Bingo Voting – Verifizierbare Wahlen mit Wahlmaschinen

Michael Bär
EISS, Universität Karlsruhe (TH), 76128 Karlsruhe
Email: MichaelBaer@gmx.de

Jens-Matthias Bohli*
NEC Laboratories Europe, 69115 Heidelberg
Email: bohli@nw.neclab.eu

Christian Henrich
EISS, Universität Karlsruhe (TH), 76128 Karlsruhe
Email: henrich@ira.uka.de

Jörn Müller-Quade
EISS, Universität Karlsruhe (TH), 76128 Karlsruhe
Email: muellerq@ira.uka.de

Stefan Röhrich*
Rohde & Schwarz SIT GmbH, 12489 Berlin
Email: Stefan.Roehrich@rohde-schwarz.com

Carmen Stüber
EISS, Universität Karlsruhe (TH), 76128 Karlsruhe
Email: cstueber@ira.uka.de

30. Juni 2008

Zusammenfassung

Bingo Voting ist ein Wahlverfahren, das Wahlcomputer einsetzt, und dabei vollständige und beweisbare Verifizierbarkeit des Wahlergebnisses garantiert, ohne das Wahlgeheimnis zu gefährden. Dazu erhält der Wähler einen Beleg, mit dessen Hilfe er die korrekte Zählung seiner Stimme überprüfen kann. Die Sicherheit des Verfahrens beruht auf einem vertrauenswürdigen Zufallszahlengenerator.

*Die Arbeit wurde durchgeführt, als die Autoren am EISS, Universität Karlsruhe (TH) waren.

1 Stand der Forschung/Technik

Wahlen sind eine wichtige Grundlage jeder Demokratie. Dabei ist das Vertrauen des Bürgers in die Wahl essentiell. Jeder Bürger muss sich sicher sein können, dass bei einer Wahl das Wahlergebnis den Willen des Volkes widerspiegelt und dass insbesondere seine Stimme korrekt gezählt wird.

Bei der herkömmlichen Papierwahl kann der Wähler bei (fast) jedem Abschnitt der Wahl anwesend sein und so den Ablauf kontrollieren. Ein Problem ist jedoch, dass immer weniger Leute Interesse daran haben und Wahlhelfer fehlen, die bereit sind, bis spät in die Nacht die Auszählung durchzuführen.

Bingo Voting [2] ist ein neuartiges Wahlverfahren, bei dem Wahlmaschinen zur Stimmabgabe eingesetzt werden. Das Verfahren hat dabei keinen Einfluss auf die Stimmabgabe selbst, sondern gibt dem Wähler nach der Stimmabgabe einen Beleg, mit dem dieser die korrekte Zählung seiner Stimme überprüfen kann. Der Beleg kann allerdings nicht dazu benutzt werden, einer anderen Person zu zeigen, was gewählt wurde. Dadurch werden Stimmenkauf und Erpressung verhindert.

Um die Bedeutung von Bingo Voting deutlich zu machen, gibt dieses Kapitel eine kurze Übersicht über den Stand der Forschung und der Technik. Dabei beschränkt es sich auf Wahlverfahren, die ein Erscheinen des Wählers im Wahllokal voraussetzen.

Ein anderes Gebiet sind kryptographische Verfahren für sichere Internetwahlen, die der Benutzer von seinem PC aus durchführt. Diese Art von Wahlen sind aus kryptographischer Sicht ein sehr spannendes und anspruchsvolles Thema. Internetwahlen haben dabei allerdings mit ganz anderen Anforderungen und Ansprüchen zu kämpfen als Wahlverfahren [7], bei denen der Wähler in der Wahlkabine seine Stimme abgibt. Wir betrachten im Folgenden nur Wahlverfahren, die die Wahlfreiheit der Wahl dadurch unterstützen, dass Wahlkabinen benutzt werden.

1.1 Konventionelle Wahlverfahren

Inzwischen werden neben der Papierwahl zunehmend auch Wahlmaschinen zur Stimmabgabe eingesetzt. Diese bieten gegenüber der Papierwahl mehrere Vorteile wie eine schnelle Auszählung oder Hilfestellungen bei komplexen Wahlen, beispielsweise durch Anzeige der Anzahl der bereits verteilten Stimmen. Leider ist es bei Wahlmaschinen im Gegensatz zu der herkömmlichen Papierwahl für den Bürger sehr schwierig, das Wahlergebnis nachzuvollziehen, da eine öffentliche Auszählung nicht möglich ist. Der Wähler muss, wenn er seine Stimme an einer Wahlmaschine abgibt, darauf vertrauen, dass die Stimme korrekt gespeichert und gezählt wird. Dies führt vermehrt zu Kritik an elektronischen Wahlsystemen [1, 5, 10].

Es existieren verschiedene Ansätze, um dieses Problem zu beheben. Eine Möglichkeit ist, die Stimme nicht nur elektronisch in der Wahlmaschine zu speichern, sondern gleichzeitig auf Papier festzuhalten. Ein solcher zusätzlicher Nachweis auf Papier wird als *Voter Verified Paper Audit Trail (VVPAT)* (deutsch: vom Wähler verifiziertes Papierprotokoll) bezeichnet und macht es möglich, das Ergebnis der Wahlmaschine durch eine (beispielsweise stichprobenartige) Nachzählung der Papierstimmen zu überprüfen. Beispiele hierfür sind der Hamburger Wahlstift oder Verfahren, bei denen der Wahlzettel eingescannt wird.

Eines der Probleme mit diesen Verfahren ist, dass festgelegt werden muss, ob das elektronisch ermittelte Ergebnis bindend ist, oder ob die Stimmen auf Papier für das Ergebnis ausschlaggebend sind. Wird das amtliche Ergebnis durch die elektronische Auszählung ermittelt und die Nachzählung nur stichprobenartig zur Kontrolle durchgeführt, stellt sich die Frage, wie Abweichungen zwischen elektronischem Ergebnis und Auszählung der Papiernachweise gehandhabt werden. Auch kann sich ein Angreifer die Toleranz für Ungenauigkeiten, die gerade bei Scanverfahren durchaus auftreten, zu Nutze machen, um das Ergebnis zu beeinflussen. Wird hingegen das amtliche Ergebnis durch Auszählung der Papierstimmzettel ermittelt, dient das elektronische Verfahren nur dazu, schneller ein vorläufiges Ergebnis zu erhalten. In diesem Falle ist es fraglich, ob dies die hohen Kosten rechtfertigt.

1.2 Kryptographische Wahlverfahren

Es existieren auch kryptographische Verfahren, die dem Wähler die Möglichkeit bieten, die Korrektheit der Wahl zu überprüfen. Dies stellt einen echten Fortschritt gegenüber stichprobenartigen Kontrollen von Wahlmaschinen dar. Kryptographische Verfahren können diesbezüglich sogar Vorteile gegenüber der Papierwahl bieten, bei der ein Bürger zwar die Auszählung in seinem Wahlkreis überprüfen kann, aber dadurch nur indirekt überzeugt wird, dass seine Stimme korrekt gezählt wird.

Die meisten kryptographischen Verfahren hingegen geben dem Wähler einen Beleg an die Hand, mit dessen Hilfe er die korrekte Zählung seiner Stimme nachvollziehen kann. Dazu werden alle Belege veröffentlicht und der Wähler kann nachprüfen, dass sein Beleg ebenfalls berücksichtigt wurde. Die Schwierigkeit besteht dabei darin, dass der Beleg für Dritte keine Informationen über die Wahl des Wählers enthalten darf, da sonst Stimmenkauf und Erpressung möglich sind.

Ein Ansatz bei kryptographischen Verfahren ist die Erweiterung der Papierstimmzettel um kryptographische Überprüfungen. Beispiele hierfür sind Punchscan, Prêt à Voter und Three-Ballot-Voting. Diese papierbasierten kryptographischen Verfahren besitzen allerdings einige Nachteile, die dem praktischen Einsatz im Weg stehen. Alle drei Verfahren benutzen spezielle Wahlzettel, die vom Wähler ausgefüllt werden.

Punchscan Bei Punchscan [9, 3] besteht ein solcher Wahlzettel aus zwei übereinander fixierten Zetteln. Der obenliegende Zettel hat dabei Aussparungen, durch die Buchstaben zu sehen sind, die auf dem unteren Zettel an die entsprechenden Stellen gedruckt sind. Die Zuordnung der Buchstaben zu den Aussparungen ist dabei zufällig, und pro Aussparung ist nur ein Buchstabe aufgedruckt. Auf dem oberen Blatt sind die Kandidaten aufgelistet, zusammen mit je einem ihnen zugeordneten Buchstaben.

Um für einen Kandidaten zu stimmen, muss der Wähler diesen zunächst in der Liste auf dem oberen Blatt suchen und den dem Kandidaten zugeordneten Buchstaben dann im Markierungsbereich finden (also die Aussparung, durch die der entsprechende Buchstabe auf dem unteren Blatt sichtbar ist). Diese Aussparung wird dann mit einem speziellen Stempel, dessen Stempelfläche größer als die Aussparung ist, so markiert, dass sowohl das obere als auch das untere Blatt deutlich an dieser Stelle gekennzeichnet wird (siehe Abb. 1).

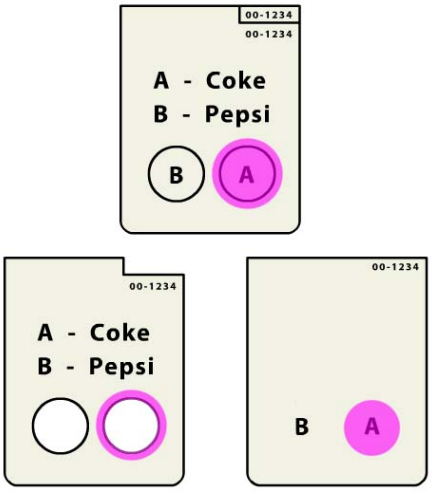

Abbildung 1: Ein markierter Punchscan-Wahlzettel (oben) und beide Teile getrennt (unten).

Werden nun die beiden Zettel voneinander getrennt, kann man dem einzelnen nicht mehr ansehen, für welchen Kandidaten die Stimme abgegeben wurde. Dem oberen Zettel fehlt die Zuordnung, welche Aussparung zu welchem Buchstaben gehört, der untere Zettel hingegen trägt keine Zuordnung von Buchstabe zu Kandidat. Der Wähler kann nun eine Kopie einer der beiden Hälften des Wahlzettels als Beleg mit nach Hause nehmen. Die andere Hälfte wird vor den Augen des Wählers in einem Schredder zerstört. Um die Stimme dennoch rekonstruieren zu können, tragen beide Hälften eine Identifikationsnummer, mit dessen Hilfe die Wahlautorität die Zuordnung von Kandidat zu Buchstabe und Position der Ausparung bzw. des Buchstaben auf dem Beleg und mit Hilfe der Markierung die Stimme rekonstruieren kann.

Der Hauptnachteil von Punchscan ist der ungewöhnliche und umständliche Wahlvorgang sowie die Schwierigkeiten, die beim Kumulieren entstehen. Außerdem existiert die Möglichkeit, dass der Wähler beweisen kann, dass er eine zufällige Partei gewählt hat (beispielsweise indem er vorher vereinbart, welche Aussparung er markiert), was dem Grundsatz der freien Wahl widerspricht.

Prêt à Voter Prêt à Voter [4] benutzt ebenfalls zweigeteilte Stimmzettel, bei denen eine Hälfte als Beleg dient, die Information über den Kandidaten jedoch nur aus beiden Hälften zusammen ersichtlich wird. Bei Prêt à Voter ist der Stimmzettel (siehe Abb. 2) durch eine Perforation längs so aufgeteilt, dass auf der einen Seite die Kandidaten in einer zufälligen Reihenfolge stehen, und auf der anderen Hälfte der Wähler seine Wahl notieren kann (beispielsweise durch das traditionelle Kreuz). Dadurch wird es auch sehr einfach möglich zu kumulieren oder sogar Ranking-Wahlen durchzuführen.

Das größte Problem mit Prêt à Voter ist, dass die Kandidaten in einer zufälligen Reihenfolge stehen *müssen*, um die Sicherheit des Verfahrens zu gewährleisten. Dies kollidiert mit Wahlgesetzen, die die Reihenfolge der Kandidaten auf dem Stimmzettel fest vorschreiben. Und genau wie bei Punchscan ist es bei Prêt à Voter möglich, dass der Wähler beweisen kann, dass er einen

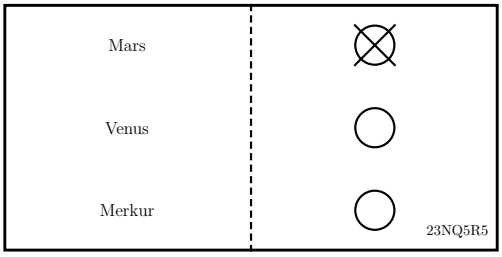

Abbildung 2: Ein Wahlzettel des Prêt à Voter Verfahrens. Die Reihenfolge der Kandidaten ist zufällig, die Stimme kann nur mit Hilfe der Identifikationsnummer des Stimmzettel (unten rechts) rekonstruiert werden.

Stimmzettel zufällig ausgefüllt, seine Stimme also wahrscheinlich einer bestimmten Partei nicht gegeben hat.

Three-Ballot-Voting Three-Ballot-Voting benutzt ebenfalls einen speziellen Wahlzettel, von dem ein Teil als Beleg dient. Im Gegensatz zu Punchscan und Prêt à Voter besteht der Wahlzettel allerdings nicht aus zwei verschiedenen, sondern aus drei nahezu identischen Teilen, die jeweils die vollständige Kandidatenliste (in beliebiger, also auch nichtzufälliger Reihenfolge) sowie je eine Identifikationsnummer tragen (siehe Abb. 3). Die Identifikationsnummern werden so gewählt, dass jeder Teil eine eigene Nummer trägt und drei zusammenhängende Zettel nicht über die Nummern in Verbindung gebracht werden können. Zur Stimmabgabe vergibt der Wähler zunächst an *jeden* Kandidaten eine Stimme auf einem der drei Teilzettel. Danach vergibt er an den Kandidaten, den er wählen möchte, eine weitere Stimme auf einem Teilzettel, der bis jetzt noch keine Stimme für den gewählten Kandidaten enthält. Danach werden die drei Teile des Stimmzettels getrennt. Jetzt hat jeder Kandidat auf mindestens einem Stimmzettel eine Stimme, der gewählte Kandidat hat auf zwei Teilzetteln eine Stimme bekommen, aber einem einzelnen Teilzettel kann man nicht ansehen, für welchen Kandidaten der Wähler tatsächlich gestimmt hat. Dies macht es möglich, dem Wähler die Kopie eines Teilzettels als Beleg mitzugeben.

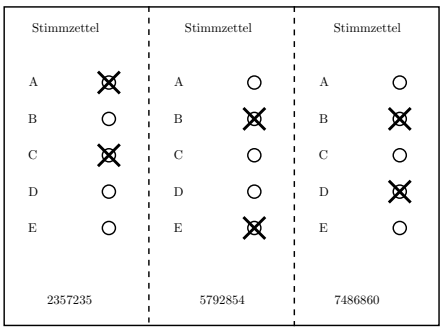

Abbildung 3: Ein ausgefüllter Wahlzettel des Three-Ballot-Verfahrens. Hier wurde Kandidat B geählt.

Neben der umständlichen und unintuitiven Stimmabgabe ist bei Three-Ballot-Voting *pattern voting* möglich, wodurch Stimmenkauf und Erpressung möglich werden. Bei dem Verfahren ist zudem Kumulieren nicht vorgesehen. Der wohl größte Nachteil von Three-Ballot-Voting ist allerdings, dass vor der Abgabe der Stimmzettels kontrolliert werden muss, dass alle Kandidaten mindestens eine und nur ein Kandidat zwei Stimmen erhalten hat, da sonst die Wahl verfälscht würde.

Wahlverfahren von Moran und Naor Neben den Verfahren, die Papierwahlzettel benutzen, gibt es auch kryptographische Verfahren, die Wahlmaschinen einsetzen. Ein Beispiel dafür ist das Verfahren, das von Neff vorgeschlagen und von Moran und Naor weiterentwickelt wurde [8], sowie einige Varianten davon. Das Prinzip des Verfahrens basiert darauf, dass die Wahlmaschine dem Wähler einen speziellen Beweis (Zero-Knowledge-Beweis) für die korrekte Zählung der Stimme liefert. Dabei benutzt sie die Eingabe von Zufall durch den Wähler. Damit dem Beleg nicht anzusehen ist, für welchen Kandidaten der Wähler gestimmt hat, müssen auch für die anderen Kandidaten Beweise existieren. Da für diese aber keine Stimme abgegeben wurde, müssen diese Beweise „gefälscht“ werden. Dies ist möglich, wenn die Maschine die Zufallseingabe des Wählers erhält, bevor sie den Beweis durchführt. Die Stimmabgabe beim Verfahren von Moran und Naor funktioniert also folgendermaßen: Der Wähler wählt einen Kandidaten an der Wahlmaschine, diese verlangt dann die Eingabe von Zufall für alle Kandidaten, die der Wähler *nicht* gewählt hat. Dann wird ein Beleg gedruckt mit den ersten Teilen der Beweise. Danach verlangt die Wahlmaschine eine Eingabe von Zufall für den gewählten Kandidaten. Dann druckt die Wahlmaschine den Rest des Beweises und gibt den Beleg aus. Der Wähler kann sich nun davon überzeugen, dass der eingegebene Zufall korrekt in die Beweise eingeflossen ist. Da die Wahlmaschine den Zufall für den gewählten Kandidaten erst bekommen hat, nachdem sie die erste Hälfte des Beweises ausgedruckt hat (und sich damit darauf festgelegt hat), muss dieser Beweis authentisch sein. Ein Dritter, der den Beleg zu sehen bekommt, kann allerdings diesen Beweis nicht von den anderen unterscheiden, damit bleibt das Wahlgeheimnis gewahrt.

Der Vorteil des Wahlverfahrens von Moran und Naor ist, dass der Wähler erst nach der Stimmabgabe mit dem Wahlschema in Berührung kommt. Dies wird allerdings mit großem Aufwand bei der Stimmabgabe erkauft, insbesondere ist ein Mensch ein sehr schlechter Zufallsgenerator. Dies wird insbesondere deutlich, wenn der Wähler mehrere Stimmen abgeben kann, da er für jede Stimme für jeden Kandidaten Zufall eingeben muss.

1.3 Fazit

Keines der bisher vorgeschlagenen oder eingesetzten Wahlverfahren bietet alle gewünschten Eigenschaften. Die klassische Papierwahl ist zwar intuitiv und nachvollziehbar, bietet dafür aber keine Unterstützung bei der Stimmabgabe (was sich in einer hohen Zahl ungültiger Stimmen bei komplexen Wahlen niederschlägt) und eine langsame Auszählung. Der Einsatz von Wahlcomputern zur Stimmabgabe oder zur Auszählung stellt die Nachvollziehbarkeit in Frage.

Bisherige kryptographische Verfahren bieten zwar eine schnelle Auszählung und Nachvollziehbarkeit, dies wird jedoch durch eine umständliche Stimmabgabe sowie Einschränkungen beim Kumulieren erkauft. Daher lassen sich auch diese Verfahren nicht real einsetzen.

2 Idee

Bingo Voting ist ein neuartiges Verfahren, das es dem Wähler erlaubt, das Wahlergebnis zu überprüfen und insbesondere die korrekte Zählung seiner Stimme nachzuvollziehen. Dabei wird das Wahlgeheimnis nicht gefährdet und der zusätzliche Aufwand ist gering und zudem noch optional.

Die Grundidee des Verfahrens ist es, dem Wähler einen Beleg in die Hand zu geben, aus dem er seine Stimme ersehen kann, und nach der Wahl Kopien aller Belege zu veröffentlichen. Dies gewährleistet:

1. Jeder Wähler kann nachprüfen, dass sein Beleg veröffentlicht wurde, und damit, dass seine Stimme berücksichtigt wurde.
2. Jeder kann die Auszählung anhand der veröffentlichten Belege nachprüfen.

Das Bingo-Voting-Verfahren bietet dabei Belege, aus denen nur der Wähler selbst seine Stimme ersehen kann und niemand sonst. Dadurch kann der Wähler mit seinem Beleg keiner anderen Person beweisen, was er gewählt hat. Stimmenkauf und Erpressung werden unmöglich.

Die Stimmen auf dem Beleg werden durch (Zufalls-) Zahlen repräsentiert, die neben einem Kandidaten stehen. Neben der eigentlichen Stimme, also der Zufallszahl, die neben dem gewählten Kandidaten steht, ist der Beleg mit so genannten Füllstimmen aufgefüllt, so dass neben jedem Kandidaten eine Zahl steht. Diese Füllstimmen sind Zufallszahlen, die vor der Wahl festgelegt und gleichmäßig an die Kandidaten verteilt wurden. Die echte Stimme wird durch eine Zufallszahl repräsentiert, die in der Wahlkabine vor den Augen des Wählers von einem vertrauenswürdigen Zufallszahlengenerator erzeugt wird. Dadurch kennt nur der Wähler die Zuordnung zwischen Zufallszahl und gewähltem Kandidaten, für jeden anderen ist die echte Stimme von einer Füllstimme nicht zu unterscheiden. Da die vor den Augen des Wählers frisch generierte Zufallszahl mit an Sicherheit grenzender Wahrscheinlichkeit nicht identisch zu einer Füllstimme ist, hat der gewählte Kandidat nun eine Füllstimme übrig behalten. Die Anzahl der übrig gebliebenen Füllstimmen gibt also das Wahlergebnis in einer Form wieder, die einen mathematischen Beweis der Korrektheit erlaubt.

Im Folgenden wird das Verfahren über die drei Phasen Wahlvorbereitung, Wahl und Auszählung detaillierter wiedergegeben.

Wahlvorbereitung Zur Vorbereitung der Wahl werden für jeden Kandidaten gleich viele Zufallszahlen erzeugt. Die Anzahl dieser Zufallszahlen pro Kandidat sollte größer oder gleich der maximalen Anzahl von Wählern sein. Diese Zufallszahlen dienen als Füllstimmen und es muss für den Wähler nachvollziehbar sein, dass diese Stimmen vor der Wahl unabänderlich festliegen. Um die Zufallszahlen vertrauenswürdig zu hinterlegen, werden sie zusammen mit dem Namen des Kandidaten, für den diese Füllstimme steht, geeignet verschlüsselt und veröffentlicht. Für die Verschlüsselung werden sogenannte Commitments verwendet, die das kryptographische äquivalent zu einem versiegelten Umschlag sind. Die Verschlüsselung der Füllstimmen garantiert die Ununterscheidbarkeit von Füllstimmen und echten Stimmen und das Veröffentlichen stellt sicher, dass die Füllstimmen fest liegen.

Neben der Unabänderlichkeit der Füllstimmen sollte für den Wähler nachvollziehbar sein, dass jeder Kandidat gleich viele Füllstimmen erhalten hat. Dies ist sehr einfach und überzeugend durch zufällige Stichproben belegbar. Noch präziser als Stichproben sind sogenannte Zero-Knowledge-Beweise, die es ermöglichen nachzuweisen, dass jeder Kandidat gleich viele Füllstimmen erhalten hat, ohne dabei irgendwelche Information darüberhinaus preiszugeben[1].

Vor der Wahl ist also sichergestellt, dass jeder Kandidat gleich viele Füllstimmen erhalten hat und dass die Füllstimmen sowie die Zuordnung zu den Kandidaten unabänderlich festliegen. Da der Nachweis für alle Wähler derselbe ist, können keine einzelnen Wähler betrogen werden. Es wird damit eine hohe Sicherheit gewährleistet, da auch Medien und unabhängige Wahlbeobachter diese Nachweise überprüfen werden.

Wahl Die für das Verfahren notwendige Wahlmaschine besteht aus einem Wahlcomputer mit einem Bildschirm, einem Eingabegerät (etwa ein Touchscreen, bei unserem Prototypen eine Maus), einem Drucker und einem vertrauenswürdigen Zufallszahlengenerator mit eigener Anzeige.

Ein Wähler gibt seine Stimme an einer Wahlmaschine ab, nachdem seine Wahlberechtigung wie bei der klassischen Papierwahl geprüft wurde. Dabei sind durch das Verfahren selbst keine Einschränkungen gegeben. Die Darstellung und Stimmabgabe sowie etwaige Hilfen können an die Wahl angepasst werden.

Nachdem der Wähler seine Stimme abgegeben hat, erzeugt der Zufallszahlengenerator eine Zufallszahl und zeigt diese auf einem eigenen Display an. Der Wähler bekommt nun einen ausgedruckten Beleg und kann direkt in der Wahlkabine überprüfen, ob der Beleg korrekt ist. Dazu vergleicht er die Zufallszahl, die seine Stimme repräsentiert, mit der Zufallszahl, die vom Zufallszahlengenerator angezeigt wird. Stimmen diese überein, kann er sicher sein, dass die Wahlmaschine seine Stimme korrekt erhalten hat. Da die neue Zufallszahl frisch erzeugt wurde, ist der Wähler überzeugt, dass diese nicht von einer Liste mit Füllstimmen stammt. Deswegen wird die Stimme später gezählt.

Im Idealfall ist der Zufallszahlengenerator so gestaltet, dass es für den Wähler sofort ersichtlich ist, dass er korrekt arbeitet. Dies kann mechanisch geschehen, beispielsweise mit einer Lottotrommel oder einem Bingokäfig. Daher stammt auch der Name „Bingo Voting“.

Die Zufallszahlen auf dem Beleg, die nicht die abgegebene Stimme repräsentieren, stammen von den vorher festgelegten Listen der entsprechenden Kandidaten. Der Wahlcomputer streicht diese Zufallszahlen von den Listen, sobald sie für einen Beleg verwendet wurden, so dass eine Füllstimme nicht ein zweites Mal benutzt wird. Der gewählte Kandidat hat eine Füllstimme übrig behalten, wohingegen alle anderen Kandidaten eine Füllstimme für den Beleg „aufbrauchen“. Dies bildet die Basis für den nach der Wahl erfolgenden Beweis der Korrektheit der Auszählung.

Welche der Zahlen auf dem Beleg die frische Zufallszahl ist, hat nur der Wähler selbst gesehen. Daher ist es nicht möglich, mit diesem Beleg einem Dritten zu beweisen wie gewählt wurde.

[1] Konkret verwendet unser Prototyp Zero-Knowledge-Beweise nach dem Prinzip des Randomized Partial Checking. Um dies effizient zu erlauben werden als Commitment-Verfahren sogenannte Pedersen Commitments eingesetzt. Die während des Beweises zu treffenden Zufallswahlen werden, der allgemeinen Nachvollziehbarkeit wegen, über Hashfunktionen berechnet (Fiat Shamir Methodology).

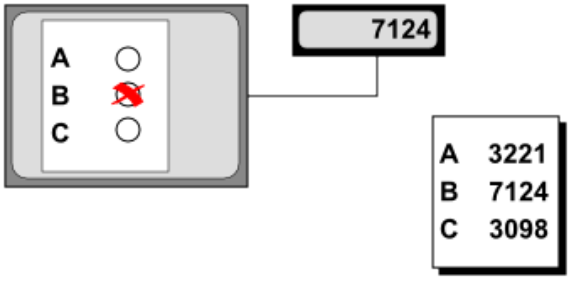

Abbildung 4: In der Wahlkabine: Der Wähler hat per Wahlcomputer (links) Kandidat B gewählt und bekommt einen Beleg (rechts), bei dem die zu Kandidat B gehörende Zufallszahl mit der Anzeige des Zufallszahlengenerators (mitte) übereinstimmt.

Erpressung oder Stimmenkauf sind dadurch ausgeschlossen, und trotzdem kann der Wähler die Korrektheit seiner Stimme prüfen.

Auszählung Die Auszählung geschieht anhand der nicht benutzten Füllstimmen. Der Kandidat, der die meisten Füllstimmen in seiner Liste behalten hat, gewinnt die Wahl. Die genaue Verteilung der Stimmen lässt sich aus der Anzahl der unbenutzten Füllstimmen und der Anzahl der Wähler berechnen.

Nach der Wahl werden neben dem Wahlergebnis noch weitere Informationen veröffentlicht:

- Alle unbenutzten Zufallszahlen (Füllstimmen) von den Listen der Kandidaten werden veröffentlicht (die Commitments werden geöffnet).
- Alle Belege werden veröffentlicht.
- Für jeden Beleg wird ein Zero-Knowledge-Beweis veröffentlicht, der beweist, dass der Beleg die richtige Anzahl Füllstimmen enthält. Aus dem Beweis wird dabei nicht ersichtlich, welche Stimme keine Füllstimme ist. Dieses Vorgehen sichert das Wahlgeheimnis.

Mit der Hilfe dieser veröffentlichten Daten kann

- jeder Wähler überprüfen, dass sein Beleg veröffentlicht und damit seine Stimme bei der Zählung berücksichtigt wurde,
- jeder nachvollziehen, dass für jeden Beleg von jeder bis auf einer Liste mit Füllstimmen eine Zufallszahl gestrichen wurde, und
- jeder nachvollziehen, dass die Anzahl der Belege mit der Anzahl der Wähler und dem Wahlergebnis korrespondiert.

Die letzten beiden Punkte können von jedem überprüft werden, unabhängig von der Teilnahme an der Wahl oder der Auszählung. Dadurch ist wieder eine hohe Sicherheit gewährleistet, da auch Medien und Wahlbeobachter diese Nachweise überprüfen können. Die Überprüfung, dass die Anzahl der Belege mit der Anzahl der Wähler übereinstimmt, erfolgt analog zur klassischen Papierwahl.

3 Nutzen

Das Ziel des Bingo-Voting-Verfahrens ist, die Vorteile von der Papierwahl, insbesondere die Überprüfbarkeit und Nachvollziehbarkeit der Auszählung, mit den Vorteilen von Wahlmaschinen zu verbinden, ohne die Benutzbarkeit des Verfahrens zu beeinträchtigen.

In diesem Abschnitt werden die konkreten Vorteile des Verfahrens anhand der vier Bereiche *Nachvollziehbarkeit*, *Wahlgeheimnis*, *Bedienbarkeit* und *Praktikabilität* vorgestellt.

Nachvollziehbarkeit Bingo Voting erlaubt es jedem Wähler die Korrektheit der Wahl zu überprüfen. Die Überprüfbarkeit des Wahlergebnisses und die damit verbundene höhere Legitimation der Regierung kann die Wahlbeteiligung erhöhen und der Politikverdrossenheit entgegenwirken. Hierzu ist es besonders wichtig, dass die Überprüfung nicht pauschal ist, sondern der Wähler die Wirksamkeit seiner eigenen Stimme direkt beobachten kann.

Bingo Voting schützt vor Wahlmanipulation ebenso wie vor fehlerhaftem Auszählen, da keine Annahmen über die Funktionsweise der Wahlmaschine oder die Korrektheit der Implementierung getroffen werden. Dies ist beispielsweise nicht der Fall für Verfahren, die mit Scannern und Mustererkennung arbeiten, denn dort muss aufgrund der Fehleranfälligkeit des Scanprozesses immer eine gewisse Toleranz gegeben werden, die prinzipiell auch für Wahlfälschung ausgenutzt werden kann. Im Unterschied dazu muss bei Bingo Voting für die beweisbare Korrektheit des Ergebnisses einzig dem Zufallszahlengenerator vertraut werden und nicht der ganzen Wahlmaschine.

Die Vertrauenswürdigkeit eines Zufallszahlengenerators ist viel leichter nachvollziehbar sicherzustellen, als die Sicherheit einer Maschine von der Komplexität eines Computers. Dabei hilft, dass für eine Wahlfälschung eine leichte Verschiebung der Verteilung der Zufallszahlen bei weitem nicht ausreicht. Idealerweise sollte der Zufallsprozess direkt beobachtbar sein. Bingo Voting kann mit einem Zufallszahlengenerator ähnlich einer Lotto-Maschine (oder eines Bingokäfigs) eingesetzt werden. Eine direkt beobachtete Lotto-Maschine ist in sehr hohem Maße manipulationssicher. Aber auch für den Zufallszahlengenerator, der bei dem ersten Praxiseinsatz von Bingo Voting verwendete wurde, ist die Vertrauenswürdigkeit in hohem Maße nachvollziehbar: Der Zufallszahlengenerator bestand aus einem zertifizierten Klasse-3-Chipkartenleser und einer zertifizierten Chipkarte.

Ein großer Vorteil von Bingo Voting ist die Entkopplung von der Teilnahme an der Wahl und der Überprüfbarkeit der Korrektheit der Auszählung. Bis auf den Vergleich der Zufallszahl, die bei dem gewählten Kandidaten steht, mit der Zahl, die der Zufallszahlengenerator anzeigt, sind alle Schritte des Beweises für jeden, also auch von Medienvertretern oder Wahlprüfern, nachvollziebar. Dies erhöht die gefühlte wie die reale Sicherheit, da man sich darauf verlassen kann, dass die komplizierteren Teile des Verfahrens „doppelt und dreifach“ verifiziert werden.

Wahlgeheimnis Wie bei den momentan eingesetzten Wahlmaschinen muss für die Geheimhaltung der abgegebenen Stimme die Wahlmaschine selbst auch manipulationssicher sein. Leider wird es auch keine einfache und von jedem Wähler nachvollziehbare Lösung dieses Problems geben, da nicht direkt nachgewiesen werden kann, dass die Maschine zu abgegebenen Stimmen

nicht die Uhrzeit notiert, oder dass die Wahlkabine durch eine Kamera überwacht wird.

Ist eine bei Bingo Voting eingesetzte Maschine nicht manipuliert, so ist die Geheimhaltung sogar informationstheoretisch sicher, d. h. das Wahlgeheimnis ist auch vor Angreifern mit unbegrenzter Rechenleistung geschützt. Da der Beleg für Dritte keinerlei Information über die abgegebene Stimme enthält, ermöglicht er weder Stimmenkauf noch Erpressung.

Im Vergleich zu einer Papierwahl wird in einem speziellen Punkt sogar das Wahlgeheimnis gestärkt. Bei einer Wahl mit klassischen Papierstimmzetteln, bei der Stimmen kumuliert werden können, kann im Zuge der Auszählung festgestellt werden, von wie vielen Wählern die Stimmen stammen. Damit können Personen, die bei der Auszählung anwesend sind, unterscheiden, ob ein Kandidat beispielsweise von vielen Wählern jeweils nur wenige Stimmen erhalten hat oder ob er von wenigen Wählern die jeweils größtmögliche Anzahl an Stimmen erhalten hat.

Weiterhin nimmt das Verfahren dem Wähler die Möglichkeit, seinen Stimmzettel zu markieren, beispielsweise indem er den Stimmzettel mit einem χ statt einem Kreuz versieht. Auch kann der Wähler nicht gezwungen werden, seinen Wahlzettel in einem bestimmten Muster auszufüllen („pattern voting“), was für den Angreifer aus der Quittung nicht ersichtlich wäre.

Praktikabilität Ein wichtiger Vorteil gegenüber herkömmlichen Wahlen ist, dass die Auszählung praktisch sofort nach der Wahl, die Nachprüfung der Korrektheit aber zeitlich und räumlich von der Wahl getrennt möglich sind. Dies erleichtert zum einen den Wahlhelfern die Arbeit erheblich. Zum Anderen ist es nicht mehr nötig, an einem bestimmten Tag bei einem bestimmten Wahllokal vor Ort zu sein, um die Auszählung zu überprüfen. Dies kann auch noch Tage und Wochen später mit öffentlichen Daten geschehen. Auch ist man nicht auf die Überprüfung eines einzigen Wahllokals beschränkt, sondern kann die Auszählungen aller Wahlbezirke und somit das Gesamtergebnis bequem von zu Hause aus nachprüfen.

Bedienbarkeit Gerade in einer Übergangszeit, in der der Einsatz von Wahlcomputern neu für den Wähler ist, spielt die Benutzbarkeit eine nicht zu unterschätzende Rolle. Der Wähler bedient den Wahlcomputer meist das erste mal in der Wahlkabine, d.h. er muss ihn ohne Vorbereitung verwenden können. Bingo Voting ist ein sehr flexibles Verfahren, das keine speziellen Anforderungen an die graphische Benutzeroberfläche des Wahlprogramms stellt. Diese kann somit so gestaltet werden, dass der Wahlvorgang für den Wähler intuitiv wird. Insbesondere stellt das Verfahren keine Anforderungen an das Layout des Wahlzettels, welcher so das dem Wähler vertraute Aussehen beibehalten kann. Verwendet man nun zur Stimmabgabe einen Touchscreen mit speziellem Stift, so muss der Wähler sich kaum anpassen. Der Einsatz von Bingo Voting bei der Studierendenparlamentswahl an der Universität Karlsruhe (TH) Anfang 2008 hat gezeigt, dass zumindest Studenten unvorbereitet mit dem Verfahren zurechtkommen.

Der Einsatz von Wahlcomputern zusammen mit einem flexiblen Wahlverfahren wie Bingo Voting bietet viele Möglichkeiten, den Wähler beim Wahlvorgang zu unterstützen: Es kann praktisch ausgeschlossen werden, dass versehentlich ein ungültiger Stimmzettel abgegeben wird. Außerdem kann der Wähler unterstützt werden, indem ihm die Anzahl der Stimmen angezeigt wird, die er noch vergeben kann. Gerade wenn die Wahl Kumulieren und Panaschieren erlaubt, ist eine solche Unterstützung hilfreich. Menschen mit Sehschwäche könnte eine Funktion zur Vergrößerung der

Schrift entgegenkommen. Die Installation einer zusätzlichen Audio-Ausgabe für blinde Wähler sowie weitere Unterstützungen für Menschen mit Behinderung wären denkbar.

Fazit Gegenüber herkömmlichen Wahlmaschinen bietet Bingo Voting den Vorteil, dass das Wahlergebnis nachprüfbar ist und selbst bei einer defekten oder manipulierten Wahlmaschine nicht unbemerkt verfälscht werden kann. Dabei werden die Vorteile von Wahlmaschinen gegenüber herkömmlicher Papierwahl hinsichtlich schneller Auszählung und Unterstützung bei der Stimmabgabe übernommen. Das Bingo-Voting-Verfahren vereinigt somit die Vorteile von Papierwahl und Wahlmaschinen, indem es eine schnelle Auszählung ermöglicht wärend die Verifizierbarkeit und einfache Benutzbarkeit erhalten bleiben.

4 Marktchancen

Der breite Einsatz von Wahlmaschinen hat gezeigt, dass das Interesse an Wahlverfahren, die eine schnelle Auszählung bieten, groß ist. So wurde in den Niederlanden flächendeckend mit Wahlmaschinen gewählt. Und in Deutschland werden die Wahlmaschinen von HSG Wahlsysteme (die die Wahlmaschinen von Nedap in Deutschland zur Verfügung stellen) nach eigenen Angaben inzwischen in etwa 90 Städten und Gemeinden in fünf Bundesländern eingesetzt.

Die Tatsache, dass in einigen Fällen von der weiteren Verwendung von Wahlmaschinen Abstand genommen wurde, zeigt auch, dass die bisherigen Lösungen nicht zufriedenstellend sind. In den Vereinigten Staaten von Amerika wird überlegt, nur noch Wahlmaschinen mit Papierbeleg einzusetzen. Und die Niederlande haben tatsächlich sämtliche Wahlmaschinen wieder abgeschafft, nachdem der Verein „Wij vertrouwen stemcomputers niet“ in einer publikumswirksamen Aktion demonstriert hat, dass eine Wahlmaschine vom Typ Nedap leicht zu einem Schachcomputer umfunktioniert werden kann [6].

An dieser Stelle können kryptographische Wahlverfahren glänzen, die Vorteile von Wahlmaschinen mit der Sicherheit und Akzeptanz der Papierwahl kombinieren. Beweisbare Korrektheit und Nachvollziehbarkeit gewinnen einen hohen Stellenwert bei der Bewertung und Auswahl des Wahlverfahrens.

Bei Bingo Voting ist die Korrektheit beweisbar, und damit insbesondere unabhängig vom Vertrauen in den Hersteller des Wahlcomputers. Der Vertrauensanker ist lediglich der Zufallszahlengenerator. Ein solches Gerät lässt sich allerdings so simpel konstruieren, dass es leicht fällt, die volle Funktionalität nachzuvollziehen und zu zertifizieren. Da ein solches Gerät auch recht klein sein kann (Signaturkarten tragen einen Zufallszahlengenerator in sich, so dass im Wesentlichen das Display die Größe bestimmt) ist auch die sichere Lagerung und Verteilung leicht sicherzustellen.

Da die Beweisbarkeit der Korrektheit auch unabhängig von der genauen Architektur des Wahlcomputers ist, kann dieser problemlos mit Software betrieben werden, deren Quellcode öffentlich bekannt ist (Open Source). Auch dies trägt zur Akzeptanz bei.

Ein weiterer wichtiger Faktor für die Akzeptanz ist dabei auch die Ergonomie des Wahlverfahrens. Hier liegt die große Stärke von Bingo Voting gegenüber anderen kryptographischen Verfahren. Es bietet nicht nur beweisbare Korrektheit, sondern ist dabei auch noch einfach zu bedienen – andere kryptographische Wahlverfahren haben hier deutliche Schwächen.

Der Mehraufwand für den Wähler ist gegenüber einer normalen Wahlmaschine gering. Sollte er von einzelnen Wählern dennoch als zu hoch empfunden werden, kann er sämtliche Schritte, die den Beleg betreffen, einfach auslassen. Damit bietet das Verfahren für ihn mindestens die Sicherheit und den Komfort heutiger Wahlmaschinen. Auch dies ist bei anderen Wahlverfahren so nicht möglich, da die Schutzmaßnahmen zu eng mit dem eigentlichen Wahlvorgang verzahnt sind.

Bei der Verwendung von Bingo Voting entstehen gegenüber herkömmlichen Wahlmaschinen dabei nur geringe Mehrkosten. Für die erste Wahl, die mit dem Bingo-Voting-Verfahren durchgeführt wurde, wurde ein Zufallszahlengenerator auf einer Signaturkarte verwendet. Die Wahl-

maschine selbst bestand aus einem handelsüblichen PC mit Drucker.

Bingo Voting sieht auch nicht vor, dass die Wahlmaschinen untereinander oder mit einem zentralen Server vernetzt sind. Dies ist nicht nur wichtig, um Aufwand und Kosten des Verfahrens so gering wie möglich zu halten, sondern auch um Angriffe zu vermeiden.

Durch die Entkopplung von Auszählung und Überprüfung des Wahlergebnisses ist das Verfahren auch für Demokratien geeignet, bei denen der Verdacht der Wahlmanipulation besteht. Bingo Voting macht es unabhängigen Wahlbeobachtern leichter, auch mit einer geringen Zahl von Beobachtern die Auszählung zu überprüfen.

Bingo Voting wurde bereits bei einer studentischen Wahl eingesetzt und konnte dabei seine Leistungsfähigkeit bei einer Wahl mit 70 Kandidaten und neun Stimmen pro Wähler sowie Kumulieren und Panaschieren unter Beweis stellen. Ähnliche Wahlen treten beispielsweise bei einigen Kommunalwahlen in Deutschland auf. Kein anderes kryptographisches Wahlverfahren bietet zur Zeit die Möglichkeit, eine solch komplexe Wahl praktikabel durchzuführen.

Bingo Voting bietet damit nicht nur die Vorteile von Wahlmaschinen, sondern räumt auch die Nachteile aus, die einem breiten Einsatz bisher im Wege gestanden haben.

Literatur

[1] Benjamin B. Bederson, Bongshin Lee, Robert M. Sherman, Paul S. Herrnson, and Richard G. Niemi. Electronic voting system usability issues. In *CHI '03: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 145–152, New York, NY, USA, 2003. ACM.

[2] Jens-Matthias Bohli, Jörn Müller-Quade, and Stefan Röhrich. Bingo Voting: Secure and Coercion-Free Voting Using a Trusted Random Number Generator. In A. Alkassar and M. Volkamer, editors, *VOTE-ID 2007*, volume 4896 of *Lecture Notes in Computer Science*, pages 111–124. Springer-Verlag, 2007.

[3] David Chaum. Punchscan, 2006. `http://punchscan.org/`.

[4] David Chaum, Peter Y.A. Ryan, and Steve Schneider. A Practical Voter-Verifiable Election Scheme. In Sabrina De Capitani di Vimercati, Paul Syverson, and Dieter Gollmann, editors, *Computer Security – ESORICS 2005*, volume 3679 of *Lecture Notes in Computer Science*, pages 118–139. Springer, 2005.

[5] Paul S. Herrnson, Richard G. Niemi, Michael J. Hanmer, Benjamin B. Bederson, Frederick G. Conrad, and Michael Traugott. The not so simple act of voting: An examination of voter errors with electronic voting, 2007.

[6] Constanze Kurz, Frank Rieger, and Rop Gonggrijp. Beschreibung und Auswertung der Untersuchungen an NEDAP-Wahlcomputern, 2007.

[7] Lucie Langer, Axel Schmidt, and Johannes Buchmann. Secure online elections in practice. Cryptology ePrint Archive, Report 2008/157, 2008. `http://eprint.iacr.org/`.

[8] Tal Moran and Moni Naor. Receipt-Free Universally-Verifiable Voting With Everlasting Privacy. In Cynthia Dwork, editor, *Advances in Cryptology – CRYPTO 2006*, volume 4117 of *Lecture Notes in Computer Science*, pages 373–392. Springer, August 2006.

[9] Stefan Popoveniuc and Ben Hosp. An Introduction to Punchscan. IAVoSS Workshop On Trustworthy Elections, WOTE 2006, 2006. `http://punchscan.org/papers/popoveniuc_hosp_punchscan_introduction.pdf`, online version dated 2006-10-15.

[10] Michael W. Traugott, Michael J. Hanmer, Won-Ho Park, Paul S. Herrnson, Richard G. Niemi, Ben B. Bederson, and Frederick G. Conrad. The impact of voting systems on residual votes, incomplete ballots, and other measures of voting behavior, 2005.