ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Institut für Theoretische Informatik

ETH Zentrum IFW E45.1
CH-8092 Zürich

Prof. Ueli Maurer
Haldeneggsteig 4
Tel. +41-1-632 74 20
Fax +41-1-632 11 72
maurer@inf.ethz.ch

Herr
Prof. Dr. Walter F. Tichy
Dekanat der Fakultät für Informatik
Am Fasanengarten 5
D-76131 Karlsruhe
Deutschland

Gutachten

zur Dissertation
„Entwurfskriterien und Methoden zur Erlangung von Kommunikationssicherheit",

vorgelegt von
Hadmut Danisch
an der Universität Karlsruhe

Die vorliegende Arbeit erfüllt meiner Meinung nach ganz klar die Anforderungen an eine Dissertation an einer Fakultät für Informatik nicht. Die wichtigste Voraussetzung für eine Dissertation, nämlich dass sie neue Ideen, interessante intellektuelle Gedankengänge oder neuartige Einsichten enthält, ist meiner Ansicht nach klar nicht erfüllt. Ich habe beim Lesen der Dissertation nicht ein einziges Mal ein „Aha"-Erlebnis gehabt, es hat mich kein neuartiger Gedankengang überrascht, und es war auch keine Freude, den Bericht zu lesen, auch wenn die sprachliche Qualität gut ist.

Eine solche Meinung klar zu begründen, ist naturgemäss nicht einfach, da das Fehlen von Ideen schwieriger zu untermauern ist als zum Beispiel allfällige Fehler aufzuzeigen. Deshalb ist das Gutachten auch nicht sehr detailliert, indem es auf jedes Teilkapitel Bezug nehmen würde. Zudem darf der Anspruch an ein solches Gutachten nicht gestellt werden, dass es für jede Aussage und jeden Gedankengang der Dissertation aufweist, wo in der Literatur dies bereits bekannt ist.

Umgekehrt bestünde der Anspruch an eine Dissertation, klar zu machen, was denn nun der Neuheitsanspruch ist. Dies ist in der Dissertation aber nicht der Fall. Ein Anspruch, aber sehr allgemein formuliert, kann in der Einführung (Kapitel 1.1) und in Kapitel 6 ausgemacht werden. Der Pauschalanspruch, einen Beitrag zur Analyse, Beschreibung und den Entwurf von Sicherheitssystemen im Bereich der Kommunikation zu leisten, wird aber weit verfehlt, und in der Arbeit selbst wird dieser Anspruch auch nicht weiter vertieft. Der Text erscheint mir vielmehr eine Sammlung von Bekanntem, in etwas willkürlicher Reihenfolge zusammengeschrieben, zwar in gutem Deutsch, aber gedanklich etwas unklar geordnet. Selbst dem Anspruch einer guten Zusammenfassung eines Themas, auch bei Weglassung eines Neuheitsanspruchs, wird die Arbeit meiner Meinung nach nicht gerecht.

Kapitel 1 ist in grossen Teilen völlig oberflächlich, ohne jeglichen Tiefgang, und ohne klar ersichtlichen Bezug zum Rest der Arbeit. Das gleiche gilt leider auch für Kapitel 2, obwohl hier eigene Gedankengänge auszumachen sind, zum Beispiel bei der Klassifikation des Angreifers (z.B. Abbildung 2.3). Allerdings halte ich diese Gedankengänge nicht für sehr relevant, und insbesondere ist wiederum kein Bezug zum Rest der Arbeit vorhanden. Auch in Kapitel 3 und 4 verbessert sich die Situation nicht, ausser dass hier auch Zweifel aufkommen, ob der Kandidat alles versteht, worüber er schreibt. Beispiel 3.30 lässt bei mir den Eindruck entstehen, er verstehe nicht viel von Quantenkryptographie.

Kapitel 5 ist das einzige, in dem man klare Gedankengänge findet. Allerdings sind diese nicht neu, sondern aus der Literatur resp. aus Unterrichtsmaterial entnommen, insbesondere der Teil über Informationstheorie. Warum kommt überhaupt ein Teil über Informationstheorie, wenn er gar nicht wirklich zu Neuen gebraucht wird, ausser für die Argumentation zum Theorem 5.17? Dies bestärkt wieder den Eindruck, der Kandidat möchte eher Seiten füllen statt klare eigene Gedankengänge vermitteln.

Der einzige interessante Punkt ist Theorem 5.17, welches der Kandidat vermutlich selbst erarbeitet hat, das allerdings trivial ist und deshalb als bekannt angesehen werden kann. Zunächst ist zu sagen, dass „zensierbar" nicht klar definiert ist, was man aber tun könnte. Dadurch ist auch das Theorem nicht ein mathematisches Theorem, aber es könnte präzise formuliert werden. Der (korrekte) Gedankengang ist, dass wenn ein Kanal mit maximaler Rate (gleich der Kapazität) betrieben wird, somit also keine zusätzliche Information mehr übertragen werden kann, ein Widerspruch entstehen würde, wenn man annimmt, man könnte am Ausgang des Kanals feststellen, ob der Input eine bestimmte Eigenschaft aufweist (z.B. chiffriert zu sein oder nicht). Diese Erkennung würde ja gerade erlauben, ein weiteres Bit zu übertragen.

Zusammenfassend muss ich leider klar empfehlen, diese Arbeit nicht als Dissertation anzunehmen. Auch eine Überarbeitung würde nicht genügen, sie in eine akzeptable Dissertation umzuschreiben. Es fehlt schlicht das Rohmaterial. Ich werde den Eindruck nicht los, der Kandidat verstehe gar nicht richtig, was wissenschaftliche Forschung ist. Deshalb wird er vielleicht auch Mühe haben, die hier geäusserte Kritik zu akzeptieren. Ich bin etwas erstaunt, dass jemand nach vermutlich mehrjähriger Arbeit an einem wissenschaftlichen Institut nicht entweder die Befähigung zur wissenschaftlichen Arbeit erworben hat, oder früher die Konsequenzen gezogen hat und den Lebensweg den eigenen Stärken gemäss gewählt hat. Es bleibt mir, die Hoffnung auszudrücken, dass der Kandidat auch ohne Doktortitel eine gute berufliche Karriere haben wird.

Zürich, 30. Juli 2003

Ueli Maurer

Prof. Ueli Maurer