



Hochschule für Telekommunikation Leipzig
University of Applied Sciences

Secure Hash Algorithm Familie – Die Bedeutung der Kollisionssicherheit von kryptologischen Hashalgorithmen

Studienarbeit
von

Chi Trung Nguyen

an der Hochschule für Telekommunikation Leipzig
in der Studienrichtung Wirtschaftsinformatik

Erstgutachter:

Prof. Dr. Jens Wagner

Bearbeitungszeit: 11.Juni 2012 – 11.Juli 2012

Ich erkläre hiermit, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.

Karlsruhe, den ???. ?????? 201?

Inhaltsverzeichnis

1 Einleitung	1
1.1 Zielsetzung der Arbeit	1
1.2 Gliederung der Arbeit	1
2 Grundlagen	3
2.1 Abschnitt 1	3
2.2 Abschnitt 2	3
2.3 Verwandte Arbeiten	3
3 Analyse	5
3.1 Anforderungen	5
3.2 Existierende Lösungsansätze	5
3.3 Weiterer Abschnitt	5
3.4 Zusammenfassung	7
4 Entwurf	9
4.1 Abschnitt 1	9
4.2 Abschnitt 2	9
4.3 Zusammenfassung	11
5 Implementierung	13
5.1 Abschnitt 1	13
5.2 Abschnitt 2	13
6 Evaluierung	15
6.1 Abschnitt 1	15
6.2 Abschnitt 2	15
6.3 Zusammenfassung	15
7 Zusammenfassung und Ausblick	17

1. Einleitung

Hinweis: In die Einleitung gehört die Motivation und Einleitung in die Problemstellung. Die Problemstellung kann in der Analyse noch detaillierter beschrieben werden.

Bla fasel...

1.1 Zielsetzung der Arbeit

Was ist die Aufgabe der Arbeit?

Bla fasel...

1.2 Gliederung der Arbeit

Was enthalten die weiteren Kapitel?

Bla fasel...

2. Grundlagen

Die Grundlagen müssen soweit beschrieben werden, dass ein Leser das Problem und die Problemlösung versteht. Um nicht zuviel zu beschreiben, kann man das auch erst gegen Ende der Arbeit schreiben.

Bla fasel...

2.1 Abschnitt 1

Bla fasel...

2.2 Abschnitt 2

Bla fasel...

2.3 Verwandte Arbeiten

Hier kommt „Related Work“ rein. Eine Literaturrecherche sollte so vollständig wie möglich sein, relevante Ansätze müssen beschrieben werden und es sollte deutlich gemacht werden, wo diese Ansätze Defizite aufweisen oder nicht anwendbar sind, z. B. weil sie von anderen Umgebungen oder Voraussetzungen ausgehen.

Bla fasel...

3. Analyse

In diesem Kapitel sollten zunächst das zu lösende Problem sowie die Anforderungen und die Randbedingungen einer Lösung beschrieben werden (also nochmal eine präzisierte Aufgabenstellung).

Dann folgt üblicherweise ein Überblick über bereits existierende Lösungen bzw. Ansätze, die meistens andere Voraussetzungen bzw. Randbedingungen annehmen.

Bla fasel...

3.1 Anforderungen

Anforderungen und Randbedingungen . . .

3.2 Existierende Lösungsansätze

Hier kommt eine ausführliche Diskussion von „Related Work“.

Bla fasel...

3.3 Weiterer Abschnitt

Bla fasel... hat auch schon [?] gesagt und [? ? ?] sollte man mal gelesen haben.
Abbildung 3.1 auf S. 6 sollte man sich mal anschauen.

Abbildungen sollten möglichst als EPS (Encapsulated Postscript) bzw. PDF eingebunden werden. Zur Erzeugung sauberer EPS-Dateien empfiehlt sich das Tool `ps2eps` zur Nachbearbeitung von Postscript-Dateien. Mit `epstopdf` kann dann eine PDF-Datei zum Einbinden erzeugt werden.

Abbildung 3.1: Testabbildung

Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext
Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext
Blindtext Blindtext Blindtext Blindtext

3.4 Zusammenfassung

Am Ende sollten ggf. die wichtigsten Ergebnisse nochmal in *einem* kurzen Absatz zusammengefasst werden.

4. Entwurf

In diesem Kapitel erfolgt die ausführliche Beschreibung des eigenen Lösungsansatzes. Dabei sollten Lösungsalternativen diskutiert und Entwurfsentscheidungen dargelegt werden.

Bla fasel...

4.1 Abschnitt 1

Bla fasel...

4.2 Abschnitt 2

Bla fasel...

Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext
Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext
Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext

Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext
Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext
Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext
Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext

Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext
Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext
Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext
Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext
Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext
Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext
Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext Blindtext
Blindtext Blindtext Blindtext Blindtext

4.3 Zusammenfassung

Am Ende sollten ggf. die wichtigsten Ergebnisse nochmal in *einem* kurzen Absatz zusammengefasst werden.

5. Implementierung

Bla fasel...

5.1 Abschnitt 1

Bla fasel...

5.2 Abschnitt 2

Bla fasel...

6. Evaluierung

Hier kommt der Nachweis, dass das in Kapitel 4 entworfene Konzept auch funktioniert. Leistungsmessungen einer Implementierung werden auch immer gerne gesehen.

Bla fasel...

6.1 Abschnitt 1

Bla fasel...

6.2 Abschnitt 2

Bla fasel...

6.3 Zusammenfassung

Am Ende sollten ggf. die wichtigsten Ergebnisse nochmal in *einem* kurzen Absatz zusammengefasst werden.

7. Zusammenfassung und Ausblick

Bla fasel...

(Keine Untergliederung mehr!)

