E-Voting – Risiko oder Chance?

Abstimmen und Wählen mit dem Stimmzettel im Wahllokal ist einfach und sicher. Um die gleiche Sicherheit bei der elektronischen Umsetzung zu erreichen, muss aufwändige Kryptographie eingesetzt werden. Im Gegenzug wird das Abstimmungs- und Wahlverfahren für die Stimmbürgerinnen und Stimmbürger transparenter.

Prof. Dr. Eric Dubuis
RISIS, E-Voting Group
Foto: www.arteplus.ch ?

Prof. Dr. Stephan Fischli
RISIS, E-Voting Group
Foto: Kathrin Blumenthal?

Prof. Dr.Rolf Haenni
RISIS, E-Voting Group
Foto: www.arteplus.ch

Die rasanten Entwicklungen der Informationstechnologien verändern viele Bereiche des täglichen Lebens. Sie betreffen zunehmend auch den Informationsaustausch zwischen Bürgern und Behörden. Vor diesem Hintergrund hat man sich in der Schweiz vor Jahren entschlossen, das Abstimmen und Wählen zukünftig auch mittels elektronischer Verfahren anzubieten. In den Kantonen Genf, Neuenburg und Zürich wurden drei E-Voting-Pilotprojekte gestartet, die mehrfach bei Abstimmungen und Wahlen eingesetzt wurden. Die Schweiz nimmt damit weltweit eine Pionierstellung ein.

Einfache Anforderungen – einfacher Prozess

Das Wählen und Abstimmen gehört zu den Grundrechten der Bürgerinnen und Bürger einer Demokratie und ist in entsprechenden Verfassungs- und Gesetzestexten verankert. Aus diesen ergeben sich folgende Grundprinzipien:

- Nur berechtigte Personen dürfen stimmen.
- Eine berechtigte Person kann maximal eine Stimme abgeben.
- Jede korrekt abgegebene Stimme wird gezählt.
- Die Stimme ist geheim.
- Das Resultat bleibt bis zum Ende der Wahl oder Abstimmung geheim.

Diese Grundprinzipien lassen sich mit Papier und dem klassischen Wahllokal einfach bewerkstelligen. Der Ablauf, welcher von Wahlbeobachtern oder interessierten Stimmbürgern überwacht werden kann, lässt sich in drei Phasen aufteilen:

- In der ersten Phase werden mit dem Stimmregister die Stimmberechtigten festgelegt, die Stimmausweise gedruckt und den Stimmbürgerinnen und -bürgern verschickt.
- In der zweiten Phase geben die Stimmberechtigten ihre Stimme im Wahllokal ab (siehe Abbildung 1). Dabei belegt der Stimmausweis, dass eine Person berechtigt ist, an der Wahl teilzunehmen. Das Stimmgeheimnis wird durch das Ausfüllen des Stimmzettels in der Wahlkabine gewahrt, und der Wahlhelfer bei der Urne garantiert schliesslich, dass jede bzw. jeder Stimmberechtigte nur eine Stimme in die Urne legt.
- Nach Ablauf des Wahl- oder Abstimmungsvorgangs wird durch die Mitglieder der Wahlkommission der Inhalt der Urne gezählt und das Ergebnis publiziert.

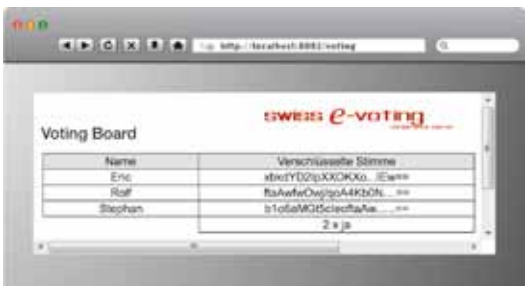

Abbildung 3
Bei dieser Variante des Anschlagbretts wird die verschlüsselte Stimme mit dem Namen des/der Abstimmenden veröffentlicht. Dank der homomorphen Verschlüsselung bleibt aber die Stimme für immer verschlüsselt. Am Ende wird nur die Summe der verschlüsselten Stimmen entschlüsselt und publiziert.

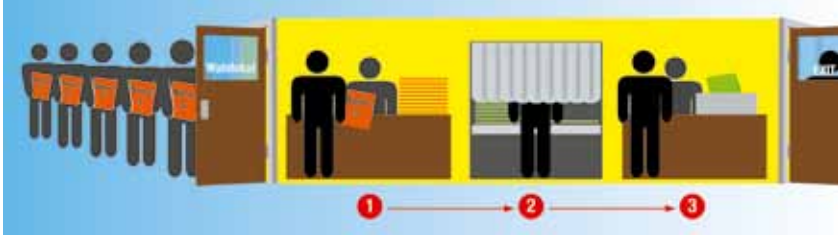

Abbildung 1
Der/die Stimmberechtigte gibt den Stimmausweis dem Wahlhelfer ab (1). Danach geht er/sie in die Wahlkabine (2), füllt einen leeren Stimmzettel aus, faltet ihn und verlässt die Wahlkabine. Er/sie geht zur Urne und legt den Stimmzettel hinein (3) und verlässt danach das Wahllokal.
Grafiken:
E-Voting Group

Mit dem Internet wird es viel schwieriger

Das Abstimmen übers Internet macht alles viel komplizierter. Wir greifen zwei Probleme heraus. Das erste ist die scheinbare Unvereinbarkeit des Stimmgeheimnisses mit der Forderung, dass nur berechtigte Personen stimmen dürfen. Denn um letzteres zu erreichen, muss das Wahlsystem den Stimmbürger zuerst eindeutig identifizieren. Das Wahlsystem «kennt» also den Stimmbürger oder die Stimmbürgerin und kann somit die abgegebene Stimme mit der entsprechenden Identität verknüpfen. Gerade dies muss aber verhindert werden, um das Stimmgeheimnis zu wahren. Wie aber kann man die Identität der Stimmberechtigten von der jeweiligen Stimme entkoppeln?
Das andere Problem ist, dass das Wahlsystem und seine Betreiber erst in der dritten Phase wissen dürfen, welche Stimmen abgegeben wurden. Dies bedeutet, dass bis zu diesem Zeitpunkt die Stimmen verschlüsselt bleiben müssen. Wie kann dies sichergestellt werden, und welche Schlüssel sollen dafür verwendet werden?

Ein Ziel – zwei Lösungsansätze

Für diese Probleme gibt es zwei Lösungsansätze. Der erste wurde bei den in der Schweiz eingesetzten Wahlsystemen verfolgt: Man baut ein Wahlsystem, betreibt es an einem sicheren Ort, und die Stimmberechtigten bringen den Betreibern das entsprechende Vertrauen entgegen.
Beim anderen Lösungsansatz wird fortschrittlichste Kryptographie eingesetzt. Damit kann man nicht nur die obigen Probleme lösen, sondern zusätzlich Transparenz für die Stimmberechtigten schaffen. Wir unterscheiden zwei verschiedene Verfahren:

- Beim Verfahren mittels blinder Signaturen (Siehe Kasten «Blinde Signatur») erzeugt der/die Stimmberechtigte ein geheimes Pseudonym und lässt es von der Wahlbehörde blind signieren. Im zweiten Schritt verschlüsselt der/die Stimmberechtigte die Stimme und schickt sie, zusammen mit dem signierten Pseudonym, an die öffentlich einsehbare Urne; den Schlüssel schickt er/sie an den Kollektor (eine Art Schlüsselbrett). Am Ende des Wahlvorgangs werden die Stimmen mit den Schlüsseln des Kollektors entschlüsselt und gezählt. Das Ergebnis kann von allen Beteiligten verifiziert werden (Abbildung 2).
- Beim Verfahren mittels homomorpher Verschlüsselung (Siehe Kasten «Homomorphe Verschlüsselung») macht man sich erst gar nicht die Mühe, die Stimme vom Stimmenden zu trennen. Die Stimme wird vom Stimmenden verschlüsselt – und bleibt verschlüsselt, auch beim Zählen (Abbildung 3)!

Stand unserer Arbeiten und Ausblick

Im Projekt TrustVote entwickelten wir einen Prototyp auf der Basis der blinden Signaturen. Eine Weiterentwicklung soll den Einsatz für eine reale Abstimmung (z.B. eine studentische Wahl im Kontext einer Hochschule) ermöglichen. Gegenwärtig befassen wir uns mit den homomorphen Verfahren. Unser Ziel ist, diese praktisch umzusetzen und in zukünftige Wahlsysteme einfliessen zu lassen ■

Kontakt:
> eric.dubuis@bfh.ch
> Infos: www.e-voting.ti.bfh.ch

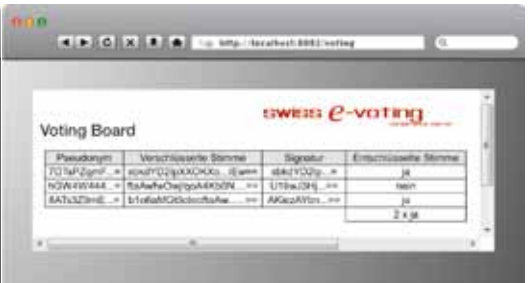

Abbildung 2
Nach Abgabe ihrer Stimme übers Internet können die Stimmberechtigten das öffentliche Anschlagbrett mit ihrem Browser anschauen. Dort findet jedermann sein Pseudonym und seine verschlüsselte Stimme. Die Spalte «Entschlüsselte Stimme» ist noch leer. Die Signaturen der Wahlbehörde garantieren, dass nur Stimmen von Stimmberechtigten auf dem Anschlagbrett vorhanden sind. Nach der Abstimmung werden die Stimmen mit den Schlüsseln des Kollektors entschlüsselt, und jedermann kann das Ergebnis ermitteln.

Blinde Signaturen

Möchte jemand ein Dokument signieren lassen, ohne dessen Inhalt preiszugeben, so steckt er das Dokument mit einem Durchschlagpapier in einen verschlossenen Umschlag und lässt diesen signieren. Das Durchschlagpapier bewirkt, dass die Unterschrift auf das Dokument übertragen wird, sodass nach dem Entfernen des Umschlags das signierte Dokument vorliegt. In der Kryptographie wird dieses Prinzip durch sogenannte «blinde Signaturen» nachgebildet. Dabei wird zunächst eine «Verblindung» durchgeführt, welche das zu signierende Dokument unkenntlich macht (entspricht dem Umschlag). Dann wird das «verblindete» Dokument signiert. Durch das «Entblinden» (Entfernen des Umschlags) erhält man das mit der Unterschrift versehene Dokument zurück.

Homomorphe Verschlüsselung

Um das Gewicht von zwei Äpfeln zu bestimmen, kann man entweder beide Äpfel einzeln wägen und die Gewichte zusammenzählen, oder man kann beide Äpfel gemeinsam auf die Waage legen. Beim Wägen von Äpfeln handelt es sich also um eine «additiv homomorphe Funktion», bei welcher es keine Rolle spielt, ob man zuerst die Funktion berechnet und dann zusammenzählt oder zuerst zusammenzählt und dann die Funktion berechnet. In der Kryptographie gibt es Verschlüsselungsfunktionen, die genau diese Eigenschaft besitzen. Diese kann man verwenden, um die Summe von verschlüsselten Zahlen zu bestimmen, ohne die einzelnen Zahlen zu entschlüsseln.