Kritik an „Bingo Voting“

Hadmut Danisch, 9.11.2008

(Für Nicht-Informatiker stark vereinfachte und gekürzte Version der Kritik an „Bingo Voting“; sprachliche Korrekturen und Ergänzung vom 11.11.2008)

Was ist Bingo Voting ? 1
Problematik der elektronischen Wahlmaschinen 1
Ziele und Ansprüche von Bingo Voting 2
Wie funktioniert Bingo Voting? 3

Grundsätzliche Kritik und Funktionstauglichkeit 4
Widersprüchliche und fehlerhafte Voraussetzungen 4
Konstrukt des Wahlleiters 5
Kryptographische Grundsätze mißachtet 5
Kollisionen der Zufallszahlen 5

Nachträgliche Sabotage – Denial of Service 6
Nachträgliche Sabotage durch Maschine/Wahlleiter . . . 7
Nachträgliche Sabotage durch Wähler 7

Angriffe gegen das Wahlgeheimnis 8
Verstoß gegen Grenzen des Wahlgeheimnisses 8
Kein Wahlgeheimnis – ein Hütchenspielertrick 8
Faule Permutationen 10
Faule Commitments 10
Ausrechnen der abgegebenen Stimmen 10

Angriffe gegen die Wahlkorrektheit 11
Erpressung 11
Kollisionen der Zufallszahlen 12
Die Papierkorb-Methode 13
Man-in-the-Middle-Attacke durch Skimming 13

Hintertüren in der Implementierung 14

Fazit 14

Was ist Bingo Voting ?

Bingo Voting ist ein 2007 von mehreren Wissenschaftlern der Universität Karlsruhe vorgestelltes Verfahren für elektronische Wahlen (wie Landtags-, Bundestags- und ähnliche Wahlen). Zu näheren technischen Informationen siehe www.bingovoting.de.

Problematik der elektronischen Wahlmaschinen

Aus verschiedenen Gründen möchte man das herkömmliche Wahlverfahren mit einfachen Stimmzetteln, auf dem die Wahlkandidaten angekreuzt werden, den Einwurf in einfache Urnen und das anschließende Auszählen durch computerbasierte Wahlmaschinen ersetzen. Unter anderem sollen Wahlen dadurch billiger werden, es soll zu weniger ungültigen Stimmen und weniger Fehlern beim Auszählen kommen, es soll weniger Manipulationsmöglichkeiten – oder gar keine mehr – geben, das Ergebnis soll schneller zur Verfügung stehen und fehlerfrei übermittelt werden.

Zwar gibt es bereits verschiedene Wahlcomputer, die in den USA und in Europa eingesetzt werden, sie gelten aber nicht als vertrauenswürdig und haben schon mehrfach fehlerhafte Ergebnisse geliefert oder Funktionsstörungen und Bedienungsprobleme gezeigt. Organisationen wie der Chaos Computer Club konnten Manipulationen der Software vorführen, beispielsweise indem sie einem Wahlcomputer das Schachspielen beibrachten. Aus den USA liegen Berichte von Fehlfunktionen und übergangenen Wahlstimmen vor. Gerade erst vor wenigen Tagen führte der Einsatz von Wahlmaschinen in Finnland zum Fiasko. Der Wähler sollte sich gegenüber der Maschine durch eine Smart Card ausweisen, seine Wahl eingeben und zweimal mit „OK“ bestätigen. Viele Wähler gaben aber nur einmal „OK“ ein, weshalb ihre Stimmen nicht gezählt wurden

und die Wahl deshalb wiederholt werden mußte. Dementsprechend wird Wahlcomputern großes Mißtrauen entgegengebracht.

Hinzu kommen juristische Vorbehalte, weil Wahlen öffentlich abzuhalten sind und gerichtlich überprüfbar sein müssen. Eine »Black Box«, die einfach nach der Wahl ein nicht mehr nachprüfbares Endergebnis ausdruckt, das man so hinzunehmen hätte, gilt deshalb als nicht ausreichend. Computerbasierte Verfahren stehen generell unter dem Vorwurf mangelnder Transparenz, nicht zuletzt, weil manche Hersteller die Software geheim halten.

Ein weiteres Problem von Wahlcomputern liegt in der Gefährdung des Wahlgeheimnisses, weil von aussen und für den Wähler nicht ersichtlich ist, wie und welche Daten der Wahlcomputer speichert. Beispielsweise könnte der Computer Uhrzeit oder Reihenfolge der abgegebenen Stimmen aufzeichnen, über die später mit anderen Informationen über die Wähler das Wahlgeheimnis kompromittiert werden könnte. Auch wären die Übermittlung per Funk oder die sog. „kompromittierende Abstrahlung“ möglich, womit ein Dritter von außerhalb der Wahlkabine feststellen kann, wie jemand gewählt hat.

Ziele und Ansprüche von Bingo Voting

Genau in diese Lücke möchte Bingo Voting stoßen und ein Verfahren vorstellen, das diese Bedenken ausräumt. Dazu stellt sich „Bingo Voting“ im wesentlichen folgende Ziele bzw. nimmt für sich in Anspruch, die folgenden Anforderungen **vollständig, zu 100% und kryptographisch hart beweisbar** zu erfüllen:

1. Die Wahl soll geheim und – mehr noch – erpressungssicher sein. Es soll also ausgeschlossen sein, daß man zur Abgabe einer bestimmen Stimme von Dritten durch Erpressung gezwungen oder durch Bestechung motiviert werden kann.

   Die kryptographische Überlegung ist, daß man als Wähler immer in der Lage sein muß, gegenüber Dritten risikolos und ohne Gefahr ertappt zu werden, lügen und behaupten zu können, man habe – wie verlangt – den Kandidaten A gewählt, obwohl man in Wirklichkeit den Kandidaten B gewählt hat.

   Daraus folgen die Anforderungen, daß weder ein anderer feststellen kann, wie man gewählt hat, noch daß man selbst es einem anderen nachweisen kann, denn sonst könnte er ja diesen Nachweis verlangen.

   Bingo Voting wird als vollständig „coercion-free“, also erpressungssicher hingestellt.

2. Die Wahl soll unfälschbar sein. Der mathematische Nachweis der Korrektheit soll öffentlich erbracht werden und jeder soll sich anhand der veröffentlichten Daten von der Korrektheit der Wahl überzeugen können, insbesondere indem sich jeder Wähler vergewissern kann, daß seine Stimme korrekt berücksichtigt wurde.

3. Bingo Voting löst nicht das Problem der unsicheren Wahlmaschine, sondern unterstellt sogar, daß man Wahlmaschinen generell nicht sicher bauen kann. Die Autoren reduzieren die Anforderungen dazu explizit darauf, daß nur ein bestimmtes Funktionsteil, nämlich ein Zufallszahlengenerator, aufgrund seiner einfachen Struktur vertrauenswürdig gebaut werden kann und muß.

   Bingo Voting nimmt daher für sich in Anspruch, daß Manipulationen an der Wahlmaschine nicht prinzipiell verhindert, aber in jedem Fall erkannt werden bzw. sich die Öffentlichkeit anhand der veröffentlichten Daten davon überzeugen kann, daß die Maschine *nicht* manipuliert war.

4. Es wird unterstellt, daß der Wähler auf »einfache« Art wählt, also seine Stimme nicht verschlüsselt – etwa mit Hilfe eines eigenen Computers – eingibt, sondern ganz gewöhnlich und einfach an der Wahlmaschine Tasten für die gewählten Kanidaten bzw. Parteien drückt. (Es gibt Wahlverfahren, die mit einer solchen Verschlüsselung arbeiten.)

Wie funktioniert Bingo Voting?

Das Verständnis der Funktionsweise von Bingo Voting setzt erhebliche Kenntnisse in Informatik und Kryptographie voraus. Die Beschreibung kann hier deshalb nur angerissen werden.

Der Leser sollte jedoch verstanden haben, was ein »Commitment« ist. Dabei handelt es sich um eine kryptographische Grundfunktion, die man sich so vorstellen kann, als würde man eine geheime Zahl bei einem Notar hinterlegen, die man bei Bedarf aufdecken kann, und über die man den Nachweis hat, daß man sich schon vorher auf diese Zahl festgelegt, sie also nicht nachträglich verändert hat. Denkt man sich also eine geheime Zahl x aus, kann man einem Dritten das daraus errechnete Commitment $C(x)$ mitteilen. Der Dritte kann daraus nicht feststellen, was x ist, die Zahl x bleibt also vorerst geheim. Trotzdem kann man zu einem späteren Zeitpunkt x aufdecken und beweisen, daß nur x zu diesem vorher mitgeteilten Commitment paßt. Man kann also beweisen, daß man sich das x nicht erst nachträglich ausgesucht, sondern schon vorher festgelegt hatte.

Die Grundidee von Bingo Voting ist, daß man Manipulationen dadurch ausschließt, daß man jede abgegebene Stimme in eine Liste aufnimmt, mit einer eindeutigen Seriennummer versieht und dem Wähler eine Quittungszettel mit der Stimme und der Seriennummer mitgibt. Nach der Wahl veröffentlicht man diese Liste. Jeder Wähler kann sich anhand der Liste und der eindeutigen Seriennummer seiner Wahlabgabe davon überzeugen, daß seine Stimme in der Liste steht. Und weil jeder die Liste selbst nachzählen kann, so die Überlegung, könne auch keine Manipulation stattgefunden haben.

Damit wäre natürlich das Wahlgeheimnis verletzt. Deshalb versucht man, alle Stimmen zu verschlüsseln, indem man sie hinter Commitments versteckt, damit man nicht mehr sehen kann, was Ja- und was Nein-Stimmen sind. Trotzdem kann man später durch einen Trick nachweisen, daß die Stimmen nicht unter der Verschlüsselung manipuliert wurden.

Das Verfahren gliedert sich in vier logische Schritte:

Eine Vorbereitungsphase, in der für jeden Kandidaten so viele »Nein-Stimmen« erzeugt werden, wie es Wähler gibt. Eine solche Stimme besteht aus dem Namen des Kandidaten und einer Zufallszahl. Diese bleiben zunächst geheim. Es werden aber Commitments erzeugt und veröffentlicht, damit diese Stimmen nicht mehr verändert oder ausgetauscht werden können.

Eine Wahlphase, in der jeder Wähler in die Wahlkabine geht und die Taste für den gewünschten Kandidaten drückt.

Die Wahlmaschine entnimmt der Liste der Nein-Stimmen einen Satz Nein-Stimmen, für jeden Kandidaten je eine (wenn man sich die Liste als Tabelle vorstellt, eine Zeile).

Bei dem gewählten Kandidaten wird die Nein-Stimme ausgesondert und in eine separate Liste verschoben, also quasi eine Liste der Wahleingaben erstellt. An die Stelle dieser entnommenen Nein-Stimme wird eine neue Zufallszahl gesetzt, die dem Wähler angezeigt wird. Da sie genau wie die anderen Zufallszahlen aussieht, kann man später nicht mehr erkennen, welches die frisch erzeugte Zufallszahl war, an welcher Stelle der Wähler also eine Ja-Stimme eingegeben hat. Diese neue Zufallszahl übernimmt die Funktion einer eindeutigen Seriennummer für die Stimme.

Auf einer Quittung werden dem Wähler für jeden Kandidaten die entsprechende Zufallszahl gedruckt, bei Ja die neue Zufallszahl, bei Nein die alte. Dadurch soll jeder Wahlquittungszettel eindeutig und einzigartig sein. Die frisch eingesetzte Zufallszahl soll sicherstellen, daß die Stimme eindeutig registriert wurde, aber es soll – außer für den Wähler selbst – nicht ersichtlich sein, welche der Zufallszahlen die Seriennummer darstellt und damit die Ja-Stimme repräsentiert. Man sieht nur eine Liste von Zufallszahlen, für jeden Kandidaten eine.

Eine Ergebnisphase, in der die Maschine nach der Wahl das Ergebnis und die ausgesonderten Ja-Stimmen (also die nicht verwendeten Nein-Stimmen) angibt, indem sie die Commitments aufdeckt, um nachzuweisen, daß von den ursprünglichen Stimmen exakt die für das Wahlergebnis benötigten Stimmen ausgesondert (also als Ja-Stimmen verwendet) wurden.

Außerdem wird eine Liste mit den Kopien all der ausgedruckten Quittungen ausgegeben, anhand derer jeder Wähler mit seiner Quittung vergleichen soll, ob seine Stimme aufgelistet ist.

Eine Nachweisphase, in der nachgewiesen werden soll, daß keine Manipulationen stattfanden.

Dazu wird die ursprüngliche Liste aus Commitments, in der ja nun alle die fehlen, die als Ja-Stimmen ausgesondert wurden, durch neue Commitments aus den als Seriennummern verwendeten neuen Zufallszahlen aufgefüllt. Das wird dann veröffentlicht.

Aus diesen Commitments wird eine zweite Generation von Commitments erzeugt, gemischt und wieder veröffentlicht. Damit kann die Öffentlichkeit nicht sehen, welches Commitment der zweiten Generation welchem der ersten Generation entspricht.

Und dann wird eine weitere, dritte Generation erzeugt, wieder gemischt, wieder veröffentlicht, und sogar aufgedeckt.

Anhand dieser schließlich aufgedeckten Paare (Kandidatenname und Zufallszahl) kann man nun vergleichen, ob diese von der Anzahl her stimmen, nämlich für jeden Kandidaten gleich viele, und zwar so viele wie es Wähler gibt, und daß sie mit den veröffentlichten Quittungen übereinstimmen. Man soll daran aber nicht mehr erkennen können, was eine alte Nein-Stimme und was eine während der Wahl erzeugte Seriennummer ist.

Nun könnten die Zufallszahlen ja generell in der Maschine ausgetauscht worden sein. Um deren Echtheit zu beweisen, müßte man die ursprünglichen Commitments aufdecken. Damit wäre aber das Wahlgeheimnis verletzt, weil jeder sehen könnte, was alte Nein-Stimmen und was frische Seriennummern sind (die ja an Stelle von Ja-Stimmen stehen).

Deshalb wird für jede dieser Zahlen zufällig nur die Übereinstimmung zwischen der ersten und der zweiten oder der zweiten und der dritten Generation von Commitments nachgewiesen. Damit hat jede einzelne Manipulation eine Wahrscheinlichkeit von 50%, erkannt zu werden. Stimmt etwas nicht, ist die Wahl ungültig. Da man für jede Manipulation ja mehrere Stimmen verändern müßte und bei zehn Veränderungen die Nichtentdeckungsquote schon 1:1024 wäre, geht man davon aus, daß jede Veränderung detektiert wird.

Die weitere Überlegung ist, daß niemand das Wahlgeheimnis brechen kann, weil man ja nur an der ersten Generation von Commitments sehen kann, was alte Nein-Stimmen und was neue Serien-Nummern an Stelle der Ja-Stimmen sind, es aber nie eine Aufdeckung über alle drei Generationen hinweg gibt.

Grundsätzliche Kritik und Funktionstauglichkeit

Widersprüchliche und fehlerhafte Voraussetzungen

Die Ziele, die Bingo Voting sich setzt und erfüllt zu haben für sich in Anspruch nimmt, sind in sich widersprüchlich und so nicht gegeben und nicht erfüllbar. Das merken auch die Autoren selbst, indem sie sich selbst widersprechen.

Zum einen nimmt man an, daß nur der Zufallszahlengenerator vertrauenswürdig zu bauen ist und schreibt das auch in den Titel der Veröffentlichung. Und nur daraus ergibt sich die Daseinsberechtigung für ein solches Verfahren, denn wäre die Wahlmaschine vertrauenswürdig, wäre ein kryptographisches Verfahren überflüssig, da würde ein einfacher Zähler in der Wahlmaschine

genügen. Der Ruf nach besseren Verfahren basiert ja nur auf der Befürchtung, daß die Maschine manipuliert sein könnte.

In dem Moment, in dem man aber seine Stimme abgibt, indem man an einem nicht vertrauenwürdigen Computer Tasten drückt, ist das Wahlgeheimnis schon kompromittiert, denn der Computer kann das bereits aufgezeichnet haben. Jedes weitere kryptographische Verfahren zur Geheimhaltung ist dann nur noch Hokus-Pokus, ein Hütchenspielertrick. Und dazu steht im Paper an unauffälliger Stelle der kurze Satz

> ***„The voting machine reorders the votes and has to be trusted in order to guarantee anonymity.“***

Das heißt, daß die Autoren schon selbst von anderen Voraussetzungen ausgehen, als sie oben angeben, nämlich daß die Maschine vertrauenswürdig sei. Wenn man das voraussetzen muß, braucht man aber kein kryptographisches Verfahren. Auf der anderen Seite wollen sie mit dem Korrektheitsnachweis erkennen, ob die Maschine manipuliert war, sie also doch als nicht vertrauenswürdig angesehen wird. Damit ist bereits der Titel des Papers „Bingo Voting: Secure and coercion-free voting using a trusted random number generator“ unrichtig, weil secure und coercion-free auf unterschiedlichen, sich ausschließenden Annahmen beruhen.

Welchem Zweck dient ein kryptographisches Wahlverfahren, wenn man dafür voraussetzt, daß die Wahlmaschine vertrauenswürdig sein muß?

Konstrukt des Wahlleiters

Die Autoren unterstellen außerdem mehr oder weniger stillschweigend, daß es einen vertrauenswürdigen Wahlleiter gibt, der die verschiedenen Protokollschritte abarbeitet. An anderer Stelle gibt es sogar explizite Äußerungen der Autoren, daß man dem Wahlleiter durchaus trauen müßte, wie man sich auch bei einer Papierwahl darauf verlassen können müßte, daß keine Überwachungskameras installiert worden seien. Derartige Äußerungen deuten stark darauf hin, daß den Autoren schon selbst bewußt ist, daß ihr Verfahren die versprochenen Eigenschaften nicht aufweist.

Wenn man fordert, daß dem Wahlleiter zu vertrauen ist, welches Problem löst dann Bingo Voting? Und woher kommt die Annahme, daß der Wahlleiter vertrauenswürdig wäre? Ist er das nämlich nicht, bietet Bingo Voting erheblich weitergehende Angriffsmöglichkeiten als eine Papierwahl.

Kryptographische Grundsätze mißachtet

Ein schwerer Konstruktionsfehler des Verfahrens ist, daß *sämtliche* kryptographischen Geheimnisse an einer einzigen Stelle, nämlich in der Maschine und beim Wahlleiter liegen, und der damit das gesamte Protokoll und damit das Wahlgeheimnis aufdecken kann. Es gibt im Protokoll keine zweite Stelle, an der Geheimnisse abgelegt werden, oder Geheimnisse, die vernichtet werden.

Das heißt, das gesamte Wahlgeheimnis hängt davon ab, der Maschine und dem Wahlleiter zu vertrauen, während die Korrektheitsbeweise von Bingo darauf beruhen, daß man ihm *nicht* vertraut.

Kollisionen der Zufallszahlen

Bingo Voting beruht auf Zufallszahlen. Generell kann man in der Kryptographie Zufallszahlen als beliebig oder hinreichend lang unterstellen, so daß man gewisse unangenehme Effekte, nämlich

daß eine Zufallszahl zufällig später noch einmal gezogen wird, gewohnheitsmäßig vernachlässigt und nicht betrachtet. Die Autoren unterstellen einfach stillschweigend, daß jede Zahl von Natur aus nur einmal gezogen wird. Hier erweist sich das aber als verhängnisvoll.

Die Zufallszahlen können hier nämlich nicht beliebig lang werden. Es wird gefordert, daß der Wähler – und damit auch alte, gebrechliche Leute, bequemlich-faule Zeitgenossen, Analphabeten und einfach strukturierte Gemüter – sorgfältig überprüfen müssen, ob eine Zufallszahl auf ihrem Quittungszettel mit einer Anzeige auf einem Zufallszahlengenerator übereinstimmt. Und damit sind Grenzen gesetzt, bis zu welcher Länge dies der Bevölkerung zumutbar ist und ernsthaft geprüft würde.

Die Autoren selbst unterstellen, daß man dies bis zu einer Länge von 40 Bit, also einer Zahl mit etwa 13 Stellen (oder eine Hexadezimalzahl mit 10 Stellen) zumuten könnte.

Das genügt nicht. Spätestens bei einer Wahl in der Größenordnung einer normalen Bundestagswahl kommt es mit hoher Wahrscheinlichkeit dazu, daß Zufallszahlen doppelt gezogen werden, ohne daß man dies verhindern könnte.

Die Folgen wären subtil und paradox: Taucht in dem späteren Korrektheitsbeweis oder in der veröffentlichten Liste dieselbe Zahl zweimal auf, müßte man zwangsläufig von einer Manipulation ausgehen und die Wahl für ungültig erklären, obwohl eine Manipulation nicht stattgefunden hat und die doppelt auftauchende Zahl nur eine Folge statistischer Schwächen des Verfahrens ist. Kurioserweise bietet eine solcher Fall, in dem eine Zufallszahl doppelt gezogen wird, der Maschine die Möglichkeit, *eine Stimme zu fälschen*. Das würde sich zwar kaum auf das Wahlergebnis auswirken, würde aber dann zu einem Ergebnis führen, das als korrekt angezeigt würde. Es läge also die paradoxe Situation vor, daß eine nicht manipulierte Wahl als manipuliert angezeigt würde, während eine manipulierte Wahl als korrekt bewiesen würde.

Es zeigt, daß der Nachweis nicht korrekt ist und das Protokoll damit nicht so wie versprochen funktioniert. Es zeigt außerdem, daß das Verfahren schon im Normalbetrieb ohne Manipulationen Funktionsstörungen aufweist und ordnungsgemäß abgelaufene Wahlen trotzdem wiederholt werden müßten. Ein Wahlverfahren, das auch fehlerfrei abgelaufene Wahlen angreifbar macht und zur Wahlwiederholung führt, ist aber aus rechtlichen Gründen nicht verwendbar.

Man müßte die Zufallszahlen also erheblich länger machen. Schon bei den von den Autoren angegebenen 40 Bit (bzw. 13 Stellen) dürfte aber zweifelhaft sein, ob ein hinreichend großer Bevölkerungsteil sich die Mühe macht, dies zu überprüfen.

Nachträgliche Sabotage – Denial of Service

Die Autoren unterstellen fehlerhaft ein gewisses Wohlverhalten der beteiligten Wähler und des Wahlleiters bzw. der Wahlmaschine. Zweck eines kryptographischen Protokolls und erklärte Eigenschaft von Bingo Voting soll aber gerade sein, gegen *Fehlverhalten und Angriffe* zu schützen. Also kann man nicht unterstellen, daß alle brav mitspielen.

Ein Konstruktionsfehler von Bingo Voting liegt darin, daß nach der Veröffentlichung des Wahlergebnisses noch eine Beweisphase anschließt, von der abhängt, ob man die Wahl als korrekt ansieht oder nicht.

Das ermöglicht eine eigene Art von Angriff: Man könnte die Wahl zunächst normal ablaufen lassen ohne sie zu manipulieren, und abwarten, ob das erwünschte Ergebnis herauskommt. Entspricht das Ergebnis nicht den eigenen Ewartungen, kann man *nach der Wahl* den Korrektheitsbeweis angreifen und so eine Wiederholung einer als manipuliert anzusehenden Wahl erzwingen.

Nachträgliche Sabotage durch Maschine/Wahlleiter

Bingo Voting will auch gegen den Fall schützen, daß der Wahlleiter manipuliert oder die Maschine selbst manipuliert ist. Gerade dagegen ist Bingo Voting aber anfällig.

Nach der Wahl muß die Wahlmaschine die Korrektheit der Wahl nachweisen, indem sie die drei Commitment-Generationen erzeugt, die dritte Generation aufdeckt und in Abhängigkeit von einer Zufallsbitfolge für jede Stimme entweder die Übereinstimmung zwischen erster und zweiter oder zwischen zweiter und dritter Generation nachweisen. Dann kann die Öffentlichkeit nachrechnen und wenn alles stimmt, dann wird die Wahl als korrekt angesehen. Halten die veröffentlichten Daten einer Nachrechnung aber nicht stand, geht man davon aus, daß die Wahl nicht korrekt war und wiederholt werden muß.

Gefällt einem Angreifer das Wahlergebnis nicht, könnte er also einfach gezielt fehlerhafte Zahlen ausgeben und einfach abwarten, daß irgendwer in der Öffentlichkeit oder ein Komplize erkennt, daß die Zahlen nicht stimmen, und eine Wiederholung der Wahl einklagt.

Nachträgliche Sabotage durch Wähler

Auch ein Wähler könnte eine Wahl mit einem ihm unangenehmen Ergebnis nachträglich sabotieren. Er könnte eine Wahlquittung fälschen oder seine Wahlquittung verfälschen und dann behaupten, die Wahl sei manipuliert worden, weil die Zahlen auf seiner Quittung nicht – wie notwendig – auf der veröffentlichten Liste auftauchen.

Die Spezifikation der Autoren geht ausdrücklich nur davon aus, daß der Zufallszahlengenerator selbst nicht manipulierbar ist. Von fälschungssicheren Wahlquittungen ist nicht die Rede. Selbst wenn man unterstellt, daß man Quittungen fälschungssicher gestalten würde, ergeben sich Widersprüche.

Von fälschungssicherem Papier und ähnlichem darf man nicht ausgehen, denn es war ja gerade die Voraussetzung – und wurde von einem der Autoren vor dem Bundesverfassungsgericht auch so darstellt – daß schon die Versiegelung von Wahlmaschinen nicht fälschungssicher durchzuführen ist. Solche Siegel seien genauso leicht wie Geld zu fälschen, was vom Bundesverfassungsgericht als bekanntlich leicht eingestuft wurde. Man kann nicht einerseits behaupten, daß man Bingo Voting bräuchte, weil man Wahlmaschinen nicht fälschungssicher versiegeln kann, und dann andererseits fordern, daß die ausgedruckten Wahlquittungen fälschungssicher sind.

Auch digitale Signaturen helfen hier nicht weiter, denn im Falle einer Manipulation der Maschine wäre der Angreifer ja gerade nicht daran interessiert, korrekte Signaturen auszustellen. Der Wähler kann diese auch nicht an Ort und Stelle verifizieren und sich sofort beschweren. Also könnte eine manipulierte Wahlmaschine dem Wähler auf die Quittung drucken, was er tatsächlich gewählt hat, damit er zufrieden ist, dies aber falsch signieren. Intern registriert die Maschine eine andere Wahl. Zwar würde der Wähler dies später bemerken und sich beschweren, weil aber die Signatur auf seiner Quittung nicht stimmt, würde er selbst als Fälscher dastehen. Im Ergebnis würde Bingo Voting dann nicht die Manipulation aufdecken, sondern im Gegenteil den diskreditieren, der sich über die Manipulation beschwert. Das würde Bürger sogar davon abhalten, sich zu beschweren.

Andererseits wäre die Frage, was denn wäre, wenn ein Wähler sich mit einer gefälschten Quittung und falscher Signatur beschwert. Würde man die Quittung als gefälscht ansehen oder würde man umgekehrt aus der falschen Signatur auf eine Manipulation der Wahlmaschine schließen?

Läßt man die Fälschungssicherheit der Wahlquittungen aber – wie auch von den Autoren – völlig unter den Tisch fallen, dann herrscht Chaos, weil man dann davon ausgehen muß, daß die üblichen Spaßvögel, Hacker und Querulanten, aber auch protestierende Normalbürger den von den

Autoren vorgeschlagenen Wahlprüfungsvereinen in größeren Mengen gefälschte Quittungszettel zuspielen würden. Selbst wenn man wüßte, daß darunter viele Fälschungen sind, würde es die Überprüfung der echten Quittungen vereiteln und Bingo Voting damit im Kern angreifen.

Ein Angreifer könnte dies ausnutzen, indem er das Wahlergebnis verfälscht und dann eine größere Anzahl falscher Quittungen in die Wahlprüfungsvereine sendet, um die Nachprüfung zu verhindern und auch die echten Quittungen, die die Manipulationen aufdecken könnten, unglaubwürdig zu machen.

Angriffe gegen das Wahlgeheimnis

Verstoß gegen Grenzen des Wahlgeheimnisses

Ein Wahlgeheimnis ist in der Konsequenz und Perfektheit, wie Bingo Voting sie für sich in Anspruch nimmt, nicht möglich, und zwar schon aus grundsätzlichen Erwägungen. Betrachten wir »pathologische« Randfälle:

- Gibt es nur einen Wähler, dann stimmt das Wahlergebnis direkt mit seiner Wahl überein. Kein Wahlgeheimnis.
- Verzichten alle Wähler bis auf einen auf ihr Wahlgeheimnis und legen ihre Stimmen offen, ist auch der letzte Wähler „angeschmiert“, seine Wahl offengelegt.
- Erhält ein Kandidat 0 Stimmen, dann wissen alle, daß man diesen Kandidaten nicht gewählt hat, und man kann es auch nachweisen.
- Gibt es mehr Kandidaten als Wähler, dann gibt es notwendigerweise auch Kandidaten, die keine Stimmen erhalten, also ist aus obigem Grund die Anforderung des Wahlgeheimnisses und des »coercion-free« von vornherein nicht erfüllbar.
- Bekommt ein Kandidat alle Stimmen, dann ist ebenfalls bekannt, wie die Wähler gestimmt haben.
- Bekommt ein Kandidat nur eine Stimme oder alle Stimmen bis auf eine, dann weiß der, der abweichend gewählt hat, wie die anderen Wähler gewählt haben.
- Verzichten alle Wähler, die einen Kandidaten gewählt haben, oder die ihn nicht gewählt haben, auf ihr Wahlgeheimnis, dann ist auch bekannt, was die anderen Wähler gewählt oder nicht gewählt haben.

Das kann gefährlich werden. Stellen wir uns vor, man würde vor der Wahl erpresst. Jemand drohte mit einem Übel, wenn man nicht den Kandidaten A wählte. Man geht also zur Wahl, vertraut auf die angebliche Eigenschaft von Bingo Voting, daß es »coercion-free« sei, wählt B, kommt wieder heraus, und behauptet, man hätte A gewählt. Dann wird das Wahlergebnis bekannt gegeben und A hat überraschend 0 Stimmen bekommen. Der Erpresser weiß dann sofort, daß man gelogen hat.

Das Wahlgeheimnis hat also schon in sich natürliche Grenzen, die auch ein Wahlprotokoll nicht überschreiten kann. Behauptet jemand – so wie hier Bingo Voting – dennoch, ein perfektes Wahlgeheimnis bis hin zu »coercion-free« erreicht zu haben, kann daran etwas nicht stimmen. Der Beweis muß falsch sein.

Kein Wahlgeheimnis – ein Hütchenspielertrick

Besonders frappierend an Bingo Voting ist, das man es nicht einmal angreifen muß. Ein Wahlgeheimnis wird erst gar nicht hergestellt, das behaupten die Autoren nur.

Wie oben beschrieben beruht Bingo Voting auf der Annahme und Voraussetzung, daß die Wahlmaschine nicht vertrauenswürdig ist, darin liegen Anspruch und Daseinsberechtigung von Bingo Voting. Weiter wird angenommen, daß der Wähler seine Wahl nicht verschlüsselt eingibt, sondern Oma-tauglich direkt an einer Tastatur der Wahlmaschine die Tasten für die gewählten Kandidaten drückt.

Wir haben gerade, noch bevor irgendetwas kryptographisch passiert ist, die Wahl einer nicht vertrauenswürdigen Maschine offenbart, das Wahlgeheimnis ist schon mit Drücken der Taste gebrochen. Alles, was danach noch an Krypto-Hokus-Pokus passiert, ist nur noch Augenwischerei und Blendwerk.

Es wird unterstellt, daß die Wahlmaschine einen Computer enthält bzw. nicht vertrauenswürdig ist, man also einen entsprechenden Computer einbauen könnte. Und damit kann die Maschine speichern, in welcher Reihenfolge die Kandidaten über den Wahltag hinweg abgegeben werden. Und das wäre noch nicht einmal eine Manipulation, denn das tut sie ja sowieso durch Aussonderung und Auflistung der Ja-Stimmen. Selbst wenn man die Maschine genau analysierte, wäre dies nicht einmal als Manipulation erkennbar sondern würde als normale Funktionalität erscheinen. »Dual-Use«, sozusagen.

Die Autoren geben schon in gewisser Weise selbst zu, daß Bingo Voting dahingehend nicht funktioniert, wenn sie schreiben

> ***„The voting machine reorders the votes and has to be trusted in order to guarantee anonymity.“***

Darin liegt aber nur eine substanzlose Phrase, denn es ist nicht klar, wo genau da noch die Eigenschaften liegen, unter denen man die Maschine noch als „trusted“ ansehen würde und wo die Manipulation anfängt. Die Autoren spezifizieren an keiner Stelle, welche Eigenschaften die Wahlmaschine haben und was sie tun muß, um das Wahlgeheimnis zu bewahren. Die Maschine soll einfach „trusted“ sein, ohne daß ersichtlich würde, welche Eigenschaften da „trusted“ sein sollen. Wäre eine Maschine, die die ausgesonderten Stimmen in der richtigen Reihenfolge speichert und damit das Wahlgeheimnis verletzt, noch „trusted“? Wogegen würde sie denn verstoßen? So gesehen wäre nicht einmal die von den Autoren selbst vorgenommene Implementierung zur Studentenwahl der Universität Karlsruhe als „trusted“ anzusehen, denn diese hatte eine Hintertür und speicherte versteckt die Uhrzeiten mit ab.

Wie die Autoren in ihrem Paper aber selbst schreiben, fehlen Bingo Voting zwei ganz wichtige Sicherheitseigenschaften:

- Es verhindert bei einer Wahlbeteiligung unter 100% nicht, daß die nicht genutzten Wahlstimmen durch Unbefugte verwendet werden, die also quasi an Stelle der nicht erschienenen Wähler stimmen.
- Es verhindert nicht die mehrfache Stimmabgabe, daß also ein Wähler mehrfach zur Wahl erscheint.

Deshalb schreiben die Autoren, daß neben Bingo Voting noch das herkömmliche Wahlbuch verwendet werden muß, mittels dessen geprüft wird, wer überhaupt Wähler ist und wer schon gewählt hat. Das Wahlbuch wird damit implizit aber ohne Erwähnung im Protokoll zum Teil des Wahlverfahrens. Im Wahlbuch wird bei herkömmlichen Papierwahlen abgehakt, welche Wähler schon gewählt haben, um zu verhindern, dass Wähler mehrfach ihre Stimme abgeben. Ein Angreifer im Wahlbüro kann leicht zusätzlich die Uhrzeit oder auch nur die Reihenfolge der Stimmabgabe aufzeichnen. Bei klassischen Papierwahlen stellt das kein Problem dar, weil die Stimmen in der Urne schon während der Stimmabgabe und beim Ausschütten der Urne vor der Auszählung hinreichend durchmischt werden, so dass eine Zuordnung einzelner Stimmen zu einzelnen Wählern anhand der Uhrzeit der Stimmabgabe oder auch nur anhand der Reihenfolge in der Urne nicht möglich ist. Bei Bingo Voting kann die Liste der Wahlzeitpunkte oder der Wahlreihenfolge zusammen mit einer koompromittierten Wahlmaschine genutzt werden, um das Wahlgeheimnis aufzudecken.

Selbst ohne Wahlbuch wäre das aufzuklären, denn der fundamentale Entwurfsfehler ist, daß es kein Geheimnis gegenüber der Maschine gibt. Die Maschine weiß alles, kennt alle Geheimnisse, und das obwohl sie nicht vertrauenswürdig ist. Sogar dann, wenn die Maschine überhaupt nicht manipuliert ist, und somit auch kein Rechtsmittel helfen würde, kann der, der die Maschine ausliest, an sämtliche geheimen Zufallszahlen und die Commitments kommen und damit sofort zu jedem Wahlquittungszettel anhand der Zahlen darauf sagen, für welchen Kandidaten gestimmt wurde. Man kann also jeden Wähler (auch mit Gewalt oder heimlichen Wohnungsdurchsuchungen) nach seinem Zettel fragen und sofort erkennen, was er gewählt hat, bzw. ihn zum Nachweis der gewünschten Wahl durch Vorlage seines Zettels zwingen.

Eine Maschine kann nicht „trusted“ sein, solange nicht spezifiziert ist, welche Eigenschaften sie dazu haben muß, und solange man unter der Flagge segelt, daß nur der Zufallszahlengenerator „trusted“ sein müsse.

Faule Permutationen

Bingo Voting versucht, die Korrektheit der Wahl nach Veröffentlichung des Wahlergebnisses nachzuweisen, ohne dabei das Wahlgeheimnis zu verletzten. Dazu werden drei Generationen von Commitments für jede Stimme erzeugt und nach zufälligen Mustern Übereinstimmungen nachgewiesen, so daß jede Manipulation mit gewisser Wahrscheinlichkeit erkannt würde. Auf die kryptographischen Einzelheiten wird hier nicht eingegangen.

Damit das Wahlgeheimnis aber nicht auf triviale Weise über deren Reihenfolge gebrochen werden kann, müssen für jede Generation der Commitments deren Reihenfolge geändert und die Stimmen neu gemischt werden. Es besteht aber keinerlei Möglichkeiten nachzuprüfen, ob diese Permutationen wirklich zufällig und geheim ablaufen. Es kann auch keine Wahlbeobachter geben, weil diesen gegenüber damit das Wahlgeheimnis ebenfalls offenbart wäre. Damit aber könnte die Permutation nach vorher abgesprochenen Regeln erfolgen und damit ein Dritter ohne weitere Kommunikation allein anhand der veröffentlichten Daten das Wahlgeheimnis brechen.

Unklar läßt das Paper, wer diese Permutationen eigentlich ausführen soll. Sie fallen quasi vom Himmel.

Faule Commitments

Ein ähnlicher Angriff ist auch über die verwendeten Commitments möglich. Die Commitments sollen sicherstellen, daß man sich im Protokoll auf bestimmte Stimmen festlegt, ohne diese aber zu offenbaren. Man veröffentlicht sie, um eine Veränderung auszuschließen, gleichzeitig aber die Stimmen geheim zu halten.

Zur Berechnung der Commitments müssen weitere Zufallszahlen verwendet werden. Auch hier besteht keinerlei Möglichkeit nachzuweisen, daß diese wirklich ohne Manipulation gezogen wurden. Währen auch diese vorher abgesprochen könnte auch hier ein Dritter das Wahlgeheimnis anhand der veröffentlichten Daten aufdecken.

Auch zu den Commitments ist nicht ersichtlich, wer oder welche vertrauenswürdige Stelle sie ausführen soll. Auch sie fallen vom Himmel.

Ausrechnen der abgegebenen Stimmen

Bingo Voting steht in dem Dilemma, daß es einerseits die Stimmen geheim halten will, andererseits nachweisen muß, daß die Stimmen innerhalb der Wahlmaschine nicht verändert wurden.

Dazu wendet Bingo Voting einen kryptographischen Trick an, ein von anderen entwickeltes Verfahren namens „Randomized Partial Checking“. Dazu werden zu den Stimmen jeweils drei Commitments erzeugt, und diese in ihrer Reihenfolge gemischt. Von dem ersten Commitment weiß man, welches Ja- und vor der Wahl erzeugte Nein-Stimmen sind. Das dritte Commitment wird aufgedeckt, um nachzuweisen, daß die Zufallszahlen mit den Stimmquittungen übereinstimmen. Würde man den direkten Zusammenhang nachweisen, wäre das Wahlgeheimnis verletzt.

Also weist man für jede Stimme nur entweder die Übereinstimmung zwischen erstem und zweitem oder zwischen zweitem und drittem Commitment nach. Damit wird jede einzelne Manipulation mit einer Chance von 50% erkannt, während – so die Autoren – das Wahlgeheimnis trotzdem vollständig gewahrt bleibt, weil nie ein durchgehender Zusammenhang zwischen erstem und drittem Commitment offengelegt wird.

Das ist so aber nicht richtig. Die Autoren haben übersehen, daß sie hier eine etwas andere Problemstellung haben als die, für die diese Technik entwickelt wurde. Der Angreifer muß gar nicht alle Zusammenhänge zwischen den Stimmen exakt kennen, um das Wahlgeheimnis aufzudecken.

Der Angreifer sieht, welche der Stimmen im ersten Commitment Ja- und Nein-Stimmen sind. Fällt die zufällige Auswahl so aus, daß alle Ja- oder alle Nein-Stimmen zwischen dem ersten und dem zweiten Commitment auf Übereinstimmung geprüft werden (oder kann er fehlende Informationen durch Kooperation mit Wählern offenlegen), dann kann der Angreifer auch das zweite Commitment nach Ja- und Nein-Stimmen aufklären. Es ist dabei nicht notwendig zu erkennen, um welche Ja- und Nein-Stimme es sich handelt. Es genügt schon die Information, ob Ja oder Nein. Und damit kann dann auch ein Teil des dritten Commitments aufgeklärt werden, über Abzählen dann weitere Teile des dritten Commitments. Da das dritte Commitments aber aufgedeckt ist, wird daraus auch erkennbar, welche Zufallszahlen Ja- und Nein-Stimmen sind. Das Wahlgeheimnis ist in diesem Fall gebrochen.

Zwar ist dies ein eher theoretischer Angriff, weil die Wahrscheinlichkeit, daß die Aufdeckung zufällig gelingt, mit steigender Zahl von Wählern und Kandidaten rapide sinkt. Es zeigt aber, daß das Verfahren Konstruktionsfehler hat, daß es die angebliche Eigenschaft 100%-iger Sicherheit nicht erfüllt und daß die angeblichen Beweise für die Sicherheit nicht zutreffen können.

Es zeigt auch, daß die Autoren ihr eigenes Verfahren weit überschätzen und sich der Konsequenzen ihrer Vorgehensweise nicht bewußt sind.

Angriffe gegen die Wahlkorrektheit

Erpressung

Geradezu bösartig an Bingo Voting ist, daß es zwar behauptet, »coercion-free«, also erpressungssicher zu sein, aber das Gegenteil erreicht, nämlich durch die Wahlquittungszettel die Erpressbarkeit erst herstellt. Plötzlich muß der Wähler einem Erpresser gegenüber eine opportune Wahl durch Vorlage des Zettels nachweisen.

Der wesentliche Konstruktionsfehler liegt darin, daß Bingo Voting zwar behauptet, es könne Manipulationen an der Wahlmaschine erkennen, dies tatsächlich aber nur für eine begrenzte Sorte von Manipulationen leistet. Manipulationen, die sich gegen das Wahlgeheimnis richten, auch das nachträgliche Auslesen der Maschine, werden von Bingo Voting überhaupt nicht erkannt. Der Wähler muß also nicht nur befürchten, daß das Wahlgeheimnis verletzt wird, er muß sogar davon ausgehen, denn der Einsatz von Bingo Voting beruht ja gerade auf der Annahme einer noch stärkeren Kompromittierung, nämlich der versuchten Manipulation des Wahlergebnisses.

In dem Moment, in dem der Wähler aber die Verletzung des Wahlgeheimnisses befürchten muß oder sich jedenfalls nicht davon vergewissern kann, daß dies nicht der Fall ist, ist er erpressbar. Dabei würde ich folgende Arten der Erpressung unterscheiden:

Erpressung erster Ordnung: Der Erpresser kann die Wahlzettel tatsächlich aufdecken, weil er Zugang zur Maschine hat oder einen der oben vorgestellten Angriffe durchführt, und straft nach der Wahl jeden ab, der nicht wie erwartet gewählt hat.

Erpressung zweiter Ordnung: Der Erpresser täuscht eine Erpressung erster Ordnung vor. Er läßt sich von den Wählern deren Zettel zeigen und behauptet einfach willkürlich mit einer Quote, die dem Wahlergebnis entspricht, die Wähler hatten anders als gefordert gestimmt, egal ob es stimmt oder nicht, und bestraft sie öffentlich. Man unterstellt ihnen einfach, sie hätten unerwünscht gewählt und behauptet einfach, dies ginge aus den Zetteln (oder deren Fehlen) hervor. Der Wähler kann das ja kraft Protokollkonstruktion nicht widerlegen, falls er doch opportun gewählt hat. Hinreichend Angst und Schrecken sind gewiss.

Erpressung dritter Ordnung: Der Erpresser behauptet gegenüber dem Wähler vor der Wahl, er könnte die Wahlzettel aufdecken, obwohl er es nicht kann. Weil das Verfahren so viele Schwächen hat, daß der Wähler sich nie sicher sein kann und sich – entgegen der Behauptung der Autoren – überhaupt nicht davon überzeugen kann, daß das Wahlgeheimnis gewahrt ist, muß der Wähler zumindest annehmen oder befürchten, daß der Erpresser dies könnte, insbesondere wenn es sich um staatliche Erpresser handelt.

Aufgrund der Protokollschwächen wirkt die Erpressung also auch dann, wenn der Erpresser gar nichts kann und sich auch nie wieder blicken läßt.

Erpressung vierter Ordnung: Der Erpresser behauptet gegenüber dem Wähler vor der Wahl, die Wahlquittungszettel wären nicht verschlüsselt, sondern die Zahlen würden direkt sagen, was der Wähler gewählt hat. Das ist zwar falsch, aber für die meisten Wähler nicht erkennbar, das Verständnis des Verfahrens überfordert schon die meisten Informatiker.

Im Ergebnis wird letztlich ein einfaches Einfordern des Wahlquittungszettels für hinreichende Erpressungswirkung sorgen, weil der Wähler überhaupt nicht abschätzen kann, wie weit das Wahlgeheimnis kompromittiert ist.

Kollisionen der Zufallszahlen

Oben auf Seite 5 habe ich erwähnt, daß es zu Kollisionen der Zufallszahlen kommen kann, denn der Zufallszahlengenerator hat ja kein Gedächtnis, um einmal verwendete Zahlen auszuschließen.

Die Begrenzung der Zufallszahlen auf 40 Bit führt bei einer Wahl mit realistischen Maßstäben fast zwangsläufig zu Kollisionen, die meist wie eine Manipulation aussehen könnten und zur Ungültigkeit der Wahl führen.

Haben aber zwei Wähler zufällig dieselbe Zufallszahl und haben sie denselben Kanidaten gewählt, könnte die Maschine dem zweiten Wähler eine identische Kopie des Quittungszettels des ersten Wählers audrucken. Solange die beiden nicht zufällig aufeinandertreffen oder ihre Zettel demselben Wahlprüfungsverein gegeben, würde das nicht bemerkt. Die Maschine hat also eine Wahl frei und kann unerkannt selbst an Stelle des zweiten Wählers wählen.

Das ist zwar zugegebenermaßen relativ unwahrscheinlich und würde nur wenige Stimmen betreffen, aber die könnten es ja gerade ausmachen. Und damit ist widerlegt, daß das Protokoll beweist, daß die Wahl korrekt abgelaufen ist. Der Beweis stimmt nicht.

Die Papierkorb-Methode

Der von den Autoren unterstellte Beweis der Korrektheit der Wahl beruht auf einer Annahme, die nicht haltbar und realitätsfern ist. Sie unterstellt, daß *jeder Wähler* nach der Wahl die Zahlen auf seiner Wahlquittung mit der veröffentlichten Liste auf Übereinstimmung prüft. In der Realität werden aber eine signifikant hohe Zahl von Bürgern dazu nicht in der Lage sein oder dies aus anderen Gründen nicht tun.

Sobald der Angreifer aber Kenntnis davon erlangt, *welche* der Wahlquittungen nicht überprüft werden, weiß er – aufgrund der Konstruktion mit den Seriennummern – sofort, welche Stimmen er risikolos und unerkannt manipulieren kann.

Dazu bieten sich Methoden des Human Engineering an. Man könnte vor das Wahlbüro einfach einen Papierkorb aufstellen, was mit ziemlicher Sicherheit dazu führen wird, daß manche Wähler ihren Wahlquittungszettel direkt da reinwerfen. Der Angreifer muß die Zettel nur entnehmen und weiß sofort, welche Stimmen er manipulieren kann ohne daß dies später erkennbar oder gar nachweisbar wäre.

Alternativ könnte man auch – wie sogar von den Autoren selbst vorgeschlagen – einen »Briefkasten« eines Wahlprüfungsvereins oder Partei zur vorgeblichen Nachprüfung der Stimmen aufhängen, was ebenfalls die gewünschte Angriffswirkung hätte.

Man-in-the-Middle-Attacke durch Skimming

Bingo Voting ist anfällig gegen einen Standard-Angriff der Kryptographie, die sogenannte »Man-in-the-Middle-Attacke«, bei der sich ein Angreifer in die Kommunikation einschaltet. Durchführen könnte man dies etwa durch ein sogenanntes Skimming. Darunter versteht man die bei Geldautomaten immer öfter angewandete Technik, die Bedienungselemente durch täuschend echte Attrappen zu überkleben, die dann die PIN-Eingabe abfangen und den Magnetstreifen der Scheckkarte mitlesen.

Der Konstruktionsfehler der Autoren besteht in der Annahme, daß ein vertrauenswürdiger Zufallszahlengenerator auch eine Anzeige haben muß, die man vertrauenswürdig ablesen kann. Der Mensch hat aber keine kryptographisch vertrauenswürdigen Sinnesorgane, wie die Vielzahl von Angriffen auch im Internet nachhaltig belegen.

Würde ein Angreifer es schaffen, etwa morgens durch den ersten Wähler, die Wahltastatur, den Ausgabeschlitz für die Wahlquittung und die Anzeige des Zufallszahlengenerators zu überkleben, oder die Software manipulieren und nur die Anzeige überkleben, könnte er das Wahlergebnis beliebig verändern, ohne daß dies nachträglich zu erkennen wäre.

Die Lücke besteht darin, daß bei Bingo Voting die als Seriennummern fungierenden Zufallszahlen konstruktionsbedingt nicht von den als Nein-Stimmen fungierenden Zufallszahlen zu unterscheiden sind. Würde der Wähler den Kandidaten A wählen, könnte sich die Maschine so verhalten, als hätte er den Kandidaten B gewählt und eine entsprechende Quittung ausdrucken. Kann der Angreifer dabei die Anzeige der Zufallszahl durch eine überklebte zweite Anzeige so verändern, daß er statt der frischen Zufallszahl für B die alte Nein-Stimme für A anzeigt, kann der Wähler dies nicht erkennen.

Der Wähler muß glauben, daß seine Stimme korrekt und fehlerfrei gezählt wurde und würde dies anhand seiner Quittung und der später veröffentlichten Daten auch weiter glauben und behaupten, er habe sich von der Richtigkeit der Wahl überzeugt. Auch bei einer kompletten Aufdeckung des Wahlgeheimnisses wäre der Angriff erst dann nachweisbar, wenn der Wähler andere Beweise vorbringen könnte, daß er A und nicht B gewählt hat, was er laut Konstruktion von Bingo Voting aber gerade nicht können soll.

Bingo Voting nimmt für sich in Anspruch, Manipulationen des Wahlergebnisses *nachträglich* erkennen zu können. Das ist hier nicht der Fall.

Hintertüren in der Implementierung

Anfang 2008 wurde an der Universität Karlsruhe eine Studentenparlamentswahl mit einer prototypischen Implementierung von Bingo Voting durchgeführt. Als Argument gegenüber den bisher üblichen Wahlverfahren wurde vorgebracht, daß diese das Wahlgeheimnis nicht hinreichend schützten.

Soweit bisher aus den teilweise offengelegten Quelltexten hervor geht, hatte die Implementierung eine subtile Hintertür, die jedenfalls dem ungeübten Leser nicht ohne weiteres ersichtlich ist.

Jeder Wahlquittungszettel wurde in eine lokale Datei abgespeichert und später zur Abschlußphase daraus wieder ausgelesen. Damit verbleibt aber zu jedem Wahlquittungszettel eine Datei mit der Uhrzeit, die man später auslesen kann. Außerdem wurde auf jeden Wahlquittungszettel zusätzlich eine Signatur ausgedruckt, bei der es sich vermutlich um eine X.509-Signatur handelte, also auf jedem Wahlquittungszettel ebenfalls versteckt die Uhrzeit aufgedruckt wurde.

Weil in Karlsruhe ein besonderes System namens FriWahl eingesetzt wird, das zur Vermeidung von Mehrfachwahlen die Wahl jedes Wählers einschließlich der Uhrzeit und des Ortes bzw. der Urne registriert, kann somit jeder Wahlquittungszettel bzw. dessen Speicherbild dem Wähler zugeordnet werden. Die Schwächen des Verfahrens erlauben es aber auch, jeden Wahlquittungszettel sofort zu entschlüsseln und die abgegebene Stimme aufzudecken.

Das Wahlgeheimnis war damit (potentiell) vollständig gebrochen. Das System wurde damit beworben, daß das bis dahin übliche Verfahren das Wahlgeheimnis nicht hinreichend schützen würde.

Fazit

Anhand der Fehler und Widersprüchlichkeiten wird ersichtlich, daß Bingo Voting nicht einfach nur Fehler hat. Da steckt keine ordentliche ingenieurwissenschaftliche Konstruktion dahinter. Es werden einfach irgendwelche kryptographischen Funktionen zusammengerührt, dann werden irgendwelche Behauptungen aufgestellt und Ansprüche erhoben, und die Fugen werden mit BlaBla und unsubstantiierten Buzzwords verkittet.

Dazu paßt, daß aus dem Kreis des Programmkomitees der Konferenz, auf der Bingo Voting vorgestellt wurde, inzwischen die Äußerung kam, daß es eine akzeptable Vorgehensweise sei, etwas nur zu behaupten und abzuwarten, ob es jemand widerlegen könnte. Im Paper zu Bingo Voting gibt es keine ernsthaften und stichhaltigen Beweise.