E-Demokratie: E-Voting

Eric Dubuis

Inhalt

Zusammenfassung

Der Einsatz elektronischer Wahlsysteme oder E-Voting-Systeme bei politischen Abstimmungen oder Wahlen wird sowohl unter Fachleuten wie auch unter Bürgerinnen und Bürger kontrovers diskutiert. Die einen sehen E-Voting-Systeme als eine natürliche Weiterentwicklung verbreiterter Dienste wie E-Shopping oder E-Banking, während bei den anderen die möglichen Gefahren oder gar die Gefährdung der Demokratie im Vordergrund stehen. Aufbauend auf allgemeinen Anforderungen und entsprechenden Herausforderungen bei der Umsetzung werden im Folgenden generelle vertrauensbildende Massnahmen für den Einsatz von E-Voting-Systemen dargestellt. Kryptografische Verfahren und Bausteine für E-Voting-Systeme werden beschrieben. Sie ermöglichen gewisse widersprüchliche Anforderungen aufzulösen, wie zum Beispiel die Wahrung des Stimm- und Wahlgeheimisses in Verbindung mit der individuellen und universellen Verifikation. Zwei Synthesen dieser Bausteine bilden den Schluss dieses Beitrags: Ein E-Voting-System mit postalischer Zustellung des Stimmrechtsausweises sowie

E. Dubuis (✉)
Leiter des Research Institute for Security in the Information Society, Berner Fachhochschule, Biel, Schweiz
E-Mail: eric.dubuis@bfh.ch

J. Stember et al. (Hrsg.), *Handbuch E-Government*,
https://doi.org/10.1007/978-3-658-21596-5_39-1

ein medienbruchfreies E-Voting-System, welches vollständig über das Internet funktioniert.

Schlüsselwörter
E-Voting · Elektronische Wahlsysteme · E-Voting-Systeme · Anforderung an E-Voting-Systeme · Transparenz bei E-Voting-Systemen · Bausteine für E-Voting-Systeme · Individuelle Verifikation · Universelle Verifikation · Medienbruchfreie E-Voting-Systeme

1 Einleitung

In der realen Welt existiert eine Reihe verschiedenster Prozesse, um eine demokratische Meinungsbildung und Entscheidungsfindung herbeizuführen. Zur Meinungsbildung dienen wenig strukturierte Stammtischgespräche ebenso wie politische Manifestationen zu einem Thema, welche beispielsweise politische Parteien oder Organisationen durchführen. Grundsätzlich strukturierter zu und her geht es bei der anschliessenden Entscheidungsfindung, bei der ausschliesslich strukturierte Entscheidungsprozesse zum Tragen kommen. Es sind dies meist offene oder geheime Abstimmungen und Wahlen, mit welchen ultimativ bindende Entscheidungen herbeigeführt werden.

In der digitalen Welt ist es nicht anders. Auf der Seite der unstrukturierten Meinungsbildung haben wir die Foren und Twitter, welche im Charakter dem Stammtischgeplauder sehr ähnlich gestellt sind. Verbindlichkeiten gibt es fast keine, und die Authentizität einer Aussage ist manchmal infrage zu stellen. Auf der anderen Seite des Spektrums steht das E-Voting, welches durch Abstimmungen und Wahlen bindende Entscheidungen herbeiführt, ähnlich wie im Wahllokal, nur jetzt über das Internet. Im Folgenden werden die Schwierigkeiten, die sich bei E-Voting-Systemen ergeben, sowie konkrete Lösungsansätze beschrieben.

2 Abgrenzung des E-Voting

Mit dem Begriff E-Voting werden alle Stimm- und Wahlprozesse in Verbindung gebracht, bei welchen elektronische Hilfsmittel zum Einsatz gelangen (Wikipedia 2018a). Streng genommen fällt also ein Prozess, bei dem ein Tabellenkalkulationsprogramm zur Auszählung der Stimmen verwendet wird, auch darunter. Ganz sicher fallen die elektronischen Wahlmaschinen (*voting machines*) darunter, wie sie in vielen Ländern in den Wahllokalen verwendet werden. Obwohl sich diese Wahlmaschinen unter der Kontrolle und dem Betrieb der örtlichen Wahlbehörden befinden, wurden in der Vergangenheit Sicherheitslücken entdeckt (Holland 2017). So konnte gezeigt werden, dass sich diese Geräte so manipulieren lassen, dass sie unbemerkt und ohne Spuren zu hinterlassen das Ergebnis verändern können (Morris 2006).

Heutzutage verstehen die meisten Leute unter dem Begriff „E-Voting“ das Abstimmen oder Wählen über das Internet, also den Akt „aus Distanz“ vorzunehmen, und nicht innerhalb einer kontrollierten Umgebung, wie sie das Wahllokal darstellt. Dabei muss folgende, sicherheitsrelevante Unterscheidung beachtet werden:

- Medienbruchfreies E-Voting: Beim medienbruchfreien E-Voting werden sämtliche Abstimmungs- und Wahlinformationen und gegebenenfalls auch die Berechtigung zum Abstimmen oder Wählen per Internet zugestellt. Das Zustellen der Berechtigung entfällt, wenn eine elektronische ID oder ein anderer, mehrfach verwendbarer Mechanismus vorhanden ist.
- E-Voting mit postalischer Zustellung der Wahlberechtigung: In diesem Fall werden hier die Berechtigungen (zusammen mit weiteren Abstimmungs- und Wahlunterlagen) der wahlberechtigten Person per Briefpost zugestellt. Die Berechtigungen sind nur für die bevorstehende Abstimmung oder Wahl gültig.

Ein wichtiger Aspekt im Zusammenhang mit der Stimmabgabe ist die Anzahl der verfügbaren Kanäle. Ist E-Voting der einzige Kanal, oder gibt es für die gleiche Abstimmung oder Wahl noch andere Kanäle? Falls E-Voting als zusätzlicher Kanal zu den bestehenden Kanälen wie Briefpostwahl und das Wählen oder Abstimmen an der Urne angeboten wird, so kann beim E-Voting im Fehlerfall auf einen alternativen, Papier basierten Kanal ausgewichen werden.

3 Anforderungen an E-Voting-Systeme

Wie bei Papier basierten Systemen müssen E-Voting-Systeme eine Reihe von Anforderungen erfüllen (Dubuis et al. 2010). Das Spezielle an diesen Anforderungen ist, dass sie zu einander in Konkurrenz stehen, ja widersprüchlich sind. So gilt es zum Beispiel das Stimmgeheimnis zu wahren. Gleichzeitig muss aber auch sichergestellt werden, dass nur identifizierte und somit berechtigte Personen ihre Stimme abgeben können. Dies lässt sich zwar mit Papier im Wahllokal relativ einfach bewerkstelligen; im elektronischen Fall ist es hingegen viel schwieriger.

Die ersten Anforderungen betreffen unser demokratisches Verständnis:

1. Nur Stimmen von Personen, welche das Stimm- oder Wahlrecht besitzen, dürfen erfasst und ins Ergebnis der Abstimmung oder Wahl fliessen.
2. Pro stimmberechtigte Person darf maximal eine Stimme erfasst und ins Ergebnis der Abstimmung oder Wahl fliessen.[1]

[1]Wir beziehen uns hier auf die Verhältnisse in der Schweiz. Hier darf die stimmberechtige Person maximal eine Stimme über einen beliebigen Kanal abgeben. In anderen Ländern (z. B. Estland) darf die stimmberechtige Person mehrmals seine Stimme abgeben, aber nur die zuletzt abgegeben zählt. Und in wieder anderen Ländern kann sie eine „Erst-“ und eine „Zweit-Stimme“ abgeben, und beide zählen

3. Das Ergebnis einer Abstimmung oder Wahl darf erst am Ende des Urnenganges bekannt werden.

Die nächsten Anforderungen betreffen den Schutz der Privatsphäre:

4. Die Stimme ist geheim.
5. Die stimmende Person kann niemanden beweisen, wie sie gestimmt oder gewählt hat.
6. Die stimmende Person kann ihre Stimme frei von jeglichen Einflüssen abgeben.

Die folgenden Anforderungen betreffen die Korrektheit des Ergebnisses:

7. Jeder Einzelne kann sich vergewissern, dass seine Stimme bei der Ermittlung des Ergebnisses unverändert berücksichtigt worden ist.
8. Alle, also stimmberechtigte wie auch nicht stimmberechtigte Personen, können sich von der korrekten Ermittlung des Ergebnisses überzeugen.
9. Alle, also stimmberechtigte wie auch nicht stimmberechtigte Personen, können sich überzeugen, dass keine unberechtigten Stimmen in die Ermittlung des Ergebnisses eingeflossen sind.

Nicht jede der obigen Anforderungen kann beim E-Voting vollumfänglich erfüllt werden. So ist es zum Beispiel praktisch unmöglich zu garantieren, dass die Stimmabgabe vollkommen frei vor jeglichen ungewollten Einflüssen stattfinden kann, zum Beispiel wenn von zu Hause aus abgestimmt wird.

4 Herausforderungen bei der Erfüllung der Anforderungen

Schauen wir einige der Anforderungen zusammen an und fragen uns, welches denn die Schwierigkeiten deren Erfüllung bei E-Voting-Systemen sein könnten. Wir fangen mit der Berechtigung, eine Stimme oder Wahl abzugeben, an. Damit ein E-Voting-System prüfen kann, ob eine Person das Recht hat, eine Stimme oder Wahl abzugeben, muss es entweder die Person identifizieren oder sonst irgendwie feststellen können, dass sie zur Gruppe der stimm- oder wahlberechtigten Personen gehört. Im ersten Fall bedeutet dies in Bezug auf die Wahrung des Stimmgeheimnisses, dass nach Abgabe der verschlüsselten Stimme zwingend eine Entkopplung der Identität des Stimm- oder Wahlberechtigten und seiner verschlüsselten Stimme vorgenommen werden muss, bevor die Stimme entschlüsselt wird. Die Möglichkeit der Entkopplung einer Identität von der verschlüsselten Stimme mit Hilfe eines Mix-Netzwerkes wird später beschrieben.

Im zweiten Fall wird die Berechtigung mit der Überprüfung, ob eine Person zur Gruppe der stimm- oder wahlberechtigten Personen gehört, festgestellt. Das kann zum Beispiel mit der Anonymisierung der Berechtigungs-Identifikatoren (Spycher und Haenni 2010) erfolgen, welche wiederum mit einem Mix-Netzwerk (Chaum 1981) gemacht werden kann. Damit unter keinen Umständen ein Rückschluss der

abgegebenen, verschlüsselten Stimme auf die abgebende Person erfolgen kann, muss zusätzlich ein anonymer Kanal verwendet werden, zum Beispiel das Tor-Netzwerk (Wikipedia 2018b). Im zweiten Fall gelangen also zwei kryptografische Verfahren zur Entkopplung der Identität des Stimmenden von seiner Stimme zum Einsatz.

Die Wahrung des Stimm- und Wahlgeheimnisses ist auch dann garantiert, wenn nach erfolgter Verschlüsselung der Stimme diese gar nie geöffnet wird. Die Herausforderungen hier sind: Wie kann aus den verschlüsselten Stimmen ein Ergebnis ermittelt werden? Wie kann garantiert werden, dass in einer verschlüsselten Stimme nur korrekte Werte (zum Beispiel nur einmal eine Ja-Stimme, und nicht zweimal) vorkommen?

5 Vertrauensbildende Massnahmen

Damit das Ergebnis einer Abstimmung oder Wahl von allen, also auch von den Unterlegenen, bedingungslos als richtig anerkannt wird, sind verschiedene vertrauensbildende Massnahmen nötig (Dubuis et al. 2011). Im Kontext von E-Voting-Systemen sind das: Transparenz, Offenlegung der Funktionsweise und der Vertrauensannahmen sowie die Verifizierbarkeit des Stimm- und Wahlergebnisses.

Transparenz Zur Förderung des Vertrauens in ein E-Voting-System ist eine offene Informationspolitik grundlegend. Sämtliche organisatorischen Prozesse, Schritte und Handlungen, die bei einer Abstimmung oder Wahl vorkommen, sind zu dokumentieren. Im Weiteren muss festgehalten werden, welche Beteiligte welche Rolle besitzen, und wer zu welchem Zeitpunkt was macht oder machen muss. Ein Sicherheitskonzept muss erstellt und veröffentlicht werden, welches zum Beispiel zeigt, wie die korrekte Ermittlung des Endergebnisses und die Wahrung des Stimmgeheimnisses gewährleistet wird. Prozeduren für den Fehlerfall (Störung im Betrieb, aber auch bei Angriffen) müssen im Voraus definiert und publiziert sein. Die Protokolle, welche entsprechenden Schritte einer Durchführung festhalten, müssen vorliegen und (digital) unterzeichnet sein.

Spezifikation des E-Voting-Systems Die formale Spezifikation des E-Voting-Systems legt auf mathematisch präzise Weise fest, wie es funktioniert. Ein Beispiel einer umfassenden, präzisen Spezifikation ist CHVote (Haenni et al. 2018b). Die Spezifikation definiert das eigentliche E-Voting-Protokoll. Sie legt die zu bestimmenden kryptografischen Parameter und ihre Güte fest, und sie erklärt die präzise Funktionsweise der am Protokoll beteiligten Komponenten und ihre Interaktionen. Die formale Spezifikation bildet die Ausgangslage für die formale Spezifikation der universellen Verifikation. Beide Spezifikationen, die des E-Voting-Systems sowie die der Verifikationssoftware, müssen veröffentlicht sein (Haenni et al. 2018a).

Idealerweise wird mathematisch bewiesen, dass die Spezifikation ein E-Voting-System definiert, welches unter den gegebenen Vertrauensannahmen eine Reihe von Anforderungen erfüllt. Ein solches Dokument mit formalen Beweisen wurde für CHVote erstellt (Bernhard et al. 2018). Der öffentliche Zugang zur formalen

Spezifikation und, falls vorhanden, zu den mathematischen Beweisen stellen wesentliche, vertrauensbildende Massnahmen dar.

Verifizierbarkeit Die Verifizierbarkeit ist ein wesentlicher Bestandteil in der Vertrauensbildung der Stimm- und Wahlberechtigten in das Ergebnis einer Abstimmung oder Wahl. Die *individuelle Verifizierung* erfolgt unmittelbar bei der Stimmabgabe der Stimmenden. Das System muss also den Stimmenden die Möglichkeit geben, sich auf unmissverständliche Art und Weise zu vergewissern, dass ihre Stimme unverfälscht übermittelt (*cast-as-intended*), erfasst (*recorded-as-cast*) und am Ende richtig ausgezählt (*counted-as-recorded*) worden ist. Oft ist beim eigentlichen Akt der Stimmabgabe nur der erste Teil der individuellen Verifikation möglich, nämlich der der Überprüfung der unverfälschten Stimmabgabe. Dieser ist aber enorm wichtig, denn damit kann eine allfällige Verfälschung der Stimme durch einen Virus im persönlichen Stimm- und Wahlgerät entdeckt werden. Im Fehlerfall bieten sich je nach E-Voting-System zwei Optionen. Bei der ersten Option weicht der Stimmende auf ein anderes Wahlgerät aus, von dem er annimmt, dass es keinen Virus hat. Eine Wiederholung des Wahlprozesses auf dem infizierten Gerät bringt nichts. Die zweite Option, wie zum Beispiel das Abstimmen oder Wählen am Wahlsonntag an der Urne, gilt nur, wenn alternative Kanäle zur Stimmabgabe zur Verfügung stehen. Falls ein Wahlsystem mehrere Kanäle anbietet, müssen Vorkehrungen getroffen werden, dass niemand mehr als eine Stimme über verschieden Kanäle abgeben kann.

Mittels der *universellen Verifizierung* wird die Korrektheit des Abstimmungs- oder Wahlergebnisses bewiesen. Grundsätzlich kann jeder, also auch Personen, welche nicht stimm- oder wahlberechtigt gewesen sind, mit geeigneter Verifikationssoftware die Korrektheit überprüfen. Die Überprüfung der Korrektheit umfasst das Prüfen sämtlicher Wahldaten. Die Wahldaten bestehen aus:

- Der Definition der Abstimmungs- und Wahldaten (Abstimmungsfrage, Kandidierende, Regeln)
- Der Menge der Abstimmungs- oder Wahlberechtigten
- Der Definition des Abstimmungs- oder Wahlprozesses (Start- und Enddatum, kryptografische Parameter, Identitäten der Autoritäten)

Zusätzlich zu diesen Daten ergeben sich weitere Daten während der Ausführung der Abstimmung oder Wahl:

- Kryptografische Evidenzen (digitale Signaturen, kryptografische Beweise)
- (am Schluss) Wahlresultat

Ein E-Voting-System mit universeller Verifikation erlaubt die Überprüfung dieser Daten auf:

- Vollständigkeit: Sind sämtliche Daten des Abstimmungs- oder Wahlprozesses vorhanden, um die gesamte Kette der Verifikationsschritte bis hin zum Ergebnis auszuführen?

- Integrität: Entsprechen die Daten den Definitionen der formalen Spezifikation? Sind sie im vorgesehenen Wertebereich?
- Konsistenz: Sind die Daten mit Bezügen untereinander konsistent?
- Evidenz: Sind die kryptografischen Beweise korrekt? Sind die digitalen Signaturen gültig?
- Authentizität: Stammen die Daten von den dafür vorgesehenen Autoritäten und Stimmenden?

Personen, welche die vollständige Überprüfung obiger Punkte durchführen, erstellen einen Verifikationsbericht und veröffentlichen ihn (Haenni et al. 2018a).

6 Bausteine fürs E-Voting

Um den verschiedenen, zum Teil widersprüchlichen Anforderungen an E-Voting-Systeme gerecht zu werden, setzt man kryptografische Verfahren ein, deren Bausteine im Folgenden kurz erklärte werden.

Digitaler Fingerabdruck Von einem gegebenen, elektronischen Dokument beliebiger Grösse lässt sich ein eindeutiger Fingerabdruck mit fester, endlicher Grösse (darstellbar zum Beispiel mit 256 Bits) erstellen. Dabei wird die binäre Darstellung des Dokuments einer kryptografischen Streuwertfunktion (engl. *hash function*) zugewiesen (Wikipedia 2018c), welche den Fingerabdruck (Hash-Wert) berechnet. „Gute" Fingerabdrücke erhält man, wenn die Streuwertfunktion folgende Eigenschaft aufweist:

- Einwegfunktion: Es ist praktisch unmöglich, aus einem gegebenen Fingerabdruck das Eingabedokument zu finden, welches eben diesen Fingerabdruck ergibt.
- Starke Kollisionsresistenz: Es ist praktisch unmöglich, zwei verschiedene Eingabedokumente zu finden, welche den gleichen Fingerabdruck ergeben.

Digitale Signatur Verknüpft man den Fingerabdruck eines Dokuments auf geeignete Weise mit einem geheimen Wert, welcher nur der Ersteller des Dokuments kennt, so lässt sich eine digitale Signatur (Wikipedia 2018d) des Dokuments erstellen. Die digitale Signatur drückt aus, dass das Dokument authentisch ist und zum Beispiel nicht von einem Dritten geändert wurde. Der geheime Wert wird *privater* Schlüssel genannt. Zum privaten Schlüssel gibt es einen passenden, *öffentlichen* Schlüssel. Die beiden Schlüssel wurden vorgängig gemeinsam mittels eines geeigneten Verfahrens erstellt, und die Zuordnung des öffentlichen Schlüssels an den Ersteller wurde von einer offiziellen Stelle beglaubigt. Ein drittes, passendes Verfahren erlaubt nun jedem, die Signatur eines Dokuments zu prüfen und so die Authentizität zu bestimmen.

Asymmetrische Verschlüsselung Um den Inhalt eines elektronischen Dokuments von Dritten geheim zu behalten, muss es verschlüsselt werden. Um die elektronischen Stimmen auf geheime Weise in eine elektronische Urne legen zu

können, werden sie mit dem *öffentlichen* Schlüssel, der zu elektronischen Urne gehört, verschlüsselt (Wikipedia 2018e). Erst am Ende einer Abstimmung oder Wahl werden die verschlüsselten Stimmen mit dem passenden *privaten* Schlüssel entschlüsselt. Um das Stimmgeheimnis garantieren zu können, ist die Entschlüsselung noch etwas komplizierter: Die Entschlüsselung erfolgt nicht mit *einem* privaten Schlüssel, sondern über ein mehrstufiges Anwenden mehrerer, aufeinanderpassender Entschlüsselungen mit jeweils passenden, *privaten Teilschlüssel*. Der öffentliche und die passenden privaten Teilschlüssel wurden vorgängig auf geeignete Weise erzeugt.

Homomorphe Verschlüsselung Die homomorphe Verschlüsselung (Wikipedia 2018f) ist eine spezielle Art der asymmetrischen Verschlüsselung. Sie erlaubt, Berechnungen über die Verschlüsselungen anzustellen. So können beispielsweise Verschlüsselungen addiert werden. Wenn nun ein „nein" mit null und ein „ja" mit eins verschlüsselt wird, so ergibt die Addition der Verschlüsselung die verschlüsselte Summe der Ja-Stimmen in einem Exponenten. Mit der Entschlüsselung der verschlüsselten Summe und einem einfachen Durchprobieren erhält man das Abstimmungsergebnis, ohne dass man je die einzelnen Stimmen entschlüsselt hat. Das Verfahren ist nur bei Abstimmungen effizient.

Eine weitere Anwendung der homomorphen Verschlüsselung ist die Wiederverschlüsselung. Hier wird eine verschlüsselte Meldung nochmals neu verschlüsselt, ohne die verschlüsselte Meldung vorher entschlüsseln zu müssen. Die Wirkung ist, dass die „Verschlüsselungshülle" der verschlüsselten Meldung ihr „Aussehen" ändert. Dieses Verfahren wird beim kryptografischen Mischen mittels verifizierbaren Mix-Netzwerken gebraucht.

Commitment-Verfahren Ein weiterer, wichtiger kryptografischer Baustein stellt ein Commit-Verfahren dar (Wikipedia 2017). Mit einem Commitment kann eine Partei sich auf einen festen, unveränderbaren Wert festlegen, ohne ihn offenlegen zu müssen. Wenn es dann später für andere wichtig wird, diesen Wert kennenzulernen, so kann diese Partei das Commitment öffnen und so den zuvor unbekannten Wert bekannt geben. Commitment-Verfahren werden u. a. für nicht-interaktive Zero-Knowledge-Beweise gebraucht.

Nicht-interaktive Zero-Knowledge-Beweise In nicht-interaktiven Zero-Knowledge-Beweisen (Wikipedia 2018g) beweisen sogenannte „Beweiser", dass sie sich gemäss den Regeln eines Protokolls verhalten, ohne dass sie dabei zu viel Information (z. B. einen geheimen Wert) preisgeben. Sogenannte „Verifizierer" können andererseits die Beweise prüfen, ob sie stimmen, ohne dass sie etwas Nützliches lernen (z. B. den vom Beweiser verwendeten, geheimen „Wert" wie das Mischen der verschlüsselten Stimmen). Nicht-interaktive Zero-Knowledge-Beweise werden in den Mix-Netzwerken verwendet.

Verifizierbare Mix-Netzwerke Bei E-Voting-Systemen ist die abgegebene, verschlüsselte Stimme an einen Identifikator gekoppelt. Falls die Stimme jetzt entschlüsselt würde, liesse sich über den Identifikator schliessen, wie eine Person gestimmt oder gewählt hat. Somit wäre das Stimm- bzw. Wahlgeheimnis verletzt.

Das verifizierbare Mix-Netzwerk verhindert dies (Terelius und Wikström 2010). Es besteht aus zwei oder mehreren, unabhängigen Stufen. Jede Stufe arbeitet für sich und führt im Wesentlichen diese beiden Operationen durch:

1. Die Liste der verschlüsselten Stimmen (*ohne* ihre Identifikatoren) werden gemischt. Das Mischen muss man sich so vorstellen, dass die Reihenfolge der Stimmen am Ausgang der Stufe mit der Reihenfolge der Stimmen am Eingang nicht mehr dieselbe ist. Zudem beweist die Stufe mittels nicht-interaktivem Zero-Knowledge-Beweis, dass sie korrekt gemischt, also keine Stimme unterschlagen und keine Stimme dupliziert hat.
2. Das Bitmuster jeder verschlüsselten Stimme wird geändert, ohne dass der Inhalt der verschlüsselten Stimme geändert wird. Das ist nötig, damit man die Stimmen am Ausgang der Stufe nicht den Positionen der Stimmen am Eingang zuordnen kann. Könnte man dies, so könnte man von hinten her das Stimm- oder Wahlgeheimnis brechen, sobald die Stimme entschlüsselt ist. Dazu ist die oben erwähnte Wiederverschlüsselung notwendig. Zudem beweist die Stufe für jede Stimme, dass sie eine neue und geheime Zufallszahl für die Wiederverschlüsselung verwendet hat.

Verteilung der Macht: Anschlagbrett und Kontrollkomponenten Aus der Sicht der Stimm- und Wahlberechtigten besteht ein E-Voting-System in erster Linie aus einem monolithischen E-Voting-Server. Tatsächlich besteht ein E-Voting-System aus n unabhängigen Servern (den Kontrollkomponenten) und dem öffentlichen Anschlagbrett. Die Kommunikation des Wahlgeräts mit den Servern erfolgt über das Anschlagbrett. Das Anschlagbrett zeichnet die Meldungen auf, die es einerseits vom Stimm- oder Wahlberechtigten und andererseits von den Kontrollkomponenten erhält. Eine wichtige Eigenschaft des Anschlagbretts ist, dass es Meldungen nur anfügen kann; es kann keine bestehenden Meldungen ändern oder löschen. Täte es das, so würde man es merken.

Die Kontrollkomponenten sind voneinander unabhängig. Sie koordinieren sich über das Anschlagbrett. Wichtig ist, dass sie von unabhängigen Personen oder Organisationen betrieben werden. Sie bewältigen eine Vielzahl von Aufgaben:

- Während der Wahlvorbereitung: (je nach Art des E-Voting-Systems) Berechnung der Prüf-, Bestätigungs- und Finalisationsziffern für die Stimmrechtsausweise der Wählenden; verteilte Berechnung des öffentlichen Schlüssels für die Verschlüsselung der Stimmen.
- Während der Abstimmungs- oder Wahlphase: Prüfung des elektronischen Stimmzettels der Wählenden; (je nach Art des E-Voting-Systems) Berechnung der benötigten Information für die Prüfziffern; aufzeichnen, wer schon gewählt oder gestimmt hat (die Prüfziffern werden höchstens einmal an das Wahlgerät des Wählenden geschickt).
- Während der Auszählphase: Kryptografisches Mischen der Stimmen (jede Kontrollkomponenten entspricht einer Stufe); Teilentschlüsselung der verschlüsselten und gemischten Stimmen; Dekodierung und Auszählung.

Alle von den Kontrollkomponenten erzeugten Daten werden auf dem elektronischen Anschlagbrett aufgezeichnet, ausser den geheimen Teilschlüsseln für das Entschlüsseln der Stimmen, den verwendeten Permutationen beim Mischen, den Randomisierungen der Wiederverschlüsselungen sowie die privaten Signierschlüssel. (Haenni und Hauser 2018) modellieren die Eigenschaften eines elektronischen Anschlagbretts.

Das Drucken des Stimmrechtsausweises Für E-Voting-Systeme mit postalischem Kanal für die Zustellung der Stimmrechtsausweise: Die in der Wahlvorbereitung erstellten Identifikatoren, Prüf-, Bestätigungs- und Finalisationsziffern sowie Adressdaten werden der Druckerei per sicherem, verschlüsselten Kanal geschickt. Die Druckerei druckt die Stimmrechtsausweise und verschickt sie den Stimm- und Wahlberechtigten.

Prüfziffern Für E-Voting-Systeme mit postalischem Kanal für die Zustellung der Stimmrechtsausweise: Sobald die stimm- oder wahlberechtigte Person ihre Stimme dem Wahlgerät anvertraut hat, wird diese verschlüsselt und dem E-Voting-System geschickt. Das Wahlgerät könnte aber durch einen Virus manipuliert sein, welcher die Stimme unmittelbar vor der Verschlüsselung verändert. Die stimm- oder wahlberechtigte Person würde davon nichts merken. Auch die Verschlüsselung würde diese Manipulation nicht verhindern bzw. offenlegen. Das E-Voting-System würde es ebenfalls nicht merken, da die Stimmabgabe geheim erfolgt.

Mit Hilfe von Prüfziffern hingegen kann ein allfälliger Virus entdeckt und seine Wirkung verhindert werden. Dazu existieren verschiedene Verfahren. Mit dem *Oblivious Transfer*-Verfahren (Chu und Tzeng 2005) schickt das Wahlgerät zusätzlich zur verschlüsselten Stimme eine Aufforderung an das E-Voting-System, eine Bestätigung an das Wahlgerät des Wählers zurückzuschicken. Die Bestätigung ist so konstruiert, dass das Wahlgerät individuelle Prüfziffern berechnen kann, welche dem Wähler angezeigt werden. Der Wähler vergleicht die Prüfziffern mit den Werten, welche er auf dem Stimmrechtsausweis vorfindet. Ein Virus, das im Wahlgerät steckt, kann keinesfalls diese Werte kennen. Stimmen die am Bildschirm angezeigten Werte mit denjenigen auf dem Stimmrechtsausweis überein, so wurde die Stimme des Wählenden unverfälscht dem E-Voting-System übertragen, und der Wähler kann unbesorgt den Bestätigungsziffer dem E-Voting-System schicken. Die Finalisationsziffer vom E-Voting-System beendet den Stimm- oder Wahlvorgang.

Dieser Mechanismus verhindert auch eine vermeintliche „man-in-the-middle"-Attacke: Ein Angreifer, dem es gelingt, sich zwischen das Wahlgerät und dem E-Voting-System zu setzen, könnte *nicht* unbemerkt die Stimmen *ändern*, denn dazu müsste er die individuellen Prüfziffern kennen. Allerdings könnte er herausfinden, wie jemand gestimmt oder gewählt hat (ohne die Stimme zu ändern). Das wäre, wie wenn jemand dem Stimmenden oder Wählenden während des Aktes über die Schultern schauen würde.

7 Synthese

Aus den oben skizzierten Bausteinen lassen sich verifizierbare E-Voting-Systeme auf zwei unterschiedliche Arten bauen. Beiden Arten gemeinsam ist das elektronische Anschlagbrett, welches für die universelle Verifikation notwendig ist.

E-Voting mit postalisch zugestelltem Stimmrechtsausweis Die erste Art verwendet zwei Kanäle für die Wählenden. Der eine Kanal, über den die Stimm- oder Wahlberechtigung einer Person erteilt wird, verwendet die Briefpost. Die unmittelbare Vertrauensannahme ist, dass die Druckerei und der Postweg zuverlässig sind, und die zugestellte Information (u. a. der Stimmrechtsausweis) nicht verändert wird und geheim bleibt. Der per Briefpost zugestellte Stimmrechtsausweis enthält den Identifikator sowie die Prüf-, Bestätigungs- und Finalisationsziffern.

Die stimm- oder wahlberechtigte Person bereitet ihre Wahl mit dem Wahlgerät vor. Danach schickt sie ihre Stimme ab und vergleicht die angezeigten Prüfziffern mit denjenigen, welche sie auf dem per Post erhaltenen Stimmrechtsausweis vorfindet. Wenn alles stimmt, bestätigt sie dies mit der Bestätigungsziffer, was mit dem Abschicken der Finalisationsziffer des Wählenden an den E-Voting-Server quittiert wird (Haenni et al. 2018b).

Medienbruchfreies E-Voting-System Dieser Typus verwendet nur den elektronischen Kanal für das eigentliche Abstimmen oder Wählen. Allerdings sind die Stimm- oder Wahlberechtigten im Besitz von Anmeldedaten, welche sie vorgängig erhalten oder sich beschafft haben, z. B. in Form einer elektronischen Identität.

Das Anzeigen von Prüfziffern macht hier keinen Sinn, denn sie können mit keiner vertrauensvollen Referenz verglichen werden. Ein Virus im Wahlgerät könnte jederzeit dem Wählenden irgend etwas vorgaukeln. Solche E-Voting-Systeme können nur in Kontexten verwendet werden, bei denen mögliche Angreifer den Aufwand scheuen, die Wahlgeräte der Abstimmenden oder Wählenden mit Viren zu infiltrieren, wie zum Beispiel bei Wahlen von Studierendenvertretungen, Vereinswahlen oder dergleichen.

Für Abstimmungen und Wahlen in politischen Kontexten ist davon auszugehen, dass die kriminelle Energie von Angreifern wesentlich grösser ist. Man muss mit der Verbreitung von Viren rechnen. Ein vollständig medienbruchfreies E-Voting kann in dem Fall nur dann in Betracht gezogen werden, wenn den Wählenden nebst dem eigentlichen Wahlgerät (Laptop, Smartphone) ein zusätzliches, unfälschbares, vertrauenswürdiges Gerät abgegeben wird. Mit diesem Gerät wird am Ende des Abstimmungs- oder Wahlaktes und nach eingehender Kontrolle der Abstimmungs- und Wahlintention des Wählenden die Stimme verschlüsselt, (typischerweise) elektronisch signiert und auf geeignete Weise abgeschickt. Das Konzept eines solchen Gerätes wurde in (Dubuis et al. 2012) vorgestellt. Solange keine zusätzlichen, unfälschbaren Geräte vorhanden sind, ist von medienbruchfreien E-Voting-Systemen im politischen Kontext abzusehen.

8 Fazit

Kehren wir zu den Anforderungen zurück und betrachten wir, was erreicht wurde. Anforderung 1 „nur Stimmen von stimm- oder wahlberechtigten Personen“ und Anforderung 2 „pro stimm- oder wahlberechtigte Person maximal eine Stimme“ können mit einmal zu verwendenden Identifikatoren oder mit digitalen Signaturen relativ einfach realisiert werden. Anforderung 3 „Ergebnis nach Schliessung der Urne“ wird mittels verteilter Entschlüsselung durch die Kontrollkomponenten gewährleistet.

Anforderung 4 „Stimmgeheimnis“ wird durch die Entkopplung der verschlüsselten Stimme mit dem Identifikator mittels verifizierbarem Mix-Netzwerk erreicht. Für die Realisierung dieser Anforderung gibt es auch andere Verfahren. Anforderung 5 „Unbeweisbarkeit des Inhalts der Stimme“ ist durch die vorgestellten Verfahren gewährleistet. Anforderung 6 „frei von jeglichen Einflüssen“ kann mit keiner Form des Abstimmens oder Wählens in unkontrollierbaren Umgebungen erfüllt werden. Sollte das öffentliche Anschlagbrett für alle einsehbar ist, dann ist für einen allfälligen Erpresser auch feststellbar, dass jemand abstimmen oder wählen ging, obwohl er andere Instruktionen erteilte.

Anforderung 7 „korrekte Ablieferung der Stimme“ kann dank der Prüfziffern erfüllt werden oder aber es stehen den Wählenden vertrauenswürdige Geräte zur Verfügung, und „wurde (m)eine Stimme bei der Ermittlung des Ergebnisses berücksichtigt“ ist durch das Vorhandensein von entsprechenden Evidenzen, welche von den Kontrollkomponenten stammen, indirekt erfüllt. Anforderung 8 „korrekte Ermittlung des Resultats“ und Anforderung 9 „nur Stimmen von stimm- und wahlberechtigten Personen“ kann mittels universeller Verifikation erfüllt werden.

Es ist aber in aller Deutlichkeit zu sagen, dass jederzeit eine oder mehrere Kontrollkomponenten gehackt oder das elektronische Anschlagbrett manipuliert werden können. Dies ist auch mit den besten Vorkehrungen nie ganz auszuschliessen. Wichtig ist aber, dass ein solcher Angriff entdeckt würde, ausser der Angreifer hätte alle Kontrollkomponenten und das Anschlagbrett unter seiner Kontrolle. Im letzten Fall könnte nämlich der Angreifer die Aufzeichnung auf dem Anschlagbrett auf konsistente Art neu schreiben. Hätten die Wählenden eine dauerhaft gültige Quittung für die abgegebene Stimme oder Wahl, wäre auch das nicht mehr möglich. Allerdings: Eine starke Quittung würde Tür und Tor für das Erpressen der Stimmenden oder für den Stimmenkauf öffnen.

Zwar ist Anforderung 4 „Stimmgeheimnis“ aus Sicht des E-Voting-Systems gewährleistet. Dennoch könnte ein Spionage-Virus sich im Wahlgeräte des Stimmenden einnisten und unmittelbar vor der Verschlüsselung der Stimme diese über einen versteckten Seitenkanal an einen Dritten weiterleiten. Falls der Spionage-Virus flächendeckend verbreitet würde, könnte der Dritte das Stimmverhalten vieler Bürgerinnen und Bürger erfassen und auf gezielte Weise auswerten. Nur ein zusätzliches, unfälschbares, vertrauenswürdiges Gerät könnte hier Abhilfe bieten.

Beim oben skizzierten E-Voting-System mit postalischer Zustellung der Stimmrechtsausweise ist wichtig zu verstehen, auf welchen Vertrauensannahmen das Ganze beruht. Es sind deren drei:

1. Mindestens eine der Kontrollkomponenten arbeitet so, wie das Protokoll es vorsieht.
2. Die Druckerei macht genau das und nur das, was ihr aufgetragen wird.
3. Die Wahlgeräte der stimm- oder wahlberechtigten Person besitzen keine versteckten Kanäle zu Dritten.

Das medienbruchfreie E-Voting ist eine grosse Herausforderung. Einerseits liegt es auf der Hand, dass dies viele wollen, speziell die im Ausland lebenden Stimm- und Wahlberechtigten. Andererseits wird der Stimmfälschung durch Viren in den Wahlgeräten Tür und Tor geöffnet. Medienbruchfreies E-Voting bedingt die Bereitstellung spezifischer, vertrauenswürdiger Hardware.

Ideal wäre, wenn das elektronische Anschlagbrett für alle öffentlich einsehbar für alle wäre. Dann könnte jedermann die universelle Verifikation durchführen. Nicht nur aus Gründen des Datenschutzes (die Namen der Wählenden oder mindestens die Identifikatoren wären einsehbar) wäre dies ein Problem. Es gäbe noch ein zweites Problem: Würde man mit *Brute Force*-Attacken die Wahldaten analysieren, so könnte nach sehr langer Zeit das Stimmgeheimnis gebrochen werden. Dieses *Everlasting privacy*-Problem stellt zurzeit eine grosse Herausforderung für die E-Voting-Forscher dar.

Literatur

Bernhard, D., Cortier, V., Gaudry, P., Turuani, M., & Warinschi, B. (2018). Verifiability analysis of CHVote (13 Juli 2018).

Chaum, D. (1981). Untraceable electronic mail, return addresses and digital pseudonyms. *Communications of the ACM, 24*(2), 84–88.

Chu, C.-K., & Tzeng, W.-G. (2005). Efficient k -out-of- n oblivious transfer schemes with adaptive and non-adaptive queries. In S. Vaudenay (Hrsg.), *PKC'05, 8th international workshop on theory and practice in public key cryptography* (Bd. LNCS 3386, S. 172–183). Les Diablerets: Springer.

Dubuis, E., Fischli, S., & Haenni, R. (2010). E-Voting-Systeme: für mehr Transparenz. *eGov Präsenz, 2*, 32–33.

Dubuis, E., Spycher, O., & Volkamer, M. (2011). Vertrauensbildung bei Internetwahlen. *digma – Zeitschrift für Datenrecht und Informationssicherheit, 3*, 126–129.

Dubuis, E., Haenni, R., & Koenig, R. E. (2012). In S. Bundeskanzlei (Hrsg.), *Konzept und Implikationen eines verifizierbaren Vote Électronique Systems* (21 Februar 2012). https://www.bk.admin.ch/dam/bk-intra/de/dokumente/pore/politische_rechte/konzept_berner_fachhochschule.pdf.download.pdf/konzept_berner_fachhochschule.pdf. Zugegriffen am 14.10.2018.

Haenni, R., & Hauser, S. (2018). Modeling a Bulletin Board Service based on Broadcast Channels with Memory. *22nd International Conference on Financial Cryptography.* Willemstadt/Curaçao.

Haenni, R., Dubuis, E., Koenig, R. E., & Locher, P. (2018a). Process models for universally verifiable elections. In R. Krimmer, M. Volkamer, V. Cortier, R. Goré, M. Hapsara, U. Serdült & D. Duenas-Cid (Hrsg.), *Electronic voting, third international joint conference, E-vote-ID 2018* (Bd. LNCS 11143). Bregenz/Österreich: Springer.

Haenni, R., Koenig, R. E., Locher, P., & Dubuis, E. (2018b). *Cryptology ePrint archive: CHVote system specification* (11 September 2018). https://eprint.iacr.org/2017/325.pdf. Zugegriffen am 31.10.2018.

Holland, M. (2017). *Heise* (15 Juni 2017). https://www.heise.de/security/meldung/US-Wahlcomputer-Gravierende-Sicherheitsluecken-in-Georgia-gefunden-3744965.html. Zugegriffen am 14.10.2018.

Morris, C. (2006). *Heise* (06 Oktober 2006). https://web.archive.org/web/20070117143032/http://www.heise.de/english/newsticker/news/79106. Zugegriffen am 14.10.2018.

Spycher, O., & Haenni, R. (2010). A novel protocol to allow revocation of votes in a hybrid voting system. In *ISSA'10, 9th Annual Conference on Information Security.* Sandton/Südafrika.

Terelius, B., & Wikström, D. (2010). Proofs of restricted shuffles. In D. J. Bernstein & T. Lange (Hrsg.), *AFRICACRYPT'10, 3rd international conference on cryptology in Africa* (Bd. LNCS 6055, S. 100–113). Stellenbosch/Südafrika: Springer.

Wikipedia. (2017). Commitment-Verfahren. In *Wikipedia, die freie Enzyklopädie*. https://de.wikipedia.org/wiki/Commitment-Verfahren. Zugegriffen am 14.10.2018.

Wikipedia. (2018a). Elektronische Stimmabgabe. In *Wikipedia, die freie Enzyklopädie*. https://de.wikipedia.org/wiki/Elektronische_Stimmabgabe. Zugegriffen am 14.10.2018.

Wikipedia. (2018b). Tor (Netzwerk). In *Wikipedia, die freie Enzyklopädie*. https://de.wikipedia.org/wiki/Tor_(Netzwerk). Zugegriffen am 14.10.2018.

Wikipedia. (2018c). Hashfunktion. In *Wikipedia, die freie Enzyklopädie*. https://de.wikipedia.org/wiki/Hashfunktion. Zugegriffen am 14.10.2018.

Wikipedia. (2018d). Digitale signatur. In *Wikipedia, die freie Enzyklopädie*. https://de.wikipedia.org/wiki/Digitale_Signatur. Zugegriffen am 14.10.2018.

Wikipedia. (2018e). Asymmetrisches Kryptosystem. In *Wikipedia, die freie Enzyklopädie*. https://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem. Zugegriffen am 14.10.2018.

Wikipedia. (2018f). Homomorphe Verschlüsselung. In *Wikipedia, die freie Enzyklopädie*. https://de.wikipedia.org/wiki/Homomorphe_Verschl%C3%BCsselung. Zugegriffen am 14.10.2018.

Wikipedia. (2018g). Non-interactive zero-knowledge proof. In *Wikipedia, the free encyclopedia*. https://en.wikipedia.org/wiki/Non-interactive_zero-knowledge_proof. Zugegriffen am 14.10.2018.