Sicherheitstheoretische Aspekte bei elektronischen Wahlen

Gerald Fischer, Wolfgang Zuser

Forschungsgruppe Industrielle Software
Technische Universität Wien
Karlsplatz 13, 1040 Wien
{gerald.fischer, wolfgang.zuser}@inso.tuwien.ac.at

Schlagworte: eVoting, elektronische Wahlen, Internetwahlen, Onlinewahlen, Kryptographie, geheime Wahl, Übertragungssicherheit

Abstract: Es wird ein Algorithmus zur Steigerung der Übertragungssicherheit bei elektronischen Wahlen vorgestellt. Die abgegebenen Stimmen werden dabei so verändert, dass sie unabhängig von der eigentlichen Stimmverteilung einer Gleichverteilung unterliegen. Der Algorithmus ist universell in vorhandenen und geplanten Wahlsystemen einsetzbar.

1. Einleitung

Eines der größten Probleme bei Onlinewahlen stellt die mangelnde *nachhaltige* Sicherheit der verwendeten kryptographischen Verfahren dar. Gängige Systeme wie zB: RSA[1] bieten zum heutigen Zeitpunkt den höchsten bekannten Grad an Sicherheit, sind aber von der Länge der verwendeten Schlüssel und dem Fehlen von schnellen Algorithmen, zB zur Primfaktorzerlegung, abhängig. Weiters bieten Systeme basierend auf solchen kryptographischen Verfahren keinen Schutz vor Manipulationen auf dem Wahl-PC (zB durch Trojaner) vor der eigentlichen Übertragung der Stimme.

Bei Onlinewahlen ist aber ein nachhaltiger Schutz der Daten über eine beliebig lange Zeitdauer notwendig. Das mögliche Entschlüsseln der Stimme eines Wählers, auch Jahre nach Ablauf der Wahl, stellt einen Eingriff in das verfassungsmäßige Recht der geheimen Wahl dar. Das einzige kryptographische Verfahren, das diesen Anforderungen genügt, ist das one-time pad. Der hier vorgestellte Algorithmus bietet die Sicherheit eines one-time pads bei Onlinewahlen.

---

[1] *Rivest, Shamir, Adlemann:* A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM 21/120-126, Februar 1978.

2. Der „Vote scrambling algorithm“ (VSA)

Ausgehend von der Forderung nach einem Algorithmus, der kurze Nachrichten (zB Stimmen) am Übertragungsweg nachhaltig schützt und es unmöglich macht, deren Inhalt auch nach intensiver und zeitlich unbegrenzter Berechnung zu entschlüsseln, wurde der „Vote Scrambling Algorithm“ (VSA) entwickelt.

Stimmen, die mittels VSA kodiert werden, sind von unverschlüsselten Stimmen nicht zu unterscheiden. Bei einem Versuch, ihren wahren Inhalt zu berechnen, liefern sie als Ergebnis eine weitere gültige Stimme, wobei die Wahrscheinlichkeit für die Korrektheit des Ergebnisses immer 1 / Anzahl der möglichen Stimmen beträgt.

Weiters unterliegen die übertragenen Stimmen bei vollständiger Umsetzung des VSA immer einer Gleichverteilung und zwar unabhängig von der eigentlichen Stimmverteilung. Somit bleiben auch die in der Kryptoanalyse oft zur Entschlüsselung verwendeten Häufigkeitsanalysen erfolglos.

2.1. Funktionsweise des VSA

Alle WählerInnen erhalten vor Beginn jeder Wahl eine Zufallszahl SK (Scrambling Key). Die Anzahl der zur Wahl stehenden Parteien wird im Folgenden mit EP (Electoral Parties) bezeichnet. Die Zufallszahl SK ist aus dem Intervall [0..EP-1] zu wählen. Die mit der Ausgabe der SK betraute Stelle muss sicherstellen, dass alle Elemente aus dem Intervall [0..EP-1] gleich oft vergeben werden.

Zur Umwandlung der Stimme wird der ganzzahlige Divisionsrest (Modulus) verwendet. Die verschlüsselte Stimme SV (Scrambled Vote) wird aus der Stimme V (Vote) folgendermaßen berechnet:

SV = (V + SK) Modulo EP

Die Wahlurne kennt die jeweilige SK der WählerIn und berechnet den eigentlichen Wert der Stimme mittels:

V = (SV - SK) Modulo EP

Man kann zeigen, dass Stimmen, die nach diesem Verfahren kodiert werden, immer einer Gleichverteilung unterliegen. Der vollständige Beweis ist als Technical Report verfügbar[2].

---

[2] http://www.inso.tuwien.ac.at/publications/.

2.2. Beispiel: Nationalratswahl in Österreich 2002

Die abgegebenen Stimmen der Nationalratswahl 2002 wurden mittels des VSA kodiert, um die daraus resultierende Stimmverteilung vor der Übertragung der einzelnen Stimmen zu zeigen:

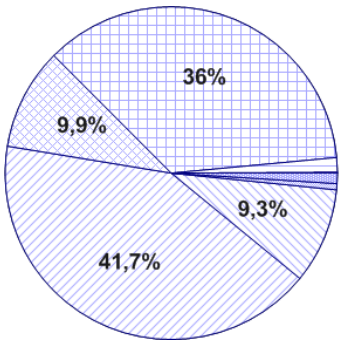

Abb 1

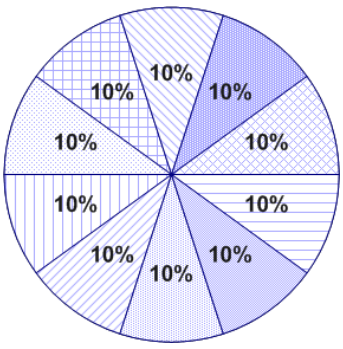

Abb 2

Abb 1 zeigt die tatsächliche Verteilung der Stimmen zwischen den Parteien, wobei aus Platzgründen auf die Beschriftung verzichtet wurde. Abb 2 zeigt die Gleichverteilung der Stimmen nach Anwendung des VSA.

3. Anwendungsmöglichkeiten des VSA

Der vorgestellte Algorithmus eignet sich zur Anwendung in jedem Wahlsystem, da er aus einer gültigen Stimme wieder eine gültige Stimme berechnet. Eine Einbettung in vorhandene Wahlsysteme ist durch diese Eigenschaften ebenfalls möglich und dient dazu, die Übertragungssicherheit zu erhöhen.

Da die im VSA verwendeten Rechenoperationen auch auf einfacher Hardware schnell abgearbeitet werden können, ist ein Einsatz auf Chipkarten ebenso denkbar wie eine eigene Hardwareimplementierung, die den WählerInnen zur Verfügung gestellt wird. Dazu ist ein Gerät denkbar, das die Stimmenerzeugung mit Hilfe von SK und EP ermöglicht. Dieses Gerät, VSD (Vote Scrambling Device), führt nach Eingabe der gewünschten Partei, SK und EP die Verschlüsselung der

Stimme durch und gibt die verschlüsselte Stimme auf einem Display aus.

Die mit dem VSD erzeugte Stimme kann nun vom Wähler direkt an Stelle seiner ursprünglichen Stimme in die Wahlapplikation eingetragen werden, wodurch möglicherweise am Wahlcomputer vorhandene Trojaner keine Information über die Originalstimme erhalten.

4. Weitere Eigenschaften des VSA

Die Laufzeit kann – verglichen mit den notwendigen kryptographischen Verfahren bei elektronischen Wahlen – als vernachlässigbar eingestuft werden, da eine ganzzahlige Addition und eine Moduloperation ausreichen, um eine verschlüsselte Stimme zu erzeugen.

Die Gleichverteilung der übertragenen Stimmen ist eine zentrale Eigenschaft des VSA, denn dadurch ist ein Dekodieren der Stimmen durch Dritte nicht möglich. Der VSA erfüllt die Äquivalenz mit dem one-time pad, da ohne den richtigen Schlüssel alle berechneten Ergebnisse gleich wahrscheinlich sind. Ein potentieller Angreifer erhält bei einem Versuch, den Inhalt zu berechnen, keine Information darüber, ob der Versuch erfolgreich war.

Der VSA kann aber auch in einer hybriden Form (dh nur ein Teil der abgegebenen Stimmen wird mittels VSA kodiert) eingesetzt werden. Der korrekte Rückschluss auf den Inhalt einer einzelnen Stimme ist weiterhin nicht möglich.

Die Anwendung des VSA ersetzt nicht die Verwendung von kryptographischen Verfahren wie zB RSA oder ECC zum Signieren und Kodieren von Stimmen. Der VSA stellt eine Steigerung der Übertragungssicherheit auf one-time pad Niveau dar.

Größtmögliche Sicherheit bei Onlinewahlen bietet der VSA in Kombination mit externer Hardware (zB VSD), da die eigentliche Stimme bis zum Dekodieren in der Wahlurne nicht berechnet werden kann. Dies macht es auch lange Zeit nach der Wahl unmöglich, den Inhalt einzelner Stimmen zu eruieren und garantiert dadurch das Grundrecht der geheimen Wahl.