Über die Probleme der Automatisierung demokratischer Wahlen

Pavel Mayer, 10. November 2008
Version 1.7.1

URL: http://aggregat7.ath.cx/files/Wahlautomatisierung.pdf

Mail: pavel.mayer@gmail.com

„Diejenigen die wählen gehen entscheiden gar nichts. Die die Stimmen zählen entscheiden alles.“ - Josef Stalin zugeschrieben

„Es wird nie ein Wahlgerät geben können, das für sich alleine manipulationssicher ist.“
– Herbert Schulze Geiping: Geschäftsführer HSG Wahlsysteme GmbH / Nedap Deutschland

„Vertrauen ist gut, Kontrolle nicht möglich.“
– CCC: Fazit zur Wahl in Cottbus, bei der 74 Nedap-Wahlmaschinen eingesetzt wurden.

„Wenn die Leute vom Chaos-Computer-Club gezeigt haben, wie sie einen Wahlcomputer in 60 Sekunden hacken können, dann zeige ich ihnen, dass ich eine Wahlurne mit Stimmzetteln in 30 Sekunden austauschen kann.“
– Carl-Christian Dressel, stellv. Vors. des Wahlprüfungsausschusses des Bundestags: Stellungnahme in der mündlichen Verhandlung des Bundesverfassungsgerichts am 28. Oktober 2008 in Karlsruhe

Zusammenfassung

Weltweit ist derzeit kein Wahlcomputer im Einsatz, der die Anforderungen an demokratische Wahlen so gut erfüllt wie Urnenwahlen mit Stift, Papier und Handauszählung. Derzeitige Wahlcomputer und sogar automatische Zählhilfen brechen zudem die bei Urnenwahlen präsente *Selbstkontrollkette*, die es dem Wähler ermöglicht, sich persönlich vom Eingehen seiner Stimme in das Wahlergebnis zu überzeugen.

Demokratieverträgliche Wahlcomputer sind zwar denkbar, aber leider nicht praktikabel, denn die Sicherheit muss durch Mehrkosten oder erhöhten Aufwand für den Wähler so teuer erkauft werden, dass in der Praxis bei der Automatisierung auf Sicherheit und Kontrollmöglichkeiten verzichtet wird.

Die Ursache liegt im *Dilemma der elektronischen Wahl*: Man kann **mit einem elektronischen Gerät allein keine Wahl durchführen kann, die maximal gleich, geheim und frei ist**. Weil elektronische Datenverarbeitung unsichtbar ist und daher nicht unmittelbar kontrolliert werden kann, braucht es zusätzliche Massnahmen in Form sichtbarer Protokollierung, die jedoch das Wahlgeheimnis aufweicht und daher eigenständiger Schutzmechanismen bedarf. Auch weitere Methoden, etwa durch Expertengutachten, Offenlegung der Quellcodes, Kryptographie und Redundanz das Problem der Unsichtbarkeit zu kompensieren, erweisen sich bei näherer Betrachtung oft als ungeeignet oder sogar als problemverschärfend.

Auch Urnenwahlen mit Stift, Zettel und öffentlicher Handauszählung sind nicht hundertprozentig sicher, legen aber den Massstab sehr hoch. Was die Automatisierung so schwer macht, ist die Tatsache, dass Sicherheitsanforderungen an Wahlcomputer ungleich höher sein müssen als die bei Urnenwahlen, so wie die Sicherheitsanforderungen an eine computergesteuerte Magnetschwebebahn ganz andere sind, als die an ein Paar Schuhe. Eine Manipulation an einer Urne betrifft nur die Urne und kann durch Beobachter vor Ort verhindert werden. Eine Manipulation an der Software und Hardware von Wahlcomputern hingegen kann leicht Millionen von Wähler betreffen und so ausgeführt sein, dass sie nicht entdeckt werden kann.

Um den notwendigen Aufwand zu skizzieren, der für einen demokratieverträglichen Wahlcomputer notwendig ist, werden zwei unterschiedliche computerisierte Wahlverfahren skizziert, die die Grundanforderungen an demokratische Wahlen auch bei der notwendig strengen Auslegung erfüllen: Eine hinreichend sichere ***Stimmzetteldruckmaschine*** mit gesicherter Auszählung, und ein sehr einfaches zahlenbasiertes Verfahren, das ***Intermingled Key Voting*****,** das auch die Auszählung absichert und im Verhältnis von Einfachheit und Sicherheit vermutlich nahezu optimal ist.

Beide Verfahren jedoch können in der Praxis nicht gegen die Urnenwahl mit Papier und Stift bestehen, weil sie vielfach teuerer oder umständlicher zu bedienen wären als heute existierende Geräte. Dabei sind bereits die jetzigen billigen und unsicheren Wahlcomputer zu umständlich zu bedienen und prinzipiell unwirtschaftlich, da sie zu selten zum Einsatz kommen, um sich innerhalb ihrer Lebensdauer zu amortisieren.

Inhalt

Politischer Hintergrund

Nicht nur in in Deutschland liefern sich seit einigen Jahren Gegner und Befürworter von Wahlcomputern heftige Auseinandersetzungen auf politischer und juristischer Ebene.

Bei den Befürwortern stehen natürlich die Hersteller, zusammen mit den politischen Vertretern und Behörden, die Wahlmaschinen genehmigt oder für viel Geld beschafft haben, aber auch viele Wahlhelfer, die früher nach Hause können. Interessanterweise ist auch das Vertrauen der überwiegenden Mehrzahl der deutschen Wähler in Wahlcomputer bisher recht hoch, wenn auch aufgrund zunehmender Skandale im Abnehmen begriffen.

Auf der anderen Seite machen technisch versierte Experten und Bürgerrechtsgruppen zunehmend Druck, da das Ausmass der Sicherheitsprobleme von den Wahlmaschinenbefürwortern offenbar nicht als ausreichend gravierend betrachtet wird, als das sie von sich aus Konsequenzen daraus ziehen würden.

Die Auseinandersetzung vollzieht sich auch auf der semiotischen Ebene: Befürworter bezeichnen Wahlcomputer lieber verharmlosend als Wahlmaschinen, Gegner präferieren den Begriff *Wahlcomputer*, ähnlich wie bei Gegnern von *Atom*- und und Befürwortern von *Kern*kraft. Der Gesetzgeber verwendet die Bezeichnung *Wahlgeräte*, denn die Verordnung stammt bereits aus dem Jahre 1975, eine Zeit, in der die ersten Mikroprozessoren gerade frisch am Markt waren und noch niemand zu Hause einen Computer hatte.

Im 28. November 2006 wurde beim Petitionsauschuss des Deutschen Bundestages eine der mit 45.126 Namen unterzeichnete Petitionen behandelt: Eine Petition zum Verbot von Wahlcomputern.

Automatisierungsdrang

Die Gründe für den Wunsch nach Wahlcomputern liegen auf der Hand: Der Einsatz von Wahlcomputern vermittelt den Anschein von Modernität und erscheint irgendwie zeitgemäss. Handarbeit ist teuer und rückständig. Und tatsächlich: Automatisierung kann grundsätzlich viel Zeit und Geld sparen und die Produktqualität stark verbessern. Das sind wir aus der Automobilproduktion genau so gewohnt wie beim Einsatz von Computern in Unternehmen und Verwaltungen. Computer können grosse Mengen von Daten speichern, auswerten, übertragen und dieses mit einer hohen Präzision wiederholen. Dies wäre sicher auch beim Wählen wünschenswert.

Am besten wäre es sogar, wenn man sich zum Wählen gar nicht zum Wahllokal begeben müsste, denn das ist das Teuerste am Wählen. Jede Wahl im Wahllokal dürfte mit Hin- und Rückweg rund 25 Minuten dauern, was im Durchschnitt auf 7 Euro Kosten für den Wähler hinausläuft, während die öffentliche Hand 2 Euro je Wähler bei Urnenwahlen aufwenden muss. [O]

Allerdings wären Online-Wahlen von Zuhause aus in Deutschland ohnehin nicht ohne weiteres möglich, denn das Bundesverfassungsgericht hat der Präsenzwahl im Wahllokal absoluten Vorrang eingeräumt. Nach Ansicht des Bundesverfassungsgerichts ist nur bei der Präsenzwahl sicher, dass die Stimmen geheim bleiben und nicht verkauft oder erpresst werden können. [POHLE07]

Vorteile von Wahlcomputern

Wahlcomputer ermöglichen schnelles Auszählen: In einem typischen deutschen Wahllokal spart ein Wahlcomputer rund zwei Stunden Arbeitszeit von vier Wahlhelfern ein; das sind ca. 20% der Zeit, die von den Wahlhelfern aufgebracht werden muss. Personal wird in deutschen Wahllokalen nicht eingespart, das Gesetz schreibt dieselbe Zahl an Wahlhelfern vor wie bei Urnenwahlen. [BWahlGV]

Ansonsten wird noch gelegentlich ins Feld geführt, dass mit Wahlcomputern vielsprachige Benutzerschnittstellen möglich sind, was aber mit Stimmzetteln auch möglich ist. Des weiteren ermöglichen Wahlcomputer noch besonders komplizierte Wahlverfahren, die bei der Durchführung mit Stimmzetteln oft viele ungültige Stimmen aufweisen.

Gute Benutzerschnittstellen können sicherlich auch helfen, die richtige Wahl zu treffen. Dass die Benutzerschnittstellen gegenwärtiger Wahlcomputer dies leisten, kann nicht überzeugend behauptet werden. Im besten Fall sind diese Stimmzetteln nachempfunden. [PTB04]

Wahlcomputer können auch unter Umständen Manipulationen durch abgesprochene Wahlhelfer erschweren.

Nachteile von Wahlcomputern

Wahlcomputer sind teuer. Die Kosten von Wahlen mit Wahlcomputern in Amsterdam, Köln und Cottbus waren jeweils etwa doppelt so teuer wie die Wahlen mit Stimmzetteln. [O]

Der Einsatz von Wahlcomputern ist riskant. Derzeit erfüllt kein existierender Wahlcomputer die Standards für demokratische Wahlen, die seit der Einführung von Wahlurnen in Australien im Jahre 1858, seit 1892 in den USA und seit 1924 in Deutschland gelten.

Wahlcomputer schrecken Wähler ab und senken die Wahlbeteiligung. Darauf wird im Kapitel *Psychologische Effekte beim Wahlcomputereinsatz* näher eingegangen.

Urnenwahlen

Urnenwahlen sind einfach, robust, sicher und anonym. Und haben sich seit Jahrhunderten bewährt. Aber sie sind nicht perfekt.

Als Problem der Urnenwahl wird oft angeführt, dass Fehler beim Ausfüllen eines Wahlzettels diesen ungewollt ungültig machen können. Allerdings muss es auch beim Wählen am Computer möglich sein, eine ungültige Stimme abzugeben. Und wer damit überfordert ist, einen Wahlschein richtig auszufüllen, würde womöglich sein Kreuz ohnehin an der falschen Stelle machen. Da ist ihm mit einem ungültigen Wahlschein besser gedient.

Wenn aber das Wahlverfahren so kompliziert ist, dass es sich für Urnenwahlen nicht gut eignet, sollte man sich auch die Frage stellen, ob es sich für den Wähler eignet.

Die Genauigkeit von Urnenwahlen ist in der Regel ausreichend, es gibt aber sicher Fehler. Bruce Schneier erwähnt allerdings Fehlerquoten von 5%, ohne jedoch eine Quelle zu nennen.[SCHNEIER04] Verlässliche Untersuchungen oder gar Vergleiche zwischen Urnen- und Computerwahlen, die mit einer repräsentativen Gruppe von Wählern durchgeführt wurden, sind nicht bekannt.

Ist ein Wahlausgang sehr knapp, werden immer wieder Zweifel an der Genauigkeit der Auszählung geäußert. Es wäre in einer solchen Situation sicher schön, wenn jeder Wähler überprüfen könnte, dass seine Stimme gezählt wurde. Das leisten Urnenwahlen nur in Verbindung mit hohem zusätzlichen Zeitaufwand für den Wähler, aber sie leisten es. Jeder Wähler kann, wenn es ihm wichtig ist, seinen Wahlschein unauffällig individuell markieren und bei der Handauszählung zusehen. Und er kann in der Zeitung nachlesen, ob das richtige Ergebnis für seinen Wahlkreis bekanntgegeben wurde. **Fällt die Handauszählung weg, so bricht diese Kette.** In der Praxis gibt es sicher derzeit nur wenige Wähler, die diesen Aufwand betreiben, es ist aber wichtig, dass jeder es könnte, wenn es einmal darauf ankäme. Schöner wäre natürlich, wenn man als Wähler mit geringerem Aufwand die Berücksichtigung der eigenen Stimme im Wahlergebnis feststellen könnte.

Denn Manipulation von Urnenwahlen sind möglich, fallen aber in der Regel auf, wenn sie in größerem Umfang praktiziert werden, denn grossflächige Manipulationen von Urnenwahlen sind sind aufwändig und erfordern viele Mitwisser, in der Regel mehrere tausend, um wenige Prozent der Stimmen umzuverteilen. [BREN06] Und es ist meist nicht schwer, Manipulationen nachzuweisen. Und das manchmal sogar nach über 2400 Jahren: Im Jahre 1937 wurden bei Ausgrabungen an der Akropolis grössere Mengen Tonscherben eines Scherbengerichts gefunden, dass im Jahre 471 v.Chr. stattfand[BRON38]. Die Scherben waren von nur 14 verschieden Personen beschriftet, was auf Verschwörung zum Wahlbetrug hindeutet. Ob das mit dazu beigetragen hat, dass Themistokles beim Scherbengericht schuldig gewählt wurde und das Land verlassen musste, ist allerdings unwahrscheinlich. Die “gefälschten” Scherben waren an einem Platz und sind also entweder aussortiert worden oder gar nicht zum Einsatz gekommen. Es hat also entweder die Abschreckung bei der Urnenwahl funktioniert, oder sie wurden erwischt.

Erfolgreich hingegen war das in Italien lange Zeit praktizierte nachträgliche Ankreuzen leerer Stimmzettel beim Auszählen, dass für überzeugte linke Wahlhelfer Ehrensache war.

Im Übrigen ist das Auszählen von Stimmzetteln per Hand zwar keine intellektuell herausfordernde, aber eine ehrenvolle und durchaus interessante Arbeit; der spannende Höhepunkt eines langen Tages als Wahlhelfer. Es gibt sicher genug Menschen, die diese Arbeit gern tun.

Und es sollte sich jeder dafür interessieren, in der Praxis aber siegt bei den meisten von uns die Bequemlichkeit, und wir überlassen das Zählen unbeaufsichtigt Anderen, die werden es schon richtig machen und sich gegenseitig kontrollieren. Dabei ist das Vertrauen derzeit wohl auch gerechtfertigt.

Wahlgeheimnis angesichts von DNA- und Fingerabdruckdatenbanken

Ein mag zwar als Kuriosum erscheinen, aber das umfängliche Sammeln von DNA- und Fingerabdruckdatenbanken, wie es auch in vielen Demokratien angestrebt wird, gefährdet die Merkmale “frei” und “geheim” bei der Urnenwahl, da der Wähler auf dem Wahlschein DNA und Fingerabdrücke hinterlässt, so dass Wahlzettel eindeutig Wählern zugeordnet werden könnten. Computerwahlen sind zwar hinsichtlich DNA- und Fingerabruckspuren prinzipbedingt sicherer, bieten aber dafür einfachere Möglichkeiten, das Wahlgeheimnis zu verletzen, wie etwa “Covert Channels” oder kompromittierende elektromagnetische Emission (Tempest) und sind daher nicht sicherer. Abhilfe schafft nur das Verbot derartiger breit angelegter Sammlungen von Daten unbescholtener Bürger.

Zusammenführung und Bekanntgabe von Wahlergebnissen

Für den einzelnen schwieriger zu entdecken sind Manipulationen bei der Zusammenführung und der Bekanntgabe des Ergebnisses, da diese im Gegensatz zur Stimmabgabe selbst in Deutschland nicht öffentlich sind. Das Problem tritt aber bei Computerwahlen ebenfalls und dort in potentiell verschärfter Form auf, falls Daten automatisch erhoben und übermittelt werden.

Allerdings gibt es derzeit für den Wähler die Möglichkeit, bei der Bekanntgabe der Wahlergebnisse im Wahllokal diese aufzuschreiben und dann mit den veröffentlichen Zahlen zu vergleichen. Dies wird zwar eher selten praktiziert, allerdings genügt die Möglichkeit, dieses zu tun, um Betrüger abzuschrecken.

In Italien etwa wurde der Versuch vereitelt, bei der Auszählung einen Teil der ungültigen Stimmen auf eine Partei umzuverteilen. [TS06],[SZ06],[TISC06]

Selbstkontrollkette

Wie wir sehen konnten, gibt es bei ordentlich praktizierten Urnenwahlen mit Stift und Zettel sowie einer öffentlichen Handauszählung und Bekanntgabe des Ergebnisses im Wahllokal eine sehr sichere *Selbstkontrollkette*, die der Wähler selbstständig verfolgen kann, ohne Dritten vertrauen zu müssen. Er kann die leere Urne bei Wahlbeginn sehen, den ganzen Tag auf die Urne aufpassen, bei der Auszählung mit zusehen, seinen Wahlschein unauffällig markieren und sich von seiner richtigen Zählung überzeugen. Und er kann überprüfen, dass das veröffentlichte Ergebnis mit dem im Wahllokal ermittelten Ergebnis übereinstimmt.

Das Vorhandensein dieser Kette ist nicht nur eine Massnahme, die Wahlbetrug verhindert, sie stärkt vor allem das Vertrauen der Wähler in den Wahlvorgang und ist Vorraussetzung für die Legitimation der Gewählten. Wer in einer Wahl ohne intakte *Selbstkontrollkette* gewählt wird, muss sich zu Recht dem Zweifel der Wähler aussetzen, ob er tatsächlich legitimiert ist. Dem sollte keinem Mandatsträger zugemutet werden.

Gegenwärtig ist aber die *Selbstkontrollkette* bei Urnenwahlen in Deutschland eher die Theorie als die Praxis. Das muss aber nicht immer so bleiben, und die Möglichkeit der Kontrolle abzuschaffen, nur weil sie nicht genutzt wird, mag zwar kurzfristig ökonomisch sinnvoll, langfristig möglicherweise verheerend sein.

Auch mit Wahlcomputern lässt sich eine derartige *Selbstkontrollkette* realisieren. Da dies nicht einfach zu bewerkstelligen ist, brechen sämtliche derzeit existierenden Wahlcomputer diese Kette. Mittels Wahlcomputern gewählte Mandatsträger sind also derzeit potentiell nicht legitimiert.

Ein theoretischer Ausweg wäre ein Verfahren wie das später beschriebene *Intermingled Key Voting*, das aber bei Wählern und Wahlveranstaltern für wenig Begeisterung sorgen dürfte.

Anforderungen an eine Demokratische Wahl

Demokratische Wahlen müssen unter anderem gleich, geheim und frei sein. [GG] (Art.38) “Gleich” bedeutet, das jeder Wähler nur eine Stimme hat, und kein Kandidat systematisch benachteiligt wird. “Geheim” bedeutet, das niemand wissen kann, wie ein bestimmter Wähler abgestimmt hat, was eine wichtige Voraussetzung für “freie” Wahlen ist, bei denen niemand Stimmen kaufen oder erpressen kann.

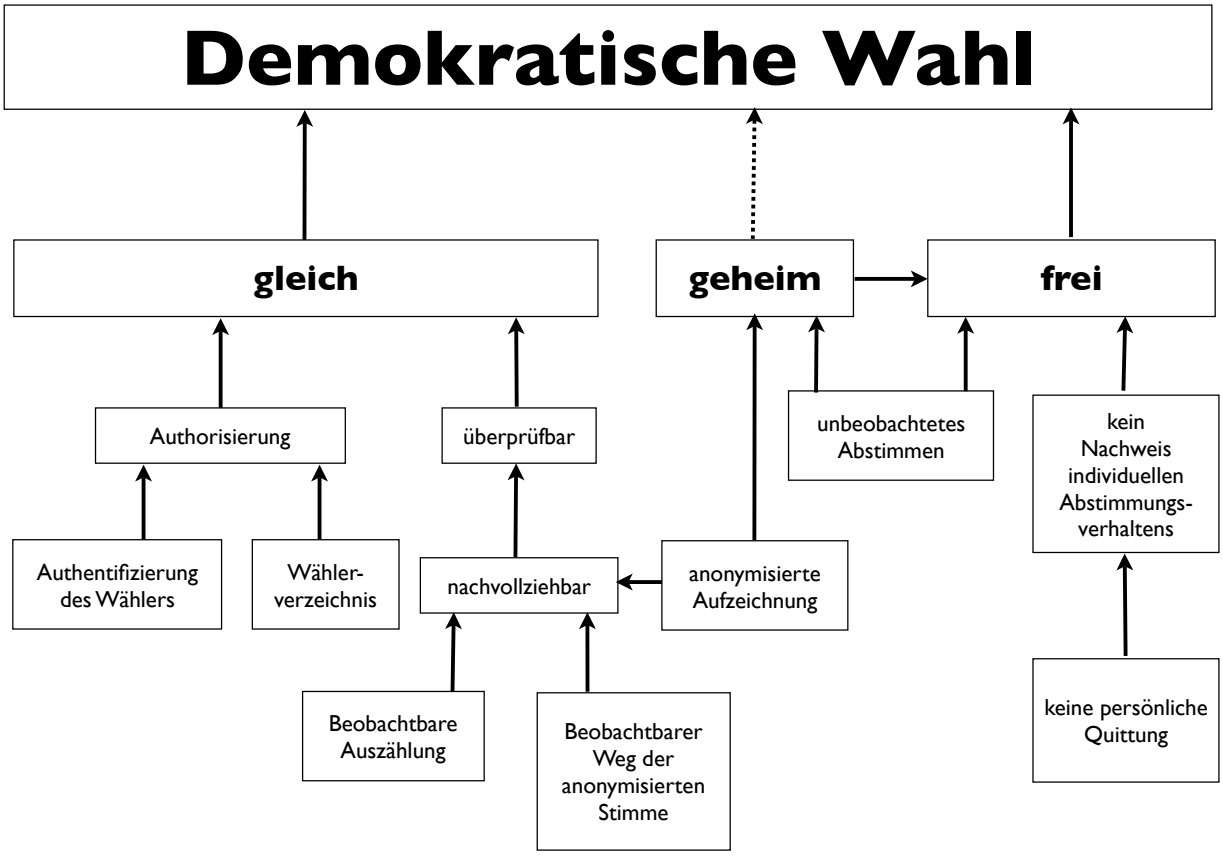

Bild 1

Kausalitäten bei der Erfüllung der Anforderungen an eine Demokratische Wahl

"**Gleiche** Wahlen" bedeutet im Wesentlichen, dass jeder Wähler genau eine Stimme hat. Er muss davon abgehalten werden, mehrere Stimmen abzugeben, was bei uns durch Authentifizieren, Abgleichen mit und Abstreichen im Wählerverzeichnis erfolgt.

Es muss also gesichert sein, dass die abgegebene Stimme auch zählt, und niemand die Möglichkeit hat, diese zu verfälschen oder zusätzliche Stimmen einzuschleusen. Hierzu muss der Wahlvorgang **überprüfbar** sein. Um ihn zu überprüfen, muss die Wahl durch Dritte **nachvollziehbar** sein, was wiederum einer **Aufzeichnung** bedarf, etwa ein Kreuz auf einem Stimmzettel, dessen Weg wiederum einschliesslich der Auszählung **beobachtbar** sein muss.

Das Wahlen **geheim** sein müssen, ergibt sich aus der Anforderungen, dass der Wähler **frei** von Zwang oder direkter Belohnung seine Stimme abgeben kann. Dazu muss die Aufzeichnung seiner Stimme **anonymisiert** werden, und er muss die Stimme **unbeobachtet** abgeben.

Um schliesslich eine Beeinflussung durch Stimmenkauf zu unterbinden, darf der Wähler auch keine Möglichkeit erhalten, sein individuelles Abstimmungsverhalten nachzuweisen; eine etwaige Quittung darf also keine Hinweise darauf enthalten.

Urnenwahlen erfüllen diese Anforderungen. Sie sind zwar nicht perfekt, aber erstaunlich leistungsfähig. Das liegt vor allem an deren Einfachheit, Beobachtbarkeit und Nachvollziehbarkeit. Stimmzettel können in einer Wahlkabine unbeobachtet ausgefüllt werden. Sie werden beim Einwurf in die Urne anonymisiert. Die Urne kann von Wahlbeginn an beobachtet werden: Dass sie zu Beginn der Wahl leer ist, und dass sich während der Wahl niemand daran zu schaffen macht, wird durch ein einfaches Schloss erschwert. Ein Austausch der Urne ist zwar möglich, kann aber durch Beobachter leicht unterbunden werden.

Gelegentlich wird durch Verschwörung der Wahlhelfer versucht, echte Stimmzettel gegen gefälschte auszutauschen, was zwar riskant, aber machbar ist, sofern kein aufmerksamer fremder Beobachter zugegen ist.

Schwieriger hingegen ist es, Wahlzettel überzeugend zu fälschen, da jeder Wähler die Kreuze auf dem Wahlzettel mit unterschiedlicher Linienführung, Stifthaltung, Andruck und Beschleunigung ausführt, so dass das überzeugende Fälschen einer hohen Zahl von Stimmzetteln schwierig ist. Allerdings wurden in der Vergangenheit häufiger in Italien erfolgreich leer eingeworfene Stimmzettel beim Auszählen nachträglich für eine Partei markiert. [TS06]

Warum ist es so schwer, mit einem Wahlcomputer den Standard von Urnenwahlen zu erreichen oder zu übertreffen? Schliesslich gibt es auch Systeme, die täglich Milliarden von Zahlungstransaktionen durchführen. Es gibt Geldautomaten, Spielautomaten, Fahrschein- und Flugticketautomaten. Warum sollte es keine praktikablen Wahlcomputer geben?

Das Problem ist, das die Anforderungen an Wahlcomputer wesentlich höher sind als die Anforderungen an obige Geräte: Es entspricht dem Problem, ein Konto bei einer Bank zu führen, wobei die Bank den Kontostand nicht kennen darf und ich keine Möglichkeit haben darf, meinen Kontostand einem Dritten nachzuweisen, aber dennoch sichere Finanztransaktionen durchführen kann.

Zudem sind die Anreize für eine Manipulation so extrem hoch, das sie meist unterschätzt werden. Mann stelle sich vor, wie viel eine US-Präsidentschaft oder eine Mehrheit im Bundestag wert sind.

Gelegenheit macht Diebe: Aus der Sicherheitsforschung ist bekannt, dass die Tatbereitschaft eines Kriminellen im wesentlichen von der Höhe der potentiellen Beute und von der vermuteten Wahrscheinlichkeit der Entdeckung abhängen. Das zu erwartende Strafmaß ist dabei weniger entscheidend, und auch die moralische Ächtung eines bestimmten Verhaltens ist, wie sich immer wieder zeigt, auch bei hohen Amtsträgern und wichtigen Personen des öffentlichen Lebens keine Garantie für Gesetzes- und Moraltreue - Kriminelle gibt es allen sozialen Schichten und Berufen. Hingegen ermöglichen es das öffentliche Vertrauen und die Mittel, über die derartige Personen und die von ihnen geführten Organisationen verfügen, die Entdeckungswahrscheinlichkeit erheblich zu verringern und damit zum Teil über Jahrzehnte hinweg fortgesetzt kriminell tätig sein zu können.

Schwerwiegender aber ist, dass Wahlcomputer im Gegensatz zu Wahlurnen Manipulationen ermöglichen, die von **einer einzigen Person** an der richtigen Stelle ausgeführt werden können und sämtliche Wahlcomputer betreffen. Damit bekommt ein kleiner Personenkreis oder ein Einzelner einen mächtigen Hebel in die Hand, und Millionen müssen blind darauf vertrauen, dass niemand der Versuchung erliegt, ihn zu betätigen.

Die mögliche Beute dabei ist hoch: Politik ist der Ausgleich von Interessen unterschiedlicher Interessengruppen, und bundespolitische Entscheidungen bewirken meist die Umverteilung vieler Milliarden Euro und können die Lebensbedingungen von Menschen bis hin zur physischen Existenz beeinflussen. Auch hängt die Prosperität vieler Branchen in erheblichem Masse von den gesetzlichen Rahmenbedingungen ab, selbst wenn man die Rolle des Staates als kaufkräftiger Auftraggeber ausser acht lässt.

Abseits finanzieller Erwägungen stellt aber die Demokratie ein so wichtiges Gut dar, dass es sich mit Geld tatsächlich nicht messen oder aufwiegen lässt. In letzter Konsequenz handelt es sich, auch wenn es pathetisch klingen mag, um eine Frage von Leben und Tod.

Zwar verfügt unsere Demokratie über zusätzliche Sicherungsmechanismen, wie etwa Presse-, Organisations- und Versammlungsfreiheit und eine aus dem Grundgesetz abgeleitete Rechtsprechung, aber selbst der “Ewigkeitsschutz” der §§1-20 des Grundgesetzes, so hat sich 1933 gezeigt, kann nicht verhindern, das der Gewinn einer einzigen Wahl eine Dynamik mit katastrophalen Folgen heraufbeschwört.

Ablauf einer Wahl

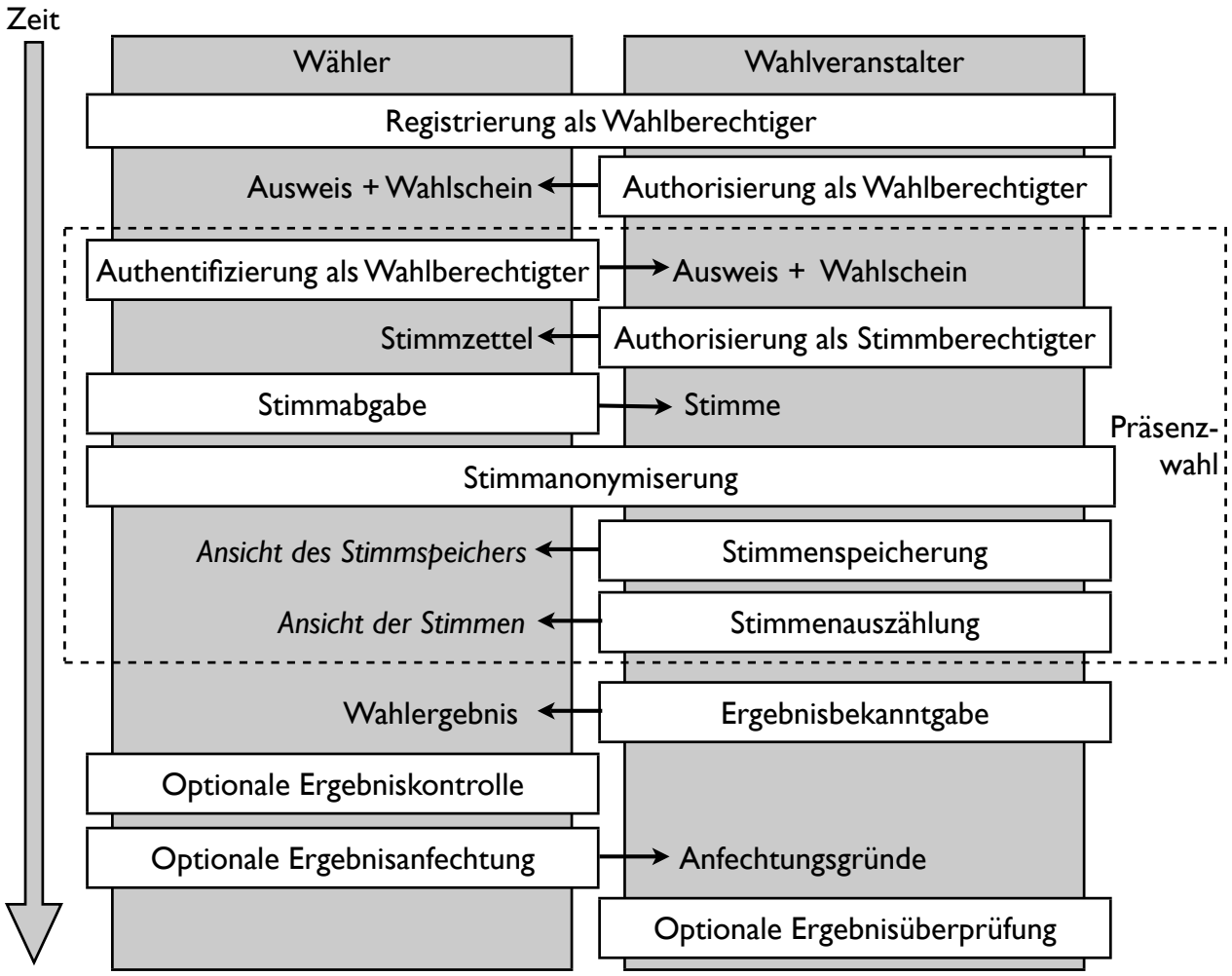

Bild 2

Der hier vereinfacht dargestellte Wahlprozess ist eine vielstufige Interaktion zwischen Wähler und Wahlveranstalter. Dabei werden Informationen ausgetauscht, bei der Urnenwahl in Form von "Token", üblicherweise bedrucktes und/oder beschriebenes Papier. Zusätzlich findet potentiell Kommunikation durch die passive Beobachtung des Wählers statt, etwa bei der Beobachtung des Ablaufs oder der Auszählung.

Eine freie und geheime Wahl ist ein überraschend vielstufiger Prozess, der aber einfach genug sein muss, dass ihn jeder Bürger vollziehen kann.

Im Zentrum der Wahl steht die Kommunikation der individuellen Wahlentscheidung. Sie wird vom Wähler kodiert und gesendet. Beim Empfang darf die Identität des Senders nicht zusammen mit der Wahlentscheidung gespeichert werden, aber auch die Wahlentscheidung muss geheim bleiben, so lange sie nicht anonym gespeichert ist.

Im Nachhinein soll aber überprüfbar sein, dass die Entscheidung so getroffen wurde und nicht anders, und dass nur die Entscheidungen Berechtigter Eingang ins Ergebnis gefunden haben.

Wenn die Stimme für eine Partei vollkommen selbstidentisch gespeichert wird, entfällt jede Nachprüfbarkeit. Es muss also eine Zusatzinformation zur Stimme gespeichert werden, die irgend eine Art von Überprüfung ermöglicht. Diese Zusatzinformation schwächt aber prinzipiell das Wahlgeheimnis. Insofern müssen grundsätzlich Abwägungen hinsichtlich der Anforderung der Gleichheit und der Freiheit der Wahl getroffen werden.

Verzichtet man auf die Speicherung der Zusatzinformation zur Stimme und damit auf die Nachprüfbarkeit, so kann man theoretisch durch Transparenz und lückenlose Beobachtbarkeit des Wahlvorgangs ebenfalls die Korrektheit des Wahlergebnisses sicherstellen. Das ist aber in der Praxis schwierig und bei elektronischer Verarbeitung unmöglich. Dies führt zum *Dilemma der elektronischen Wahl*.

Das Dilemma der elektronischen Wahl

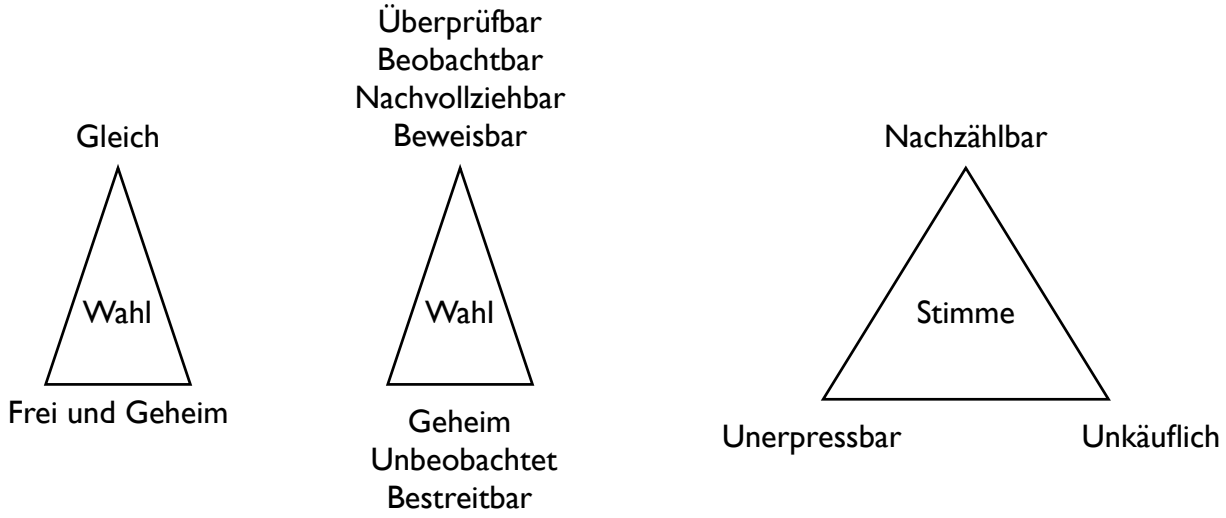

Bild 3

Das *Dilemma der elektronischen Wahl* entspringt dem offensichtlichen funktionalen Konflikt zwischen den Anforderungen *Geheim* und *Überprüfbar* in Verbindung mit der *Unsichtbarkeit* elektronischer Datenverarbeitung.

Beim Entwurf von Wahlverfahren ergibt sich für den Entwickler der Eindruck, dass jede Verbesserung des Verfahrens hinsichtlich einer der Eigenschaften unvermeidbar Verschlechterungen hinsichtlich einer der anderen Eigenschaften nach sich zieht.

Dies ist Ausgangspunkt für die These, dass man **mit einem elektronischen Gerät allein keine Wahl durchführen kann, die zugleich maximal gleich, geheim und frei ist**. Das gilt auch für kryptographische Verfahren, denn diese speichern Zusatzinformationen zur Stimme, so dass diese nicht mehr selbstidentisch ist und damit potentiell eine Entscheidung einem Wähler zugeordnet werden kann[1]. Verzichtet man auf die Speicherung der Zusatzinformation, so geht die Nachprüfbarkeit verloren.

Um elektronisch Wählen zu können, gilt es also, ein vernünftiges Gleichgewicht zwischen diesen Anforderungen auf hohem Niveau zu erzielen. Das ist bei elektronischen Verfahren besonders schwierig, denn elektronische Verfahren beinhalten grundsätzlich ein *Dematerialisieren* der Stimmabgabe. Ein Tastendruck bewirkt eine Ladungsverschiebung, die sich unsichtbar im Gerät als digitales Signalfeld fortpflanzt in in Form elektrischer Ladungen oder magnetischer Felder gespeichert wird.

[1] Es können zwar Schutzmassnahmen in Form geeigneter kryptografischer Methoden getroffen werden, die aber bei Bekanntwerden von Schlüsseln oder Angriffen auf das Verfahren ausgehebelt werden können. Siehe Kapitel “Kryptografische Methoden”, “Intermingled Key Voting” und “Bingo Voting”.

Der Mensch verfügt über keine Sinne, die derartige Ladungen und Felder direkt wahrnehmen können. Die Signalfelder repräsentieren digitale Informationen, die im Gerät durch programmierbare Logikschaltkreise so verrechnet und hin und her kopiert werden, das zu einem späteren Zeitpunkt beispielsweise digitale Summen gebildet werden können. Dieser Vorgang ist an sich deterministisch, das heisst, theoretisch kann bei Kenntnis aller Details des Verarbeitungsvorgangs logisch geschlussfolgert und bewiesen werden, dass Stimmabgaben in Form von Tastendrücken in allen Fällen zu einem korrekten Wahlergebnis führen.

Zu den Details, deren Kenntnis es zur Überprüfung bedarf, gehören neben den Programmen (Software) auch detaillierte Kenntnis der Hardware einschliesslich der Logik des Prozessors, der Speicherbausteine, der Schnittstellen sowie Ein/Ausgabegeräte. In der Praxis hingegen ist es noch immer nicht möglich, die Korrektheit von Programmen zu beweisen, die nur einige hundert Funktionen bzw. Codezeilen enthalten. Ausserdem ist es keinem einzelnen Menschen mehr möglich, die Funktionsweise eines modernen Mikroprozessors mit Millionen von Logikfunktionen vollständig nachzuvollziehen. Sämtliche Mikroprozessoren enthalten hunderte bekannter und unbekannter Designfehler, die unter bestimmten Umständen zu Fehlfunktionen führen, die oft unbemerkt bleiben. Aus der Forschung sind auch Mikroprozessoren bekannt, die Hintertüren enthalten, mit denen jeder in Software enthaltener Schutzmechanismus ausgehebelt werden kann. [LEET-08][DSB05][PM08]

Schwerwiegender aber ist, das eine selbst lückenhafte und oberflächliche Untersuchung nur durch Experten zu leisten ist, die auch noch Falle der meisten kommerziellen Systeme vom Staat oder vom Hersteller bezahlt werden und ihre Ergebnisse nur lückenhaft veröffentlichen. Die Hersteller weigern sich, Geräte für unabhängige Prüfungen zur Verfügung zu stellen, da durch eine unabhängige, öffentliche Prüfung die praktizierte *Security by Obscurity* sofort vollständig unwirksam würde. Die Aufdeckung der Schwachstellen im Falle der NEDAP-Computer hat daher einige Jahre auf sich hat warten lassen. So wurde eine Zulassung für diese Geräte erlangt, und obwohl sie in Holland aus dem Verkehr gezogen wurden, werden in Deutschland noch immer verkauft und verwendet. Dabei ist NEDAP eine holländische Firma, und die Geräte wurden in 90% aller Wahlbezirke und damit nahezu flächendeckend eingesetzt, so dass die Entscheidung zum Verbot von Wahlcomputern sicher nicht leicht gewesen ist. [DEPAC07]

Dass die einfache Manipulierbarkeit der Geräte nicht öffentlich bekannt war, schließt aber eine erfolgte Manipulation oder Fehlfunktionen nicht aus, im Gegenteil: Wie man aus hunderten bei *blackboxvoting.org* dokumentierten Fällen in den USA weiss, finden ohne gesundes Misstrauen die Ergebnisse selbst schwerwiegender Manipulationen und krasser Fehlfunktionen Eingang ins offizielle Wahlergebnis. [BBV][HEISE161106]

Public Source Voting

Doch nehmen wir an, der Gesetzgeber würde dafür sorgen, dass alles öffentlich gemacht werden muss und Wahlcomputer jederzeit einzeln unabhängig geprüft werden können und alle technischen Informationen und Quellcodes veröffentlicht werden müssen, könnte man elektronischen Wahlcomputern dann vertrauen?

Zwar wären derartige Wahlcomputer scheinbar vertrauenswürdiger als die heutigen Geräte, aber eine Wahl mit diesen Geräten wäre immer noch nicht überprüfbar, denn es gibt keine Möglichkeit für den Wähler im Wahllokal zu überprüfen, ob der Wahlcomputer tatsächlich mit dieser offengelegten Software arbeitet, und selbst wenn dies der Fall ist, kann immer noch die Hardware manipuliert sein.

Die gängige Form der Überprüfung läuft zudem ins Leere. Wenn ein Wahlcomputer vor und nach der Wahl korrekt funktioniert, deutet das nach unserer alltäglichen Erfahrung zwar darauf hin, dass er auch während der Wahl korrekt funktioniert hat, im Falle programmierbarer Rechner kann aber eine absichtliche oder unabsichtliche Fehlfunktion so programmiert sein, dass sie nur bei echten Wahlen auftritt, sich nach getaner Arbeit selbst löscht, und sie kann auch auf nur einen geringen Prozentsatz der Stimmen beschränkt sein und damit jede Plausibilitätsprüfung bestehen. [WVSCN06]

Eine wirkungsvolle Prüfung wie das Nachzählen von Stimmen ist mit rein elektronischen Geräten nicht möglich. Allenfalls kann das Stimmmodul erneut ausgelesen werden, das meist als elektronischer oder magnetischer nichtflüchtiger Speicher ausgeführt ist, dem der Speicherinhalt mit menschlichen Sinnen ebenfalls nicht zu entnehmen ist und daher mittels weiterer Computer ausgelesen werden muss, wobei sich neue Manipulationsmöglichkeiten auftun.

Ob das ausgelesene Muster tatsächlich dem Wählerwillen entspricht, kann nicht nachgeprüft werden. In dem Moment nämlich, als der Wähler seine Stimme in das elektronischen System eingegeben und bestätigt hat, wurde die Stimme wurde zu einem unsichtbaren Signalfeld.

Anschliessend erfolgten im Gerät unsichtbare Vorgänge, die zu einem unsichtbaren Ergebnis führten, das der Wähler nicht beobachten konnte.

Später wird dann das unsichtbare Ergebnis der unsichtbaren Vorgänge sichtbar gemacht, als Ausdruck auf Papier oder Anzeige auf einem Display. Hier stellt sich noch zusätzlich das Problem, ob beim Sichtbarmachen der Information alles mit rechten Dingen zugeht, was zur Zeit ebenfalls nicht vom Wähler überprüft werden kann.

In der Praxis sind den USA etwa Systeme im Einsatz, bei denen die Stimmmodule nachträglich unbemerkt umgeschrieben werden können. [FELDMAN06] Grundsätzlich ist die Anzahl möglicher Angriffe und möglicher Fehlfunktionen praktisch grenzenlos und unbekannt. Die Existenz einer wirksamen Angriffsmethode kann **niemals** ausgeschlossen werden.

Zwar sind auch Manipulationen bei der Urnenwahl möglich, die fehlende Automatisierung erfordert aber eine hohe Zahl an Mitwissern und hinterlässt leicht verdächtige Spuren wie schlecht vernichtete Originalstimmzettel und monoton ausgefüllte Fälschungen.

Anonymität vor Überprüfbarkeit

Die meisten derzeit verwendeten Wahlgeräte favorisieren Anonymität gegenüber Nachprüfbarkeit. Meist wird direkt im Augenblick der Wahl zufällig ein Speicherort ausgewählt und die Stimme dort gespeichert. Im Augenblick der Speicherung wird die Stimme damit anonymisiert. [PTB04] Dieser Vorgang ist damit prinzipiell weder für den Wähler, noch die Wahlhelfer oder anwesende Beobachter nachprüfbar. Ob und welche Stimme da gespeichert wird, hängt eben von nicht beobachtbaren Vorgängen in der Maschine ab. Damit ist der Wähler gezwungen, Dritten blind zu vertrauen.

Änderbare Stimme

Auf den ersten Blick wenig offensichtlich ist, das bei teilweiser Aufgabe der Anonymität der Stimme Stimmenkauf und Erpressung durch Aussentäter entgegengewirkt werden kann, indem eine elektronische Wahl so gestaltet wird, dass jeder Wähler seine Stimme beliebig oft ändern kann. Dies erfordert aber eine eindeutige Zuordnung von abgegebener Stimme und Wähler auf Seiten der Wahldurchführenden, wodurch zumindest subjektiv das Gefühl entsteht, das der Staat Kenntnis von der individuellen Wahlentscheidung hat oder erlangen kann, selbst wenn Sicherheitsvorkehrungen dagegen bestehen. Ein entsprechendes Verfahren wurde in Estland bei Internetwahlen eingesetzt. [SPIE05]

Elektronische Zeugensysteme

Ein weiterer Ansatz, bei elektronischen Verfahren Nachprüfbarkeit herzustellen, sind sogenannte *Zeugensysteme*, die beispielsweise Fotos vom Bildschirm machen und speichern, oder unabhängige Geräte, die den Datenverarbeitungsvorgang unabhängig mitprotokollieren. Derartige Systeme können zwar auch für mehr Sicherheit sorgen, sind aber ebenfalls manipulierbar und weichen das Wahlgeheimnis auf.

Paper Trails

Ein zunächst vernünftig klingender Versuch, Überprüfbarkeit herzustellen, ist der sogenannte *Voter Verified Paper Trail* (VVPAT), der entweder als fortlaufender Protokollstreifen ausgeführt ist oder Einzelquittungen auf Papier bannt.

Damit wird die Wahlmaschine faktisch zum teuren Stimmzettel-Drucker. In Verbindung mit einer herkömmlichen Urne scheint das ganze auf den ersten Blick genauso sicher und nahezu so anonym wie die reine Urnenwahl zu funktionieren. Wahlcomputer mit Stimmzetteldruckern sind aber wesentlich teuerer in Anschaffung und Betrieb, und vor allem störanfälliger. [NIST06]

Auch die Auszählung ist teurer als bei rein elektronischen Geräten, da man sich allein auf die elektronische Zählung nicht verlassen kann und nicht nur hinreichend viele manuelle Kontrollzählungen veranstalten muss, sondern zusätzliche Massnahmen benötigt, um die Integrität der *Selbstkontrollkette* zu garantieren.

Zudem handelt man sich bei vielen der existierenden Geräte Anonymitätsprobleme ein, wenn sie die Stimmen fortlaufend auf einem Papierband protokollieren. Damit ist etwa das Votum des ersten und letzten Wählers klar zu erkennen.

Noch problematischer ist aber, das auch bei Verwendung von Protokoll- oder Stimmzettel-druckern Automatisierungsvorteile für Wahlfälscher entstehen: Werden die Stimmzettel von Computern ausgefüllt, so lassen sich ohne viele Mitwisser schnell grosse Mengen ausgefüllter Stimmzettel erzeugen, die ausserdem nicht von den “echten”, von realen Wählern mit der Hand ausgefüllten Stimmzetteln zu unterscheiden sind, die mit unterschiedlich verlaufenden Anpressdruck, Geschwindigkeit, Stiftwinkel und vor allem individueller Linienführung beim Ankreuzen markiert sind.

Zudem liegen allein die Wartungs- und Verbrauchskosten der Geräte wesentlich über den Kosten gedruckter Stimmzettel, die unter 2 Cent/Stück zu haben sind. Daher sperren sich viele Kommunen in den U.S.A. gegen diesen Gerätetyp, für den es in Deutschland bisher keine Zulassung gibt. Aus Sicht der Kommunen ist das nur verständlich: Warum in Anschaffung und Betrieb teuerere Geräte kaufen, wenn es doch billigere zugelassene Geräte gibt, die offenbar irgendwer geprüft und für tauglich erklärt hat.

Tempest und andere kompromittierende Emissionen

Bei allen derzeit existierenden Wahlcomputern, die daraufhin untersucht wurden, konnte das Abstrahlen kompromittierender elektromagnetischer Signale gemessen werden. Dadurch kann mit einer geeigneten Empfangsanlage die Wahl von ausserhalb des Wahllokals abgehört werden. [WVSCN06]

Mindestens einem Gerät wurde die Zulassung verweigert, weil aus dem Geräusch des Druckers leicht die Wahlentscheidung herausgehört werden konnte. [O]

Kryptographische Methoden und Protokolle

Ein wichtiger Bestandteil moderner Computersicherheit sind kryptographische Methoden, bei denen mit Hilfe mathematischer Verfahren Daten so transformiert werden, dass bestimmte Verarbeitungsvorgänge nur durch Kenntnis geheimer Schlüssel möglich werden.

Der Vorgang ist dabei unabhängig von der verwendeten Hardware. Die Sicherheit beruht also nicht auf einer bestimmten an in Raum und Zeit vorhandenen physikalischen Anordnung von Energie oder Materie, sondern abstrakten mathematischen Verfahren. Die Sicherheit dieser Methoden wird durch mathematisch-wissenschaftlichen Diskurs von Kryptologen gewährleistet, die sich die Methoden ausdenken, veröffentlichen und zum Angriff durch andere Kryptanalysten freigeben.

Ein kryptographisches System ist dann als sicher zu betrachten, wenn es mindestens zehn Jahre den Angriffen der besten Köpfe auf diesem Planeten standgehalten hat. Der Verschlüsselungsstandard AES oder asymmetrische Verfahren wie RSA gehören in diese Kategorie, aber alle über Signieren und Verschlüsseln hinausgehende kryptographische Verfahren, wie sie für elektronische Wahlen vorgeschlagen wurden, sind so neu, das sie nicht als sicher genug für den realen Einsatz betrachtet werden können, was sich aber in einigen Jahrzehnten ändern könnte.

Wohl nicht ändern werden sich aber zwei andere **prinzipielle Probleme beim Einsatz von Kryptographie bei Wahlen**:

- Der Zusatzaufwand beim Wähler und Wahlveranstalter
- Die Expertenabhängigkeit

Kryptographie verlangt dem Benutzer zusätzlichen Aufwand ab. Die meisten Wähler dürften es eher als Problem empfinden, in der Wahlkabine mit irgendwelchen Codes hantieren zu müssen, wenn doch eigentlich ein Kreuz auf einem Blatt Papier genügt. Etwas anderes ist die elektronische Wahl von zu Hause aus - hier würden kryptographische Methoden von vielen sicher als weniger lästig empfunden als der Gang zum Wahllokal. Online-Wahlen von zu Hause aus haben aber derart viele zusätzliche Probleme hinsichtlich Erpressbarkeit und Stimmenkauf sowie der Sicherheit der Endgeräte, dass ein derartiger Schritt selbst mit Spezialhardware im Besitz jedes einzelnen Wählers zumindest in Deutschland kaum denkbar wäre.

Das schwerwiegendere, nicht zu umgehende oder tolerierbare Problem mit kryptographischen Verfahren ist, das der Kreis von sachverständigen Experten umso kleiner wird, je höher entwickelt die Verfahren sind. Es gibt weltweit nur einige hundert solcher Menschen, die mathematische Beweise für ein Wahl-Kryptosystem führen und prüfen können. Damit ist praktisch auch jeder Politiker von einer direkten Prüfung ausgeschlossen, zusammen mit fast allen Bürgern.

Es dürfte sehr wahrscheinlich sein, das sich unter den Abgeordneten des Bundestages kein entsprechender Experte befindet, auch wenn derzeit etwa zwei Dutzend Mathematiker, Informatiker, Naturwissenschaftler und Ingenieure ein Abgeordnetenmandat haben.

Ausserdem garantiert ein Kryptosystem allein noch keine Sicherheit. Verschiedene robuste Implementierungen, sichere Generierung und Handhabung der Schlüssel sowie sichere Handhabung aller Geräte und Programme sind zusätzliche Voraussetzungen, die in der Praxis meist nur mit hohem Aufwand gewährleistet werden können und dabei ohne sichtbaren Nutzen sind. Diese für die Sicherheit notwendigen Massnahmen sind ein prädestiniertes Opfer bei Sparmassnahmen oder werden erst gar nicht vorgenommen.

Man vergleiche ein solches eher monströs und magisch anmutendes Kryptosystem mit der einfachen Eleganz der Urnenwahl mit Kreuzen auf papiernen Stimmzettel in einem Kasten mit Schlitz und Schloss.

Funktion und Nutzen kryptographischer Wahlverfahren
Kryptographie kann an vielen Stellen im Wahlverfahren zum Einsatz kommen:

- zur Sicherung der Software
- zur Authentifizierung von Wählern, Geräten, Wahlvorständen und Speichermodulen
- zur Anonymisierung der Stimme
- zur Signatur
- zur verschlüsselten Auszählung
- zur sicheren Kommunikation mit Peripheriegeräten
- zur anonymen Überprüfung von Verarbeitungsvorgängen

Grundsätzlich kommen aber zusätzliche “Geheimnisse” in Form von Schlüsseln ins Spiel. Während bei der Urnenwahl das einzige Geheimnis die geheime Stimme ist, wimmelt es bei den kryptographischen Methoden oft von vielen weiteren Geheimnissen, die meist in Form von Zahlenketten oder Wörtern daher kommen und zusätzlich schutzbedürftig sind.

Ein anderes gemeinsames Merkmal aller kryptographischen Verfahren ist das Vorhandensein unterschiedlicher Parteien, die jeweils nur über Teilwissen verfügen. Verfügt eine Partei über vollständiges Wissen, kennt also alle Schlüssel, so kann sie beliebige Manipulati-

onen durchführen. Das beste Kryptosystem ist nutzlos, wenn die Schlüssel dem Angreifer bekannt sind.

Damit sollte klar sein, das ein Kryptosystem ohne zusätzliche physikalische und organisatorische Massnahmen keinen Nutzen für die Sicherheit bringt, sondern umgekehrt die Überprüfung erheblich erschwert und die Nachvollziehbarkeit stark beeinträchtigt.

Physikalische Massnahmen sind etwa der Quittungsdruck auf Papier. Organisatorische Massnahmen betreffen die Verteilung und Geheimhaltung der Schlüssel und die Handhabung der Geräte.

Auch bei Geräten, die bei der Stimmabgabe eine vom Wähler selbst verifizierbare Spur in Form einer Quittung für jede Stimmabgabe produzieren, gilt das Dilemma der elektronischen Wahl, denn die einzige Möglichkeit zu überprüfen, ob eine dematerialisierte Stimme auch Eingang ins Endergebnis gefunden hat, ist eine teilweise Aufgabe der Anonymität.

Diese kann zwar kryptographisch geschützt oder verschleiert werden, aber dieser Schutz muss entweder aufwändig durch eine komplizierte Kette von Massnahmen aufrecht erhalten werden, oder verlangt dem Wähler Zusatzaufwand ab.

Zulassung von Wahlcomputern

In Deutschland ist die *Physikalisch-Technische Bundesanstal*t (PTB) für die Bauartprüfung von Wahlcomputern zuständig. Der Einsatz der Geräte muss darüberhinaus von den entsprechenden Landes- oder Bundesinnenministerien genehmigt werden, in der Regel für jede neue Wahl einzeln. [BWG35] In der *Bundeswahlgeräteverordnung* sind an sich sehr sinnvolle Prüfkriterien für die Zulassung von Wahlgeräten niedergelegt. Eine Prüfung erfolgt aber offenbar nur nach dem Stand der Technik. Bereits am Tag nach der Prüfung kann durch technischen Fortschritt oder neue wissenschaftliche Erkenntnisse das Prüfergebnis in entscheidenden Punkten obsolet sein. Nach 20 Jahren, und so lange sollen nach Herstellerangaben die Geräte eingesetzt werden, ist insbesondere die Sicherheit längst nicht mehr gewährleistet. Das ergibt sich allein aus dem Technologiegefälle zwischen den aktuellen Angriffsmethoden und -werkzeugen einerseits, und den musealen Angriffszielen in Form von Wahlcomputern andererseits.

Würde man nun die technische Entwicklung der Angriffstechnik über die Lebenszeit der Geräte und Verfahren extrapolieren, wie es bei IT-Sicherheitsanwendungen üblich ist, und nur Geräte zulassen, die mit hoher Wahrscheinlichkeit die Prüfkriterien in zehn Jahren noch erfüllen werden, dürfte kein heute existierender Wahlcomputer eine Zulassung erhalten haben, selbst wenn den Prüfern die hier dargelegten prinzipiellen Probleme nicht bewusst waren. Auch führt ein häufig anzutreffender technischer Machbarkeitsglaube dazu, sich prinzipiellen Problemen zu verschliessen.

Da es aber zugelassene Geräte gibt, deren Unsicherheit nachgewiesen ist, ist offensichtlich, das bei den Prüfkriterien in der Vergangenheit die Zukunftssicherheit keinen bedeutenden Einfluss gehabt hat oder der technologische Fortschritt falsch eingeschätzt wurde. Wer Fehler nicht als solche erkennt, wird sie wiederholen.

Leider fehlt im Gegensatz zu Holland oder Kalifornien in Deutschland den Verantwortlichen noch der Mut, die gemachten Fehler anzuerkennen und in Konsequenz die Gerätezulassung zu zurückzuziehen oder nicht mehr neu zu erteilen.

Bei strenger Auslegung der *Bundeswahlgeräteverordnung* hätte kein derzeit existierendes Gerät Aussicht auf Zulassung.

Automatisierter Wahlbetrug

Die Automatisierungsvorteile, die sich durch den Einsatz von Wahlcomputern ergeben, sind vor allem für Wahlbetrüger erheblich. Während bei Urnenwahlen eine grosse Zahl von Helfern eingeweiht sein muss, um in grossem Stil abzuräumen, genügt bei Wahlcomputern im besten Fall eine einzige Person an der richtigen Stelle, um die entsprechenden Befehlscodes in allen Wahlmaschinen zu verstecken.

Das ist zwar nicht ganz so einfach, aber allein in Deutschland dürfte weit über hunderttausend Menschen mit dem erforderlichen Fachwissen geben, und der Aufwand an Zeit und Geld liegt in der Grössenordnung eines Mannmonats für eine professionelle Lösung, wenn diese von Insidern erstellt wird.

Ein mit der Maschine vertrauter Mitarbeiter des Herstellers kann in wenigen Stunden bereits schwer entdeckbare Manipulationen durchführen.

Mit der Investition von einigen hunderttausend Euro ist es auch Dritten sogar möglich, praktisch nicht zu entdeckende Manipulationen vorzunehmen, die die weitgehende Fernkontrolle eigentlich nicht vernetzter Maschinen erlauben und damit am Wahltag eine “minimal invasive” Umverteilung der Stimmen in Echtzeit vorzunehmen oder sogar auf Wahlbetrug zu verzichten, wenn sich ein befriedigendes Ergebnis abzeichnet.

Erst durch die mit Wahlcomputereinsatz einhergehenden Automatisierungsvorteile wird es in einem Land wie Deutschland wirtschaftlich und organisatorisch möglich, erfolgreich in grossem Umfang Wahlfälschungen durchzuführen.

Ökonomische Betrachtung

Wahlcomputer haben grundlegende Wirtschaftlichkeitsprobleme. Normalerweise werden Datenverarbeitungsgeräte ständig genutzt. Die Anschaffungskosten sind dabei meist deutlich geringer als die Kosten für das Personal, das die Geräte oft täglich nutzt. Leider veralten Computer noch immer relativ schnell und werden daher in Unternehmen alle drei bis fünf Jahre ersetzt.

Wahlcomputer hingegen kommen nur an Wahltagen zum Einsatz, und die liegen meist Jahre auseinander. Unterstellt man eine extrem hohe Lebensdauer von 20 Jahren, werden die Geräte während ihrer Lebenszeit kaum öfter als zehn bis zwanzig mal genutzt. Und wollte man Wahlcomputer für Bundestagswahlen nutzen, so bräuchte jeder Wahlkreis seine eigenen Geräte - ein Mitnutzungsszenario ist damit ausgeschlossen.

Nimmt man nun Kosten für sichere Lagerung, Updates, Ersatzgeräte, Sicherheitsüberprüfungen und den Kapitalzins hinzu, ergibt sich ein Mehrfaches des Neugerätepreises, der je nach Gerät zwischen 4.100 [HSG06] und 5.000 Euro liegt, so dass die TCO (Total Cost of Ownership) pro derzeitigen unsicheren Wahlcomputer bei rund 10.000 Euro liegen dürfte.

Nach bisherigen Erfahrungen braucht man für 1000 Wahlberechtigte eine Wahlmaschine. Bei zehn Wahlen/Wahlmaschine käme man auf mindestens 1000 Euro je Wahlmaschine und Einsatz, die nur teilweise bekanntgewordenen tatsächlichen Kosten scheinen in der Praxis aber bei mehreren Tausend Euro pro Einsatz und Maschine zu liegen.

Genauere unabhängige Untersuchungen über die Wirtschaftlichkeit von Wahlmaschinen in Deutschland sind nicht bekannt, die einzigen Untersuchungen dazu sind mit Herstellerbeteiligung entstanden und ebenfalls nicht öffentlich. Einige Details zu den Kosten in Holland finden sich in [DEPAC07], wobei dort nicht alle Kosten, etwa für die sichere Lagerung, mit erfasst wurden.

Und falls die Wahlmaschinen aus irgendwelchen Gründen, wie etwa dem Verlust der Zulassung, nur ein bis zweimal zum Einsatz kommen oder defekt werden, wird das sogar noch viel teurer. Selbst dem Bürgermeister einer reichen Gemeinde, die sich jeden Luxus leisten kann, müsste man daher empfehlen, für Wahlen lieber Stift, Papier und Urnen zu nehmen und die Wahlhelfer, die ohnehin in voller Stärke vor Ort sein müssen, ein bis zwei Stunden länger arbeiten zu lassen, was einmal im Jahr zumutbar sein müsste.

Möchte man partout Geld in moderne Technik investieren, so bieten sich etwa mit leichteren Laptops, schnelleren Servern oder einer besseren Netzwerkinfrastruktur für Stadtverwaltung und Schulen sicher vorteilhaftere Gelegenheiten.

Hybridsysteme und Zählhilfen

Das *Dilemma der elektronischen Wahl* gilt nicht zwangsläufig für Hybridsysteme oder Zählhilfen. Damit sind Systeme wie etwa der “Hamburger Wahlstift” oder Maschinen gemeint, die handmarkierte Stimmzettel optisch abtasten und elektronisch auswerten. Solche Systeme haben sogar das Potential, neben einer Zeitersparnis die Urnenwahl robuster und sicherer zu machen. In der Praxis hat sich aber gezeigt, dass auch hier mit der Automatisierung neue Gefahren Einzug halten, denn sobald die Systeme vernetzt werden oder Datenträger ausgetauscht werden, besteht zumindest bei heutigen Systemen die Gefahr, das die Auszählung unbemerkt manipuliert wird.

Ein Aufdecken von Manipulationen ist dann zwar ebenso möglich, wie ohne den Einsatz der Geräte, aber es bedarf dazu der zusätzlichen Handauszählung von drei bis zehn Prozent der Wahlkreise, um Manipulationen mit ausreichender Wahrscheinlichkeit aufzudecken. Ausserdem dürfen die Wahlkreise, in denen eine Überprüfung stattfindet, vorher nicht bekannt sein, das heisst, das alle Wahlkreise ihre Helfer für eine potentielle Handauszählung vorhalten müssen.

Möchte man aber die *Selbstkontrollkette* für den einzelnen Wähler aufrechterhalten, bedarf es über Stichprobenkontrollen hinaus entweder einer vollständigen Handauszählung oder sichtbarer, eindeutiger Seriennummern auf den Wahlscheinen, die mit dem Wahlergebnis veröffentlicht werden. Dies bietet aber keines der existierenden Systeme.

Eine Besonderheit ergibt sich beim sogenannten *Hamburger Wahlstift* [WELT06], wo nicht die für die Wähler sichtbare Markierung auf dem Wahlschein gelesen wird, sondern eine Kamera aus einem Muster auf dem Wahlschein ihre Position ermittelt. Das Problem ist, dass hierbei für den Wähler nicht erkennbar manipulierte Wahlscheine im Umlauf sein können, deren Koordinatenmuster nicht mit der Beschriftung übereinstimmt. Auch ist nicht gesamte Wahlsystem geprüft und zertifiziert, so dass die geplante Verwendung 2007 abgesagt wurde.[HEISE161107][HEISE101107]

Ein weiteres Problem ist, dass die Daten dazu genutzt werden könnten, schwieriger als Fälschungen zu erkennende gefälschte Stimmzettel herzustellen, die exakt das individuelle Kreuz enthalten, das dann aber von einem Plotter an anderer Stelle platziert wird.

Zudem besteht die Gefahr, das die Daten im Moment der Erhebung von Dritten bereits unbemerkt abgehört werden und damit das Wahlgeheimnis kompromittiert wird.

Und auch wird beim *Hamburger Wahlstift* die *Selbstkontrollkette* gebrochen; die reguläre Auszählung von Stimmzetteln kann nicht beobachtet werden. Damit wird es schwierig, überhaupt Anhaltspunkte für eine Manipulation zu erlangen.

Zählhilfen, die Wahlzettel einscannen, sind in den USA durch beunruhigende Fehlfunktionen aufgefallen und insbesondere auch im Zusammenhang mit Wahlmanipulationen aufgefallen. Hinzu kommt, dass aufgrund der Kosten der Geräte Stimmzettel aus Wahlkreisen zu zentralen Auszählungsorten transportiert wurden und auf dem Weg dorthin zum Teil ausgetauscht wurden. Auch derartige Zählhilfen brechen die *Selbstkontrollkette*, wenn das Wegfallen der Handauszählung auch hier nicht durch Seriennummernveröffentlichung kompensiert wird.

Psychologische Effekte beim Wahlcomputereinsatz

Der Einsatz von Computern führt zu veränderter Wahrnehmung von Wahlen und beeinflusst das Verhalten aller Akteure.

Bei den Wählern

Wähler reagieren aus eigener Beobachtung sehr unterschiedlich auf den Computereinsatz. Die überwiegende Mehrzahl der Wähler vertraut Wahlcomputern blind. Eine Minderheit, insbesondere die Mehrheit der Informatiker, lehnt Computerwahlen ab und zeigt aus eigener Beobachtung und Befragung bisweilen sehr heftige und aggressive Ablehnung, die zum Teil lautstarke Unmutsäußerungen im Wahllokal beinhaltet. [O]

Es zeigt sich aber, dass auch viele “normale Bürger” nach entsprechender Aufklärung von sich aus Vorbehalte gegen die Computerwahl entwickeln. Auf die Frage, ob sie sich den in der Lage sähen, Manipulationen bei einer Computerwahl zu entdecken, antworteten praktisch alle Befragten mit “Nein”, aber sie gingen davon aus, dass die “zuständigen Stellen” das wohl im Griff hätten. [O]

Auch assoziieren viele Wähler die Wahlcomputer bisher nicht mit anderen Computern aus ihrem Umfeld. Auf die Frage, ob sie denn Vertrauen die die Korrektheit der Verarbeitungsergebnisse ihres eigenen Computers oder den Computeranlagen an ihrer Arbeitsstelle hätten, antwortet bei einer nicht repräsentativen Befragung eine knappe Mehrheit der Befragten mit “Nein”. [O]

Als weiterer Effekt zeigt sich, dass einige Wähler bei Wahlcomputern generell ein ungutes Gefühl hinsichtlich des Wahlgeheimnisses verspüren. Bei den NEDAP-Geräten verfügt etwa die Steuereinheit, die beim Wahlleiter steht und durch ein Kabel mit dem Wahlcomputer verbunden ist, über ein eigenes Display. Dies provoziert gelegentlich Fragen von Wählern wie: “Können Sie da etwa sehen, was ich wähle?”. Da bei den wenigen vom CCC durchgeführten Wahlbeobachtungen diese Frage häufiger zu hören war, gibt es vermutlich eine deutlich größere Zahl an Wählern, die sich nicht äußern und bei der nächsten Computerwahl vielleicht lieber wegbleiben. [CCC06]

Das Wähler wegbleiben könnte auch an einer längeren Wartedauer bei Stosszeiten im Wahllokal liegen, da aus Kostengründen in einem Wahllokal meist nur ein Wahlcomputer im Einsatz ist, während bei der Urnenwahl mehrere Wahlkabinen gleichzeitig benutzt werden können.

Was auch die Gründe sein mögen, hinsichtlich der Wahlbeteiligung kann man davon ausgehen, dass Wahlcomputer eine negative Auswirkung auf die Wahlbeteiligung haben. Dies konnte durch statistische Auswertung der Entwicklung der Wahlbeteiligung in Brandenburg und Hessen recht deutlich gezeigt werden, wo bei der jeweils zweiten Computerwahl bei Bezirken mit Wahlcomputern ein stärkerer Rückgang der Wahlbeteiligung festgestellt wurde, als in Bezirken ohne Wahlcomputer. [WIES08][FEHN08]

Dass sich dieser Rückgang erst bei der zweiten Computerwahl bemerkbar machte deutet darauf hin, dass Wähler, die bei der ersten Computerwahl Probleme oder Unbehagen verspürten, bei der nächsten Computerwahl tatsächlich ferngeblieben sind. Die Auswertung wurde von Wahlcomputergegnern durchgeführt, und die Relevanz wird von Wahlbehörden bestritten, obwohl diese hierzu keine eigenen Untersuchungen angestellt haben. Dies ist eine unverständliche Nachlässigkeit, da dies mit geringem Aufwand möglich wäre. Da sämtliche Zahlen öffentlich verfügbar sind, kann jeder Interessierte aber eigene Untersuchungen anstellen.

Bei den Wahlhelfern, Wahlleitern und öffentlichen Amtspersonen
Wahlhelfer sind in der Regel überwiegend begeistert von Wahlcomputern, da sie früher nach Hause können. Es besteht aber ein gewisses Unbehagen und eine Unsicherheit beim Umgang mit den Geräten, die sich insbesondere bei der Beobachtung durch Dritte bemerkbar machte. [O]

Viele Wahlhelfer sind mit der korrekten Handhabung der Geräte überfordert, und auch die Prüfung und Verwahrung der Geräte wird in der Praxis in vielen Fällen nicht vorschriftsmässig durchgeführt, obwohl die verwendeten NEDAP-Geräte noch einfach zu handhaben sind im Vergleich zu Geräten, die das Hantieren mit kryptografischen Schlüsseln erfordern würden.

Bei Wahlleitern und Amtspersonen, die den Einsatz von Wahlcomputern mit zu verantworten haben, ist in der Regel eine Abwehr- und Verteidigungshaltung gegenüber Beobachtern und Kritikern festzustellen. Die Wahlcomputer werden nach aussen hin als sicher betrachtet, es bestehen zugleich aber Zweifel, ob Manipulationen nicht doch möglich sind, was sich in vielen Fällen durch unangemessene Geheimhaltung und Zugangsverweigerung für unabhängige Wahlbeobachter geäussert hat.

Insbesondere Vertretern des CCC werden gelegentlich “magische Kräfte” zugesprochen, als wenn diese allein durch ihre Anwesenheit den Wahlcomputer manipulieren könnten.

Ein Innentäterszenario oder eine Verschwörung von Mitarbeitern des Herstellers wird dagegen als vollkommen unwahrscheinlich betrachtet, da eine solche Ungeheuerlichkeit speziell in Deutschland ausserhalb dessen liegt, was als Möglichkeit vorstellbar ist. (“Es kann nicht sein, was nicht sein darf.”) Eine derartige Arglosigkeit verringert natürlich das Entdeckungsrisiko für Innentäter erheblich, da die Bereitschaft gering ist, gegen eine vermeintlich nichtexistente Bedrohung Massnahmen zu treffen, und selbst im Verdachtsfall die Schwelle hoch ist, überhaupt Ermittlungen aufzunehmen.

Des weiteren führt ein Computereinsatz zu einer Art Verantwortungsübertragung auf den Computer. Für etwaige Fehler fühlt sich der Einzelne nicht verantwortlich, es ist dann eben die “Technik”, die Schuld ist. Das ist aus anderen Bereichen von Verwaltungen nur allzu bekannt: “Ich würde ja gerne, aber der Computer nimmt das nicht an.”, oder “Im Computer steht aber...”.

Massnahmen zur Verbesserung von Wahlcomputern

Im folgenden wird der Versuch unternommen, einen nach dem Stand der Technik möglichst guten Wahlcomputer zu entwerfen, der die Anforderungen demokratischer Wahlen möglichst erfüllt.

Weitere, aber untergeordnete Kriterien bei dem Versuch sind, dass ein derartiger Wahlcomputer klaren Zusatznutzen gegenüber der gängigen Urnenwahl bietet und wirtschaftlich ist. Untergeordnet bedeutet in diesem Zusammenhang, das wirtschaftliche Vorteile oder Bequemlichkeit nicht gegen die Anforderungen *Gleich, Geheim und Frei* aufgewogen werden können.

Der Ausgangspunkt für die Betrachtung ist, dass ein rein auf einfacher elektronischer Verarbeitung beruhender Wahlcomputer, so wie es die derzeit in Deutschland zugelassenen Geräte sind, die Anforderungen ohne zusätzliche Massnahmen nicht erfüllen kann.

Beim dem Entwurfsversuch werden daher möglichst viele Techniken in Kombination genutzt, um die prinzipielle *Unsichtbarkeit* der Stimmabgabe und Verarbeitung zu kompensieren. Es ist aber zu beachten, dass jede der Techniken nicht nur Vorteile bietet, sondern zusätzliche Nachteile mit sich bringen kann, die wiederum durch weitere Techniken kompensiert werden müssen.

Das amerikanische Pendant zur deutschen *Physikalisch-Technischen Bundesanstalt* (PTB), das *National Institute of Standards and Technology* (NIST), plädiert für *Software Independence* und und empfiehlt hierzu *Voter Verified Paper Trails* [NIST06], um Wahlcomputer sicher zu machen, greift aber dabei noch zu kurz, wie wir sehen werden.

Der Ansatz von *Software Independence* allein berücksichtigt nicht, dass der Benchmark Urnenwahlen sind, und jede Form von Automatisierung weitreichende Folgen haben kann, die nicht vorhersehbar sind. Entscheidend ist die Vertrauenswürdigkeit eines Verfahrens, und selbst wenn das Verfahren perfekt ist, der Wähler dies aber nicht selbst überprüfen kann, ist der Demokratie nicht geholfen.

Was kann denn nun konstruktiv getan werden, um demokratieverträgliche automatisierte Wahlen durchzuführen?

Auf der nächsten Seite findet sich eine Liste von Techniken, die Wahlcomputer sicherer machen können, samt ihrer Vor- und Nachteile. Eine mehr gerätebezogener Vergleich findet sich in [DEPAC07].

Technik	Vorteile	Nachteile
Sichtbarer Protokolldruck (Papierstreifen im Gerät mit sichtbarem Verlaufsprotokoll des Wahlvorgangs, VVPAT)	Bessere Nachprüfbarkeit bei Fehlern	Leichtere Fälschbarkeit der Belege, Schlechtere Anonymität, Teuer
Quittungsdruck (individuelle Quittung zum Mitnehmen)	Bessere Nachprüfbarkeit bei Fehlern, Manipulation nachweisbar	Erfordert spezielles Verfahren gegen Stimmenkauf und Stimmenerpressung, Teuer
Stimmzetteldruck (Ausdruck eines Stimmzettels, der in Urne eingeworfen wird)	Weniger Fehler	Leichtere Fälschbarkeit der Stimmzettel, Schlechtere Anonymität, Teuer
Zufällige Seriennummern auf Stimmzetteln	Bei deren Veröffentlichung Verzicht auf Handauszählung möglich	Teuerer, Zusatzaufwand für Infrastruktur, Gefahren für Wahlgeheimnis
Zeugensysteme	Bessere Nachprüfbarkeit bei Fehlern, Manipulation erschwert	Teuerer, Zusatzaufwand für Infrastruktur, Gefahren für Wahlgeheimnis
Kryptographie zum Schutz der **Hard- und Software** (“Trusted Platform”)	Manipulation schwieriger durchzuführen, Einfache Manipulation entdeckbar, besserer Schutz gegen Fehlfunktion	Teuerer, Gute Manipulation schwieriger zu entdecken, Aufwand und Gefahren bei der Schlüsselverwaltung
Kryptographie zum Schutz der **Stimme** (Signaturen oder Schlüssel auf Stimmzetteln)	Manipulation schwierig	Umständliche Handhabung, Fehleranfällig, nur von wenigen Experten überprüfbar, Anonymität kann bei Bruch der Verschlüsselung oder Bekanntwerden von Schlüsseln gefährdet sein
Kryptographie zum Schutz der **Auszählung** (z.B. spezielles Kryptosystem, das jedem Wähler ermöglicht, selbst zu prüfen, ob seine Stimme korrekt Eingang ins Endergebnis gefunden hat)	Verhindert potentiell Manipulationen bei der Auszählung oder Bekanntgabe	Ermöglicht Stimmenkauf oder Erpressung oder verlangt umständliche Handhabung, Fehleranfällig, nur von wenigen Experten überprüfbar, Anonymität kann bei Bruch der Verschlüsselung oder Bekanntwerden von Schlüsseln gefährdet sein
Stimmänderung (Mehrfache Stimmabgabe möglich, letzte Stimme zählt)	Erschwert Stimmenkauf und -erpressung	Anonymität ist subjektiv aufgehoben, objektiv gefährdet

Technik	Vorteile	Nachteile
Public Source Code	Verringert Abneigung gegen Wahlcomputer bei bestimmten Gruppen	Senkt geringfügig Angriffskosten für Aussentäter, schafft falsches Vertrauen

Tabelle 1

Demokratieverträglicher Ansatz #1: Wahlcomputer als Stimmzetteldrucker
Der “sichere” Wahlcomputer ist kein alleinstehendes System, sondern eingebettet in eine Vielzahl organisatorischer Massnahmen, benachbarter Systeme und individueller Sicherheitstechnik.

Zunächst einmal erscheint für die Software dieses Wahlcomputers ein “Public Source”-Ansatz hilfreich, bei dem der Quellcode öffentlich verfügbar ist. Auch die gesamte Gerätespezifikation sowie Testgeräte sollten für jedermann verfügbar sein. Dies allein schafft aber vor allem Vertrauen in die Qualität und Betriebssicherheit der Geräte, bringt aber hinsichtlich der Sicherheit keinen wesentlichen Fortschritt, denn für den Wähler im Wahllokal gibt es keine Möglichkeit festzustellen, ob der Wahlcomputer auch mit genau dieser Software arbeitet.

Selbst hypothetische Prüfgeräte, die die Software auslesen, lassen sich einfach täuschen, etwa durch das Vorhalten des Originalprogramms für Prüfungszwecke. Der Einsatz kryptografischer Methoden zum Schutz des Systems (Trusted Platform) bringt hier sogar noch Nachteile für die Überprüfbarkeit.

Daher ist unser idealer Wahlcomputer mit möglichst einfacher Technologie realisiert.

Aufgrund des *Dilemmas der elektronischen Wahl* nehmen zusätzlich wir eine physikalische, mit menschlichen Sinnen wahrnehmbare und vom Wähler überprüfbare Protokollierung der Wahl. Dies lässt sich etwa mit einem *Voter Verified Paper Trail* in Form eines Protokolldruckers mit Sichtfenster für den Wähler bewerkstelligen.

Das Problem mit einem *Paper Trail* auf einem fortlaufenden Papierstreifen ist, das die Anonymität nicht gewahrt wird, die Wahlentscheidung etwa des ersten und letzten Wählers ist klar zu erkennen.

Unser *Paper Trail* müsste also ein Papierband an zufälliger Stelle beschreiben und die bedruckte Stelle dem Wähler in einem Fenster anzeigen, so dass er sich von der Korrektheit des Ausdrucks überzeugen kann. Ein solcher Drucker wäre zwar teuer und fehleranfälliger als die üblichen Bondrucker, ist aber technisch machbar.

Der Streifen müsste zudem noch vor und nach der Wahl von den Wahlhelfern unterschrieben werden und in Gänze inspiziert werden: Vorher, um sicher zu gehen, dass er auch leer ist, danach, um festzustellen, ob er vollständig und lesbar bedruckt ist.

Ausserdem muss der Ausdruck derart gestaltet sein, das eine Verfälschung durch Hinzufügen von Information ausgeschlossen ist. Leerstellen auf dem Band müssen daher vor der Entnahme “entwertet” werden. Die Entwertung von Leerstellen darf natürlich nicht durch vollständiges Schwärzen erfolgen, und der Drucker muss von sich aus ein deutlich hörbares Arbeitsgeräusch abgeben, aus dem es aber nicht möglich sein darf, auf das Wählervotum zu schliessen, was etwa bei unterschiedlichen langen Partei- oder Kandidatennamen leicht möglich ist.

Auf das *Public Source*-Kriterium kann aber nicht verzichtet werden kann, auch wenn das *Paper Trail* - Verfahren genutzt wird, da öffentlich überprüfbar sein sollte, dass die Auswahl der Speicherstellen auf dem Band tatsächlich mit ausreichender Zufälligkeit erfolgt. Leider sind auch hier Manipulationen, die die Anonymität aushebeln, nicht auszuschliessen, wir können aber davon ausgehen, dass der Nutzen einer derartigen Manipulation nur einmalig wäre und sich der Aufwand für den Angreifer vermutlich nicht lohnen würde.

Das Gehäuse sollte darüber hinaus teilweise transparent ausgeführt sein, so dass sich der Wähler und die Wahlhelfer davon überzeugen können, dass im Gerät kein zweiter Drucker installiert ist.

Dieses System erscheint auf den ersten Blick bereits sicher genug. Dummerweise haben wir mit dem an beliebigen Stellen frei beschreibbaren Band eine neue Angriffsmöglichkeit geschaffen: Die Software kann so manipuliert sein, dass dem Wähler einfach eine Stelle auf dem Band angezeigt wird, die eigentlich zu einem anderen Wähler gehört und der gewünschten Wahl entspricht, tatsächlich aber etwas anderes auf das Band geschrieben wird.

Das könnte entweder dadurch ausgeschlossen werden, dass der Druckvorgang beobachtbar ist und insbesondere beobachtet werden kann, dass ein leerer Papierstreifen entsprechend dem Wählervotum beschriftet wird.

Alternativ können wir zu einem anderen Mittel greifen: Neben oder besser anstatt des *Paper Trails* kann ein Stimmzettel ausgedruckt werden, der dann in eine gewöhnliche Urne eingeworfen wird. Leider müssen wir an dieser Stelle ein weiteren Sicherheitsnachteil in Kauf nehmen: Da die Stimmzettel automatisch ausgefüllt werden, kann ein Betrüger auch leichter ausgefüllte Stimmzettel fälschen. Daher benötigen wir noch spezielles, nummeriertes und fälschungssicheres Spezialpapier, dessen Weg vom Hersteller ins Wahllokal dokumentiert werden muss.

Das allein reicht immer noch nicht aus - es muss sichergestellt werden, dass das Gerät bei seiner Arbeit keine kompromittierenden elektromagnetischen Abstrahlungen erzeugt. Diese *TEMPEST*-Sicherheit ist leider nicht billig zu haben, sie kann den Gerätepreis leicht vervielfachen, und die Standards und Geräte unterliegen weitgehend der militärischen Geheimhaltung, so dass die holländische Untersuchungskommission eine technische Lösung als aussichtslos erachtet hat als einziges Mittel vorgeschlagen, das Abhören von Wahlcomputern besonders unter Strafe zu stellen. Das ist praktisch eine Kapitulationserklärung. [DEPAC07]

Ausserdem wissen wir noch immer nicht, ob die vom Gerät gemeldeten Summen auch tatsächlich mit den abgegebenen Stimmen identisch sind - hierzu müssen in 3-10% der Wahllokale entweder die Papierstreifen von Hand überprüft werden, was deutlich unangenehmer ist, als sortierte Haufen von Stimmzetteln nachzuzählen, oder es werden dafür zusätzliche, unabhängig hergestellte Zählgeräte verwendet, die den Papierstreifen einlesen und noch mal unabhängig Summen bilden.

Leider reicht das alles noch nicht aus. **Der Wähler kann** nämlich im Gegensatz zur Urnenwahl mit Papier und Bleistift **nicht überprüfen, ob seine Stimme gezählt wurde**. Bei der Urnenwahl kann er auf dem Stimmzettel dagegen ein besonders auffälliges Kreuz oder einen auffälligen Knick ins Papier machen. Bei der **Handauszählung** kann er dann sehen, **ob sein Zettel richtig mitgezählt** wurde. Müssen wir dem dem Wähler bei der Computerwahl auch noch einen Stift in die Hand drücken, damit auf dem Bon noch rummalen kann? Das ist auch aber auch nicht zulässig, da es Stimmenkauf erleichtern würde. Ein denkbarer Ausweg ist eine kurze zufällige und gut sichtbare *Seriennummer* auf dem Stimmzettel, die man sich merken oder aufschreiben kann. Und anschliessend brauchen wir dann entweder eine vollständige Handauszählung, oder es müssen alle Seriennummern einschliesslich der Partei, auf die sie entfallen sind, mit dem Wahlergebnis veröffentlicht werden. Allerdings leidet insbesondere bei der Veröffentlichung der Seriennummern die Anonymität, da es Stimmenkauf ermöglicht.[2]

Der bis zu dieser Stelle skizzierte Wahlcomputer erfüllt die Anforderungen an eine demokratische Wahl mehr schlecht als recht, und das auch nur, wenn eine entsprechende Handhabung gewährleistet sowie sämtliche skizzierten Sicherheitstechniken ohne Abstriche vorhanden sind.

Der Verzicht auf nur ein einziges dieser Merkmale, etwa
- der Einsatz von Standardpapier
- die Verwendung eines gewöhnlichen seriellen Bondruckers
- der Verzicht auf Seriennummern in Verbindung mit Handauszählung
- der Verzicht auf Tempest-Sicherheit

bewirken, dass ein derartiges Gerät weit hinter dem Standard von handausgezählten Urnenwahlen mit Stift und Zettel zurückbleibt und damit einen grossen Rückschritt in Bezug auf seine Eignung für demokratische Wahlen darstellt.

Das *Dilemma der elektronischen Wahl* hingegen bleibt weiterhin gültig, da wir bei genauerem Hinsehen nichts anderes gemacht haben, als mit hohem technischen Aufwand eine Urnenwahl mit Papier, Bleistift und Handauszählung zu reproduzieren.

Um die Anforderungen zu erreichen, benötigen wir ein Gerät, das ein Vielfaches von dem kostet, was heute existierende Wahlcomputern kosten - dagegen müssten diese etwa um den Faktor zwei bis vier billiger werden, um mit den Kosten einer Urnenwahl konkurrieren zu können. Dieser Wahlcomputer hätte praktisch keine Chancen, sich jemals in grossem Maßstab gegenüber der Urnenwahl durchzusetzen, und hätte erst Recht keine Chance gegenüber heutigen preiswerteren Geräten, die zwar zugelassen sind, aber die Anforderungen an demokratische Wahlen nicht erfüllen.

Daher wird dieses Gerät in der Praxis wohl niemals geben.

---

[2] Der Wähler kann sich die Seriennummer aufschreiben und vor der Veröffentlichung an den Stimmkäufer weitergeben.

Demokratieverträglicher Ansatz #2: Ein zahlenbasiertes Wahlsystem
Wenn *Paper Trails* so teuer sind, lässt sich dann mit kryptografischen Methoden ein demokratiegerechter Wahlcomputer bauen?

Kryptographie beeinhaltet in der Regel zwei Arten von Geheimnissen: Zum einen eine zu schützende Information, die verschlüsselt gespeichert wird, zum anderen einen Schlüssel, der es ermöglicht, die verschlüsselte Information in entschlüsselten Klartext zurückzuwandeln.

Dabei sind viele unterschiedliche Spielarten und Kombinationsmöglichkeiten bekannt: [SCHNEIER96]

Schlüssel können auf verschiedene Personen verteilt werden, so dass eine Entschlüsselung nur bei Zusammenlegen einer Mindestzahl von Schlüsseln möglich ist.

Asymmetrische Verschlüsselung ermöglicht es, verschiedene Schlüssel für das Ver- und Entschlüssen zu haben, die praktisch nicht auseinander abgeleitet werden können.

Des weiteren ermöglichen es digitale Signaturen, Informationen verfälschungssicher zu speichern oder zu übermitteln.

Und möchte man es so richtig wissen, kann man auch noch Eigenschaften einer Menge als Zahlen kodierter Informationen beweisen, ohne zu wissen, welche Information sich hinter welcher Zahl verbirgt, so genanntes *Zero Knowledge Proofing*.

Des weiteren gibt es eine Vielzahl kryptographischer Protokolle, die durch den Austausch von Geheimnissen *Garantien* erzeugen, anhand derer man Sachverhalte beweisen kann, etwa dass eine Kommunikation stattgefunden hat oder eine bestimmte Wahl getroffen wurde.

Ausgangspunkt für kryptografische Massnahmen ist zunächst die Frage, was vor wem gegen was gesichert werden soll.

Das wäre zum einen die Stimme, die gegen Verfälschung gesichert werden soll. Der Wähler könnte also seine Stimme mit einer digitalen Signatur versehen. Das allein wäre aber das Äquivalent zur Unterschrift auf dem Stimmzettel, was aus gutem Grund nicht vorgesehen ist. Zusätzlich müsste also die Signatur als solche noch mal gegen Einsicht geschützt werden. Leider reicht das immer noch nicht, da der Wähler ja nicht nachweisen können darf, wen er gewählt hat, um Stimmenkauf oder Erpressung zu verhindern.

Doch auch dafür bietet Kryptographie eine Lösung: statt eines Schlüssels bekomme ich mehrere Schlüssel an die Hand, die jeweils eine andere, nicht von mir vorgenommene Wahl offenbaren, und ein Erpresser oder Stimmenkäufer kann nicht wissen, ob ich ihm den richtigen Schlüssel gezeigt habe. Die Dummy-Schlüssel können dabei auch einfach die Schlüssel eines anderen Wählers sein, der etwas anderes gewählt, was den Vorteil hätte, dass das Verfahren mit nur wenigen Dummy-Schlüsseln auskommt.

Nach der Wahl werden nun alle abgegeben Stimmen im Internet oder als Buch vollständig veröffentlicht. Der Einfachheit halber kann man sich vorstellen, dass je Partei eine sortierte Liste aller Schlüssel vorliegt, die diese Partei gewählt haben. Als Wähler brauche ich dann nur zu schauen, ob sich mein Schlüssel in der richtigen Liste befindet. Für einen Erpresser oder Stimmenkäufer habe ich ja meine Alternativschlüssel.

Im Prinzip könnte man an dieser Stelle die Signatur und ihre Verschlüsselung auch ganz weglassen und allein mit den Schlüsseln arbeiten, die dann nichts anderes wären als zufällig gewählte Zahlen.

Es fehlt aber noch ein entscheidender Schritt: Ich muss sicher sein, dass mir das System für meine tatsächliche Wahl auch einen echten Schlüssel anbietet und nicht etwa einen Schlüssel von jemandem, der dieselbe Partei gewählt hat und stattdessen meine Stimme jemand anderem gibt. Diesen Angriff bezeichne ich als *Vote Sharing Attack.*

Um diesen Angriff abzuwehren, muss ich in der Lage sein, den Schlüssel teilweise frei zu wählen. Einem Schlüssel, den mir das Gerät allein vorschlägt, kann ich nicht vertrauen.

Ich darf den Schlüssel aber nicht völlig frei wählen können, da ich ansonsten wieder erpressbar oder käuflich werde.

Das Problem ist zwar lösbar, erfordert aber entweder ein kompliziertes Hantieren am Wahlcomputer oder einen eigenen, persönlichen Schlüsselgenerator mit Display, dem ich voll vertrauen kann und der einen Teil des Schlüssels zuliefert. Das eigene Display ist notwendig, da mich ansonsten der Wahlcomputer belügen und einfach andere Zahlen einsetzen könnte.

In jedem Fall wird die Interaktion am Wahlcomputer komplexer und dauert länger, was wohl in der Praxis inakzeptabel sein dürfte, da bereits bei heutigen Wahlcomputern eine geringe Zahl von Wählern offenbar der Wahl fernbleibt, da sie nicht am Computer wählen wollen.

Auch würde wohl nur eine Minderheit von Wählern von der Möglichkeit Gebrauch machen, ihre Stimme zu überprüfen, aber das wäre genug, um Fehler oder Betrug mit hoher Wahrscheinlichkeit aufzudecken. Eine einzige nachgewiesen fehlende Stimme würde ausreichen, um die Wahl anzufechten.

Der Wähler bekäme bei der Wahl einen individuell gedruckten Wahlschein als Quittung mit nach Hause, auf dem für jede mögliche Wahl ein entsprechender Schlüssel vermerkt ist. Jeder dieser Schlüssel würde dann bei der Überprüfung das korrekte Ergebnis liefern, so dass ein Nachweis, was der Inhaber der Quittung gewählt hat, nicht möglich ist. Der Wähler könnte aber sicher sein, dass seine Stimme gezählt wurde, wenn der von ihm frei mitbestimmte Schlüssel bei der richtigen Partei mitgezählt wurde.

Intermingled Key Voting

Im folgenden ist ein entsprechendes Verfahren skizziert, das ich *Intermingled Key Voting* genannt habe. Eigentlich ist das Verfahren so einfach, das man es kaum als *Kryptographie* bezeichnen kann, mit Ausnahme der Erzeugung der Zufallszahlen, wobei es aber nicht einmal besonders auf die Qualität des Zufalls ankommt. Es sollte sich nur um Zahlen handeln, die kein allzu offensichtliches Muster aufweisen und nicht vollständig vorhersagbar sind. Ein physikalisch *geseedeter* PRNG mit langer Periode sollte mehr als ausreichen.

Dass die Sicherheit nicht von der Qualität des Zufalls abhängt, kann man sich dadurch vergegenwärtigen, dass selbst wenn der Zufallsgenerator eine aufsteigende Zahlenfolge liefern würde oder sich vollständig unter Kontrolle des Angreifers befände, Betrug nachweisbar oder das Wahlergebnis mit hoher Wahrscheinlichkeit überprüfbar korrekt wäre. Allenfalls die Anonymität wäre gefährdet, aber in geringerem Maße als bei einem linearen *Paper Trail*. Das Verfahren an sich ist also vergleichsweise sehr robust, wenn auch nicht absolut perfekt.

Im folgenden wird das Verfahren in einzelnen Schritten gezeigt. Eine Stimme besteht dabei aus einer eindeutigen[3] Zahl, die einer Partei zugeschlagen wird. Im vorliegenden Beispiel werden neunstellige Zahlen verwendet. Sollten in einem Wahlkreis mehrere Wahlcomputer zum Einsatz kommen, kann man einfach eine weitere vorgegebene Ziffer einführen, die dann den Wahlcomputer bezeichnet und dann immer vorangestellt oder angehängt wird und unveränderlich ist.

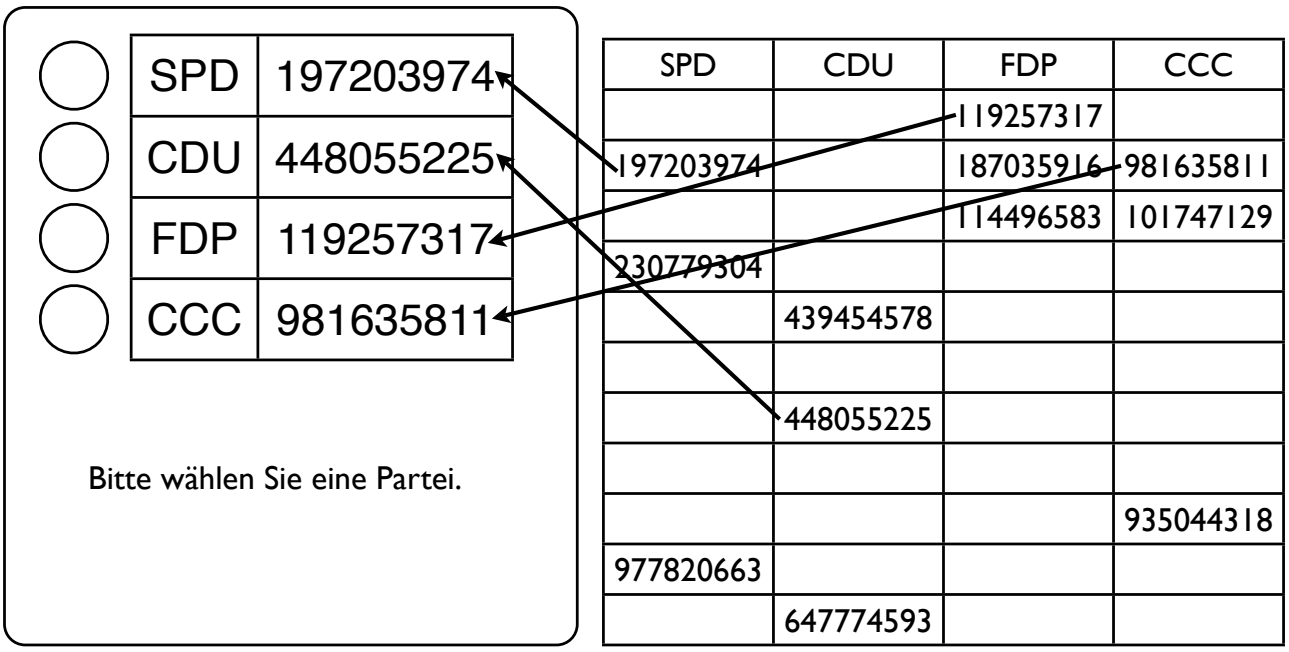

Bild 4

*Schritt1: Bei Wahlbeginn werden **für jede Partei die gleiche Zahl Füllstimmen** generiert, hier beispielsweise **drei Füllstimmen je Partei**, die sogar in der Praxis ausreichen sollten. Die bekannte Anzahl Füllstimmen wird bei der Auszählung wieder abgezogen. Die Füllstimmen dienen ausschliesslich dem Zweck, dass die **ersten Wähler vollständige Quittungen** erhalten können. Theoretisch würde sogar eine Füllstimme je Partei ausreichen. **Stimmen**, auch die Füllstimmen, werden **an zufälliger Stelle im Stimmspeicher abgelegt**. Kommt nun ein Wähler, so **wählt der Rechner zufällig aus dem Stimmspeicher** für **jede Partei** eine Schlüsselzahl aus der **zu der Partei gehörenden Liste** und zeigt sie **auf dem Bildschirm** an.*

[3] eindeutig innerhalb des Wahlcomputers oder Stimmbezirks

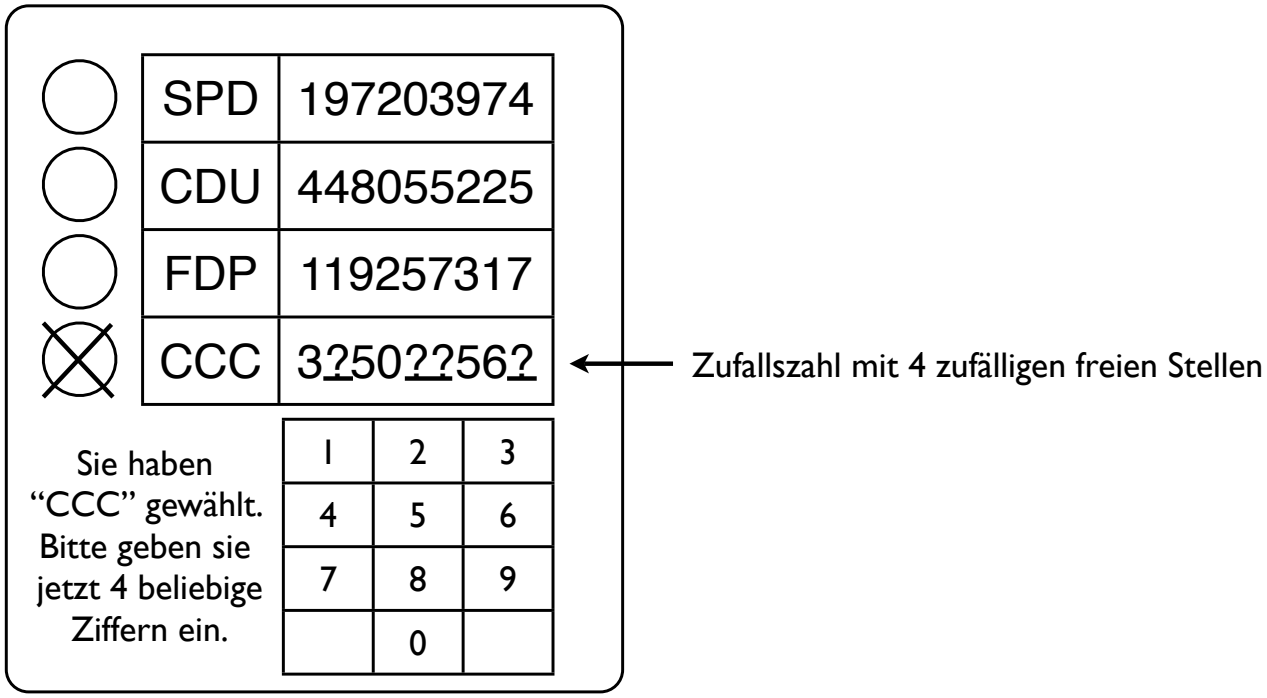

Bild 5

*Schritt 2: Der Wähler wählt die gewünschte Partei. Danach erscheint **hinter der gewählten Partei eine neue, zufällig gewählte Zahl**, die **an vier zufällig gewählten Stellen leer** ist. Der Computer stellt dabei sicher, dass es zu keiner Kollision mit vorhandenen Stimmen kommen kann. (Ein manipulierter Computer würde genau das Gegenteil tun, aber ohne grosse Aussicht Erfolg, s.u.)*

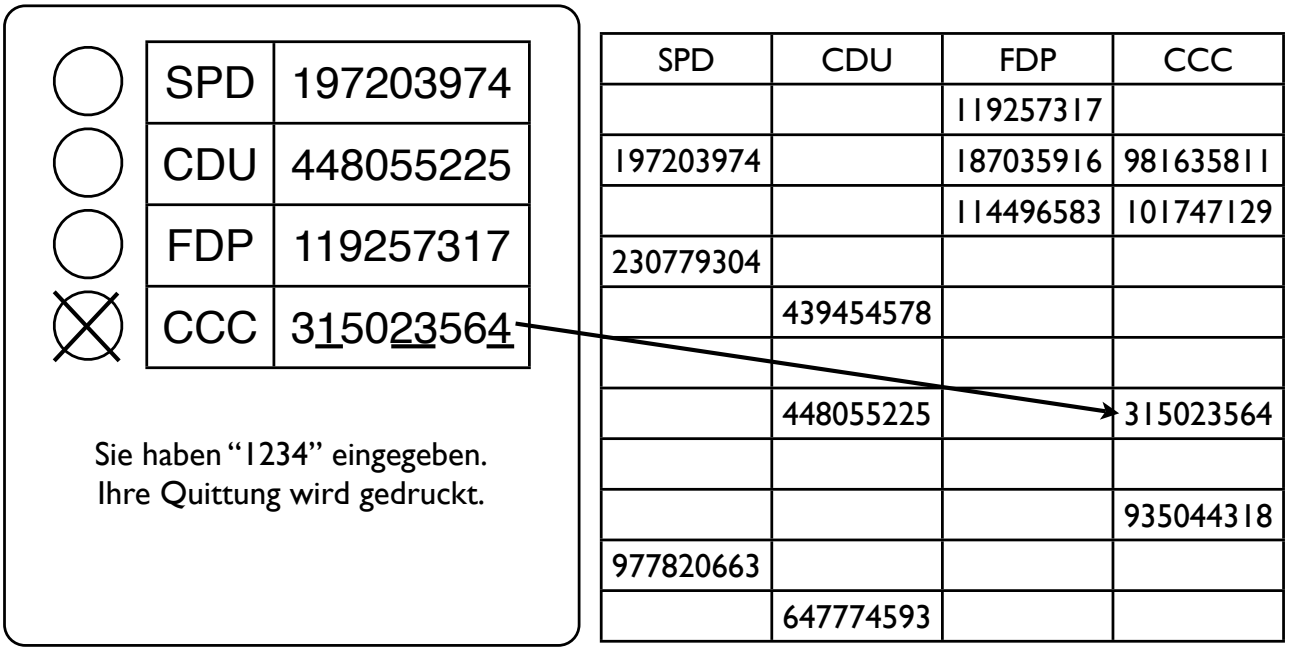

Bild 6

*Schritt 3: Der Wähler gibt **vier beliebige Ziffern** ein, mit denen die **Leerstellen aufgefüllt** werden. Die neu entstandene Zahl wird an einem zufälligen Platz **bei der gewählten Partei** eingetragen. **Diese Zahl steht anschliessend als weitere Füllstimme für andere Wähler zur Verfügung.***

SPD	197203974
CDU	448055225
FDP	119257317
CCC	315023564

Die ist ihre Wahlquittung, die
Sie nach Hause mitnehmen
und aufbewahren können.

Sie können auf der Internetseite
"https://wahlergebnis.de/"
ab morgen überprüfen, daß Ihre Stimme
korrekt gezählt wurde.

.

Anleitung zum Überprüfen: Geben Sie in ihrem Browser die
Adresse "https://wahlergebnis.de/wahlkreis=120" ein.

Sie finden dort für für jede Partei eine Liste mit Zahlen.
Wenn die zu Ihrer Partei gehörende Zahl in der entsprechenden
Liste enthalten ist, wurde ihre Stimme korrekt gezählt.
Wenn die Zahl in der Liste fehlt, kontaktieren sie bitte den
Wahlleiter.

Bild 7

*Schritt 4: Es wird eine Quittung gedruckt, die **je einen gültigen Stimmcode** für **jede Partei** enthält. Alle Stimmcodes sind gültig, da es sich entweder um Füllstimmen, echte Stimmen von vorherigen Wählern oder um die eigene gültige Stimme handelt.*

Welche Partei gewählt wurde, ist daher aus der Quittung nicht zu entnehmen.

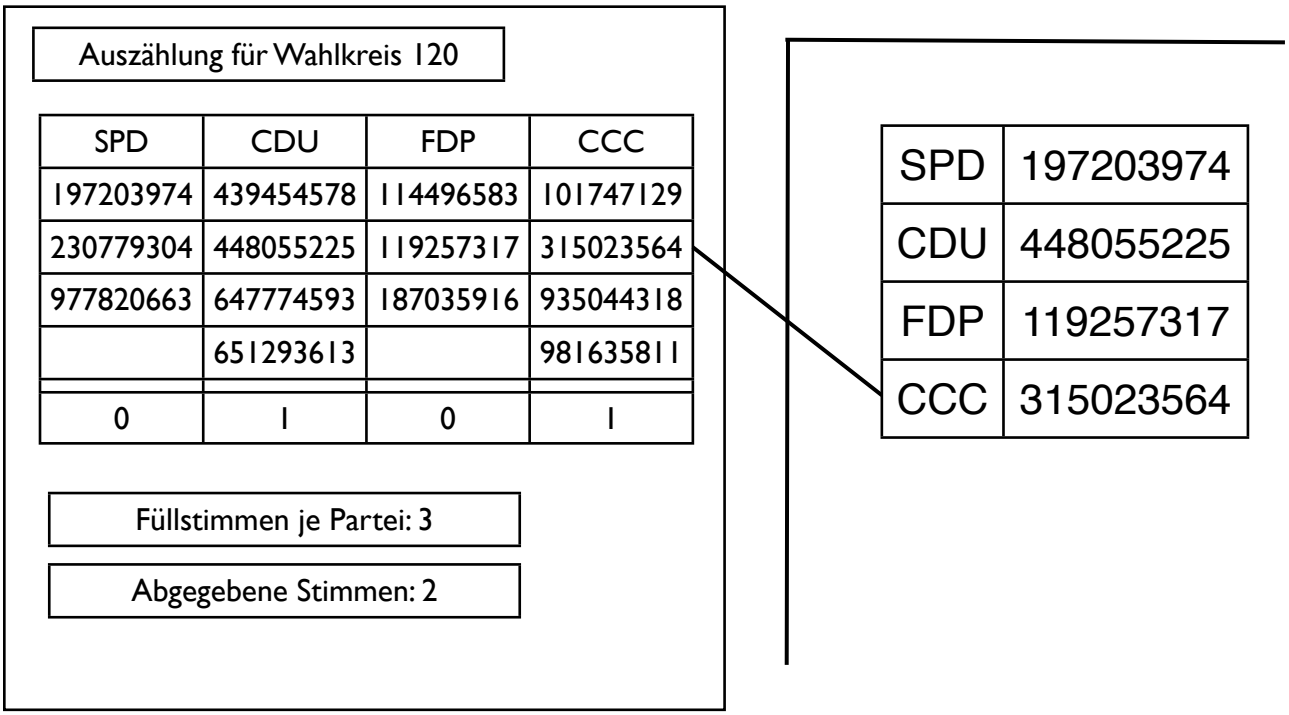

Bild 8

Schritt 5: Für die Auszählung werden nun die Stimmspeicher ausgelesen und die Zahl der Stimmen für jede Partei gezählt, abzüglich der vorher bekannten Zahl an Füllstimmen. Die Gesamtzahl der abgegeben Stimmen muss mit dem handschriftlich geführten Wählerverzeichnis übereinstimmen.

Am nächsten Tag werden im Internet die Stimmcodes für jeden Wahlkreis veröffentlicht. Der Wähler kann anhand seiner Quittung überprüfen, ob die von ihm gewählte Schlüsselzahl bei der korrekten Partei auftaucht. Tatsächlich müssen sogar alle Schlüsselcodes auf der Quittung bei der jeweiligen Partei vermerkt sein; der Wähler kann quasi auch noch drei weitere Stimmen auf Korrektheit überprüfen. Wie man sieht, kann bereits bei Abgabe von nur zwei Stimmen aus der Quittung nicht darauf geschlossen werden, für wen der Wähler gestimmt hat.

Das Hauptproblem ist, dass man dem Wählern wohl kaum das Hantieren mit Zahlen bei der Wahl zumuten kann, insbesondere bei Wahlen, wo mehrere Stimmen abgegeben werden müssen. Ansonsten dürfte dieses Verfahren hinsichtlich Einfachheit und Sicherheit kaum zu überbieten sein.

Könnte man nun nicht auf die Eingabe des Teilschlüssels verzichten? Leider nein, denn sonst könnte die Maschine mehreren Wählern den selben Schlüssel für die gewählte Partei anbieten und im Hintergrund die “eingesparten” Stimmen auf andere Parteien verteilen (*Vote Sharing* Angriff), ohne dass dieses aufgedeckt werden könnte, es sei denn, zwei Wähler würden zufällig ihre Quittungen miteinander vergleichen. Als Beweis wären diese Quittungen aber nicht geeignet, da sie jeweils unterschiedliche Füllstimmen enthalten könnten.

Wie lang der einzugebende Teilschlüssel im Verhältnis zur Gesamtlänge des Schlüssels optimalerweise sein sollte, hängt davon ab, inwieweit man Sicherheit gegen Anonymität gewichtet. Je mehr Ziffern eingegeben werden, umso weniger anonym wird der Schlüs-

sel[4], und je weniger Ziffern eingegeben werden, umso mehr Möglichkeiten hätte ein Manipulator, durch provozierte Schlüsselkollisionen Stimmen einzusparen und umzuverteilen.

Allerdings könnten bereits bei einer einzigen einzugebenden Stelle nur 10% der Stimmen umverteilt werden, bei zwei Stellen nur 1% und bei drei Stellen wäre erfolgreicher Betrug auf 0.1% begrenzt; bei den vorgeschlagenen vier Stellen wäre es unwahrscheinlich, das selbst bei mehreren tausend Wählern pro Wahlcomputer auch nur eine einzige Stimme unbemerkt umverteilt werden könnte, selbst wenn der Rechner manipuliert wäre.

Die Eingabe der Ziffern schützt also vor dem *Vote Sharing* Angriff, denn selbst wenn ein Angreifer den Rechner unter seiner Kontrolle hat, so darf er nur gültige Quittungen erzeugen. Er darf auch nur so viele Stimmschlüssel erzeugen, wie Wähler sich beteiligen.

Die Stimmen müssen auf jeden Fall veröffentlicht werden, und es wäre auch zulässig aber nicht förderlich, die Quittungen zu veröffentlichen, denn es würde die Sicherheit nicht verbessern und die Anonymität verschlechtern[5].

Wenn ich also beim Wählen eine Zahl (mit)bestimme, die ins Wahlergebnis aufgenommen werden soll, habe ich gewissermassen ein unbedingtes Vorschlagsrecht. Betrachtet man nur den von mir mitbestimmten Teil, so gilt folgendes: Wenn ich sage, die Nummer 1234 soll eine CCC-Stimme sein, wird das ja öffentlich gemacht. Steht die Zahl nicht drin, der Wahlcomputer hat mir aber quittiert hat dass sie drinsteht, dann ist wohl nachweisbar etwas schiefgegangen.

Hier ist also für den Manipulator nichts zu holen. Die einzige Möglichkeit, für den manipulierten Computer zu betrügen ist, zwei Personen dieselbe Zahl zu quittieren und Kollisionen auszunutzen. Kollisionen können auch nur bedingt provoziert werden. Hier sorgt der vom Wahlcomputer bereitgestellte Teil der Zahl für zusätzliche Sicherheit.

Wenn der Computer mir eine Zahl mit Leerstellen präsentiert, so legt er sich seinerseits fest und kann diese nicht mehr verändern.

Für eine Manipulation könnte er mir aber statt einer “kollisionssicheren” neuen Zufallszahl eine Zahl aus dem Stimmspeicher nehmen und davon etwa vier Zahlen zur Eingabe zulassen.

Wenn ich mich nun entscheide, zufällig die selben vier Zahlen einzugeben, die der Rechner bereits im Stimmspeicher hat, dann hat er gewonnen und kann die Stimme stehlen.

Wenn der Rechner aber falsch geraten hat, muss er mir demütig meine Stimme korrekt quittieren, falls er nicht ertappt werden will.

---

[4] Um die Anonymität zu verbessern, könnte der Wahlcomputer auch versuchen, möglichst viele solcher Stimmen als Füllstimmen zu nehmen, die dieselben Ziffern in derselben Reihenfolge enthalten, wie vom Wähler eingegeben wurden. (Siehe SPD-Füllstimme im Beispiel.) Dann würden die Füllstimmen erst nach der Eingabe ausgewählt, was der Sicherheit keinen Abbruch tun sollte.

[5] Aus den vollständigen Quittungen lässt sich eine individuelle Wahl herauslesen, wenn eine Zahl nur auf einer einzigen Quittung auftaucht. Da jedoch jede Zahl durchschnittlich auf so vielen Quittungen auftaucht, wie es im Verhältnis Wähler anderer Parteien gibt, dürfte das Problem überhaupt nur dann und dann auch nur vereinzelt auftreten, wenn eine Partei mehr als 50% der Stimmen auf sich vereint.

Der manipulierte Rechner hat bei einer Wahl mit 1000 Wählern und 4 Ziffern also 1000 mal die Möglichkeit, die “richtige” Zahl aus 10.000 möglichen zu erraten. Wäre der Mensch ein guter Zufallsgenerator, so betrüge bei jedem Versuch des Computer die Chance 1:10000. Bei 1000 Versuchen stünde die Chance 1:10 gegen den Computer, unbemerkt auch nur eine Stimme zu stehlen.

Der Mensch ist aber kein perfekter Zufallsgenerator, er ist *biased* oder *unausgewogen*, wird also bestimmte Zahlenkombination häufiger wählen, als andere. Dem liesse sich aber abhelfen, indem anstelle einer Tastatur vier Wahlräder genommen, virtuelle wie auf dem iPhone, oder echte physikalische Räder. Jedes Rad müsste bewegt werden, bevor der Wähler die Wahl bestätigen kann. Nicht dass das schneller wäre als eine Tastatur, es wäre aber sicherer für ahnungslose Wähler.

Für den manipulierten Rechner wäre wohl die beste Strategie, mit einer durchschnittlichen Häufigkeitsverteilung derjenigen Zahlen zu beginnen, die Menschen erfahrungsgemäss eingeben, wenn man sie bittet, vier Zahlen einzugeben, und diese während des Wahlverlaufs statistisch anzupassen. Wenn der Rechner diese häufigste Zahl findet, dann hängt die Zahl aussichtsreicher Kollisionen umgekehrt von der Bereitschaft des Wählers ab, eine echte Zufallszahl einzugeben oder seinem menschlichen Instinkt zu folgen. Allerdings ist der Rechner aufgrund des *Intermingling* nicht völlig frei in seinen Versuchen, Kollisionen zu provozieren; er muss sich aus dem Pool gültiger Stimmen bedienen, kann aber die Ziffern frei auswählen, so dass sich durchaus vielfältige Betrugsoptimierungsstrategien ergeben. Er muss aber unbedingt vermeiden, die selbe Stimme zu oft zu “verwetten”, denn falls er verliert, kommt ein Schlüssel ins Wahlergebnis, der verdächtige Ähnlichkeit mit einem anderen Schlüssel aufweist[6].

Wenn ich als Wähler also dem Computer eine möglichst schlechte Chance geben will, bringe ich meinen eigenen Zufallsgenerator mit. Oder ich generiere mir zuhause oder vor Ort eine Zufallszahl, indem ich einen zehnseitigen Würfel mitbringe, oder ich nehme einfach eine von meinen Bank-Pins. Entscheidend ist, dass ich als Wähler meine Stimme quasi mit einem selbstgewählten Code schützen kann, wie bei einem Zahlenschloss mit frei wählbaren Code.

Und man könnte den Schlüssel leicht länger machen. Je länger der Schlüssel aber wird, umso eher wäre der Wähler in der Lage, den Schlüssel zu markieren, indem er etwa vier bestimmte gleiche Zahlen eingibt. Generell ergibt sich durch statistische Auswertung die Möglichkeit, die vom Benutzer *mitbestimmten* Schlüssel von automatisch generierten mit einer gewissen Wahrscheinlichkeit zu unterscheiden. Da das Verfahren aber insgesamt mit einer im Vergleich zu den Gesamtstimmen relativ kleinen Zahl von synthetischen Füllschlüsseln auskommt, könnte man bei einer solchen Auswertung allenfalls mit einer gewissen Wahrscheinlichkeit darauf schliessen, dass jemand ein oder zwei Parteien vermutlich nicht gewählt hat. Beweisen könnte man das aber nicht.

---

[6] Diese Tatsache liesse sich sogar dazu nutzen, das Verfahren noch sicherer zu machen, indem der Computer nur Zahlen präsentieren darf, bei denen mit Ausnahme der Leerstellen alle Ziffern komplett kollsionssfrei sein müssen. Damit würde selbst ein einziger fehlgeschlagener Versuch, eine Kollision herbeizuführen, einen Manipulationsversuch offenbaren. In diesem Fall käme man sogar mit der Eingabe einer einzigen Zahl aus. Allerdings würden dadurch die Zahlen unpraktikabel lang, und die Sicherheit des Verfahrens an sich wäre dadurch für den Laien schwieriger zu durchschauen und böte möglicherweise neue Angriffsmöglichkeiten.

Was passiert nun, wenn einer der Schlüssel nicht in der richtigen Liste auftaucht, von der der Wähler glaubt, das er auftauchen müsste? Er kann dann mit der Quittung zum Wahlleiter gehen und die Wahl anfechten, sogar ohne seine Wahl preisgeben zu müssen. Er kann aber nicht böswillig behaupten, dass seine Stimme nicht gezählt wurde.

Gibt es weitere Schwächen dieses Verfahrens? Nun, ein manipulierter Wahlcomputer könnte anstelle zufällig ausgewählter Schlüssel die dem Wähler angebotenen Zahlen so auswählen, dass ein Rückschluss auf die Wahlentscheidung getroffen werden kann, etwa wenn jeweils ein Satz von ausschliesslich geraden Zahlen angeboten wird und die neue Zahl für die Wahl immer ungerade ist oder umgekehrt. Das das nicht versehentlich passiert, lässt sich durch eine *Public Source* Politik am ehesten vermeiden.

Allerdings kann ein manipulierter Wahlcomputer beliebige andere, einfachere Methoden verwenden und etwa die Wahlentscheidung leicht per Funk übertragen, oder eine mit Zeitstempeln versehe Liste für den späteren Abruf speichern. Generell kann sich ein Wähler bei Einsatz von manipulierten Wahlcomputern nicht gegen einen Verrat seiner Wahl schützen, während er selbst beim Einsatz von Kameras bei der Zettelwahl noch eine gewisse Chance hat, seine Wahl zu verbergen.

Ein weiteres Problem ergibt sich noch aus den Füllstimmen. Wenn der Rechner sie selbst *erfinden* kann, könnte ein manipulierter Rechner sie einfach umverteilen. Das wären zwar je nach Anzahl nur ein bis drei Stimmen je Partei, das könnte aber wahlentscheidend sein. Dafür gibt es aber einen Ausweg, der aber auch nicht ganz ohne Mehrarbeit zu haben ist:

Die Wahlhelfer führen zu Beginn der Wahl eine *Initialisierungswahl* durch. Bei der *Initialisierungswahl* werden aber statt einer alle Parteien “angekreuzt”; dies kann auch automatisch erfolgen. Praktisch kämen also vor Beginn der Wahl so viele Wahlscheine aus der Maschine, wie es Füllstimmen pro Partei gibt, also in der Praxis etwa drei. Damit sind die Füllstimmen praktisch bekannt, und die Aufgabe des Wahlleiters wäre es dann, am nächsten Tag die Quittungen genau so wie jeder Wähler zu überprüfen und ansonsten vertraulich zu behandeln. Das ist nicht schön, denn es müsste ja jeder Bürger das Recht haben, dem Vorgang beizuwohnen und damit die Füllstimmen zu sehen. Sie wären damit nicht geheim, sollten aber auch nicht allgemein veröffentlicht werden.

Damit wäre das Wahlgeheimnis für die ersten Wähler zwar nicht so gut geschützt wie für spätere Wähler, aber immer noch besser als bei einem fortlaufenden Papierstreifen oder durch die Tatsache, dass ein Wahlschein in der Urne ganz unten liegt. Beides ist nicht perfekt, in der Realität aber wohl tolerierbar. Wichtiger ist, dass ein Umverteilen der Füllstimmen nur dann möglich wäre, wenn sowohl der Wahlcomputer manipuliert ist als auch die Wahlhelfer beim Betrug mitmachen würden.

Das Prozedere der Füllstimmengenerierung ist zwar lästig, würde die Wahlhelfer insgesamt wohl auch nicht wesentlich mehr (über)fordern als der Einsatz existierender Wahlcomputer.

Ein besonders dreister Wahlbetrüger könnte den Computer noch so programmieren, dass die Quittung gelegentlich nicht mit der Bildschirmanzeige übereinstimmt und darauf hoffen, dass der Wähler dass nicht im einzelnen prüft. Dabei könnte er etwa auch die Zahlen auf dem Bildschirm möglichst unauffällig in andere Zahlen *morphen*. Aussicht auf erfolgreiche Manipulation in grossem Umfang bietet diese Vorgehensweise aber nicht, da der eine oder andere aufmerksame Wähler dies sicher bemerken würde.

Insgesamt erscheint *Intermingled Key Voting* aufgrund seiner Transparenz sehr sicher und robust gegen unbemerkbare Manipulation. **Das Wahlergebnis kann auch durch beliebige Manipulation des Wahlcomputers nicht unbemerkt manipuliert werden**. Es erfüllt also die NIST-Empfehlung bezüglich *Software Independence* des Wahlergebnisses. [NIST06]

Hinsichtlich der Vertraulichkeit der Wahl gibt es Schwächen, die hinsichtlich der Erpressbarkeit insgesamt nicht schwerwiegender sind, als Fingerabdrücke und DNA-Spuren auf Wahlzetteln, aber problematischer sind als kompromittierende Abstrahlung, da das Abhören einen hohen zielgerichteten Aufwand *während der Wahl* erfordert und dabei eher geringe Wirkung entfaltet und allenfalls in Sonderfällen lohnt, etwa bei Amtsträgern oder Prominenten.

Generell bietet das Verfahren aber keinen Schutz der Vertraulichkeit, wenn der Wahlcomputer manipuliert ist, was aber ein Verfahren mit *Ende zu Ende Sicherheit* prinzipiell nicht leisten kann.

Die Praktikabilität muss aber nicht aus Sicherheits- oder Vertraulichkeitsmängeln bezweifelt werden, es ist der Zusatzaufwand bei Wählern und Wahlveranstaltern, der das System unattraktiv macht. Ausserdem deckt IKV nicht nur Betrug, sondern auch sämtliche etwaigen Fehler in der Kette schonungslos auf und dürfte daher zu einer höheren Zahl erfolgreicher Wahlanfechtungen führen.

Unterschiede zum *Bingo Voting*

Das *Intermingled Key Voting* ähnelt dem sogenannten *Bingo Voting*,[BOHLI07] ist aber tatsächlich von mir unabhängig erdacht worden. Das spricht zunächst für *Bingo Voting*, da offenbar ähnliche Überlegungen zu scheinbar ähnlichen Lösungen geführt haben. Interessanterweise scheitert *Bingo Voting* an mehreren Problemen, die das *Intermingled Key Voting* vermeidet. Darüberhinaus ist *Intermingled Key Voting* um Größenordnungen einfacher, da es auf komplizierte Kryptographie verzichtet, im Gegensatz zu *Bingo Voting*, das auf eine Reihe komplexer und für den Nichtexperten völlig unverständliche kryptographische Verfahren setzt und damit das Gegenteil von transparent ist.

Intermingled Key Voting und *Bingo Voting* ähneln sich insofern, dass bei beiden Verfahren eine ähnliche Quittung mit Schlüsseln für jede Partei ausgestellt wird. Bei beiden Verfahren werden die entsprechenden Abstimmungslisten anschliessend veröffentlicht.

Beide Verfahren nutzen Füllstimmen, aber auf sehr unterschiedliche Art. IKV nutzt Füllstimmen nur, um den ersten Wählern eine gewisse Vertraulichkeit zu bieten, nutzt aber im Wesentlichen die Stimmen anderer Wähler als Gross der Füllstimmen.

Bingo Voting benötigt dagegen für jeden potentiellen Wähler eine Füllstimme je Partei. Diese Füllstimmen werden im Vorfeld erzeugt, gespeichert und in verschlüsselter Form veröffentlicht. Sie bestehen aus einer zufälligen ID und der Zuordnung zu einer Partei. Dabei wird mit Hilfe einer weiteren Zufallszahl so verschlüsselt, dass sich die Zugehörigkeit zu einer bestimmten Partei entschlüsseln lässt, ohne die ID preiszugeben. Damit kann im Vorfeld gezeigt werden, dass auf jede Partei gleich viele Füllstimmen entfallen, ohne die IDs offenzulegen. Gezeigt heisst hier aber, dass sich Experten davon überzeugen können, allerdings auch unabhängige Experten.

Während der Wahl wird nun, ähnlich wie beim IKV im Falle des ersten Wählers, aus der Liste der Füllstimmen ein *Quittungsentwurf* generiert, wobei für jede Partei dem Wähler eine Füllstimme präsentiert wird. Dabei werden die IDs wie beim IKV neben der jeweils zugehörigen Partei angezeigt. Wie die geheimen IDs in die Wahlmaschine und im Klartext auf den Bildschirm gelangen, ist nicht ganz klar, aber es gibt eigentlich nur zwei Wege: Entweder sie werden im Gerät erzeugt dort samt der Schlüssel gespeichert, und vor dem Wahltag ausschliesslich verschlüsselt exportiert, oder sie werden vorher außerhalb erzeugt und mitsamt der Schlüssel ins Gerät übertragen.

Im nächsten Schritt wird bei der Wahl durch einen Zufallsgenerator eine garantiert zufällige ID erzeugt. Der Zufallsgenerator soll dabei unmittelbar nachvollziehbar zufällig arbeiten, also eine Art mechanisches Lotto-, Roulette- oder Würfelgerät sein. Diese ausgewürfelte neue ID ersetzt die ID der Füllstimme der gewählten Partei auf dem Bildschirm, und wie beim IKV erhält der Wähler eine Quittung mit den allen IDs und Parteien, wobei bis auf eine ID alle IDs Füllstimmen sind.

Nach Abschluss der Wahl werden dann folgende Dinge veröffentlicht:
- Das Wahlergebnis
- Eine Liste aller Quittungen
- Eine Liste aller unbenutzten Stimme/Kandidaten-Paare, einschliesslich der Schlüssel zum Entschlüsseln
- Ein Zero-Knowledge Beweis, das alle unveröffentlichten (geheimen) Füllstimmen auch in die Auszählung eingegangen sind

Die Schlüssel für die benutzen Leerstimmen müssen unbedingt vertraulich bleiben; wer im Besitz einer Kopie ist, kann aus jeder Quittung die tatsächliche Wahlentscheidung ermitteln und z.B. Belohnung auszahlen. Beim *Intermingled Key Voting* dagegen gibt es nur wenige Leerstimmen, bei deren Bekanntwerden nur das Wahlgeheimnis weniger Wähler betroffen ist.

Die Sicherheit beim *Bingo Voting* steht und fällt aber mit dem hypothetischen, beobachtbar sicheren Zufallsgenerator. Faktisch wird ein komplexes, nicht realisierbares System, der *sichere Wahlcomputer*, durch ein etwas einfacheres, weniger komplexes, aber gleichfalls nicht realisierbares System ersetzt: Den *vertrauenswürdigen Zufallsgenerator*. Das ist in jedem Fall ohne jeden Sarkasmus ein Fortschritt, aber nur ein theoretischer, denn bei dem bisher eingesetzten Prototypen wurde aus Gründen der Realisierbarkeit als Zufallsgenerator eine Chipkarte verwendet, die damit das einzige potentiell Vertrauen stiftende Merkmal von *Bingo Voting* zunichte macht. Denn wieso sollte der Wähler einem unsichtbaren Zufallsgenerator vertrauen, der aus fremder Hand stammt? Und benutzt man einfach eine Chipkarte ohne eigenes Display, kann der manipulierte Wahlcomputer diese einfach ignorieren, eine Quittung wieder verwenden und die Stimme frei vergeben.

Die prinzipiellen Unterschiede zwischen IKV und *Bingo Voting* bestehen darin, dass beim *Bingo Voting* die Füllstimmen zwingend mit hohem Aufwand geheim gehalten werden müssen, und das der Wähler keinen *eigenen Zufall* einbringen kann, sondern dem *Zufall des Herstellers* vertrauen muss. Ersteres gefährdet das Wahlgeheimnis, zweites aber ermöglicht Manipulation.

Die Fehler, die die Entwickler des *Bingo Voting* gemacht haben, resultieren vermutlich aus einer zentralistischen Denkweise. Es war offenbar der Wunsch vorhanden, Fehler und Betrug zentral feststellbar zu machen, bevor das Ergebnis veröffentlicht wird. Man wollte vielleicht unbewusst die Kontrolle zentralisieren, und als Wahlveranstalter nicht nur das Ergebnis, sondern den glorreichen Beweis für die Korrektheit des Wahlergebnisses veröffentlichen dürfen, auch wenn ihn praktisch niemand versteht. Durch diese verständliche, aber sachlich eher untergeordnete Anforderung ist eine gute Idee ins Abseits gelaufen und zu nicht mehr als einer netten akademischen Spielerei geworden.

Bei *Bingo Voting* wurden wichtige Grundregeln für den Entwurf sicherer Systeme missachtet:
1. *Policy before Protocol*: Bevor man eines Schutzmechanismus entwirft, sollte man sich genau überlegen, was man eigentlich vor wem schützen möchte
2. *Sparsamer Umgang mit Geheimnissen*: Wenn man Geheimnisse erzeugt, sollte man dabei höchst sparsam sein, denn jedes Geheimnis, etwa ein Schlüssel, erzeugt zusätzlichen Aufwand für dessen sichere Handhabung.

Beim *Bingo Voting* werden im Vorfeld gewaltige Mengen an Schlüsselmaterial erzeugt, die sicher verwahrt und transportiert werden müssen, wenn sich nicht alles nur innerhalb der Wahlmaschine abspielt. Dann werden geheime Schlüssel auch noch sortiert, teilweise veröffentlicht und verarbeitet. Geradezu grotesk ist, dass das gesamte Schlüsselmaterial quasi in den Händen der Wahlveranstalter lagert und ihnen damit das Privileg von Stimmenkauf und Erpressung einräumt. Man mag einräumen, dass die Schlüssel nur innerhalb der Maschine gelagert und vor den Wahlveranstaltern geschützt sind, aber da bleibt mir als Wähler wieder mal nur Vertrauen in die Hersteller. Damit ist man beim Vertrauen keinen Millimeter weiter als heute, auch wenn der tatsächliche Bruch des Wahlgeheimnisses in der Praxis für den Angreifer deutlich weniger Wert hat, als eine unentdeckte Manipulation des Wahlergebnisses. Beim Wahlgeheimnis ist entscheidender, dass der Wähler das subjektive Gefühl hat, dass die Wahl geheim ist. Dabei schneiden Computerwahlen grundsätzlich schlechter ab.

Schwerwiegender ist, dass die Betrugssicherheit von *Bingo Voting* von der Sicherheit von Teilen der Maschine abhängt, die vom Wähler nicht überprüft werden kann, und nicht vom Verfahren, wie beim *Intermingled Key Voting*. Dazu ist das das Ganze unnötig kompliziert, und die *Failure Modes* sind katastrophal. Trotz einer grossen oberflächlichen Ähnlichkeit zum IKV weist das *Bingo Voting* hinsichtlich der Sicherheit sehr gegensätzliche Eigenschaften auf. Inbesondere erfüllt es nicht die Anforderung der *Software Independence*.

Dass ein solches Verfahren auch noch mit einem Innovationspreis [ITSP08] bedacht wird, offenbart eine bemerkenswerte Ahnungslosigkeit und einen hohen Realitätsabstand der Branche, wenn man nicht bereit ist, Böswilligkeit und niedere Absichten zu unterstellen.

Das Votum von Karlsruher Studenten, die *Bingo Voting* bei der Unabhängigen Wahl praktisch erfahren durften, war ebenfalls wenig euphorisch. [WOLF08]

Qualitätsvergleich verschiedener Wahlverfahren

Die folgende Tabelle versucht einen subjektiven Vergleich der Wahlverfahren hinsichtlich verschiedener für den Einsatz wichtiger Eigenschaften. Die Bewertungen orientieren sich dabei an einer groben, in der Betriebswirtschaft üblichen stark vereinfachend Kategorisierung in *gering, mittel, hoch*. Für Ausnahmefälle gibt es noch zwei weiteren Kategorien, falls ein Merkmal extrem ausserhalb des Rahmens liegt. Dazu korrespondieren die in Klammern stehenden Symbole (+,o,-), bzw. (++,--), die jedoch angeben, inwieweit das Merkmal vorteilhaft ist, also *gut, mittel, schlecht*. Zudem ist die Bewertung eher relativ als absolut zu sehen, *hoch* bedeutet als nicht absolut *hoch*, sondern *hoch* im Vergleich mit anderen Bewertungen in derselben Zeile. Die zusammengefassten Kategoriebewertungen sind so zu lesen: Das erste Symbol ist entscheidend, das zweite, sofern vorhanden, gibt eine Tendenz an. “o+” bedeutet also im Prinzip “etwas besser als mittel”, “+o” bedeutet “gut, aber nur fast gut”.

	Stift/Papier/Urne	**Computerisierte Urnenwahl**	**Interminngled Key Voting**	**Bingo Voting**	**Blackbox Voting (NEDAP ESD1-3)**
Kosten	**o+**	**o-**	**-**	**-**	**o**
- Beschaffung	gering (+)	hoch (-)	hoch (-)	hoch (-)	mittel (o)
- Betrieb	gering (+)	hoch (-)	hoch (-)	hoch (-)	mittel (o)
- Vor- und Nachbereitung	mittel (o)	mittel (o)	hoch (-)	hoch (-)	mittel (o)
- Personal	mittel (o)	gering (+)	gering (+)	gering (+)	gering (+)
Transparenz	**+**	**+**	**o**	**-o**	**-o**
Verständlichkeit	hoch (+)	hoch (+)	mittel (o)	gering (-)	mittel (o)
Nachvollziehbarkeit	hoch (+)	hoch (+)	mittel (o)	gering (-)	gering (-)
Beobachtbarkeit	hoch (+)	hoch (+)	mittel (o)	mittel (o)	gering (-)
Sicherheit	**+o**	**+o**	**+**	**o+**	**-**
Ausfallsicherheit	hoch (+)	mittel (o)	gering (-)	gering (-)	mittel (o)
Messpräzision	mittel (+)	hoch (+)	hoch (+)	hoch (+)	mittel (+)
Manipulationsschwelle	gering (-)	mittel (o)	hoch (+)	hoch (+)	mittel (o)
Manipulationseffektivität	gering (+)	gering (+)	gering (+)	sehr hoch (--)	sehr hoch (--)
Manipulationsentdeckungsrisiko	hoch (+)	mittel (o)	sehr hoch (++)	mittel (o)	sehr gering (--)

	Stift/Papier/Urne	**Computerisierte Urnenwahl**	**Intermingled Key Voting**	**Bingo Voting**	**Blackbox Voting (NEDAP ESD1-3)**
Nachprüfbarkeit					
- für Experten	hoch (+)	hoch (+)	sehr hoch (++)	sehr hoch (++)	nein (--)
- für Wähler	mittel (o)	mittel (o)	mittel (o)	gering (-)	nein (--)
Anonymität	**+o**	**o**	**o-**	**o-**	**o**
- Belauschbarkeit	gering (+)	mittel (o)	mittel (o)	mittel (o)	mittel (o)
- Verrat durch technische Manipulation	gering (+)	hoch (-)	sehr hoch (--)	sehr hoch (--)	hoch (-)
- Verrat durch-Wahlschein/Quittungsanalyse	mittel (o)	gering (+)	mittel (o)	mittel (o)	nein (++)

Tabelle 2

Resumé

In diesem Papier wurden zwei Varianten von elektronischen Wahlsystemen vorgestellt, die die Anforderungen an demokratische Wahlen theoretisch erfüllen, bei zwei weiteren gezeigt, warum sie hier durchfallen. Alle Systeme wurden Papierwahlen gegenübergestellt.

Die erste demokratiekompatible Variante ist aber tatsächlich eine verkappte Urnenwahl und aus Kostengründen wohl nicht praktikabel, möchte man sie richtig machen. Zudem enthält sie Restrisiken, die bei technischem Fortschritt eine konkrete, zugelassene Ausführung etwa hinsichtlich der elektronischen Abstrahlung demokratieunverträglich machen können. Dazu kommt, das in einem solchen Fall ein Entzug der Verwendungsgenehmigung offenbar wiederum erst den Gang zum Bundesverfassungsgericht erfordern könnte, da die Verantwortlichen sich den Gefahren der Verwendung selbst offensichtlich unzulässiger Geräte vehement verschliessen.

Der zweite Ansatz, das *Intermingled Key Voting*, versucht mit einer einfachen kryptografischen Methode eine *Ende zu Ende Sicherheit* (E2E) vom Abstimmen am Gerät bis zur Veröffentlichung der Ergebnisse herzustellen, scheitert letzen Endes an der notwendigen umständlicheren Bedienung der Geräte, wobei der Versuch nur sehr knapp scheitert und durchaus eine Wahl mit einem Höchstmass an Sicherheit bei einem sparsamen Technologieeinsatz ermöglicht. Genau genommen handelt es sich aufgrund des Quittungsdrucks auch nicht um ein rein elektronisches Verfahren, allerdings wäre der Quittungsdruck verzichtbar, wenn man sich die Zahlen merken würde oder elektronisch vor Ort übermittelt bekäme, etwa als digital signierte SMS auf seinem Handy oder E-Paper-Device. Das ist zwar wenig praktikabel, zeigt aber, dass die Sicherheit des Verfahrens nicht von der gegenständlichen Manifestation einer Quittung abhängt.

Für *Hochsicherheitswahlen*, wo es auf jede einzelne Stimme ankommt und die Wähler bereit sind, den Zusatzaufwand für die bessere Sicherheit in Kauf zu nehmen, könnte sich das Verfahren anbieten, allerdings wird wohl auch die Papstwahl für die nächsten zweitausend Jahre ohne Computer auskommen.

Im folgenden noch einmal der Vergleich der Wahlverfahren als Auszug. Die besten einer Kategorie sind fett umrahmt:

	Stift/Papier/Urne	**Computerisierte Urnenwahl**	**Intermingled Key Voting**	**Bingo Voting**	**Blackbox Voting (NEDAP ESD1-3)**
Kosten	**o+**	**o-**	**-**	**-**	**o**
Transparenz	**+**	**+**	**o**	**-o**	**-o**
Sicherheit	**+o**	**+o**	**+**	**o+**	**-**
Anonymität	**+o**	**o**	**o-**	**o-**	**o**
Gesamt	**+o**	**o+**	**o-**	**-o**	**-o**

Tabelle 3

Es zeigt sich, das es kein “bestes” Verfahren über alle Kriterien hinweg gibt, wobei die **Urnenwahl** insgesamt den besten Kompromiss darstellt, wenn man alle vier Kriterienbereiche gleich gewichtet. In drei von vier Kategorien ist sie das Beste, was man kriegen kann.

Dies ist auch das Ergebnis, zu dem die irische *Commission on Electronic Voting* und die niederländiche *Election Process Advisory Commission* gekommen sind. [ICOEV06],[DEPAC07]

Auch mit der ***computerisierten Urnenwahl*** kann man leben, wenn man bereit ist, deutlich mehr Geld auszugeben und dabei keine Kompromisse bei der Sicherheit macht, denn die Tabelle gilt nur für Systeme, die praktisch eine Wahlurne benötigen, die *Selbstkontrollkette* bewahren, über *Public Source* Hard- und Software verfügen, unabhängig geprüft sind, sicher verwahrt werden, und alles nach dem *letzten Stand der Forschung*, nicht dem *Stand der Technik*. Ein einziger Fehler in der Konstruktion oder Nachlässigkeit in der Handhabung können die Sicherheit oder Anonymität nachhaltig gefährden.

Intermingled Key Voting würde man den Vorzug geben, wenn es allein auf Sicherheit ankäme, aber der Zusatzaufwand ist nicht zu unterschätzen, vor allem für den Wähler, obwohl er im wesentlichen “nur” aus der Eingabe einer vierstelligen Zahl je “Kreuz” besteht. Schön daran ist, dass der Wähler im Nachgang überprüfen kann, ob seine Stimme gezählt wurde. Das kann natürlich zum Horror für Wahlveranstalter werden.

In einem Satz zusammengefasst: Hinreichend sichere Wahlcomputer sind theoretisch möglich, die Sicherheit muss aber so teuer erkauft werden, dass in der Praxis entweder darauf verzichtet oder zur Wahlurne gegriffen werden muss.

Für das Deutsche Bundesverfassungsgericht stellt sich derzeit eine schwierige Aufgabe. Es muss in den nächsten Monaten über die Zulässigkeit von computerisierten Wahlen entscheiden, und möchte sicher einem technischen Fortschritt, der bequemeres und sicheres Wählen ermöglicht, nicht im Wege stehen.

Andererseits zeigt die gegenwärtige Situation, dass es auf der Welt keinen einzigen real existierenden Wahlcomputer gibt, der die Anforderungen an demokratische Wahlen erfüllt, und vermutlich in absehbarer Zukunft auch nicht geben wird.

Gegenwärtige real existierende Wahlcomputer stellen Gefahren für die Demokratie dar. Die Ursache darin liegt vor allem im ökonomischen Druck. Urnenwahlen sind nicht teuer, sicher und einfach. Wahlcomputer sind bequem für die Wahlveranstalter, doch diese haben kein gesteigertes Interesse an Sicherheit und sollen möglichst Geld sparen.

Wäre ich Richter am Bundesverfassungsgericht, so würde es mir schwerfallen, Wahlcomputer grundsätzlich zu verbieten, obwohl dies angesichts aller bisherigen Erfahrungen, vor allem international, das Einfachste und Sinnvollste wäre.

Doch auch wenn ich Tür einen Spalt offen ließe, ich wäre nicht bereit, weniger Transparenz und Sicherheit als bei der Urnenwahl zuzulassen. Ich würde eine physikalische Manifestation der Stimme verlangen, aber nicht in Form eines fortlaufend beschriebenen Papierbandes, das die Anonymität aushebelt, und ich wäre nicht bereit, Wahlbetrügern das Leben einfacher zu machen. Ich würde auch bei der elektromagnetischen Abstrahlung das Wahlgeheimnis nicht wesentlich geringer gewichten als das Bedürfnis von Militärs und Geheimdiensten, sich nicht auf den Bildschirm schauen zu lassen.

Und ich würde den Wählern nicht zumuten, durch irgendwelche Reifen zu hüpfen, wenn sie ihre Stimme abgeben. Ich würde daher Studien mit unabhängiger Begleitung vorschreiben, die die Bedienung und das Gefühl der Wähler dazu untersuchen, und diese alle zehn Jahre wiederholen lassen.

Des weiteren würde ich mir die Leichtfertigkeit, Unbekümmertheit, den Starrsinn und die kommerziellen Interessen der Verantwortlichen und der Wähler vor Augen halten sowie deren Bereitschaft, Schlupflöcher zu suchen, anstatt Moral walten zu lassen.

Ich würde vor allem darauf bestehen, dass die bei Urnenwahlen bestehende *Selbstkontrollkette* für den Wähler unter allen Umständen erhalten bleibt.

Damit wären Wahlcomputer in Deutschland zwar nicht theoretisch, aber praktisch tot, denn niemand wäre bereit, für das bisschen Bequemlichkeit den notwendigen hohen Preis zu zahlen, wenn keine Abstriche mehr an der Demokratieverträglichkeit der Geräte erlaubt wären.

Und wenn ich schon dabei wäre, ein Urteil zu formulieren, dann würde ich auch die für die Auszählung eingesetzten Computer mit einbeziehen, denn neben dem Problem der Stimmabgabe ist der Einsatz von Computern zur Feststellung des Wahlergebnisses eine weitere potentielle Fehlerquelle und eröffnet Raum für Manipulationen.

Nach Gerüchten wurde in Italien und in den U.S.A. versucht, Prognosen, Übermittlung und Bekanntgabe von Wahlergebnissen zu manipulieren, um Zeit für Upstream-Manipulationen und deren Verschleierung zu gewinnen. Nicht alle Versuche sollen geglückt, nicht alle gescheitert sein. [TS06],[SZ06],[TISC06],[BBV]

Und nicht das Zustandekommen solcher Gerüchte schadet der Demokratie und der Legitimation der Gewählten, sondern die Tatsache, dass die Öffentlichkeit gegenwärtig von der Beobachtung und Überprüfung des Zusammenrechens der Ergebnisse weitgehend ausgeschlossen ist. An dieser Stelle wäre durchaus noch Spielraum für technische und gesetzgeberische Verbesserungen.

Für die Stimmabgabe und Auszählung im Wahllokal aber brauchen wir zum Glück keine Wahlcomputer, Stift und Papier sind da kaum zu übertreffen, wobei ich als Nerd natürlich viel mehr Spass an *Intermingled Key Voting* hätte.

Über dieses Papier

Dieses Papier ist aus einem Blogeintrag und einem Artikel für die Datenschleuder heraus entstanden und wurde von mir über einen Zeitraum von zwei Jahren mehrfach überarbeitet.

Und es ist viel länger geworden, als ursprünglich beabsichtigt und eher zu lang. Es wendet sich zugleich an Fachleute, es sollte aber auch für Nichtfachleute verständlich sein, das ist jedenfalls die Intention.

Es steht nicht im Zusammenhang mit meinen beruflichen Aktiviäten und ist nicht notwendigerweise ist offizielle Haltung des CCC zum Thema Wahlcomputer.

Danksagung

An dieser Stelle Dank an die Mitglieder oben stehender NGOs, ohne deren unermüdliche Arbeit ich wohl niemals auf die Idee gekommen wäre, mit mit einem bei oberflächlicher Betrachtung so langweiligen Thema wie Wahlcomputern zu beschäftigen. Auf den zweiten Blick aber offenbart es sich nicht nur als wichtiges Anliegen, sondern durchaus als intellektuelle Herausforderung, obwohl es ja eigentlich nur um Zählen von Tastendrücken geht.

Dank vor allem auch an die Nerds aus dem Berliner Club, deren Gepflogenheiten gemäß ich auch auf die Nennung von Namen verzichte. Sie haben mit ihrem Input und Feedback dieses Papier maßgeblich mitgeprägt.

Über die Quellen

Die Quellen umfassen zunächst eine Reihe von Information aus erster Hand: Schaltpläne und Quellcodes von Wahlcomputern, persönliche Untersuchungen an realen Wahlcomputern, persönliche Beobachtung von Computerwahlen, Gesetzestexte, Prüfverordnungen, Prüfberichte, persönliche Interviews mit Computerwählern, Computerwahlhelfern und Wahlvorständen von Computerwahlen.

Hinzu kommen Veröffentlichungen kommunaler Haushalte, Protokolle des Petitionsausschusses des Bundestages, Verfassungsgerichtsurteile, Berichte ausländischer Untersuchungskommissionen, Gespräche mit Vertretern deutscher, holländischer und amerikanischer NGOs.

Dankenswerterweise verfügen insbesondere die drei NGOs, die sich gegen Wahlcomputer engagieren, über gut gepflegte Quellensammlungen im Internet: Der *Chaos Computer Club*[1], die holländische Vereinigung *Wij vertrouwen stemcomputers niet* [2] sowie die amerikanischen Organisation *BlackBoxVoting.org* [3] unter folgenden URLs:

[1] https://berlin.ccc.de/wiki/Wahlcomputer
[2] http://www.wijvertrouwenstemcomputersniet.nl/
[3] http://www.blackboxvoting.org/

Eine umfangreiche Quellensammlung und eine gute Übersicht zu dem Thema findet sich vor allem in der deutschen, aber auch der englischen und holländischen Wikipedia.

http://de.wikipedia.org/wiki/Wahlcomputer
http://en.wikipedia.org/wiki/Voting_machine
http://nl.wikipedia.org/wiki/Stemcomputer

Quellenverzeichnis

Kürzel	Name/Bezeichnung	Autor(en)	Datum	Quelle	URL
BBVM	Latest Investigations from Black Box	Verschiedene	Nov. 2008	Blackboxvoting.org	http://www.bbvforums.org/forums/messages/1954/1954.html
BOHLI07	Bingo Voting: Secure and coercion-free voting using a trusted random number generator	Bohli et. al.	03.05.2007	Cryptology ePrint archive	http://eprint.iacr.org/2007/162.pdf
BREN06	THEMACHINERY OF DEMOCRACY: PROTECTING ELECTIONS IN AN ELECTRONIC WORLD	Norden et al.	2006	Brennan Center	http://brennan.3cdn.net/a56eba8edf74e9e12e_r2m6b86s2.pdf
BRON38	Excavations on the North Slope of the Acropolis, 1937	Oscar Broneer	1938	Hesperia 7 Issue 2	http://www.ascsa.edu.gr/index.php/publications/hesperia/article/7/2/161-263

Kürzel	Name/Bezeichnung	Autor(en)	Datum	Quelle	URL
BWahlG	BWahlG § 35 Stimmabgabe mit Wahlgeräten	Deutsche Bundestag	28.07.1979	juris	http://bundesrecht.juris.de/bwahlg/
BWahlGV	Bundeswahlgeräteverordnung - BWahlGV	Deutsche Bundestag	03.09.1975	juris	http://bundesrecht.juris.de/bwahlgv/
CCC06	Bericht der CCC-Wahlbeobachtergruppe von der Oberbürgermeisterwahl in Cottbus	CCC	24.10.2006	ccc.de	http://www.ccc.de/updates/2006/bericht-ob-wahl-cottbus
DEPAC07	Voting with confidence	(Dutch) Election Process Advisory Commission	27.09.2007	Durch Government	http://www.wijvertrouwenstemcomputersniet.nl/images/0/0c/Votingwithconfidence.pdf
DSB05	Defense Science Board Task Force On HIGH PERFORMANCE MICROCHIP SUPPLY	Wiliam Schneider et al.	Feb. 2005	Defense Science Board	http://media.popularmechanics.com/documents/DSB-hardware.pdf
FEHN08	Landtagswahl Hessen 2008:Deutlicher Rückgang der Wahlbeteiligung in Gemeinden mit Wahlcomputern	Martin Fehndrich	15.03.2008	wahlrecht.de	http://www.wahlrecht.de/news/2008/11.htm
FELDMAN06	Security Analysis of the Diebold AccuVote-TS Voting Machine.	Feldman, Halderman, Felten	13.09.2006	Princeton Univ.	http://citp.princeton.edu/voting/ts-paper.pdf
GG	Grundgesetz der Bundesrepublik Deutschland	Parlamentarischer Rat	28.08.2006	Bundestag	http://www.bundestag.de/parlament/funktion/gesetze/gg_jan2007.pdf
HEISE081106	Erneut Wahlmaschinen-Debakel in den USA	pmz	08.11.2006	heise.de	http://www.heise.de/newsticker/Erneut-Wahlmaschinen-Debakel-in-den-USA--/meldung/80722
HEISE101107	Für den Wahlstift "ist die Zeit nicht reif"	Richard Sietmann	10.11.2007	heise.de	http://www.heise.de/newsticker/Fuer-den-Wahlstift-ist-die-Zeit-nicht-reif--/meldung/98764
HEISE161106	Wahlcomputer in Florida unterschlagen jede achte Stimme	pmz	16.11.2006	heise.de	http://www.heise.de/newsticker/Wahlcomputer-in-Florida-unterschlagen-jede-achte-Stimme--/meldung/81171
HEISE161107	Aus für den digitalen Wahlstift	Richard Sietmann	16.11.2007	heise.de	http://www.heise.de/newsticker/Aus-fuer-den-digitalen-Wahlstift--/meldung/99089
HSG06	Angebot der HSG Wahlsysteme an die Stadt Cottbus	Herbert Schulze Geiping	24.07.2006	CCC-RD #40894	
ICOEV06	Secrecy, Accuracy and Testing of the Chosen Electronic Voting System	(Irish) Commission on Electronic Voting	04.07.2006	Irish Government	http://www.cev.ie/htm/report/download_second.htm
ITSP08	2. Deutscher IT-Sicherheitspreis	-	2008	Horst Görtz Stiftung	http://www.horst-goertz.de/it_auszeichnung_2008.html
ITSP08-2	Bingo Voting – Verifizierbare Wahlen mit Wahlmaschinen	Bär et al.	30.05.2008	EISS, Universit¨at Karlsruhe	http://www.horst-goertz.de/1_Preis_2008.pdf
LEET-08	Designing and implementing malicious processors	Samuel T. King, et. al.	April 2008	University of Illinois at Urbana Champaign	http://www.usenix.org/event/leet08/tech/full_papers/king/king.pdf
NIST06	DRAFT Whitepaper "Requiring Software Independence in VVSG 2007: STS Recommendations for the TGDC	NIST-TGDC-STS	01.12.2006	NIST	http://vote.nist.gov/DraftWhitePaperOnSIinVVSG2007-20061120.pdf
PM08	Counterfeit Chips Raise Big Hacking, Terror Threats, Experts Say	Popular Mechanics	April 2008	Popular Mechanics	http://www.popularmechanics.com/technology/industry/4253628.html
POHLE07	Wahlrecht und Wahlcomputer	Jörg Pohle	02.11.2007	HU-Berlin	http://waste.informatik.hu-berlin.de/~pohle/studium/studienarbeit-wahlcomputer-wahlrecht.pdf
PTB04	Baumusterprüfung eines Wahlgerätes ESD1	PTB	12.05.2004	Physikalisch-Technische Bundesanstalt	http://www.wahlrecht.de/doku/doku/PB-ESD1-SW03.08-BTW.pdf
RIV06	The ThreeBallot Voting System	Ronald L. Rivest,	01.10.2006	MIT	http://people.csail.mit.edu/rivest/Rivest-TheThreeBallotVotingSystem.pdf
RIVWAC06	On the notion of "software independence" in voting systems	Ronald L. Rivest, John P. Wack	28.07.2006	MIT	http://vote.nist.gov/SI-in-voting.pdf
SCHNEIER04	The Problem with Electronic Voting Machines	Bruce Schneier	10.11.2004	Schneier on Security	http://www.schneier.com/blog/archives/2004/11/the_problem_wit.html
SCHNEIER96	Applied Cryptography Second Edition	Bruce Schneier	1996	ISBN 0-471-11709-9	http://www.schneier.com/book-applied.html
SPIE05	Estland wählt erstmals online	Der Spiegel	16.10.2005	Der Spiegel	http://www.spiegel.de/netzwelt/web/0,1518,379802,00.html
SZ06	Berlusconis Helfer sollen Stimmauszählung manipuliert haben	Süddeutsche Zeitung	24.11.2006	Süddeutsche Zeitung	http://jetzt.sueddeutsche.de/texte/anzeigen/348364/TrkMagTsr5
TISC06	Demokratie kaputt?	Carsten Wollenweber	24.11.2006	Tiscali News	http://europa.tiscali.de/10f160e66dd.html
TS06	Hat Berlusconi bei der Wahl manipuliert?	Paul Kreiner	27.11.2006	Der Tagesspiegel	http://www.tagesspiegel.de/politik/;art771,2241268

Kürzel	Name/Bezeichnung	Autor(en)	Datum	Quelle	URL
WELT06	Wähler sollen künftig digitale Kreuze machen	Florian Hanauer	05.04.2006	Die Welt	http://www.welt.de/print-welt/article208768/Waehler_sollen_kuenftig_digitale_Kreuze_machen.html
WIES08	Wahlcomputereinsatz wirkt sich negativ auf Wahlbeteiligung bei den Kommunalwahlen in Brandenburg aus.	Ulrich Wiesner	03.10.2008	ulrichwiesner.de	http://ulrichwiesner.de/nachrichten.html
WOLF08	Zwei mal drei macht neun - Bingo-Voting bei den Unabhängigen Wahlen – Ein Kommentar	Andreas Wolf	14.07.2008	Der Funke 150, Seite 7	http://fachschaft.etec.uni-karlsruhe.de/images/stories/Funke/funke_150.pdf
WVSCN06	Nedap/Groenendaal ES3B voting computer - a security analysis	Gonggrijp et al.	06.10.2006	NGO wijvertrouwenstemcomputersniet	http://www.wijvertrouwenstemcomputersniet.nl/images/9/91/Es3b-en.pdf

Mit [O] bezeichneten Quellenverweise kennzeichnen Informationen, die aus persönlichen Beobachtungen und Gesprächen gewonnen wurden und daher nicht von Dritten nachgeprüft werden können. Für einige der Gespräche gibt es Video- und/oder Audioaufzeichnungen, die sich in der Obhut des CCC befinden und aus Gründen des Persönlichkeitsrechts nicht öffentlich zugänglich sind.

Über den Autor

Ich, Pavel Mayer, Jahrgang 1965, beschäftige mich seit 1980 professionell mit Elektronik und Computertechnik und habe in dieser Zeit elektronische Schaltungen, Computersysteme, Betriebssysteme, Frameworks und Anwendungen für eine Vielzahl von Branchen entwickelt, eine Reihe von Forschungsprojekten durchgeführt und mehrere Unternehmen gegründet.

Ich verfolge im Zusammenhang mit Wahlcomputern keine wirtschaftlichen Interessen, meine Motivation für diese Arbeit liegt ausschliesslich in der Tatsache begründet, dass ich Demokratie und Menschenrechte für die wichtigsten Errungenschaften unserer Kultur halte, und die demokratische Wahl zu den Kernelementen der Demokratie gehört.

*Ich bin allerdings grundsätzlich technik- und wirtschaftsfreundlich und hätte viel lieber als Ergebnis den Entwurf eines sicheren **und** praktikablen Wahlcomputers präsentiert, auch wenn ich letzten Endes dem Ziel deutlich näher gekommen bin, als ich zwischendurch für möglich gehalten hätte. Ich bin daher über das Ergebnis meiner Überlegungen zum Thema Wahlcomputer insofern erfreut, als das dieses Ergebnis vielleicht dazu beitragen kann, Gefahren für die Demokratie abzuwehren und es mir als Steuerzahler und Dritten erspart, Lebenszeit und Geld in ein eher aussichtsloses und schädliches Unterfangen zu investieren.*

Würden in Deutschland flächendeckend heutige Wahlcomputer für Bundestagswahlen eingesetzt, so würde ich es mir fachlich zutrauen, mit einem Budget von weniger als zehn Millionen Euro mit weniger als fünf Mitwissern und einem Vorlauf von einem Jahr mittels nicht nachweisbarer technischer Mitteln eine beliebige Verschiebung des Wahlergebnisses in einem plausiblen Rahmen zu bewirken.

Zu meinem Glück gibt es in Deutschland bisher nur einen sehr eingeschränkten Einsatz von Wahlcomputern, so dass ein solches Szenario gegenwärtig nicht realistisch ist, und Geld wäre für mich kein Anreiz, an so etwas mitzuwirken.

Sollten aber in Deutschland flächendenkend unsichere Wahlcomputer zum Einsatz kommen, wäre ich in der Versuchung, allein aus sportlichen Gründen einer politischen Gruppierung meiner Wahl an die Macht zu verhelfen.

Wenn das Bundesverfassungsgericht schlechten Wahlcomputern keinen Einhalt gebietet, dann bin mir nur sicher, dass ich auf lange Sicht nicht der Einzige sein werde, der sich auf diese Weise vielleicht ein bisschen Spass verschaffen möchte.

Müsste ich persönlich an einem der heutigen Wahlcomputer wählen, würde ich es wohl lieber sein lassen.

Pavel Mayer