MOVK_SW11_Exercises_Maurin

December 10, 2018

1 Aufgaben Serie 11 - eVoting

1.1 Lernzielkontrolle

1. Nennen Sie 2 Grunde fur das Projekt "eVoting" in der Schweiz?
2. Warum ist die Verwendung von blinden Signaturen in einem Wahlprotokoll wichtig?
3. Warum ist die Zahl x (gewählt vom stimmberechtigten Burger) von bestimmter Struktur fur eVoting mit asymmetrischem Verfahren-RSA?
4. Ist ein eVoting-System basiert auf Paillier-Verfahren skalierbar? Warum?

1.1.1 Antworten

1. Auslandsschweizer können einfacher abstimmen, mehr Leute dazu überreden, überhaupt abzustimmen
2. Vertraulichkeit und Geheimhaltung der Abstimmungsergebnisse gewährleisten
3. Damit wir sicher sind, dass die öffentlichen Schlüssel, welche der Wahlbehörde zugesendet werden, garantiert ein Stimmzettel sind. Die öffentlichen Schlüssel müssen also diese spezielle Struktur vorweisen, damit sie eindeutig als Wahlzettel identifiziert sind.
4. Begrenzt oder nicht skalierbar, da Ergebnisse nur in binär angegeben werden können.

1.2 Aufgabe 1 - Digitale Demokratie

Lesen Sie die der Aufgabe zugehörigen Dokumente und beantworten Sie die folgenden Fragen:

1. ***Trägt das eVoting zur Demokratie bei? Begrunden Sie Ihre Antwort.***
2. ***Vergleichen Sie das eVoting-Projekt in Estland und in der Schweiz.***

Antworten:

1. Bei eVoting hofft man vorallem auf eine höhere Wahlbeteiligung, dadurch auf eine Steigerung der Systemlegimitation. Je nach Staat ist der Anstieg der Wahlbeteiligten bisher jedoch nicht merklich gross. Man will in Zukunft auch die jüngere Bevölkerung dazu animieren, öfter abzustimmen. Durch längere Erfahrungen gelangte man grösstenteils jedoch bereits zur Ansicht "Wer wählen will, der geht auch wählen, sei es nun offline oder online". Der Vorteil, den Wahl- oder Abstimmungsprozess mittels dem Internet zu vereinfachen, ist klar ersichtlich, jedoch ist beispielsweise in der Schweiz der landesweite Zweifel an der Sicherheit der eVoting-Systeme zu gross, als dass man dies komplett in staatliche Abstimmungen und Wahlen einführen könnte. Ob sich die Vorteile des eVoting für

die Demokratie gegen die Nachteile aufwiegen können, kann bisher nicht definitiv gesagt werden. Das Risiko der Manipulation ist bisweilen noch zu hoch, um daher eine definitive Aussage machen zu können.

2. In der **Schweiz** wird von den Betreibern ein Schlüsselpaar aus öffentlichem und privatem Schlüssel erzeugt. Alle öffentlichen Schlüssel werden kombiniert und allein für eine Gruppe von Spezialisten der Wahlkommission und ausgewählte Dritte zugänglich gemacht. Die Stimmberechtigten erhalten Zugangs- und Prüfcodes per Post, loggen sich mit dem Zugangscode ein und geben ihren Stimmzettel ab. Zusammen mit dem kombinierten Schlüssel wird der Stimmzettel E2E-verschlüsselt und abgesendet. Im System wird daraus ein Prüfcode generiert, welcher mit dem des Stimmberechtigten verglichen wird. Stimmen werden erst in der Auszählphase verschlüsselt, zuvor werden sie durch "kryptographisches Mischen" voneinander getrennt $\rightarrow$ Stimmgeheimnis In **Estland** wiederum wird zur Identifizierung der Wahlberechtigten der Personalausweis verwendet, welcher mit einer digitalen Signatur ausgestattet ist. Der Chip darauf ermöglicht es, sich mit einem speziellen Kartenlesegerät einzuloggen und die Identifizierung mit Eingabe eines PINs abzuschliessen. Ein zweiter Code dient als digitale Unterschrift zur Bestätigung der Stimmabgabe, danach ist die Stimme eingegeben. Es ist aber möglich, seine Stimme im Nachhinein noch abzuändern oder via Stimmzettel abzustimmen (wobei letzteres die ultimative Gültigkeit hat). Die Lösung von Estland hat sich nun bereits seit 2007 etabliert, wohingegen das Schweizer Projekt sich erst noch weiterhin beweisen muss. Ob dies mit der bisherigen moralischen Einstellung gegenüber dem eVoting in der Schweiz überhaupt behaupten kann, bleibt in den nächsten Jahren noch zu bezweifeln.

1.3 Aufgabe 2 - Wahlprotokoll mit symmetrischer Verschlusselung

Wir betrachten zwei Wählerinnen Alice und Eve. Am Ende des symmetrischen eVoting Protokolls mit blinder Signatur (bitte s. in der Vorlesungsfolien) möchte Eve ermitteln, wie Alice gewählt hat. Kann Sie es? Begrunden Sie Ihre Antwort.

Antwort:

Nein, Eve kann nicht ermitteln, was Alice gewählt hat. Das wäre nur möglich, wenn Eve im Zählsystem oder als Administrator fungieren würde. So hätte sie die Möglichkeit, die verschlüsselte Stimme von Alice zu rekonstruieren oder aufgrund des von Alice ans Zählsystem übergebenen Schlüssels K die zugehörige Stimme ausfindig zu machen. Aber da Eve ebenfalls Wählerin ist und sie lediglich die am Ende vom Zählsystem veröffentlichte Liste mit den verschlüsselten Stimmen (samt Schlüssel) sehen kann, hat sie keine Möglichkeit, eine der Stimmen genau Alice zuzuordnen, da sie nicht Alices Schlüssel K kennt.

1.4 Aufgabe 3 - additives homomorphes Wahlprotokoll

Nehmen Sie die Pailler-Verschlusselung von der Aufgabe 3 (SW10) und berechnen Sie das Wahlergebnis fur die folgenden Daten:

Achtung: In der dritten Zeile der Tabelle in der Aufgabenstellung gibt es einen Fehler (von Frau Pooyan bestätigt): r_3 ist **4**, nicht 5.

Wähler	Gewähltes	r_i
V_1	10	2
V_2	1	8