

## Echtzeit Wasserzeichensystem für Sprache

Name des Diplomanden/der Diplomandin	Mario Jurcevic, Markus Gloor
Name des Examinators/der Examinatorin	Prof. Dr. Guido M. Schuster
Vertiefungsrichtung	Digitale Signalverarbeitung

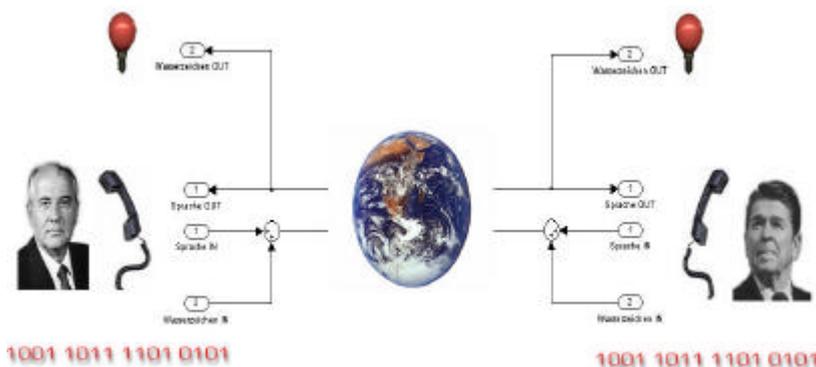
### Kurfassung der Diplomarbeit

#### Motivation

Es soll ermöglicht werden, dass Telefongespräche welche aufgezeichnet werden, später nicht manipuliert werden können. Eine Anwendung für diese Technologie findet man bei einer Bank, welche Aufträge über das Telefon entgegen nimmt. Es ist später nicht möglich mit einer manipulierten Aufzeichnung des Gesprächs zu behaupten, dass ein anderer Auftrag gegeben wurde.

#### Lösungsansatz:

Die Idee des Wasserzeichens in einer Banknote lässt sich auch auf Sprache anwenden. In diesem Fall versteht man unter einem Wasserzeichen eine digitale Codesequenz, also eine bestimmte Folge von Nullen und Einer.



Der Sender mischt dem Sprachsignal ein unhörbares Wasserzeichen bei. Dieses Mischsignal wird nun über einen Telefonkanal gesendet. Obwohl das Wasserzeichen für einen Menschen unhörbar ist, kann es mit dem entwickelten Verfahren am anderen Ende der Leitung im Empfänger wieder detektiert werden.

Als Wasserzeichen wird ein Zähler verwendet. Damit kann später festgestellt werden, ob eine Aufzeichnung zusammengeschnitten wurde, oder ob es eine

Originalaufzeichnung ist. Damit der zusammengeschnittenen Aufzeichnung nicht einfach ein neues Wasserzeichen aufgespielt werden kann, wird das Originalwasserzeichen mit dem 3DES Verfahren verschlüsselt. Am Empfänger kann diese Verschlüsselung nur mit dem selben Schlüssel wie der Sender benutzt hat, entschlüsselt werden. Auf der Leitung erscheint nun ein zufällig aussehendes Wasserzeichen, welches nicht mehr ohne weiteres reproduziert werden kann. Natürlich müssen Sender und Empfänger den gleichen Schlüssel benutzen und dieser wird mit dem Diffie Hellmann Verfahren automatisch erstellt.