Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik
FH Zentralschweiz

I.BA_MOVK_MM – Kryptographie

Übung: eVoting

Dr. Ladan Pooyan-Weihs

Semesterwoche 11

Aufgabe 1: Digitale Demokratie

Lesen Sie Dokumente unter dem Link unten und beantworten Sie die folgenden Fragen:

1. Trägt das eVoting zur Demokratie bei? Begründen Sie Ihre Antwort.
2. Vergleichen Sie das eVoting-Projekt in Estland und in der Schweiz.
3. Warum hat der Bundesrat darauf verzichtet, die elektronische Stimmabgabe als ordentlichen Stimmkanal zu etablieren?
4. Wer ist Sarah Jamie Lewis und welche Rolle hat sie in Bezug auf das Projekt e-Voting in der Schweiz gespielt?

Link auf ILIAS: SW11

Aufgabe 2: Wahlprotokoll mit symmetrischer Verschlüsselung

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

Aufgabe 3: additives homomorphes Wahlprotokoll

Nehmen Sie die Pailler-Verschlüsselung von der Aufgabe 3 (SW10) und berechnen Sie das Wahlergebnis für die folgende Daten

Wählerin	Gewähltes	ri
V1	10	2
V2	1	8
V3	1	4
V4	1	2

Die Verschlüsselung von der Aufgabe 3 (SW10):

P =3, q = 5, n = p*q = 15, g = 16 und $\lambda = kgV((p-1),(q-1)) = 4$.

Viel Vergnügen!