JeDEM 2(1): 79-88, 2010
ISSN 2075-9517
http://www.jedem.org

Ein PKI-basiertes Protokoll für sichere und praktikable Onlinewahlen

Lucie Langer, Axel Schmidt, Melanie Volkamer, Johannes Buchmann

Technische Universität Darmstadt / CASED, {langer, axel, buchmann}@cdc.informatik.tu-darmstadt.de, volkamer@cased.de

Abstract: *Wir stellen ein Protokoll für Onlinewahlen vor, welches auf dem Schema von Ohkubo et al. (1999) basiert. Besonders an diesem Protokoll ist, dass der Auszähler nicht vertrauenswürdig sein muss. Der geheime Schlüssel des Auszählers wird am Ende der Wahl veröffentlicht und ermöglicht so die universelle Verifizierbarkeit der Stimmauszählung. Wir diskutieren die Sicherheit des Protokolls angesichts der allgemein anerkannten Sicherheitsanforderungen für elektronische Wahlschemata.*

Keywords: Onlinewahlen, PKI, Verifizierbarkeit

Acknowledgement: Diese Arbeit wurde unterstützt durch CASED (Center for Advanced Security Research Darmstadt).

1. Einleitung

Das nachfolgend dargestellte Protokoll für Onlinewahlen ist eine Weiterentwicklung des Protokolls von Ohkubo et al. (1999): Statt den Auszählprozess auf mehrere Instanzen zu verteilen, beschränken wir uns auf einen Auszähler, der dennoch nicht vertrauenswürdig sein muss: Sein geheimer Schlüssel wird am Ende der Wahl auf einem öffentlichen schwarzen Brett publiziert. Dadurch kann die korrekte Auszählung von jedem verifiziert werden.

Das Protokoll zielt darauf ab, eine effiziente Implementierung des Wahlsystems zu ermöglichen. Daher wird auf schwer umsetzbare Annahmen (z.B. „untappable channels“ (Juels & Catalano & Jakobsson, 2005)) oder komplizierte Primitive verzichtet. Die wesentlichen Sicherheitsanforderungen an elektronische Wahlsysteme werden dennoch erreicht.

Im folgenden Abschnitt werden die Sicherheitsanforderungen an elektronische Wahlprotokolle erläutert. Abschnitt 3 präsentiert das eigentliche Protokoll. In Abschnitt 4 analysieren wir das Protokoll im Hinblick auf die in Abschnitt 2 definierten Sicherheitsanforderungen. In Abschnitt 5 gehen wir auf Fragen hinsichtlich der Implementierung ein. Abschnitt 6 schließt den Beitrag mit einer Zusammenfassung.

2. Sicherheitsanforderungen

Ein elektronisches Wahlprotokoll muss verschiedene Sicherheitsanforderungen erfüllen. Im Folgenden werden diese Sicherheitsanforderungen definiert. Sie werden in dieser oder ähnlicher Form beispielsweise in (Burmester & Magkos, 2003; Cetinkaya, 2007; Hirt, 2001; Lambrinoudakis & Gritzalis & Tsoumas & Karyda & Ikonomopoulos, 2003; Riera, 1998) beschrieben.

Exaktheit:

- Ein abgegebenes Votum kann nicht dupliziert, gelöscht oder unberechtigt verändert werden.
- Alle gültigen Voten werden gezählt.

Demokratie:

- Nur berechtigte Wähler können ein Votum abgeben.
- Jeder berechtigte Wähler gibt höchstens ein Votum ab.[1]

Geheimhaltung:

- Anonymität: Es ist nicht möglich, ein Votum mit dem Wähler zu assoziieren, der es abgegeben hat.
- Fairness: Alle Voten bleiben bis zum Ende der Wahlphase geheim.
- Quittungsfreiheit: Kein Wähler kann beweisen, dass er ein bestimmtes Votum abgegeben hat.
- Unzwingbarkeit: Kein Wähler kann gezwungen werden, ein bestimmtes Votum abzugeben.

Verifizierbarkeit:

- Universell: Jeder kann verifizieren, dass alle gültigen Stimmen gezählt wurden.
- Individuell: Jeder Wähler kann verifizieren, dass seine gültige Stimme gezählt wurde.

3. Ein sicheres elektronisches Wahlprotokoll

In diesem Abschnitt präsentieren wir ein PKI-basiertes Onlinewahlprotokoll. Dazu definieren wir zunächst die Akteure des Wahlsystems und die Notationen, die wir verwenden. Außerdem beschreiben wir die Annahmen, welche wir zu Grunde legen.

3.1. Kommunikation und kryptographische Primitive

Das Protokoll setzt die Existenz eines authentischen öffentlichen *schwarzen Bretts* (auch bekannt als „bulletin board“ (Benaloh, 1987; Cohen & Fischer, 1985) voraus. Diese Komponente wird bei elektronischen Wahlverfahren eingesetzt, um universelle und individuelle Verifizierbarkeit zu erreichen. Jeder kann die dort publizierten Nachrichten lesen, aber nur autorisierte Akteure können Nachrichten dort ablegen. Weiterhin kann niemand einmal geschriebene Nachrichten löschen oder überschreiben.

Außerdem werden *blinde Signaturen* nach Chaum (1983) eingesetzt. Dieser Mechanismus verhindert, dass der Signierer die zu unterschreibende Nachricht lesen kann. Eine weitere verwendete Anonymisierungstechnik ist das *Mix–Netz* (Chaum, 1981). Grundsätzlich empfängt ein Mix–Netz eine Menge von Nachrichten und sendet diese in randomisierter Reihenfolge weiter. Es bricht damit die Verbindung zwischen eingehenden und ausgehenden Nachrichten auf. Für Geheimhaltung und Authentifikation werden Public–Key–Systeme benutzt, wie z.B. RSA von Rivest, Shamir and Adleman (1978). Die eingesetzte Verschlüsselung ist probabilistisch, d.h. die Schlüsseltexte sind durch Zufallszahlen randomisiert.

3.2. Akteure

Folgende Akteure sind an dem Protokoll beteiligt:

Wähler W	gibt seine Stimme über eine sichere Internetverbindung ab
Bestätiger B	bestätigt die Wahlberechtigung des Wählers durch eine Signatur des Votums
schwarzes Brett SB	authentischer öffentlicher Aushang

[1] Ein Votum kann dabei durchaus Stimmen für mehrere Kandidaten enthalten; gemeint ist hier lediglich, dass alle Wähler den gleichen Einfluss auf den Ausgang der Wahl haben.

Mix–Netz M	mischt die abgegebenen Voten
Auszähler A	zählt die abgegebenen Voten aus

3.3. Notation

Das Protokoll wird mit Hilfe folgender Notation beschrieben:

$E_P(m)$	Verschlüsselung der Nachricht m mit dem öffentlichen Schlüssel des Akteurs P
$S_P(m)$	Signatur der Nachricht m mit dem geheimen Schlüssel des Akteurs P
B(m,r)	Blenden der Nachricht m mit dem Blendfaktor r
UB(m,r)	Entblenden der Nachricht m mit dem Blendfaktor r
v	ausgefüllter Stimmzettel (Votum)

3.4. Annahmen

Wir setzten die folgenden Fakten als gegeben voraus:

- Es steht eine vertrauenswürdige Public–Key–Infrastruktur (PKI) zur Verfügung. Alle benutzten öffentlichen Schlüssel sind validiert. Eine Zertifizierungsstelle gibt entsprechende PKI–Zertifikate heraus. Das impliziert, dass alle Verschlüsselungen mit den richtigen öffentlichen Schlüsseln gemacht werden. Alle Akteure nehmen an der PKI teil. Die eingesetzte Kryptographie ist stark und praktisch nicht zu brechen.
- Zur Kommunikation wird ein Protokoll wie z.B. TCP/IP benutzt, welches das Ankommen der Nachrichten sicherstellt. Wir nehmen außerdem an, dass die Kommunikation durch ein Protokoll wie z.B. PKI–basiertes TLS (Dierks & Allen 1981) geschützt wird, welches die gegenseitige Authentisierung der Akteure und die Geheimhaltung der Kommunikation garantiert.
- Die Registrierungsphase verläuft korrekt.
- Der Wähler wird bei der Stimmabgabe nicht beobachtet.
- Bei der Stimmabgabe wird das Votum vom Endgerät des Wählers nicht verändert. Es wird genau das Votum erstellt, welches der jeweilige Wähler abgeben will.
- Der Wähler kann kein ungültiges Votum (d.h. falsche Struktur, fehlerhafte Verschlüsselung) erzeugen. Er hat jedoch die Möglichkeit, sich aktiv von der Wahl zu enthalten, z.B. durch eine entsprechende Option auf dem Wahlzettel.
- Der Wähler kennt weder den zum Blenden des Votums benutzten Faktor noch die für die Verschlüsselung seines Votums verwendeten Zufallszahlen.
- Dem Wähler wird das für ihn auf dem schwarzen Brett veröffentlichte verschlüsselte Votum innerhalb des Wahlvorgangs angezeigt.
- Dem Bestätiger wird wie folgt vertraut:
    - Er signiert nur Voten wahlberechtigter Wähler.
    - Er gibt seinen geheimen Schlüssel nicht preis.
    - Er trennt die Signatur des Wählers von dessen Votum ab.
    - Er konspiriert nicht mit anderen Akteuren.
- Dem schwarzen Brett wird wie folgt vertraut:
    - Es authentisiert die Akteure korrekt und autorisiert den Zugriff gemäß ihrer Rolle.
    - Es kann die Veröffentlichung von Informationen durch autorisierte Akteure nicht verweigern.
    - Es kann keine Informationen verändern oder löschen.
    - Es konspiriert nicht mit anderen Akteuren.

- Das Mix–Netz ist vertrauenswürdig in folgendem Sinne:
    - Es mischt korrekt.
    - Es gibt seinen geheimen Schlüssel oder die benutzte Permutation nicht preis.
    - Es verändert, löscht und dupliziert keine Voten.
    - Es konspiriert nicht mit anderen Akteuren.
- Die vertrauenswürdigen Akteure sind also:
    - Bestätiger
    - Schwarzes Brett
    - Mix–Netz
- Nicht notwendig vertrauenswürdig sind:
    - Wähler
    - Auszähler
- Ein gültiges Votum ist eines, das
    - die (technisch) korrekte Form hat,
    - vom Bestätiger signiert ist,
    - mit dem öffentlichen Schlüssel des Auszählers und des Mix–Netzes in der korrekten Reihenfolge verschlüsselt ist und
    - auf dem schwarzen Brett veröffentlicht ist.

3.5. Protokollbeschreibung

3.5.1. Registrierungsphase

Die Registrierungsphase liegt außerhalb des Protokolls. Wir verlangen nur, dass am Ende dieser Phase eine vom Wahlvorstand signierte Liste mit berechtigten Wählern und ihren Zertifikaten auf dem schwarzen Brett veröffentlicht ist. Diese Liste kann von jedem verifiziert werden.

3.5.2. Wahlphase

Schritt 0

Der Bestätiger holt die Liste der berechtigten Wähler vom schwarzen Brett. Dies wird einmalig zu Beginn der Wahlphase gemacht. Die folgenden Schritte 1-3 werden für jeden Wähler wiederholt.

Schritt 1

Der Wähler authentisiert sich beim schwarzen Brett und fordert den Stimmzettel an. Das schwarze Brett überprüft an Hand der Wählerliste, ob der Wähler wahlberechtigt ist. Es überprüft außerdem, ob der Wähler noch keine Stimme abgegeben hat. Sind beide Bedingungen erfüllt, erhält der Wähler einen Stimmzettel. Der Wähler füllt daraufhin den Stimmzettel aus und erzeugt so sein Votum v. Dann wird ein Blendfaktor r erzeugt, mit welchem der Wähler das Votum blendet, d.h. er berechnet $x = B(v,r)$. Der Wähler signiert x, authentisiert sich beim Bestätiger und übermittelt $(x, S_W(x))$.

Schritt 2

Der Bestätiger prüft die Wahlberechtigung des Wählers an Hand der Wählerliste und verifiziert dessen Signatur. Dann trennt der Bestätiger die Signatur des Wählers ab, signiert x und sendet $S_B(x)$ zurück zum Wähler.

Schritt 3

Der Wähler entfernt den Blendfaktor r und erhält die Bestätiger–Signatur $S_B(v)$ des Votums, welche er anschließend verifiziert. Ist diese korrekt, so verschlüsselt der Wähler das Votum v zusammen mit der Bestätiger–Signatur $S_B(v)$ mit dem öffentlichen Schlüssel des Auszählers, d.h. er berechnet $E_A(v, S_B(v))$. Dann verschlüsselt er das Ergebnis mit dem öffentlichen Schlüssel des Mix–Netzes. Das Ergebnis $E_M(E_A(v, S_B(v)))$ wird dem Wähler angezeigt. Der Wähler authentisiert sich beim schwarzen Brett und übermittelt $E_M(E_A(v, S_B(v)))$. Das schwarze Brett prüft, ob der Wähler wahlberechtigt ist und noch kein Votum abgegeben hat. Sind beide Bedingungen erfüllt, wird das doppelt verschlüsselte, signierte Votum $E_M(E_A(v, S_B(v)))$ auf dem schwarzen Brett abgelegt.

3.5.3. Misch- und Auszählphase

Schritt 4

Nach der Wahlphase holt sich das Mix–Netz die doppelt verschlüsselten Voten vom schwarzen Brett. Es entfernt die äußere Verschlüsselung der Voten mit seinem geheimen Schlüssel. Dann mischt es sie und legt die neue Liste wieder auf dem schwarzen Brett ab. Die Einträge der Liste haben nun die Form $E_A(v, S_B(v))$, d.h. die Voten sind noch immer mit dem Auszählerschlüssel verschlüsselt.

Schritt 5

Der Auszähler holt sich die Liste der einfach verschlüsselten Voten vom schwarzen Brett und entschlüsselt sie. Er verifiziert die Bestätiger–Signaturen der Voten und berechnet anschließend das Wahlergebnis.

Schritt 6

Schließlich veröffentlicht der Auszähler alle Voten v inklusiver ihrer Signaturen $S_B(v)$ auf dem schwarzen Brett. Dort veröffentlicht er außerdem seinen geheimen Schlüssel und das Wahlergebnis.

4. Analyse des Protokolls

4.1. Exaktheit

Ein abgegebenes Votum kann nicht dupliziert, gelöscht oder unberechtigt verändert werden.

Alle Voten sind ab dem Moment der Stimmabgabe signiert und verschlüsselt. Um ein Votum in ein anderes (gültiges) Votum zu ändern, müsste die Signatur und die Verschlüsselung gebrochen werden, was nach Voraussetzung praktisch unmöglich ist. Außerdem lässt das schwarze Brett keine unberechtigten Änderungen zu. Das Mix–Netz ist vertrauenswürdig und verändert, löscht oder dupliziert daher keine Voten. Bis zur Auszählung können außerdem keine Voten dupliziert werden, da auf Grund der probabilistischen Verschlüsselung Duplikate erkannt werden. Der Auszähler kann keine Voten unbemerkt verändern, löschen oder duplizieren, da sein geheimer Schlüssel am Ende der Wahl veröffentlicht wird. Nach dem Auszählen ist die Integrität der Voten weiterhin durch die Signatur des Bestätigers geschützt.

Alle gültigen Voten werden gezählt.

Nach Voraussetzung wird vom Endgerät des Wählers genau das Votum erstellt, welches dieser abgeben will. Die doppelt verschlüsselten Voten liegen auf dem vertrauenswürdigen schwarzen Brett, welches keine Voten löscht oder verändert. Da das Mix–Netz ebenfalls vertrauenswürdig ist, löscht oder invalidiert es keine Voten. Nach dem Mischen sind die Voten nur noch mit dem Auszählerschlüssel verschlüsselt. Ein betrügerischer Auszähler könnte die Voten entschlüsseln und ein gefälschtes Ergebnis veröffentlichen. Da jedoch der Auszähler in der Auszählphase seinen geheimen Schlüssel veröffentlichen muss, kann jeder nachprüfen, ob alle Voten korrekt ausgezählt wurden.

4.2. Demokratie

Nur berechtigte Wähler können ein Votum abgeben.

Nur Wahlberechtigte bekommen einen Stimmzettel ausgehändigt. Da der Bestätiger vertrauenswürdig ist, signiert er nur Voten berechtigter Wähler. Da das schwarze Brett vertrauenswürdig ist, weist es Voten nicht wahlberechtigter Personen zurück.

Jeder berechtigte Wähler gibt höchstens ein Votum ab.

Nur Wähler, die noch kein Votum abgegeben haben, bekommen einen Stimmzettel ausgehändigt. Das vertrauenswürdige schwarze Brett authentifiziert den Wähler und akzeptiert dessen Votum nur, wenn der Wähler noch kein Votum abgegeben hat.

4.3. Geheimhaltung

Es ist nicht möglich, ein Votum mit dem Wähler zu assoziieren, der es abgegeben hat.

Der Bestätiger kann den Inhalt des Votums nicht einsehen, da es geblendet ist. Der Bestätiger ist vertrauenswürdig und trennt die Signatur des Wählers von dessen Stimme ab. Der Wähler schickt sein Votum verschlüsselt an das schwarze Brett, d.h. der Inhalt des Votums ist nicht einsehbar. Jedes Votum bleibt bis zur Auszählung verschlüsselt.

Es ist nicht möglich, ein Votum durch Vergleichen des Wahlzeitpunktes und des Zeitpunktes, zu dem ein Votum auf dem schwarzen Brett erscheint, mit dem Wähler zu verknüpfen, da die Voten vor der Entschlüsselung gemischt werden. Um die Voten zu entschlüsseln, bevor sie gemischt werden, wäre die Kenntnis des geheimen Schlüssels des Mix–Netzes nötig. Da das Mix–Netz vertrauenswürdig ist, gibt es diesen nicht weiter.

Alle Voten bleiben bis zum Ende der Wahlphase geheim.

Die Voten sind doppelt mit den Schlüsseln des Mix–Netzes und des Auszählers verschlüsselt. Ein betrügerischer Auszähler könnte die Voten vor dem Mischen nicht offen legen, da diese dann noch mit dem Schlüssel des Mix–Netzes verschlüsselt sind. Da das Mix–Netz vertrauenswürdig ist, gibt es seinen geheimen Schlüssel nicht heraus. Gibt ein betrügerischer Auszähler seinen geheimen Schlüssel bereits vor Ende der Wahl an einen Angreifer heraus, so kann dieser die Voten entschlüsseln, sobald das Mix–Netz sie wieder auf das schwarze Brett abgelegt hat. Da zu diesem Zeitpunkt jedoch die Stimmabgabe bereits beendet ist, können hierdurch keine Zwischenergebnisse bekannt werden.

Kein Wähler kann beweisen, dass er ein bestimmtes Votum abgegeben hat.

Der Wähler kann sein Votum dem Bestätiger gegenüber nicht beweisen, da er nach Voraussetzung seinen Blendfaktor nicht kennt. Außerdem kennt der Wähler die Zufallszahlen nicht, welche für die Verschlüsselung des Votums verwendet wurden, und kann daher nicht nachweisen, dass sein Votum zu einem bestimmten Schlüsseltext verschlüsselt wurde, der auf dem schwarzen Brett zu sehen ist. Für die Quittungsfreiheit des Wahlsystems spielt es jedoch außerdem eine Rolle, ob deterministische oder probabilistische Signaturen verwendet werden (siehe Abschnitt 5.1).

Kein Wähler kann gezwungen werden, ein bestimmtes Votum abzugeben.

Das vorgestellte Protokoll erfüllt diese Anforderung nicht.

4.4. Verifizierbarkeit

Jeder kann verifizieren, dass alle gültigen Stimmen gezählt wurden.

Nach der Registrierungsphase ist eine Liste aller berechtigter Wähler auf dem schwarzen Brett veröffentlicht. Diese Liste erlaubt es jedem zu prüfen, wer wahlberechtigt ist. Außerdem können die zugehörigen Zertifikate verifiziert werden.

Sowohl die Liste der doppelt verschlüsselten Voten, als auch die Liste der einfach verschlüsselten Voten ist auf dem schwarzen Brett veröffentlicht. Daher kann jeder die Anzahl der Voten in beiden Listen vergleichen. Da schwarzes Brett und Mix–Netz vertrauenswürdig sind, werden von ihnen keine Voten verändert, gelöscht oder dupliziert.

Der Auszähler veröffentlicht seinen geheimen Schlüssel auf dem schwarzen Brett. Dies erlaubt es jedem, die Voten zu entschlüsseln und ihre Signaturen zu prüfen. Somit kann jeder verifizieren, dass alle gültigen Stimmen gezählt wurden.

Jeder Wähler kann verifizieren, dass seine gültige Stimme gezählt wurde.

Nach Voraussetzung kann der Wähler kein (technisch) ungültiges Votum erzeugen. Auf Grund der probabilistischen Verschlüsselung hat jedes verschlüsselte Votum eine eindeutige Form. Der Wähler kann demnach überprüfen, ob das auf dem schwarzen Brett veröffentlichte Votum demjenigen entspricht, welches er in der Wahlphase erstellt hat. Wie wir oben gesehen haben, ist es nachprüfbar, dass alle auf dem schwarzen Brett veröffentlichten gültigen Voten gezählt wurden. Hieraus folgt, dass jedes einzelne gültige Votum gezählt wurde.

5. Implementierungsfragen

Das Wahlsystem setzt eine PKI voraus. Jeder Akteur erhält für die Authentifizierung ein Schlüsselpaar und das entsprechende Zertifikat. Für die Verschlüsselung der Stimmen werden entsprechend zusätzliche Schlüsselpaare an Mix–Netz und Auszähler ausgegeben. Die Kommunikationskanäle zwischen Wähler und Bestätiger sowie zwischen Wähler und schwarzem Brett sind wechselseitig authentifizierte und verschlüsselte TLS/SSL-Verbindungen. Die Authentifizierung erfolgt durch die Verwendung der entsprechenden geheimen Schlüssel und Zertifikate der beteiligten Akteure in der Handshake-Phase des TLS/SSL-Protokolls.

Die probabilistische Verschlüsselung ermöglicht individuelle Verifizierbarkeit: Auf Grund der probabilistischen Verschlüsselung hat jedes verschlüsselte Votum eine eindeutige Form. Der Wähler kann dadurch überprüfen, ob sein in der Wahlphase verschlüsseltes Votum auf dem schwarzen Brett veröffentlicht ist. Ein Angreifer, der sich unberechtigten Zugriff auf das schwarze

Brett verschafft, kann dementsprechend auch keine verschlüsselten Stimmen unerkannt duplizieren.

5.1. Wahl des Signaturschemas

Probabilistische Signaturen

Sind die Voten mit probabilistischen Signaturen des Bestätigers versehen, so kann ein betrügerischer Auszähler keine Voten duplizieren (und gleichzeitig andere löschen, um die Gesamtanzahl nicht zu verändern). Dies würde auffallen, da mehrere Voten die gleiche Signatur hätten. Hinzufügen neuer Stimmen wäre dem Auszähler ebenfalls nicht möglich, da er hierfür die Signatur fälschen müsste. Damit bräuchte auch der geheime Schlüssel des Auszählers nicht veröffentlicht zu werden, um dessen korrekte Arbeitsweise überprüfen zu können.

Es wäre in diesem Fall sogar möglich, ganz auf den Auszähler zu verzichten und das Auszählen dem Mix–Netz zu überlassen. Der Wähler würde also seine vom Bestätiger signierte Stimme nur mit dem öffentlichen Schlüssel des Mix–Netzes verschlüsseln und dann an das schwarze Brett schicken. Das Mix–Netz müsste dann (bis auf die Herausgabe des geheimen Schlüssels) auch nicht mehr vertrauenswürdig sein, denn man könnte seine korrekte Funktionsweise überprüfen: Die vom Mix–Netz ausgegebenen Stimmen würden im Klartext vorliegen und wären auf Grund der probabilistischen Signatur eindeutig, d.h. man würde Duplikate erkennen. Neue Stimmen könnte das Mix–Netz nicht erzeugen, da es dafür die Signatur des Bestätigers fälschen müsste; nach Voraussetzung ist dieser jedoch vertrauenswürdig und gibt seinen geheimen Schlüssel nicht preis. Das Mix–Netz könnte auch keine Stimmen löschen, da dies durch Vergleichen der Anzahl der Voten vor und nach dem Mischen auffallen würde. Da man dem Mix–Netz nur noch hinsichtlich der Geheimhaltung seines geheimen Schlüssels vertrauen müsste, würde das Protokoll eine stärkere Form der Verifizierbarkeit bieten.

Der große Nachteil dieses Ansatzes ist jedoch, dass es dem Wähler durch die probabilistische Signatur der Stimme einfach gemacht würde, seine Stimme zu verkaufen. Er bräuchte dem Angreifer lediglich die signierte Klartextstimme zu zeigen, die er in der Wahlphase verschlüsselt hat. Der Angreifer könnte sich mit Hilfe des schwarzen Bretts dann davon überzeugen, dass der Wähler diese Stimme auch tatsächlich abgegeben hat.

Deterministische Signaturen

Falls für die Bestätiger-Signaturen der Voten ein deterministisches Signaturverfahren eingesetzt wird, könnte der Auszähler nach der Entschlüsselung signierte Klartextvoten unbemerkt löschen und duplizieren. Wenn sich die Gesamtanzahl der Voten dadurch nicht ändert, könnte diese Manipulation nicht entdeckt werden. Diesem Problem beugt das Protokoll vor, indem der geheime Schlüssel des Auszählers nach der Auszählung veröffentlicht wird, da dann die Auszählung öffentlich nachvollzogen und verifiziert werden kann. Die Auszählung kann in diesem Fall nicht durch das Mix–Netz erfolgen. Dessen Schlüssel darf nicht veröffentlicht werden, da dann der Vorgang des Mischens öffentlich rückgängig gemacht werden könnte.

Ein Vorteil der deterministischen Signatur ist, dass sie die Quittungsfreiheit des Wahlsystems stärkt. Das signierte Klartextvotum kann vom Wähler nicht als Beweis für die Stimmabgabe verwendet werden, da die Signatur nicht einzigartig ist und das Votum dem Wähler somit nicht eindeutig zuzuordnen ist. Es ergibt sich dadurch allerdings auch ein Angriffszenario. Da die deterministische Signatur der Klartextvoten nicht einzigartig ist, können diese signierten Voten dupliziert werden. Ein Angreifer könnte duplizierte signierte Klartextvoten in das Wahlsystem einschleusen, indem er sich unberechtigten Zugriff zum schwarzen Brett verschafft. Der Angreifer kann signierte Klartextvoten auf zwei Wegen erhalten. Entweder zwingt er andere Wähler dazu, sich entsprechende Voten vom Bestätiger signieren zu lassen und sie dann dem Angreifer auszuhändigen. Oder der Angreifer ist selbst Wähler und lässt sich beim Bestätiger beliebige Voten signieren. Um die Problematik im letzteren Fall einzugrenzen, wäre es sinnvoll, pro Wähler

nur eine Stimme vom Bestätiger signieren zu lassen. Der Wähler kann jedoch dann seine Wahlentscheidung nach dem Signieren nicht mehr ändern.

Die Wahl eines probabilistischen oder deterministischen Signaturverfahrens sollte daher in Abhängigkeit der Anforderungen des Wahlszenarios getroffen werden. Falls Quittungsfreiheit besonders wichtig ist, sollten deterministische Signaturen verwendet werden. Falls eine starke Verifizierbarkeit gefordert ist und Quittungsfreiheit vernachlässigbar ist, sollten probabilistische Signaturen verwendet werden.

6. Schluss

Wir haben wir ein PKI–basiertes Protokoll für sichere Onlinewahlen vorgestellt. Ziel war es dabei, eine effiziente Implementierung des Wahlsystems zu ermöglichen.

Wir haben den Bestätiger, das schwarze Brett und das Mix–Netz als vertrauenswürdig vorausgesetzt. Im Gegenzug muss den Wählern und dem Auszähler nicht vertraut werden. Bei Einsatz eines probabilistischen Signaturschemas kann das Mix–Netz die Auszählung übernehmen, ohne vertrauenswürdig sein zu müssen; allerdings mit dem Nachteil, dass der Wähler seine Stimme dann auf Grund der probabilistischen Signaturen beweisen kann. Im Hinblick auf die Quittungsfreiheit haben wir angenommen, dass dem Wähler bestimmte Informationen verborgen bleiben (Blendfaktor und Zufallszahlen). Dies muss durch eine entsprechend sichere Implementierung gewährleistet werden.

Wir beschränken uns auf Standardverfahren und –primitive und ermöglichen so eine einfache Integration in bestehende IT–Infrastrukturen. Durch den Verzicht auf komplizierte Beweisverfahren bietet das Protokoll Benutzerfreundlichkeit und Effizienz, erfordert gleichzeitig aber auch vertrauenswürdige Komponenten. In Wahlszenarien, bei denen eine stärkere Verifizierbarkeit gefordert wird, können komplexere Primitive wie beispielsweise verifizierbare Mix–Netze (Neff, 2001) eingesetzt werden.

Abschnitt 4 hat gezeigt, dass die wichtigsten Sicherheitsanforderungen durch das vorgeschlagene Protokoll erfüllt werden. Fortgeschrittene Sicherheitsanforderungen wie Quittungsfreiheit und Unzwingbarkeit sind mit dem Protokoll nur bedingt bzw. gar nicht zu erreichen. Hierfür wären komplexere Primitive nötig, auf die jedoch bewusst verzichtet wurde.

Literatur

Benaloh, J. D. C. (1987). *Verifiable secret-ballot elections*. PhD thesis, Yale University, New Haven, CT, USA.

Burmester, M. & Magkos, E. (2003). Towards secure and practical e-elections in the new era. In Gritzalis, D. (Ed.), *Secure Electronic Voting*, Chapter 5, Volume 7 of Advances in Information Security. Kluwer Academic Publishers.

Cetinkaya, O. (2007). *Verifiability and Receipt-freeness in Cryptographic Voting Systems*. PhD thesis, Middle East Technical University, Ankara, Turkey.

Cohen, J.D. & Fischer, M. J. (1985). A robust and verifiable cryptographically secure election scheme. *FOCS '85: Proceedings of the 26th Annual Symposium on Foundations of Computer Science*. Washington, DC, USA: IEEE Computer Society, 372–382.

Chaum, D. (1981). Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms. *Communications of the ACM, 24(2),* ACM, 84–88.

Chaum, D. (1983). Blind Signature System. In Chaum, D. (Ed.), *Advances in Cryptology: Proceedings of Crypto '83.* Plenum Publishing, 153–156.

Dierks, T. & Allen, C. (1981). The TLS Protocol. *IETF RFC 2246*. Retrieved April 1, 2010, from http://www.ietf.org/rfc/rfc2246.txt.

Hirt, M. (2001). *Multi-Party Computation: Efficient Protocols, General Adversaries, and Voting*. PhD thesis, ETH Zurich. Reprint *ETH Series in Information Security and Cryptography*, Volume 3, Konstanz: Hartung-Gorre Verlag.

Juels, A. & Catalano, D. & Jakobsson, M. (2005). Coercion-resistant electronic elections. In Atluri, V., Capitani di Vimercati, S. De & Dingledine, R. (Eds.), *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society (WPES),* ACM, 61–70.

Lambrinoudakis, C. & Gritzalis, C. & Tsoumas, V. & Karyda, M. & Ikonomopoulos, S. (2003). Secure electronic voting: The current landscape. In Gritzalis, D. (Ed.), *Secure Electronic Voting*, Chapter 7, Volume 7 of Advances in Information Security. Kluwer Academic Publishers, Boston, USA.

Neff, Andrew C. (2001). A verifiable secret shuffle and its application to e-voting. In Samarati, P. (Ed.), *Proceedings of the 8th ACM conference on Computer and Communications Security*, ACM, 116–125.

Ohkubo, M. & Miura, F. & Abe, M. & Fujioka, A. & Okamoto, T. (1999). An Improvement on a Practical Secret Voting Scheme. In Mambo, M. & Zheng, Y. (Eds.), *Second International Workshop on Information Security (ISW)*, Lecture Notes in Computer Science, Volume 1729, Springer, 225–234.

Riera, A. (1998). *An Introduction to Electronic Voting Schemes*. Technical Report PIRDI 9-98, Universitat Autònoma de Barcelona, Spain. Retrieved April 1, 2010 from http://pirdi.uab.es/document/pirdi9.ps.

Rivest, R. L. & Shamir, A. & Adleman, L. M. (1978). A Method for Obtaining Digital Signatures and Public–Key Cryptosystems. *Communications of the ACM*, *21(2),* ACM, 120–126.

Über die Autoren

Lucie Langer

Lucie Langer ist seit Abschluss ihres Mathematikstudiums wissenschaftliche Mitarbeiterin am Lehrstuhl von Prof. Johannes Buchmann am Fachgebiet Theoretische Informatik der Technischen Universität Darmstadt. Sie forscht auf dem Gebiet der Verifizierbarkeit und langfristigen Sicherheit elektronischer Wahlen und hat an verschiedenen Projekten zur elektronischen Identität und zur Langzeitarchivierung elektronischer Daten mitgewirkt.

Axel Schmidt

Axel Schmidt studierte Mathematik und arbeitet als Wissenschaftler im Fachgebiet für Kryptographie und Computeralgebra an der Technischen Universität Darmstadt in Deutschland. Sein Forschungsbereich umfasst die Sicherheit von elektronischen Wahlen, Trust Modeling und IT-Evaluationsmethoden. Er arbeitete außerdem an zahlreichen Projekten im Bereich E-Voting, E-Card Security und E-Identity.

Melanie Volkamer

Melanie Volkamer studierte an der Universität des Saarlandes Informatik. Sie promovierte im Oktober 2008 an der Universität Koblenz. Melanie Volkamer präsentierte ihre Arbeit bei zahlreichen eVoting Konferenzen und Veranstaltungen, war/ist Mitglied verschiedener Beratungsgremien rund um das Thema elektronische Wahlen; insbesondere war sie als OSCE Wahlbeobachterin bei der ersten landesweiten Internetparlamentswahl in Estland und war Sachverständigende beim Bundesverfassungsgericht. Sie ist Co-Autorin von zwei vom BSI zertifizierten Common Criteria Schutzprofilen. Seit Dezember 2008 arbeitet Sie als Post Doc an der technischen Universität Darmstadt und koordiniert bei CASED (www.cased.de) den Arbeitsbereich "Sichere Daten".

Johannes Buchmann

Prof. Dr. Johannes Buchmann ist Direktor von CASED und Leiter der Arbeitsgruppe für Kryptographie und Computeralgebra am Fachbereich Informatik der TU Darmstadt. Als Experte auf dem Forschungsgebiet der Kryptographie hat er zahlreiche wissenschaftliche Aufsätze sowie mehrere Fachbücher publiziert. Er ist in verschiedenen wissenschaftlichen und redaktionellen Beiräten sowie als wissenschaftlicher Gutachter tätig. Unter anderem ist Prof. Dr. Johannes Buchmann Mitglied des Kuratoriums des Fraunhofer-Instituts SIT.