UNIVERSITÄT KARLSRUHE
FAKULTÄT FÜR INFORMATIK
Institut für Algorithmen und Kognitive Systeme
Prof. Dr. Th. Beth

Am Fasanengarten 5
76128 Karlsruhe

Telefon: 07 21 / 608-
Fax: 07 21 / 69 68 93
4205



**Gutachten**

**über die von**

**Herrn Dipl.-Inform. Hadmut Danisch**

**vorgelegte Dissertation:**

**"Entwurfskriterien und Methoden zur Erlangung von Kommunikationssicherheit"**

## Voraussetzungen und Aufgabenstellung

Ziel dieser Dissertation war es, angesichts der immer deutlicher werdenden Sicherheitsproblematik in großen, zumeist offen Netzen, wie dem Internet, aber auch Telefon-Netzen , die Frage der Sicherheit vor allem bei Kommunikationsverbindungen zu untersuchen, wobei einer angemessenen Behandlung des Themas unter Berücksichtigung der verschiedenen Sicherheitsbegriffe und der diversen physikalischen, system-, modell- und informationstheoretischen sowie (krypto)-logischen Sicherungs- und Sicherheitstechniken ein hoher wissenschaftlicher Gehalt zuzumessen ist.

Der Kandidat hatte sich während seiner mehrjährigen Mitarbeit am EISS in die praktische Sicherheitstechnik von Kommunikationsnetzen und Rechnersystemen soweit eingearbeitet, dass aufgrund seiner offensichtlichen Kenntnisse der Informatik und der Kryptologie eine wissenschaftliche Abhandlung anhand systematischer Untersuchungen und beispielhafter ingenieurmäßiger Implementierungen ein erfolgversprechendes Promotionsthema über Kommunikationssicherheit in offenen Netzen sich abzeichnete. Nachdem der Kandidat trotz seiner umfangreichen Kenntnisse mehrere vom Betreuer gestellte, forschungsbedürftige Aufgaben im Bereich der Kryptographie und des Schlüsselmanagements angesichts der Übertragungsformate und Kompressionsverfahren in - damals noch nicht verfügbaren sicheren - Kommunikationsendgeräte wegen der aus Kandidaten-Sicht mangelnden Promotionswürdigkeit zurückgewiesen hatte, wurde aufgrund aktueller Weiterentwicklungen der Kommunikation im Internet und den Aktivitäten des Kandidaten entsprechend das Thema der Arbeit im Bereich der sicheren Rechnerkommunikation in offenen Netzen vereinbart. Da aufgrund der vielfachen Praxis-Projekte des Instituts, an denen der

Kandidat beteiligt war, umfangreiche Gelegenheit bestand, die o.g. Untersuchungen und Implementierungen erfolgreich durchzuführen, wurde der Kandidat am 18.12.1996 als Doktorand der Fakultät für Informatik angenommen.

Die Wahl des Themas, "Entwurfskriterien und Methoden zur Erlangung von Kommunikationssicherheit", erfolgte auf Vorschlag und nachhaltiges Insistieren des Kandidaten, nachdem der Betreuer auf die Schwierigkeiten hingewiesen hatte, die mit der Bedeutung des Wortes "Erlangen" verbunden sind.
Das Thema war und ist von grosser Bedeutung für die Entwicklung der Informatik und Informationstechnologie mit einer gewissen Brisanz aufgrund der Diskussionen um Chiffrier-Verfahren und -Verbote sowie Schlüsselhinterlegung, und der gleichzeitigen Debatte über Abhörgesetzgebung sowie systematische Lauschattacken im Internet. Eine angemessene Behandlung des Themas sollte durch explizite Verbesserungsvorschläge und Implementierungen oder auch durch die Angabe von Unmöglichkeitsbeweisen für die Existenz bestimmter Sicherheits-Eigenschaften bzw.-Systeme nachgewiesen werden.

## Durchführung der Arbeit

Die Arbeit gliedert sich in fünf Kapitel und eine Zusammenfassung nebst Einordnung mit 177 Textseiten sowie ein Literaturverzeichnis von 142 Zitaten und einen Lebenslauf , enthält aber kein Schlagwortregister. Beim ersten Lesen besticht die Arbeit durch einen spannenden, journalistisch zu nennenden Schreibstil, der zunächst auch Experten den Eindruck eines gut verständlichen, inhaltsreichen und in sich konsistenten Textes vermittelt.

Das **Kapitel 1:** "Einführung" beschäftigt sich mit einer Begriffsfindung und ersten Szenarios der gegenwärtigen Situation der Sicherheitstechnik aus Sicht des Kandidaten. Was von jedem Leser zunächst für ein zentrales Thema der modernen Informatik gehalten werden dürfte, nämlich das uns alle beschäftigende Thema Systemsicherheit, wird in diesem Kapitel im Wesentlichen dazu benutzt, um unter der Tarnung eines spannend geschriebenen Textes, den Leser durch konträre Aussagen und Darstellungsmethoden, die dem Magazinjournalismus entnommen zu sein scheinen, für die vom Kandidaten vertretenen Thesen, die in den späteren Kapiteln deutlich werden, zu gewinnen. So sind die Definitionen über die entscheidenden Begriffe der Sicherheitstechnik rein sprachlicher Natur, um vor allen Dingen durch eine etymologische Auseinandersetzung mit altgriechischen Begriffen, versuchsweise nachzuweisen, dass schon die in der Sicherheitstechnik benutzte Sprache ohnehin unangemessen sei und mit anderen Begriffen versehen werden müßte. So behauptet der Kandidat, dass die Begriffe Kryptographie und Steganographie gerade mit vertauschter Bedeutung benutzt werden, um dann mit einem neuen Begriff, der nach Kenntnis des Gutachters im Wörterbuch der deutschen Sprache nicht vorhanden ist, nämlich "Adälographie", als neuen

Oberbegriff einzuführen .(N.B. Ich frage mich, was die *seniores* unserer deutschen Zunft, nämlich der Kollege F.L. Bauer in München und Dr. Otto Leiberich in Bonn oder gar der verstorbene Kollege Ernst Henze zu diesem Thema zu sagen hätten).

In ähnlicher Weise beschäftigt sich der Kandidat in den Abschnitten 1.4 und 1.5 mit den vorliegenden Handbüchern zur Sicherheitstechnik und widmet sich einer ihm m. E. nicht zustehenden Kritik dieser Handbücher, die für die Entwicklung der Informationstechnologie in USA, D und EU entscheidend waren: An der Aussage (p.14) *„Es ist nicht nachvollziehbar, wie es die Sicherheit eines Systems verbessern soll, wenn es statt mit normaler mit eingeschränkter Sprache und eingeschränkter Satzstruktur beschrieben wird"* muss der Kandidat auch seinen eigenen Text messen (lassen). Aus heutiger Sicht wäre eine wissenschaftliche Auseinandersetzung ein durchaus promotionswürdiges Thema. Im vorliegenden Text jedoch handelt es sich bei der Bearbeitung dieses Themas nicht um einen Beitrag zur wissenschaftlichen Informatik, sondern eher um eine Darstellung einer möglicherweise juristischen in techniknahe Bereiche übersetzten Behandlung der Frage Sicherheitstechnik.Diese ist im wissenschaftlichen Gehalt keinesfalls dem gemäß, was den Standards der Fakultät für Informatik entspricht.

Abschnitt 1.6 beschäftigt sich mit formalen Sicherheitsmodellen und gibt zunächst zur Hoffnung Anlaß, dass an dieser Stelle, an der in den letzten 25 Jahren erhebliche Anstrengungen von fundamentaler Bedeutung und hohen wissenschaftlichen Gehalts unternommen wurden, die wissenschaftliche Abhandlung beginne. Leider endet auch dieser Abschnitt nur als verbale Auseinandersetzung, die im Wesentlichen der Kritik an heutigen Methoden dient, ohne dass dabei konkrete Verbesserungsvorschläge gemacht werden oder gar auf Publikationen neueren Datums verwiesen wird, wie etwa das Buch von Dieter Gollmann: "Computer Security", Wiley & Sons, Erscheinungsdatum: Januar 1999 (dieses Buch hätte vom Kandidaten, da die Arbeit erst im Wintersemester 1999 abgegeben wurde, zitiert werden müssen, da es zu diesem Zeitpunkt erschienen und bekannt war) oder auf die dem Kandidaten durchaus bekannte BAN- Sicherheits-Logik mit der Erweiterung von BKY (siehe: Th.Beth, B. Klein, R. Yahalom: "Trust Relationships in Secure Systems - A Distributed Authentication Perspective "Proceedings 1993 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, CA, USA, 1993, IEEE Computer Society Press, 1993, S. 150-164) .

Insbesondere hatte der Kandidat Zugang zu einem Reichtum an Quellen und Aufsetzpunkten, ü.a. aufgrund weiterer Veröffentlichungen, die im E.I.S.S. entstanden sind, wie z.B.

Journal of Cryptology, Special Issue, Protocol Failure, Vol.7, No. 2, Springer-Verlag, 1994

oder

Special Issue Journal of Computer Security, Vol.2, No.1, IOS Press, 1993.

Zusammenfassend ist zu diesem Abschnitt zu sagen, dass selbst die Definitionen nur auf sprachlicher Ebene und nicht richtig getroffen werden. Insbesondere hat der Kandidat gerade die wichtige Unterscheidung von Security und Safety, wie sie z.B. in der von ihm erwähnten Dissertation von Peer Wichmann aus dem Jahre 1998 [137] vorgenommen wird, weder zitiert noch verbessert, noch in irgendeiner Weise versucht, formal auf diese Unterscheidung einzugehen.

**Abschließende Bewertung zu Kapitel 1:**

Wie beschrieben sind die gemachten Aussagen des Kandidaten nicht richtig oder bewußt in Kollision zu der gängigen und heute in der Sicherheitswissenschaft betriebenen Form gesetzt worden. Auch wenn dieses erste Kapitel den Stil einer gut gemachten Einleitung in ein kritisches und auf Öffentlichkeitswirkung bedachtes Benutzerhandbuch vermitteln will, ist die o.g. Aufgabenstellung, die Grundlage für eine angemessene Behandlung des Themas zu schaffen , nicht erfüllt. Vor allen Dingen fehlt jegliche Art von Belegen oder Beweisen, die Quellenzitate sind nicht vorhanden, und Nachweise für irgendwelche Behauptungen und Gerüchte sind ebenfalls nicht zu finden. Typisch dafür ist z.B. die Untersuchung der als Beispiel gegebenen konkreten Betrachtung einer Zertifizierung 1.5.2, in der ein aktueller Zertifizierungsreport der BSI analysiert und kritisiert wird, ohne dies zu formalisieren oder Verbesserungsvorschläge zu realisieren.

Das **Kapitel 2** "Die System- und Bedrohungsanalyse" gliedert sich in fünf Abschnitte, deren Gliederung zunächst den Eindruck des Versuchs einer systematischen Problemanalyse zu geben,versucht, obwohl der Autor auf Seite 1 seines Textes sagt: "*So ist zu beobachten, dass der Begriff 'Bedrohungsanalyse' gern verwendet wird, weil er eine wissenschaftliche Untersuchung suggeriert und den Eindruck hervorruft, kein System von der Stange, sondern eine maßgeschneiderte Problemlösung hervorzubringen*". Abgesehen von gewissen Ungewöhnlichkeiten im Stil (das Wort "Baustelle" auf Seite 29,Z.-2 ist wohl eher ugs.), ebenso wie einige Schreibfehler, die sonst eher selten zu beobachten sind (z.B. Seite 30, Zeile 1) wird durch die Einführung in dieses Kapitel in den mit vier "bullets" abgesetzten Themen, die den Rahmen für die folgenden Abschnitte liefern sollen, die Verwirrung größer. Dies läßt beim Leser die Frage aufkommen, was der Autor denn mit diesem Text eigentlich beabsichtigt: Dazu sei auf die Aussage der Zeile -8 verwiesen, dass "*der - reale oder hypothetische - Angreifer stets als fester Bestandteil mitbetrachtet*" werden soll, um dann zwei Zeilen weiter zu lesen: "... *kann es weder einen realen noch einen hypothetischen Angreifer geben, braucht man keine Sicherung*". Abgesehen davon, dass diese Aussage aus wissenschaftlicher Sicht nicht konsistent ist, entbehrt diese Aussage, falls sie denn logisch haltbar sein sollte, aus Mangel an Formalisierung jeder praktischen und technischen Bedeutung: Hier straft sich der Autor selbst, weil er die in Kapitel 1 gegebenen Begriffe von Sicherheit nicht formal gefaßt hat und somit übersehen hat, dass Security über die formale Spezifikation auch Aussagen über das Komplement einer i.a. rekursiven Menge bedeutet, über das außer ihrer rekursiven Aufzählbarkeit nicht viel mehr bekannt ist. Somit kann die Frage, ob es einen realen oder hypothetischen Angreifer

gebe, im Allgemeinen überhaupt nicht beantwortet werden. In jedem Fall ist dem Kandidaten diese Fragestellung als zentrales Forschungsproblem der Sicherheitstechnik bekannt. Der Kandidat wurde von seinem Betreuer mehrfach - offensichtlich vergeblich - darauf hingewiesen, sich der genaueren formalen Definition zu bedienen.

Abschnitt 2.2 versucht eine Analyse der befugten Parteien zu geben, jedoch wird dem im Gebiet erfahrenen Leser sofort klar, dass der Begriff der Partei nicht nach wissenschaftlichen Gesichtspunkten getroffen wurde, denn sonst hätte der Kandidat auf das schon vor nahezu zwei Jahrzehnten von Roger Needham eingeführte und seither bewährte Konzept des "principal" zurückgegriffen und nicht wieder versucht, mit einer eigenen Definition zusätzliche nomenklatorische Neuentwicklungen zu beginnen.

Ähnliches ist zu Bemerkung 2.2 zu sagen, in der die drei Grundparteien vorgestellt werden. Hier handelt es sich ganz offensichtlich um das Wiretap-Modell, nur beschrieben mit Worten, die der vom Kandidaten bevorzugten Sprache entsprechen. Nachdem der Parteibegriff im Wesentlichen durch den des „Interessenträgers" gekennzeichnet ist, hat es der Kandidat versäumt, in Abschnitt 2.2., insbesondere in Subabschnitt 2.2.1 neben Identität und Adressen auch noch die Interessen zu definieren.

Allein schon dieser Teilabschnitt kann als Beleg - *pars pro toto* - für die im Wesentlichen vom Kandidaten angestrebte metatheoretische und versuchsweise philosophische Auseinandersetzung mit dem Thema gewertet werden kann. Dass diese Aussagen nicht technischer Natur sind und zum Teil nicht einmal die dem Kandidaten durchaus bekannte praktische Realität der Netze widerspiegeln, ist an den letzten drei Zeilen auf Seite 32 zu sehen, welche sich angesichts der wohlbekannten Existenz von "cookies" als falsch oder zumindest realitätsfremd darstellen. Ähnliche Kritik ist auch aus mathematisch formaler Sicht an diesem Abschnitt 2.2 zu üben, da z.B. die Definition 2.3 des Begriffes Partition zu einen überflüssig wäre, da dies ein bekannter Begriff aus der Mengenlehre ist und als Datenstruktur zum Stoff des Grundstudiums gehört. Leider ist dem Kandidaten bei diesem Versuch einer formalen Definiton gegen seine Absicht ein Fehler unterlaufen, da er die Typen der Parteien nach Bemerkung 2.2 gerade in dem Begriff der Partition hat berücksichtigen wollen.

Definition 2.4 ist ein Beispiel für eine sprachliche Tautologie, wobei insbesondere die Frage, was die Vorstellungen eines Interessenträgers seien wohl eher dem Bereich der Psychologie zuzuordnen ist und somit nicht Gegenstand einer Informatikuntersuchung sein dürfte.

Darüberhinaus zeigt Definition 2.5, dass der Kandidat auch hier wohl siehe Definition 2.3 etwas anderes gemeint als geschrieben hat, und dabei wohl übersehen hat, dass der Begriff einer Abbildung in der Mathematik schon seit langem festliegt und seine Definition, genau

betrachtet, wegen ungenauen Ausdrucks so nicht stimmt. Auch die Behandlung von Ressourcen und Kosten zeigt, dass der Kandidat offensichtlich sich in der Diktion seiner Thesen verfangen hat, da die versuchsweise Definition des Begriffes Leistungsfähigkeit nicht nur rein sprachlich von ihm verwechselt wird mit dem Begriff des Aufwandes, den er dem Attackierer zuordnet, wie man auf Seite 54 sehen kann. Dieser Fehler wird auf Seite 72 in Abschnitt 3.4 deutlich, wo der Kandidat gerade bei Betrachtung des Kosten-Nutzen-Verhältnisses für Angreifer beide in Abschnitt 2.2 bzw. 2.4 in selbstgemachten Definitionen durcheinander bringt und damit auch den Leser in einiger Verwirrung zurück läßt.

"Freilich laufen alle Methoden darauf hinaus, den Angriff zu erschweren. Hier aber liegt der Schwerpunkt der Verursachung von *Kosten* für den Angreifer." (Anm. des Kandidaten Fußnote 2, Seite 73)

An Beispiel 2.9 wird klar, in welche Verwirrung sich der Kandidat selbst gebracht hat. Was hat die Frage, dass die Fälschung von Briefmarken ähnlich teuer sein würde wie die Fälschung von Geldnoten, mit dem Thema der Arbeit zu tun? Dieses letzte Beispiel zeigt, wie wenig der Kandidat seine Thematik vom Gesichtspunkt der Informatik aus untersucht hat.

Der Abschnitt 2.3 über die Eigenschaften des Übertragungsmediums hätte entsprechend der Aufgabenstellung eine wesentlich tiefere Auseinandersetzung darstellen müssen, nachdem diese etwa in Einführungsvorlesungen über Sicherheitstechnik ausführlicher und genauer behandelt werden. So ist z.B. die Aussage "*Fehlerkorrektur bedeutet Redundanz; Redundanz bedeutet Angriffsfläche für einen Angriff gegen die Vertraulichkeit ...*" ein typisches Beispiel für die auf dogmaähnlichen Kernsätze zusammengeschrumpften Erkenntnisse aus der Informatik, ohne dass diese belegt, expliziert oder ausgeführt werden. Der wissenschaftliche Gehalt und die saubere wissenschaftliche Vorgehensweise fehlen hier nicht nur, sondern werden von dem Kandidaten durch die Benutzung dieses eher journalistischen Mittels bewußt in Frage gestellt. In Folge dieser Ungenauigkeit bei der von ihm angestrebten Taxonomie des Problems verfängt der Kandidat sich dann offensichtlich in der eigenen Nomenklatur, wie etwa in den ersten Zeilen von Abschnitt 2.3.4, in denen die drei Arten der Parteienbeteiligung, nämlich die Rolle des Empfängers, die Rolle des Senders und die dritte Art „Mischformen" (welche?) als drei separate Klassen angesehen werden. Es ist aus Sicht der wissenschaftlichen Informatik völlig unakzeptabel und in der Sicherheitstechnik möglicherweise gefährlich, diese Art von oberflächlicher Kategorisierung im Rahmen wissenschaftlicher Texte oder gar einer Dissertation zu benutzen oder gar niederzuschreiben.

In Abschnitt 2.3.5 mit der Überschrift: "Nebenwirkungen und Risiken der Absicherung" unterläuft dem Kandidaten der nicht verzeihbare Lapsus, zu Ende des vorletzten Absatzes das Beispiel medizinischer Patientendaten, die im Notfall nicht verfügbar seien, zu erwähnen, ohne dieses auszuführen, und vor allen Dingen, ohne dabei darauf hinzuweisen, dass dieses Beispiel der vom EISS für den Deutschen Bundestag angefertigten Studie [44] entlehnt wurde.

Der folgende Abschnitt 2.4, der sich mit dem Modell (in welchem Sinne?) des Angreifers beschäftigt, basiert im Wesentlichen auf dem wissenschaftlich nicht haltbaren Grundsatz"*Wer oder was nicht zweifelsfrei zuverlässiger Freund ist, gehört zum Feindbild* ".Diese Aussage ist für den Gutachter kaum nachvollziehbar, offensichtlich aber nicht informatischer Art. Diese müßte eher von einem Gutachter aus der Psychologie oder Soziologie beurteilt werden.

Die diagrammatischen Veranschaulichungen ( Abb.2.3, p.48) der Positionen des Angreifers im Kommunikationsschema wecken beim ersten Lesen den Anschein der in der Aufgabenstellung angestrebten Taxonomie. Jedoch stellt sich weiter unten beim Lesen des Textes auf Seite 122 heraus, dass durch das dort gegebene Diagramm in Abbildung 5.1, wie der Autor selbst feststellt, sein Diagramm 2.3c ergänzungsbedürftig ist. An dieser Stelle wird in jedem Falle deutlich, dass die vorgelegte Dissertation niemals über das Entwurfsstadium hinausgewachsen ist, was der Betreuer bereits vor Jahren aufgezeigt hat. Spätestens an dieser Stelle sollte es dem Autor nach Schreiben des Abschnittes 5.1 aufgefallen sein, dass er den Abschnitt 2.1 revidieren hätte müssen. Dabei hätte er festgestellt, dass die Begriffe, die er hier z.T. neu prägt, formalisiert werden müßten, um damit in wissenschaftlich arbeiten zu können. Die Art der Auseinandersetzung mit dem Thema, die wegen ihrer engen Verbindung der Kryptologie mit der Sicherheitstechnik und mit dem damit verbundenen Wertetransfer ein hohes Risiko beinhaltet, hätte höchster Sorgfalt und Genauigkeit bedurft. Beispiel 2.18 gibt mit der in der Fußnote gegebenen Bemerkung über schwache Schlüssel einen Einblick in die nahezu fahrlässig zu nennende Ungezwungenheit, mit der der Kandidat über existierende Kryptosysteme urteilt und damit wie auch immer geartete Bewertungen, die möglicherweise zu erheblichen Folgen führen könnten, einfließen läßt.

Ähnlich unvollständig und schwer nachvollziehbar ist die Auseinandersetzung mit dem Thema „Schutzobjekt" in Abschnitt 2.5. Die Begriffe: Integrität, Authentizität, Vertraulichkeit etc. sind seit Jahrzehnten in der Informatik diskutiert, und erfolgreich definiert worden, wie dieses dem Kandidaten aus Vorlesungen und Seminaren sowie Projekten seit Jahren bekannt ist. Definition 2.20 ist formal gesehen keine, liegt orthogonal zu den akzeptierten Definitionen und entspricht nicht dem Stand der Kunst und dem Stand des Wissens. Insgesamt ist dieser Abschnitt aus wissenschaftlich-technischer Sicht kaum nachvollziehbar, wie auch das Zitat 2.19 aus dem StGB an dieser Stelle zeigt.

Subabschnitt 2.5.2.4 stellt eine Mischung zwischen philosophisch-psychologischer Argumentation und einer möglicherweise juristischen Argumentation dar, die auf keinen Fall aus informatischer Sicht als wissenschaftliche Aussage zu bewerten ist.

Auf Seite 62 wird in Subabschnitt 2.5.2.5 wieder einmal auf den Unterschied zwischen Safety und Security hingewiesen, wobei der Kandidat selbst, wie oben gezeigt, mehrfach zwischen den beiden Gebieten nicht zu unterscheiden imstande ist. Aber auch aus technischer Sicht ist durch die verwirrende Art der Beschreibung, die

durch Abbildung 2.7 kaum verbessert wird, der vom Kandidaten beschrittene Weg nicht nachvollziehbar.

Absatz 1 von Abschnitt 2.5.3 zeigt die völlige Begriffsverwirrung und gibt eine falsche Darstellung technischer Details. Es ist falsch, dass beim Telefonieren die Telefonnummern übertragen werden müssen. Der Kandidat scheint dabei ausschließlich an die im Moment praktizierten ISDN-Protokolle zu denken und hat dabei übersehen, dass z.B. insb. bei Packet Switched Networking mit Public-Key Adressierung, wie sie von dem vor wenigen Tagen verstorbenen Donald Davies F.R.S. als ursprüngliche Grundlage für die Einführung von PSN betrachtet wurde, genau diese Problem umgangen werden sollte (siehe dazu auch : The Times, London, Mittwoch, 31.05.2000). Wie sehr sich der Kandidat ohne Not in eine Falle bezüglich seiner eigenen völlig unbrauchbaren Taxonomie gebracht hat, zeigt die Bearbeitung der Subabschnitte 2.5.3.1 bis 2.5.3.10. Hier hat er, vermutlich nur um seinem eigenen im Top-down-Entwurf früherer Gliederungen auferlegten Muster zu genügen, jeden Punkt mit wenigen Zeilen gefüllt, ohne wirklich Inhalte oder gar wissenschaftliche Statements zu vermitteln.

Ein abschließendes Exempel für die Nichtnachvollziehbarkeit und die Verwirrung, die dieses ganze Kapitel stiftet, ist in Beispiel 2.26 gegeben, wo überhaupt nicht klar wird, wieso das dort beschriebene Szenario einen Angriff(?) gegen einen "anonymus remailer" darstellt.

**Abschließende Bewertung zu Kapitel 2:**

Das Kapitel ist aus Sicht der wissenschaftlichen Informatik, wie schon mehrfach nachgewiesen, nicht akzeptabel, bedient sich populistischer Szenarios außerhalb des Themas der Arbeit, liefert statt exakter Definitionen, wie in der Informatik und den exakten Wissenschaften üblich, zirkuläre Begriffsbildungen und vermeidet die formale Auseinandersetzung mit dem Thema der Arbeit. Insgesamt handelt es sich um ein kaum verständliches Durcheinander von generisch scheinenden Begriffsbildungen und dem vergeblichen Versuch, diese durch redundante Beschreibungen und Aussagen der Aufgabenstellung gemäß wissenschaftlich zu behandeln.

**Kapitel 3** trägt die Überschrift: "Sicherungsmethoden". Der Kandidat unterscheidet in der Einführung auf den ersten vier Zeilen zwischen Methoden und Maßnahmen, was beim Leser die Hoffnung erweckt, dass dem Wissensstand der Informatik entsprechend nunmehr mit abstrakten und konkreten Datentypen und modelltheoretischen Methoden gearbeitet wird. Dieses ist mitnichten der Fall. Die in Tabelle 3.1 zusammengestellten Abschnitte eröffnen nicht die in der Aufgabenstellung erwünschte Taxonomie. Auch der mit dem Gebiet unvertraute Leser wird sofort anhand der Länge der Abschnitte feststellen, dass dies ein Ergebnis der unseligen Top-down-Strukturierung von Texten ist, wie oben bereits schon einmal erwähnt, und den Kandidaten nach einmal gewählter Gliederung dazu gezwungen hat, Inhalte einzufüllen, wo es möglicherweise keine gab, oder wo es mehr Platz und Zeit benötigt hätte, um diese auszuführen.Beispiel 3.2

ist ein weiters Beispiel für die Unausgewogenheit, mit der der Kandidat in dieser Arbeit die Beschreibung seiner Maßnahmen vorgenommen hat. So wird, um offensichtlich der geplanten Länge dieser Abschnitte zu genügen, das Beispiel 3.2 Systemschutz durch die Java Virtual Machine nur in wenigen Zeilen beschrieben, obwohl hier zum ersten Mal ein wirklich formales Modell aus wissenschaftlicher Sicht, aber auch um den Leser entsprechend zu befriedigen, vorgeführt werden müßte, um die Mechanismen zu erläutern. Der Kandidat ist, dies sei ihm zugute gehalten, sicher mit der JAVA VM bis aufs Feinste vertraut. Er entläßt aber nicht nur den ungeübten Leser in die Situation der Nichtnachvollziehbarkeit, da auch in den Abschnitten 3.6 und 3.11, auf die verwiesen wird, keine Details ausgeführt werden. Bezüglich Abschnitt 3.4 wurden weiter oben bereits ausführliche Bemerkungen gemacht, wobei sich insbesondere für "bullet" 3 aus Subabschnitt 3.4.1 die Frage stellt, ob der Vorschlag der Einführung eines Risikos für den Angreifer, z.B. Strafandrohung, Hinterlegung von Pfand usw., vom Kandidaten als allgemeines Informatikkonzept angesehen wird.

Dabei ist nicht nachvollziehbar, warum der Kandidat hier nicht bemerkt, wie sehr er in der von ihm eingeführten Taxonomie verfangen ist,- (welche Rolle spielt der bedrohte Mensch?) und wie nötig eine Überarbeitung seines Konzeptes wäre.

Auch die Abschnitte 3.4.2 und 3.5 sind aus Sicht der Informatik nicht nachvollziehbar, wobei bezüglich Bemerkung 3.4 noch einmal exemplarisch darauf hingewiesen werden soll, wie hoch aufgrund einer schlagwortartigen Überschrift und einer eindrucksvollen Behauptung die Gefahr einer Irreleitung für ungeübte Leser ist, so dass es möglicherweise im technischen Bereich zu Fehlentscheidungen oder gar der Schädigung von Herstellern kommen kann. Die in Abschnitt 3.6 gegebenen Definitionen und Beispiele entsprechen ebenso wenig den wissenschaftlichen Grundsätzen der Informatik wie die Definition 3.18 und 3.21., mit denen nun zum wiederholten Male die Begriffe "kryptographisch" und "verschleiernd" eingeführt werden. Bisher handelte es sich um sprachliche Umschreibungen und keine Definitionen im eigentlichen Sinne, sondern eher um eine zirkuläre, wenn nicht gar selbstreferentielle Verweismethode, wobei sich insbesondere die Frage nach Verschleierungstechnik im Zusammenhang mit der gegenwärtig aktuellen Wasserzeichentechnologie stellt(siehe dazu: R.Anderson ed.: Information Hiding LNCS 1174 , Springer-Verlag, 1996. Diese Quelle hat der Kandidat nicht erwähnt. ).

Die Beispiele 3.9.1 liefern eine weitere Verwirrung von Begriffen, wobei insbesondere auch die Unsicherheit des Kandidaten über die Definition der Begriffe verdeckter und versteckter Kanal (vgl. die Seiten 25 und 106) zum wiederholten Male deutlich wird. Die Behauptung, die im zweiten Absatz unter "Nivellierung der Sicherungsmechanismen" gegeben wird, ist unbewiesen. Der Begriff der Unizitäts-Länge, der vorher schon in Fußnote 10 auf Seite 41 undefiniert benutzt wird, wird hier wieder ohne Definition benutzt,

wobei der Kandidat auf die ihm bekannten Stellen bei G.J.Simmons hätte verweisen müssen.

Der oberflächliche Stil drückt sich auch in der sprachlichen Gestaltung des nächsten Abschnitts aus. Mit Fachkauderwelsch allein kann eine wissenschaftliche Auseinandersetzung mit einem Thema nicht bestritten werden-, - ebensowenig wie mit unbewiesenen Lehrsätzen, wie sie etwa unter der Überschrift "Überflutung" des Angreifers auf Seite 87 zu finden ist. Die Tatsache, dass dieses sich möglicherweise mit der allgemeinen Lebenserfahrung deckt, ist noch keine Begründung für eine wissenschaftliche Auseinandersetzung mit dem Thema.

Die Abschnitte 3.10 und 3.11 enthalten weder Neues noch sind sie aus wissenschaftlicher Sicht nachvollziehbar, ebensowenig wie z.B. die in Abschnitt 3.12 gegebenen Beispiele 3.29 und 3.30: Während das Erstere wohl kaum zur Informatik zu rechnen ist, und vor allen Dingen auch nicht durch Zitate oder Herkunftsnachweise belegt ist, oder falls diese Idee neu sein sollte, in irgendeiner Weise technisch untermauert wird, ist die Beschreibung der Quantenkommunikation nicht nur oberflächlich und für die meisten Leser unverständlich, sondern auch nicht korrekt. Eine Auseinandersetzung mit den Originalquellen, die dem Kandidaten bekannt sind, aber im Literaturverzeichnis nicht zitiert werden, hätte hier das Schlimmste verhütet. Der in Beispiel 3.31 beschriebene Angriff auf RAID-Systeme wurde vom Betreuer während eines Arbeitsgesprächs u.a. mit dem Kandidaten entdeckt und im Rahmen eines eingeladenen Vortrages "Security in Electronic Publishing: Sicherheit ist mit Sicherheit eine Herausforderung für elektronische Zeitschriften und Bibliotheken" beim IuK-Workshop: "Wege in die Zukunft - Elektronische Zeitschriften II - International Symposium on Electronic Journals", Berlin, 16.02.1998 international vorgestellt und ins Netz gestellt wurde, was dem Kandidaten bekannt war. Hier fehlt ebenfalls ein Zitat im Literaturverzeichnis.

**Abschließende Bewertung zu Kapitel 3:**

Das in der Einleitung zu diesem Kapitel beschriebene Ziel, Sicherungsmethoden vorzustellen wurde nicht erreicht. Die vorgeschlagene Taxonomie erreicht nicht die notwendige Tiefe einer wissenschaftlichen Behandlung des Themas. Der wichtige Zusammenhang sowie die Unterscheidung zwischen Spezifikationstreue, Korrektheit, Effizienz und den verschiedenen Sicherheitsarten wird völlig unzureichend behandelt. Die diversen Szenarios dienen höchstens der drastischen Veranschaulichung der Problematik, konkrete Maßnahmen werden weder angegeben noch realisiert. Damit wird die Aufgabenstellung auch in diesem Kapitel aus system-und modelltheoretischer sowie informatischer Sicht nicht erfüllt.

**Kapitel 4** ist für den Referenten kaum verständlich. Hierzu trägt vor allen Dingen die vom Kandidaten postulierte, höchst fragwürdige Einführung von Schicht -8- Adressen, wie auf Seite 98 und in der Folge vorgeschlagen, bei. Die Korrektheit und Sinnhaftigkeit dieser Aussagen kann nur von Protokoll- und Netzwerkspezialisten beurteilt werden. Das Fehlen jeder formalen Beschreibung in Form von Sprachen,

Protokollen oder den nötigen Verifikationen zeigt jedoch unabhängig davon, dass der wissenschaftliche Standard der Informatik nicht erreicht wird. Das in Beispiel 4.3 beschriebene Unterlaufen der Schichtenstruktur im Bell-LaPadula-Modell mittels sogenannter verdeckter Kanäle (siehe dazu meine Bemerkung oben zu Seite 86) ist ein altes Beispiel ("covered channel", siehe dazu Butler Lampson: A Note on the Confinement Problem, CACM,16(10),pp.613-615,October 1973), das, wie die anderen Schwächen, die der Kandidat in seiner Fußnote auf Seite 106 erwähnt, nicht durch Literaturzitate belegt wird, wieweil er offensichtlich über diesen Kenntnisstand verfügt. Die unverständliche sprachliche Beschreibung von Beispiel 4.1 hätte z.B. durch ein Protokoll explizit den Standards der Informatik entsprechend algorithmisch gegeben werden müssen. Ähnliches gilt für die anderen Aussagen und Beispiele, wie beschrieben. Die Hektik, mit der dieses Kapitel erstellt zu sein scheint, drückt sich u.a. auch darin aus, dass dem Kandidaten, der sonst auf Rechtschreibung nach der jeweilig gültigen Norm Wert legt, auf Seite 96 im vorletzten Absatz den Satz nicht abgeschlossen hat und Zeilen darüber offensichtlich einen Begriff, für den ihm noch kein geeignetes Wort eingefallen ist, vorläufig schon einmal durch einen Stellvertreter (?) belegt hat.

Damit kommen wir zu **Kapitel 5**, dem nach erstem Anschein einzigen technischen Kapitel. Sieht man einmal von der politischen Orientierung, die durch die Überschrift deutlich wird, ab, ist die Frage, was die juristischen Zitate auf der Seite 119 aus Sicht dieser Dissertation bewirken sollen, ebensowenig wie die Beschreibung im einleitenden „Überblick" nach Kriterien der wissenschaftlichen Informatik nachvollziehbar ist. Der auf Seite 121 eingeführte Begriff des „Zensors", der - wenigstens in der Informatik - ein neuer *terminus technicus* wäre und für die weiteren Entwicklungen, insbesondere im Theorem 5.17 eine Rolle spielt, wird nicht exakt und auch sprachlich höchstens phänomenologisch eingeführt, wobei es der Kandidat versäumt hat, bei der Auflistung auf Seite 119 , Art.5(1) GG zu zitieren:..."*Eine Zensur findet nicht statt.*"

Abschnitt 5.2 beschreibt Grundlagen der Informationstheorie in einer Ausführlichkeit, die einer Einführungsvorlesung der Informationstheorie entspricht. Hier drückt sich wieder die oben schon erwähnte Unausgewogenheit in der Detaillierung dieser Arbeit deutlich aus. Der Kandidat scheint die Dinge, die ihm weniger vertraut sind oder deren formaler Herkunft er eine gewisse Wirkung nicht abzusprechen imstande ist, ausführlicher darstellen zu wollen, - in diesem Fall den Formalismus der bedingten Wahrscheinlichkeiten und Bayes-Regeln sowie der damit verbundenen relativierten Entropie- und Informationsbegriffe.

Hätte der Kandidat, solche Präzision bei der Beschreibung seiner diversen Beispiele, Protokolle und Systemspezifikationen den Standards der Informatik entsprechend angewandt, wären ihm viele Fehler und Oberflächlichkeiten sowie Unwissenschaftlichkeiten , wie bereits mehrfach erwähnt, nicht unterlaufen. Die Begeisterung des

Kandidaten, seine Theorien endlich mit (wohlgemerkt: altbekannten!) formalen Mechanismen untermauern zu können, drückt sich z.B. in der völlig überflüssigen Mitführung des Index a für die Basiskonstante des Logarithmus über den ganzen Abschnitt aus, obwohl er, wie in Definition 5.5 betont, davon ausgeht, dass es sich um die Zahl a=2 handelt.

Der Abschnitt 5.3 behandelt dann in weitgehend nicht nachvollziehbarer Weise und in ungewöhnlich schlechtem Stile die eigentliche Frage des Kapitels, nämlich der staatlichen Informationsüberwachung, mit einer Mischung aus metainformatischen Aussagen, die möglicherweise philosophischen und juristischen oder soziologischen Charakter haben, was vom Referenten aber im Rahmen dieses Gutachtens nicht beurteilt werden kann. Diese benutzt der Kandidat u.a., um aus seinem Theorem 5.17, welches die einzige Aussage dieser Dissertation mit einem eigenen, potentiell neuen wissenschaftlichen Resultat darstellt, völlig verwirrende Schlüsse zu ziehen.

Die dem Beweis zugrundeliegende Idee klingt zunächst bestechend einfach. Leider enthält der zugehörige Beweis 5.18 an entscheidender Stelle einen Fehler, auf den der Kandidat bereits im Mai 1998 vom Betreuer unter Bezugnahme auf den fundamentalen Shannon´schen Satz und seine Umkehrung hingewiesen wurde, den der Kandidat im Rahmen von Abs.5.2 nicht erwähnt und auch sonst nicht zitiert.

Zuallererst sind die Voraussetzungen, die der Kandidat in diesem Beispiel betrachtet, fast immer nicht erfüllt bzw technisch nicht zu erfüllen: Ein voll ausgenutzer Kanal endlicher Kapazität besitzt eben nach Definition als Kanalkapazität $c$ das Maximum des Transinformationsgehaltes, wie in Definition 5.12 beschrieben. Damit wäre Satz 5.17 noch nicht falsch, da eine falsche Voraussetzung jede Aussage zuläßt.

Leider ist der Kandidat bei der Ausnutzung der Kanalkapazität $c$ zunächst über den üblichen Denkfehler gestolpert, dass in diesem Fall $c$ als das Maximum aufgrund der Konvexität der beteiligten Optimierungsmengen definiert werden darf, obwohl $c$ im Allgemeinen nur als Supremum betrachtet werden kann. Die Zahl $c$ ist jedoch offensichtlich eine allgemeine reelle und keine rationale Zahl und kann, selbst wenn sie es sein sollte, in ihrer Bruchzerlegung in fast jedem Fall nicht exakt bestimmt werden,- es sei denn, es handele sich um theoretische Kanäle mit ganz besonderen garantierten Eigenschaften (siehe dazu auch McEliece: "The Theory of Information and Coding", Encyclopaedia of Mathematics, Bd. 3, 1997, Addison-Wesley, Publishing Company, S. 81). Der Vorschlag, genau mit der vollen Kapazität übertragen zu wollen, ist darüberhinaus aus Sicht der Umkehrung des Satzes von Shannon ( siehe dazu McEliece, ibid., p.126) nach der *rate-distorsion*-Theorie nicht haltbar. Ein Kanal endlicher Kapazität kann aber durch Nachrichten endlicher Längen durch Übertragungsraten der Form $k/n < c$ beliebig "gut" betrieben werden. In diesem Fall können natürlich zwischen $c$ und der durch das System beschriebenen

rationalen Rate *k/n* beliebig viele Brüche und somit höhere Raten größeren Nenners mit einer nach dem Shannon´schen Theorem beliebig kleinen Störrate liegen, so dass durch Einsatz eines Zensor-Vereinigungs-Automaten mit Shannon Codierung sehr wohl zusätzliche Bits übertragen werden können - unter Ausnutzung gerade des Widerspruchs, den der Kandidat zur *reductio ad absurdum* in seinem Beweis 5.18 nutzen will , obwohl der Betreuer den Kandidaten anläßlich der Vorabversion vom 30.04.1998 auf die Probleme mit dem Beweis dieses Satzes nachdrücklich hingewiesen hat.

N.B: Dies ist eine Art von *subliminal channels* , die der Kandidat weiter unten auf p.175 im finalen Abschnitt 5.7.3 kurz erwähnt.

Zugunsten des Kandidaten sollte bemerkt werden, dass die Kasuistik des Beweises mit einem hypothetischen Schaltkreis durchaus eine gewisse intellektuelle Eigenleistung darstellt, die dem Kandidaten durch seine langjährige Beschäftigung mit Simulationen im Bereich von Zero-Knowledge- Protokollen u.ä. geläufig sein dürfte. Die Vertrautheit mit dieser Art von Argumentation hat der Kandidat schon auf Seite 40 in Fußnote 9 gezeigt. Leider ist er jedoch seiner eigenen unpräzisen Arbeitsweise zum Opfer gefallen, da eben dieses Argument sich hier nicht zum Widerspruch benutzen läßt.

Daraus Schlußfolgerungen in positiver Richtung zu ziehen, die möglicherweise für die Analyse von neuen Typen von Kryptosystemen der gewünschten Art möglich sind, gelingt ihm nicht. Die Diskussion der Seite 134, in denen er versucht hat, einige von den Argumenten weiter auszuführen, ist eine Vermischung von mathematischen Grundsätzen, informatischen Prinzipien und möglicherweise juristischen Gedanken, wie auf Seite 134 im Zusammenhang mit den Fußnoten 6&7 ("Ein Schelm, wer...") angedeutet, und der Stolperstein, über den die wissenschaftliche Exaktheit seine Beweisführung leider ins Absurde gerät.

Es ist ferner zu bemerken, dass mit dem drittletzten Absatz auf der Seite 132 der Kandidat den genannten Vereinigungsautomaten, der vom Referenten als Beispiel für die Inkorrektheit des Argumentes gebracht wird, implizit erwähnt hat, wobei der Kandidat sich möglicherweise durch den unpräzisen Umgang mit dem Begriff Kaskadieren selbst behindert hat. Dieser Begriff wird später noch einmal in undefiniertem Sinne und irreführend benutzt (siehe dazu Seite 151).

Die Beschäftigung mit diesem Abschnitt ist möglicherweise selbstreferentiell im Rahmen dieser Dissertation zu sehen, wie in Bemerkung 5.19 auf Seite 135 geschehen, wo im letzten Absatz zu finden ist: "Fazit: Der Zensor ist nicht absolut auszuschließen, aber man kann es ihm beliebig schwer machen". Welche technischen ingenieurmäßigen oder wissenschaftlichen Kosequenzen daraus zu ziehen sind, überläßt der Kandidat offensichtlich dem Referenten bzw. dem Leser der Arbeit. Ein weiterer Versuch, algorithmische Details über die obenerwähnten in die Arbeit hineinzubringen, wird auf Seite 138 unternommen, wobei sich die Frage stellt, wieso hier plötzlich eine semiformale Algorithmen-Beschreibung für eine völlig triviale Methode gewählt wird, wobei bei anderen wesentlich komplizierteren

und nach wissenschaftlichen Grundsätzen zu beweisenden Protokollen, wie mehrfach aufgelistet, genau diese Vorgehensweise nicht beschritten wird. Die Skurrilität der Argumentationsweise, gegen die der Kandidat sich mit seinen verbalen Entwürfen zu schützen versucht, ohne daraus eine technische Implementierung herzuleiten oder gar zu realisieren, wird in der Bemerkung 5.23 unter der Überschrift: "Gefahr falscher Verdächtigung" für jeden auch fachfremden Leser deutlich.

Abschnitt 5.4 beschäftigt sich mit Beschränkungen der Schlüssellänge im Hinblick auf das Problem der staatlichen Informationsüberwachung . Angesichts der Aufmerksamkeit die diesem Thema international gewidmet wird, ist die Auflistung der Suchaufwände in Tabelle 5.1 ausgesprochen irreführend und gefährlich, weil ungeübte Leser daraus möglicherweise den falschen Schluß ziehen könnten, mit bestimmten Kryptoverfahren auf Jahrtausende sicher zu sein. Der Kandidat erwähnt nicht, in welcher Form durch das Moore´sche Gesetz für die Technologieentwicklung die Rechnerleistungen relativiert werden müssen und wie gefährlich die Sicherheitsbeurteilung dieser Algorithmen ist. Es fehlt an dieser Stelle ein genauer Verweis auf die Quellen und die Voraussetzungen, unter denen diese Abschätzungen gemacht wurden, womit die Wissenschaftlichkeit und nicht nur die Bedeutung dieser Aussage aufs Höchste fragwürdig ist.

Die folgenden informationstheoretischen Betrachtungen entstammen wiederum den Einführungskursen der Informationstheorie bzw. der Kryptologie. Die Blockschaltbilder für die verschiedenen Modes von Chiffrierverfahren sind ebenfalls seit zwei Jahrzehnten Stand des Wissens und dienen nicht der Vorbereitung der Definition der sogenannten schlüssellosen Chiffre, der beim ersten Lesen einer gewissen Attraktivität nicht entbehrt. Leider ist die Definition bei genauerem Hinsehen unsinnig und nicht an der Realität orientiert, da als Qualitätskriterium für die Chiffre nur der Lawineneffekt aufgezählt wird. Der Kandidat übersieht dann vor allen Dingen die nötige Erweiterung der Definition auf eine probabilistische Abbildung, deren Inverse im Rahmen von entropischen Überlegungen wohl definiert sein könnte, wie dies etwa bei dem von ihm weiter oben erwähnten Jefferson Wheel Cipher (siehe Seite 128) der Fall ist. Leider ist das von ihm gegebene Zitat der populären Literatur entnommen, so dass weitere Untersuchungen entsprechend der o.g.Aufgabenstellung über den informationstheoretischen Hintergrund dieses Verfahrens, das möglicherweise eine der bedeutendsten Erfindungen eines der größten Köpfe der Menschheit darstellt, nicht erwähnt wurden.

Die im Beispiel 5.26 beschriebene schlüssellose Chiffre wird weder formal algorithmisch eingeführt, noch auf die Kriterien aus Definition 5.25 hin untersucht und genügt damit allein schon nicht den wissenschaftlichen Ansprüchen, die im Rahmen des Gebietes anzulegen sind. Darüber hinaus hat dieses Verfahren einen inhärenten, möglicherweise großen Designfehler, da aus dem Schaltbild in Abbildung 5.5 deutlich wird, dass der Kandidat auf, wenn auch implizitem Wege, eine Key-Feedback-Schaltung zurückgreift, - gegen

die Regeln der Kunst, was dem Kandidaten auch aus der eigenen Arbeit im Europäischen Institut für Systemsicherheit bekannt sein müßte.

Da durch die Iteration nach diesem Verfahren bei einfacher Anwendung de Data Encryption Standard eine nicht vernachlässigbare Schlüsselverkürzung stattfindet, ist ohne eine genauere (experimentelle!) Untersuchung keine wissenschaftliche Aussage darüber möglich, ob dieses Verfahren den benötigten Sicherheitsstandards entspricht.

Leider hat der Kandidat trotz einer möglicherweise guten Idee die Gelegenheit nicht wahrgenommen, im Rahmen seiner Tätigkeit am Institut des Betreuers die dort vorhandenen Ressourcen für ähnliche statistische Untersuchungen zu nutzen, wozu er vom Betreuer über Jahre hinweg nachhaltig aufgefordert wurde. Somit kann auch diesem Vorschlag keine wissenschaftliche Bedeutung beigemessen werden.

Der Vorschlag aus Beispiel 5.31, eine Feed-Forward-Schaltung im Cipher Block Chaining Mode durchzuführen, liest sich bei erstem Hinsehen als interessante Idee. Der Kandidat stellt jedoch in der Fußleiste zur Abbildung von 5.6 selbst fest, dass die von ihm vorgeschlagene Schaltung keinen Sicherheitsvorteil bringt, und macht dann die leider unbewiesene Behauptung, die Stärke des Verfahrens liege in der Kaskadierung (s.o.). Die Definition von Kaskadierung bleibt hier ebenso aus, wie eine Sicherheitsuntersuchung, der einzige Vorschlag, der hier nunmehr in Bemerkung 5.32 folgt, ist ein kaum verständlich beschriebenes Verfahren, das anschließend mit einer Aufwandsrekurrenz analysiert wird, obwohl keine formale Beschreibung oder ein formaler Beweis vorliegt, wie er im Rahmen einer wissenschaftlichen Arbeit durchgeführt werden müßte.

Da es sich jedoch hier nicht um ein Verfahren handelt, dessen Effizienz und Korrektheit ausschließlich zur Diskussion stehen, sondern um einen sicherheitstechnischen Vorschlag, ist es aufgrund des Fehlens jeder sicherheitstechnischen Analyse bis hin zu den dringend notwendigen mathematischen oder experimentellen Untersuchungen unmöglich, auch diesen potentiell ideenreichen Beitrag im Rahmen einer Dissertation den Standards unserer Fakultät gemäß entsprechend würdigen zu können.

Angesichts der Aufgabenstellung der Arbeit wäre die genaue Untersuchung des vorgeschlagenen Feed-Forward-Prinzips allein schon deswegen interessant gewesen, da im Rahmen des Third Generation Partnership Program der USA, der EU und Japans ( dem next-generation -Mobiltelefonie-Nachfolgeprogramm , siehe dazu: http://www.3gpp.org) die Problematik solcher Feed-Forward-Mechanismen erkannt wurde und Ergebnisse darüber durchaus in die Untersuchung von Kollisionverhalten bzw. Cyclingverhalten solcher Chiffren eingehen müssen, aber bisher nicht beweisbar waren.

Die folgenden Überlegungen über Offenlegung des Schlüssels etc. sind im Wesentlichen wieder verbaler Natur und im Rahmen einer wissenschaftlichen Dissertation nicht nachvollziehbar. Die Aussage auf Seite 158, dass ein Datenkompressionsverfahren "immer nur für ein

bestimmtes statistisches Modell" ausgelegt sei, sollte dem Kandidaten eigentlich nicht entruscht sein, da er aufgrund seiner Arbeit und ihrer ursprünglichen Aufgabenstellung, (s.o.) angesicht der engen Einbindung in Arbeit des Instituts nicht nur mit den in der Tat quellabhängigen Kompressionsverfahren, wie etwa bei MPEG4, sondern auch mit den quellunabhängigen bahnbrechenden Verfahren LZ oder MTF vertraut ist und somit festgestellt haben müßte, dass seine Aussage in dieser Allgemeinheit falsch ist.

Die abschließenden Seiten sind im Wesentlichen wieder verbale Auseinandersetzungen, die mit unverständlichen oder populistischen Modellen untermauert werden, wie z.B. das Beispiel 5.33 über die Telefonverschlüsselung. Hätte der Kandidat diese Idee, die bereits zum Beginn seiner Mitarbeit am E.I.S.S. diskutiert wurde, benutzt, um die vom Betreuer vorgeschlagene Hardwarerealisierung einer solchen Schaltung zu demonstrieren, läge zumindest eine technische Realisierung im Rahmen der Arbeit vor, die einen technisch wissenschaftlichen Charakter einer Dissertation ergeben würden.

Spätestens nach dem Studium der Seite 173 wird dem Leser mit Beispiel 5.40 "*Waschmaschine und Käsekuchen*" klar gemacht, welche wissenschaftlichen Ziele der Autor mit diesem Text verfolgt.

Die Ausführungen in Abschnitt 5.6.3 müßten, um verständlich und bewertbar zu sein, algorithmisch untermauert und dem Stil einer Dissertation an unserer Fakultät entsprechend formalisiert sein. Das Gleiche gilt für das Beispiel in Abschnitt 5.6.4. Die einzige hier zu findende formale Auseinandersetzung im Bereich der Signatursicherheit ist eine Wiederholung des seit 15 Jahren bekannten ElGamal-Signaturschemas. Daraus zieht der Kandidat keine neuen technischen Schlüsse. In dem in Abschnitt 5.7.2 gegebenen Beispiel wird nur die bekannte Lücke im naiven Diffie-Hellman-Schlüsselaustauschprotokoll wiedergegeben. Statt an dieser Stelle einen konkreten Protokollverbesserungsvorschlag in formaler mathematisch nachvollziehbaren Art und Weise vorzustellen, fällt der Kandidat auch hier wieder auf eine verbale Beschreibung zurück, so dass eine Eigenleistung aus informatischer Sicht nicht festzustellen ist.

Der letzte Abschnitt 5.7.3 schließlich beschäftigt sich mit der Simmons´schen Theorie des subliminal channels, wobei, wie oben angemerkt, nicht alle Zitate angegeben werden sind, obwohl diese dem Kandidaten bekannt sind: Der Kandidat hätte den Artikel aus dem IEEE Journal on Selected Areas in Communications (Mai 1998) zitieren müssen, in dem die Artikel von Gustavus Simmons auf den Seiten 452 und 463 ihm einige Einsicht in die von ihm untersuchten Fragestellung vermittelt hätten, nachdem er vom Betreuer anläßlich der Vorabversion vom 30.04.1998 auf den Zusammenhang mit Theorem 5.17 hingewiesen wurde. Leider besteht dieser Abschnitt nur aus einer Seite Text und zieht keinerlei konstruktive Rückschlüsse gerade im Rückblick auf die Auführungen in Beweis 5.18. bzgl. der wesentlichen Eigenschaften, die den Simmons´schen Entdeckungen zu entnehmen sind, wie sie etwa im Handbook of Applied Cryptography, CRC Press, 1997 auf Seite 485 in kurzer, aber exakter Weise beschrieben werden.

**Abschließende Bewertung zu Kapitel 5:**

Zusammenfassend ist zu sagen, dass dieses Kapitel aus der interessanten und hochaktuellen Beschäftigung mit dem so genannten Kryptoverbot entstanden ist. Der Betreuer hat den Kandidaten ermutigt, seine Überlegung in diesem Bereich auszuarbeiten und zu formalisieren. Leider hat der Kandidaten sich nicht an die Aufgabenstellung bezüglich der mathematischen Beschreibung , technischen Implementierung und experimentellen Untersuchungen gehalten, sondern entgegen den Empfehlungen des Betreuers die Verwendung von durchaus verfügbaren Resultaten aus seiner wissenschaftlichen Mitarbeit am Institut des Betreuers weitgehend vermieden. Der Versuch des Kandidaten, auf wissenschaftliche Art und Weise zu zeigen, dass solche Verbote nicht durchsetzbar sind, ist mit seinen Methoden leider gescheitert. Andere Methoden hat der Kandidat, obwohl sie ihm zur Verfügung standen, nicht für einen Beweis genutzt. Der entscheidende Fehler, der im Zusammenhang mit Beweis 5.18 detailliert vom Referenten aufgezeigt wird, wurde dem Kandidaten bereits Anfang Mai 1998 im Rahmen der Dissertation des Entwurfes vom 30.04.1998 erläutert, aber leider nicht korrigiert. Auch die anderen aufgezeigten Fehler bzw. Lücken bei den vorgeschlagenen Kryptoverfahren sind von grundsätzlicher Natur. Aufgrund der vorliegenden Form des Kapitels ist ein wissenschaftlich begründete Anspruch nicht erkennbar, wobei die Gefahr bei Fehlinterpretation dieses Textes durch Nichtfachleute unübersehbar ist, auf die mit einem Wort des Kandidaten hingewiesen wird: "Zur Risiken und Nebenwirkungen lesen Sie die Systemspezifikation oder fragen Sie Ihren Informatiker!" (Zitat S. 114).

**Kapitel 6** schließt mit der Bemerkung, daß die Ergebnisse dieser Arbeit die Grundlage eines Gutachtens für den Deutschen Bundestag darstellen, auf das der Kandidat in seiner Literaturliste mit [44] verweist . Dieses Zitat ist unvollständig und inkorrekt, da der Kandidat mitnichten der alleinige Autor ist. Dieses Gutachten wurde durch die intensive Arbeit eines Teams von Proponenten und Opponenten erstellt, die die diversen Szenarien für ein solch wichtiges Gutachtens nach den Regeln der Systemsicherheit bearbeitet haben. Im Entwurf vom 30.04.1998 waren diese Zitate noch korrekt vorhanden und sind erst in der eingereichten Version verändert worden, ebenso wie wichtige andere Zitate, die der Kandidat im Rahmen seiner Arbeit benutzt hat, gestrichen wurden, wozu insbesondere Materialien gehören, die dem Kandidaten vom Betreuer zur Bearbeitung der vorgegebenen Themen überlassen wurden. Diese Auslassungen sind somit als mutwillig zu beurteilen und nicht als Flüchtigkeitsfehler zu entschuldigen. Damit hat der Kandidat auch an dieser Stelle den wissenschaftlichen Grundsätzen, die unsere Fakultät bei Promotionen voraussetzt, nicht entsprochen.

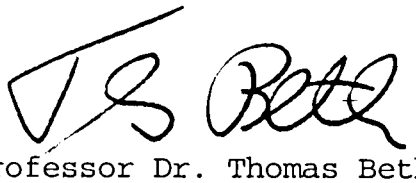
## Bewertung der Arbeit

Insgesamt ist festzustellen, dass es sich um eine unfertige Arbeit handelt, die in den vom Gutachter nachvollziehbaren Teilen erhebliche Ungenauigkeiten und Fehler enthält. Eine korrekte Beweisführung für die gemachten Aussagen und Behauptungen in theoretischer oder experimenteller Art nach mathematisch-naturwissenschaftlichen Grundsätzen ist nicht zu erkennen. Algorithmen, Neuentwicklungen oder Ideen mit wissenschaftlich wesentlicher Erfindungshöhe sind nicht realisiert worden. Somit liegt auch eine ingenieurmäßige Leistung nicht vor.

Die Zusammenfassung und Einordnung der Dissertation, die in Kapitel 6 vom Kandidaten vorgenommen wird, behauptet im dritten Absatz: *"Die vorliegende Arbeit ist damit nicht völlig abstrakt, sondern zielt klar auf die tatsächliche Erstellung realer Systeme ab"*. Angesichts des Titels: "Entwurfskriterien und Methoden zur Erlangung von Kommunikationssicherheit" ist nach Lesen dieser 177 Seiten festzustellen, dass es dem Kandidaten weder gelungen ist, die Augabenstellung den Standards der Fakultät für Informatik gemäß zu bearbeiten, obwohl er vom Betreuer nachdrücklich über lange Zeit dazu angehalten wurde und langmütige Unterstützung erfahren hat, noch hat er das selbstgewählte Ziel, mit seiner Dissertation Beiträge zur Erlangung von Sicherheit ( d.h. von garantierter, vorher noch nicht erreichter Qualität) machen zu wollen, erreicht. Auch partielle Ergebnisse oder dem Thema widersprechende Unmöglichkeitsbeweise, die als Ergebnis einer wissenschaftlichen Dissertation durchaus gerechtfertigt sind, liegen nicht vor. Somit ist trotz der oben zitierten Behauptung nicht nur das Thema der Arbeit verfehlt. Der Gehalt dieser Dissertation, die der Kandidat entgegen den mit dem Betreuer besprochenen Aufgabenstellungen und Hinweisen vorzulegen sich entschieden hat, reicht für eine Promotion an der Fakultät für Informatik nicht aus.

Die Bewertung der Arbeit kann leider mit der einleitenden Bemerkung des Kandidaten (siehe p.1) zusammengefaßt werden: es "*.... ist aber kein adäquater Fortschritt beim Entwurf der Analyse und der Beschreibung von Sicherheitssystemen zu bemerken.*"

**Zusammenfassend** kommt der Betreuer somit zu dem eindeutigen Schluß, dass er der Fakultät die Annahme dieser Arbeit als Dissertation im Fach Informatik an der Fakultät für Informatik der Universität Karlsruhe **nicht empfehlen** kann.



Professor Dr. Thomas Beth
(Referent)

14.Juni 2000