- **Prüfer: Dr. Walter Unger**
- **Dauer der Prüfung: 60 Minuten**
- **Note: 1.3**

Die Theorieprüfung war meine erste Informatik-Diplomprüfung. Ich war sehr nervös, und konnte schwer abschätzen ob ich "richtig" gelernt hatte. Die vielen Prüfungsprotokolle haben mir aber sehr bei der Einschätzung geholfen. Walter Unger und sein Assistent haben sich sehr engagiert, die Prüfung in einer angenehmen Atmosphäre abzuhalten. So war die Nervösität erstmal schnell weg. Ich kann euch auf den Weg geben, dass ihr euch was das angeht, wahrscheinlich bei keinem anderen Lehrstuhl auch nur die geringsten Sorgen machen müsst.

Die Reihenfolge der Fächer durfte ich mir aussuchen.

Algorithmische Kryptographie, 30 Minuten
Es wurden wirklich nur nach den Ideen hinter den Verfahren gefragt, wobei man natürlich die entsprechenden Fachbegriffe fallenlassen sollte. Es wird immer nach dem "warum" gefragt. Das einzige das ich mathematisch zeigen sollte war die Methode zum Bitcommitment.
Wenn Walter Unger mit schweren Fragen einsteigt sollte man hier auf jeden Fall versuchen entspannt zu bleiben. Einfach sagen was man weiss - es kann eigentlich nicht schiefgehen, wenn man das mal mit Verstand durchgelesen hat. Zum Lernen reichen die Folien und eventuell noch irgendein Buch. Wichtig ist, dass ihr die Idee der Protokolle versteht, und euch die Tricks merken könnt.

- **U: Kennen sie ZKP-Protokolle?** - Natürlich. Da gibts ja viele verschiedene. Fing an aufzuzählen.
- **U: Was sagen sie denn zu ZKP mit 3SAT?** - Uff, das ist ja das unangenehmste. Naja, habe sehr grob beschrieben wie der Aufbau aussieht. Hat aber schnell gereicht.
- **(Dann kam ein ZKP Beispiel aus der Vorlesung, das mit der Spülmaschine)**
- **U: Welche Sicherheit bietet ZKP für den Proofer?** - hab ich ausführlich erklärt und begründet.
- **U: Sie sagtem etwas von dem Simulator. Sie sagten der wäre deterministisch?** - Upps, naja, habs erklärt und dann war das auch ok.
- **U: So ein Commit, wie macht man das mathematisch?** - Erklärt, aufgemalt, fertig.
- **U: Wahlen. Wie macht man das mit mehreren Mischern?** - Das mit dem nacheinander symmetrisch verschlüsseln meinen sie sicher nicht? (Man kanns ja mal probieren...). Habe dann das mit der ϕ-Funktion ganz grob erzählt. **U: Wie verschlüsselt man da die Stimme?** - Diskreter Logarithmus. Wollte es näher erklären, aber es ging direkt weiter. **U: Was macht denn die ϕ-Funktion genau?** - wollte die Formel erklären, aber es ging nur um den Sinn dahinter.
- **U: Elektronisches Geld - was wissen sie da?** - ich habe nur SEHR grob erklärt worum es da geht. War schnell genug.

- **U: Es gibt ja die sogenannten Threshold-Schemes...** - Habe erklärt was es damit auf sich hat, das mit den Stützstellen eines Polynoms erläutert, und erwähnt das man das noch gewichten kann etc. Dann kamen noch ein paar Rückfragen, wie man das denn dann ausrechnet, in welchem Körper man das macht, und warum (Rundungsfehler wollte er nicht hören, ich weiss nicht was die "richtige" Antwort gewesen ist.)

- **U: Was sagen ihnen homomorphe Verschlüsselungen?** - Uhhh, nur allgemeines. **U: Ja erzählen sie mal...** - Erklärt was der Vorteil ist, wo man das nutzt (Wahlen ohne richtiges Öffnen der Stimmen). Dann wurde noch gefragt wie das mathematisch geht. Habe dann improvisiert, ging so halbwegs.

Parallele Algorithmen, 15 Minuten

Hier wurde bei den drei angesprochenen Themen ziemlich lange gebraucht. Viel haben wir nicht geschafft. Bei einer anderen Auswahl hätte ich stundenlang erklären können. Dumm gelaufen. Aber hat offenbar gereicht. Gelernt habe ich mit "Dissimination of Information in Communication Networks", "Efficient Parallel Algorithms" und vielen vielen Papern und Skripten anderer Hochschulen. Und Walter Ungers Sprechstunde :-). Sinnvoll ist auch ein Blick in die Vorlesungen zu Graphenalgorithmen, die Folien sind um Welten besser, und decken viele Themen aus PA genauso ab. Geht am besten in die Sprechstunde!

- **U: Welche Algorithmen kennen sie auf PRAM?** - Uhh, Blackout. Sortieren und Maximum-finden erwähnt.

- **U: Welche Modelle für PRAM kennen sie denn?** - Kombinationen aus exklusivem und konkurrierendem Lese- und Schreibzugriff erwähnt. **U: Welches Problem lässt ist den sehr abhängig vom verwendeten Modell?** - Ich bin nicht darauf gekommen, Blackout. **U: Fängt an zu zeichnen.** - Ach ja, Maximum finden. Erklärt warum. Naja.

- **U: Wie geht denn Einweig-Gossip auf Kreisen?** - Sehr holprig erklärt. Hatte ich glücklicherweise erst am Vortag wiederholt. Die Idee mit dem Senden in Blöcken/Wellen, und Gossip auf den Blöcken erwähnt. War glücklicherweise genug.

- **U: Und wie lange dauert das?** - Wusste ich nicht aus dem Kopf. Haben wir dann kurz zusammen vorgerechnet.

- **U: Wie geht denn Zweiwege-Gossip auf Butterfly?** - Wusste ich. Konnte ich auch begründen. Habe eine Kleinigkeit vergessen, konnte aber erklären warum das nicht fehlen darf. Die Laufzeit war wieder etwas holprig erklärt.

Compilerbau, knapp 15 Minuten

Gelernt habe ich mit einer verkürzten Mitschrift von *s-inf.de*. Man muss vor allem die Zusammenhänge in der lexikalischen und syntaktischen Phase verstanden haben. Schon vor Beginn des Compilerbau-Teils wurde von **U** erwähnt, dass die Codegenerierung fies zu prüfen wäre :-).

- **U: Was tut ein Compiler?** - Erklärt.

- **U: Welche Phasen gibts da?** - Erklärt.

- **U: Lexikalische Phase bitte.** Genauer erklärt.

- **U: Warum ist denn der Scanner dann deterministisch?** - Erklärt.
- **U: Diese LA-Mengen, was sind das?** Erklärt.
- **U: (Es kamen noch vier, fünf kurze Fragen, nichts wildes.**
- **U: Syntaktische Analyse. Erzähl mal.** Getan.
- **U: Wie analysiert mann denn CFG normalerweise?** - CYK...? **U: Genau. Laufzeit? ...warum?** Halbwegs erklärt.
- **U: Warum gehts bei LL(k) und LR(k) schneller?** - Erklärt. **U: Das k steht wofür?** - Klar.
- **U: Diese Auskunft-Mengen die es da gibt ...** *Der Beisitzer bricht ab, mit Hinweis auf die Zeit :-)* - Kenn ich aber :-). **U: Gut! Raus jetzt :-).**

Nach knappen 10 Minuten durfte ich wieder rein. Die Fragen seien sehr schwer gewesen, wenn ich etwas nicht gewusst hätte, hätte ich gut improvisiert und versucht das logisch herzuleiten. Ich bin aber auch echt ein paarmal fies auf dem falschen Fuß erwischt worden. Es dauert manchmal auch ein paar Sekunden, bis man kapiert was die Fragen bezwecken. Wendet euch für Lernmethoden an jemanden der das schon hinter sich hat. Es lohnt sich.
Alles in allem war es trotz holpriger Stellen eine *sehr* angenehme Prüfung ohne Nervösität.