

# **Online-Wahlen**

## und die Forderung nach zeitlich unbegrenzt geheimen Wahlen

**Melanie Volkamer**

**Robert Krimmer**

**Working Paper Series on  
Electronic Participation  
and Electronic Voting  
Nr. 2/2006**

**Editor:  
E-Voting.CC: Competence Cen-  
ter for Electronic Participation  
and  
Electronic Voting**

**[www.e-voting.cc/topics/wp/](http://www.e-voting.cc/topics/wp/)**

 ***e-voting.cc***



# Online- Wahlen und die Forderung nach zeitlich unbegrenzt geheimen Wahlen

**Melanie Volkamer**

DFKI GmbH  
Stuhlsatzenhausweg 3  
D-66123 Saarbrücken, Germany  
[volkamer@dfki.de](mailto:volkamer@dfki.de)

**Robert Krimmer**

E-Voting.CC:  
Kompetenzzentrum für Elektronische Partizipation und Elektronische Wahlen  
Liechtensteinstraße 143/3  
A-1090 Vienna, Austria  
[r.krimmer@e-voting.cc](mailto:r.krimmer@e-voting.cc)

## Abstract

Die Diskussionen bezüglich einer möglichen Einführung von Online-Wahlen, insbesondere von remote Online-Wahlen, wird von der Problematik der geheimen Stimmabgabe bei gleichzeitiger eindeutiger Authentifizierung, angeführt. Dabei interpretieren vor allem Juristen den Wahlrechtsgrundsatz der geheimen Wahl, als zeitlich unbegrenzte Forderung. Dies kollidiert aber mit dem Einsatz von asymmetrischen oder hybriden Verschlüsselungsverfahren zur Sicherung der Stimme bei der Übertragung. Hier kann nicht gewährleistet werden, dass einzelne oder gar alle Stimmen in einigen Jahren entschlüsselt werden können. Dieser Beitrag untersucht an den drei bekannten Protokollklassen, welches Angreiferpotential dazu führt, die geheime Wahl zu verletzen. Der Aspekt der geheimen Wahl wird dabei aufgespaltet: Zunächst einmal wird analysiert, ob und wenn ja wie der Angreifer selbst die geheime Wahl brechen kann und anschließend, ob das jeweilige System ihm eine Möglichkeit bietet, diese Erkenntnis aus gegenüber dritten zu beweisen.

## Keywords

**Wahlen, E-Voting,  
Unbegrenzte Geheimhaltung**

*Dieser Beitrag wurde beim Internationalen Rechtsinformatik Symposium in Wien im Februar 2006 präsentiert.*

# 1. Einleitung

Auf den ersten Blick scheinen Online-Wahl nichts weiter als eine weitere Internet-Anwendung neben Homebanking und eBay zu sein: man meldet sich an einem Server an, authentifiziert sich und gibt seine Stimme über eine gesicherte Verbindung ab. Es existiert allerdings ein entscheidender Unterschied: Während bei den bekannten Internetanwendungen die zur Sicherung der Verbindung eingesetzten Verschlüsselungsverfahren nur eine gewisse Zeitspanne sicher sein müssen, so wird bei Wahlen insbesondere im Zusammenhang mit Online-Wahlen gefordert, dass die Stimme dauerhaft – also zeitlich unbegrenzt – geheim bleiben muss („Die Entscheidung des Wählers darf nie auf ihn zurück geführt werden können“ [1]). Und genau hier liegt aus juristischer Sicht der Grund für das derzeitige Ausbleiben eines flächendeckenden Einsatzes von Online-Wahlen: Es kann derzeit nicht garantiert werden, dass heute als sicher geltenden Verschlüsselungsverfahren wie RSA mit 2048 Bit auch zukünftig nicht entschlüsselt werden. Mit einer entsprechenden Rechenleistung sind all diese Algorithmen zu brechen bzw. einzelne Nachrichten mittels Brute-Force entschlüsselbar. Es besteht damit die Gefahr, dass verschlüsselte Stimmen, die bei aktuellen Wahlen mitgelesen werden, in der Zukunft entschlüsselt werden können.

Da wir bei Online-Wahlen in der Regel davon ausgehen, dass das Internet als Kommunikationsmedium eingesetzt wird und dieses beliebig abgehört werden kann, ist zu untersuchen, ob ein Angreifer, der die gesamte Kommunikation mitliest in der Zukunft die geheime Wahl verletzen kann. Gegenstand der Analyse ist dabei nicht die Sicherstellung der geheimen Wahl bei der Stimmabgabe und während der Wahlperiode. Der Angreifer hat dabei nur Zugang zu den Datenpaketen auf dem Netz, arbeitet aber weder mit einem Wähler noch mit einem der Wahlserver zusammen um zusätzliche Informationen zu erhalten.

Dieser Beitrag diskutiert zunächst das Angriffsziel, den Hintergrund und die Auswirkungen einer Offenlegung einzelner Wählerstimmen einige Zeit nach der Wahl - insbesondere auch dann, wenn der Angreifer seine gewonnene Erkenntnis nicht beweisen kann. Anschließend wird die Sicherstellung der geheimen Wahl bei den traditionellen Wahlformen (papierbasierte Präsenzwahl und Distanzwahl in Form der Briefwahl)

untersucht, um später einen Vergleich zwischen Online-Wahlen und traditionellen Wahlen bzgl. der Sicherstellung der geheimen Wahl zu ermöglichen. Anschließend werden für die bekannten Klassen von Online-Wahlprotokollen die Angriffszenarien beschrieben und ausgewertet. Bei der Auswertung wird der Informationsgehalt durch die Auswertung der erspähten Daten untersucht. Im Vordergrund steht dabei die Beweiskraft gegenüber Dritten, dass eine bestimmte entschlüsselte Stimme eindeutig einem Wähler zugeordnet werden kann. Am Ende werden die Ergebnisse ausgewertet und Empfehlungen für die Konstruktion von Wahlprotokollen im Hinblick auf eine zeitlich unbegrenzte geheime Wahl gegeben.

## 2. Hintergrund des Grundsatzes der geheimen Wahl

Bereits im Grundgesetz sind die fünf Wahlrechtsgrundsätze einer freien, allgemeinen, unmittelbaren, gleichen und geheimen Wahl verankert und gelten damit für alle demokratischen Wahlen. Der Wahlrechtsgrundsatz der geheimen Wahl bedeutet, dass nur der Wähler vom Inhalt seiner Wahlentscheidung Kenntnis nehmen kann. Der Inhalt darf damit keiner anderen Person bekannt werden. Dieser Wahlrechtsgrundsatz verpflichtet die Wahlverantwortlichen die Wahl so zu gestalten, dass unbekannt bleibt, wer wie gewählt hat [2]. Die zentrale Funktion der geheimen Wahl liegt darin die freie Wahl zu gewährleisten. Der Wähler kann seine Stimme nur dann ohne (indirekten) Zwang abgeben, wenn er sicher sein kann, dass seine Stimme dauerhaft geheim bleibt.

Online-Wahlen stellen an vier Stellen eine Gefährdung für die geheime Wahl dar: Einmal besteht ähnlich wie bei der Briefwahl die Gefahr, dass der Wähler bei seiner Stimmabgabe beobachtet wird [Für eine ausführliche Diskussion siehe 3]. Des Weiteren kann der Rechner des Wählers mit Malware infiziert sein, die die Stimme vor dem Verschlüsseln mitliest und dem Angreifer im Klartext zu schickt. Letztere ist dabei der Punkt, der noch am wenigsten untersucht ist und daher die Schwachstelle jedes Verfahrens darstellt. Eine weitere Gefahr verbirgt sich in den eingesetzten Servern, deren Systemadministratoren beispielsweise zu-

sammenarbeiten könnten, um Stimme und Wähler zusammenzuführen. Dieser Gefahr wird derzeit organisatorisch behandelt, beispielsweise durch die Anwendung des Vier-Augen-Prinzips für die Zugangskontrolle. Die vierte Möglichkeit die geheime Wahl zu verletzen stellt die Kommunikation zwischen Wählern und Servern dar, da diese einfach vom Angreifer abgehört werden kann. Untersuchungsgegenstand dieses Beitrags ist die letzte Gefahr. Der Schwerpunkt liegt hierbei auf der Tatsache, dass die geheime Wahl das gesamte Wahlverfahren umgreift und damit auch nach der Wahl seine Gültigkeit behält [4, S. 169].

Der Hintergrund für einen Angreifer, die Stimme nach der eigentlichen Wahl zu ermitteln, kann entweder der sein, dass er während der Wahl einzelne Wähler zwingt ihre Stimme auf eine bestimmte Weise abzugeben, indem er ihnen droht das später nachzuprüfen oder aber weil er in die Medien kommen möchte, in der beweist, dass das Online-Wahl-System unsicher ist, weil er von bekannten Persönlichkeiten die Stimme nachweislich entschlüsseln kann. Diesen Angriff zwecks Stimmenkaufs durchzuführen ist denkbar aber nicht besonders wahrscheinlich, da der Käufer erst weit in der Zukunft feststellen könnte, ob sich die Wähler daran gehalten haben und ihnen dann erst ihre Stimme bezahlen würde.

### **3. Analyse der traditionellen Wahlformen**

Der Ablauf bei der traditionellen Wahl sieht wie folgt aus: Die im Wahllokal in einer Wahlkabine ausgefüllten Stimmzettel, werden vom Wähler gefaltet in eine Urne geworfen. Diese stellt nach §33 Abs. 1, S.2 des Bundeswahlgesetzes [BWG] eine Einhaltung des Wahlgeheimnisses sicher. Die Wahlbriefumschläge - bestehend aus Wahlumschlag und Wahlschein mit den Wählerangaben - werden nach §66 Abs. 1 der Bundeswahlordnung [BWO] zunächst vom Briefwahlvorstand geöffnet, um Wahlschein und Wahlumschlag zu entnehmen. Letzterer wird nach der Wahlberechtigungsprüfung im Hinblick auf die Gültigkeit des Wahlscheins ungeöffnet in eine Urne geworfen.

Diese sich jeweils in der Urne befindenden Stimmzettel sind auf den ersten Blick ano-

nym, da keine persönlichen Angaben des Wählers darauf stehen. Aber, jeder Stimmzettel könnte trotzdem dem Wähler zugeordnet werden, denn auf jedem Stimmzettel wird sich der Fingerabdruck des Wählers befinden. D.h. auch wenn eine offensichtliche Zuordnung zwischen Stimmzettel und Wähler nicht möglich ist, kann dies über den Fingerabdruck auch nach der Wahl noch geschehen. Der Zugang zu den Stimmzetteln ist allerdings strengstens in §73 „Übergabe und Verwahrung der Wahlunterlagen“ der BWO geregelt: So bündelt der Wahlstand nach Erledigung seiner Aufgaben die Stimmzettel und die eingenommenen Wahlscheine und versiegelt die einzelnen Pakete, die dann an die Gemeindebehörde übergeben werden. „(2) Die Gemeindebehörde hat die Pakete zu verwahren, bis die Vernichtung der Wahlunterlagen zugelassen ist (§ 90). Sie hat sicherzustellen, dass die Pakete Unbefugten nicht zugänglich sind.“

Falls es jemandem trotz der strengen Regelungen gelingen sollte, Zugriff zu diesen Paketen zu erlangen, dann bleiben noch zwei Probleme: zum einen braucht dieser Angreifer die Fingerabdrücke der Wähler, um sie mit denen auf dem Stimmzettel zu vergleichen und zum anderen sollte er die Möglichkeit haben, die Pakete wieder zu versiegeln, damit der Vorfall nicht bemerkt wird. In den traditionellen Verfahren existiert damit zwar theoretisch eine Zusammenordnung zwischen Wähler und Stimme, sie ist aber durch organisatorische Maßnahmen für niemanden zugänglich.

### **4. Analyse verschiedener Online-Wahl Techniken**

Bei einer (remote) Online-Wahl erfolgt sowohl die Berechtigungsprüfung als auch die Stimmabgabe elektronisch. Dies bedeutet insbesondere, dass sowohl die Wähler spezifischen Identifikationsdaten über das Internet geschickt werden als auch die (verschlüsselte) Stimme. Je nach Protokoll kann dies in einem oder mehreren Protokollschritten geschehen. Das Internet bietet nun an unterschiedlichen Knotenpunkten die Möglichkeit, den Datenverkehr unbemerkt mitzulesen. So kann ein Angreifer, der sich an einem Knoten in der Nähe des „Stimmenspeichernden“-Servers (Urnen-Server) be-

findet, sämtliche Wahlnachrichten mitprotokollieren und zu einem späteren Zeitpunkt auswerten. Der Zugriff zu diesen Daten ist im Vergleich zu den traditionellen Wahlen leichter, erfordert aber technisches Know-How. Kann ein entsprechender Knotenpunkt angezapft werden, so ist es dem Angreifer auf die gleiche Art und Weise möglich von beliebig vielen Wählern die Daten mitzulesen, zu speichern und auszuwerten. An dieser Stelle sei aber angemerkt, dass eine Offenlegung mitgelesener und entschlüsselter Daten, unabhängig ob es Stimmdateien sind oder Daten in einem anderen Kontext, nach §202 a StGB [4, S. 175] strafbar ist.

Gehen wir im Folgenden davon aus, ein Angreifer hat sich dem widersetzt und die Daten mitgelesen. Er beginnt nun nach der Wahl die gesammelten Daten auszuwerten. Welche Informationen der Angreifer daraus ableiten kann und wie die Beweiskraft für seine Aussage „Wähler X hat Partei Y gewählt“ gegenüber dritten ist wird im Folgenden anhand einfacher Protokollbeispiele gezeigt.

Seit Anfang der 80er Jahren wurden zahlreiche unterschiedliche Wahlprotokolle entwickelt und teilweise in einsatzfähige Online-Wahl-Systeme umgesetzt. Die Systeme lassen sich in die folgenden drei Protokollfamilien unterteilen (1) Systeme mit vorgelagerter Wähleridentifizierung, (2) Systeme mit verdeckter Auswertung (Homomorphe Systeme, Hardware Security Module) und (3) Systeme mit Blinder Signatur [3]. Jede der drei Protokollfamilien wird im Anschluss bzgl. der Umsetzung der geheimen Wahl untersucht. Dabei wird angenommen, dass der Angreifer nur die Daten auf der Leitung kennt, nicht aber mit einem Wähler oder einem der Server zusammenarbeitet. Der Angreifer kennt aber das Protokoll und die eingesetzten Verschlüsselungsalgorithmen. Bei der Auswertung der Daten wird unterschieden, ob (Angriff A) der Angreifer nur einzelne Stimmen im Klartext kennt oder (Angriff B) das Verfahren gebrochen hat, so dass er in der Lage ist, alle Stimmen zu entschlüsseln ohne den privaten Schlüssel zu kennen oder (Angriff C) der Angreifer den privaten Schlüssel errechnet hat und damit sämtliche Nachrichten entschlüsseln kann. Im ersten Fall gehen wir von einem wie folgt gearteten probabilistischen Verschlüsselungsverfahren aus: Eine zu verschlüsselnde Nachricht  $m$  wird zuerst mit einer Zufallszahl  $r$  erweitert und die so erhaltene neue Nachricht  $m'$  wird mit dem Verfahren verschlüsselt ( $ver'$ ) unter Verwendung des ent-

sprechenden öffentlichen Schlüssels eines Wählers oder eines Servers  $X$ . Für die Notation ergibt sich:

$ver_X(m) := ver'_X(m')$  mit  $m' = m \# r$ <sup>1</sup>.

Der Angreifer erzeugt dann die Verschlüsselung mit dem öffentlich zugänglichen Schlüssel von  $X$  alle möglichen Nachrichten  $s$  (bei Wahlen beispielsweise alle möglichen Stimmen) zusammen mit allen Möglichkeiten für die Zufallszahl  $r$  (Brute Force) und vergleicht die so erhaltenen Cyphertexte mit dem abgefangenen Cyphertext. Stimmen diese überein, kennt der Angreifer den Inhalt der Nachricht bzw. bei Wahlen die Stimme im Klartext und hat das Wahlgeheimnis eines Wählers gebrochen. Für das Brechen des Wahlgeheimnisses eines weiteren Wählers würde er analog vorgehen. Dieser Angriff ist immer möglich, auch in angemessenen Zeiten, aber eben jeweils nur für einen Wähler.

Im Fall dass der Angreifer eine Methode entwickelt mit der er auch ohne den geheimen Schlüssel zu kennen effizient die Nachricht entschlüsseln kann, gelingt ihm dies für alle Nachrichten. Er kann dieses Verfahren aber i.d.R. nicht einsetzen, um Nachrichten zu signieren. Im dritten Fall geht der Angreifer anders vor: Er versucht mittels der entsprechenden Rechenoperation den geheimen Schlüssel  $sk$  von  $X$  zu berechnen. Mit diesem  $sk$  kann er dann alle für  $X$  verschlüsselten Nachrichten entschlüsseln bzw. jegliche Nachrichten im Namen von  $X$  mit dessen geheimen Schlüssel signieren. Im Fall eines Online-Wahl-Systems wenn  $X$  der Urnen-Server ist, kann der Angreifer mit der Kenntnis von  $sk$  alle Stimmen entschlüsseln. Für das Verständnis der folgenden Diskussion ist wichtig zu sehen, dass diese eine vereinfachte Darstellung der eigentlichen Protokolle ist, die nur die Aspekte der Anonymisierung der Stimme beinhalten. Insbesondere wird die IP-Adresse von Absender und Empfänger mit angegeben, da diese für die geheime Wahl bzw. das Brechen der geheimen Wahl eine entscheidende Rolle spielen. Es wird angenommen, dass das System aus zwei Servern besteht: einem Wahlberechtigungs-Server (WBS), der die Wahlberechtigung des Wählers überprüft und einem Urnen-Server (US), der die abgegebenen Stimmen speichert und am Ende der Wahlperiode auszählt. Da das zugehörige System auch die anderen Wahlrechts-

<sup>1</sup> Notation:  $Algorithmus_{Schlüssel\text{inhaber}}(Nachricht)$ . Ob der geheime oder der öffentliche Schlüssel verwendet wird, hängt davon ab, ob der Nachricht verschlüsselt oder signiert wird. Zusammengesetzte Nachrichten, werden durch das Zeichen # verknüpft.

grundsätze erfüllen muss, sind die Protokolle in Wirklichkeit komplizierter.

#### 4.1. Vorgelagerte Wähleridentifizierung

Bei Wahlprotokollen, die auf dem Prinzip der vorgelagerten Wähleridentifizierung beruhen, wird i.d.R. jedem Wähler vor der Wahlperiode eine Wahl-PIN zugestellt (z.B. auf dem Postweg). Diese nutzt er zusammen mit persönlichen Daten (z.B. sein Name und sein Geburtsdatum), um sich gegenüber

dem Wahlberechtigungs-Server zu authentifizieren (Schritt 1). Alternativ zur Wahl-PIN kann der Wähler auch eine entsprechende Wahlnachricht bestehend aus seinen persönlichen Daten signieren, falls er über ein eigenes Schlüsselpaar verfügt und eine entsprechende Public Key Infrastructure (PKI) vorhanden ist. Der Wahlberechtigungs-Server stellt der anfragenden Person eine Zufallszahl aus, falls diese wahlberechtigt ist (Schritt 2). Diese Zufallszahl berechtigt den Wähler zur Stimmabgabe am Urnen-Server. In einem dritten Schritt gibt der Wähler seine Stimme ab und sendet diese zusammen mit der Zufallszahl an den Urnen-Server (Schritt 3).

Wähler → WBS WBS → Wähler Wähler → US:	Wahl-PIN	Wähler-Signatur-Karte
<b>Web-basierte Lösung</b>	$ver_{SSL-WBS} (Name\#Wahl-PIN)$ $ver_{SSL-Wähler} (Zufallszahl)$ $ver_{SSL-US} (Zufallszahl\#Stimme)$	$sig_{Wähler} (Name)$ $ver_{Wähler} (Zufallszahl)$ $ver_{SSL-US} (Zufallszahl\#Stimme)$
<b>Wahlclient</b>	$ver_{WBS} (Name\#Wahl-PIN\#pk_{Wähler})$ $ver_{Wähler} (Zufallszahl)$ $ver_{US} (Zufallszahl\#Stimme)^2$	$sig_{Wähler} (Name)$ $ver_{Wähler} (Zufallszahl)$ $ver_{US} (Zufallszahl\#Stimme)$

Tabelle 1: Wahlprotokolle mit vorgelagerter Wähleridentifikation

<sup>2</sup> Es ist zu beachten, dass nun in Schritt 1 und 3 der verwendete Schlüssel bei jedem Wähler ein anderer ist, während bei der Wahl-Client Variante wie aus dem obigen Protokoll ersichtlich von allen Wählern der gleiche öffentliche Schlüssel jeweils für Wahlberechtigungs-Server und Urnen-Server verwendet wurde.

Die Kommunikation wird dabei entweder über vorhandene Protokolle wie SSL abgesichert, falls das Wahlsystem als reine Web-Lösung implementiert ist, oder über das im Wahlclient implementierte Verschlüsselungsverfahren. Tabelle 1 bietet einen Überblick über die vorhandenen Protokolle. Die gängigste Lösung ist hierbei die Web-basierte Lösung und der Einsatz von Wahl-PINs. Ein Beispiel, welches diese Konzepte umsetzt, ist das zu den GI-Wahlen eingesetzte Polyas-System [5]. Die Untersuchung konzentriert sich daher auf diese Form der vorgelagerten Wähleridentifizierung (Wahl-PIN und webbasiert):

1. Wähler → WBS:

$IP_{\text{Wähler}} \# IP_{\text{WBS}} \# ver_{\text{SSL-WBS}} (\text{Name\#Wahl-PIN})$

2. WBS → Wähler:

$IP_{\text{WBS}} \# IP_{\text{Wähler}} \# ver_{\text{SSL-Wähler}} (\text{Zufallszahl})$

3. Wähler → US:

$IP_{\text{Wähler}} \# IP_{\text{US}} \# ver_{\text{SSL-US}} (\text{Zufallszahl\#Stimme})$

Zur Verschlüsselung der Nachrichten wird jeweils der zuvor ermittelte SSL-Sitzungsschlüssel verwendet.

Nehmen wir an, dem Angreifer gelingt es, die Nachrichten mitzulesen und zu speichern. Darüber hinaus kennt er in einigen Jahren einzelne Nachrichtensätze im Klartext (Angriff A). Bei der Zuordnung von Wähler und Stimme orientiert sich der Angreifer an den IP-Adressen: einmal kennt er nach der Entschlüsselung die Zuordnung IPWähler - Name (aus Schritt 1) und zum anderen die Zuordnung IPwähler – Stimme (aus Schritt 3). Offensichtlich ist es nicht nötig, die Nachricht aus Schritt 2 entschlüsseln zu können und der Angreifer kann sich bei seinen Brute-Force Angriffen auf die Nachrichtenschritte 1 und 3 konzentrieren. Die gleiche Informationsauswertung führt der Angreifer im Fall, dass er das Verfahren gebrochen hat (Angriff B), durch: Dieses Mal ist er aber nicht nur in der Lage die Zuordnung von Stimme und Wähler für einzelne Wähler durchzuführen, sondern für alle mitgelesenen Wahlnachrichten. Der Angriff, bei dem der geheime Schlüssel der beiden Wahl-Server berechnet wird (Angriff C), führt zu dem gleichen Informationsgehalt wie Angriff B, denn mit Hilfe dieser geheimen Schlüssel kann jeweils der Sitzungsschlüssel berechnet werden. Damit gilt auch hier: die geheime Stimme von allen Wählern, zu denen der Angreifer Nachricht 1 und 3 mitgelesen hat, wird gebrochen. In jedem der drei Fälle ist die zeitlich unbegrenzte geheime Wahl ver-

letzt, wenn wir von dem beschriebenen Angriffspotential ausgehen.

Wie sieht es allerdings mit der Beweiskraft aus? Da der Angreifer nicht beweisen kann, dass die IP jeweils zu dem Wähler bzw. zu der Stimmnachricht gehört, kann der Angreifer nicht eindeutig nachweisen, dass die entschlüsselte Stimme und der entschlüsselte Wählername zusammen gehören. Denkbar wäre. Er fängt folgende Nachrichten ab:

$IP_{\text{Wähler1}} \# IP_{\text{WBS}} \# ver_{\text{SSL-WBS}} (\text{Name\#Wahl-PIN1})$

$IP_{\text{WBS}} \# IP_{\text{Wähler 1}} \# ver_{\text{SSL-Wähler 1}} (\text{Zufallszahl})$

$IP_{\text{Wähler2}} \# IP_{\text{WBS}} \# ver_{\text{SSL-WBS}} (\text{Name\#Wahl-PIN2})$

$IP_{\text{WBS}} \# IP_{\text{Wähler 2}} \# ver_{\text{SSL-Wähler 2}} (\text{Zufallszahl})$

Und behauptet nachdem er alle entschlüsselt hat, dass der Wähler Name\_1 die Stimme Stimme2 abgegeben hat indem er die Nachrichten wie folgt ändert:

$IP_{\text{Wähler1}} \# IP_{\text{WBS}} \# ver_{\text{SSL-WBS}} (\text{Name\#Wahl-PIN1})$

$IP_{\text{WBS}} \# IP_{\text{Wähler 2}} \# ver_{\text{SSL-Wähler 2}} (\text{Zufallszahl})$

Einen Nachweis hätte er nur dann, wenn es ihm gelingt, sich die mitgelesenen Nachrichten schon direkt nach der Wahl bestätigen zu lassen. Es dürfte aber schwierig sein, jemanden zu finden, der solche Nachrichtensätze bestätigt, da alleine durch das Mitlesen und Speichern eine kriminelle Handlung vorliegt.

## 4.2. Systeme mit verdeckter Auswertung

Die Idee der verdeckten Auswertung ist die, dass die einzelnen Stimmen geheim bleiben, deren Besitzer aber beweisbar bekannt ist und nur die Summe über alle Stimme im Klartext bekannt wird. Vor der Summenberechnung wird für den jeweiligen Stimmdatensatz geprüft, ob er von einer wahlberechtigten Person geschickt wurde. Zu solchen Systemen zählen sowohl die homomorphen Verfahren als auch solche die zur Anonymisierung Hardware Security Module (HSM) einsetzen. Wahlsysteme mit verdeckter Auswertung sind wegen der erforderlichen Client-Verschlüsselungs-Funktionalität nicht als Web-Lösung einsetzbar sondern nur als Wahl-Client. Bei den homomorphen Verfahren geschieht die Summenberechnung über die Homomorphie-Eigenschaft des zur Verschlüsselung eingesetzten Algorithmus.

Eingesetzt wird dieser Ansatz beispielsweise im System des CypherVote Projekts[6]. Die Idee bei den HSM-Verfahren ist die, dass der zur Entschlüsselung der Stimm Datensätze benötigte geheime Schlüssel nie bekannt wird. Das Modul ist so gestaltet, dass weder dieser Schlüssel noch die einzelnen entschlüsselten Stimmen das Hardware Security Modul jemals verlassen oder ausgelesen werden können. Auf der Verwendung eines Hardware Security Moduls baut z.B. das in Estland zur letzten Kommunalwahl eingesetzte Wahlsystem [7] auf.

Die Ausprägung beider Varianten ist in Tabelle 2 dargestellt. HSM-Verfahren sind in der Praxis im Zusammenhang mit dem Einsatz von Signaturkarten zur Authentifizierung zu sehen. Das vereinfachte Protokoll besteht nur aus einer einzigen Nachricht:

Wähler → US:

$IP_{\text{wähler}} \# IP_{\text{US}} \# \text{sig}_{\text{wähler}}(\text{ver}_{\text{HSM}}(\text{Stimme}))$

Genau genommen, wird diese Nachricht erst ans Wählerverzeichnis geschickt, welches die Wahlberechtigung anhand der Wähler-signatur überprüft und im Fall einer Wahlberechtigung die verschlüsselte Stimme an die Urne, bzw. dort an das HSM übergibt, um die Stimmen auszuzählen.

Nehmen wir an, dem Angreifer gelingt es, die Nachrichten mitzulesen und zu speichern. Darüber hinaus kennt er in einigen Jahren einzelne Nachrichtensätze im Klartext (Angriff A). Durch die Signatur auf den entsprechenden verschlüsselten Nachrichten erhält der Angreifer damit auch die eindeutige Zuordnung von Wähler und Stimme. Er benötigt hierbei also pro Wähler nur diese eine Nachricht und ein Abgleich über die IP-Adressen ist nicht erforderlich. Im Fall, dass der Angreifer das Verfahren gebrochen hat (Angriff B), ist er in der Lage die Zuordnung von Stimme und Wähler für alle mitgelesenen Wahlnachrichten herzuleiten. Der Angriff, bei dem der geheime Schlüssel berechnet wird (Angriff C), führt zu dem gleichen Informationsgehalt wie Angriff B. Damit ist auch hier in jedem der drei Angriffsszenarien die zeitlich unbegrenzte geheime Wahl verletzt, wenn wir von dem beschriebenen Angriffspotential ausgehen.

Wähler→US:	Wahl-PIN	Wähler-Signatur-Karte
<b>HSM</b>	$\text{ver}_{\text{WBS}}(\text{Wahl-PIN} \# \text{ver}_{\text{HSM}}(\text{Stimme}))$	$\text{sig}_{\text{wähler}}(\text{ver}_{\text{HSM}}(\text{Stimme}))$
<b>Homomorphe Verfahren</b>	$\text{ver}_{\text{WBS}}(\text{Wahl-PIN} \# \text{ver}_{\text{US}}(\text{Stimme}))$	$\text{sig}'_{\text{wähler}}(\text{ver}_{\text{US}}(\text{Stimme}))$

Tabelle 2: Wahlprotokolle mit verdeckten Auswertungskanälen

Wie sieht es allerdings mit der Beweiskraft aus? Diese ist nur im Fall eines Angriffs A gegeben. Denn hier hat der Angreifer sowohl die Stimme im Klartext, als auch die verschlüsselte Stimme, die wiederum vom Wähler signiert ist. Wenn das entsprechende Verfahren bis dahin noch nicht als gebrochen gilt, dann hat der Angreifer mittels Brute-Force diese eine Nachricht entschlüsselt und war insbesondere nicht in der Lage die Signatur des Wählers zu erzeugen, weil er dazu den geheimen Schlüssel des Wählers kennen müsste. Die entschlüsselte Nachricht gehört also nachweislich zu dem Wähler der sie signiert hat. Im Fall B, indem das Verfahren als solches gebrochen ist, verliert die Erkenntnis des Angreifers jegliche Beweiskraft, denn nun ist der Angreifer in der Lage für den Wähler im Nachhinein neue Stimmen zu signieren. Bei dem letzten Angriff (C) ist die Beweiskraft auch nicht wirklich gegeben, denn analog zur Berechnung des geheimen Schlüssels zur Entschlüsselung der Stimme, könnte der Wähler auch den geheimen Schlüssel des Wählers ermittelt haben und damit eine beliebige Stimme signieren.

Da bei allen asymmetrischen Verschlüsselungsverfahren davon ausgegangen wird, dass einzelnen Nachrichten durch Kryptoanalysen gebrochen werden können, verletzen anonyme Auswertungskanäle nicht nur die geheime Wahl als solche sondern sie bieten einem Angreifer auch die Möglichkeit ihre Aussage gegenüber dritten zu beweisen, was einen Angriff im Vergleich zu den Ansätzen mit vorgelagerte Wählerauthentifizierung attraktiver werden lässt.

Die Homomorphen verfahren also solche sind in diesem Rahmen zu komplex, um sie ausführlich zu diskutieren, da hier verschiedene andere kryptografische Protokolle wie Zero-Knowledge-Beweise mit einfließen. Bzgl. der Angriffe auf die geheime Wahl sind hier die gleichen Möglichkeiten gegeben wie bei den Ansätzen, die auf einem Hardware Security Modul basieren. Die Homomorphen Verfahren sind allerdings wegen ihrer stärkeren Beweisbarkeit aus Sicht der geheimen Wahl in der Praxis weniger geeignet. Jeder Wähler veröffentlicht seine Stimme, die dem Wähler auch klar zugeordnet werden kann, auf einem öffentlichen Bulletin Board. Mit Hilfe dieses Board kann der Angreifer dann nachweisen, dass die Stimme wirklich vom Wähler selbst signiert wurde und nicht im Nachhinein (also nach dem Brechen des Algorithmus) vom Angreifer.

### 4.3. Systeme mit blinden Signaturen

Online-Wahl-Verfahren, die mit blinden Signaturen arbeiten, basieren im Wesentlichen auf dem von Chaum bereits 1981 vorgestellten Verfahren zur blinden Unterschrift [8]. Setzt man diese Technologie bei Wahlen ein, so kann das Dokument entweder der Stimmzettel sein, wie Fujioka et.al. [9], oder es dient als anonymes Pseudonym zum Lösen des Stimmzettels vom Wähler wie in [10] vorgeschlagen. Zur Authentifizierung wird daher die Signatur des Wählers eingesetzt und wegen der beim Wähler durchzuführenden Blindung kommt nur ein Wahl-Client in Frage.

Bei der **Blindung des Stimmzettels** sieht das vereinfachte Protokoll folgendermaßen aus.

1. Wähler  $\rightarrow$  WBS:  
 $IP_{\text{wähler}} \# IP_{\text{WBS}} \# \text{sig}_{\text{wähler}}(\text{blind}(\text{Stimme}))$
2. WBS  $\rightarrow$  Wähler:  
 $IP_{\text{WBS}} \# IP_{\text{wähler}} \# \text{sig}_{\text{WBS}}(\text{blind}(\text{Stimme}))$
3. Wähler  $\rightarrow$  US:  
 $IP_{\text{wähler}} \# IP_{\text{US}} \# \text{ver}_{\text{US}}(\text{sig}_{\text{WBS}}(\text{Stimme}))$

Das heißt der Wähler signiert seine geblindete Stimme und schickt sie an den Wahlberechtigungs-Server. Dieser kann den Inhalt der Stimme nicht lesen. Er überprüft an Hand der Signatur, ob die anfragende Person wahlberechtigt ist und signiert ggf. die geblindete Stimme mit dem eigenen geheimen Schlüssel, wodurch er dem Wähler seine Wahlberechtigung erteilt. Anschließend entfernt der Wähler die Blindung von der Stimme und schickt sie an den Urnen-Server. Die verwendeten Verfahren sind so gewählt, dass die Signatur des Wahlberechtigungs-Servers ihre Gültigkeit auf für die ungeblindete Stimme gültig ist. Der Urnen-Server erkennt dann anhand dieser Signatur, dass die Stimme gültig ist und speichert sie.

Die Stimme wird hier genau wie bei der vorgelagerten Wähleridentifikation ohne Angaben zum Wähler verschickt. Daher ist die einzige Möglichkeit, die mitgelesene und entschlüsselte Stimme (Angriff A) ihrem Wähler zuzuordnen, über die IP-Adresse des Wählers gegeben: Kennt der Angreifer Nachricht 1 und 3, kann er dem Wähler seine Stimme im Klartext zuordnen sobald er die Nachricht 3 entschlüsseln kann. D.h. es genügt die Nachricht 3 zu entschlüsseln. Auf diese Weise kann der Angreifer die geheime Wahl einzelner Wähler brechen. Da es genügt die dritte Nachricht zu entschlüsseln

führen Angriff B und C dazu, dass der Angreifer das Wahlgeheimnis für alle Wähler brechen kann, von denen er die Nachricht 1 und 3 mitgelesen hat.

Die Beweiskraft ist hier wieder in keiner der Angriffsszenarien gegeben, da der Angreifer die IP-Adressen der mitgelesenen Nachrichten wie bei den Systemen mit der vorgelagerten Wähleridentifikation beschreiben austauschen kann. Die Signatur auf der geblindeten Stimme aus Protokollschritt 1 kann nicht zum Nachweis verwendet werden, da nicht bewiesen werden kann, dass die Stimme aus Schritt 3 der geblindeten aus Schritt 1 entspricht. Denn hinter der geblindeten Stimme kann jede Stimme sich verbergen.

Die **Blindung eines anonymen Pseudonyms** erfolgt vereinfacht folgendermaßen:

In diesem Ansatz schickt der Wähler dem Wahlberechtigungs-Server ein eigens gewähltes und anschließend geblindetes Wahlberechtigungs-Token. Die Wahlberechtigung selbst erfolgt wieder über die Signatur des Wählers. Dieses Mal signiert der Wahlberechtigungs-Server das geblindete Token und erteilt dem Wähler damit die Wahlberechtigung. Der Wähler entfernt dann die Blindung und schickt das vom Wahlberechtigungs-Server signierte Token zusammen mit der Stimme an den Urnen-Server.

Nehmen wir wieder an, es ist dem Angreifer gelungen die Wahlprotokoll-Nachrichten mitzulesen und einzelne Stimmen zu entschlüsseln (Angriff A). Da der Sinn des Blindens der ist, dass zu einem *blind(Token)* je nach Wahl des Blindungsfaktors jedes *Token* gehören kann, kann auf diesem Weg keine Zuordnung zwischen Wähler und Stimme geschehen. Auch hier kann der Angreifer die geheime Wahl aber über die IP-Adresse des Wählers, deren Stimme er entschlüsselt hat brechen. Bei den beiden anderen Angriffsszenarien kann der Angreifer analog über die IP-Adressen allen Wählern ihre Stimme zuordnen. Durch die Möglichkeit des Angreifers die IP-Adressen zu vertauschen, gibt auch dieses Protokoll dem Angreifer keine Möglichkeit seine Stimme zu beweisen.

Die Analyse der einzelnen Protokolle hat gezeigt, dass in der beschriebenen Form und bei dem beschriebenen Angreiferpotential keines eine zeitlich unbegrenzte Wahl sicherstellen kann. Das Hauptproblem ist dabei die Bindung der Nachrichten an die IP-Adresse des Wählers. Außerdem hat sich herausgestellt, dass der Angreifer in fast allen Fällen keine Möglichkeit hat diese Erkenntnis gegenüber dritten zu beweisen. Im

folgenden Kapitel soll nun herausgearbeitet werden, wie eine Loslösung von der IP-Adresse erreicht werden kann.

## 5. Empfehlungen

Eine allgemein bekannte und gut untersuchte Möglichkeit die Stimme bzw. den Wähler von der IP-Adresse zu lösen, ist der Einsatz von Mix-Netzen [8]. Diese lassen sich auch recht einfach in jedes Wahlprotokoll mit Wahl-Client integrieren. Dies würde den Angriff einschränken, denn der Angreifer kann nun nicht beliebige Netzpunkte abhören sondern muss sich vor den ersten Mix setzen. Falls mehrere Mix-Kaskaden eingesetzt werden kann der Angreifer durch den Zugriff an einer Stelle nur noch eine sehr begrenzte Menge an Stimmprotokollen mitlesen. Insbesondere würde sich die Sicherheit dann erhöhen, wenn die Authentifizierung und die Stimmabgabe über unterschiedliche Mix-Kaskaden abgewickelt werden.

Ein anderer Ansatz wird von Prosser/Müller [10] im Zusammenhang mit ihrem Ansatz nur Anonymisierung mittels blinder Signaturen vorgeschlagen: ein zweiphasiges Protokoll. Dabei kann der dritte Protokollschritt – die eigentliche Stimmabgabe zu einem späteren Zeitpunkt und von einem anderen Rechner aus als die Schritte 1 und 2 ausgeführt werden. Auf diese Weise ist dann die IP des Wählers nicht die gleiche in allen drei Schritten und kann nicht verwendet werden, um die Zuordnung zwischen Wähler und Stimme herzustellen. Insbesondere heißt dies, dass es keine Möglichkeit für einen Angreifer gibt, der alle Nachrichten mitgelesen hat und auch die Verschlüsselungen der Nachricht gebrochen hat, die geheime Wahl zu verletzen. Organisatorisch würde dieser Ablauf in etwa dem Vorgehen bei der Briefwahl entsprechen. Man erfragt erst die Unterlagen – im elektronischen Fall einen Berechtigungsnachweis – und gibt dann seine Stimme zu einem späteren Zeitpunkt ab.

Dieser Ansatz ist allerdings nicht auf alle Verfahren anwendbar. Bei dem blind signieren des Stimmzettels wäre der Wähler schon im Vorfeld der Wahl, also bei der Anfrage der Unterlagen gezwungen sich auf eine Stimme festzulegen, da er diese später nicht mehr ändern kann. Auch die Anwendung bei den Verfahren mit verdeckter Auswertung ist schwierig, da es hier der Wähler nicht an der Zweitteilung von Wahlberechtigung

gungsprüfung und Stimmabgabe beteiligt ist. Einer Umsetzung bei den Verfahren mit vorgelagerter Wählerauthentifikation spricht nichts entgegen.

Ein weiteres Problem ist die sichere Übertragung der im ersten Schritt erhaltenen Berechtigungstoken von einem Rechner zum anderen. In Prosser/Müller wird vorgeschlagen hierzu die Chipkarte einzusetzen. Alle anderen Medien werfen Probleme bzgl. der anderen Wahlrechtsgrundsätze auf. Beispielsweise könnte das Medium zwecks Stimmenkaufs weitergegeben werden an einen Käufer, der dann damit die Stimme abgeben kann.

## 6. Zusammenfassung

Ganz allgemein hat sich gezeigt, dass im Vergleich zur traditionellen Wahl die Problematik der zeitlich unbegrenzten Wahl verschoben hat: Während bei der traditionellen Wahl über den Fingerabdruck eindeutig die Zugehörigkeit von Wähler und Stimmzettel nachgewiesen werden könnte, ist dies bei der Online-Wahl nur bei den Verfahren mit einer vorgelagerten Wähleridentifikation möglich. Außerdem ist im traditionellen System der Zugang zu den Stimmzetteln organisatorisch gesichert und damit sichergestellt, wogegen die Protokolle als solche zunächst einmal die geheime Wahl gegenüber einem Angreifer, der die gesamte Kommunikation abhören und in der Zukunft einzelne oder alle Nachrichten entschlüsseln kann, nicht sicherstellen können.

## 7. Literatur

1. Ullmann, M., Koob, F., Kelter, H: *Anonyme Online-Wahlen (2001): Lösungsansätze für die Realisierung von Online-Wahlen*. DuD - Datenschutz und Datensicherheit, Vol. 25, Nr. 11, S. 643-647.
2. Will, M. (2002): *Internetwahlen: verfassungsrechtliche Möglichkeiten und Grenzen*, Die Deutsche Bibliothek – CIP Einheitsaufnahme, Boorberg.
3. Volkamer, M., Krimmer, R. (2006): *Die Online-Wahl auf dem Weg zum Durchbruch*. Informatik Spektrum, Nr. 2, S. 98-113.
4. Hanßmann, A. (2003): *Möglichkeiten und Grenzen von Internetwahlen* Nomos Verlag, Baden-Baden.
5. Micromata GmbH (2005): *Online-Wahlen für Verbände und Vereine*. [http://micromata.de/produkte/documents/polyas\\_broschuere\\_72dpi.pdf](http://micromata.de/produkte/documents/polyas_broschuere_72dpi.pdf) [abgerufen am 2006-04-15].
6. Schoenmakers, B.: *A Simple Publicly Verifiable Secret Sharing Scheme and Its Application to Electronic Voting*, *Advances in Cryptology - Crypto99*, (Vol. 1666) Springer-Verlag, S. 148-164 (1999)
7. *Local Government Council Election*, <http://www.vvk.ee/k05/enginfor.html> [abgerufen am 2006-04-15].
8. Chaum, D. (1981): *Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms*, *Communications of the ACM*, Vol. 24, Nr. 2, S. 84-88.
9. Fujioka, A., Okamoto, T., Ohta, K. (1993): *A Practical Secret Voting Scheme for Large Scale Elections*. In: *Advances in Cryptology – AUSCRYPT92*. Springer-Verlag, Berlin, S. 244–251.
10. Prosser, A., Müller-Török, R.: *E-Democracy: Eine neue Qualität im demokratischen Entscheidungsprozess*, *Wirtschaftsinformatik*, Vol. 44, Nr. 6, S. 545-556.