Wollt raus aus dem Studien- und Arbeitsalltag? Seid bereit euch auf eine andere Kultur einzulassen, wollt neue Leute kennenlernen? Dann ist ein Freiwilligendienst genau das Richtige. Diese werden von verschiedenen Organisationen in so gut wie jedem Land der Welt angeboten.

Voraussetzungen

Neben der Offenheit für andere Kulturen und Menschen gibt es häufig eine Altersgrenze für Freiwillige. In den meisten Fällen liegt diese bei 16 bis 27 Jahren.

Bewerbung

Bei »long-terms« muss man sich in der Regel zehn bis zwölf Monate im Voraus bewerben. Bei einem Workcamp reicht es aus, wenn ihr euch wenige Wochen vorher anmeldet.

Dauer

Bei einem Freiwilligendienst handelt es sich entweder um »short-terms« bzw. Workcamps von zwei bis drei Wochen oder um »long-terms«, die zwischen mehreren Monaten und einem Jahr lang sind.

Wie kann ich mir die Arbeit vorstellen?

Das ist von Projekt zu Projekt verschieden. Freiwilligendienste finden häufig in sozialen Projekten und Einrichtungen statt. Es gibt auch Stellen mit ökologisch-nachhaltigem oder kulturellem Hintergrund. Allgemein gesprochen: Man kann der einheimischen Bevölkerung in fast allen Lebensbereichen unter die Arme greifen.

Kosten

In erster Linie müsst ihr als Freiwillige sämtliche Reisekosten tragen. Dazu kommt oft noch, dass die staatliche Förderung der Programme nicht ausreicht und von euch entweder direkt Organisationsgebühren verlangt werden oder ihr einen Unterstützer- und Förderkreis aufbauen müsst. Diese Förderkreise bestehen aus Freunden oder Bekannten, die euch eine gewisse Summe an Geld zur Verfügung stellen. Dieses Geld wird an die Partnerorganisation weitergeleitet und für anfallende Kosten während eures Aufenthalts verwendet.

Ausgewählte Programme

Weltwärts

- entwicklungspolitischer Freiwilligendienst vom Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung
- sozial orientierte Projekte, die zum Gemeinwohl der lokalen Bevölkerung beitragen
- Arbeit für 6 bis 24 Monate an einem Projekt in einem Entwicklungsland
- *www.weltwaerts.de*

WWOOF

- World Wide Opportunities on Organic Farms
- Unterstützung der Arbeit auf dem Bauernhof (organische Landwirtschaft)
- prinzipiell weltweit, besonders ausgeprägt in Großbritannien und den USA
- *www.wwoofinternational.org*

Kulturweit

- vom Auswärtigen Amt finanziert und gegründet
- zur Vermittlung deutscher Kultur im Ausland
- vor allem pädagogische Stellen in Schulen und Bildungseinrichtungen
- *www.kulturweit.de*

EFD

- Europäischer Freiwilligendienst, Teil des Aktionsprogrammes Jugend in Aktion der Europäischen Union
- in erster Linie soziale Projekte, aber auch Stellen in den Bereichen Jugendförderung, Umweltschutz und Kultur
- Datenbank aller Stellen: *ec.europa.eu/youth/evs/aod*, weitere Informationen: *www.go4europe.de*

Praktikum

Ihr wollt lieber praktische Erfahrungen sammeln, anstatt auf unbequemen Hörsaalstühlen der Theorie zu lauschen? Dabei auch Geld verdienen? Dann sind das die besten Voraussetzungen, euch einen Praktikumsplatz zu suchen.

Bewerbung

Ihr solltet für eure Bewerbung etwa neun Monate Vorlaufzeit einplanen. Bei den meisten großen Firmen läuft der Prozess online über eine Bewerbungsplattform. Eure Chancen auf einen Praktikumsplatz erhöhen sich jedoch, wenn ihr bereits Kontakte zu Mitarbeitern habt, denen ihr eure Bewerbung direkt schicken könnt. Eine Möglichkeit, solche Kontakte zu knüpfen, ist die HPI-Connect-Messe, die bereits im Mai 2014 wieder stattfindet.

Wurde eure Bewerbung für gut befunden, müsst ihr euch oft mehreren Interviews stellen. Dort wird zu Beginn eure technische Expertise auf den Prüfstand gestellt, anschließend gibt es häufig noch ein Telefonat. Mögliche Fragen und Erfahrungsberichte zu Interviews bei verschiedenen Unternehmen findet ihr unter *www.glassdoor.com*.

Dauer

Ein Auslandspraktikum dauert in der Regel mindestens zehn Monate. Google empfiehlt sogar eine Mindestlaufzeit von zwölf Monaten. Diese Zeit ist nötig, um sich mit seiner Arbeitsumgebung vertraut zu machen und ein vollwertiges Mitglied im Team zu werden.

Warum?

Als Student hat man die einmalige Gelegenheit, in die Arbeitskultur eines Unternehmens hineinzuschauen. Oft erwirbt man in einem Praktikum mehr Wissen als im gesamten Studium. Hier wird man ins kalte Wasser geworfen und lernt neben vielen technischen Raffinessen auch die Strukturen und Prozesse innerhalb einer Firma kennen. Erfahrungen, die wohl kein Dozent so aktuell zu vermitteln vermag.

Tipp: »Bei Fragen: fragen!« – Zu Beginn ist häufig vieles unklar. Also zögert nicht, sondern geht auf eure Kollegen zu.

Bezahlung

Die Bezahlung ist von Land zu Land und Unternehmen zu Unternehmen unterschiedlich. Meistens verdient man bei einem Praktikum in den USA mehr als in Europa. Auch die Urlaubsregelungen sind verschieden. Lest eure Verträge aufmerksam durch!

Viele größere Unternehmen haben eine Kantine, sodass ihr euch nicht um Verpflegung kümmern müsst. Oft werden Reisekosten erstattet. Eine eigene Unterkunft muss man in den meisten Fällen selbst finden.

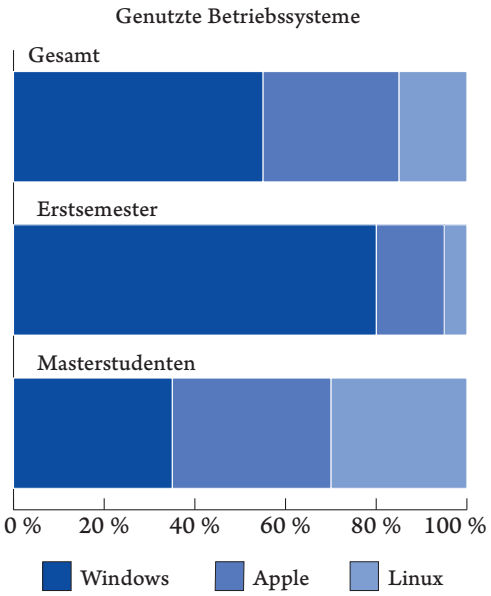
Raus aus dem Studienalltag

Wer nicht nur auf unbequemen Hörsaalstühlen der Theorie lauschen möchte, kann stattdessen einen Praktikumsplatz suchen oder an einem Freiwilligendienst teilnehmen.

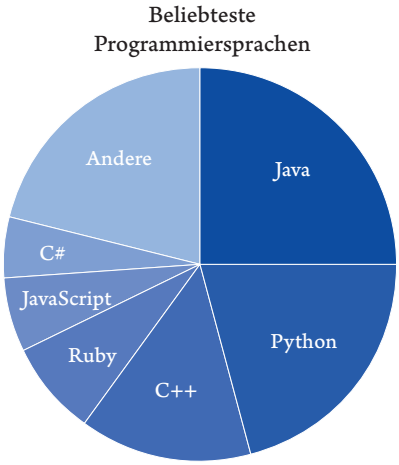
Windows, Java, Eclipse

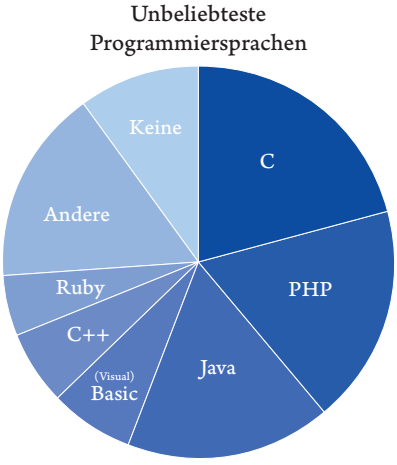
Jeder HPI-Student hat unterschiedliche Vorlieben bei der Arbeit am Computer. Welche ist im Moment die beliebteste Programmiersprache? Welches Betriebssystem wird am häufigsten verwendet? Und wie verändern sich bestimmte Vorlieben über die Zeit?
Wir haben versucht, Licht ins Dunkel zu bringen.

Betriebssysteme:
Bei den Betriebssystemen liegt Windows mit 55 % an der Spitze, vor Apple (30 %) und Linux (15 %). Die Werte für die einzelnen Semester unterscheiden sich dabei erheblich. Während der ersten beiden Studienjahre verwenden die mit Abstand meisten HPI-Studenten Windows (80 %). Dem gegenüber stehen gerade einmal 15 % der Studenten, die Mac bevorzugen, und der verschwindend geringe Anteil der Linux-Nutzer (5 %). Die Verhältnisse gleichen sich über die Jahre hinweg immer mehr einander an. Schließlich liegen im fünften und sechsten Studienjahr Windows und Mac, mit jeweils 35 %, gleichauf. Selbst die am Anfang kaum genutzten Linux-basierten Betriebssysteme werden von 30 % der Studierenden genutzt.

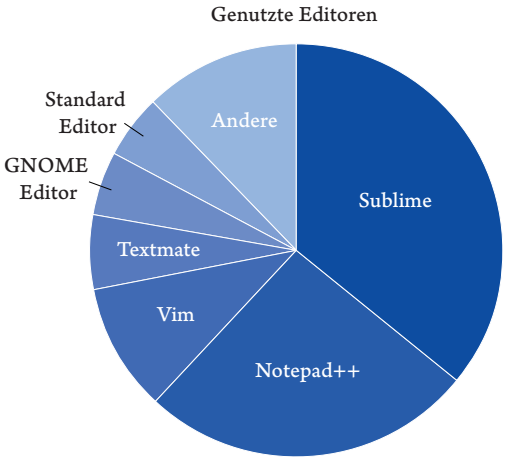


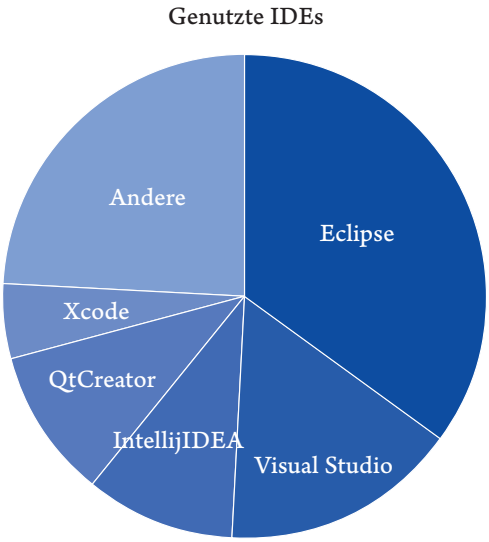
Programmiersprachen:
Bei den beliebtesten und unbeliebtesten Programmiersprachen gehen die Meinungen z. T. auseinander. So ist Python, die zweitbeliebteste Programmiersprache, bei fast niemandem unbeliebt, während Java als die beliebteste Programmiersprache auch auf Platz drei der unbeliebtesten Programmiersprachen vertreten ist. Und auch wenn deutlich ist, das mit jedem Studienjahr die Zahl der Studenten ohne »verhasste« Programmiersprache sinkt, sind C und PHP die bei HPI-Studenten unbeliebtesten Programmiersprachen.





Editoren:
Sublime Text (36 %) und Notepad++ (26 %) sind die beiden führenden Editoren, gefolgt von Vim und Textmate. Während Notepad++ unter den Windows-Usern häufiger verwendet wird, arbeiten die Apple-User am HPI vorwiegend mit Sublime und Textmate. Allerdings existiert Notepad++ lediglich für Windows. Dennoch ist dieses Ergebnis etwas überraschend, da Notepad++ der einzige Editor ist, der es in die oberen Regionen der Downloadcharts schafft, während Sublime deutschlandweit klar den Kürzeren zieht. Das kann sich allerdings daraus erklären, dass Windows weltweit am meisten benutzt wird.

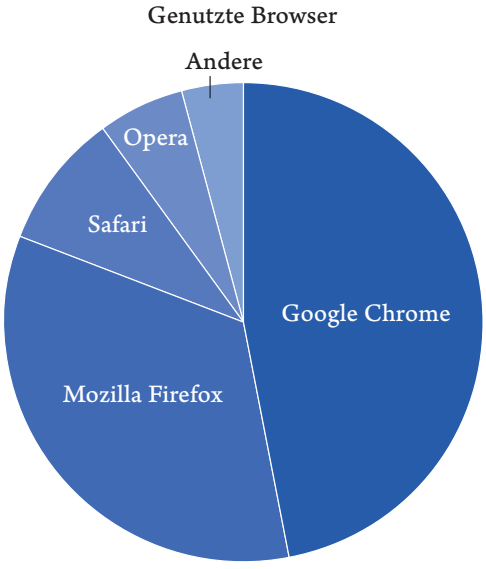




Entwicklungsumgebungen / IDEs:
Die Entscheidung der besten Entwicklungsumgebung ist sehr eindeutig ausgefallen. Unabhängig vom Studienjahr und dem genutzten Betriebssystem ist Eclipse, mit fast doppelt so viel Prozent wie Visual Studio auf dem zweiten Platz, die meistgenutzte Entwicklungsumgebung. Das liegt vermutlich an seiner Vielfältigkeit und Benutzerfreundlichkeit.

Browser:
Hier hat Google Chrome die Nase vorn und führt vor Mozilla Firefox, gefolgt von Safari und Opera. Diese Daten sind semesterunabhängig und stimmen auch fast mit den weltweiten Werten überein. Die einzige Ausnahme bildet hierbei Internet Explorer, welcher dort an dritter Stelle steht, am HPI jedoch nicht ein einziges Mal verwendet wird.

– Maximilian Götz



Die Umfrageauswertung erfolgte anhand von 100 Stimmabgaben von HPI-Studenten.

Tipps für Informatiker

Sieben Tipps und Tricks, um sich als Informatiker in ein soziales Umfeld einzufügen.

1. Versuche dein Aussehen anzupassen und nicht besonders aufzufallen.

Setze dich von Zeit zu Zeit dem Sonnenlicht aus, damit dein Hautteint sich langsam dunkelt.

Achtung! Beginne mit kurzen Intervallen, damit dein Körper Zeit hat sich an das Sonnenlicht zu gewöhnen. Jetzt kannst du auch weitere Wege bei Tag zurücklegen als bis zur Uni und zum Elektronikmarkt.

2. Geh zum Friseur.

Wenn du Tipp 1 befolgt hast, sollte dein Körper nun widerstandsfähig genug sein, um gefahrlos den Weg zum Friseur zurückzulegen. Viele erwarten von langhaarigen Personen, dass sie Informatiker sind, demnach fällst du mit kurzen Haaren weniger auf.

Ausnahme: Wenn du in der Umgebung von Wacken wohnst, dann ist es egal, wie lang deine Haare sind.

Achtung! Nimm dir an einem sehr sonnigen Tag etwas Sonnencreme für deinen Nacken mit, da er, wenn du vom Friseur zurückkehrst, zum ersten Mal der Sonne ausgesetzt sein wird.

3. Zieh dir etwas Ordentliches an.

Das ein oder andere T-Shirt mit einem lustigen Spruch darauf ist schön und gut, aber ein bisschen Abwechslung schadet deinem Kleiderschrank nicht. Lass dich am besten von einem Nicht-Informatiker beraten.

Achtung! Dein Ausflug zum Kleidungsladen sollte möglichst erst nach deinem Friseurbesuch stattfinden.

4. Sei lustig und unterhaltsam.

Zu den ersten zehn Witzen, die dir spontan einfallen: Nein! Die Hälfte davon versteht keiner, der nichts mit Informatik zu tun hat, und die anderen fünf sind nicht lustig.

Google am besten ein paar Witze. Benutze keine, die Star Trek oder Star Wars-Kenntnisse erfordern. Versuche spontan zu sein, kopiere Witze von anderen oder mach dich einfach auf Kosten anderer lustig. Das funktioniert fast immer.

5. Nicht alles und jeden korrigieren.

Versuche kleinere Fehler zu ignorieren, denn nichts erzürnt die weniger Intelligenten mehr, als sie auf ihre Fehler hinzuweisen.

6. Erzähl nicht jedem sofort, dass du Informatiker bist.

Es gibt immer noch viele Vorurteile gegenüber Informatikern. Du, der sich durch das Lesen dieser Tipps für ein Leben mit sozialen Kontakten entschieden hat, solltest den anderen die Möglichkeit geben, sich ein unvoreingenommenes Bild von dir zu schaffen.

Ausnahme: Du verdienst sehr viel Geld und suchst eine Frau für eine Nacht, dann sag ihr ruhig, dass du Informatiker bist, aber lasse im selben Atemzug einen Hinweis auf deinen Kontostand fallen.

7. Gib dich selbstbewusst.

Ein häufiger Fehler ist es, zu zurückhaltend und schüchtern zu sein. Bringe immer, wenn du kannst, deine Meinung ein und sie werden dich als einen der Ihren anerkennen.

– Maximilian Götz

Die Bedeutung des Einzelnen

Ein kleiner Kern, noch in der Erde,
der träumte gern, dass er was werde.

Einmal ein Baum sein, das wär fein!
Doch stieß er bald auf einen Stein.

Dieser, gar nicht recht erfreut,
dass jemand Kerne dort gestreut,

begann, den Wurzelweg zu sperren,
es half nichts, noch so sehr zu zerren.

So wuchs und wuchs der kleine Baum
nach oben, wie in seinem Traum.

Doch, im Boden braucht er Halt
und so war er noch nicht alt,

schon spürte er ein leichtes Wanken,
das war dem Stein wohl zu verdanken.

Er kam aus seinem Gleichgewicht,
die flachen Wurzeln hielten nicht.

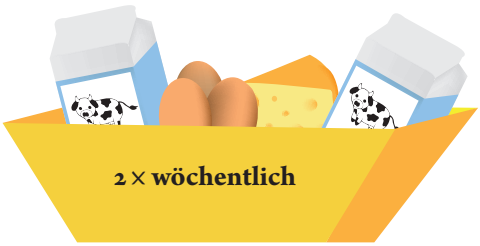
Darauf ein sehr schwerer Sturz,
zugegeben, er war kurz,

doch war's das Ende eines Lebens.
Was denkt nun ihr, war es vergebens?

Beachtung fand der Baum noch nicht,
doch heute gibt es ein Gedicht.

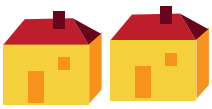
Wenn ein Reh den Baum auch frisst,
gib, dass du ihn nicht vergisst!

Mensa Griebnitzsee



Der Einkauf

Bestellt wird für alle Mensen zentral. Gemüse wird dreimal, Molkereiprodukte werden zweimal wöchentlich und Tiefkühlprodukte – wie auch das Fleisch – fast täglich geliefert. Beim Gemüse wird, beispielsweise bei Kartoffeln, versucht in der Region einzukaufen.



Die Zukunft

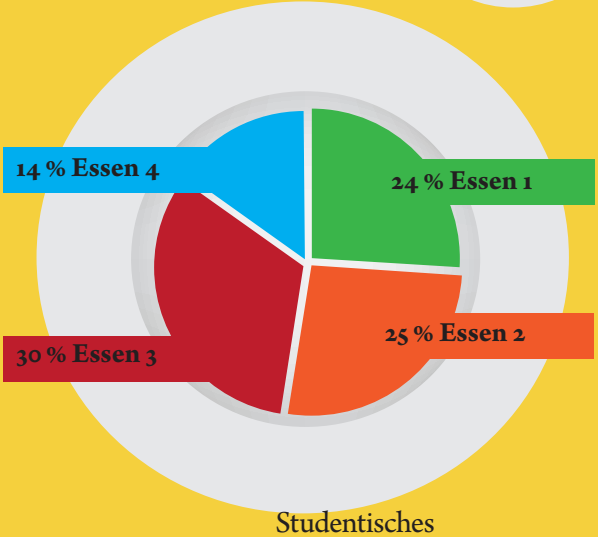
Ein Umbau wird in den nächsten Jahren notwendig sein. Die bisherige Essensausgabe ist eigentlich heute schon zu klein, so dass Wartezeiten zu Hochzeiten unabdingbar sind. Aus dieser Not heraus wurden daher auch Angebote wie die Nudeltheke oder der Grill im Hof aufgebaut, um die Essensausgabe zu entlasten.

6,4 % Salat

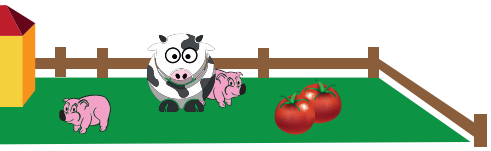
200 täglich

Der Kunde

In Brandenburg werden jedes Jahr ca. 1,5 Millionen Malzeiten von 30 000 Studenten verzehrt. In der Mensa am Griebnitzsee werden täglich ca. 2 000 Essen ausgeteilt.



Wissenswertes über die Abläufe und Beteiligten der Mensa



von Jasper Schulz

Der Speiseplan

Einmal im Monat treffen sich alle Mensaleiter und besprechen den Speiseplan. Einfluss haben darauf unter anderem das Feedback der Studenten und die Beliebtheit der einzelnen Speisen. Es wird dabei darauf geachtet, dass es jeden Tag eine ausgewogene, sich abwechselnde Auswahl zwischen Fisch, Fleisch und vegetarischem Essen gibt. Zu bestimmten Events, wie dem Nachhaltigkeitstag oder an internationalen Tagen, werden die Mensen angefragt und spezielle Menüs zusammengestellt.

Die Zubereitung

Gekocht wird direkt nach der Lieferung um 7 Uhr morgens. Das Essen wird dabei bis ca. 3 Uhr am Nachmittag chargenweise zubereitet. Ab 10 Uhr wird zudem die Cafeteria der Filmhochschule beliefert.

Der Preis

Der Preis für jedes Gericht wird vom Studentenwerk festgelegt. Das durchschnittliche Gericht kostete 2012 4,37 €. Daher wurden 2013 die Preise das erste Mal seit zehn Jahren angehoben. Die Mensen selber haben somit ein festes Budget, dass sie pro Gericht ausgeben dürfen. Subventioniert wird das Essen für Studenten vom Land Brandenburg.

Essen 1		**Essen 3**	
Studierende:	1,40 €	Studierende:	2,50 €
Bedienstete:	2,60 €	Bedienstete:	3,85 €
Gäste:	3,50 €	Gäste:	5,00 €
Essen 2		**Essen 4**	
Studierende:	2,00 €	Studierende:	2,50 €
Bedienstete:	3,35 €	Bedienstete:	3,85 €
Gäste:	4,50 €	Gäste:	5,00 €

Von BS II bis VHDL

In den ersten Semestern hat man seinen Stundenplan am HPI noch relativ fest vorgegeben, doch ab dem dritten Semester steht man vor der Qual der Wahl: Welche Vertiefungsgebiete soll man wählen? Wir haben einige HPIler gefragt, die sich schon entschieden haben. Sie stellen euch elf häufig gewählte Vertiefungsgebiete vor.

– Carolin Fiedler

Empfehlung:

Betriebssysteme II

Art: Vorlesung SWS: 4 LP: 6 Teilnehmer: 30

Übung: freiwillige, zwei- bis dreiwöchige Übungen, Übungstermin anstelle der Vorlesung
Übungsaufwand: 5 h pro Übung

Im SoSe 2013 hielten Frank Feinbube und Christian Neuhaus die Vorlesung Betriebssysteme II. Sie orientierten sich dabei thematisch an BS I, und nutzten Inhalte aus ihren eigenen Forschungsarbeiten, um die Vorlesung spannend zu gestalten. Mithilfe von Praxisbezügen aus Bereichen wie zum Beispiel Mobile Computing und Cloud Computing motivierten sie uns zur Bearbeitung von Themen wie Fehlertoleranz, Dateisysteme und Virtualisierung. Verglichen wurden dabei verschiedene Betriebssysteme, jedoch lag das Hauptaugenmerk auf Windows. In den Veranstaltungen fanden viele Diskussionen statt, besonders in den von Bernhard Rabe geleiteten Übungen. Zudem boten die freiwilligen Übungen viel Freiraum für Experimente.

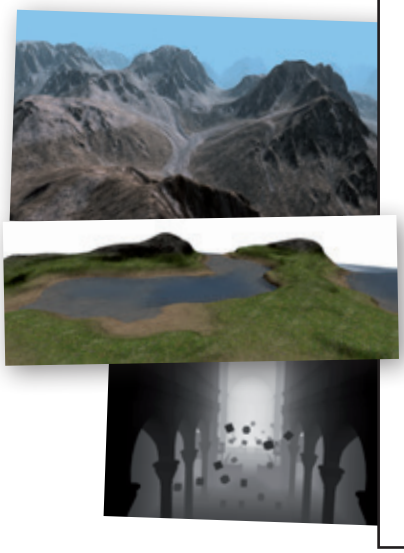
– Carolin Fiedler und Karsten Tausche

Empfehlung:

Computergrafik II

Art: Vorlesung SWS: 4 LP: 6 Teilnehmer: 15 bis 45

Übung: im Zweiwochentakt, Übungstermin anstelle der Vorlesung
Übungsaufwand: 6 bis 8 h pro Übung



Die Inhalte der Vorlesung bauen auf dem Wissen der Vorgängerveranstaltung auf, können allerdings auch von den Studenten aktiv mitbestimmt werden.

Neben dem Vorlesungsskript werden zu den behandelten Themen ergänzende Materialien zum Selbststudium zur Verfügung gestellt. Übungen werden, wie bereits in CG I, in Zweiergruppen bearbeitet. Umfang und Schwierigkeitsgrad der Übungen variieren manchmal sehr. Jedoch sind die Betreuer sehr entgegenkommend und unterstützen die Studenten gern. In den Übungen vertieft man den Umgang mit C++, OpenGL und lernt GLSL kennen.

– Suhanyaa Nitkunanantharajah und Carolin Fiedler

Legende für den Empfehlungswert der jeweiligen Veranstaltung:

 »Ich würde es jederzeit wieder belegen«

 »Naja, ich bereue es nicht, aber nochmal muss auch nicht«

 »Nee, nie wieder«

Empfehlung:

Cops & Robbers

Art: Seminar SWS: keine Angabe, da keine regelmäßige Veranstaltung LP: 6 Teilnehmer: 6 bis 10

Zeitaufwand: 5 bis 60 h pro Woche, abhängig von aktueller Phase

Interessant für diejenigen, die sich wirklich für Security interessieren. Zwei Teams mit je vier bis fünf Personen treten in teils selbst entworfenen Szenarien gegeneinander an. Und natürlich wollen beide einerseits so viel wie möglich vorher wissen und andererseits verhindern, dass die anderen etwas Nützliches erfahren. Die Aufgaben geben meist nur einen Rahmen vor, die Teams können und müssen sehr selbstständig arbeiten. Die Seminarsprache ist Englisch. Bewertet werden alle Aktivitäten vor und während der Szenarien, deren Dokumentation und ein Einzelvortrag. Gute Ergebnisse in ISec sind Voraussetzung für die Teilnahme. Sehr zeitaufwändig, sehr spannend, akute Gefahr von Paranoia.

– *Sven Knebel*

Empfehlung:

Datenbanksysteme II

Art: Vorlesung SWS: 4 LP: 6 Teilnehmer: 20 bis 30

Übung: zusätzlich zur Vorlesung, wöchentlich bis dreiwöchentlich
Übungsaufwand: 1 bis 3 h pro Woche

Während es in Datenbanksysteme I hauptsächlich um die mathematischen Grundlagen von Datenbanken und eine geeignete Aufteilung von Daten auf Tabellen geht, blickt der zweite Teil der Serie hinter die Kulissen. Die Vorlesung tastet die verschiedensten Themengebiete von der Historie und dem Aufbau von Datenbanken über verschiedene Datenstrukturen bis hin zum Zusammenschluss zu Clustern ab. In der Übung werden parallel dazu unter anderem minimale und maximale Zugriffszeiten bei verschiedenen Datenstrukturen berechnet, die Auswirkung von Indizes auf Anfragen gemessen und sogar ein Einblick in die Anwendung von Map-Reduce-Algorithmen gegeben. Die Übung kann wie gewohnt in Teams von zwei Personen absolviert werden.

– *Daniel Dummer*

Empfehlung:

Game Programming

Art: Projektseminar SWS: 4 LP: 6 Teilnehmer: 15 bis 30

Projekt: Spieleprojekt über das gesamte Semester, Treffen mit Betreuer nach Absprache
Projektaufwand: 4 bis 8+ h pro Woche

Wie bereits der Name verrät, dreht sich das Seminar rund um die Spieleprogrammierung. In kleinen Gruppen von zwei bis vier haben Studenten die Chance, ein Spiel ihrer Wahl zu kreieren, wobei der Wahl des Themas nahezu keine Grenzen gesetzt sind. Im Laufe des Semesters sind pro Team drei kurze Präsentationen zu halten – eine Konzeptvorstellung, eine Zwischenstandspräsentation sowie eine Abschlusspräsentation. Jedes Team wird dabei durch einen Mitarbeiter über das gesamte Semester hinweg betreut. Das Seminar wird während der gesamten Zeit durch Vorträge rund um das Thema ergänzt.

– *Suhanyaa Nitkunanantharajah*

Empfehlung:

Grafikprogrammierung mit OpenGL und C++

Art: Projektseminar SWS: 4 LP: 6 Teilnehmer: 12

Projekt: Projekt über das gesamte Semester (wechselnde Teams, Aufgabenstellungen)
»Hands-On« zweiwöchig, Inhaltsvorlesungen wöchentlich

Projektaufwand: 6 bis 10 h pro Woche

Das Ziel des Seminars war die gemeinschaftliche Entwicklung eines Viewers für unterschiedliche 3D-Formate. Ausgehend von einer einfachen Anwendung sollten verschiedenste Navigations-, Rendering- und Kameratechniken implementiert werden. Dabei erfolgte die Aufgabenzuteilung im Team und richtete sich nach den persönlichen Interessen und Kenntnissen in OpenGL, GLSL und C++. Im Projektverlauf gab es zwei Meilensteine, an denen die jeweiligen Teilergebnisse aller Teams zusammengeführt wurden. Zur Versionsverwaltung wurde dabei Git genutzt und der Umgang damit in der Vorlesung erklärt. Es ist geplant, das Projekt im nächsten Semester weiterzuführen.

– Carolin Fiedler und Karsten Tausche

Empfehlung:

HCI: Building Interactive Devices and Computer Vision

Art: Vorlesung SWS: 4 LP: 6 Teilnehmer: ca. 20

Assignment: Jede Woche ist ein Assignment zu lösen, das nicht in die Benotung eingeht.
Aufwand pro Assignment: Zwischen einer und acht Stunden ist alles möglich, je nachdem mit wie viel Liebe zum Detail gearbeitet wird.

HCI 2 richtet sich an den Erfinder- und Tüftlergeist in euch. Hier wird entworfen, gebaut, gelasercuttet und gelötet. Am Anfang beschäftigt man sich allerdings erst einmal viel mit Computer Vision. Unter anderem baut ihr euren eigenen Touchscreen mit Kinect und Beamer. Dann geht es um mechanisches und elektronisches Design von Fahrzeugen oder Booten, das ändert sich immer wieder. Krönender Abschluss ist das Rennen der verschiedenen Gruppen mit ihren entworfenen Fahrzeugen am Ende des Semesters. Meiner Meinung nach nicht so viel Aufwand und mehr Spaß als in HCI 1.

– Julia Wachtel

Empfehlung:

Internet Security

Art: Vorlesung SWS: 4 LP: 6 Teilnehmer: ca. 50

Übung: wöchentliche Übung
Übungsaufwand: 1 bis 8 h pro Woche

Die Übungen geben einen brauchbaren Überblick auf verschiedene Aspekte von IT-Sicherheit und relevante Techniken. Für wirkliches Verständnis und Wissensgewinn muss man jedoch das Gebotene als Anregung verstehen und selbst weiter recherchieren, da viele Themen nur angeschnitten oder in den Grundlagen erklärt werden. Zweimal finden »Hands-on-Sessions« statt, bei denen praktische Angriffe erprobt werden. Die Übungsleiter haben in den letzten Jahren oft gewechselt, wodurch sich Details beim Übungsablauf ändern. Die Sprache in Vorlesung und Übungen ist Englisch.

– Sven Knebel

Empfehlung:

Softwaretechnik II

Art: Vorlesung, Projekt SWS: 4 LP: 6 Teilnehmer: ca. 20 bis 30

Projekt: Umsetzung eines Softwareprojekts im großen Team in ca. vier Sprints
Projektaufwand: Man kann sich auf ziemlich genau einen Tag Arbeit pro Woche einstellen – eine geregelte Arbeitszeit gehört zum Projekt.

Zu lernen gibt es in dieser Veranstaltung vieles, was in moderner Softwareentwicklung von Bedeutung ist: Test- und verhaltensgetriebene Entwicklung, der Scrum-Prozess, praktische Versionsverwaltung mit Git, und auch Continuous Integration kommen zur Sprache und können gleich angewandt werden. Mein Tipp: Lieber den Prozess durchziehen, als mit aller Macht versuchen, die Applikation fertigzubekommen. So kann man sehr viel darüber lernen, was im Team funktioniert. Außerdem lernt man, was einen aufhält und wie man am besten Prioritäten setzt.

Alles in allem fühlte sich in meiner HPI-Zeit kaum ein Projekt realistischer als das SWT-II-Projekt an. Deswegen ist Softwaretechnik II eine große Chance – aber wie immer hängt es ganz von euch ab, was ihr daraus macht.

– Franz Liedke

Empfehlung:

Telemedicine

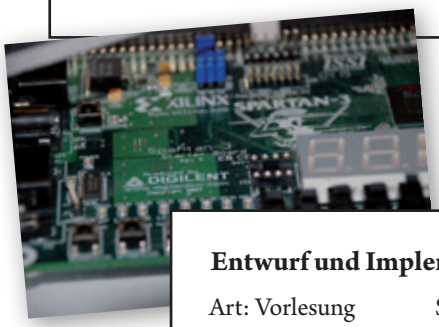
Art: Seminar SWS: 2 LP: 3 Teilnehmer: 5 bis 12

Abgaben: 25′-Vortrag (+ 15′ Diskussion) + 10-seitige Seminararbeit pro Person
Aufwand: 2 h Vorbereitung pro Seminar (Anwesenheitspflicht zu allen Vorträgen / Veranstaltungen) + 50 h für Vortrag und Arbeit

---

Umfang und Aufwand sind abhängig von der Gruppengröße – je mehr Teilnehmer, desto mehr Themen werden behandelt. Prinzipiell ist die Bearbeitung eines Themas alleine vorgesehen, nach Absprache ist es aber zu zweit möglich (mit doppelter Zeit und Seitenzahl). Die Seminarsprache ist Deutsch. Diskussionen erstrecken sich z. T. über den informatisch-technischen Teil hinaus, zugunsten von Moral und Ethik. Es gibt eine aufmerksame Betreuung, welche offen für Fragen und in der Gestaltung des Themas ist. Es ist sehr theorielastig, aber bei Interesse an medizinisch-klinischer Informatik empfehlenswert.

– Caroline Göricke



Empfehlung:

Entwurf und Implementierung digitaler Schaltungen mit VHDL

Art: Vorlesung SWS: 4 LP: 6 Teilnehmer: ca. 15

Übung: praktische und freiwillige Übung, ähnlich zu GdS
Übungsaufwand: praktische Übungen während des Semesters: 1 bis 3 h; letzte praktische Übung (Projekt): >5 h

---

Wen in GdS Hazards fasziniert haben, dem wird auch VHDL gefallen. Hier geht es prinzipiell zwar um die Hardwarebeschreibungssprache VHDL, aber auch um den allgemeinen Entwurf und die Simulation von Schaltungen. Jede Übungsgruppe von jeweils zwei Studenten bekommt schon zu Beginn ein eigenes FPGA-Board. Der Übungsaufwand ist ähnlich zu GdS. Am Ende des Semesters gibt es eine größere Projektaufgabe. Hier kann jeder seine Gewandtheit auf dem FPGA-Board und im Umgang mit VHDL unter Beweis stellen. Insgesamt eine Vorlesung in angenehmer Atmosphäre und mit fairem Arbeitsaufwand.

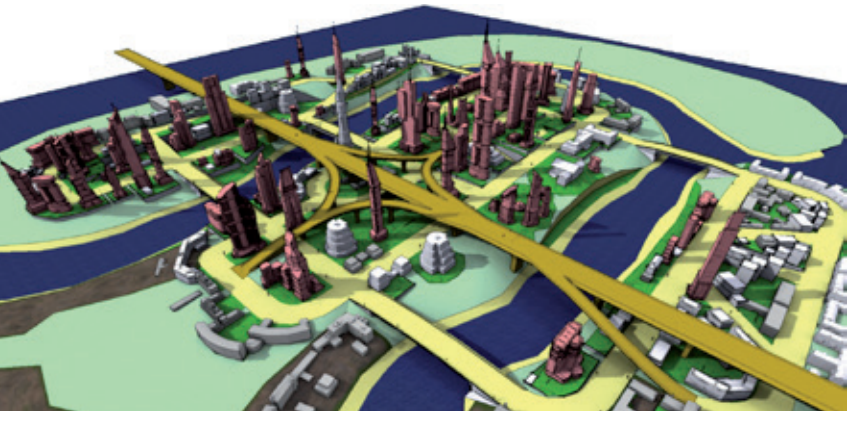
– Julia Wachtel

Nichtfotorealistische Visualisierung virtueller 3D-Stadtmodelle

Die nichtfotorealistische Bildsynthese stellt ein umfangreiches, innovatives Repertoire zur grafischen Gestaltung bereit, die eine wirkungsvolle Visualisierung komplexer raumbezogener Informationen ermöglicht. Der Fachbereich für computergrafische Systeme beschäftigt sich u. a. mit dem Design, der Implementierung und Evaluierung von nichtfotorealistischen Visualisierungstechniken für virtuelle 3D-Umgebungen – ein Forschungsbericht von Amir Semmo.

Virtuelle 3D-Umgebungen haben sich zu einem wirkungsvollen Medium für die interaktive Kommunikation von komplexen raumbezogenen Informationen entwickelt. Aufgrund der steigenden Leistungsfähigkeit von Computergrafik-Hardware und der damit möglichen Echtzeit-Visualisierung von massiven, komplexen Geodaten lassen sich virtuelle 3D-Umgebungen als interaktives Medium nutzen, u. a. in der Stadtplanung, Navigation, Touristeninformation und im Katastrophenschutz. Virtuelle 3D-Stadtmodelle präsentieren eine spezialisierte Form virtueller 3D-Umgebungen und sind im Allgemeinen gekennzeichnet durch ein zugrunde liegendes digitales 3D-Geländemodell, darin befindliche 3D-Bebauungsmodelle sowie das dazu komplementäre Straßen-, Grünflächen- und Naturraummodell.

Virtuelle 3D-Stadtmodelle abstrahieren gezielt von der Realität, um die Verständlichkeit und Wahrnehmbarkeit ausgewählter Informationsaspekte zu ermöglichen. Allerdings sind die meisten Visualisierungssysteme für diese Modelle durch ihre fotorealistische Darstellung gekennzeichnet. Ein bekanntes Beispiel ist Google Earth. Viele Anwendungsgebiete erfordern jedoch eine explizite grafische Gestaltung der dargestellten Informationen und deren Semantik. Dies ist z. B. bei der effizienten Kommunikation von Straßenkreuzungen der Fall, um eine schnelle Entscheidungsfindung bei der Navigation zu ermöglichen oder bei Anwendungen, bei denen aus Prinzip eine fotorealistische Visualisierung nicht anwendbar ist, z. B. im Fall thematischer Informationen zur Stadtplanung und -analyse. Eine effektive Kommunikation von Informationen hängt in diesen Szenarien signifikant davon ab, wie wichtige Informationen hervorgehoben und weniger wichtige Informationen abstrahiert werden bzw. kognitiv in einem Anwendungskontext verarbeitet werden. Dieser schließt das Hintergrundwissen eines Nutzers, den 3D-Szeneninhalt, die Ansicht auf die 3D-Umgebung und die Bildauflösung mit ein. Hierzu werden Visualisierungstechniken benötigt, die eine Kombination von detaillierten sowie nichtfotorealistischen Grafikstilen vornehmen. Da virtuelle 3D-Umgebungen in Bezug auf Geometrie, Erscheinung und thematischer Information komplex sind, ist das Design und die Implementierung von kombinierten Grafikstilen eine große Herausforderung: Diese müssen nahtlos integriert,



Nichtfotorealistische Visualisierung eines virtuellen 3D-Stadtmodells

Die grafische Repräsentation und Farbgebung orientieren sich an einer kartographischen Visualisierung, um thematische Informationen hervorzuheben.

interaktiv parametrisiert und in Echtzeit ineinander überführt werden.

Die am Fachbereich für computergrafische Systeme entwickelten, echtzeitfähigen Visualisierungstechniken ermöglichen es, Abstraktionsstufen von dynamisch-veränderbaren thematischen Informationen nutzungskontextabhängig zu selektieren und nahtlos in die Abläufe der Bildsynthese von Grafikprozessoren zu integrieren. Hierbei stellt die Shader-Programmierung der OpenGL-API die Grundlage für eine parametrisierte Bildsynthese dar.

Texturbasierte Abstraktion

Texturen bilden eine wesentliche Kategorie von Informationsträgern für Objekte virtueller 3D-Stadtmodelle; sie vermögen insbesondere, das Bild der natürlichen Erscheinung von Objekten wiederzugeben, z. B. Gebäudefassaden. In Verbindung mit »Texture Mapping« als computergrafischem Verfahren, kann hierdurch die geometrische Komplexität von 3D-Modellen verringert, und damit deren echtzeitfähige Bildsynthese gewährleistet werden. Für eine gezielte, nichtfotorealistische Bildsynthese bedarf es daher auch einer Abstraktion von Texturinformationen.

Bildfilter stellen effektive computergrafische Werkzeuge zur Informationsabstraktion dar, bei denen Details in Bereichen hoher Kontraste abstrahiert werden, gleichzeitig aber Objektkanten erhalten bleiben, welche für die Wahrnehmung einer virtuellen Umgebung wichtig sind. Für die texturbasierte Abstraktion verwenden wir u. a. einen bilateralen und »Difference-of-Gaussians«-Filter (DoG-Filter). Im Gegensatz zu klassischen Weichzeichnungsfiltern gewichtet ein bilateraler Filter nicht nur in der Distanz, sondern gleichzeitig auch in der Domäne (z. B. Farbdifferenzen) um Objektkanten zu erhalten. Der DoG-Filter hingegen detektiert wichtige Kanten im

Bildfilterung von Luftbildern

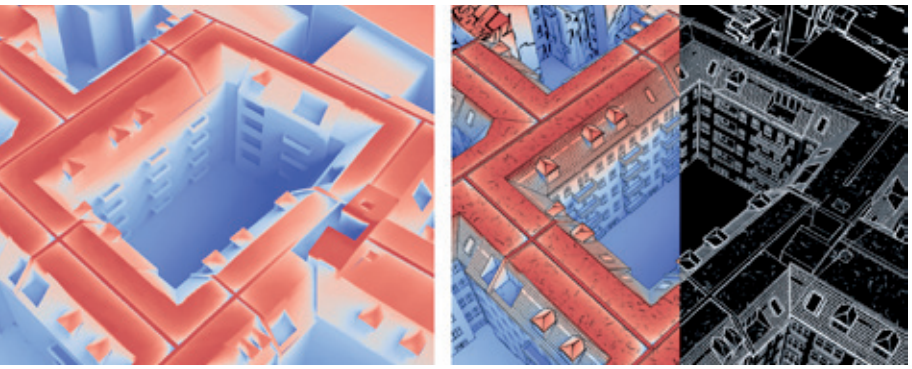
Die Anwendung eines bilateralen und DoG-Filters auf die Detailstufen eines Luftbilds (links) führt zu einem kontinuierlichen Abstraktionsgrad (mitte / rechts) bei der Visualisierung.

Farbraum und koloriert diese entsprechend ihrer Intensität. Diese Filter werden zunächst für Texturen angewendet, um eine perspektivisch-korrekte Abstraktion zu gewährleisten. Die Ergebnisse werden anschließend über ein verzögertes (engl., »deferred«) Texture Mapping auf ihre Oberflächen projiziert, ein Konzept, das auch bei modernen Computerspielen Anwendung findet. Dieser Prozess erfolgt separat für jede Detailstufe einer Textur. Mithilfe der Texturfilterung entsteht so eine kontinuierliche, sichtabhängige Abstraktion, bei der Bildbereiche einer perspektivischen Projektion, die bei fotorealistischen Darstellungen durch Informationskompression oftmals zu Bildrauschen führen, artefaktfrei dargestellt werden.

Der Einfluss einer Kantenhervorhebung auf die Wahrnehmung, wie sie beim DoG-Filter erfolgt, wurde exemplarisch anhand von thematischen Daten einer Solarpotenzialanalyse des Berliner 3D-Stadtmodells gezeigt. Diese Daten liegen als 2D-Texturen vor, deren Projektion auf die geometrischen Oberflächen zu einem Verlust von strukturellen Informationen führt, die nicht explizit als Geometrie modelliert aber für die Identifikation von Umrissen wichtig sind, z. B. bei Fenstern oder Dachstrukturen. Durch die Überblendung der Resultate des DoG-Filters können solche Informationen in die virtuelle 3D-Umgebung reintegriert werden. Eine Nutzerstudie hat hierbei gezeigt, dass die Orientierung in der virtuellen 3D-Umgebung signifikant verbessert wird sowie Distanzen besser abgeschätzt werden.

GPU-Shader

Aktuelle High-End Grafikkarten besitzen ca. 2 800 Shader-Einheiten, die als kleine progammierbare Recheneinheiten parallelisierte Bildsynthese-Effekte umsetzen. Die Umsetzung von Shadern mit WebGL kann unter *http://shadertoy.com* erprobt werden.



Visualisierung thematischer Daten

Ergebnis einer Solarpotentialanalyse (links), kombiniert mit den Ergebnissen eines DoG-Filters, um strukutrelle Informationen zu integrieren (rechts).

Kartographische Visualisierung

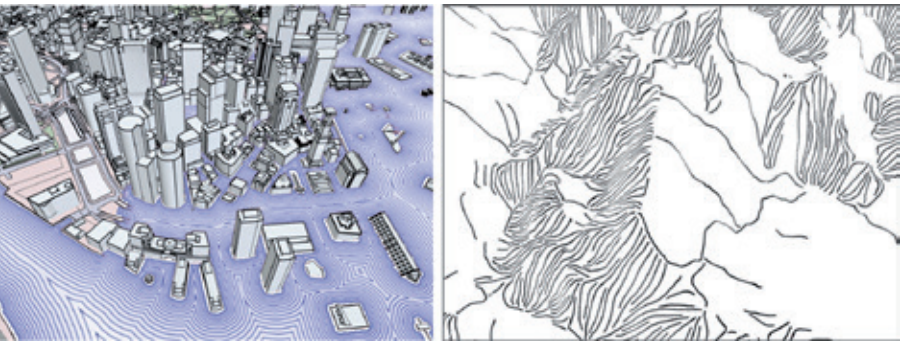
Um eine nutzer-, kontext- und medienadäquate Repräsentation thematischer Informationen zu ermöglichen, bedarf es einer Kopplung der nichtfotorealistischen Bildsynthese an semantische Informationen, um überwiegend »monotone Illustrationen« zu vermeiden. Hierzu wurden Visualisierungstechniken umgesetzt, die auf den Grundprinzipien der Kartografie aufbauen.

In der Kartografie ist die Farbgestaltung von Flächen, Linien und Punkten eine Haupttechnik in Hinblick auf eine effektive Visualisierung (neben anderen visuellen Variablen). Chromatisch gestaltete Karten haben ein wesentlich höheres Potenzial, die Aufmerksamkeit auf wichtige Informationen zu lenken, diese abzuschwächen oder hervorzuheben. Für die kartografische Visualisierung von virtuellen 3D-Stadtmodellen besitzt die Farbgestaltung von Flächen einzelner 3D-Objekte in Abhängigkeit ihrer Semantik großes Potenzial für die Unterscheidbarkeit. Ein divergierendes bzw. qualitatives Farbschema wird eingesetzt, um eine visuelle Abgrenzung von logisch oder geografisch assoziierten semantischen Klassen umzusetzen, ein sequenzielles Farbschema hingegen, sobald ein Spektrum kontinuierlicher Daten visualisiert werden soll, z. B. um thematische Informationen effektiv zu kommunizieren.

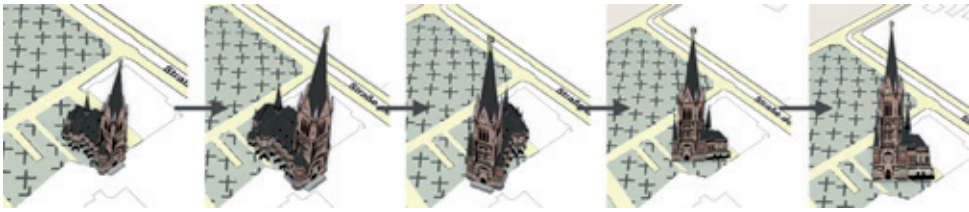
Eine kartografische Gestaltung wurde exemplarisch auch auf Objekt-Ebene umgesetzt, um Charakteristiken von Wasserflächen, Gebäuden, Infrastrukturnetzen und Geländemodellen unterschiedlich zu visualisieren. Bereits mit Anbeginn der ersten künstlerisch und kartografisch verwandten Darstellungen von 3D-Stadtansichten im Mittelalter haben Künstler von dieser Methodik Gebrauch gemacht, um den Informationsgehalt ihrer Illustrationen zu verstärken und zu fokussieren. Für Wasserflächen haben wir Visualisierungstechniken auf Basis von Distanzfeldern entworfen und implementiert um die Wahrnehmung zu verbessern. Ein Distanzfeld einer Wasserfläche wird als Textur abgebildet und beschreibt pro Bildpunkt, in welcher Entfernung (und ggf. in welcher Richtung) das nächstgelegene Ufer liegt. Durch die Projektion dieser Distanzattribute, können Schraffuren, Wasserlinien oder Punktstriche (engl., »stipples«) prozedural entlang einer Uferfläche orientiert und abhängig von der Distanz parametrisiert werden. Ähnlich wurden für digitale 3D-Geländemodelle die lokale Geländeneigung und Kurvatur berechnet, um digitalisierte, handgezeichnete Schraffuren prozedural auf dem Geländemodell zu verorten und geomorphologische Eigenschaften effektiv zu visualisieren. Ein weiteres Beispiel sind Vegetationsflächen, auf denen Signaturen prozedural und in unregelmäßigen Abständen mittels »Texture-Bombing«-Verfahren visualisiert werden, u. a. um Landnutzungsinformationen bzw. Waldgebiete zu kennzeichnen.

Wasserflächen- und Geländeabstraktion

Anwendung von Wasserlinien für eine Flutungssimulation (links) und stilisierte Darstellung eines digitalen 3D-Geländemodells (rechts).



Sichtabhängige Visualisierung



Die Visualisierung virtueller 3D-Umgebungen basiert oftmals auf statischen Grafikstilen, die entsprechend des jeweiligen Anwendungsfalls angepasst sind. Detaillierte Repräsentationen eignen sich z. B. für die Erkundung von lokalen Umgebungen, während klassische 2D-Karten als effektives Medium für Navigationszwecke eingesetzt werden. Virtuelle 3D-Umgebungen sind jedoch durch ihre interaktive Nutzung gekennzeichnet, bei denen sich der Anwendungskontext oder die Sicht auf die Umgebung dynamisch ändert. Systeme wie Google Maps integrieren vorberechnete Repräsentationen, bieten aber nicht die Möglichkeit, diese in einem Bild zu kombinieren.

Unser Lösungsansatz besteht darin, den Abstraktionsgrad von dargestellten Informationen kontextabhängig zu wählen. Hierzu haben wir ein System entwickelt, welches verschiedene Grafikstile implementiert, parametrisiert und miteinander verblendet. Ein Schlüsselkonzept stellt dabei die Fokus-&-Kontext-Visualisierung dar, bei der wichtige Informationen in Fokusregionen hervorgehoben werden, z. B. bei Objekten entlang einer Route, während weniger wichtige Informationen abstrahiert werden, z. B. bei Objekten in der Umgebung einer Route. Hierzu werden Sichtmetriken verwendet und pro 3D-Objekt evaluiert, z. B. entsprechend der Distanz zur virtuellen Kamera oder zu einer Interessensregion. Der Abstraktionsgrad wird entsprechend hoch bei weniger wichtigen Informationen und entsprechend niedrig bei wichtigen Informationen gewählt. Dazwischen erfolgt eine Interpolation. Um Landmarken für die Orientierung und Navigation visuell hervorzuheben, werden Transformationstechniken angewendet um eine 3D-Repräsentation kontinuierlich in eine symbolhafte 2D-Repräsentation zu überführen und zum Betrachter zu orientieren. So ergibt sich eine grafische Darstellung, die der einer Touristenkarte ähnelt.

Eine Evaluierung hat gezeigt, dass die umgesetzten Verfahren den Blick eines Nutzers auf priorisierte Informationen bzw. Interessensregionen lenkt, dies ist z. B. bei zeitkritischen Anwendungen wie der Fahrzeugnavigation von hoher Bedeutung. Durch die steigende Verfügbarkeit von virtuellen 3D-Stadtmodellen auf mobilen Endgeräten, wie z. B. Smartphones, ist daher zu erwarten, dass die umgesetzten Techniken in Zukunft auch im Massenmarkt Einzug erhalten.

– Amir Semmo

Weiterführende Informationen

→ *www.hpi3d.de | www.hpi3d.de/semmo*

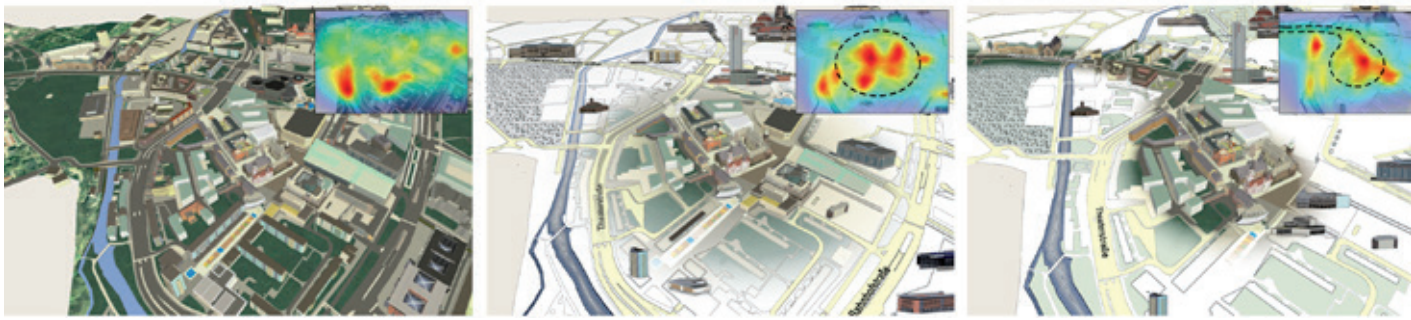
→ *www.youtube.com/hpicgs*

Landmarken-Transformation

Kontinuierliche Überführung einer 3D-Landmarke in eine optimierte, sichtorientierte 2D-Repräsentation durch mehrere, geometrische Transformationen.

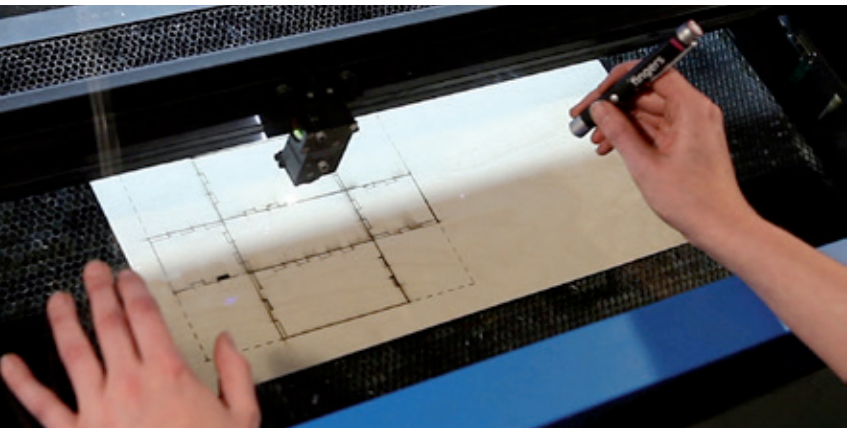
Fokus-&-Kontext-Visualisierung

Im Vergleich zu einer klassischen, detaillierten Variante (links), sind Objekte in einer Interessensregion (mitte) und entlang einer Route (rechts) detaillierter dargestellt als Objekte in der Umgebung. Die Auswirkung auf die Bildbereiche, die den Blick einfangen, ist als Heatmap erkenntlich (oben rechts).



Laser-Cutting and 3D Printing

Stefanie Müller about her work at the HCI Lab



constructable

… is an interactive drafting table based on a laser cutter. Users draw directly on the workpiece using a handheld laser pointer. The system tracks the path, beautifies the shape, and immediately cuts.

In my PhD work at the Human Computer Interaction Lab of Professor Baudisch, I develop new interfaces for personal fabrication devices, such as laser cutters and 3D printers. I'm very happy that my first three research projects are already published at the leading HCI research conferences. Together with the bachelor's and master's students who co-authored the papers, we also gave a range of demos, for which we drove our laser cutter through half of Europe.

Personal fabrication devices, such as 3D printers and laser cutters, allow users to create custom physical objects. If you have never used these tools, you are welcome to write me an email and I give you an introduction (we also use both tools in our HCI2 bachelor's course).

In a traditional workflow, users sit at the computer and create a 3D model or a 2D drawing in a digital editor. This has several advantages, such as fast interaction, high precision, and the available undo functionality. After all editing is done, users print their digital model on one of the fabrication devices and get an actual physical object.

If you think about it, this workflow is quite different from how we operate a traditional woodworking tool, such as a saw or a wood chisel. When using a saw, we normally work directly on the physical workpiece and also see the physical shape changing after every interaction.

Interactive Laser Cutting

In my first project *constructable*, I wanted to reintroduce these qualities into personal fabrication. constructable is an interactive drafting table based on a laser cutter that allows users to once again work directly on the workpiece. Users draw through the safety glass enclosure using handheld laser pointers. We attached an overhead camera to the laser cutter to track the laser dot. When the user releases the laser pointer button, *constructable* immediately cuts the path.

I often get the question, how one can create a precise drawing if the hand wiggles all the time. In *constructable*, we solve this by using different laser pointer tools for different purposes. For instance, when I use the

polyline laser pointer all my lines will end up being straight. A different tool can be used for scaling, or for creating connection joints.

constructable is written in C++ and uses OpenCV for image processing, QT for the geometry handling, the CanonSDK for the camera control, and a library for controlling the laser cutter that we got directly from the laser cutter company. We also built some custom hardware for the laser pointer tool box.

Thanks to the amazing help of my student co-authors Konstantin Käfer and Bastian Kruck, who helped me with the implementation, we were able to live-demo *constructable* at two HCI conferences in Barcelona and Paris. Together we drove our HPI laser cutter more than 6 000 km in a van through half of Europe. With great success: our demo was definitely the most crowded one.

It is also great to see magazines such as the New Scientist, Wired Design, Gizmodo and Engadget writing articles about our project.

You probably already know my second project »LaserOrigami – Lasercutting 3D objects« from an email I sent to the student mail, so I will skip it here (thanks for the voting support!).

Fast 3D Printing using bricks

In December I got the notification, that my last project was accepted for the biggest HCI conference in Toronto. Together with Tobias Mohr, Kerstin Guenther, and Johannes Frohnhofen, I developed a system that allows users to prototype 3D objects quickly. The head mounted display you see on the picture normally takes 15 hours to 3D print. You can imagine how much Club Mate that takes until you have made three or four iterations. Our idea is to use 3D printing only where necessary and to replace the remaining parts with lego bricks. For instance, for the head mounted display you only need the lens mounts at the beginning to get the optical path right. So you only print those (takes 1 h). Later on you might also want to make more comfortable pieces for your forehead, so you can easily exchange the parts.

The software is written in Coffeescript and uses the CSG library for the 3D geometry operations. We also wrote a Blender Plugin for easy integration.

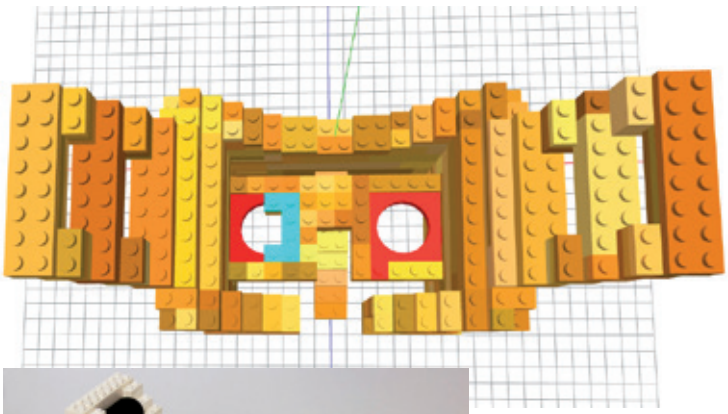
Currently, I am looking forward to demo the project with my co-authors for the 3 000 conference attendees in Toronto in May 2014.

We have a ton of new ideas for future projects in the pipeline, so if you are interested in working with me just write me an email or swing by my office (H-2.8).

– Stefanie Müller

Further information

HCI Lab:
→ www.hpi.uni-potsdam.de/baudisch
my personal page:
→ www.stefaniemueller.org



faBrickation

… saves 3D printing time by substituting sub-volumes with standard building blocks (in our case legos)

Lieblingsrezepte

des »Klub Kulinarisches«

กะหรีปับ

Thailändische Gerichte

mit persönlichen Anmerkungen von Jakob Jülich

ข้าวสวย

Hähnchencurry

Für 2 Personen

Zutaten:

- 1 EL Öl
- 1 EL selbst gemachte Currypaste oder 1 TL fertige Paste

Mae Ploy ist angeblich am besten

- 2 EL Fischsauce
- 150 ml Kokosmilch mit 100 ml Wasser

Statt 100 ml Wasser weitere 100 ml Kokosmilch ist je nach Geschmack noch besser.

- 1 TL Zucker
- ¼ Aubergine in Würfel geschnitten
- ½ Hähnchenbrust sehr klein geschnitten
- ¼ rote Chilischote klein gehackt
- 12 – 15 Thai-Basilikum Blätter

Italienisches Basilikum geht auch.

Öl in einem Topf erhitzen, von der Herdplatte nehmen, Currypaste dazugeben und kurz anschwitzen.

Nun die Pfanne wieder auf die Herdplatte stellen und die Fischsauce hinzufügen. Wenn diese verdampft ist, Kokosmilch dazugeben und zum Kochen bringen. Auberginen und Zucker hinzugeben.

Abgedeckt auf mittlerer Hitze köcheln lassen, bis das Gemüse bissfest ist.

Hähnchen dazugeben und abgedeckt 4 bis 6 Minuten – bis das Fleisch gerade so durch ist – kochen. Den Topf nun vom Herd nehmen. Chili und Basilikum dazu geben, servieren.

Die Zutaten hier kann man auch noch variieren: Statt des Hähnchens machen sich auch Shrimps gut. Als Gemüse passt so ziemlich alles, auch Kartoffeln.

Grüne Currypaste

Am besten Thai-Basilikum. Das schmeckt etwas nach Anis und ist im Asialaden erhältlich.

Zutaten:

- 2 Stängel Zitronengras
- 2 grüne Thai-Chili, in Scheiben geschnitten
- ½ Zwiebel, klein gehackt
- 4 – 5 Zehen Knoblauch
- 2 – 3 cm Galangal oder Ingwer, in dünnen Scheiben
- eine Handvoll Koriander (Blätter und Stiele)
- 12 Blätter frisches Basilikum
- ½ TL Kümmelpulver
- ½ TL Pfeffer
- ½ TL Koriandersaat
- 3 EL Fischsauce
  → *für Vegetarier: Sojasauce*
- 1 TL Shrimp-Paste
  → *für Vegetarier: schwarze Bohnen*
- 2 EL Limettensaft
- 3 – 4 EL Wasser
- 12 Kaffernlimettenblätter oder die Schale von zwei Limetten

Stinkt höllisch. Der Geruch ist leider normal.

Kaffernlimettenblätter sind ebenfalls im Asialaden erhältlich. Eventuell gibt es sie nur gefroren.

Alle Zutaten in der Küchenmaschine oder mit dem Mixer vermengen bis eine wohlriechende grüne Paste entsteht. Falls nötig, etwas mehr Wasser hinzugeben.

Salziger Geschmack kann mit einem Spritzer frischer Limette oder Zitronensaft ausgeglichen werden.

Es muss relativ scharf sein. Die Schärfe ist im fertigen Gericht weniger intensiv, als es zu diesem Zeitpunkt den Anschein erwecken mag.

Für 2 Personen

Garnelen in knusprigen Brotkrumen

Zutaten:

- 8 frische mittelgroße Garnelen
- ½ TL Grüne Currypaste (z. B. die selbst gemachte)
- 100 ml Milch
- 2 EL Fischsauce
- 1 Ei
- Mehl
- Panko Brotkrumen
- Rapsöl

Panko Brotkrumen:
Im Asialaden erhältliche, aus einem speziellen japanischen Brot hergestellte Semmelbrösel. Notfalls erfüllen normale Semmelbrösel den gleichen Zweck.

Ei, Milch, Currypaste und Fischsauce in einer Schüssel vermischen. Drei Teller bereitstellen: einen mit Brotkrumen, einen mit Mehl, einen mit dem aufgeschlagenen Ei. Nun die Garnelen erst im Mehl, dann im Ei wälzen. Abschließend mit den Brotkrumen panieren.

→ Optional nun nochmal ins Mehl, Ei und Brotkrumen: Doppelt paniert ist es noch besser.

Viel Öl nehmen, die Garnelen müssen fast schwimmen.

Danach Öl in einer Pfanne erhitzen und die Garnelen darin gold-braun braten. Zum Schluss die Garnelen auf Küchenpapier legen, damit überschüssiges Fett aufgesogen wird, und anschließend mit Salz bestreuen.

Das ganze schmeckt mit Thai-Sweet-Chili-Sauce besonders gut!

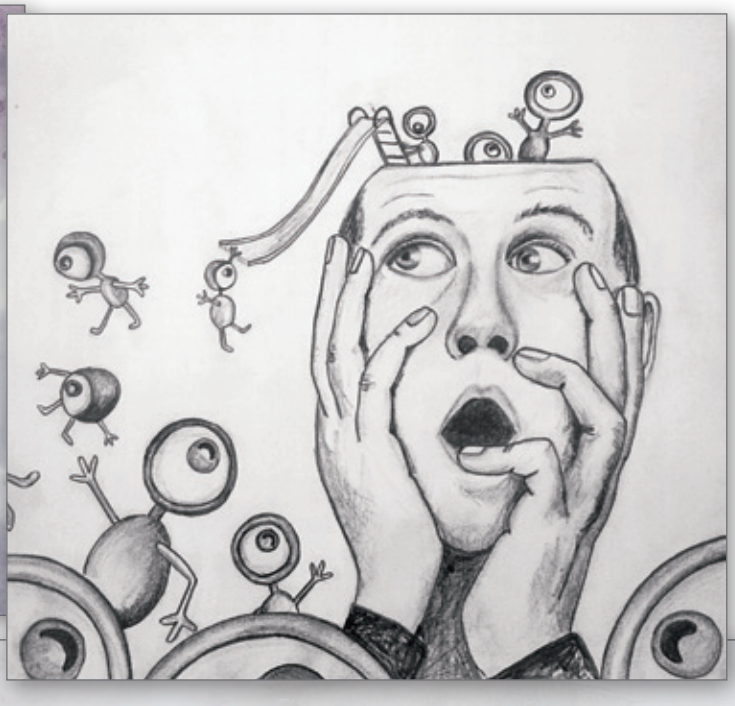
Lieblingsbilder des Kunstklubs

Auf den nächsten Seiten wollen wir euch den Kunstklub des HPI vorstellen. Wie könnte das besser gehen als mit den schönsten der in den letzten Jahren entstandenen Bildern. Regelmäßig treffen sich die Mitglieder des Klubs, um gemeinsam kreativ zu werden. Lasst euch also entführen und blickt in die Augen eines grasgrünen Frosches oder in die einer unbekannten Schönheit; bewundert Landschaften und Stillleben. Egal ob Öl, Aquarell oder Zeichnung, hier ist alles dabei. Viel Spaß beim Bewundern und Entdecken!

– *Julia Wachtel*

Die abgebildeten Werke sind von:

Yanina Yurchenko, Felix Niemeyer, Annett Seidler, Sharon Nemeth, Julia Steier, Katrin Honauer, Nicco Kunzmann, Kirstin Heidler, Juliane Waack, Rahiel Ghoraishi, Eva-Maria Herbst, Catharina Hahnfeld, Cathleen Ramson



Exportschlager HPI Research School

Kapstadt

Information and Communication Technologies for Development

Nanjing

Mass Data Analytics and Knowledge Discovery

Potsdam

Service-Oriented Systems Engineering

Haifa

Hasso Plattner Center for Scalable Computing

Vier Universitäten auf der ganzen Welt, ein gemeinsames Forschungskolleg – Die HPI Research Schools bieten PhD- und PostDoc-Stellen sowie Stipendien in Deutschland, Südafrika, Israel und China an. Insgesamt 14 Doktorinnen und Doktoren haben an den Research Schools erfolgreich promoviert, elf davon aus Potsdam, zwei aus Haifa, einer aus Kapstadt.

Unter dem Motto Service-Oriented Systems Engineering entstand das erste Forschungskolleg in Potsdam. 2007 wurde eine Zweigstelle in Kapstadt eröffnet, hier unter dem Thema Informations- und Telekommunikations-Technologien für Entwicklung. Drei Jahre später folgte das Technion in Haifa. Forschungschwerpunkt liegt dort bei Scalable Computing. Zuletzt eröffnete die HPI Research School at Nanjing University 2011. Das Thema der Studenten ist – passend zu der 5,4-Millionen Stadt – Mass Data Analytics and Knowledge Discovery.

Die verschiedenen Standorte sind mehr als nur Organisationen zur Doktoren- und Doktorandenausbildung mit HPI-Logo: Die Studenten profitieren von der Vernetzung der Fachgebiete und der Länder untereinander, es werden gemeinsame Symposien veranstaltet und Ergebnisse werden untereinander diskutiert.

Pedro Lopes, PhD-Student:
The research school […] provides a fantastic multidisciplinary environment where PhDs and Post-Docs interact with each other and share insights on their expertise. Looking at my own research […] one easily spots how other scientific knowledge plays a role here […] – this is exactly where the research school excels: at enabling us to network and collaborate with other PhD students within HPI and from the affiliated institutions in Cape Town, Haifa and Nanjing.

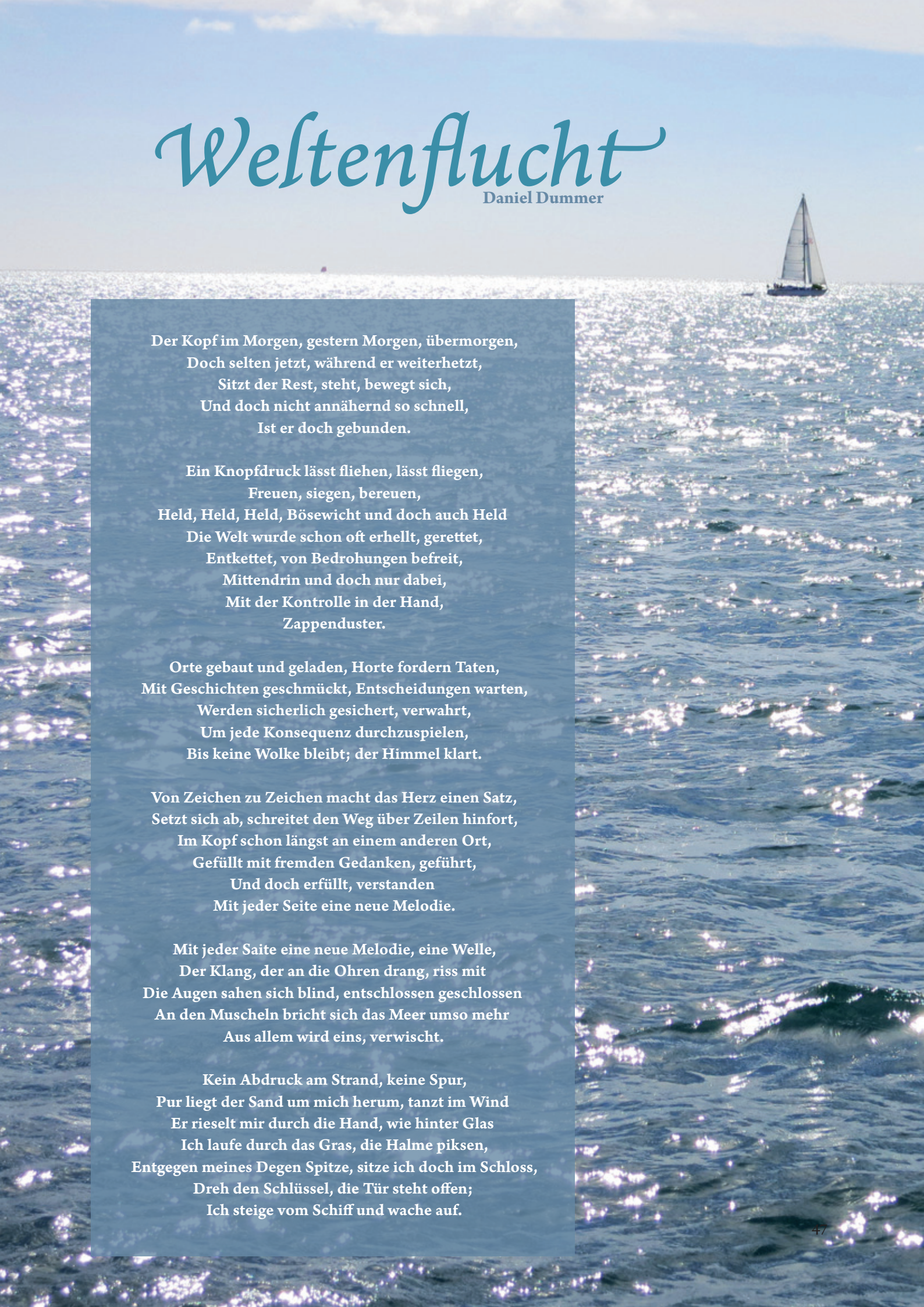
Fahad Khalid, PhD-Student:

You have a very narrow focus in your PhD. […] Because software is a complex entity [the exchange in the research schools helps you to] know the multiple aspects of software, like starting from the very low level things when it goes to hardware and then up to the business level abstraction and graphics. I think you have a much better grasp of the entire entity. […] One of the other things that the research school makes possible, is the freedom to actually branch out into a lot of different areas because you have more time and less responsibilities. That is something I really admire.

– Jonathan Striebel

Weltenflucht

Daniel Dummer



Der Kopf im Morgen, gestern Morgen, übermorgen,
Doch selten jetzt, während er weiterhetzt,
Sitzt der Rest, steht, bewegt sich,
Und doch nicht annähernd so schnell,
Ist er doch gebunden.

Ein Knopfdruck lässt fliehen, lässt fliegen,
Freuen, siegen, bereuen,
Held, Held, Held, Bösewicht und doch auch Held
Die Welt wurde schon oft erhellt, gerettet,
Entkettet, von Bedrohungen befreit,
Mittendrin und doch nur dabei,
Mit der Kontrolle in der Hand,
Zappenduster.

Orte gebaut und geladen, Horte fordern Taten,
Mit Geschichten geschmückt, Entscheidungen warten,
Werden sicherlich gesichert, verwahrt,
Um jede Konsequenz durchzuspielen,
Bis keine Wolke bleibt; der Himmel klart.

Von Zeichen zu Zeichen macht das Herz einen Satz,
Setzt sich ab, schreitet den Weg über Zeilen hinfort,
Im Kopf schon längst an einem anderen Ort,
Gefüllt mit fremden Gedanken, geführt,
Und doch erfüllt, verstanden
Mit jeder Seite eine neue Melodie.

Mit jeder Saite eine neue Melodie, eine Welle,
Der Klang, der an die Ohren drang, riss mit
Die Augen sahen sich blind, entschlossen geschlossen
An den Muscheln bricht sich das Meer umso mehr
Aus allem wird eins, verwischt.

Kein Abdruck am Strand, keine Spur,
Pur liegt der Sand um mich herum, tanzt im Wind
Er rieselt mir durch die Hand, wie hinter Glas
Ich laufe durch das Gras, die Halme piksen,
Entgegen meines Degen Spitze, sitze ich doch im Schloss,
Dreh den Schlüssel, die Tür steht offen;
Ich steige vom Schiff und wache auf.

Kurzgefasst

openHPI

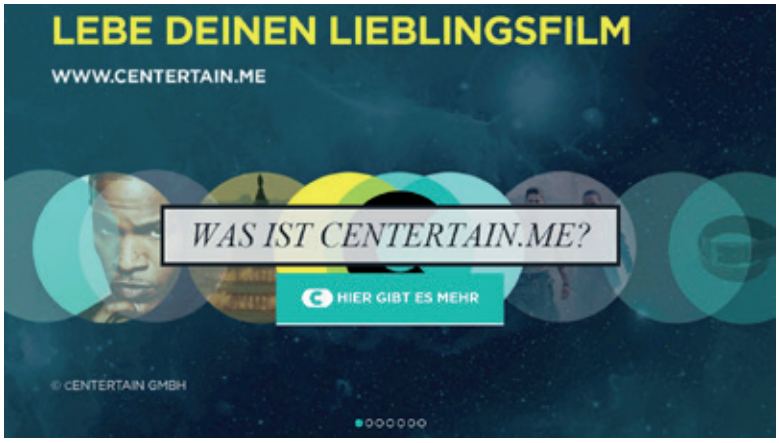
Die Plattform wird mittlerweile von rund 60 000 Nutzern aus 114 Ländern besucht.

Ausbau von openHPI

Nachdem die interaktive Bildungsplattform openhpi.de in ihrem ersten Jahr bereits großen internationalen Erfolg erzielt hat, baut das HPI sie nun weiter aus. So folgen den bereits bestehenden fünf Kursen im nächsten Jahren weitere fünf Onlinekurse, welche das HPI ebenfalls kostenlos anbietet. Neu eingebaute Extras, wie zum Beispiel die Integration von sozialen Netzwerken, machen die Massive Open Online Courses (MOOCs) noch attraktiver für Studenten. So erleichtern die Extras den Umgang mit dem openHPI-Diskussionsforum und fördern den persönlichen Kontakt zwischen den verschiedenen Teilnehmern des Kurses. Das HPI führt spielerische Elemente (»Gamification«) und Auszeichnungen etc. für Teilnehmer ein, um die Nutzeraktivität zu steigern. Zusätzlich beginnt man für die Lehrvideos Untertitel in verschiedenen Sprachen anzufertigen, um es Hörgeschädigten oder Studenten mit unzureichenden Sprachkenntnissen ebenfalls zu ermöglichen, an diesen Kursen teilzunehmen.

cENTERTAIN.ME

bietet die Möglichkeit, neue Filme auf Basis der eigenen Vorlieben zu entdecken.



Semantische Suchtechnologie

Bei der semantischen Suche wird der Text im Gegensatz zu Keyword-basierten Suchtechniken nicht nach dem Vorkommen eines bestimmten Wortes durchsucht, sondern die Bedeutung des Wortes ermittelt und anhand dessen Medien, Daten usw. mit ähnlichem Inhalt gesucht. Das Suchergebnis ist somit sehr präzise, da selbst Wörter mit unterschiedlichen Bedeutungen in den richtigen Zusammenhang gerückt werden.

Filme suchen – leicht wie nie

In Zusammenarbeit mit dem Potsdamer Start-up-Unternehmen cENTERTAIN.ME hat das Hasso-Plattner-Institut eine Website geschaffen, die Filme mittels semantischer Suche findet und ähnliche Filme vorschlägt.
Die Besonderheit hierbei ist jedoch, dass die Plattform alle Vorschläge nicht nach dem klassischen »Käufer dieses Films haben auch gesehen / gekauft …«-Prinzip ermittelt, sondern nach der Ähnlichkeit des Inhaltes. Im einfachsten Fall schlägt die Website lediglich Filme vor, die beispielsweise eine gleiche Regisseur-Schauspieler-Konstellation aufweisen. Sie achtet aber auch auf inhaltliche oder thematische Gemeinsamkeiten sowie auf Filme, die am gleichen Ort oder zur gleichen Zeit spielen, beziehungsweise sich mit gleichen Figuren oder Themen auseinandersetzen.

Des Weiteren ist das gesamte System Feedback-bezogen. Die Kunden können jede Empfehlung bewerten, wodurch das System lernt, welche davon die besten bzw. treffendsten sind. Um viele und möglichst aktuelle Randdaten zu dem Film bereitstellen zu können, verknüpft die Website verschiedene Datenquellen (z. B. Wikipedia, Filmdatenbanken etc.) miteinander.

Problemlösung des Cloud Computing

Das Hasso-Plattner-Institut hat im vergangenen Jahr ein Verfahren entwickelt, um einige Probleme des Cloud Computing zu beheben, wie zum Beispiel fehlende Datensicherheit oder Schwierigkeiten bei der Wiederherstellung von Daten. Wissenschaftler des HPIs entwickelten unter anderem ein System, das nicht wie bisher üblich alle zu speichernden Daten einem Anbieter von Speicherressourcen anvertraut, sondern diese Daten teilt, verschlüsselt und gleichmäßig an verschiedene Speicherdienste gibt. Dadurch werden Verfügbarkeit und Sicherheit der Daten erhöht. So können Daten einfacher wiederhergestellt werden und das Risiko des Datenmissbrauchs wird ebenso verringert. Das ganze System ähnelt dem RAID-Prinzip und wird deshalb auch als Cloud-RAID bezeichnet. Zusätzlich wurden weitere Verfahren veröffentlicht, die das Cloud Computing sicherer machen sollen sowie höhere Leistungen bei geringerem Energieverbrauch bewirken.

RAID
(Redundant Array of Independent Disks)

Ein RAID-System fasst mehrere physische Festplatten zu einem logischen Laufwerk zusammen und ermöglicht so eine höhere Verfügbarkeit der Daten, falls einzelne Festplatten ausfallen. Zudem erlaubt es einen größeren Datendurchsatz als ein physisches Laufwerk. Da die Informationen redundant gespeichert werden, kann man Daten wiederherstellen, auch wenn der Benutzer nicht auf alle Festplatten zugreifen kann.

HPI in Amerika

Studentinnen des HPIs haben auf der »Grace Hopper – Celebration of Women in Computing«-Messe in Minneapolis, Amerika vom 2. bis 5. Oktober 2013 das HPI vertreten. Die internationale Messe findet jährlich zu Ehren von Grace Hopper und für Frauen in der Informatik statt.

Bereits zum dritten Mal vertraten Informatikerinnen das HPI auf dieser Messe mit einem eigenen Stand. Das HPI informierte Besucher unter anderem über das openHPI, tele-TASK und tele-Board.

Unter dem Motto »Think Big, Drive Forward« versucht die Grace Hopper-Messe speziell junge Frauen für ein Informatikstudium zu begeistern. Mit über 4 750 Teilnehmern aus 53 Ländern und über 350 beteiligten Firmen ist es die weltgrößte Messe für Frauen in der Informatik.

– Maximilian Götz

Die Preisverleihung

Telle Whitney, President Anita Borg Insitute, (l.) und Alan Eustace von Google (r.) mit den drei Preisträgerinnen Shikoh Gitau, Unoma Okorafor und Violette Uwamutara (v. l. n. r.) des Change Agent ABIE Awards.

Special: Berufseinstieg

HPI Alumni berichten aus ihrem Job

Vielen Studierenden und Studieninteressierten ist nicht bewusst, welch vielfältige Berufsmöglichkeiten sich Ihnen nach einem Studium am HPI bieten. Um hier ein wenig Orientierung zu geben, haben wir HPI-Absolventen gebeten, uns aus ihrem derzeitigen Job zu berichten. Wir haben die Alumni gefragt, was ihre Aufgaben sind, was ihnen an ihrem Job gefällt und welche Anforderungen an Bewerber gestellt werden. Die folgenden drei Beispiele geben Einblick in mögliche berufliche Tätigkeiten nach einem ITSE-Abschluss – ob im großen Konzern oder kleinen Start-up, in der Rolle als Entwickler, Manager oder Berater … der Talentbedarf in der IT-Branche ist groß und wächst. Bei den schier unbegrenzten Möglichkeiten auf dem Arbeitsmarkt kann jeder das für sich Passende finden und sehr erfolgreich werden.

Christoph Mecklenburg

Beschreiben Sie kurz Ihren Job: Wo arbeiten Sie, in welcher Position, und was sind Ihre Aufgaben?

→ *Christoph Mecklenburg:* Als Product Manager bin ich für eine Reihe von Individual-Softwareanwendungen verantwortlich, die hauptsächlich für die Einkaufsprozesse (Bestellabwicklung, Lieferanten und Vertragsmanagement etc.) bei Zalando, der größten E-Commerce-Plattform Europas für Fashion, genutzt werden. Dazu gehören die Erhebung, Analyse und Verwaltung der Anforderungen verschiedener Fachbereiche (Einkauf, Accounting, Logistik, Business Intelligence). Diese übersetze ich in User Stories und definiere jeweilig die Akzeptanzkriterien, User Interfaces und Testszenarien. Die erstellten User Stories priorisiere ich im Product-Backlog und plane sie in einem wöchentlichen Zyklus für die jeweiligen Software-Releases ein. Während der Entwicklung stehe ich den Software Engineers und der Qualitätssicherung mit Rat und Tat zur Seite.

Name: Christoph Mecklenburg
Firma: Zalando GmbH, Berlin
Position: IT Product Manager
HPI-Abschluss und Jahr: M.Sc., 2012
Kontakt: *christoph.mecklenburg@gmail.com*

Was gefällt Ihnen an der Arbeit?

→ *Christoph Mecklenburg:* Besonders spannend ist es, als Vermittler und Übersetzer zwischen der fachlichen und technischen Welt zu fungieren und für fachliche Probleme kreative und benutzerfreundliche Softwarelösungen zu erarbeiten. Mich motiviert, dass ich während des gesamten Prozesses – von der Idee oder Identifikation des Problems bis zum Release entsprechender Lösungen –, beteiligt

bin und dabei Entwicklern sowie Product-Manager-Kollegen als Produktexperte zur Seite stehe.

Wie kommt man an einen solchen Job? Was sind die Anforderungen?

→ *Christoph Mecklenburg:* Hier ist man als Generalist mit einem breiten fachlichen und technischen Spektrum besonders gut aufgehoben. Als Produktmanager sollte man die fachlichen Probleme bis zum Kern verstehen wollen. Dies geht weit über das bloße Aufnehmen von Anforderungen hinaus. Denn häufig müssen die dahinterliegenden Ziele und Hintergründe erst identifiziert werden, um Lösungen mit echtem Mehrwert zu schaffen. Darüber hinaus sollte ein Produktmanager mit den Grundzügen nutzerorientierter Softwaregestaltung und Softwareentwicklungsmethoden vertraut sein und idealerweise Erfahrung in der Programmierung und im Testen von Software haben. Ein gewisses Kommunikationstalent und Selbstvertrauen sind auch sehr wichtig, da häufig Konflikte zwischen und mit Stakeholdern ausgetragen werden müssen. Dazu gehört es, auf der einen Seite als Moderator und Vermittler auftreten zu können, auf der anderen Seite aber auch mal »Nein« zu sagen. Um an einen solchen Job zu kommen, kann ich nur auf die entsprechenden Firmenauftritte im Web oder Jobportale verweisen, da der aktuelle Bedarf an Talenten groß genug ist, um auch ohne »Geheimtipp« Chancen auf eine solche Position zu bekommen.

Manuel Blechschmidt

Beschreiben Sie kurz Ihren Job: Wo arbeiten Sie, in welcher Position, und was sind Ihre Aufgaben?

→ *Manuel Blechschmidt:* Ich bin für die gesamte technische Entwicklung der Apaxo GmbH verantwortlich. Wir entwickeln ein skalierbares 1-zu-1-Marketingsystem, welches mit statistischen Verfahren eine optimale Kommunikation von Produkten vom Händler zum Endkunden gewährleistet. Meine konkreten Aufgaben sind das Sammeln von Anforderungen, das Entwickeln von Architektur in UML und FMC, das Steuern der Umsetzung in Java EE und das Testen der Anwendung. Weiterhin begleite ich einige nicht-technische Aufgaben, wie die Auswahl und die Entwicklung von Mitarbeitern und den Pre-Sales-Prozess. Bei unserem Partnerunternehmen mobizcorp bin ich zusätzlich als Projektleiter tätig und kann dort mit Teams aus 5 bis 15 Leuten Onlineshops für internationale Markenunternehmen mitentwickeln.

Name: Manuel Blechschmidt
Firma: Apaxo GmbH & mobizcorp europe Ltd.
Position: CTO & Projektleiter
HPI-Abschluss und Jahr: M.Sc., 2011
Kontakt: *blechschmidt@apaxo.de*

Was gefällt Ihnen an der Arbeit?

→ *Manuel Blechschmidt:* Ich kann mir meine Zeit frei einteilen und wichtige Entscheidungen treffen. Ich habe die Chance, etwas nachhaltig zu verändern und zu zeigen, dass die Ausbildung am HPI einem die Möglichkeit gibt, Dinge zu entwickeln, die besser als der bisherige Standard sind. Ich habe viel Kontakt zu Kunden und kann mein Team weiterbilden.

Wie kommt man an einen solchen Job? Was sind die Anforderungen?

→ *Manuel Blechschmidt:* Ich habe früh angefangen, Onlineshops zu entwickeln und mein persönliches Netzwerk aufzubauen. Technisch braucht man vor allem den Blick fürs Große, Ehrgeiz und die ständige Bereitschaft für Verbesserungen. Das »Not-Invented-Here-Syndrom« ist hinderlich und man sollte Vertrauen in Produkte Dritter entwickeln. Ich war in verschiedenen Organisationen innerhalb und außerhalb der Universität aktiv. Parallel dazu habe ich sehr aktiv am Start-up-Geschehen in Berlin teilgenommen. Ich habe kontinuierlich Kontakte zu Investoren gepflegt.

Jonas Gebhardt

Beschreiben Sie kurz Ihren Job: Wo arbeiten Sie, in welcher Position, und was sind Ihre Aufgaben?

→ *Jonas Gebhardt:* Ich bin bei Facebook in Menlo Park, Kalifornien als UI Engineer angestellt und arbeite hier primär an Instagrams Web-Frontend. Dazu gehören neben instagram.com auch diverse Webviews in den nativen Apps für iOS, Android und Windows Phone. Meine Arbeit ist in erster Linie Produkt(weiter)entwicklung mittels JavaScript, Node.js und Django / Python.

Was gefällt Ihnen an der Arbeit?

→ *Jonas Gebhardt:* Die Arbeit ist vielfältig und temporeich. Facebooks Motto »move fast and be bold« wird im relativ kleinen Instagram-Team erst recht umgesetzt (in anderen Facebook-Teams natürlich auch). Im Instagram Web-Team sind wir zu dritt – jeder hat also großen Einfluss. Instagram hat aktuell 150 Millionen Nutzer und neue Features werden demnach in kurzer Zeit von Millionen Menschen benutzt. Das ist faszinierend und gleichzeitig motivierend, denn wir sind immer bestrebt, ein möglichst gutes Nutzererlebnis zu bieten. Zwei weitere Mottos bei Facebook sind »Code wins arguments« und

Name: Jonas Gebhardt
Firma: Facebook, Menlo Park, USA
Position: Frontend Engineer
HPI-Abschluss und Jahr: B.Sc., 2011
Kontakt: *jonas.gebhardt@gmail.com*

»Nothing at Facebook is somebody else's problem« – Ingenieurskultur steht auf der Tagesordnung und Offenheit wird großgeschrieben. So bekommt jeder neue Mitarbeiter am ersten Tag Zugriff auf die gesamte Codebasis und es wird gern gesehen, wenn man anpackt und ein Problem direkt löst, anstatt nur darüber zu diskutieren. Wir arbeiten zudem viel mit Open-Source-Software und mehrere tägliche Releases erlauben ein sehr zügiges und effizientes Arbeiten.

Wie kommt man an einen solchen Job? Was sind die Anforderungen?

→ *Jonas Gebhardt:* Neben sehr guten Programmierfähigkeiten sollte ein neuer Frontend Engineer ein tiefes Verständnis von JavaScript, CSS und Webprogrammierung mitbringen. Praktikums- und Projekterfahrung außerhalb der Uni sind ebenfalls hilfreich. Ich selbst habe nach dem HPI ein Masterstudium in HCI absolviert. Ich denke, HPI-Master- sowie Bachelorstudenten mit guten Englischkenntnissen sollten keine großen Probleme haben, ein Interview zu bekommen. Das Bewerbungsverfahren besteht in der Regel aus mehrstufigen Interviews sowie einer Coding Challenge. Zudem bietet Facebook, wie viele US-Tech-Firmen, dreimonatige Praktika für Studenten an.* In den ersten sechs Wochen absolviert jeder Facebook-Neueinsteiger das sogenannte »Bootcamp«, mit dem Ziel, die verschiedenen Teile der Codebasis kennenzulernen. Je nach Qualifikation und persönlichem Interesse findet dann in Zusammenarbeit mit Managern interessierter Teams die Teamauswahl statt.

**HPI-Studenten mit generellem Interesse an Auslandspraktika in den USA kann ich nur empfehlen, sich auf den Jobseiten von Techfirmen umzuschauen. Neben dem HPI-hauseigenen SAP-Praktikum gibt es immens viele Möglichkeiten, an ein selbstorganisiertes Praktikum zu kommen. Viele Tech-Firmen in San Francisco und dem Silicon Valley, aber auch in New York, Seattle, Austin und anderen großen Städten sind ständig auf der Suche nach Praktikanten und Absolventen. Größere Firmen übernehmen in der Regel einen Großteil der Visum-, Reise- und Lebenshaltungskosten. Falls Ihr Fragen habt, schreibt mir einfach: jonas.gebhardt@gmail.com.*

Konzept und Redaktion
Nadja Antoine und Claudia Koch

Lust auf mehr?

Demnächst findet Ihr weitere spannende Karriereberichte von HPI-Alumni auch online auf einer neuen Plattform – wir informieren euch, wenn der Startschuss fällt!

Save the Date

Die nächste Gelegenheit, potentielle Arbeitgeber kennenzulernen, gibt es auf der HPI Connect 2014 am 15. Mai: *http://www.hpi.uni-potsdam.de/hpi/veranstaltungen/hpi_connect.html*

Hacks@MIT

Aren't hackers the people that break into computer networks?

Maybe to the rest of the world.

Many of us at MIT call those who break into (crack) computer systems »crackers«. At MIT, a »hacker« is someone who does some sort of interesting and creative work at a high intensity level.

[from FAQ at hacks.mit.edu]

Stellt euch vor, ihr kommt eines Morgens ins HPI und entdeckt, dass unzählige Papierschiffchen auf dem Lake HPI schwimmen, Mr. Net plötzlich Klamotten trägt oder das Foyer im Haupthaus komplett mit Post-its beklebt ist. Die Welt des grauen Studienalltags würde auf einen Schlag bunter!

Aktionen wie diese denken sich Studenten (und angeblich auch einige der Dozenten) in unregelmäßigen Abständen am Massachusetts Institute of Technology in Cambridge aus und zögern nicht, diese dann auch direkt auf ihrem Campus umzusetzen. In der langen Geschichte des MITs gab es schon einige sogenannte »Hacks«: Von einem Polizeiauto, das über Nacht auf dem Hauptgebäude der Elite-Uni auftauchte, bis hin zu abwechselnd erleuchteten Fenstern auf einem Hochhaus, die ein Tetris-Spiel simulierten, war bis jetzt alles dabei.

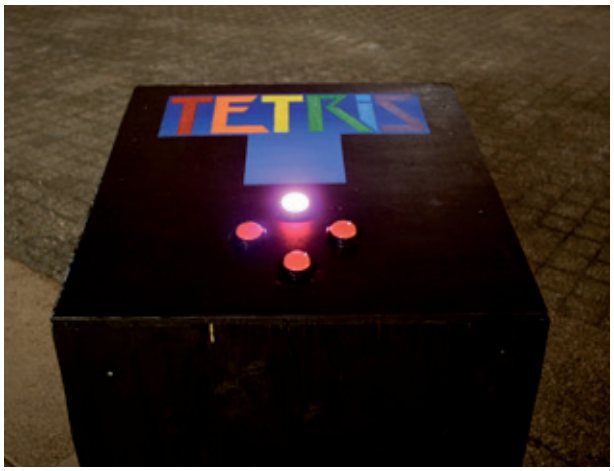
Alle diese »Hacks« sollen amüsieren und oftmals gleichzeitig die technische Gewandtheit der »Hacker« demonstrieren. Die Beteiligten agieren immer anonym und meistens über Nacht; manchmal allein, manchmal in Gruppen organisiert. Nur selten stellen sich die »Hacker« im Nachhinein der Öffentlichkeit. Bestrafungen für diese gibt es selten, denn der Großteil der »Hacks« bewegt sich im Rahmen der Hausordnung.

Offiziell dokumentiert werden die Aktionen seit dem Jahr 1989. Doch auch schon davor gab es eine Reihe von außergewöhnlichen Ereignissen auf dem Campus. Die »Hacks« gehören zur Tradition und Studentenkultur des berühmten Instituts.

Eine der ersten Aktionen bestand aus einem riesigen Wetterballon mit MIT-Logo, der plötzlich während eines Footballspiels gegen den Konkurrenten Harvard auf der Mitte des Spielfeldes aufgeblasen wurde. Diese Spiele wurden seitdem öfter von den »Hackern« genutzt. So wurde zum Beispiel

Spieleklassiker auf Riesendisplay

Das interaktive Tetrisspiel auf dem »Green Building« gehört zu den bekanntesten der »Hacks«. Eine komplette Liste findet ihr unter: *hacks.mit.edu*



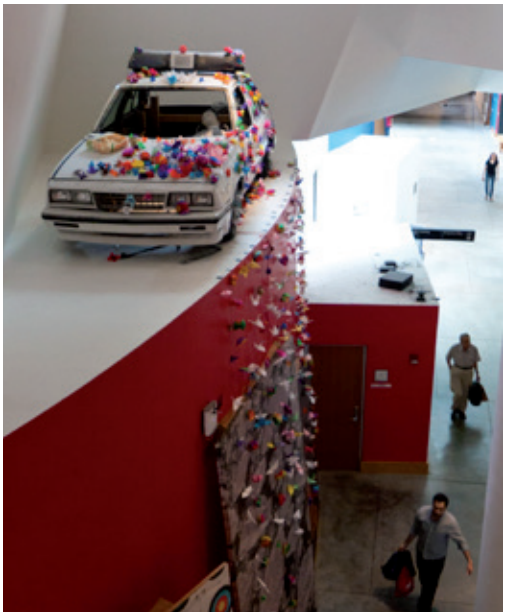
1996 die Anzeigetafel des Stadions (im wirklichen Sinne des Wortes) gehackt und das Logo der Harvard-University verändert. Anstatt VE-RI-TAS konnten die Zuschauer nun HU-GE-EGO lesen.

Das riesige Tetris-Spiel auf dem »Green Building« auf dem MIT-Campus gehört zu den bekanntesten Aktionen in der Geschichte der MIT-Hacks. Zuerst wurde es im September 2011 aufgebaut. Damals zeigte die Installation allerdings einige Aussetzer und wurde einige Tage später wieder entfernt. Die Idee war aber beliebt und wurde daher 2012 erneut aufgenommen, diesmal mit verbesserter Soft- und Hardware. So war es möglich, dass Studenten interaktiv das Spiel steuern konnten. Das Display wurde als zweitgrößtes vollfarbiges Video-Display in den USA gefeiert.

Am MIT wird seit vielen Jahren die Abkürzung IHTFP in mehreren Zusammenhängen als eine Art Insider verwendet. Dieses Akronym kennzeichnet auch die »Hacks«. So trug beispielsweise das Polizeiauto, welches im Mai 1994 eines Morgens auf dem Dach des »Great Domes« der Uni stand, diese Buchstabenfolge auf der Plakette. Ursprünglich stand IHTFP für »I Hate This Fucking Place«. Dies fanden viele Studenten jedoch bald zu derb und profan. Sie erfanden neue Bedeutungen wie »I Have The Fucking Power« (im Bezug auf das Hacking), »I Help Tutor Freshman Physics«, »It's Hard To Fondle Penguins«, »I'm Hankering To Find Paradise« und »Interesting Hacks To Fascinate People«. Diese Liste könnte endlos ergänzt werden.

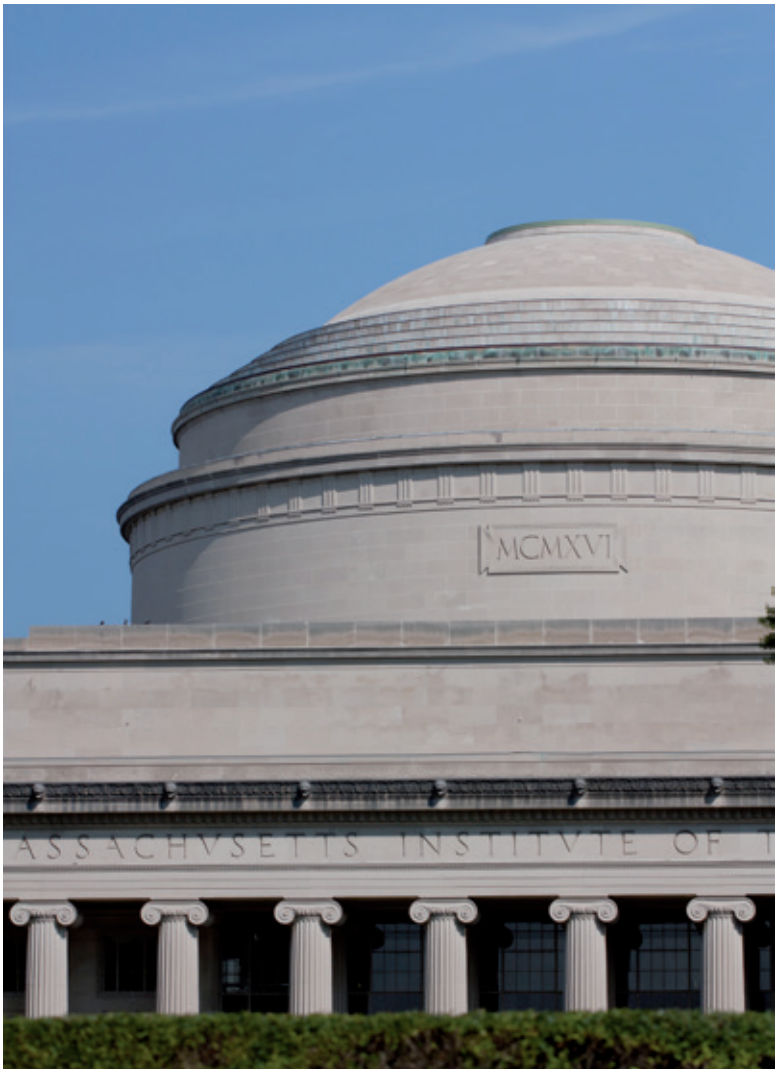
Die letzte größere, auf der Website der »Hacks« dokumentierte Aktion fand im Januar 2013 statt. Am Abend des 10. Januars erschienen Pac-Man und sein Gegenspieler, der Geist Blinky, auf einem Transparent an einem Baugerüst, oben auf dem bekanntesten Gebäude der Uni, dem »Great Dome«.

– Julia Wachtel



Der »Great Dome«

Diesen Sommer befand sich in einem der Unigebäude eine Ausstellung zu den »Hacks«. Hier sieht man das Polizeiauto, welches über Nacht auf das Dach des »Great Domes« gestellt wurde. Das wohl bekannteste Gebäude des MITs war immer wieder Ziel für verschiedene Hacks.



Unaufdringliche Bauklotz-Eleganz

Das neue Drittmittelgebäude scheidet die Geister – ein höchst unsachliches und nicht ganz ernst gemeintes Streitgespräch.

Du sag mal, dieses neue Drittmittelgebäude der Uni auf dem Campus Griebnitzsee … das kann doch nicht so gewollt sein, oder?

Mir gefällt das echt gut. Das hat etwas Eigenes. In so einem Gebäude würde ich auch wohnen.

In so einem Gebäude wohnt man nicht, da wird man höchstens festgehalten. Inhaftiert. Wie ein Gefängnis sieht das doch aus. Da fehlen nur noch Gitterstäbe vor den Fenstern.

Du beziehst dich hier ja nur auf Äußerlichkeiten. Auch so ein Gebäude hat doch innere Werte. Zumal ich diese Fenster eigentlich ziemlich schick finde, so schön nach außen gewölbt.

Ja, weil die Insassen raus wollen.

Ach komm. Schau dir mal das Portfolio der Architekten an. Ich muss sagen, die haben echt einen guten Stil.

Bloß weil man auch schön bauen kann …

Na immerhin, jetzt gibst du ja schon zu, dass sie schön bauen können.

… ist das noch lange keine Ausrede, es nicht zu tun.

Ach, vielleicht ist es auf den ersten Blick nicht so schön wie die anderen. Aber es hat doch auch Symbolik. Dieses Gebäude ist wie die Wissenschaft, die darin gelebt wird: es gibt nicht immer nur klare Wege, die man verfolgen kann. Da kommen Ecken und Kanten.

Na immerhin, jetzt gibst du ja schon zu, dass es nicht so schön ist.

Jedenfalls ist das ganz sicher kein Zufall, dass die Architekten so ein riesiges Portfolio angesammelt haben.

Ja, sieht mir auch eher nach Masse als nach Klasse aus. Vielleicht hatten die vor lauter Portfolio gar keinen Platz im Auftragsbuch und haben das die Praktikanten machen lassen. Oder die Kinder. Ja, das könnte es sein. Solche Bauklotzstrukturen kenne ich sonst eigentlich nur von Kindern. Ein Architekturkonzept, dessen herausragendes Merkmal ein Knick in der Wand ist, ist keins.

Findest du nicht auch, dass die halboffenen Fenster schön verdeutlichen, wie die Wissenschaft aus dem Gebäude geradezu herausquillt? Wie das Wissen kaum zurückzuhalten ist, trotz der verstärkten Fenster.

Sicher.

Dieses Gebäude ist das pulsierende Zentrum des Campus.

Jetzt geht's aber los. Das Einzige, was hier pulsiert, sind die Adern an meinen Schläfen, wenn ich dieses Haus erblicke. Was sollen denn bitte diese bunt zusammengewürfelten Farben? Quietschgelbe Türen, hallo? Da passt nichts zusammen, nicht mit der Umgebung und auch nicht mit sich selbst.

Das sind alles gedeckte Farben. Schließlich will das neue Haus trotz der guten Lage nicht im Mittelpunkt stehen, sondern hält sich im Hintergrund. Dezent. Und reif. Und außerdem: Jede Seite ist unterschiedlich. Das Gebäude spiegelt so die Vielfalt und Ausdruckskraft der vielen Lebenswelten und der bunten Geschichte wieder, die hier aufeinandertreffen. Wunderschön!

Wenn man es lange genug versucht, kann man alles schön reden. Ist es nicht wunderbar vielsagend, dass auf der Webseite der Architekten nur ein verdächtig kleiner Ausschnitt der Fassade gezeigt wird? Stolz sieht anders aus.

Ich finde, da braucht sich niemand zu verstecken. Dieses Haus setzt neue Impulse im Zentrum des Uni-Campus. Es ist wie ein rotes Tuch, das die anderen Gebäude herausfordert und wachrüttelt. Und zugleich besticht die Architektur durch ihre Einfachheit und die unaufdringliche Eleganz. Dieses Haus ist auch nicht langweilig, es erschließt sich nach und nach. Und deswegen finde ich, die Architekten haben ganze Arbeit geleistet.

Auf dem Schulzeugnis würde trotzdem nur stehen: Das kleine Drittmittelgebäude hat sich bemüht, den hohen Anforderungen gerecht zu werden.

Du bist halt ein Kunstbanause.

Weißt du, genau das ist mein Problem mit diesem Gebäude. Ich finde, Architektur sollte künstlerischen Wert besitzen und nicht etwas sein, was jedes Kind da so unförmig hingestellt hätte. Das muss doch auch ästhetisch sein!

Das ist eben nicht so, dass da jedes Kind so etwas hinstellen könnte.

Stimmt, jedes Kind hätte etwas Schöneres gebaut.

Oh, diese Arroganz! Viele Menschen meinen auch, Picassos Bilder könnte doch jeder zeichnen. Nur macht es nie jemand. Kunstbanausen!

Ich habe jedenfalls noch nie eine ideenärmere Fassadengestaltung gesehen.

Das finde ich jetzt ein bisschen übertrieben. Du warst doch schon mal in Ostberlin.

Ha, guter Vergleich! Gerade von der Ästhetik her sehr treffend.

Das war eine Abgrenzung, kein Vergleich. Und so was kann sich doch sehen lassen im Portfolio. Nach all den anderen Weltstädten, in denen sie gebaut haben, jetzt auch mal was in Potsdam vorweisen zu können, das war jetzt mal dran.

Es fügt sich auf jeden Fall gut in das so herrlich inkonsistente Potsdamer Stadtbild ein. Aber man muss ja auch an die zukünftigen Generationen denken.

Genau. Das ist der Stil der Zukunft, da bin ich mir sicher.

Und im Zweifel müssen die ja auch irgendwas zum Abreißen haben.

– Cornelius Bock, David Heller und Franz Liedke

Gute Hacker, böse Hacker

Stillos im großen Stil – ein Kommentar

Was haben Kernspaltung und Informatik gemeinsam? Wie so oft in der Technologie liegt die Antwort in der Wichtigkeit von verantwortungsvollem Umgang mit Talenten und Möglichkeiten.

Denn so ungeheuer faszinierend die Technik auch ist, so furchteinflößend kann ihre Macht wirken: Im Cyberwar werden ganze Infrastrukturen auf einen Schlag lahmgelegt, Drohnen bringen den automatisierten Tod und die Bevölkerung wird im großen Stil überwacht.

Wie schon Spiderman uns lehrte: Große Macht bringt große Verantwortung mit sich. Dieser Verantwortung hat sich vor allem eine Großmacht im letzten Jahr konsequent entzogen. Kaum eine Woche verging seit Juni 2013, ohne dass neue Enthüllungen über die unglaublichen Machenschaften des US-Geheimdienstes NSA durch die Zeitungen geisterten; verbunden mit der Frage, was für den ebenso gigantischen wie undurchsichtigen Schnüfflerapparat möglich ist. Vergleiche mit unbeliebten Staatsdiensten der deutschen Vergangenheit drängten sich auf, doch die Dimensionen sind längst andere.

Das Streben nach der Überwachung aller Menschen ist nicht neu und war schon Stoff zahlreicher Science-Fiction-Utopien. Doch nun ist eine Zeit erreicht, in der die Realität erstmals diesen Visionen nahe kommt. Nicht nur machbar, sondern gleich wünschenswert ist das für die NSA. Offen enthüllt sie diese Ansprüche – scheinbar völlig skrupellos.

Die Affäre zeigt wieder einmal: der Zorn des Wutbürgers ist schnell entbrannt, aber ebenso zügig ist er wieder vergessen. Für Veränderungen, die angesichts der machtlosen Lokalpolitik nötig wären, ist man zu träge. Verantwortung durch gemäßigten Gebrauch und Konsum ist den Benutzern nicht zuzutrauen. Zu groß sind die Verlockungen und der Komfort der schönen digitalen Welt. Die Cloud ist längst so real wie allgegenwärtig. Von Dropbox über das Google-Universum und Flickr bis hin zu Facebook – überall liegen unsere Daten: verstreut über die ganze Welt, immer da und doch nirgendwo. Selbstredend abgese-

hen vom zentralen Backup bei der NSA.

Was also tun? Ist hier Umdenken angebracht? Weg von zentralen Datensilos, hin zu Diensten, die einfach nur die privat gespeicherten Daten der Nutzer transportieren und verarbeiten? Eine Vision, die sicherlich näher an den ursprünglichen Idealen des »Open Web« liegt als die heutige Vorstellung von einer Cloud.

Richten müssen das die Informatiker. Wo heute Termine den Weg auf Googles Datenkontore finden, Dateien bei Dropbox abgelegt werden und Musik der Sammlung von Apple hinzugefügt wird, müssen also in Zukunft eigene Server her. Doch wie verknüpft man die Einfachheit von zentralisierten Services wie Dropbox mit der Kontrolle über die eigenen Daten?

An Problemen und Aufgabenstellungen mangelt es nicht. An Jobs ebenso wenig. Rosige Aussichten also, wenn es nur um Arbeitsplätze geht. Im Zweifel sucht ja auch die NSA ganz sicher immer Personal. Doch, um es mit Terry Pratchett zu sagen: »Wer bewacht die Wächter?« Dem riesigen Apparat auf die Finger zu schauen, ist sicherlich nicht so einfach. Aber vielleicht ist der Eine oder die Andere ja erpicht darauf, den umtriebigen Amis ihre Arbeit so schwer wie möglich zu machen. Die IT hat sich ohnehin in sämtlichen Branchen und Sparten breitgemacht, das Spektum reicht natürlich auch von gut bis böse. Wo findet man die alten Kommilitonen also demnächst wieder?

Muss ich damit rechnen, dass mich mein harmlos neben mir sitzender Pair-Programming-Partner in einigen Jahren genauso bei der Arbeit beobachten wird, allerdings ohne mein Wissen und Zutun? Das alles aus dem gemütlichen Ledersessel seines geheizten NSA-Büros heraus, während ich nichtsahnend meinen neuesten revolutionären Forschungsergebnissen den letzten Feinschliff verpasse? Werden ehemalige SWT-Dreamteams perfekt konzertierte Angriffe auf iranische Atomprogramme ausführen? Werden sich Ex-Studenten an ihren Tutoren rächen, indem sie deren Computer zu ferngesteuerten Robotern machen?

Wie kommt man einem Geheimdienst bei, der auch nicht davor zurückschreckt, Schwachstellen in scheinbar sicheren Verschlüsselungsalgorithmen einzuschleusen? Selbst dort haben die findigen Menschenrechtsverletzer ihre Finger im Spiel und manipulieren so gut sie nur können.

Und überhaupt, macht man sich dabei nicht unbeliebt? Befördert man sich so mit der eigenen Berufs- und Projektwahl direkt auf die schwarze Liste, wird zum Staatsfeind der Weltmacht Nummer eins?

Denn wer kennt das nicht? Eben mal aus Versehen einen genialen neuen Verschlüsselungsalgorithmus entworfen, und schon hetzen Sonderkommandos der selbsternannten Weltwächter hinter einem her.

Hätte ich doch lieber BWL studiert …

– Franz Liedke

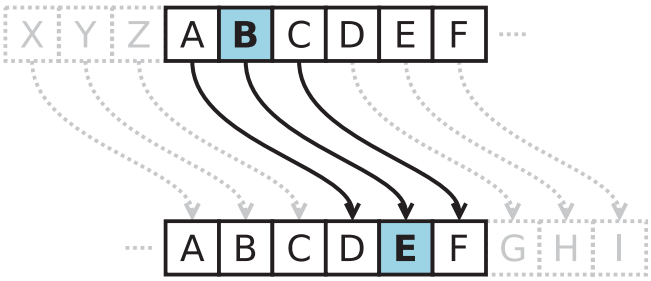
Moderne Verschlüsselungen

Verschlüsselte Hieroglyphen

Pflanze, Heuschrecke und Stoff sind Hieroglyphen, die in einigen religiösen Inschriften auftraten und vereinzelt die Lesung für Uneingeweihte erschweren sollten.

Die Kunst, eine Botschaft durch gezieltes »Verschleiern« für Fremde unkenntlich zu machen, ist fast so alt wie Schrift selbst. Schon die alten Ägypter setzten vor fünf Jahrtausenden spezielle Hieroglyphen ein, die nur einem ausgewählten Zirkel Geistlicher bekannt waren.

Um die Vertraulichkeit militärischer Korrespondenz zu wahren, setzte der römische Feldherr Gaius Julius Caesar laut Überlieferung die später nach ihm benannte Caesar-Chiffre ein: Dabei wurde jeder Buchstabe des Alphabets durch den um drei Positionen weiter hinten liegenden ersetzt.



Mit der Erfindung der Chiffrierscheibe im 15. Jahrhundert waren auch andere Verschiebungen als jene um drei Positionen trivial zu realisieren. Das Verfahren wurde verallgemeinert, Sender und Empfänger mussten sich nunmehr nur noch auf die Weite der Verschiebung einigen – einen *Schlüssel*. Das Prinzip der Trennung von Algorithmus und Schlüssel wird bis heute praktiziert.

Caesars Blockchiffre

Die klassische Caesar-Chiffre operiert nur über einzelnen Buchstaben als »Eingabe«, was sie anfällig für Muster im Text macht. Der Buchstabe E tritt meist am häufigsten auf, daher wird in einem um drei verschobenen Alphabet der Buchstabe H der häufigste sein. Über diese Korrelation lässt sich der Schlüssel schnell ermitteln.

Betrachtet man hingegen mehrere Buchstaben gleichzeitig – quasi ein Alphabet aus 26×26 Zeichen – und ersetzt sie durch die gleiche Anzahl Geheimbuchstaben, werden Korrelationen undeutlicher. Doch eine solche Übersetzungstabelle hätte bereits 676 Einträge.

```
AA | AB | AC | . . . | BA | BB | . . . | ZY | ZZ
RP | RQ | RR | . . . | SP | SQ | . . . | RN | RO
```

Für größere »Blöcke« zusammenhängender Daten ist also eher eine mathematische Beschreibung nützlich als eine Chiffrierscheibe oder Tabelle. Weisen wir also den Buchstaben A–Z die Zahlen 0 bis 25 zu. Die Caesar-Chiffe lässt sich dann einfach als Addition mit einem Schlüssel modulo 26 ausdrücken: $C = P + K \pmod{26}$. C, der verschlüsselte Buchstabe, wird als *Ciphertext* bezeichnet, der Buchstabe der ursprünglichen Nachricht P als *Plaintext* und die Verschiebung K als *Schlüssel (Key)*.

Was spricht also dagegen, 256 im Speicher liegende Bits auf einmal zu nehmen (das entspricht 32 Zeichen in ASCII-Codierung) und eine große Addition modulo 2^{256} mit einem möglichst zufälligen Schlüssel auszuführen? Zunächst nichts, alle 2^{256} Schlüssel auszuprobieren ist momentan technisch ausgeschlossen, das ist ein Fortschritt gegenüber den 26 Schlüsseln bei Caesar.

Das Problem hierbei ist nur, dass bei Kenntnis von Plaintext und Ciphertext der Schlüssel trivial via $K = C - P \pmod{2^{256}}$ gewonnen und zum Entschlüsseln anderer, eventuell unbekannter Blöcke eingesetzt werden kann.

Blockchiffren im 21. Jahrhundert

Um den Fallstricken der einfachen Addition zu entgehen, ist die Verwendung weiterer Operationen notwendig.

Häufige Operationen

```
Addition:
   1100 + 0101 = 0001 (modulo 2⁴)
Subtraktion:
   1100 – 0101 = 0111 (modulo 2⁴)
Exklusiv-Oder:
   1100 XOR 0101 = 1001
Linksrotation:
   00001100 <<< 3 = 01100000
Rechtsrotation:
   00001100 >>> 3 = 10000001
```

Diese werden nicht nur zwischen Schlüssel und Plaintext angewendet, sondern auch zwischen verschiedenen Teilen des Plaintexts selbst. Beispielsweise kann ein 256-Bit-Block auch als vier einzelne 64-Bit-Blöcke A, B, C und D betrachtet werden, die untereinander verknüpft werden, um die Ausgabeblöcke A', B', C' und D' zu erhalten:

Möglichkeit für die Verknüpfung der Ausgabeblöcke

```
A' = A + B  (modulo 2⁶⁴)
C' = C + D  (modulo 2⁶⁴)
B' = (D <<< 37) XOR C'
D' = (B <<<  5) XOR A'
```

Im *Threefish-Algorithmus* wird diese mathematische Transformation 72-mal hintereinander ausgeführt. Dabei werden stets andere Rotationsweiten als nur 37 und 5 verwendet. Alle vier Durchläufe wird ein sog. *Rundenschlüssel* auf den gesamten 256-Bit-Block addiert. Es ist zu erkennen, dass 72 / 4 = 18 Rundenschlüssel benötigt werden. Diese müssen daher durch mathematische Tricks aus

Chiffrierscheibe

Mit der Chiffrierscheibe kam das noch heute gültige Prinzip der Trennung von Algorithmus und Schlüssel.

einem einzigen 256-Bit breiten Schlüsselblock gewonnen werden – dieses Verfahren wird als *Schlüsselexpansion* bezeichnet und kann bisweilen komplizierter sein als die eigentliche Verschlüsselung.

Ziel dieses aufwändigen Durchwürfelns von Bits ist es, jeglichen Zusammenhang zwischen Plaintext, Schlüssel und Ciphertext zu verschleiern. Würde auch nur ein einziges Bit im Plaintext oder im Schlüssel verändert, entstünde ein völlig anderer, unvorhersagbarer Ciphertext. Dieser Effekt heißt *Diffusion*. Und doch ist all dies umkehrbar, wenn die Rundenschlüssel bekannt sind: Aus Addition wird Subtraktion, Linksrotation wird zu Rechtsrotation, XOR bleibt bestehen und alle Operationen werden in umgekehrter Reihenfolge angewendet, die Rundenschlüssel in umgekehrter Reihenfolge alle vier Runden subtrahiert – die Umkehroperation der oben dargestellten Transformation sei dem Leser überlassen.

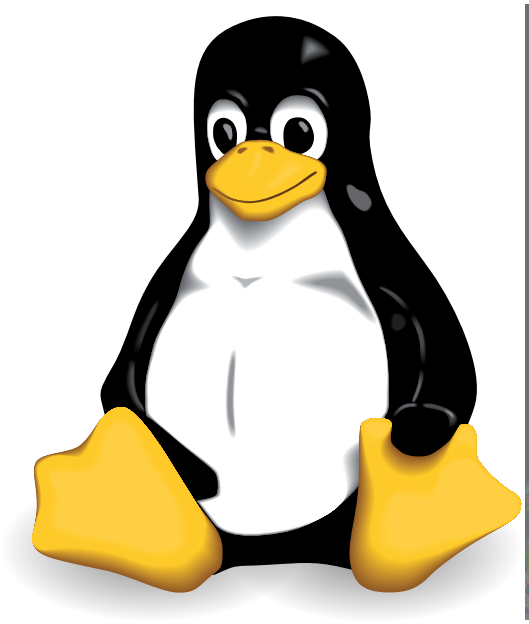
Sicherheitsaspekte bei der Implementierung

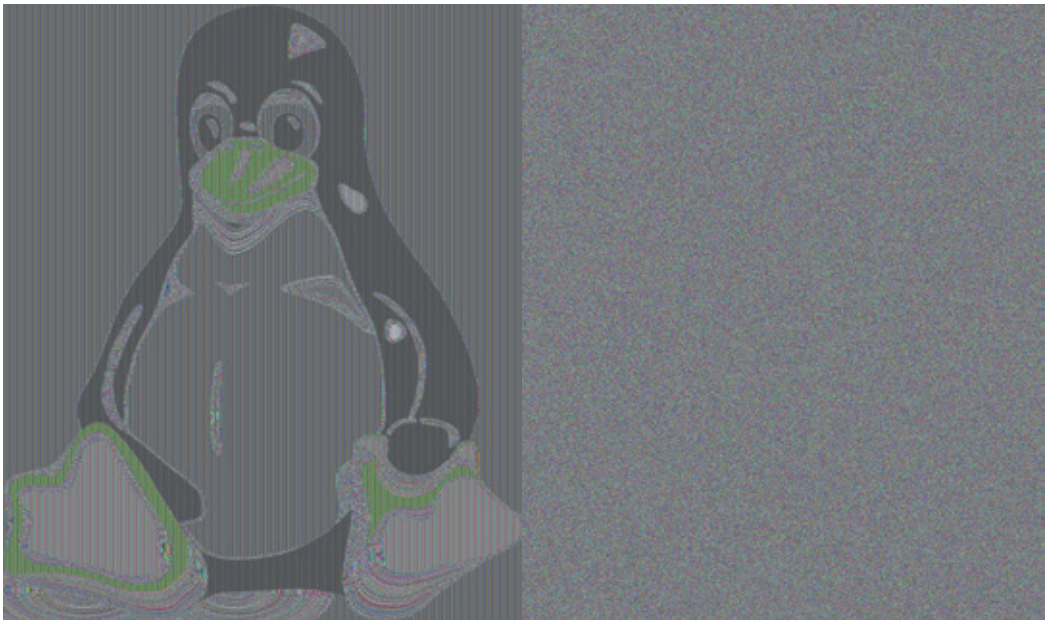
Es gibt neben dieser Variante auch Verschlüsselungen, die mathematische Operationen und das Ersetzen mittels einer großen, relativ zufällig aussehenden Ersetzungstabelle

(Substitutions- oder S-Box) abwechselnd ausführen (z. B. RC4). Auf einem modernen Rechner kann es sein, dass Tabelleneinträge im Cache der CPU abgelegt und bei erneuter Verwendung schneller gelesen werden. Beobachtet nun ein anderes Programm diese Cache-Timings, kann es Rückschlüsse auf die gerade verschlüsselten Daten ziehen. Die Möglichkeit dieser *Seitenkanal-Angriffe* sollte Verschlüsselungssoftware vermeiden, was sich technisch meist als äußerst schwer herausstellt. Threefish schließt Angriffe mittels Cache-Timings aus, da keine S-Boxen verwendet werden. Dies macht eine sichere Implementierung einfacher.

Der Pinguin Tux

Tux möchte sich verstecken. Deswegen wendet er eine Blockciffre an, trotzdem ist er noch zu erkennen. Erst durch die Verwendung von CBC ist es Tux möglich sich zu verbergen.





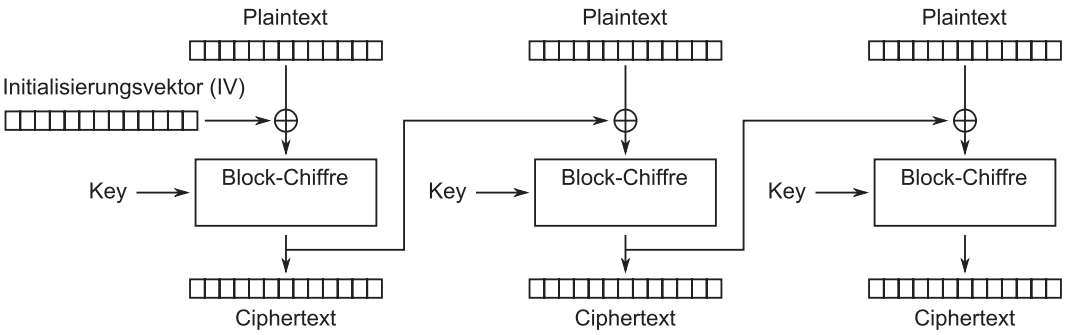
Ein weiteres wichtiges Merkmal dieser Blockchiffre ist die Verwendung von konstanten Rotationen. Viele CPUs können Rotation und Bit-Shift nicht für alle Rotationsweiten gleich schnell ausführen. Würde man die Rotationsweite abhängig von Schlüssel oder Plaintext machen, könnte eine Beobachtung der Ausführungszeiten ebenfalls Rückschlüsse auf die Daten erlauben.

Mehr verschlüsseln

16 oder 32 Bytes an gleichzeitig verschlüsselbaren Daten sind nicht allzu viel im Hinblick auf große Datenmengen. Auch hier können durch Wiederholung von ganzen Blöcken (z. B. großen schwarzen und weißen Bereichen in Bildern) Muster entstehen.

Eine Technik, dies zu vermeiden, ist das Addieren des verschlüsselten vorherigen Blocks in den Plaintext des nächsten Blocks, das sog. Cipher-Block Chaining (CBC). Der erste Block wird mit einem zufälligen Wert (*Initialisierungsvektor*) versehen, welcher unverschlüsselt mit den Daten mitgeschickt wird. Dadurch ist der Empfänger zwar gezwungen, die Blöcke in der gleichen Reihenfolge zu entschlüsseln, in der sie verschlüsselt wurden, verräterische Muster werden allerdings versteckt.

Wenn das komplette Entschlüsseln von vorn keine Option ist, z. B. in Festplattenverschlüsselungen à la TrueCrypt, kombiniert man stattdessen den Originalschlüssel mit der Position des Blocks zu einem einzigartigen



Cipher-Block Chaining

Durch die Verwendung des vorherigen Ciphertextes als Initilisierungvektor verschwinden erkennbare Muster.

Block-Schlüssel, indem die Block-Position zunächst mit dem Originalschlüssel verschlüsselt wird. Dies erlaubt es, jeden Block für sich genommen zu entschlüsseln.

Elliptische Kurven zum Schlüsselaustausch

Moderne Blockchiffren lösen zwar das Problem der sicheren Aufbewahrung und Übermittlung der Daten, sie sind jedoch *symmetrisch*: Der Schlüssel zum Entschlüsseln ist der gleiche wie zum Verschlüsseln und muss daher selbst sicher transportiert werden.

Eine erste Möglichkeit, wie zwei Parteien sich ohne Kenntniserlangung dritter *asymmetrisch* über einen Schlüssel verständigen können, wurde 1976 von Whitfield Diffie und Martin Hellman eingeführt. Eine moderne Weiterentwicklung ist heute als Elliptic Curve Diffie-Hellman (ECDH) Verfahren bekannt. Um dieses zu verstehen, betrachten wir zunächst elliptische Kurven an sich.

Elliptische Kurven

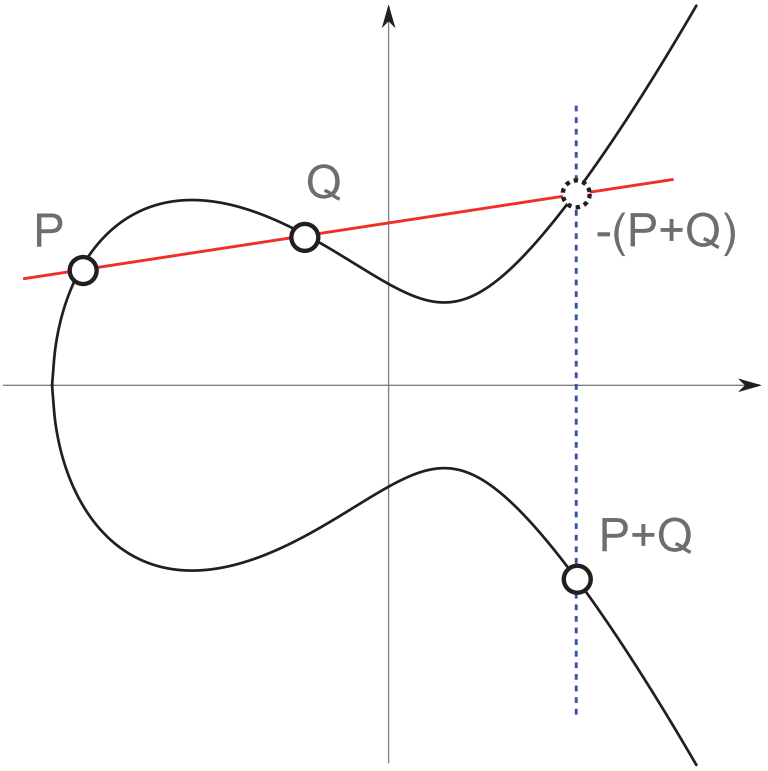
Eine Gleichung der Form $y^2 = x^3 + ax + b$ wird als elliptische Kurve bezeichnet.

Die bemerkenswerte Eigenschaft dieser Kurven ist, dass auf ihnen eine *Addition auf Punkten* definiert ist: Eine Gerade durch zwei Punkte auf der Kurve schneidet diese stets in einem dritten Punkt (oder im Unendlichen, was wir auch als gültigen Punkt auffassen). Die Spiegelung dieses Schnittpunkts an der X-Achse liefert die Summe der beiden Punkte. Weiterhin sei die Punktnegation $-P$ definiert als die Spiegelung von P an der X-Achse. Hier wird sichtbar, dass der »Nullpunkt« $o = P + (-P)$ jener Punkt im Unendlichen ist. Bei der Verdoppelung $P + P = 2P$ ist besagte Gerade einfach die Tangente durch P.

Mit diesen Werkzeugen können wir uns eine Multiplikation $n \cdot P$ definieren als n-maliges addieren. Das lässt sich durch mathematische Abkürzungen allerdings beschleunigen, z. B. ist $15 \cdot P = 16 \cdot P - P = 2 \cdot 2 \cdot 2 \cdot 2 \cdot P + (-P)$ und benötigt nur eine Negation, eine Addi-

Eliptische Kurven

Die Lösungsmenge für $a = -3$ und $b = 3$ wird hier dargestellt sowie die Addition von Punkten (rot) und Negation eines Punktes (blau).



tion und vier Verdoppelungen statt 15 Additionen. Diese Darstellung des Koeffizienten n heißt Non-adjacent form.

In der Praxis kommen allerdings keine kontinuierlichen elliptischen Kurven zum Einsatz, sondern nur deren ganzzahlige Lösungen. Weiterhin werden alle mathematischen Operationen modulo einer Primzahl N ausgeführt – das bedeutet, dass jede X- oder Y-Koordinate »überläuft«, sobald sie größer als N – 1 wird und es eine endliche Anzahl an Punkten gibt. Gute N erlauben eine große Anzahl an ganzzahligen Lösungen, z. B. bietet sich die Mersenne-Primzahl $2^{521}-1$ an. Die geometrische Punktmultiplikation funktioniert hier noch immer.

»Vertraue der Mathematik, Verschlüsselung ist dein Freund«

Bruce Schneier

Schlüsselaustausch mit Punkten

Punktmultiplikation ist assoziativ, d. h. $a \cdot (b \cdot P) = b \cdot (a \cdot P)$. Beim ECDH-Schlüsselaustausch wird diese Eigenschaft genutzt. Angenommen, Alice und Bob möchten sich auf einen Schlüssel einigen, dann verfahren sie wie folgt:

Alice und Bob einigen sich auf eine elliptische Kurve (inklusive der Primzahl N) und einen ganzzahligen Punkt P.

Alice erzeugt eine Zufallszahl a zwischen 1 und N – 1. Dies ist ihr privater Schlüssel. Sie veröffentlicht $a \cdot P$ als öffentlichen Schlüssel. Es ist technisch nicht möglich, aus zwei Punkten $a \cdot P$ und P den Koeffizienten a direkt zu berechnen, wenn N und a sehr groß sind.

Bob erzeugt seine private Zufallszahl b und veröffentlicht seinen öffentlichen Schlüssel $b \cdot P$.

Alice kann nun Bobs öffentlichen Schlüssel $b \cdot P$ beziehen und ihn mit ihrem privaten Schlüssel multiplizieren. Sie erhält $a \cdot (b \cdot P)$. Bob kann seinerseits Alice' öffentlichen Schlüssel mit seinem privaten multiplizieren und erhält $b \cdot (a \cdot P)$ und somit den gleichen Punkt.

Beide könnten nun beispielsweise die X-Koordinate des gemeinsamen Punktes als Schlüssel für ihre symmetrische Blockchiffre verwenden und so sicher kommunizieren. Sie sollten sich allerdings sicher sein, dass sie jeweils den öffentlichen Schlüssel des anderen und nicht den eines Angreifers erhalten haben, beispielsweise mittels einer digitalen Signatur.

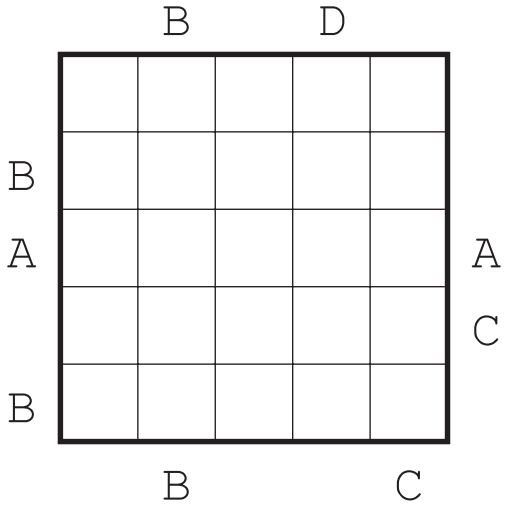
Zusammenfassung

Moderne Kryptografie ist also keine schwarze Magie, sie bedient sich einfacher, pragmatischer Konzepte, die sich leicht auf modernen CPUs implementieren lassen (z. B. Addition modulo 2^{32} oder 2^{64}, Rotation und XOR) oder geometrischer Konzepte, wie der Punktaddition auf elliptischen Kurven. Die eigentliche Schwierigkeit liegt einerseits darin, die Sicherheit mathematisch zu beweisen, und andererseits in den bereits angedeuteten Fallstricken beim Absichern der Implementierung. Bereits ein »zu wenig zufälliger« Zufallszahlengenerator kann jedes Verfahren zu Fall bringen. Dies ist auch ein Grund, weshalb es sehr wenige, wirklich sichere Implementierungen der jeweiligen Verfahren gibt. Der bedeutende Kryptologe Bruce Schneier schrieb: »Vertraue der Mathematik, Verschlüsselung ist dein Freund.« Das wahre Sicherheitsrisiko steckt allerdings im Detail der Implementierung, ob gewollt beeinflusst durch Firmen, Regierungen oder Geheimdienste oder unabsichtlich durch Programmierer.

– Toni Mattis

Rätselseite

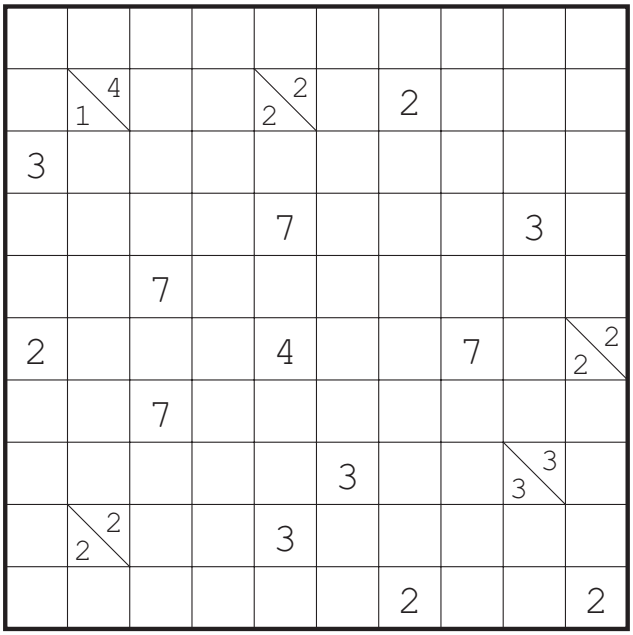
Krypto-Hochhaus:
Tragen Sie in jedes Feld ein Hochhaus der Höhe 1 bis 5 so ein, dass in jeder Zeile und jeder Spalte jede mögliche Höhe genau einmal vorkommt. Die Buchstaben am Rand stehen für Zahlen. Gleiche Buchstaben stehen für gleiche Zahlen und unterschiedliche Buchstaben stehen für unterschiedliche Zahlen. Diese Zahlen geben jeweils an, wie viele Häuser in der entsprechenden Zeile oder Spalte aus der entsprechenden Richtung gesehen werden können; niedrigere Hochhäuser werden dabei von höheren verdeckt.



Tapa: Entdecken Sie Zuse beim Lösen des Rätsels!

Schwärzen Sie einige der leeren Felder so, dass alle schwarzen Felder waagerecht und senkrecht zusammenhängen und kein 2×2-Bereich komplett geschwärzt ist. Felder mit Zahlen dürfen nicht geschwärzt werden. Die Zahlen geben an, wie viele der jeweiligen waagerecht, senkrecht und diagonal benachbarten Felder geschwärzt sind: Jede Zahl entspricht einer Gruppe aus waagerecht und senkrecht zusammenhängenden Schwarzfeldern, mehrere Gruppen sind dabei durch ein oder mehrere weiße Felder getrennt. Position und Reihenfolge der Zahlen in einem Feld spielen dabei keine Rolle.

– Maria Graber



Die Lösungen der Rätsel finden Sie auf Seite 66.

Links zu Beispielrätseln

Hochhäuser:

http://wiki.logic-masters.de/index.php?title=Hochh%C3%A4user/de (Varianten>Kryptoversion)

Tapa:

http://wiki.logic-masters.de/index.php?title=Tapa/de

Impressum

Fotos Cover, Rückseite: Florian Meinel
Aufnahmeort: Deutsches Technikmuseum, Berlin
Foto Inhaltsverzeichnis: Florian Meinel
Aufnahmeort: Deutsches Technikmuseum, Berlin
Klubfoto: Florian Meinel
Umschlagseite U3: Fotoklub (Wasserworkshop)

IT-Größen in Deutschland

Hasso Plattner
oberes Portrait Hasso Plattner: Kay Herschelmann
unteres Bild Hasso Plattner: Ludwig Wilhelm Wall
Foto August-Wilhelm Scheer: BMW Niederlassung Saarbrücken / Wolfgang Klauke
Foto Rolf Emmermann: Björn Bernat
Foto Jann Jakobs: Wikipedia
Konrad Zuse
Konrad Zuse schreibend: Privatarchiv Horst Zuse
restliche Fotos: Florian Meinel, Aufnahmeort: Deutsches Technikmuseum, Berlin
Frieder Nake
Portrait: Susanne Grabowski
Werke: Frieder Nake
Weitere IT-Größen
Grafiken: Caroline Göricke

Studentisches

Wege ins Ausland
Europakarte: Suhanyaa Nitkunanantharajah
Foto: Julia Astashova
Windows, Java, Eclipse
Grafiken: Lukas Wagner
Sieben Tipps und Tricks
Grafiken: Jasmin Mensing
Die Bedeutung des Einzelnen
Hintergrundbild: Charlotte Heinz
Mensa Griebnitzsee
Gestaltung: Tjarde Schulz

HPIintern

Von BS II bis VHDL
BS-Logos: ©FreeBSD Foundation, Windows, Larry Ewing
CGII-Bilder: Daniel Limberger
GameProg: Screenshots von Mammut, Voxel Lancer
GrafikProg: Screenshots aus cgsee
HCI II (Enten): Julia Wachtel
restliche HCI II-Fotos: Florian Meinel
VHDL-Board: Julia Wachtel
Visualisierung virtueller 3D-Stadtmodelle
Abbildungen: Amir Semmo
Laser-Cutting and 3D Printing
Stefanie Müller
Lieblingsrezepte
Zuckerschale: Sabine Rothenbücher / pixelio.de
Chilischote: w.r.wagner / pixelio.de
Möhren: Rainer Sturm / pixelio.de
angerichtetes Curry, Eischale, Teller mit panierter Garnele: Sven Knebel
restliche Fotos: Toni Mattis
Lieblingsbilder des Kunstklubs
Werke des Kunstklubs (siehe Artikel)
fotografiert von Sven Knebel, Florian Meinel
Exportschlager HPI Research School
Gruppenfoto: HPI
Weltenflucht
Hintergrundfoto: Helena Sundin
Kurzgefasst
Messefoto: HPI / Rosina Geiger

Blick über den Tellerrand

HPI-Alumni berichten aus ihrem Job
Foto Christoph Mecklenburg: Christoph Mecklenburg
Foto Jonas Gebhardt: Jonas Gebhardt / CC BY-SA
Foto Manuel Blechschmidt: Foto Schulzendorff
Hacks@MIT
Tetrisfotos: Erik Nygren
restliche Fotos: Florian Meinel
Unaufdringliche Bauklotz-Eleganz
Fotos: Florian Meinel
Gute Hacker, böse Hacker
Tunnel: Stig Nygaard (flickr, CC BY 2.0)
Hacker: Tor Håkon Haugen (flickr, CC BY-NC-SA 2.0)
Moderne Verschlüsselungen
Hieroglyphen: JSesh
Caesar-Chiffre, Chiffrierscheibe: Wikipedia
Tux: © Larry Ewing
Cipher Block Chaining: Wikipedia
elliptische Kurve: Toni Mattis
Rätselseite Rätsel: Maria Graber

Redaktionsschluss 9. Dezember 2013

Druck
Druckerei Steffen
Inhaber: Helge Steffen
Friedrich-Ebert-Str. 74
14469 Potsdam

Auflage 410 Stück

Redaktion dieser Ausgabe
Matthias Barkowsky, Andreas Burmeister, Daniel Dummer, Carolin Fiedler, Maximilian Götz, Maria Graber, Konstantin Harmuth, Pascal Lange, Franz Liedke, Suhanyaa Nitkunanantharajah, Jasper Schulz, Julia Wachtel, Lukas Wagner, Johannes Wolf

Dank an:
Sven Knebel, Florian Meinel
für die Unterstützung beim Lektorat
Sven Knebel, Toni Mattis und Florian Meinel
für das tolle Fotomaterial
Florian Meinel
für die typografische Beratung
den Kunstklub und den Klub Kulinarisches
für die grandiosen Bilder und die leckeren Rezepte
unsere externen Autoren:
Nadja Antoine, Cornelius Bock, Caroline Göricke, David Heller, Sven Knebel, Toni Mattis, Stefanie Müller, Amir Semmo, Jonathan Striebel, Karsten Tausche und den Verfasser des Gedichts »Die Bedeutung des Einzelnen«
an alle Interviewpartner, die uns mit ihrem Wissen unterstützten

Layout
Matthias Barkowsky, Carolin Fiedler, Maximilian Götz, Konstantin Harmuth, Pascal Lange, Suhanyaa Nitkunanantharajah, Lukas Wagner

Covergestaltung Carolin Fiedler

V.i.S.d.P.
Carolin Fiedler
Franz Liedke

Kontakt
klub-zeitung@hpi.uni-potsdam.de

Lösungen der Rätsel: