
Analyse von homomorpher Verschlüsselung und MIX Netzen für elektronische Wahlsysteme

Bachelor-Thesis von Arif Sami, Murat Karabulut aus Frankfurt am Main
1. Mai 2010



TECHNISCHE
UNIVERSITÄT
DARMSTADT



CASED

Analyse von homomorpher Verschlüsselung und MIX Netzen für elektronische Wahlsysteme

Vorgelegte Bachelor-Thesis von Arif Sami, Murat Karabulut aus Frankfurt am Main

1. Gutachten:

2. Gutachten:

Tag der Einreichung:

Erklärung zur Bachelor-Thesis

Hiermit versichere ich die vorliegende Bachelor-Thesis ohne Hilfe Dritter nur mit den angegebenen Quellen und Hilfsmitteln angefertigt zu haben. Alle Stellen, die aus Quellen entnommen wurden, sind als solche kenntlich gemacht. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Darmstadt, den 1. Mai 2010

(Arif Sami und Murat Karabulut)

Inhaltsverzeichnis

Inhaltsverzeichnis	2
1 Einleitung	4
1.1 Problembeschreibung	6
1.2 Ziel und Methodik	6
2 Grundlagen	8
2.1 Notation	8
2.2 Das El-Gamal Verschlüsselungsverfahren	8
2.2.1 Mathematische Voraussetzungen und Mengen	8
2.2.2 Diskretes Logarithmenproblem	9
2.2.3 El-Gamal Berechnungsoperationen	9
2.2.4 El-Gamal Rechenbeispiel	10
3 Das homomorphe Verschlüsselungsverfahren	11
3.1 Homomorphie Eigenschaft und El-Gamal	12
3.1.1 Rechenbeispiel mit El-Gamal	12
3.2 Basisidee	13
3.2.1 Anwendung der homomorphen Verschlüsselung bei elektronischen Wahlen	13
3.2.1.1 Verschlüsselung der Stimmen	13
3.2.1.2 Auszählen der Stimmen	14
3.2.2 Erfüllung der Kriterien	14
3.3 Erweiterung um Zero-Knowledge-Beweis	15
3.3.1 Anwendung des Zero-Knowledge-Beweises	16
3.3.2 Erfüllung der Kriterien	17
3.4 Erweiterung um Secret-Sharing Verfahren	17
3.4.1 Shamir's Secret-Sharing	17
3.4.1.1 Shamir's Secret-Sharing bei elektronischen Wahlen	18
3.4.1.2 Erfüllung der Kriterien	18
3.4.2 Verifiable Secret-Sharing (VSS) und Public Verifiable Secret-Sharing (PVSS)	19
3.4.2.1 Public Verifiable Secret-Sharing bei elektronischen Wahlen	22
3.4.2.2 Erfüllung der Kriterien	22
3.4.3 Secret-Sharing ohne Dealer	23
3.4.3.1 Secret-Sharing ohne Dealer bei elektronischen Wahlen	24
3.4.3.2 Erfüllung der Kriterien	25

4	Das MIX Verfahren	26
4.1	Decryption MIX (Onion MIX)	26
4.1.1	Allgemeiner Ablauf des Decryption MIX Verfahrens	27
4.1.2	Anwendung des Decryption MIX Verfahrens bei elektronischen Wahlen	29
4.1.3	Erfüllung der Kriterien	29
4.2	Re-encryption MIX	30
4.2.1	Ablauf des Re-encryption MIX Verfahrens mit El-Gamal	31
4.2.2	Wiederverschlüsselung mit El-Gamal	31
4.2.2.1	Definition Wiederverschlüsselung mit El-Gamal	32
4.2.2.2	El-Gamal Rechenbeispiel (Fortsetzung von Abschnitt 2.2.4)	32
4.2.3	Anwendung des Re-encryption MIX Verfahrens bei elektronischen Wahlen	33
4.2.4	Erfüllung der Kriterien	33
4.3	Re-encryption MIX mit Randomized Partial Checking	34
4.3.1	Alternative Ansätze	34
4.3.2	Randomized Partial Checking (RPC)	35
4.3.3	Allgemeiner Ablauf des Re-encryption MIX Verfahrens mit Randomized Partial Checking	36
4.3.4	Anwendung des Re-encryption MIX Verfahrens mit RPC bei elektronischen Wahlen	37
4.3.5	Erfüllung der Kriterien	39
5	Homomorphe Verschlüsselung und MIX Verfahren im Vergleich	40
5.1	Gemeinsamkeiten und Unterschiede im Vergleich beider Verfahren	40
5.2	Vergleich nach Evaluierungskriterien	40
5.2.1	Verifizierbarkeit	41
5.2.2	Effizienz	41
5.2.3	Unterstützte Stimmzettelarten	42
5.2.4	Aufwände/ Kosten	43
5.2.5	Praktikabilität	44
5.2.6	Transparenz/ Verständlichkeit	45
5.2.7	Allgemeine Auswertung	45
6	Fazit und Ausblick	47
6.1	Fazit	47
6.2	Ausblick	48
7	Literaturverzeichnis	50

1 Einleitung

Eines der vorherrschenden Paradigmen des 21. Jahrhunderts ist der Einzug von elektronischer Kommunikation in jeglichen Bereichen sowohl des öffentlichen als auch des privaten Lebens. Das Handling mit dem Internet, aber auch der tägliche Umgang mit E-Mails sind nun mehr nicht lediglich eine Domäne, die jungen Menschen oder gar Technik begeisterten Menschen vorenthalten sind, vielmehr greifen nun Menschen aus jeder Alters- und Gesellschaftsschicht auf diese Art der Kommunikation zurück, sodass diese zu einem festen Bestandteil an Kommunikationswege geworden ist.

Dabei ist zu beachten, dass nicht nur Freizeitaktivitäten gestaltet werden, sondern auch vermehrt datenkritische Anwendungen wie Onlinebanking, das Übermitteln von Patientendaten oder aber vertrauliche Business Anwendungen wie Videokonferenzschaltungen usw. realisiert werden.

Im Zuge der dargestellten Modernisierung der Kommunikationswege ist es nahe liegend, dass auch Wahlen von einer solchen Zukunftsorientierung nicht ausgeschlossen bleiben. Das elektronische Wahlverfahren (*E-Voting*) imitiert das traditionelle Verfahren, welches mit Papierwahlstimmen vollzogen wird, um einerseits einen Lernvorteil zu erzielen und andererseits um Vertrauen, welches das traditionelle Verfahren erworben hat, auf das elektronische Wahlverfahren zu übertragen [End07]. Dabei umfasst das E-Voting jedes Verfahren, bei dem Wahlstimmen (ggf. in einem Wahllokal) in elektronischer Form erfasst, repräsentiert oder gesammelt werden können. Eine Untermenge des E-Votings bilden die Internetwahlen (*I-Voting*). Hier wird der eigene Computer durch geeignete Software und Anbindung zum Internet zu einem Wahlcomputer umfunktioniert. Natürlich muss hier durch geeignete Mechanismen zur Sicherheit der Kommunikation zwischen Computer (*Client*) und Wahlserver beigetragen werden.

Somit gelingt es, durch eine adäquate und sichere Umsetzung von elektronischen Wahlen, von einer Fülle von Vorteilen zu profitieren:

- **Finanzielle Einsparungen:** Da bei elektronischen Wahlen Stimmzettel wegfallen, können so Gelder durch den Wegfall von Papier- und Druckkosten eingespart werden, sobald sich die Anschaffung der Wahlgeräte bzw. der Wahlserver (bei Internetwahlen) amortisiert hat. Darüber hinaus würde die Briefwahl gänzlich wegfallen. Zusätzlich kann Personal gespart werden, da auch die Auszählung der Stimmen wegfallen würde.
- **Höhere Wahlbeteiligung:** Durch die Möglichkeit seine Stimme von zu Hause oder von einem anderen, beliebigen vertrauenswürdigen Ort mit Internetzugang abzugeben, kann zu höherer Wahlbeteiligung führen, da der Weg zum Wahllokal erspart wird.
- **Vermeidung ungültiger Stimmen:** Der Einsatz von Wahlmaschinen oder einer internetbasierten Wahloberfläche ermöglicht den Einsatz von Logik, welche die abzugebende Stimme vor der Abgabe validiert. So kann die Abgabe von unabsichtlich ungültigen Stimmen verhindert werden.
- **Fehlerfreies Auszählen:** Die maschinelle Verarbeitung der abgegebenen Stimmen ermöglicht ein fehlerfreies Auszählen des Wahlergebnisses. Es ist unwahrscheinlich, dass ein fehlerhaftes Ergebnis durch ein mögliches „Verzählen“ zustande kommt.
- **Zeitnahes Wahlergebnis:** Irreführende Hochrechnungen können durch die maschinelle Auszählung verhindert werden und im Idealfall kann zeitnah, d.h. unmittelbar nach dem Schließen der Wahllokale, ein korrektes Wahlergebnis erhalten werden.
- **Geringerer Aufwand und Ausübung von direkter Demokratie:** Durch den erheblich gesunkenen Organisationsaufwand ist es möglich öfter Wahlen durchzuführen und dem Volk somit Instrumente zur Ausübung von direkter Demokratie zur Verfügung zu stellen.

- Selbstständige Stimmabgabe für Sehbehinderte: Durch die technische Umsetzung des Wahlverfahrens ist es möglich Audiunterstützung bereitzustellen, so dass es auch Bürgern mit Sehbehinderungen möglich ist, ohne die Hilfe von Dritten ihre Stimme abzugeben.

Diese Arbeit widmet sich sowohl der Verarbeitung der abgegebenen Wahlstimmen als auch der Berechnung des Wahlergebnisses und die dazugehörigen Nachweise der korrekten Verarbeitung an den jeweiligen Stationen als Kernpunkte. Die Herausforderungen bei der Übermittlung der Wahlstimme zur Urne (*Wahlserver*) werden in dieser Arbeit nicht fokussiert.

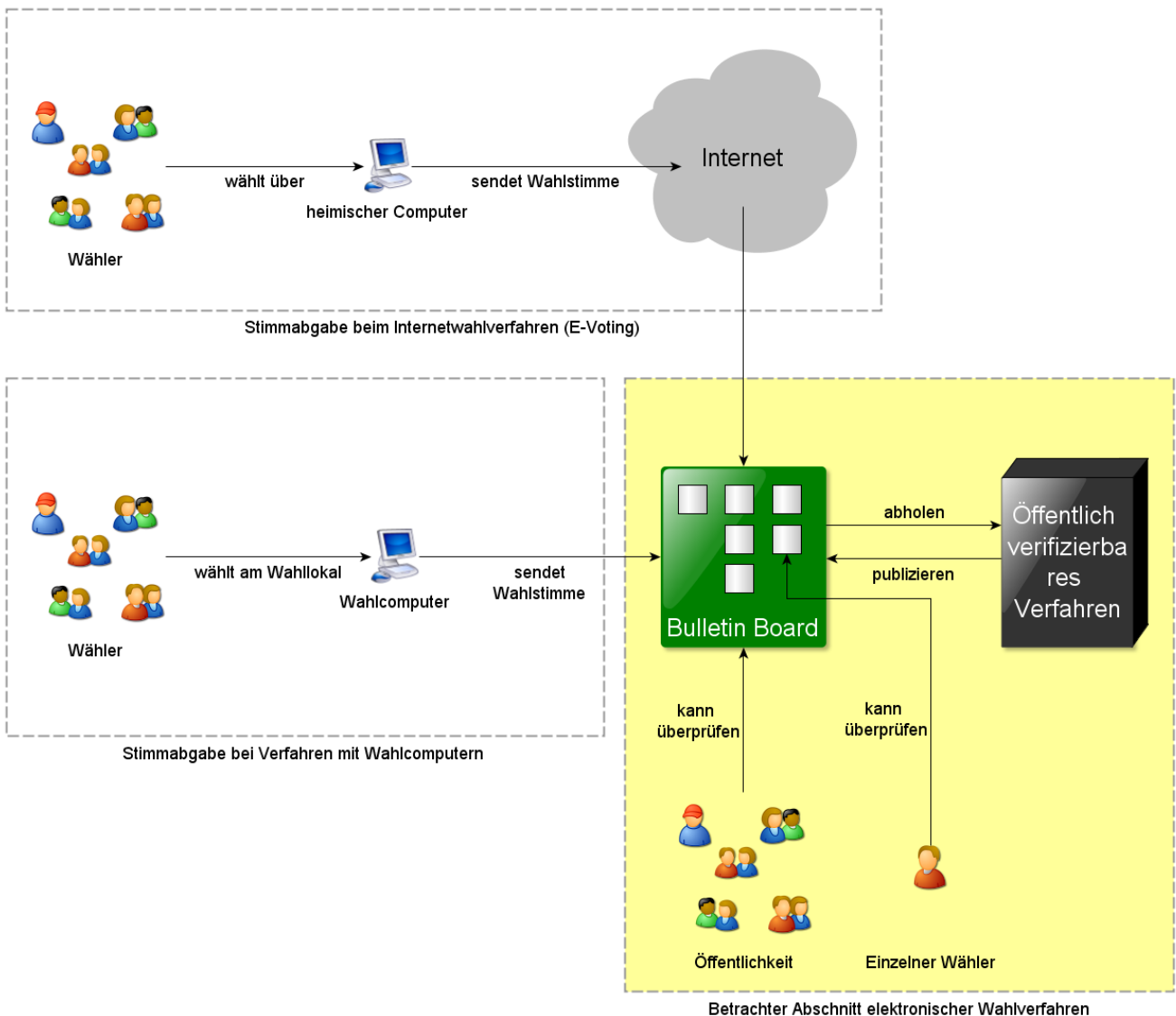


Abbildung 1.1: Allgemeine Skizze elektronischer Wahlverfahren

In obiger Abbildung 1.1 sind die beiden vorherrschenden E-Voting Verfahren allgemein skizziert. Die verschlüsselte Wahlstimme wird hier entweder über das Internet oder direkt vom Wahlcomputer zu einem virtuellen und öffentlich einsehbar Ort, dem Bulletin Board, übertragen. Dies geschieht, um Forderungen nach *individueller* und *universeller Verifizierbarkeit* nachzukommen. Dabei bedeutet individuelle Verifizierbarkeit, dass der Wähler die korrekte Verarbeitung seiner Wahlstimme durch das jeweilige Wahlverfahren verifizieren kann. Universelle Verifizierbarkeit heißt, dass sich jeder Beteiligte über den korrekten Ablauf des Wahlverfahrens überzeugen kann, um die Feststellung des Wahlergebnisses nachvollziehen zu können. Dies ist möglich, da das Bulletin Board den jeweiligen Verfahren auch dazu dient um die notwendigen Daten zur Verifikation zu veröffentlichen.

Diese Arbeit wird die universelle Verifizierbarkeit untersuchen, die den Spagat zwischen Geheimhaltung jeglicher Wählerdaten zwecks Einhaltung des Wahlgesetzes und der notwendigen Veröffentlichung von Daten des Wahlverfahrens zur Verifikation des korrekten Ablaufs der Wahl versucht. Hierfür werden zwei elektronische Wahlverfahren untersucht, die mit unterschiedlichen Ansätzen arbeiten:

- **Das homomorphe Verschlüsselungsverfahren:** Unter Ausnutzung homomorpher Eigenschaften der Darstellung einer Wahlstimme werden hier die Wahlstimmen in verschlüsselter Form aufaddiert, um dann die Summe der Verschlüsselungen zu einem Wahlergebnis zu entschlüsseln. Nach der Verschlüsselung wird die einzelne Wahlstimme nicht mehr entschlüsselt.
- **Das MIX Verfahren:** Durch Verschleierung der Input/Output Beziehungen von MIX Servern in einem MIX Netz, wird die einzelne verschlüsselte Wahlstimme anonymisiert nachdem sie im jeweiligen MIX Server gemischt worden ist.

1.1 Problembeschreibung

Elektronische Wahlsysteme werden schon seit geraumer Zeit erprobt (z.B. in der Schweiz durch den Vote électronique) oder bereits eingesetzt (bei der Gesellschaft für Informatik[End07]). Dabei haben die eingesetzten Systeme meist einen „Blackbox-Charakter“, da wegen der Wahrung des Wahlgeheimnisses der Betrieb des jeweiligen Systems einem Hersteller oder Betreiber solcher Systeme überlassen werden muss und somit nicht einsehbar ist.

Forscher plädieren schon länger für verifizierbare Wahlsysteme und sprechen sich klar gegen solche Wahlsysteme mit „Blackbox-Charakter“ aus. Zumal auch das Bundesverfassungsgericht mit den Leitsätzen zum Urteil des Zweiten Senats vom 3. März 2009 2 BvC 3/07, 2 BvC 4/07 [BVe] den Öffentlichkeitsgrundsatz einer Wahl bekräftigt hat. Demnach sind Wahlsysteme mit „Blackbox-Charakter“ für eine Wahl nicht ausreichend verifizierbar.

Zudem ist im Artikel 38 Absatz 3 des deutschen Grundgesetzes verlautet:

§ Die Abgeordneten des Deutschen Bundestages werden in **allgemeiner, unmittelbarer, freier, gleicher und geheimer** Wahl gewählt. [...]

Das Recht auf freie Wahl bedeutet seine Meinung frei bilden zu können und diese frei gebildete Meinung unverfälscht zum Ausdruck bringen zu können. Die Geheimheit der Wahl bedeutet dass niemand außer dem Wähler selbst Kenntnis von der Entscheidung des Wählers erlangt.

So muss die Wahl unter anderem einerseits anonym und geheim sein, um eine Wahl nach freiheitlich demokratischen Prinzipien zu gewährleisten, zugleich muss sie allgemein verifizierbar sein um eine korrekte Verarbeitung nachweisen und Manipulationen ausschließen zu können.

Die fehlende Öffentlichkeit einer elektronischen Wahl kann mit technischen Mitteln der Verifikation kompensiert werden. Dies bedeutet, dass es zwar unmittelbar während der Wahl nicht möglich ist den korrekten Ablauf zu verifizieren, jedoch können technische bzw. mathematische Mittel bereitgestellt werden um *nach* Ablauf der Wahl den korrekten Ablauf nachträglich und eindeutig nachweisen zu können.

1.2 Ziel und Methodik

Um die Anforderungen für Verifizierbarkeit umsetzen zu können und einen Fingerzeig in die richtige Richtung bei der Auswahl des einzusetzenden Verfahrens zu erhalten, werden in dieser Arbeit die beiden Wahlverfahren, Homomorphe Verschlüsselung und MIX Netze, vorgestellt, analysiert und letztlich gegenübergestellt. Dabei werden Vor- und Nachteile des jeweiligen Wahlverfahrens herausgestellt, um abwägen zu können welche Wahlszenarien dem jeweiligen Wahlverfahren aufgrund dessen Eignung zugeordnet werden können.

Das gegebene Wahlprotokoll des jeweiligen Verfahrens wird zunächst schematisch dargestellt, um dann dessen Anwendung in einem Wahlszenario zu veranschaulichen. Im jeweils letzten Abschnitt wird dann jedes Verfahren nach den unten angeführten Kriterien untersucht und es werden gegebenenfalls schrittweise Optimierungen eingefügt:

- *Robustheit*: Der Wahlvorgang kann nicht derart blockiert werden, so dass die Wahl abgebrochen werden muss. Ungültig erfasste Stimmen werden als solche erfasst und nicht berücksichtigt. Täuschungsversuche werden erkannt und behandelt.
- *Privatheit*: Bei der Auszählung besteht keine nachvollziehbare Beziehung zwischen dem Wähler und seiner abgegebenen Stimme. Insbesondere ist es dem Wähler nicht möglich nachzuweisen wie er gewählt hat.
- *Korrektheit*: Die von den zur Wahl zugelassenen Wählern abgegebenen Stimmen schlagen sich vollständig und ohne Veränderung im Wahlergebnis nieder. Es werden keine anderen Stimmen als die abgegebenen verarbeitet.

Diese Liste an Kriterien ist natürlich nicht erschöpfend, aber für den Erkenntnisgewinn im Rahmen dieser Arbeit ausreichend.

2 Grundlagen

Da bestimmte mathematische und kryptografische Sachverhalte vorausgesetzt sind, werden in diesem Kapitel zu deren Verständnis entsprechende Bezeichnungen und theoretische Grundlagen kurz beleuchtet und die in den folgenden Kapiteln sich wiederholenden Bezeichner einheitlich definiert.

2.1 Notation

Die in dieser Arbeit betrachteten Verfahren nutzen eine Public-Key-Infrastruktur unter Anwendung von asymmetrischen Schlüsselpaaren wobei ein öffentlicher Schlüssel und ein geheimer Schlüssel ein Paar bilden:

- (p, g, α) bezeichnet einen öffentlichen Schlüssel
- (a) bezeichnet einen geheimen Schlüssel

Diese Schlüssel können dazu angewendet werden, um Nachrichten m zu verschlüsseln oder verschlüsselte Nachrichten wieder zu entschlüsseln. Die Anwendung der jeweiligen Ver- oder Entschlüsselungsoperationen wird durch folgende mathematische Operationen definiert:

- enc bezeichnet die Verschlüsselungsfunktion zu einem öffentlichen Schlüssel (p, g, α)
 - Es gilt Verschlüsselung $C = (c_1, c_2) = \text{enc}(m)$
- dec bezeichnet die Entschlüsselungsfunktion zu einem geheimen Schlüssel (a) ,
 - Es gilt Entschlüsselung (Nachricht) $m = \text{dec}(C) = \text{dec}(\text{enc}(m))$

2.2 Das El-Gamal Verschlüsselungsverfahren

Das El-Gamal Verschlüsselungsverfahren ist ein asymmetrischer Verschlüsselungsalgorithmus der sich das, mit den heutigen zur Verfügung stehenden Mitteln, nur schwer zu berechnende diskrete Logarithmenproblem in der Mathematik zu nutzen macht, indem es diese mathematisch nur schwer umkehrbare Einwegfunktion zur Berechnung verwendet. Es wurde im Juli 1985 von Taher El-Gamal veröffentlicht und wird seither neben RSA und anderen asymmetrischen Verschlüsselungsverfahren zur Realisierung von Public-Key-Infrastrukturen verwendet.

2.2.1 Mathematische Voraussetzungen und Mengen

Um im El Gamal Kryptosystem den öffentlichen Schlüssel (p, g, α) zu erstellen, bedarf es einiger im folgenden beschriebener Voraussetzungen und mathematischer Mengen mit bestimmten Eigenschaften:

- Primzahl $p \gg 2$
- Zahlenmengen \mathbb{Z}_p und \mathbb{Z}_p^*

Die Menge \mathbb{Z}_p ist wie folgt definiert:

$$\mathbb{Z}_p = \{0, \dots, p - 1\} \tag{2.1}$$

Die Menge \mathbb{Z}_p^* definiert sich über die Teilerfremdheit von p :

$$\mathbb{Z}_p^* = \{r \in \mathbb{Z}_n : \gcd(r, p) = 1\} \quad (2.2)$$

Da p prim ist, gilt: $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$

- Untergruppe $\langle g \rangle$

Die Untergruppe $\langle g \rangle$ kann aus beliebigen $g \in \mathbb{Z}_p^*$ erzeugt werden mit:

$$\langle g \rangle = \{g^a \pmod{p} : 0 \leq a < p - 1\} \quad (2.3)$$

- Generator $g \pmod{p}$

$g \in \mathbb{Z}_p^*$ heißt Generator der Ordnung $p - 1$, falls für die aus g erzeugte Untergruppe $\langle g \rangle$ gilt: $\langle g \rangle = \mathbb{Z}_p^*$

2.2.2 Diskretes Logarithmenproblem

Aus einer Primzahl p , einem Generator $g \in \mathbb{Z}_p^*$ und einer Zahl a mit $0 \leq a < p - 1$ lässt sich $\alpha \equiv g^a \pmod{p}$ bestimmen. Hierbei ist a der diskrete Logarithmus von α zur Basis g :


$$a = \log_g \alpha \quad (2.4)$$

Das diskrete Logarithmenproblem besteht nun aus dem Problem die Umkehrung der eher simplen Exponentiation zu berechnen. Bis heute ist kein effizienter Algorithmus bekannt, der zu gegebenen p, g, α die Zahl $a = \log_g \alpha$ bestimmt [Le09].

2.2.3 El-Gamal Berechnungsoperationen

Gegeben ist

- ein Schlüsselpaar bestehend aus:
 - dem öffentlichen Schlüssel (p, g, α) mit $\alpha = g^a \pmod{p}$ und
 - dem geheimen Schlüssel (a)
- eine Nachricht m

 **Bemerkung:** Der öffentliche Schlüssel eines Schlüsselpaares steht jeder Entität zur Verfügung, die eine Nachricht m so verschlüsseln möchte, dass nur der (oder die) Besitzer des Schlüsselpaares, der als einzige Partei auch den geheimen Schlüssel kennt, die Verschlüsselung umkehren und den Klartext lesen kann. Die verschlüsselte Nachricht hat die Form $\text{enc}(m) = C = (c_1, c_2)$ und die entschlüsselte Nachricht entspricht der Form $\text{dec}(C) = \text{dec}(c_1, c_2) = m$

Die *Verschlüsselungsoperation* zu gegebenem öffentlichen Schlüssel (p, g, α) ist nach [Buc03] wie folgt definiert:

1. Wähle $r \in \{1, \dots, p - 2\}$ zufällig
2. Berechne $c_1 = g^r \pmod{p}$

3. Berechne $c_2 = m \cdot \alpha^r \pmod p$

4. Erhalte Geheimtext $\text{enc}(m) = (c_1, c_2)$

Die *Entschlüsselungsoperation* zu gegebenem geheimen Schlüssel (a) ist nach [Buc03] wie folgt definiert:

Der geheime Schlüssel ist nur dem Besitzer des Schlüsselpaares bekannt. Folglich kann nur er, unter Anwendung des dazu korrespondierenden öffentlichen Schlüssels, verschlüsselte Nachrichten entschlüsseln.

1. Berechne Exponenten $x = p - 1 - a$

2. Erhalte Nachricht $\text{dec}(c_1, c_2) \equiv c_1^x \cdot c_2 \equiv m \pmod p$

2.2.4 El-Gamal Rechenbeispiel

Im folgenden Rechenbeispiel ist zu erkennen, dass durch Ausnutzung der Gruppeneigenschaften die Nachricht auch nach mehrmaligem Verschlüsseln durch Anwendung des geheimen Schlüssels wiederhergestellt werden kann.

Gegeben ist

- ein Schlüsselpaar bestehend aus:
 - dem öffentlichen Schlüssel ($p = 13, g = 7, \alpha = 12$) mit $\alpha = 7^6 \pmod{13} = 12$ und
 - dem geheimen Schlüssel $a = 6$
- eine Nachricht $m = 7$

Anhand des gegebenen Schlüssels und eines Zufallswert $r = 3 \in \{1, \dots, p - 2\}$ lässt sich die Nachricht $m = 6$ zur Verschlüsselung $C = \text{enc}(m) = (c_1, c_2)$ mit

- $c_1 = 7^3 \pmod{13} = 5$
- $c_2 = 7 \cdot 12^3 \pmod{13} = 6$

berechnen.

Umgekehrt lässt sich aus obig berechneter und verschlüsselter Nachricht $C = (5, 6)$ die Entschlüsselung $\text{dec}(5, 6) = m$ errechnen:

- $\text{dec}(5, 6) = 6 \cdot 5^{13-1-6} \pmod{13} = 6 \cdot 5^6 \pmod{13} = 7$

3 Das homomorphe Verschlüsselungsverfahren

Im weiteren Verlauf werden die Themenbereiche „Homomorphe Verschlüsselung“, „Basis Ansatz“, „Erweiterung um Zero-Knowledge-Beweis“ und „Erweiterung um Secret-Sharing“ analysierend erläutert. Die aufgezählten Themenschwerpunkte werden mittels der selben Vorgehensweise dargestellt: Zunächst erfolgt eine Vorstellung und Erläuterung des Themas, anschließend wird selbiges in Zusammenhang mit elektronischen Wahlen erklärt, um abschließend prüfen zu können, ob die festgelegten Kriterien erfüllt werden konnten. Abbildung 1.1 skizzierte bereits einen allgemeinen Verlauf eines elektronischen Wahlverfahrens. Die ebenfalls in der Skizze thematisierte „Blackbox“ wird nun im Zusammenhang mit homomorphen Verschlüsselungen im Detail betrachtet.

Homomorphe Verschlüsselungsverfahren bieten sich in sofern an, als dass sie die Geheimhaltung der Stimmen während elektronischer Wahlverfahren gewährleisten, in den Ergebnisse erzielt werden können, ohne dabei einzelne Stimmen zu entschlüsseln. Bei diesem Verfahren können demnach verschlüsselte Nachrichten so miteinander verknüpft werden, dass die sich daraus ergebende Entschlüsselung einer Verknüpfung der Nachrichten entspricht.

Damit die Geheimhaltung der Stimmen während elektronischer Wahlen gewährleistet werden kann, müssen die Stimmen verschlüsselt werden. Dafür wird das El-Gamal Verschlüsselungsverfahren herangezogen. Eine gute Lösung bieten hierbei homomorphe Verschlüsselungsfunktionen, da hierbei Ergebnisse erzielt werden können, ohne dabei einzelne Stimmen entschlüsseln zu müssen. Mit der Addition der verschlüsselten Stimmen, bei der nur die Summe entschlüsselt wird, wird das Endergebnis erzielt (siehe Abbildung 3.1).

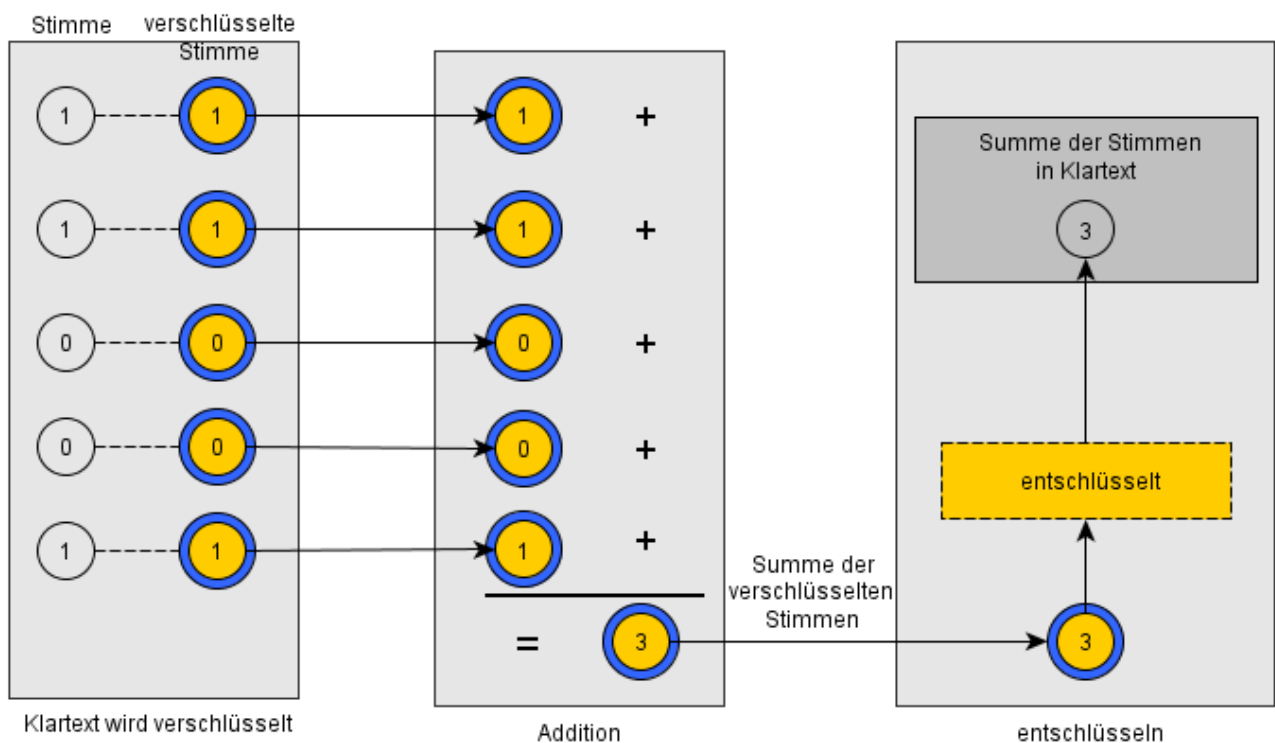


Abbildung 3.1: homomorphe Verschlüsselung

Nach der Definition [HM09] sei (G, \oplus) eine additive Gruppe und (H, \otimes) eine multiplikative Gruppe. Eine Funktion $f : G \rightarrow H$ heißt homomorph, falls für alle $x_1, x_2 \in G$ gilt, dass

$$f(x_1 \oplus x_2) = f(x_1) \otimes f(x_2).$$

wobei das Paar (\oplus, \otimes) jedes beliebige Paar von Funktionen f_1, f_2 sein kann, sofern diese die Homomorphieeigenschaft erfüllt.

3.1 Homomorphie Eigenschaft und El-Gamal

Im Abschnitt 2.2 wurde bereits auf das El-Gamal Verschlüsselungsverfahren eingegangen. Die mathematischen Grundpfeiler sowie allgemeine Information bezüglich des El-Gamal Verfahrens wurden dabei thematisiert. Nun wird die homomorphe Eigenschaft des El-Gamal Verfahrens herangezogen und erläutert. Das El-Gamal Verschlüsselungsverfahren zeichnet sich durch seine homomorphe Addition aus. Dies ist wichtig, da bei elektronischen Wahlen die homomorphie Eigenschaft verwendet wird, um auf diese Weise das Endergebnis als Summe der geheimen Stimmen zu erhalten. Die Darstellung der möglichen Nachrichten durch erzeugende Gruppenelemente g_i von G stellt eine Gelegenheit dar, Homomorphie hinsichtlich der Addition zu erzielen. Die Addition im Exponenten ($g_i g_i = g_i^{1+1}$) wird erreicht durch das zweifache Senden einer Nachricht mit primitiven Elemente g_i , das heisst eine Multiplikation zweier Chiffretexte $(g^{\alpha_1}, h^{\alpha_1} g_i)$ und $(g^{\alpha_2}, h^{\alpha_2} g_i)$. Hieraus wird deutlich, dass für eine Addition, der auf die Nachricht entfallenen Anzahlen, die Multiplikation der beiden Chiffretexte nötig ist.

Das Wertepaar $(x_i, y_i) = (g^{\alpha_i}, h^{\alpha_i} v_i)$ wird mit einer Verschlüsselung einer Nachricht v_i und mit einem zufälligen Wert α_i erreicht. Bei n verschlüsselten Nachrichten ergibt sich die komponentenweise Multiplikation zu

$$\left(\prod_{i=1}^n x_i, \prod_{i=1}^n y_i \right) = (g^\alpha, h^\alpha \cdot \prod_{i=1}^n v_i) \text{ mit } \alpha := \sum_{i=1}^n \alpha_i$$

Durch die Menge $M = \{1, n, n^2, \dots, n^{K-1}\}$ können K verschiedene Nachrichten dargestellt werden. Die Summe aller Sender von Nachrichten ist dabei $n > 1$. Damit die Nachrichten aller Stellenwerte veranschaulicht werden können, werden diese als Stellenwerte in einem Zahlensystem zur Basis n dargestellt. Wenn nun alle n Sender die gleiche Nachricht verschicken, führt es zu einer Stellenüberschreitung, da die Anzahl der Nachrichten je Nachrichtentyp höchstens n ist. In dem dargestellten Stellensystem beschreiben die Ziffern andernfalls die Anzahlen der jeweiligen Nachrichten. Ein weiterer Erzeuger γ der Gruppe G wird herangezogen, um Homomorphie hinsichtlich der Addition zu erzielen. So wird die ursprüngliche Nachricht v_i als Nachricht γ^{v_i} dargestellt. Bei der Multiplikation zweier Chiffretexte $(g^{\alpha_1}, h^{\alpha_1} \gamma^{v_1})$ und $(g^{\alpha_2}, h^{\alpha_2} \gamma^{v_2})$ mit den Nachrichten v_1 und v_2 entspricht dann die Addition der Nachrichten im Exponenten: $\gamma^{v_1} \gamma^{v_2} = \gamma^{v_1+v_2}$.

3.1.1 Rechenbeispiel mit El-Gamal

Bei der El-Gamal-Verschlüsselung ist der Raum der Klartexte eine Gruppe (G, \cdot) mit der Primzahl-Gruppenordnung $|G| = q$. Ebenfalls eine Gruppe bezüglich komponentenweiser Multiplikation ist der Raum der Chiffretexte $G \times G$.

Gegeben seien zwei Klartexte m_1 und m_2 und die dazu gehörigen Chiffretexte

$$e_1 := (g^{\alpha_1}, h^{\alpha_1} m_1) \text{ und } e_2 := (g^{\alpha_2}, h^{\alpha_2} m_2).$$

Dann ist die komponentenweise Multiplikation der Chiffretexte

$$e_1 e_2 = (g^{\alpha_1} g^{\alpha_2}, h^{\alpha_1} h^{\alpha_2} m_1 m_2)$$

eine Verschlüsselung der multiplizierten Klartexte $m_1 \cdot m_2$.

3.2 Basisidee

Die Basisidee des homomorphen Verschlüsselungsverfahrens ist vergleichbar mit der klassischen Papierwahl. Auch hierbei geht es um die Einhaltung des Wahlheimnisses. Selbst wenn beide theoretischen Grundideen identisch sind, unterscheiden sie sich dennoch grundsätzlich bei der praktischen Umsetzung. So ist es bei der klassischen und gängigen Wählart üblich, dass der Wähler in einer geheimen Wahl seine Stimme mit Hilfe von Stimmzetteln in die Wahlurne einwirft. Nach der Abgabe der Stimme ist die Aufgabe des Wählers praktisch vollendet. Die Aufgabe der Wahlbehörden, die stattgefundene Wahl auszuwerten, setzt hier an. Bei dem elektronischen Wahlverfahren wird ebenfalls der Wähler um seine Stimme gebeten. Hierbei sendet der Wähler seine Stimme verschlüsselt an das Bulletin-Board. Die Aufgabe der Wahlbehörde übernimmt hierbei die so bezeichnete Autorität, indem es die verschlüsselten Stimmen zunächst entschlüsselt, diese sodann auswertet und schließlich am Bulletin-Board für jeden sichtbar veröffentlicht. Die Vorgehensweise unterscheidet sich bis zuletzt nicht von der Vorgehensweise des MIX Verfahrens. Lediglich in der Verarbeitung der Blackbox bestehen grundsätzliche Unterschiede (siehe Abb. 1.1).

Im weiteren Verlauf des Kapitels wird das oben dargestellte elektronische Wahlverfahren detailliert beschrieben.

3.2.1 Anwendung der homomorphen Verschlüsselung bei elektronischen Wahlen

Die Anwendung des homomorphen Verschlüsselungsverfahrens setzt grundsätzlich voraus, dass die einzelnen Stimmen in keinem Fall als Klartext bekannt gemacht werden. Es wird angenommen, dass die Stimmen vom Wähler korrekt verschlüsselt an das Bulletin-Board versendet werden. Die Autoritäten holen die verschlüsselten Stimmen vom Bulletin-Board ab, summieren diese, entschlüsseln die Summe und veröffentlichen abschließend das Ergebnis auf dem Bulletin-Board. Hierbei kann eine Autorität z.B. in Form einer Wahlbehörde darstellen werden.

Explizit wird das Verfahren wie folgt angewendet: Die Autorität generiert ein Paar mit Secret-Key/ Public-Key für die Verschlüsselungsfunktion und veröffentlicht den Public-Key (PK) und behält den Secret-Key (SK) für sich. Jeder Wähler gibt seine Stimme $v \in Z_q$ ab und verschlüsselt sie als $e = E_z(v, \alpha)$ für ein zufälliges Element $\alpha \in Z_q$ mit Public-Key und El-Gamal Verfahren. Der Wähler unterschreibt die verschlüsselte Stimme und sendet diese auf den Bulletin-Board. Die einzelnen Stimmen werden nie im Klartext bekannt. Nach den Wahlen werden bei dem homomorphen Verschlüsselungsverfahren die verschlüsselten Stimmen von der Autorität aus dem Bulletin-Board geholt und addiert.

Bei einer homomorphen Verschlüsselung ist die Verwendung einer additiven Funktion erforderlich, da das Wahlergebnis die Summe der einzelnen Stimmen ist. Der Wert für eine Stimme wird in der Regel 1 bzw. 0 sein. Diese stehen für „Ja“ bzw. „Nein“. Bereits hierbei ergeben sich die ersten Lücken bei homomorphen Verschlüsselungen. Wahlen mit mehreren Auswahlmöglichkeiten erhöhen die Komplexität. Dies kann erreicht werden, indem mehrere „Ja“/„Nein“- Abstimmungen verschachtelt werden.

3.2.1.1 Verschlüsselung der Stimmen

Wie bereits erwähnt, muss bei homomorphen Verschlüsselungsverfahren der Wähler seine Stimme verschlüsselt an das Bulletin-Board schicken. Die Summe der abgegebenen verschlüsselten Stimmen werden bei Wahlprotokollen mit homomorpher Verschlüsselung berechnet. Dabei wird bei einer einfachen „Ja“/„Nein“ Abstimmung, „Ja“ als 1 und „Nein“ als 0 codiert. Aus der Summe lässt sich die Anzahl der „Ja“-Stimmen und die Anzahl der „Nein“-Stimmen berechnen. Stimmenthaltungen können ebenfalls erlaubt sein. Hierbei kann die „Ja“-Stimme als 1, die „Nein“-Stimme als -1 und die „Leer“-Stimme als 0 codiert werden. Die Differenz kann aus der Summe berechnet werden, wobei sich die absolute Anzahl an „Ja“-Stimmen nicht berechnen lässt. Damit nicht alle Stimmen mit dem selben Inhalt gleich aussehen, muss zusätzlich eine Zufallszahl generiert und an die Stimme ergänzt werden. Die Zufallszahl verhindert, dass die Stimme auf

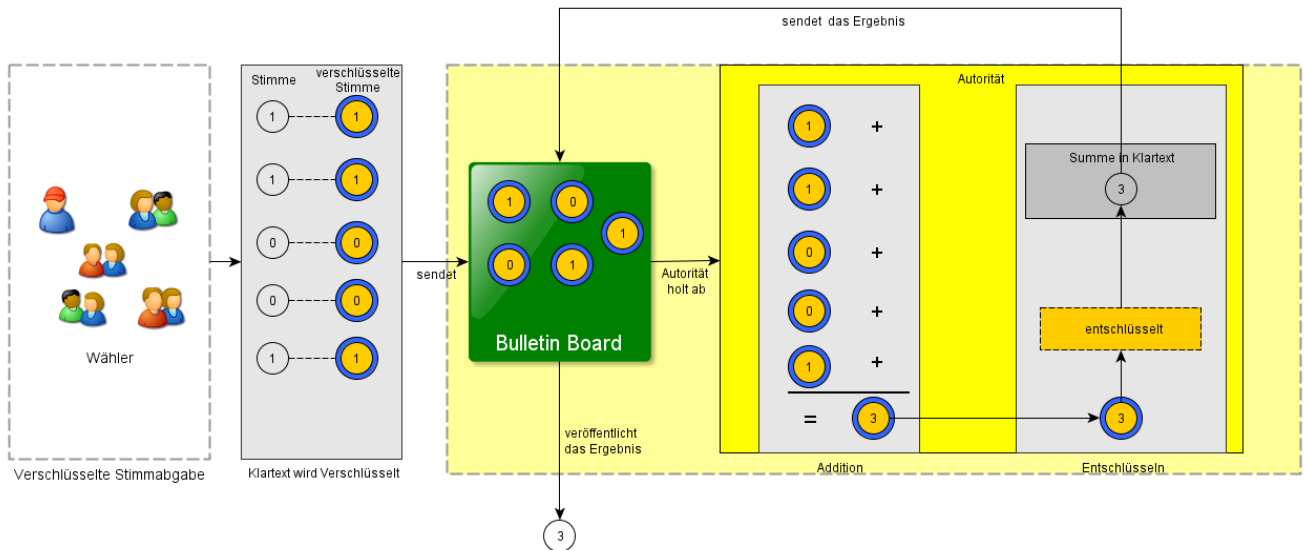


Abbildung 3.2: homomorphe Verschlüsselung bei elektronischen Wahlen

dem Bulletin-Board erkannt wird, und somit nicht nachvollziehbar wird, wie gewählt wurde. Eine 1-out-of-L Wahl ist notwendig, um beliebige Kandidatenwahlen durchführen zu können. Das heißt es gibt L Kandidaten und jeder Wähler kann exakt einem Kandidaten seine Stimme abgeben. Falls der Wähler den i -ten Kandidaten wählen möchte (für $1 \leq i \leq L$), wird die Stimme auf M^{i-1} gesetzt, wobei M die Anzahl der wahlberechtigten Personen darstellt. Aus der Summe der abgegebenen Stimmen lässt sich eruiere für welchen Kandidaten die Stimme abgegeben wurde. Damit kein Überlauf entsteht, muss $q \geq M^L$ gelten.

3.2.1.2 Auszählen der Stimmen

Die Auszählung der Stimmen erfolgt sobald alle Wähler ihre Stimmen an das Bulletin-Board verschicken und somit der Akt des Wählens vollendet ist. Es wird von der Autorität nur die Stimme T_i für $i=1, \dots, t$ berücksichtigt, welche von einer wahlberechtigten Entität unterschrieben an das Bulletin-Board verschickt wurde. Am Ende der Wahl holt die Autorität die einzelnen verschlüsselten Stimmen aus dem Bulletin-Board ab. Die akzeptierten verschlüsselten Stimmen werden unter Ausnutzung des Homomorphismus addiert und daraus ergibt sich die verschlüsselte Summe e_T . Die Summe der verschlüsselten Stimmen wird nun entschlüsselt und daraus folgt im Klartext die Summe T der Stimmen, wobei $e_T = \sum_{i=1}^t T_i$ ist und t die Gesamtanzahl der akzeptierten Stimmen abbildet. Die Summe T wird nun an das Bulletin-Board geschickt und das Ergebnis der Wahl wird veröffentlicht.

3.2.2 Erfüllung der Kriterien

Nachdem die Basisidee des homomorphen Verschlüsselungsverfahrens bei elektronischen Wahlen vorgestellt wurde, soll geprüft werden, ob die Kriterien *Korrektheit*, *Privatheit* und *Robustheit* mit dem vorgestellten Verfahren erfüllt werden können. Sofern dies nicht der Fall sein sollte, werden Verbesserungsvorschläge gemacht und im nächsten Abschnitt behandelt. Grundsätzlich gilt, dass die genannten Kriterien sowohl für den Wähler, als auch für die Autorität verbindlich sind und somit beide Perspektiven Gültigkeit haben. Folglich ist es notwendig, dass die Kriterien sowohl aus der Sicht des Wählers als auch aus der Sicht der Autoritäten betrachtet werden müssen. Um sagen zu können, dass die geforderten Kriterien vollständig erfüllt sind, müssen demnach beide Perspektiven den Kriterien Folge leisten.

Die *Korrektheit* wird im vorgestellten Verfahren weder aus der Sicht der Wähler, noch aus der Sicht der Autorität (Wahlbehörde) erfüllt. Bei der Konzeption der Basisidee wurde angenommen, dass der Wähler seine Stimme korrekt verschlüsselt an das Bulletin-Board verschickt. Es wurde weiterhin angenommen, dass der Wähler vertrauenswürdig ist und folglich seine Stimme korrekt verschlüsselt. Der Fall eines eventuellen Vertrauensmissbrauches wurde hierbei allerdings nicht weiter beachtet; könnte jedoch diverse Probleme mit sich führen. So könnte der Wähler seine Stimme beliebig verändern und diese verschlüsselt an das Bulletin-Board schicken. Da die verschlüsselte Stimme von keiner Instanz verifiziert wird und die Stimme in homomorphen Verschlüsselungsverfahren als Klartext nicht im Bulletin Board sichtbar sein sollte und der Wähler weiterhin keinen Beweis an das Bulletin-Board senden muss, kann das Kriterium der *Korrektheit* nicht erfüllt werden. Um gewährleisten zu können, dass das dargestellte Verfahren funktionieren kann, muss das Kriterium der *Korrektheit* erfüllt werden, da diese im Verfahren nicht kontrolliert werden kann.

Um das Kriterium der *Korrektheit* vollständig zu erfüllen, muss gewährleistet werden, dass die Wahlbehörde vertrauenswürdig ist. Ist dies nicht der Fall, kann auch die *Korrektheit* nicht eingehalten werden. Die Autorität ist im alleinigen Besitz des Secret-Keys und kann jederzeit die verschlüsselten Stimmen entschlüsseln. Es besteht die Möglichkeit die Stimme zu manipulieren oder nicht alle Stimmen vollständig zu behandeln.

Die *Privatheit* wird in der Basisidee nur partiell erfüllt. Zwar werden durch die Verschlüsselung die Stimmen der einzelnen Wähler nicht für andere Wähler sichtbar, dennoch kann von einer absoluten *Privatheit* nicht die Rede sein. Aufgrund der Tatsache, dass die Autoritäten durch den Besitz des Secret-Keys sich jederzeit Zugang zu den einzelnen Wählerstimmen verschaffen können und diese „böswillig“ ausnutzen könnten, ist das Kriterium der *Privatheit* nicht hinlänglich erfüllt. Bei homomorpher Verschlüsselung sollten die einzelnen verschlüsselten Stimmen niemals sichtbar sein, sondern nur die Summe aller Stimmen. Daraus ist erkennbar, dass der Schutz vor der Wahlbehörde nicht erfüllt wird, da diese die Möglichkeit haben, die einzelnen Stimmen zu entschlüsseln und nachzuvollziehen, von wem die Stimme stammt und was gewählt wurde.

Das Kriterium der *Robustheit* wird ebenfalls nicht erfüllt, da nur die Autorität die Stimmen auszählt und bei einem möglichen Ausfall oder einer möglichen Verweigerung nicht gewährleistet werden kann, dass die Wahl weiterhin fortgeführt wird.

Da keines der Kriterien vollständig erfüllt wird, muss das Verfahren erweitert werden, um die einzelnen Kriterien zu erfüllen. Beim homomorphen Verschlüsselungsverfahren müssen die Kriterien aus Sicht des Wählers, sowie aus Sicht der Autorität erfüllt werden, da die einzelnen verschlüsselten Stimmen miteinander addiert werden und nie im Klartext sichtbar sein sollten. Im anschließenden Kapitel werden eventuelle Nicht-Vertrauenswürdige Wähler in Betracht gezogen und Lösungsvorschläge vorgestellt. Hierbei wird der Frage nachgegangen, wie es möglich gemacht werden kann, dass der Wähler seine Stimme korrekt verschlüsselt an das Bulletin-Board verschickt. Das Zero-Knowledge Beweis, das nun exemplarisch erläutert werden soll, bietet sich besonders an, wenn erreicht werden will, dass die einzelnen Wähler ihre Stimmen korrekt verschlüsselt versenden.

3.3 Erweiterung um Zero-Knowledge-Beweis

Bei homomorpher Verschlüsselung muss gewährleistet werden, dass die Wähler ihre verschlüsselten Stimmen korrekt abgeben, da sonst das ganze Verfahren nicht funktionieren kann. Der Wähler könnte eine ungültige verschlüsselte Stimme an das Bulletin-Board versenden und somit die Wahl beeinflussen. Da die Stimme des einzelnen Wählers nie entschlüsselt werden darf, ist es notwendig ein Verfahren einzusetzen, dass die verschlüsselte Stimme des Wählers nicht an die Autorität oder an Dritte preis gibt. Dies kann mit dem Zero-Knowledge-Beweis durchgeführt werden.

Die vorliegende Problemstellung lautet: Wie kann der Wähler den Autoritäten beweisen, dass seine Stimme korrekt ist, ohne seine Stimme veröffentlichen zu müssen? Zur Beschreibung des Zero-Knowledge-Beweises wird von folgendem Szenario ausgegangen: Alice (Beweiser) möchte Bob (Verifizierer) zeigen, dass er einen geheimen Schlüssel besitzt, ohne dabei Informationen über den Schlüssel selbst bekannt zu geben. Alice besitzt den Schlüssel für die Tür am Ende einer Höhle, welches kreisförmig ist und die Möglichkeit besteht, Eingang A oder Eingang B zu nutzen. Alice besitzt den

Schlüssel für die Tür innerhalb der Höhle und hat damit die Möglichkeit, aus der Höhle beidseitig heraus zu kommen. Die Vorgehensweise sieht folgend aus (3.3):

- Alice benutzt entweder Eingang A oder Eingang B. Bob kann nicht sehen, welchen Eingang Alice nutzt.
- Bob ruft Alice zu, aus welchem Eingang Alice raus kommen soll.
- Falls nötig, schliesst Alice die Tür mit dem Schlüssel auf und kommt aus dem Eingang raus, das von Bob gewollt ist.

Dies wird mehrere Male wiederholt und in jeder Runde kann die Unsicherheit um 50% vermindert werden. In der zweiten Runde geht die Unsicherheit auf 25% runter und nach der dritten Runde reduziert die sich auf 12,5% usw. Nach n Runden beträgt die Unsicherheit 2^{-n} . Somit kann Bob überzeugt werden, da bei mehreren Durchläufen die Wahrscheinlichkeit steigt, dass Alice den Schlüssel besitzt.

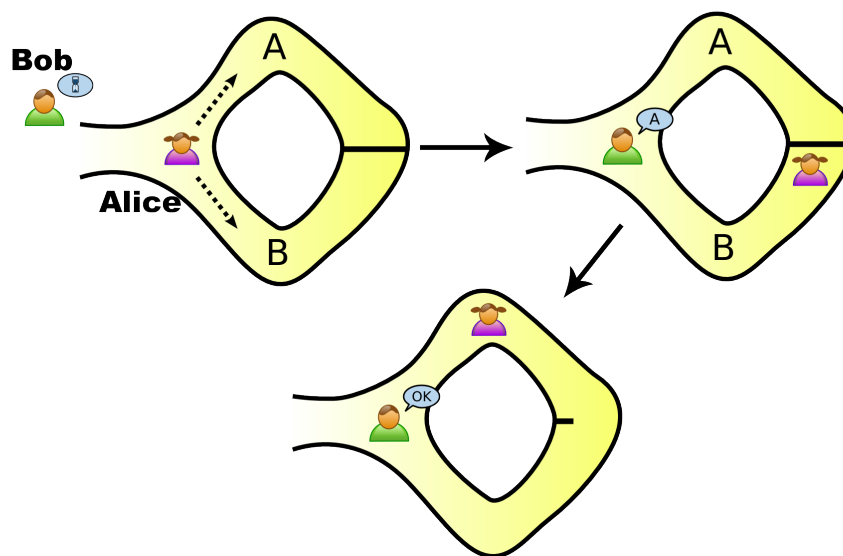


Abbildung 3.3: Szenario für Zero-Knowledge-Beweis

3.3.1 Anwendung des Zero-Knowledge-Beweises

Der Wähler sendet seine verschlüsselte Stimme an das Bulletin-Board und auch ein Zero-Knowledge-Beweis, in dem er die Autoritäten davon überzeugt, dass seine Stimme korrekt abgegeben wurde, ohne dabei Informationen über die Stimme selbst bekannt geben zu haben (Abbildung 2). Ein bekanntes Verfahren hierfür ist das Fiat-Shamir-Protokoll mit dem der Beweiser sich mit dem Verifizierer gegenüber authentisiert. Hierbei zeigt der Beweiser, dass er eine Quadratwurzel (geheimer Schlüssel) einer vorher veröffentlichten Quadratzahl (öffentlicher Schlüssel) kennt. Das Vorzeichen wird bei diesem Verfahren freigegeben und ist ein Bit. Eine Variante ist das Feige-Fiat-Shamir-Protokoll. Hierbei werden keinerlei Informationen über den geheimen Schlüssel preisgegeben. Das Verfahren arbeitet interaktiv, das heißt, es finden mehrere Runden zwischen Geheimnisträger und dem Prüfer statt. In jeder Runde kann die Kenntnis der Zahl zu 50% bewiesen werden. Nach zwei Runden bleibt eine Unsicherheit von 25%, nach der dritten Runde reduziert sich die Unsicherheit auf 12,5% usw. Nach n Runden beträgt die Unsicherheit 2^{-n} . Die Sicherheit des Fiat-Shamir-Protokolls beruht auf der Schwierigkeit, Quadratwurzeln im Restklassenring zu berechnen. Diese Berechnung ist genauso schwierig wie die Zahl $n = p \cdot q$ (p, q sind Primzahlen) zu faktorisieren und damit praktisch nicht durchführbar. Für den Wähler wäre ein nicht-interaktiver Zero-Knowledge Beweis praktischer bzw. bequemer, da er nicht gezwungen wäre mehrere Interaktionen zu tätigen. Um dieses gewährleisten zu können, muss das genannte Fiat-Shamir-Protokoll um eine Hashfunktion erweitert

werden ([HM09]). Dadurch wird ermöglicht, dass der Wähler mit seiner verschlüsselten Stimme auch ein Beweis dafür liefert, dass seine Stimme korrekt abgegeben wurde.

Wie bereits erwähnt, ist der Fokus der Bachelorarbeit nicht die Übermittlung der Wahlstimmen. Dennoch ist es der Vollständigkeit halber notwendig auch ein solches Verfahren, wenn auch nur oberflächlich, zu erwähnen und sich im Klaren darüber zu sein, dass ein solches Verfahren existiert.

3.3.2 Erfüllung der Kriterien

Mit der Einführung des Zero-Knowledge Beweises wird der Wähler verpflichtet, seine Stimme korrekt zu verschlüsseln und an das Bulletin-Board zu verschicken. Zuvor bestand das Problem, dass der Wähler die Möglichkeit hatte, seine Stimme „unkorrekt“ zu verschicken. So konnte das Kriterium der *Korrektheit* aus der Sicht des Wählers nicht erfüllt werden. Dieses Problem konnte durch die Erweiterung um das Zero-Knowledge Beweis behoben werden.

Weiterhin bestehen aus Sicht der Autorität Mängel bei der Umsetzung der *Privatheit*. Um jedoch die Kriterien *Privatheit*, *Robustheit* und *Korrektheit* vollständig erfüllen zu können, muss ein zusätzliches Verfahren herangezogen werden. Des Weiteren besteht das Problem, dass der Secret-Key lediglich von einer Person erzeugt wurde und die Wahrscheinlichkeit eines Missbrauches fortbesteht. Um dies zu verhindern zu können, muss die Erweiterung um das Secret-Sharing Verfahren erfolgen.

3.4 Erweiterung um Secret-Sharing Verfahren

Im dem vorherigen Kapitel wurde deutlich, dass niemand alleinig von den Autoritäten die Stimme der einzelnen Wähler entschlüsseln darf und somit die Möglichkeit besitzt, die Stimmen nachzuvollziehen oder zu verändern. Statt nur einer Person zu vertrauen, sollte das Vertrauen auf mehrere Personen verteilt werden. Im Hinblick auf elektronische Wahlen mit homomorpher Verschlüsselung ist es daher notwendig, den Schlüssel auf mehrere Personen zu verteilen, so dass die Auszählung von mehreren Personen durchgeführt werden muss. Um dieses zu gewährleisten, wird das sogenannte Geheimnisteilungsverfahren oder Secret-Sharing Verfahren verwendet.

Unter Secret-Sharing wird eine Technik verstanden, bei der eine Nachricht unter einer gewissen Anzahl von Autoritäten aufgeteilt wird. Somit besitzt keiner der Autoritäten die Legitimität, eine Nachricht alleine zu rekonstruieren. Je nach System ist lediglich eine Teilmenge der Autoritäten notwendig, um die Nachricht zu bestimmen. Ein Dealer ist die Autorität, welcher die Aufteilung vornimmt und die einzelnen Shares an die Shareholder verteilt. Bei einem (n,t) -Secret-Sharing Verfahren wird ein Geheimnis auf n Shareholder verteilt und es müssen mindestens t dieser Shareholder zusammen kommen, damit das Geheimnis rekonstruiert werden kann. Wenn weniger als t Shareholder sich zusammenschließen, können sie keine relevanten Informationen über das Geheimnis erhalten. Ein verbessertes Secret-Sharing Verfahren ist das Shamir's Secret-Sharing Verfahren, welches auf Polynominterpolation basiert und im nächsten Abschnitt näher vorgestellt wird.

3.4.1 Shamir's Secret-Sharing

Shamir's Secret-Sharing [Sha79] wurde 1979 von Adi Shamir entwickelt und basiert auf Polynominterpolation. Im folgenden Kapitel wird das Verfahren näher erläutert und in Zusammenhang mit elektronischen Wahlen beschrieben.

Nach [Buc03] wird der Ablauf des Verfahrens wie folgt erklärt: Der Dealer wählt bei der Initialisierung eine Primzahl p , $p \geq n+1$ und paarweise und von Null verschiedenen Elementen $x_i \in \mathbb{Z}/p\mathbb{Z}$, $1 \leq i \leq n$. Die x_i werden veröffentlicht und die Elemente von $\mathbb{Z}/p\mathbb{Z}$ durch ihre kleinsten nicht negativen Vertreter dargestellt.

In den folgenden Schritten wird beschrieben, auf welche Weise der Dealer ein Geheimnis $s \in \mathbb{Z}/p\mathbb{Z}$ verteilen will.

-
1. Der Dealer Wählt geheime Elemente $a_j \in \mathbb{Z}/p\mathbb{Z}, 1 \leq j \leq t - 1$ und konstruiert daraus das Polynom

$$a(X) = s + \sum_{j=1}^{t-1} a_j X^j. \quad (3.1)$$

Es ist vom Grad $\leq t - 1$.

2. Der Dealer berechnet die Shares $y_i = a(x_i), 1 \leq i \leq n$.
3. Der Dealer gibt dem i-ten Shareholder den Share $y_i, 1 \leq i \leq n$

Bei der Rekonstruktion des Geheimnisses wird angenommen, dass t Shareholder zusammen arbeiten. Ihre Shares seien $y_i = a(x_i), 1 \leq i \leq t$. Es wird durch Ummummerierung der Shares immer erreicht. Jetzt gilt

$$a(x) = \sum_{i=1}^t y_i \prod_{j=1, j \neq i}^t \frac{x_j - X}{x_j - x_i}. \quad (3.2)$$

Diese Formel wird von den Shareholdern benutzt, um das Geheimnis zu rekonstruieren.

3.4.1.1 Shamir's Secret-Sharing bei elektronischen Wahlen

Während den elektronischen Wahlen, mit homomorpher Verschlüsselung, erfolgt die Verteilung des Secret-Keys durch den Dealer. Die Verteilung erfolgt mit Hilfe des Shamir's-Secret-Sharing an n Personen der Wahlbehörde. Sowohl der Public-Key als auch der Secret-Key werden durch den Dealer erzeugt. Während der Public-Key veröffentlicht wird, wird der Secret-Key innerhalb der Wahlbehörden verteilt. Der Dealer wählt zunächst eine Primzahl $p > t$ und $p > n$ und konstruiert danach das Polynom und berechnet gleichzeitig n Shares, die wiederum an die Shareholder verteilt werden, wobei $n \geq t$ ist.

Um den Secret-Key erneut konstruieren zu können, müssen die einzelnen Shareholder ihren entschlüsselten Share an das Bulletin-Board senden und es dort zur Verfügung stellen. Hierbei wird keine Information vom Geheimnis offen gelegt. Lediglich der entschlüsselte Share vom jeweiligen Shareholder wird an das Bulletin-Board verschickt. Es existieren n Shareholder und es werden t Shareholder benötigt, um das Geheimnis zu entschlüsseln. Dabei ist zu beachten, dass keiner den Secret-Key alleine besitzt. Jeder Shareholder entschlüsselt seinen Teil. Falls mindesten t Shareholder ihren Share entschlüsseln und an das Bulletin-Board verschicken, wird das Geheimnis entschlüsselt (siehe Abb. 3.4) .

3.4.1.2 Erfüllung der Kriterien

Es wird wieder geprüft, ob die Kriterien *Korrektheit*, *Privatheit* und *Robustheit* mit dem erweiterten Verfahren erfüllt werden konnten. Es kommen zusätzlich zu der Sicht der Wähler und die der Autorität, auch die Sicht des Dealers hinzu.

Die *Korrektheit* wird aus der Sicht der Wähler erfüllt. Oberflächlich betrachtet scheint es, dass durch die Verteilung des Secret-Keys an mehrere Autoritäten mit der Erweiterung um „Shamir's Secret-Sharing“, die *Korrektheit* aus Sicht der Wahlbehörde erfüllt wird. Leider ist dies nicht der Fall, da der Dealer vertrauenswürdig sein muss, damit das Verfahren korrekt funktionieren kann. Es wird deutlich, dass das Problem nur verschoben wird. Der Secret-Key wird verteilt und keiner der Autoritäten besitzt die Möglichkeit es alleine zu rekonstruieren. Da allerdings der Dealer den Secret-Key verteilt bzw. kennt, ist er in der Lage diesen alleinig zu rekonstruieren. Dadurch ist es für den Dealer möglich, den Inhalt zu verändern. Weder bei der Auszählung der Stimmen, noch bei der Veröffentlichung der Wahlergebnisse kann die Wahlbehörde kontrolliert werden.

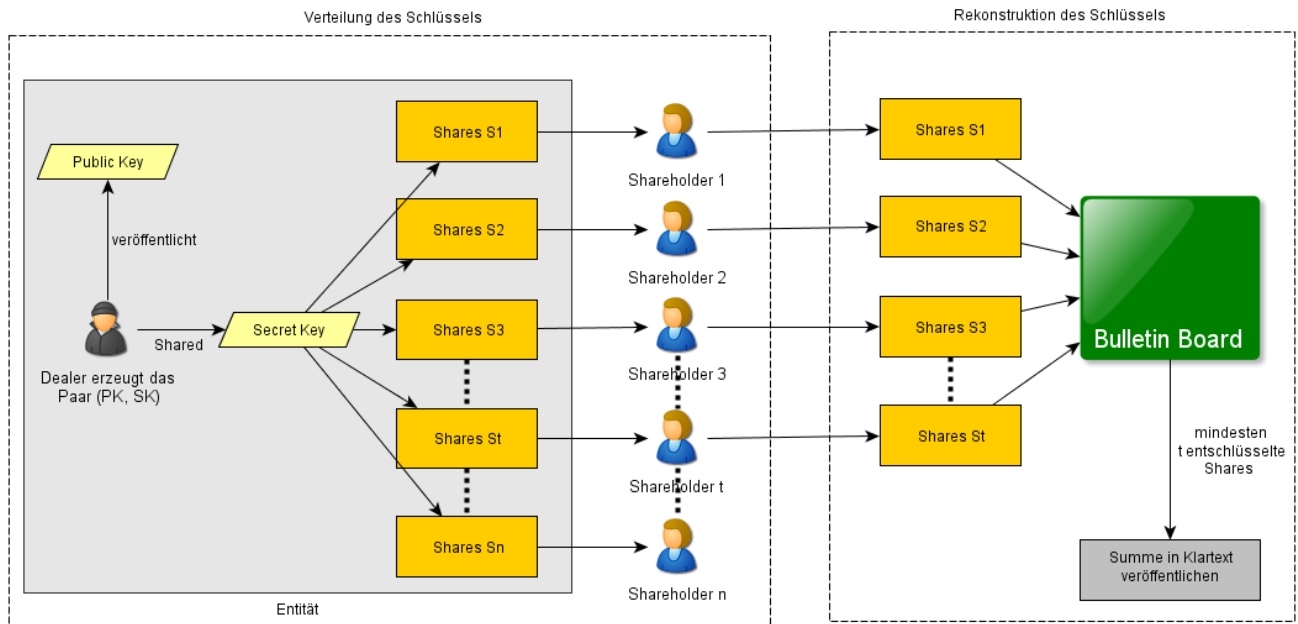


Abbildung 3.4: Shamir's Secret-Sharing

Aus der Sicht der Wahlbehörde schien es so, als ob das Kriterium *Privatheit* erfüllt wurde, da aber das Problem nur verschoben wurde wird das Kriterium *Privatheit* nicht erfüllt. Der Dealer hat die Möglichkeit, die einzelnen verschlüsselten Stimmen zu entschlüsseln. Daraus folgt, dass der Schutz vor der Wahlbehörde wieder nicht erfüllt wird.

Das Kriterium *Robustheit* wird durch das Anwenden von „Shamir's Secret-Sharing“ verbessert. So wird die Wahlbehörde verteilt und die Wahl kann bei einem eventuellen Ausfall oder bei einer eventuellen Verweigerung einzelner Autoritäten, dennoch fortgeführt werden. Dies kann nicht gewährleistet werden, wenn der Dealer ausfallen sollte oder die Wahl verweigern sollte. Daher ist das Kriterium *Robustheit* auch nicht erfüllt und muss im nächsten Schritt verbessert werden.

Es ist sichtbar, dass der Dealer und die Shareholder nicht kontrolliert werden können und somit auch die Kriterien nicht erfüllt werden. Im nächsten Abschnitt wird ein Verfahren vorgestellt, womit der Dealer und die Shareholder besser verifiziert werden können.

3.4.2 Verifiable Secret-Sharing (VSS) und Public Verifiable Secret-Sharing (PVSS)

Shamir's Secret-Sharing ist gegen das sogenannte „passive attacks“ sinnvoll. Hierbei wird angenommen, dass die Gefahren von ausserhalb kommen und dass sich die Autoritäten genau an die Regeln halten und keine bösen Absichten hegen. Gegen die sogenannte „active attack“ ist Shamir's Secret-Sharing nicht mehr sicher, da die Gefahr direkt vom Dealer oder von den Shareholder's ausgeht [Sch99]. Es muss daher sichergestellt werden, dass der Secret-Key auch nicht von den Autoritäten oder von einem Dealer alleine rekonstruiert werden kann. Weiterhin muss gesichert werden, dass die Verteilung der Shares korrekt abläuft, damit das Wahlergebnis korrekt ausfällt. Zusätzlich müssen beim Entschlüsseln und beim Auszählen die richtigen Shares verwendet werden, da falsche Shares das Ergebnis verändern könnten. Mit Verifiable Secret-Sharing wird gewährleistet, dass der Dealer und die Autoritäten sich verifizieren müssen und somit kontrolliert werden können. Die Verifizierung kann je nach Verfahren sowohl gegenüber anderen Autoritäten oder öffentlich vollzogen werden. Die Absicherung muss für folgende zwei Punkte gelten:

- Der Dealer sendet inkonsistente oder inkorrekte Shares während der Aufteilung
- Die Autoritäten geben bei der Rekonstruktion falsche Shares ab

Um diese zwei Punkte zu verhindern, muss der Dealer Verifiable Secret-Sharing (VSS) anwenden. VSS kann auch mit der Public Verifiable Secret-Sharing (PVSS) erweitert werden. Ein bekanntes Verfahren ist Feldman's VSS. Bei diesem Verfahren wird das bekannte (n,t) -Secret-Sharing benutzt und es gilt $1 \leq t \leq n$. Die Kontrolle des Dealers durch die Shareholder wird bei der Verteilung gewährleistet. Es wird angenommen, dass $g \in$ einer Gruppe G und p eine Primzahl ist, wobei $p \geq n$. Die Verteilung und die Rekonstruktion für den Dealer und die Shareholder P_1, \dots, P_n ist wie folgt definiert:

- **Die Verteilung:** Sei $s \in_R \mathbb{Z}_p$ das Geheimnis, welches vom Dealer verteilt wurde. Der Dealer wählt ein zufälliges Polynom in $\mathbb{Z}_p[x]$ mit der Form

$$a(x) = s + \alpha_1 x + \dots + \alpha_{t-1} x^{t-1},$$

und unter der Bedingung, dass $\alpha_0 = s$ ist. Der Dealer sendet die Shares $s_i = a(i)$ an die Autoritäten P_i mit $i = 1, \dots, n$ über einen sicheren Kanal zu. Weiterhin sendet der Dealer die Werte $B_j = g^{\alpha_j}, 0 \leq j < t$. Wenn die Autoritäten ihren zugehörigen Share erhalten haben, können Sie die Gültigkeit ihrer Shares mit der folgenden Formel überprüfen:

$$g^{s_i} = \prod_{j=0}^{t-1} B_j^{i^j} \tag{3.3}$$

- **Die Rekonstruktion:** Die Shares s_i der Autoritäten P_i werden mit der Gleichung 3.3 aus der Verteilung verifiziert. Nach Shamir's Verfahren werden t gültige Shares benötigt, um das Geheimnis $s = a(0)$ zu rekonstruieren.

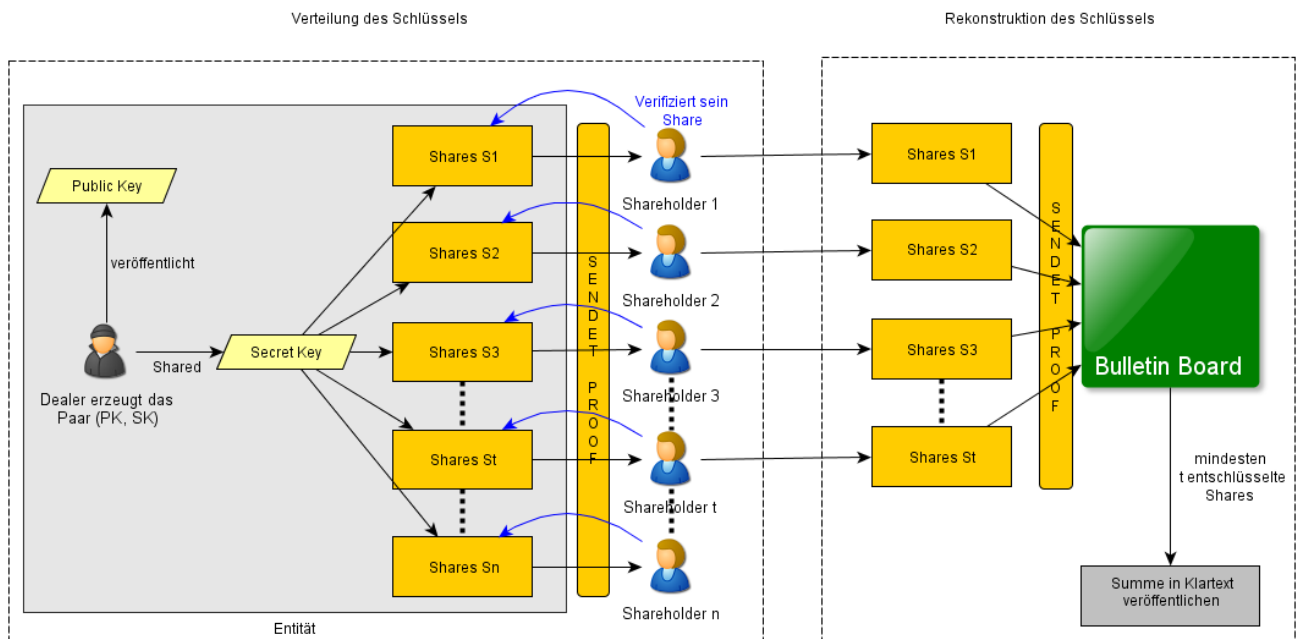


Abbildung 3.5: Verifiable Secret-Sharing

Durch die Verifizierung mit der Gleichung 3.3 ist es dem Dealer nicht möglich bei der Verteilung falsche Shares an vertrauenswürdige Autoritäten auszugeben. Der einzige Weg falsche Shares zu verteilen ist, dass der Dealer nur einigen Autoritäten falsche Shares verteilt. Falls sich mehr als t Autoritäten bei der Verifizierung beschweren, wird die Verteilung abgebrochen und der Dealer muss allen neue gültige Shares verteilen. Feldman's VSS ist also bei $t-1$ vertrauenswürdigen Autoritäten sicher.

Ein weiteres Verfahren ist das erwähnte Public Verifiable Secret-Sharing (PVSS). Die Vorgehensweise ist ähnlich wie beim VSS, nur dass hier die Verifizierung der verteilten Shares s_i nicht durch die Autoritäten P_i stattfindet, sondern von jedem öffentlich durchgeführt werden kann.

Für die Verifizierung muss ein Beweis veröffentlicht werden und hierbei wird das Chaum-Pederson Protokoll [DC98] verwendet. Es wird ein kurzer Einblick in das Protokoll gewährt und im folgenden wird dieser Beweis als $PROOF_D$ bezeichnet. Bei Chaum-Pederson Protokoll wird vorausgesetzt, dass mit dem El-Gamal Verfahren entschlüsselt wird. Ein Ciphertext $c = (\alpha, \beta)$ und ein Klartext m sind gegeben und der Prover zeigt, dass $\log_g(y) = \log_\alpha(\beta/m)$:

- Der Prüfer wählt $w \in Z_q$ und sendet $a = g^w, B = \alpha^w$ an den Verifizierer.
- Der Verifizierer Wählt $c \in Z_q$.
- Der Prüfer antwortet mit $t = w + xc$.
- Der Verifizierer kontrolliert, ob $g^t = Ay^c$ und $\alpha^t = B(\beta/m)^c$ gilt.

Es wird deutlich, wenn c und t gegeben sind, können A und B leicht berechnet werden. Das Chaum-Pederson Protokoll wird bei der Verteilung und Rekonstruktion beim PVSS verwendet.

Die Verteilung und die Rekonstruktion finden wieder wie folgt statt:

- **Die Verteilung:** Das Protokoll besteht aus zwei Schritten.

1. Verteilung des Shares

Die Verteilung von einem Geheimnis $s \in \Sigma$ wird durch den Dealer D ausgeführt. Der Dealer generiert die entsprechenden Shares s_i für die Autoritäten P_i , für $i = 1, \dots, n$. Für jede Autorität P_i veröffentlicht der Dealer den verschlüsselten Share $E_i(s_i)$. Zudem wird auch ein Beweis $PROOF_D$ veröffentlicht, um zu zeigen, dass jeder E_i einen Share s_i verschlüsselt. Darüber hinaus liefert der Beweis $PROOF_D$ die Garantie, dass bei der Rekonstruktion das gleiche Geheimnis s verwendet wird.

2. Verifikation der Shares

Alle Teilnehmer, welche den öffentlichen Schlüssel für die Verschlüsselung E_i kennen, können den Share verifizieren. Ein nicht-interaktiver Verifikationsalgorithmus kann überprüfen, dass der Beweis $PROOF_D$ für alle Autoritäten P_i mit $E_i(s_i)$ korrekt verschlüsselt wurde. Falls ein Verifizierer bemerkt, dass der Beweis nicht korrekt ist, wird es reklamiert und veröffentlicht. Da jeder, der den öffentlichen Schlüssel kennt, eine Verifizierung durchführen kann, kann jeder überprüfen, ob die Reklamation angebracht ist. Es wird im voraus festgelegt, bei wie vielen Reklamationen das Protokoll abgebrochen wird.

- **Die Rekonstruktion:** Das Protokoll besteht aus zwei Schritten.

1. Entschlüsselung der Shares

Die Autoritäten entschlüsseln Ihr Share s_i vom $E_i(s_i)$. Es ist nicht nötig, dass alle Autoritäten ihren Share entschlüsseln. Die Autoritäten liefern zu den entschlüsselten Share s_i zusätzlich ein Beweis $PROOF_{P_i}$, welches zeigt, dass die Angaben korrekt sind.

2. Vereinigung der Shares

Durch den Beweis $PROOF_{P_i}$ können die nicht vertrauenswürdigen Autoritäten und die Autoritäten mit fehlerhaft verteilten Shares ausgeschlossen werden. Dadurch sind nur noch die Autoritäten vorhanden, welche vertrauenswürdig sind und diese können ihre Shares zusammensetzen, um das Geheimnis s zu entschlüsseln.

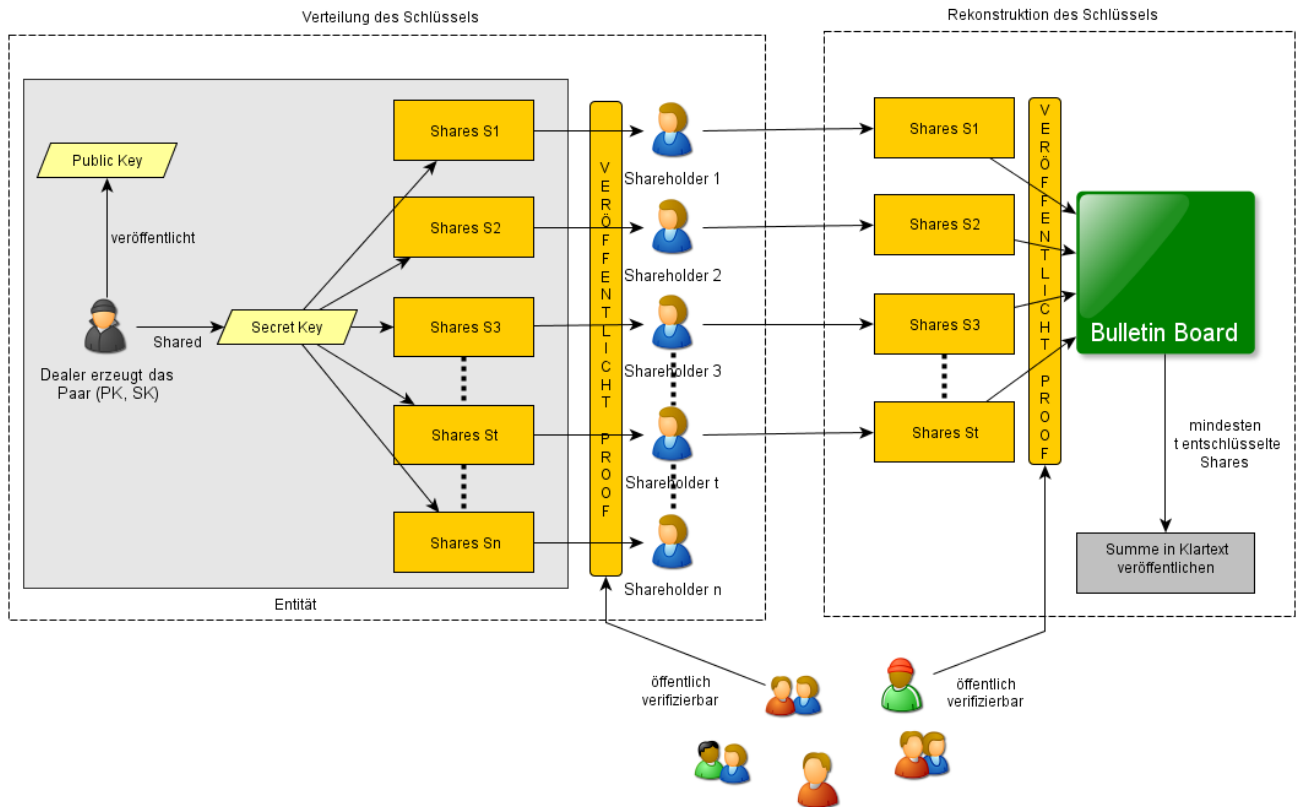


Abbildung 3.6: Public Verifiable Secret-Sharing

Bei VSS müssen die Empfänger überprüfen, ob der Dealer auch korrekte Shares verteilt hat. Dies fällt bei nicht-interaktiven PVSS aus, da jeder die Ausgabe vom Dealer verifizieren kann. Bei elektronischen Wahlen ist es besser nicht-interaktive PVSS zu verwenden, da die Shares, welche vom Dealer verteilt werden von jedem verifiziert werden können und dadurch eine höhere Transparenz der Wahl gewährleistet werden kann.

3.4.2.1 Public Verifiable Secret-Sharing bei elektronischen Wahlen

Bei elektronischen Wahlen wird das nicht-interaktive PVSS verwendet, damit die Wahl auch öffentlich verfolgt werden kann und nachvollziehbar ist. Hierbei erzeugt der Dealer das Paar Public-Key/Secret-Key und veröffentlicht den PK. Der SK wird in Shares zerteilt und unter den Shareholdern verteilt. Zusätzlich sendet der Dealer einen nicht-interaktiven Beweis, damit die Shares auch öffentlich verifizierbar sind. Somit kann jeder, der den PK besitzt, auch die Shares verifizieren. Äquivalent muss der Dealer auch ein Beweis senden, dass die Korrektheit der Rekonstruktion zeigt. Das gleiche gilt auch für die Shareholder. Sie senden ein Beweis mit dem Share, so dass diese öffentlich verifizierbar ist.

3.4.2.2 Erfüllung der Kriterien

Durch die Erweiterung mit PVSS wurde wiederholt geprüft, ob die Kriterien *Korrektheit*, *Privatheit* und *Robustheit* erfüllt werden können.

Da der Wähler ein Beweis mit seiner Stimmen sendet, wird das Kriterium *Korrektheit* aus seiner Sicht erfüllt. Auch aus der Sicht des Shareholders wird *Korrektheit* erfüllt, da die Shareholder einen Beweis senden müssen, dass bei der Zusammensetzung die Shares korrekt sind. Bei der Verteilung der Shares wird der Dealer auch verifiziert und dadurch

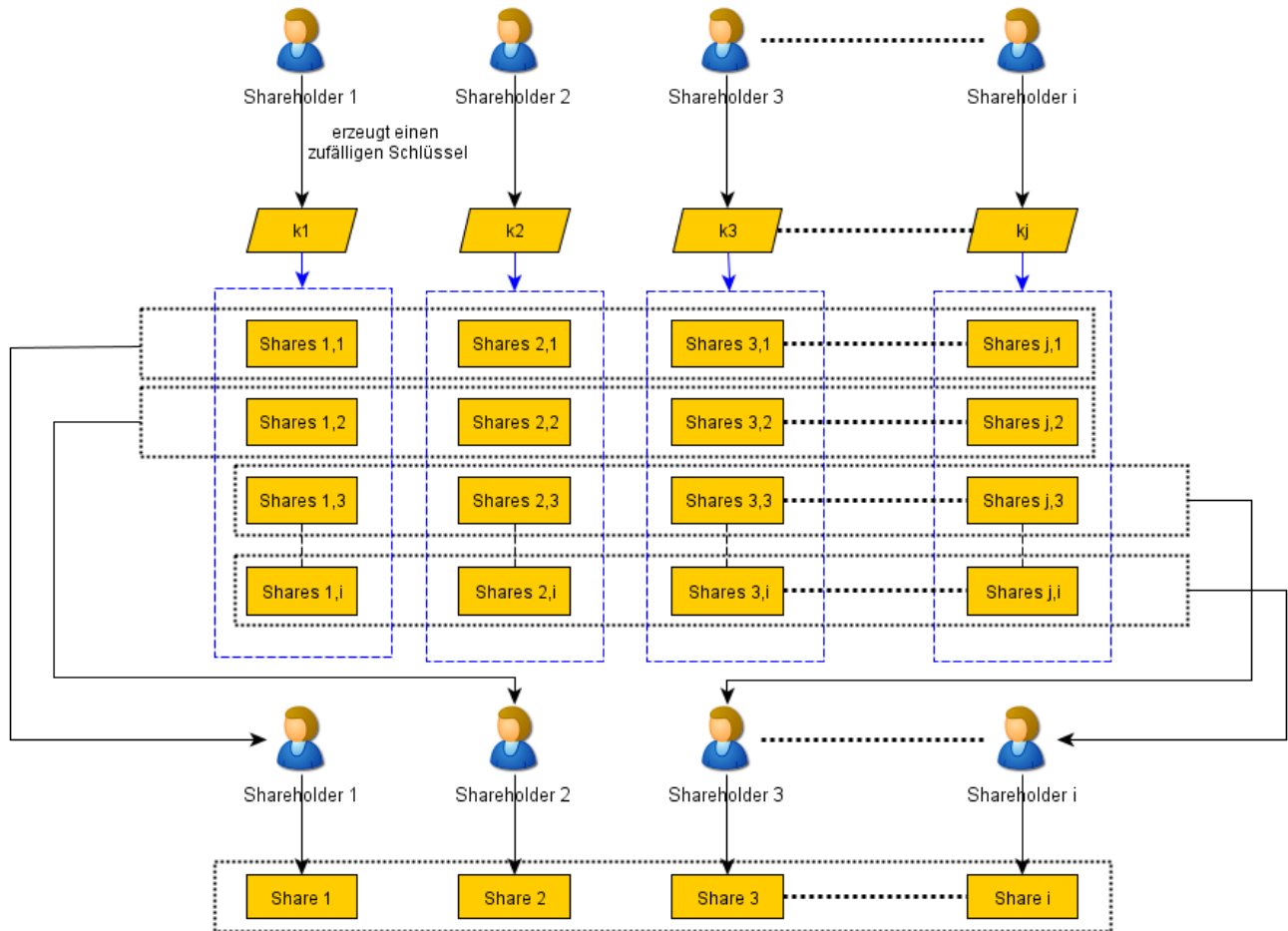


Abbildung 3.7: Secret-Sharing ohne Dealer

wird gewährleistet, dass die Shares korrekt verteilt werden. Der Dealer erzeugt immer noch alleine das Paar PK/SK und ist damit in der Lage, seine Position auszunutzen. Dadurch wird das Kriterium der *Korrektheit* nicht gänzlich erfüllt, so dass nach besseren Lösungen gesucht werden muss.

Robustheit wird aus der Sicht der Shareholder komplett erfüllt, da diese einen Beweis liefern müssen und nur ein Teil der Shareholder ausreicht, um die Wahl fortzuführen. Aus der Sicht des Dealers wird *Robustheit* nur zum Teil erfüllt. Durch die Erweiterung mit PVSS muss der Dealer korrekte Shares an die Shareholder verteilen. Gegen eine mögliche Verweigerung oder einen Ausfall des Dealers, gibt es bislang keine Absicherung und somit kann *Robustheit* noch nicht gewährleistet werden.

Da der Dealer immer noch den PK/SK kennt, ist die *Privatheit* nicht erfüllt. Durch die Erweiterung mit PVSS wurden aus der Sicht der Shareholder die Schwachstellen abgedeckt. Das Problem mit dem Dealer hingegen besteht weiterhin. Im nächsten Abschnitt wird ein Verfahren vorgestellt, das aufzeigt, wie der Dealer gemieden werden kann.

3.4.3 Secret-Sharing ohne Dealer

Bei den bisherigen Vorgehensweisen wurde deutlich, dass das Vertrauensproblem hinsichtlich der Wahlbehörde nicht gelöst werden konnte, falls der Dealer nicht vertrauenswürdig ist. Der Dealer generiert das Paar (PK, SK) alleine, kennt somit die Keys und stellt somit eine potenzielle Gefahr dar. Die Zerteilung des Secret-Keys sowie die Verteilung an die Shareholder erfolgt auch durch den Dealer und wird durch den Verifiable Secret-Sharing Verfahren kontrolliert.

Auch die Shareholder werden mit diesem Verfahren kontrolliert. Eine sicherere Vorgehensweise ist, dass die Autoritäten gemeinsam das Paar generieren, zerteilen und verteilen. Somit wird der Dealer vermieden. Diese Vorgehensweise wird von Yvo Desmedt in [Des03] beschrieben. Ein wichtiges Merkmal dabei ist, dass keiner der Autoritäten den SK selber generieren kann und kennt (siehe Abbildung 3.7).

Definition: Es wird vorausgesetzt, dass die homomorphe Eigenschaft erfüllt sein muss. Dies wird mit Shamir's Secret-Sharing erfüllt. Seien (s_1, s_2, \dots, s_l) Shares von einem Schlüssel k . Ebenso seien $(s'_1, s'_2, \dots, s'_l)$ Shares von Schlüssel k' , wobei $1 \leq i \leq l$ ist und t die Anzahl der Shareholder ist.

1. Der erste Teilnehmer erzeugt einen zufälligen Schlüssel k_1 und ist gleichzeitig der Verteiler.
2. Die Shares $(s_{1,1}, s_{1,2}, \dots, s_{1,l})$ werden vom Verteiler erzeugt, wobei $1 \leq i \leq l$ gilt.
3. Der Verteiler sendet mit einem sicheren Kanal die Shares $s_{1,i}$ an die Teilnehmer i .
4. Die Teilnehmer erzeugen Shares $s_{j,i}$ anstelle von den Shares $s_{1,i}$ und senden diese an die Teilnehmer i .
5. Ein Teilnehmer i berechnet den Share $s_i = \sum_{j \in B} s_{j,i}$ für $j \in B, B \in \Gamma$ und $B \subset A$.
6. Durch die homomorphe Eigenschaften ist s_i ein Share vom Schlüssel $k = \sum_{j \in B} k_j$ für $j \in B$.
7. t Shareholder werden benötigt, um den Schlüssel k zu generieren.

Sowohl die Generierung der Schlüssel, als auch die Zerteilung und die Verteilung erfolgen nicht mehr vom Dealer, sondern gemeinsam durch die Autoritäten. Da ein zufällig gewählter Schlüssel k_1 von dem ersten Teilnehmer erzeugt wird und die folgenden Shares davon abhängen, kennt keiner der Autoritäten den geheimen Schlüssel. Die Zusammensetzung des Shares kann nur mit t Shareholders berechnet werden. Dafür müssen die Shares zusammengesetzt werden. Weniger als t Shareholders sind nicht in der Lage den Schlüssel zusammenzusetzen oder Information über ihn zu erhalten.

3.4.3.1 Secret-Sharing ohne Dealer bei elektronischen Wahlen

Da der Dealer nicht mehr vorhanden ist, muss die Wahlbehörde das Paar (PK, SK) gemeinsam erzeugen. Hierfür wird eine Autorität aus der Wahlbehörde als Verteiler auserwählt. Dieser generiert einen zufälligen Schlüssel k_1 und teilt diesen in Shares auf. Keiner der Autoritäten hat den geheimen Schlüssel k . Die Shares werden an die Teilnehmer verteilt. Die verteilten Shares wiederum werden nochmals in Shares verteilt. Nur mit der Zusammensetzung aller Shares $s_{j,i}$ kann ein Share s_i generiert werden. Durch die homomorphe Eigenschaft kann durch den Share s_i der geheime Schlüssel berechnet werden. Es werden erneut mindestens t Shareholder benötigt, um den geheimen Schlüssel zu generieren.

Nachdem der Dealer ausgefallen ist, müssen die einzelnen Verfahren kombiniert werden. Das Public Verifiable Secret-Sharing muss mit dem Secret-Sharing ohne Dealer kombiniert werden, um gewährleisten zu können, dass die Shareholder verifizierbar sind. Hierbei müssen die einzelnen Shareholder einen Beweis liefern, dass die Shares korrekt sind. Dies kann von jedem öffentlich verifiziert werden (siehe Kapitel 3.4.2).

Abschliessend verdeutlicht Abbildung 3.8 das homomorphe Verschlüsselungsverfahren mit dem Zero-Knowledge-Proof und dem PVSS.

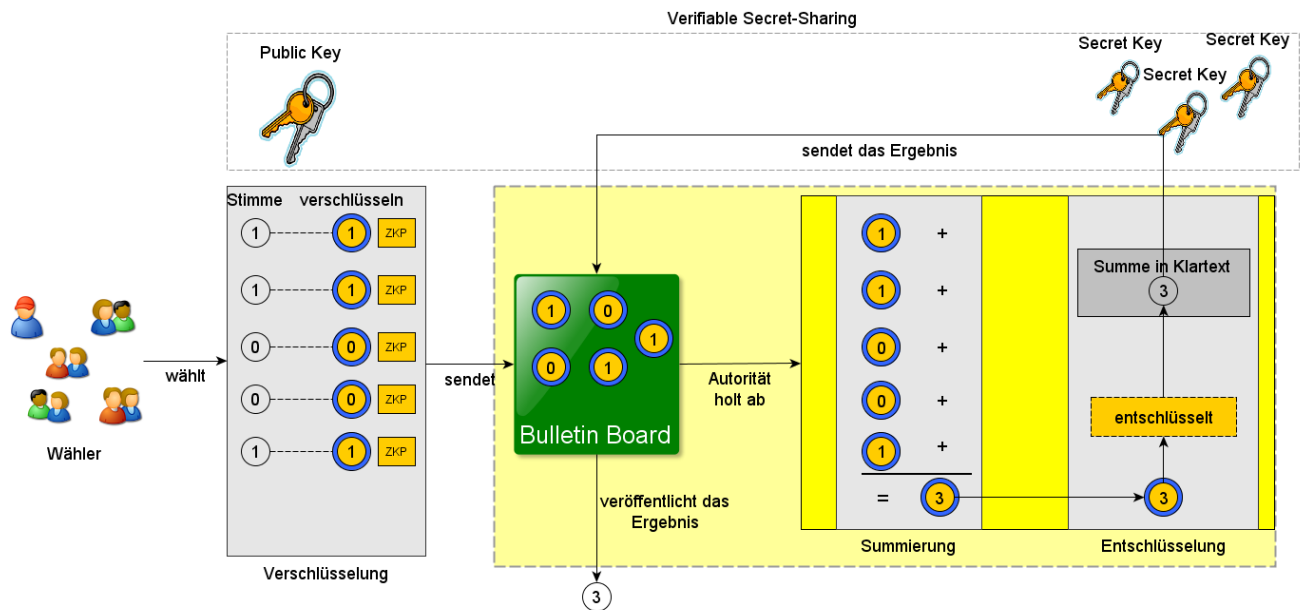


Abbildung 3.8: homomorphe Verschlüsselungsverfahren mit Zero-Knowledge-Proof und Public Verifiable Secret-Sharing

3.4.3.2 Erfüllung der Kriterien

Die Kriterien *Robustheit*, *Privatheit* und *Korrektheit* werden erneut geprüft. Bislang konnten die Kriterien bei den vorherigen Kapitel nicht erfüllt werden, da ein Dealer existierte.

Robustheit wurde zwar aus der Sicht der Shareholder erfüllt, doch im Falle eines eventuellen Ausfalls oder eine Verweigerung des Dealers, bestünde die Gefahr, dass die Wahl nicht mehr fortgesetzt werden könnte. Da die Autoritäten gemeinsam den Schlüssel generieren und von n Shareholder nur t Shareholder den Schlüssel generieren können, ist *Robustheit* gewährleistet. Die Anzahl der Shareholder ist n und t ist die minimale Anzahl der Shareholder, um den Schlüssel zu generieren.

Die Stimme des Wählers wurde zwar verschlüsselt an das Bulletin-Board verschickt, da der Dealer aber den geheimen Schlüssel besitzt, konnte er die Stimmen entschlüsseln. Durch den Wegfall des Dealers besteht keine Gefahr mehr, dass die einzelnen Stimmen entschlüsselt werden können. Das Kriterium der *Privatheit* wird demnach erfüllt.

Das Kriterium *Korrektheit* wurde bereits in den vorherigen Abschnitten erfüllt und muss hier nicht weiter ausgeführt werden.

Die Annahme, dass alle Kriterien erfüllt werden müssen, wurde bereits zu Beginn der Arbeit angeführt. Im Verlauf der Arbeit wurde deutlich gemacht, dass sich das homomorphe Verschlüsselungsverfahren eignet. Mit der Erweiterung des PVSS und Secret-Sharing ohne Dealer konnten diese Kriterien erfüllt werden. Das MIX Verfahren wird im weiteren Verlauf dieser Arbeit beschrieben und erneut wird zu prüfen sein, ob sich das Verfahren eignet, um die Kriterien zu erfüllen. Falls sich das MIX Verfahren bewähren kann, werden die Verfahren homomorphe Verschlüsselung und MIX Verfahren vergleichend gegenüber gestellt.

4 Das MIX Verfahren

Im vorangegangenen Kapitel wurde gezeigt wie Wahlstimmen mit homomorphen Verschlüsselungsverfahren verschlüsselt, in verschlüsselter Form verarbeitet d.h. addiert und schliesslich ausgewertet werden. Im Gegensatz zu diesem Verfahren, welches homomorphe Eigenschaften der Verschlüsselungsfunktion ausnutzt, steht das MIX Verfahren: Basierend auf der in [Cha81] beschriebenen Arbeit von David Chaum, der eine Vorgehensweise entwickelte um mit Hilfe von Public-Key-Infrastrukturen anonyme Kommunikationswege zu erstellen, wird im Folgenden die Anwendungsmöglichkeit von MIX Netzen bei elektronischen und Internetwahlen beschrieben. Dabei wird zunächst der von Chaum entwickelte Ansatz dargestellt, der dann sukzessive um Elemente zur Steigerung von *Robustheit*, *Privatheit* und *Korrektheit* erweitert wird.

4.1 Decryption MIX (Onion MIX)

In einem *Decryption MIX Netz* wird das Wahlverfahren ähnlich dem klassischen Wahlverfahren mit Papierstimmzettel durchgeführt: Der Wähler verschlüsselt seine Wahlstimme („Falten des ausgefüllten Wahlzettels“) und veröffentlicht diese auf dem Bulletin Board („Urnengang“). Das Verschlüsseln erfolgt mit jeweils n verschiedenen öffentlichen Schlüsseln von n MIX Servern. Die Wahlstimme wird sequentiell, beginnend mit dem öffentlichen Schlüssel des letzten MIX und endend mit dem ersten MIX des Nachrichtenpfades verschlüsselt.

Wie in Abbildung 4.3 veranschaulicht wird dieses n -fach verschlüsselte Datenpaket an MIX 1 geschickt. MIX 1 entfernt die erste Verschlüsselung, mischt die erhaltenen Datenpakete (s. Abb. 4.2) und verschickt die Datenpakete an den MIX Server dessen öffentlicher Schlüssel für die darunterliegende Verschlüsselung verwendet wurde. Die Datenpakete werden solange weitergereicht bis alle Verschlüsselungsschichten durch die jeweiligen MIX Server abgetragen worden sind. Aus der bildlichen Vorstellung der Durchführung dieses Verfahrens rührt auch der Name *Onion Decryption MIX*.

Chaum beschreibt in [Cha81] ein System mit n MIX Servern, die jeweils ein asymmetrisches Schlüsselpaar $((p, g, \alpha), a)$ mit folgenden Eigenschaften besitzen:

- Öffentlicher Schlüssel (p, g, α) : Verschlüsselung von Nachricht m mit (p, g, α) resultiert in $\text{enc}(m) = C$
- Geheimer Schlüssel (a) : Entschlüsselung von verschlüsselter Nachricht C mit geheimen Schlüssel (a) resultiert in $\text{dec}(C) = m$
- Invertierbarkeit: Es gilt $\text{dec}(\text{enc}(m)) = \text{enc}(\text{dec}(m)) = m$

Diese Schlüsselpaare werden zur Verschlüsselung von Nachrichten, die zwischen den Servern verschickt werden, eingesetzt. MIX Server können in Kaskaden oder in Netzen angeordnet werden.

Um gewährleisten zu können, dass kein beliebiger Beobachter einen Zusammenhang zwischen Eingang und Ausgang eines Datenpakets innerhalb eines MIX Servers, und somit sukzessive einen Zusammenhang zwischen einem Wähler und dessen abgegebenen Wahlstimme herstellen kann, ist es erforderlich den Weg, den ein Datenpaket nimmt, zu verschleiern. Einerseits wird dies durch Hinzunahme von Zufallswerten r zu jedem Datenpaket erreicht, so dass es dem MIX Server möglich ist immer Pakete gleicher Größe zu versenden. Andererseits kommt das wichtigste Merkmal eines MIX Servers zum Einsatz, welcher er auch seinen Namen zu verdanken hat: Das Mischen (*shuffle*) von Datenpaketen bevor sie wieder ausgegeben werden.

Bei einer Annahme von $n-1$ korrupten MIX Servern wäre somit noch immer gewährleistet, dass die Anonymität gesichert ist, da es immer noch einen ehrlichen Server gibt der korrekt mischt und damit die Anonymität aufrecht erhält. Diese Vorgehensweise wird in jedem MIX Verfahren unabhängig von der Art des Einsatzes der MIX Server angewendet.

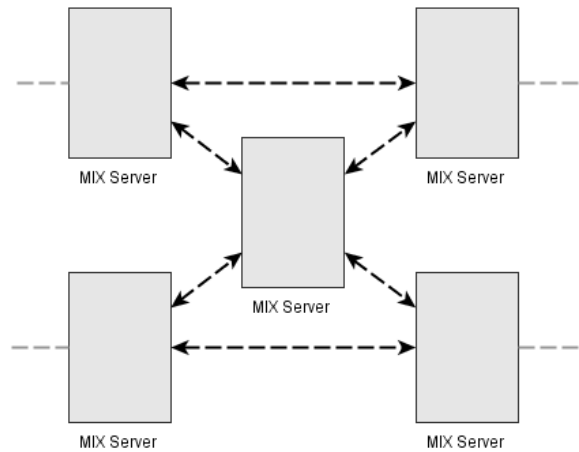


Abbildung 4.1: Schematische Darstellung von verbundenen MIX Servern zu einem MIX Netz

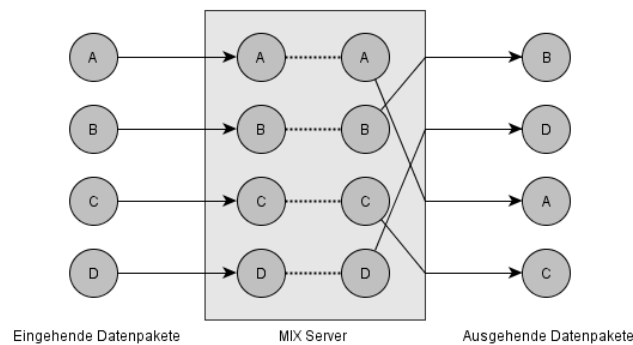


Abbildung 4.2: Shuffle: Mischen von Datenpaketen während dem Passieren eines MIX Servers

Chaum legte diesem Modell folgende Annahmen zugrunde:

- Es kann von außen keine Beziehung zwischen einer Menge von verschlüsselten und den dazu korrespondierenden Nachrichten in Klartext aufgezeigt werden ohne die Kenntnis über den Zufallswert, der bei der probabilistischen Verschlüsselung verwendet wurde, oder den entsprechenden geheimen Schlüssel zu haben.
- Jeder kann Herkunft, Ziel oder Darstellung aller Nachrichten im zugrunde liegenden Kommunikationssystem erfahren und Nachrichten einfügen, löschen oder modifizieren

4.1.1 Allgemeiner Ablauf des Decryption MIX Verfahrens

Wie eingangs beschrieben werden auf die abzugebende Wahlstimme m , n öffentliche Schlüssel $(p, g, \alpha)_i$ durch die jeweiligen Verschlüsselungsfunktionen enc_i angewendet. Diese werden während des Ablaufs des Verfahrens sukzessive mit dem jeweiligen geheimen Schlüssel $(a)_i$ durch Anwendung von Entschlüsselungsoperationen dec_i abgetragen. Dabei bezeichnet $(p, g, \alpha)_i$ den öffentlichen Schlüssel des i -ten Servers und $(p, g, \alpha)_{Rec}$ den öffentlichen Schlüssel des letzten Servers („Receiver“). Analog dazu sind die Bezeichnungen für die geheimen Schlüssel $(a)_i$ und $(a)_{Rec}$ gewählt.

r_n und r_{Rec} bezeichnen dabei die Zufallswerte die für die probabilistische Verschlüsselung genutzt werden und zur Verschleierung der Beziehung zwischen n -fach und $n-1$ -fach verschlüsselter Wahlstimme m dienen. A_{Rec} bezeichnet die Adresse des Bestimmungsorts der versendeten Wahlstimme.

1. Zu verschickende Wahlstimme m wird mit öffentlichem Schlüssel des Empfängers Rec probabilistisch verschlüsselt:
 $enc_{Rec}(r_{Rec}, m)$
2. Die verschlüsselte Wahlstimme $enc_{Rec}(r_{Rec}, m)$ wird zusammen mit der Empfängeradresse A_{Rec} mit den öffentlichen Schlüssel der MIX Server verschlüsselt:

$$enc_1(r_1, \dots (enc_n(r_n(A_{Rec}, enc_{Rec}(r_{Rec}, m))))))$$

3. Der Sender Sdr sendet

$$enc_1(r_1, \dots (enc_n(r_n(A_{Rec}, enc_{Rec}(r_{Rec}, m))))))$$

an den ersten MIX Server

4. MIX-Server i entschlüsselt

$$dec_i(enc_i(r_i, \dots (enc_n(r_n(A_{Rec}, enc_{Rec}(r_{Rec}, m)))))) = enc_{i+1}(r_{i+1}, \dots (enc_n(r_n(A_{Rec}, enc_{Rec}(r_{Rec}, m))))))$$

durch Anwendung seines geheimen Schlüssels $(a)_i$

5. MIX Server i mischt

$$enc_{i+1}(r_{i+1}, \dots (enc_n(r_n(A_{Rec}, enc_{Rec}(r_{Rec}, m))))))$$

und versendet dies an MIX Server $i + 1$

6. Die verschlüsselte Wahlstimme $enc_n(r_n(A_{Rec}, enc_{Rec}(r_{Rec}, m)))$ wird durch den letzten MIX Server zu $enc_{Rec}(r_{Rec}, m)$ entschlüsselt und an den Empfänger mit der Adresse A_{Rec} gesendet

7. Empfänger Rec entschlüsselt $dec_{Rec}(enc_{Rec}(r_{Rec}, m)) = r_{Rec}, m$ durch Anwendung seines geheimen Schlüssels $(a)_{Rec}$

Abbildung 4.3 veranschaulicht die oben beschriebenen Operationen:

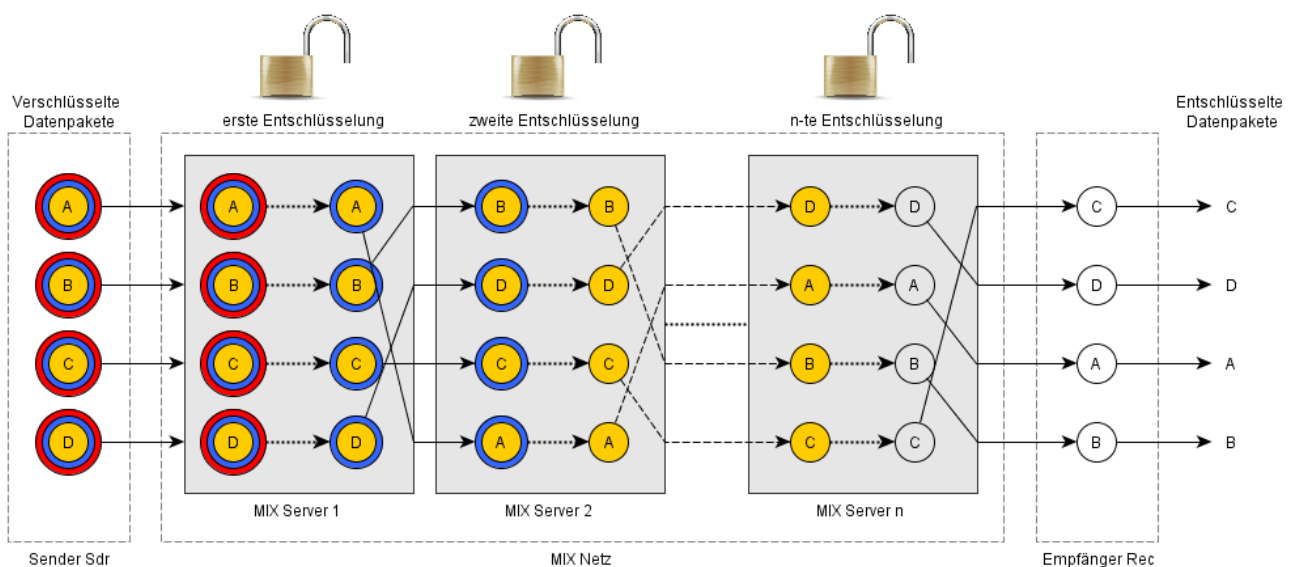


Abbildung 4.3: Sequentielle Entschlüsselungen von Nachrichten A, B, C, D in einer MIX Kaskade

4.1.2 Anwendung des Decryption MIX Verfahrens bei elektronischen Wahlen

Bei der Anwendung des Decryption MIX Verfahren bei elektronischen Wahlverfahren wird ein Schwarzes Brett (*Bulletin Board*) zur Kommunikation zwischen den einzelnen MIX Servern und zur Veröffentlichung der Zwischenschritte verwendet. Somit besteht nicht notwendigerweise ein direkter Kommunikationskanal zwischen den MIX Servern. Der Ablauf des Verfahrens, analog zum allgemeinen Decryption MIX Verfahren, lässt sich wie folgt beschreiben:

- Die Wahlstimme wird, analog zum allgemeinen Decryption MIX Verfahren, mit dem öffentlichen Schlüssel der MIX Server verschlüsselt und auf dem Bulletin Board publiziert
- MIX Server i holt sich die k -fach verschlüsselte Wahlstimme vom Bulletin Board ab und entfernt die jeweils oberste Verschlüsselungsschicht und legt die $k-1$ -fach verschlüsselte Wahlstimme nach dem Mischen wieder auf dem Bulletin Board ab
- Nach der Entschlüsselungsoperation des letzten MIX Servers wird die Wahlstimme in Klartext auf dem Bulletin Board publiziert

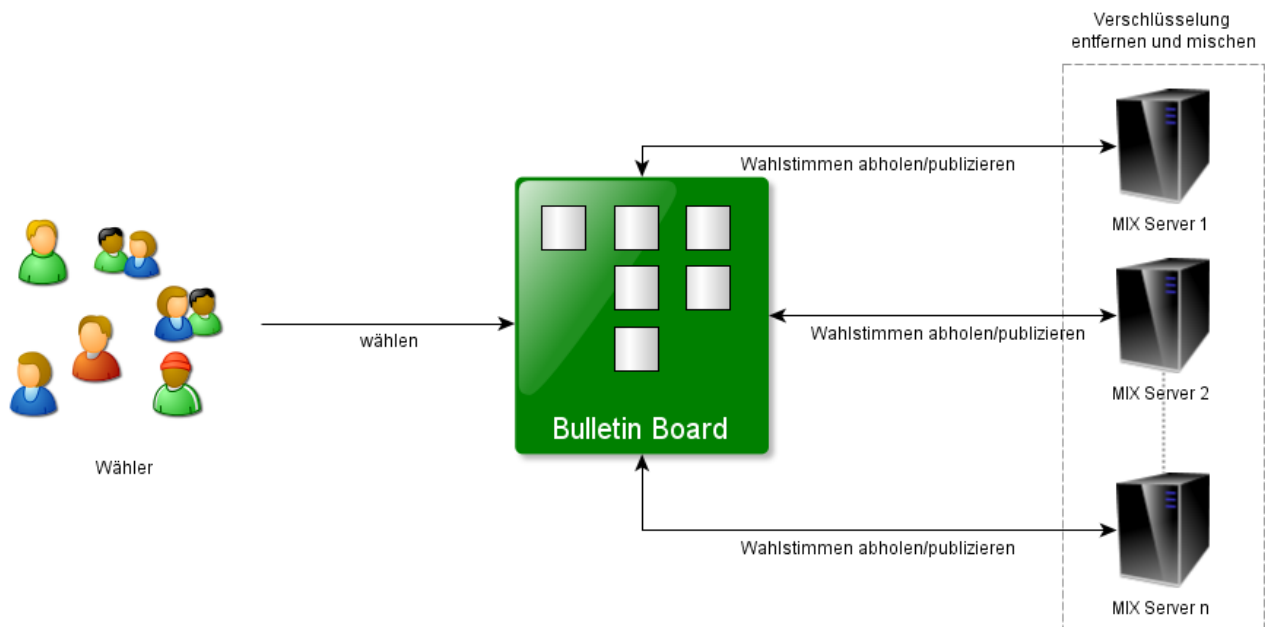


Abbildung 4.4: Anwendung des Decryption MIX Verfahrens mit Bulletin Board

4.1.3 Erfüllung der Kriterien

Die *Robustheit* dieses Verfahrens ist offensichtlich stark an der Ausfallsicherheit der einbezogenen MIX Server gekoppelt. Fällt auch nur ein MIX Server aus, können gemäß Abbildung 4.3 die noch bestehenden Verschlüsselungen nicht verarbeitet werden. So wird der ganze Wahlprozess blockiert, bis der betroffene Server ersetzt worden ist. Da der letzte MIX Server die entschlüsselten Datenpakete weiterreicht, kann so im Falle eines korrupten letzten MIX Servers die Blockade einer Wahl absichtlich herbeigeführt werden falls das Ergebnis nicht günstig erscheint. Zudem neigt dieses Verfahren mit der Anzahl der teilnehmenden Server zu Nachrichtenexpansion, da bei n Server die zu übertragende Wahlstimme n mal verschlüsselt werden muss.

Die *Privatheit* des Wählers wird, wie bei einer klassischen Wahl mit Papierstimmzettel, durch das Mischen aller Wahlstimmen in jedem MIX Server gewährleistet. Zudem werden die Wahlstimmen n -mal verschlüsselt, so dass außer dem

ersten MIX Server kein anderer MIX Server den Ursprung der Wahlstimme kennt. Ist eine Wahlstimme durch alle MIX Server gelaufen und ist die Annahme, das mindestens ein MIX Server korrekt arbeitet, wahr, kann kein Zusammenhang zwischen Wähler und Wahlstimme hergestellt werden.

Die *Korrektheit* wird in diesem Verfahren durch keinen Schritt nachweisbar verifiziert: Weder wird überprüft, ob ein Datenpaket, welches im jeweiligen MIX Server eingegangen ist, auch (in entschlüsselter Form) wieder ausgeht, noch ob unerlaubt generierte Datenpakete durch einen korrupten MIX Server den Weg in das MIX Netz finden.

Zusammenfassend sind hier die Defizite ganz klar bei der *Robustheit* und der *Korrektheit* zu sehen. Im folgenden Abschnitt wird ein Verschlüsselungsverfahren mit homomorphen Eigenschaften eingesetzt werden, um anstatt sequentieller, n-facher Verschlüsselung n-malige Wiederverschlüsselung anwenden zu können. So ist es möglich Blockaden einzelner MIX Server vorbeugen und so die *Robustheit* des MIX Verfahrens steigern zu können. Außerdem werden *secret-sharing Mechanismen* verwendet, um die auf einen einzigen MIX Server konzentrierte Kontrolle über das Wahlergebnis aufzulösen.

4.2 Re-encryption MIX

Die n-fache Verschlüsselung der Wahlstimme mit n verschiedenen öffentlichen Schlüsseln von MIX Servern kann bei einem MIX Netz mit korrupten oder defekten MIX Servern dazu führen, dass der gesamte Wahlprozess abgebrochen werden muss, da die verschlüsselten Wahlstimmen nur bis zum Erreichen des korrupten bzw. defekten MIX Servers entschlüsselt werden können. Um sich dieser Abhängigkeit von jedem einzelnen MIX Server zu entledigen, können Verschlüsselungsverfahren mit homomorphen Eigenschaften eingesetzt werden. Mit diesen Verfahren ist es möglich eine Wahlstimme m mit einem öffentlichen Schlüssel (p, g, α) unter Anwendung der Verschlüsselungsfunktion enc probabilistisch zu Darstellungen C_i wiederzuverschlüsseln (*re-encryption*), um sie schliesslich mit dem geheimen Schlüssel (a) unter der Anwendung der Entschlüsselungsfunktion dec zur Wahlstimme m in Klartext zu entschlüsseln:

$$m \xrightarrow{enc(m)} C_1 \xrightarrow{enc(C_1)} C_2 \xrightarrow{enc(C_2)} \dots \xrightarrow{enc(C_{n-1})} C_n \xrightarrow{dec(C_n)} m \quad (4.1)$$

Gleichung 4.1 zeigt schematisch, dass die probabilistische Wiederverschlüsselung die Darstellung der verschlüsselten Wahlstimme nach jeder Verschlüsselung ändert. Da nur ein Schlüsselpaar für diese Verschlüsselungsoperationen verwendet wird, kann der Ausfall eines beliebigen MIX Servers flexibler behandelt werden, so dass der Wahlprozess in solch einem Fall nicht mehr abgebrochen werden muss. Darüber hinaus ist zur Entschlüsselung nur noch eine Entschlüsselungsoperation notwendig. So wird die Anzahl der Entschlüsselungsoperationen minimiert und die Nachrichtenexpansion, die wie beim Decryption MIX Verfahren durch das mehrfache Verschlüsseln entsteht, vermieden.

Durch die Anwendung von *Secret-Sharing Mechanismen* (s. Abschn. 3.4), entfällt zudem die Schwachstelle des einzelnen (korrupten) MIX Servers, der durch die alleinige Kenntnis über den geheimen Schlüssel, das Wahlergebnis nach Belieben blockieren („Es wird keine Ergebnis herausgegeben“) oder verfälschen („Nach der Entschlüsselung der Wahlstimmen werden diese verändert, gelöscht oder dupliziert“) kann.

Nach [Riv04] kann zur Wiederverschlüsselung der Daten zum Beispiel das *El-Gamal Verschlüsselungsverfahren* (s. Abschn. 2.2) angewendet werden. Dieses Verfahren wird im weiteren Verlauf dieser Arbeit immer wieder beispielhaft betrachtet werden, obgleich auch andere Verfahren mit ähnlichen Eigenschaften existieren¹.

¹ RSA Verschlüsselungsverfahren

4.2.1 Ablauf des Re-encryption MIX Verfahrens mit El-Gamal

Nach einem initialen Verschlüsseln der Nachricht wird das so verschlüsselte Datenpaket durch n MIX Server geschleust und in jedem dieser Server gemischt, um die Anonymisierung des Datenpakts gewährleisten zu können. Nach dem passieren aller beteiligten MIX Server, wird das Datenpaket im letzten Schritt mit Hilfe des verteilten, geheimen Schlüssels a zur Wahlstimme in Klartext entschlüsselt.

1. Ein verteiltes Schlüsselpaar wird nach dem El-Gamal Verschlüsselungsverfahren generiert. Dabei bezeichnet (p, g, α) den öffentlichen und a den geheimen, verteilten Schlüssel
2. Alle Daten, die in Klartext vorliegen, werden mit Hilfe des öffentlichen Schlüssels (p, g, α) zu Verschlüsselungen $C_{1,0}, \dots, C_{1,n}$ transformiert
3. Jeder MIX Server i generiert aus den eingegangenen Datenpaketen $C_{i-1,0}, \dots, C_{i-1,n}$ wieder verschlüsselte Datenpakete $C_{i,0}, \dots, C_{i,n}$ die nach dem Mischen ausgegeben werden
4. Im letzten Schritt werden die verschlüsselten Datenpakete anhand des verteilten Schlüssels kollektiv durch eine Mindestanzahl an Shareholdern entschlüsselt (s. Abschn 3.4)

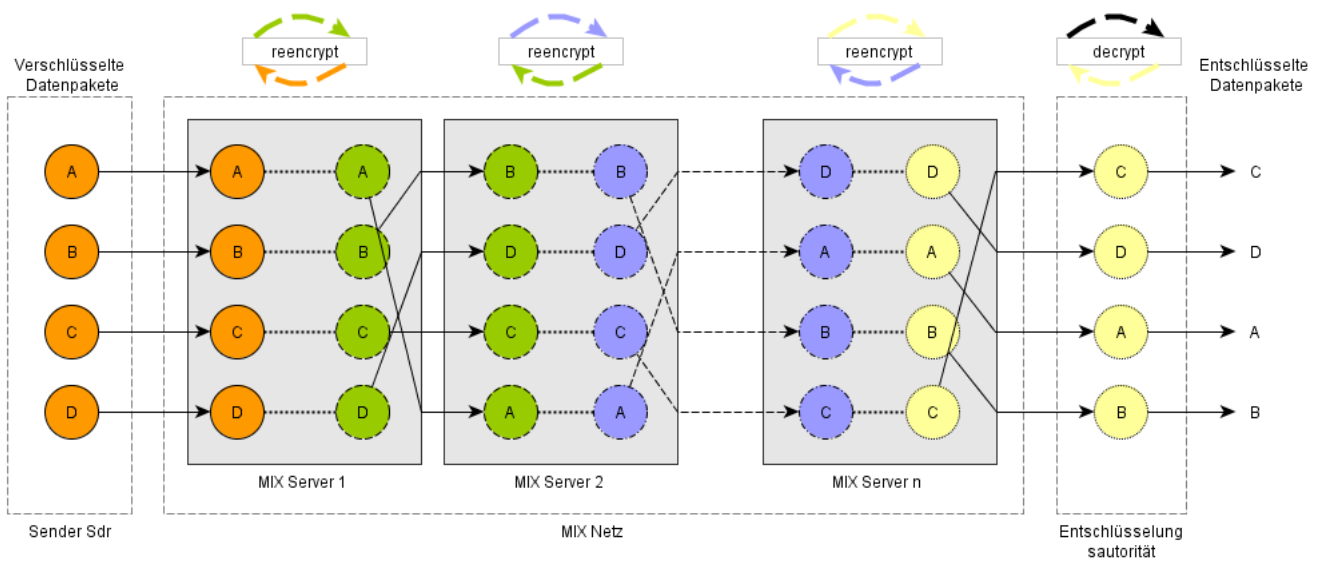


Abbildung 4.5: Nachrichtenübertragung in einem Re-encryption MIX Netz

4.2.2 Wiederverschlüsselung mit El-Gamal

In den folgenden Abschnitten werden, aufbauend auf Kapitel 2, die mathematischen Voraussetzungen für die Wiederverschlüsselungsoperation bei Anwendung des El-Gamal Verschlüsselungsverfahrens beleuchtet.

Während dem Ablauf des Re-encryption MIX Verfahrens wird die Darstellung jeder Wahlstimme von Verschlüsselungen C zu anderen Verschlüsselungen C' umgeformt. Hierbei ist zu beachten, dass ausschließlich die Darstellung und nicht der Inhalt der verschlüsselten Wahlstimme geändert wird so dass die Entschlüsselung der wieder verschlüsselten Wahlstimme wieder die Wahlstimme m ergibt (s. Gleichung 4.1).

4.2.2.1 Definition Wiederverschlüsselung mit El-Gamal

Bei Anwendung des El-Gamal Verschlüsselungsverfahrens wird aus einer verschlüsselten Wahlstimme $C = (c_1, c_2) = ((g^r), m(\alpha^r))$ die wiederverschlüsselte Darstellung $\text{enc}(C) = C' = (c_1 \cdot g^{r'}, c_2 \cdot \alpha^{r'})$ mit einem öffentlichen Schlüssel (p, g, α) hergestellt. Aus beliebigen Verschlüsselungen C' kann mit dem dazu gehörigen geheimen Schlüssel (a) wieder $\text{enc}(C') = m$ hergestellt werden. Die Funktionen enc und dec bezeichnen dabei wieder die Ver- und Entschlüsselungsfunktionen des jeweiligen Schlüsselpaares wobei gilt $r, r' \in \mathbb{Z}_p$

Die *Wiederverschlüsselungsoperation* zu gegebenem öffentlichen Schlüssel (p, g, α) und Verschlüsselung C ist nach [Riv04] wie folgt definiert:

Zur Berechnung der Verschlüsselung einer bereits verschlüsselten Nachricht ist es notwendig einen weiteren Zufallswert r' zu wählen. So kann nach [Riv04] aus einer vorhandenen verschlüsselten Nachricht $C = (c_1, c_2)$ die wiederverschlüsselte Nachricht $C' = (c'_1, c'_2)$ erstellt werden.

1. Wähle $r, r' \in \{1, \dots, p-2\}$ zufällig
2. Berechne $c'_1 = c_1 \cdot g^{r'} \pmod p = g^{r+r'} \pmod p$
3. Berechne $c'_2 = c_2 \cdot \alpha^{r'} \pmod p = m \cdot \alpha^{r+r'} \pmod p$
4. Erhalte wiederverschlüsselten Geheimtext $C' = (c'_1, c'_2)$
5. Nun kann aus dem wiederverschlüsselten Geheimtext $C' = (c'_1, c'_2)$ auf zuvor beschriebener Weise der Klartext errechnet werden:

$$\text{Erhalte Nachricht } \text{dec}(C') = \text{dec}(c'_1, c'_2) \equiv c_1^{x'} \cdot c_2' \equiv m \pmod p, x = p-1-a$$

4.2.2.2 El-Gamal Rechenbeispiel (Fortsetzung von Abschnitt 2.2.4)

Es soll gezeigt werden, dass nicht nur die einfache Verschlüsselung einer Nachricht, sondern auch die mehrfache Verschlüsselung in die ursprüngliche Nachricht transformiert werden kann, wenn man den geheimen Schlüssel auf die mehrfach verschlüsselte Nachricht anwendet. Nach Beispiel 2.2.4 gilt:

- Öffentlicher Schlüssel $(p, g, \alpha) = (13, 7, 12)$
- Geheimer Schlüssel $(a) = 6$
- Nachricht $m = 7$
- Verschlüsselte Nachricht $C = \text{enc}(m) = (5, 6)$

Anhand des gegebenen Schlüssels und eines Zufallswert $r' = 2 \in \{1, \dots, p-2\}$ lässt sich $C' = \text{enc}(C) = (c'_1, c'_2)$ mit

- $c'_1 = 7^{3+2} \pmod{13} = 11$
- $c'_2 = 7 \cdot 12^{3+2} \pmod{13} = 6$

berechnen.

Aus der so erhaltenen Wiederverschlüsselung von C lässt sich die verschlüsselte Nachricht $\text{dec}(C') = 6 \cdot 6^{13-1-6} \pmod{13} = 7 = m$ entschlüsseln (s. Kap. 2).

4.2.3 Anwendung des Re-encryption MIX Verfahrens bei elektronischen Wahlen

Das Re-encryption MIX Verfahren erfordert nur die einfache Verschlüsselung der Wahlstimme womit es dem Wähler, im Gegensatz zum Decryption MIX Verfahren, erspart bleibt n verschiedene öffentliche Schlüssel in einer bestimmten Reihenfolge zur Verschlüsselung seiner Wahlstimme anzuwenden.

Diese wird nun durch einen, durch das El-Gamal Verschlüsselungsverfahren hergestellten, öffentlichen Schlüssel (p, g, α) verschlüsselt und auf dem Bulletin Board veröffentlicht. Analog zum Decryption MIX Verfahren durchläuft das verschlüsselte Datenpaket das MIX Netz, wird aber bei jedem Durchlauf probabilistisch wiederverschlüsselt.

Der letzte MIX Server hat nun nicht mehr die alleinige Autorität das jeweilige Datenpaket zu einer Wahlstimme zu entpacken. Viel mehr wird dieses nun kollektiv durch eine Mindestanzahl von MIX Servern, die den verteilten Schlüssel zusammensetzen, entschlüsselt.

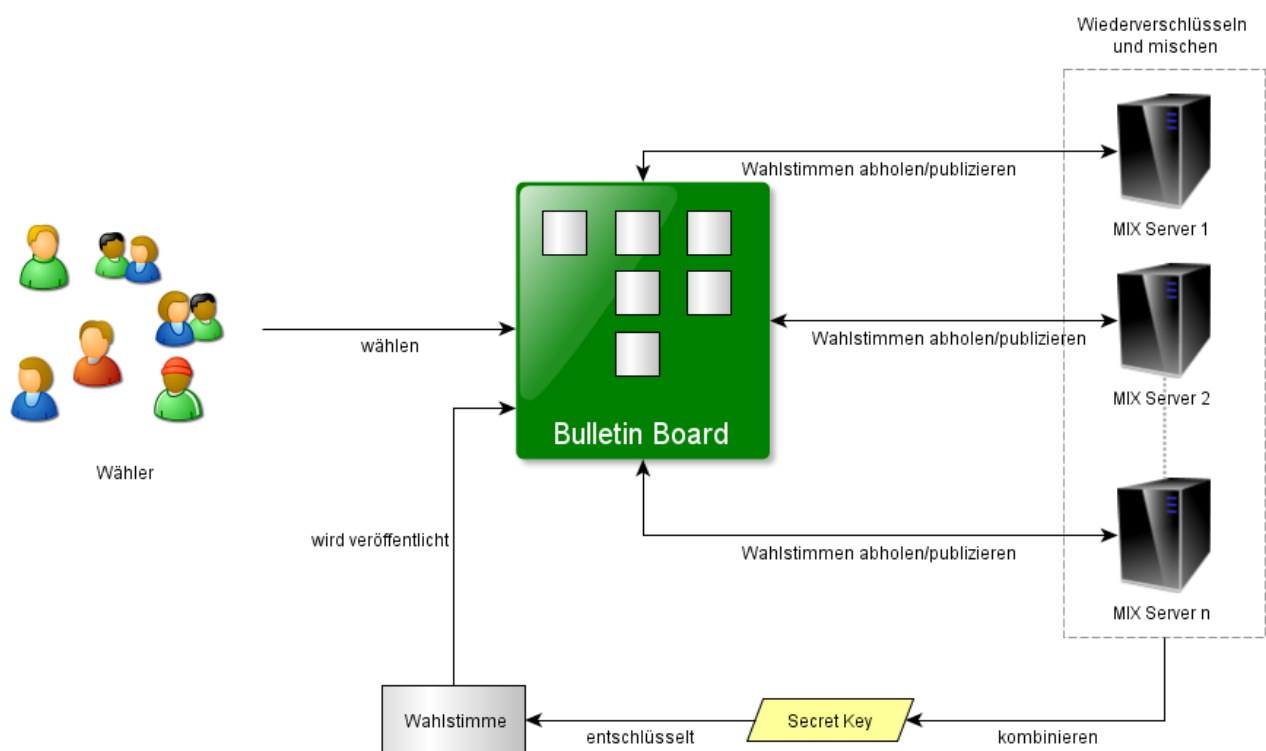


Abbildung 4.6: Anwendung des Re-encryption MIX Verfahrens mit Bulletin Board

4.2.4 Erfüllung der Kriterien

Die *Robustheit* des Wahlverfahrens mit Re-encryption ist durch das Wiederverschlüsseln mit *einem* Schlüsselpaar um ein vielfaches gestiegen, da es nun einem beliebigen MIX Server nicht mehr möglich ist den Wahlvorgang zu blockieren. Falls ein MIX Server, beabsichtigt oder unbeabsichtigt nicht funktioniert, kann dieser emuliert oder aus dem Wahlverfahren ganz ausgeschlossen werden. Das Wahlverfahren würde danach wie vorgesehen weitergeführt werden und es müsste nicht wiederholt werden. Des Weiteren wird anstatt der mehrfachen Verschlüsselung des ganzen Datenpakets eine einzige Wiederverschlüsselung der Wahlstimme mit dem öffentlichen Schlüssel und einem Zufallswert r angewendet. Dies trägt dazu bei, dass unnötige Datenlast durch Nachrichtenexpansion, welche durch die mehrfache Verschlüsselung entsteht, vermieden wird. So werden, im Gegensatz zum *Decryption MIX* Verfahren, weniger Ressourcen und Zeit zur Berechnung der Entschlüsselung gebraucht.

Die *Privatheit* ist, wie beim *Decryption MIX*-Verfahren gewährleistet, da auch beim Re-encryption MIX-Verfahren die Daten in jedem MIX Server derart durchmischt, dass bei Ankunft der Wahlstimme auf dem Bulletin Board keine Rückschlüsse auf den Wähler bzw. Versender gezogen werden können falls mindestens ein MIX Server ehrlich ist. Durch das Verteilen des geheimen Schlüssels (a) mittels *Secret-Sharing Mechanismen* (s. Abschn. 3.4) ist gewährleistet, dass es einem oder weniger als t korrupten MIX Servern unmöglich ist die abgegebene Wahlstimme zu öffnen und zu ändern.

Die *Korrektheit* des Verfahrens kann auch hier, analog zum *Decryption MIX*-Verfahren, auf keine Weise (insbesondere nicht öffentlich) sicher verifiziert werden, da aufgrund des Mischens der Wahlstimmen von außen kein Zusammenhang zwischen eingehenden und ausgehenden Datenpaketen herstellbar ist. Zwar kann, aufgrund der Veröffentlichung der verschlüsselten Wahlstimmen auf dem Bulletin Board, festgestellt werden ob die Anzahl der verarbeiteten Wahlstimmen korrekt ist, jedoch können noch immer Wahlstimmen in einem MIX Server gelöscht und durch Duplikate von anderen Wahlstimmen ersetzt werden. Die Verschleierung der Herkunft einer Wahlstimme ist natürlich aus oben genannten Gründen der Anonymisierung des Wählers erwünscht führt aber gleichzeitig auch zur Verschleierung der Operationen innerhalb der MIX Server. Der Prozess des Entschlüsselns der einzelnen Wahlstimmen ist nun nicht mehr nur auf einen MIX Server zentriert und es ist somit unwahrscheinlich dass eine Stimme nach dem Entschlüsseln noch vor der Ausgabe verändert wird, jedoch wird noch immer keine zusätzliche Information geliefert, die einen Nachweis über die Äquivalenz zwischen eingegangenen Wahlstimmen und ausgegangenen Wahlstimmen eines MIX Servers liefert.

Mit der Anwendung von Verschlüsselungsverfahren mit homomorphen Eigenschaften konnte die *Robustheit* des Wahlverfahrens durch Anwendung von Re-encryption erheblich gesteigert werden. Einzelnen, eventuell korrupten MIX Servern ist es nun nicht mehr möglich den Wahlvorgang durch Blockade vorzeitig abubrechen. Durch die Anwendung von Secret-Sharing Mechanismen wurde zudem die Entschlüsselungskompetenz auf mehrere MIX Server verteilt und so die Wahrscheinlichkeit der Ausgabe eines falschen Wahlergebnisses durch einen einzelnen MIX Server minimiert. Wie beim Decryption MIX Verfahren ist die allgemeine Verifizierbarkeit der Operationen eines MIX Servers noch immer nicht gegeben und wird im folgenden Abschnitt durch eine Verschiebung der Anonymität angenähert.

4.3 Re-encryption MIX mit Randomized Partial Checking

Um verifizieren zu können, dass es einem (oder mehreren) MIX Server² nicht möglich ist Wahlstimmen während des Mischens abzuändern oder sie durch Duplikate zu ersetzen, bedarf es eines Beweises oder zumindest eines starken Nachweises („*strong evidence*“)[JJR02], dass der Ausgang eines MIX Servers äquivalent zu seinem Eingang ist. Dieser Nachweis wird in Form einer teilweisen Aufdeckung der Input/Output Beziehungen eines jeden MIX Servers erbracht und erlaubt so eine (probabilistische) Verifizierung dessen Operationen.

RPC kann mit verschiedenen Verschlüsselungsverfahren, wie z.B. El-Gamal oder RSA, zum allgemeinen Nachweis korrekter Operationen von MIX Servern verwendet werden. Da hier kein komplexer und meist rechenintensiver Beweis³ notwendig ist, ist RPC vergleichsweise effizient. Im Folgenden wird die Verfeinerung des im vorangegangenen Abschnitt beschriebenen Re-encryption MIX-Verfahrens mit El-Gamal Verschlüsselung durch RPC beschrieben. Durch die Hinzunahme dieser Technik soll letztendlich die Nachweisbarkeit der korrekten Arbeitsweise des Wahlverfahrens sichergestellt werden.

4.3.1 Alternative Ansätze

Jakobsson und Juels in [JJ99] wie auch Abe in [Abe99] verwenden effiziente Zero-Knowledge Beweise um Äquivalenzen von verschlüsselten Nachrichten nachzuweisen. Durch die Effizienz der Zero-Knowledge Beweise erhalten sie so zwar allgemeine Verifizierbarkeit, jedoch ist diese Vorgehensweise nur für kleinere Nachrichtenmengen gebräuchlich und wird aufgrund des asymptotischen Verhaltens des Berechnungsaufwandes unpraktikabel für größer angelegte Wahlen.

² hier eingesetzt im Re-encryption MIX Verfahren, Einsatz im Decryption MIX Verfahren möglich

³ z.B. Zero-Knowledge Beweis (s. Abschn. 3.3)

Allgemein verifizierbare Secret-Sharing Verfahren wurden von Neff in [Nef01] und unabhängig davon von Furukawa und Sako in [FS01] angewendet, um eine eventuelle Korrumpierung der Wahlstimmen zu erkennen. Im Gegensatz zur Verwendung von Zero-Knowledge Beweisen, ist dieser Ansatz auch für Wahlen im größeren Umfang geeignet. Nichtsdestotrotz zeichnet sich der hier beschriebene Ansatz mit Randomized Partial Checking durch höhere Effizienz und Vielseitigkeit aus.

4.3.2 Randomized Partial Checking (RPC)

Jakobsson et al. stellen in [JJR02] eine Methode zur Verifikation korrekt durchgeführter Operationen (s. Abb. 4.2) in MIX Servern vor, die gänzlich ohne aufwändige Beweise auskommt.

Durch das Aufdecken zufällig bestimmter Input/Output Beziehungen eines Servers, ist es möglich einen starken Nachweis über die korrekte Arbeitsweise eines MIX Servers zu erbringen. Hierfür werden die MIX Server dahingehend verändert, dass sie nun als gepaarte Einheiten (s. Abb. 4.7) im MIX Netz auftreten. Somit bilden nun jeweils zwei MIX Server aus den herkömmlichen MIX Verfahren einen MIX Server im MIX Verfahren mit RPC. Diese Modifikation ermöglicht es Mechanismen zur Überwachung von Misch-Operationen in MIX Servern einzusetzen, die gleichzeitig die *Privatheit* des Wählers wahren.

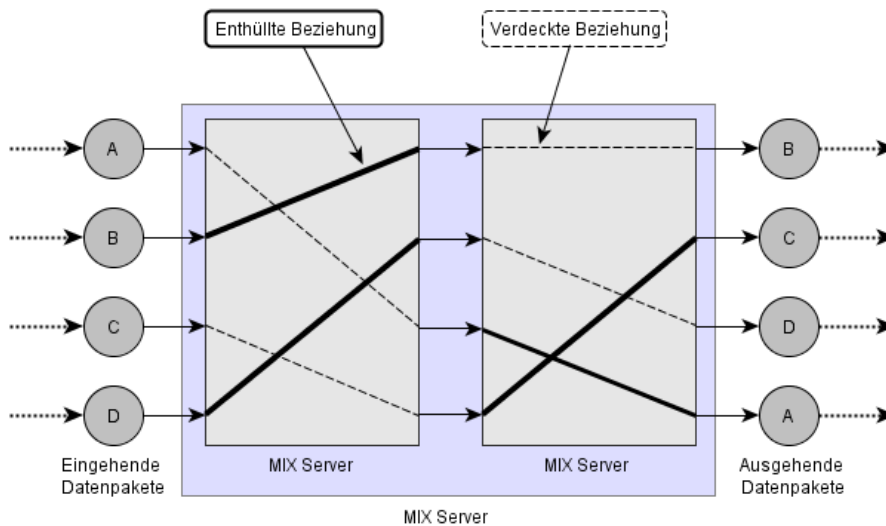


Abbildung 4.7: Mix Server mit enthüllten und verdeckten Beziehungen

Abbildung 4.7 zeigt in schematischer Darstellung die Beziehungen in einem MIX Server welches aus zwei gepaarten MIX Servern besteht. Die fett gezeichneten Verbindungen innerhalb eines Servers stellen die enthüllten Beziehungen zwischen Input und Output eines Servers dar. Korrespondierend dazu sind durch die gestrichelten Linien die noch verhüllten Beziehungen dargestellt. Durch das wechselseitige Aufdecken von Beziehungen wird verhindert, dass der Ursprung von gemischten Daten durch das MIX Netz ermittelt werden kann.

Die zufällige Aufdeckung von Beziehungen innerhalb eines Servers geschieht nach Ablauf der Wahlphase, wenn alle Mischoperationen der MIX Server schon abgeschlossen sind. Welche Beziehung in einem Server aufgedeckt wird und somit im korrespondierenden Nachbarserver verdeckt bleibt, bestimmen entweder die anderen MIX Server gemeinsam oder ein Zufallsorakel, indem ein Seed⁴ $Q = h(r, BB)$ mit einer geeigneten Hashfunktion h mittels eines von den MIX Servern gemeinsam generierten Zufallswerts r und den Inhalten des Bulletin Boards errechnet wird. Jeder Server S_j kann nun einen eigenen von Q abgeleiteten Seed Q_j generieren, um Zufallswerte für das Aufdecken von Beziehungen zu erhalten.

⁴ Wert oder Vektor um einen Pseudozufallsgenerator zu initialisieren

Da in dem hier beschriebenen Wahlverfahren das El-Gamal Verschlüsselungsverfahren eingesetzt wird, können anhand zusätzlich veröffentlichter Informationen zur probabilistischen Verschlüsselung der einzelnen Wahlstimmen Nachberechnungen durchgeführt werden die, die Beziehung von Input zu Output eines MIX Servers zweifelsfrei nachweisen. Diese implizite Eindeutigkeit beruht auf dem diskreten Logarithmenproblem (s. Abschn. 2.2.2) welches mit *unconditional hiding* und *conditional binding* Eigenschaften ausgestattet ist. In [JJR02] wird ein allgemein einsetzbarer Ansatz durch die Veröffentlichung von Commitments zu Permutationsoperationen (Mischen) in jedem MIX Server eingeführt, der innerhalb dieser Arbeit nicht weiter betrachtet wird.

4.3.3 Allgemeiner Ablauf des Re-encryption MIX Verfahrens mit Randomized Partial Checking

Der Ablauf des Re-encryption MIX Verfahrens mit Randomized Partial Checking ist deckungsgleich mit dem Verfahren ohne RPC bis auf den Unterschied, dass bei der Anwendung von RPC jeder Server Tripel der Form (k, i, r_{jki}) enthüllt nachdem der MIX Prozess abgeschlossen ist. Durch die so erhaltenen k und i lassen sich die Permutationen, entstanden aufgrund des Mischens, nachvollziehen. r_{jki} stellt den für die Wiederverschlüsselung verwendeten Zufallswert dar. In Verbindung mit dem öffentlichen Schlüssel und den jeweiligen Outputs lässt sich mit dieser Information der Weg einer Stimme zu Ihrer Darstellung als Input zurückverfolgen.

$$C_{k,j-1} \xleftarrow{(k,i,r_{jki})} C_{i,j} \quad (4.2)$$

Alle Inputs, Outputs und zur Nachbildung von Inputs benötigte Informationen (k, i, r_{jki}) werden zur allgemeinen Verifizierbarkeit veröffentlicht. Zur Vereinfachung der nachfolgenden Veranschaulichungen wird immer eine durchschnittlich 50 %-ige Enthüllung der Beziehungen eines Servers angenommen. So gilt in einem Server Paar immer dass ein Server eine Hälfte seiner Beziehungen offenlegt und der dazu gepaarte MIX Server die wechselseitig andere Hälfte wie in Abbildung 4.7 beschrieben. Des Weiteren wird angenommen, dass eine gerade Anzahl von t MIX Server vorhanden ist, so dass jeder MIX Server Teil eines Paares ist.

Somit ergibt sich folgende Ergänzung zum Re-encryption MIX Verfahren:

1. Ein verteiltes Schlüsselpaar wird nach dem EL-Gamal Verschlüsselungsverfahren generiert. Dabei bezeichnet (p, g, α) den öffentlichen und a den geheimen, verteilten Schlüssel
2. Alle Daten, die in Klartext vorliegen, werden mit Hilfe des öffentlichen Schlüssels (p, g, α) zu Verschlüsselungen $C_{1,0}, \dots, C_{1,n}$ transformiert
3. Jeder MIX Server i generiert aus den eingegangenen Datenpaketen $C_{i-1,0}, \dots, C_{i-1,n}$ wiederverschlüsselte Datenpakete $C_{i,0}, \dots, C_{i,n}$ die nach dem Mischen ausgegeben werden
4. Nachdem alle Stimmen abgegeben worden sind, werden die Input/Output Beziehungen jedes Servers nach den vorher festgelegten Bestimmungen der Aufdeckung (hier $p = \frac{1}{2}$) enthüllt. Diese werden mit den Tripeln (k, i, r_{jki}) zur allgemeinen Verifizierbarkeit veröffentlicht
5. Im letzten Schritt werden die verschlüsselten Datenpakete anhand des verteilten Schlüssels kollektiv durch eine Mindestanzahl an Shareholdern entschlüsselt (s. Abschn 3.4)

Die trotz der Enthüllung von Beziehungen vorhandene Anonymität des Wählers ist an einer simplen Beobachtung zu veranschaulichen: Es wird angenommen, dass ein Angreifer eine beliebige Anzahl $< \frac{t}{2}$ an Server kontrolliert und somit auch Kenntnis über deren Input/Output Beziehungen hat. Weiter wird angenommen, dass mindestens ein Server Paar korrekt arbeitet und somit vertrauenswürdig ist. So kann eine Identifikation der Beziehungen durch den Angreifer mit einer Wahrscheinlichkeit von höchstens $p = \frac{2}{n}$ geschehen, wenn die Anzahl der korrupten Server $< \frac{t}{2}$ ist. n bezeichnet dabei die Anzahl der Stimmen im System.

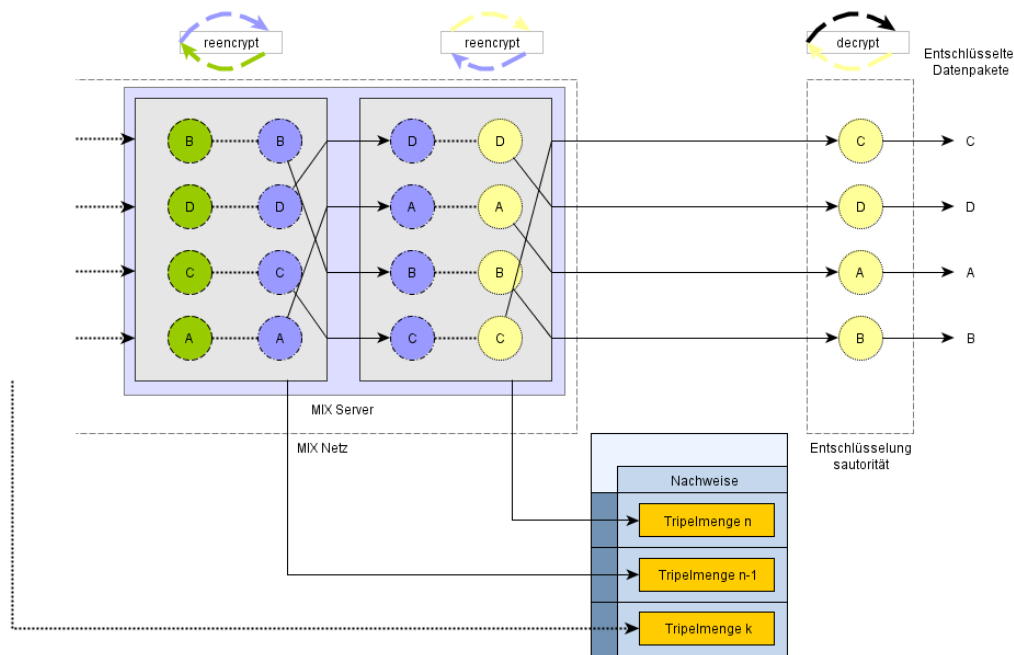


Abbildung 4.8: Re-encryption MIX Netz mit veröffentlichten Tripel (k, i, r_{jki}) von jedem Server S_j

4.3.4 Anwendung des Re-encryption MIX Verfahrens mit RPC bei elektronischen Wahlen

Das Re-encryption MIX Verfahren mit RPC weist im Vergleich zum Re-encryption MIX Verfahren ohne RPC keine Unterschiede bei der Verarbeitung der Wahlstimmen auf. Die Wahlstimmen werden mit einem öffentlichen Schlüssel (p, g, α) verschlüsselt, um nach dem Passieren des MIX Netzes mit dem geheimen und verteilten Schlüssel (a) durch eine Mindestanzahl an t MIX Servern wieder entschlüsselt zu werden. Die Neuerung schlägt sich in der Überprüfung der korrekten Verarbeitung der Wahlstimmen wider wobei beim Re-encryption MIX Verfahren mit RPC nun weitere Informationen zur allgemeinen Verifikation auf dem Bulletin Board veröffentlicht werden. Diese Informationen in der Form von Tripeln (k, i, r_{jki}) ermöglichen es die Äquivalenz von Inputs und Outputs eines MIX Servers durch Nachrechnung nachzuweisen.

Ein schematischer Aufbau der durchzuführenden Schritte ist im Folgenden beschrieben:

1. **Stimmzettelvorbereitung und Verschlüsselung:** Jeder Wähler V_i verschlüsselt seine Stimme M_i initial, so dass er eine verschlüsselte Darstellung $C_{i,0}$ erhält und diese auf dem Bulletin Board veröffentlicht.
2. **Stimmzettelüberprüfung:** Nach dem Ende der Stimmabgabe werden die Stimmen durch alle MIX Server überprüft. Dabei werden alle ungültigen oder doppelten Stimmen (bei Bewahrung der ersten Version der Stimme) durch einvernehmlichen Beschluss der Server verworfen.
3. **Verarbeitung der Stimmen im MIX Netz:** Jeder Server S_j erhält eine Menge von verschlüsselten Stimmen $\{C_{i,j}\}_{j=0}^{t-1}$ als Input. Auf diese Stimmenmenge wird die Verschlüsselungsfunktion d.h. der öffentliche Schlüssel (p, g, α) in Verbindung mit einem Randomwert r_{jki} angewendet. Die so erhaltenen Verschlüsselungen werden in jedem MIX Server gemischt, so dass ein permutierter Output erzeugt wird.
4. **Überprüfung der korrekten Verarbeitung:** Durch Anwendung des Randomized Partial Checking wird die korrekte Arbeitsweise der MIX Server überprüft. Falls Betrugsversuche festgestellt werden, wird der betreffende MIX Server entfernt und für einen erneuten MIX Durchgang emuliert. Dabei wird das Protokoll nicht von Beginn an gestartet, sondern auf der Stufe des korrupten Servers wiederaufgenommen.

5. **Entschlüsselung der Stimmen:** Sobald der korrekte Ablauf der Operationen überprüft ist, werden die Wahlstimmen entschlüsselt. Da ein *Secret-Sharing* Mechanismus zur Aufteilung des geheimen Schlüssels angewendet wird, werden die Stimmen von den Inhabern des geheimen Schlüssels gemeinsam entschlüsselt, so dass die Wahlstimmen nun in Klartext verfügbar sind.

6. **Festlegen eines Grenzwertes:** Die Wahlautoritäten berechnen nun die minimale Anzahl k an verfälschten Wahlstimmen, die notwendig gewesen wären, um das Wahlergebnis signifikant zu ändern. Dann wird die Wahrscheinlichkeit des Eintritts dieses Ereignis berechnet und anhand dieser die Hypothese eines Angriffs angenommen oder verworfen.

7. **Bestätigung des Wahlergebnisses:** Falls die Überprüfung auf korrekte Verarbeitung der Wahlstimmen durch die Server mit positivem Ergebnis abschliesst und die Wahrscheinlichkeit eines Angriffs so gering ist dass dieses Ereignis vernachlässigt werden kann, dann wird ein bestimmter Anteil (hier zur Vereinfachung 50%) der Input/Output Beziehungen (k, i, r_{jki}) eines Servers mit den dazu gehörigen Zufallswerten zur allgemeinen Verifizierbarkeit veröffentlicht.

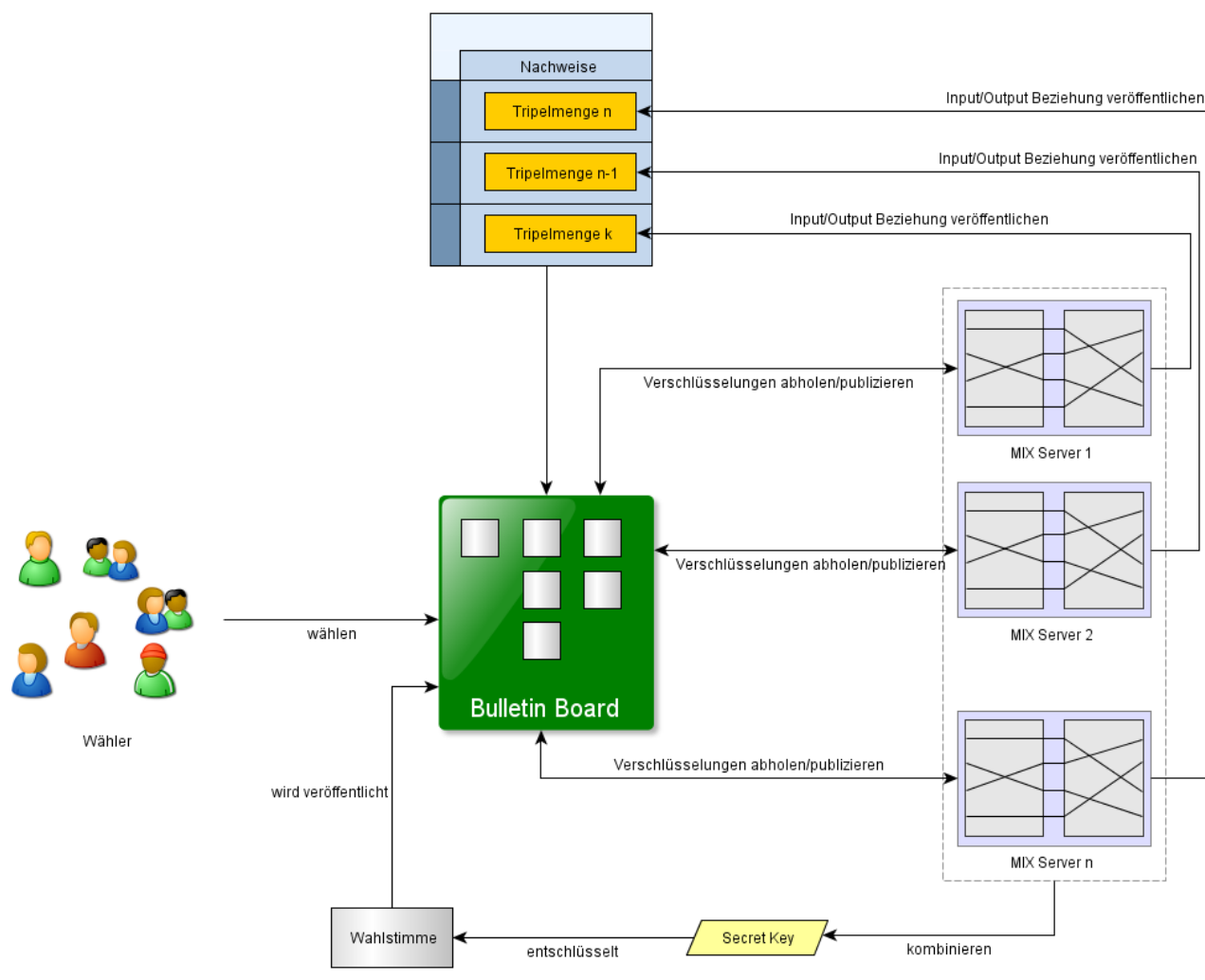


Abbildung 4.9: Anwendung des Re-encryption MIX Verfahrens mit RPC

4.3.5 Erfüllung der Kriterien

Die *Robustheit* des Re-encryption MIX Verfahrens mit Randomized Partial Checking wird, wie schon zuvor, einerseits durch Anwendung von Wiederverschlüsselung der Wahlstimmen und effizienter und sicherer secret-sharing Techniken erreicht. Das Anwenden von El-Gamal Verschlüsselung birgt zudem den Vorteil, dass es bei Entdecken eines korrupten MIX Servers nicht notwendig ist den kompletten MIX Prozess zu wiederholen. Es genügt den korrupten Server zu emulieren und das Verfahren von diesem Punkt aus fortzusetzen. Bedingt durch die Hinzunahme von RPC werden nun zu jeder Menge von gemischten Wahlstimmen auch Informationen zur Enthüllung von Input/Output Beziehungen auf dem Bulletin Board veröffentlicht. Diese Informationen werden zur Verifikation der korrekten Arbeitsweise der MIX Server benötigt. Weder die Veröffentlichung dieser Informationen noch die Verifikation ändern die *Robustheit* des Re-encryption MIX Verfahren mit RPC gegenüber dem klassischen Re-encryption MIX Verfahren .

Die *Privatheit* bei der Verarbeitung der Wahlstimmen ist nach wie vor durch das Re-encryption MIX Verfahren und der Anwendung von Secret-Sharing Techniken gewährleistet (s. Abschn. 4.2.4). Jedoch wurde, durch die Hinzunahme von RPC, nun die *Privatheit* des Wählers zugunsten der Verifizierbarkeit der Operationen jedes MIX Servers geringfügig eingeschränkt. Ohne die Anwendung von RPC beträgt die Wahrscheinlichkeit eine Input/Output Beziehung innerhalb eines Servers festzustellen $p = \frac{1}{n}$ bei n Input/Output Beziehungen. Werden durch Hinzunahme von RPC nun die Hälfte aller Beziehungen aufgedeckt ist eine beliebige, verdeckte Beziehung durch $\frac{n}{2}$ verdeckte Beziehungen verschleiert. So bleibt einem möglichen Angreifer eine Wahrscheinlichkeit von $p' = \frac{\frac{1}{n}}{2} = \frac{2}{n}$ eine verdeckte Beziehung festzustellen. Zudem ist durch die Paarung der Server die *Privatheit* nun nicht schon gegeben wenn nur ein einzelner MIX Server ehrlich ist. Es muss, gemessen am Verhältnis der aufgedeckten Beziehungen, ein bestimmter Teil des MIX Netzes korrekt arbeiten, um vollständige *Privatheit* zu erreichen.

Die *Korrektheit* kann letztendlich durch Hinzunahme von Randomized Partial Checking verifiziert werden. Bedingt durch die zufällige Aufdeckung von Beziehungen, wäre es theoretisch möglich dass aufeinander folgende Beziehungen so aufgedeckt werden, dass im ungünstigsten Fall der ganze Pfad von der Abgabe der Stimme bis zur Entschlüsselung enthüllt wäre. Bei steigender Serveranzahl sinkt die Wahrscheinlichkeit dieses Ereignisses zwar, dennoch wird dem zusätzlich vorgebeugt, indem benachbarte Server jeweils ein Paar bilden und jeder MIX Server Teil eines Paares ist. Mit der Regel dass nur dann eine Input/Output Beziehung einer Wahlstimme innerhalb eines Servers aufgedeckt werden kann wenn diese Beziehung im benachbarten Server verhüllt bleibt, wird der Eintritt des oben beschriebenen Falls vermieden. Somit ist nun nachweisbar gewährleistet, dass ein MIX Server zu verarbeitende Wahlstimmen weder durch Duplikate anderer Wahlstimmen noch durch selbst generierte Wahlstimmen ersetzen kann. Auch wenn dieses Verfahren, bedingt durch die nur partielle Aufdeckung der Beziehungen, „nur“ einen starken Nachweis über die Richtigkeit der Verarbeitung erbringt, sollte dieser Nachweis hinreichend für die Verifikation sein.

Das Re-encryption MIX Verfahren mit RPC vereint die Vorteile des klassischen Re-encryption MIX Verfahren mit der Möglichkeit der öffentlichen Verifizierbarkeit innerhalb des Wahlverfahrens. Es lässt die *Robustheit* und die *Privatheit* des Re-encryption MIX Verfahren nahezu unverändert liefert aber nun einen starken Nachweis über die korrekte Verarbeitung von Wahlstimmen im MIX Netz.

5 Homomorphe Verschlüsselung und MIX Verfahren im Vergleich

In den ersten beiden Kapiteln wurden die beiden vorherrschenden Verfahren, die bei elektronischen Wahlen zum Einsatz kommen, in verschiedenen Variationen beschrieben. Beide Verfahren wurden zunächst in ihrer Grundform vorgestellt um dann sukzessive um optimierende Techniken erweitert zu werden. Schliesslich wurden sie soweit verfeinert, dass sie den anfangs definierten Kriterien *Robustheit*, *Privatheit* und *Korrektheit* genügen.

Nun da beide Verfahren detailliert vorgestellt worden sind, ist es möglich einen Vergleich anzustellen um zeigen zu können wo die Stärken und Schwächen beider Verfahren liegen und um herauszufinden welches Verfahren sich am ehesten für den Einsatz bei elektronischen Wahlen eignet.

5.1 Gemeinsamkeiten und Unterschiede im Vergleich beider Verfahren

Die Gemeinsamkeiten beider Verfahren ist, dass beide Verfahren Zero-Knowledge-Beweise nutzen. Das homomorphe Verschlüsselungsverfahren benötigt diese Beweise um die *Korrektheit* der Stimme des Wählers zu verifizieren, welche mit der Wahlstimme zusammen versendet werden. Hier ist ganz klar zu erkennen, dass zuerst der Beweis geliefert werden muss, damit die Stimme verarbeitet werden kann. Das MIX Verfahren nutzt prinzipiell einen Zero-Knowledge-Beweis, wenn Randomized Partial Checking auf das jeweilige MIX Netz angewendet wird. Zeitlich folgt dieser „Beweis“ nach Verarbeitung der Stimmen zur Verifikation der korrekten Arbeitsweise der MIX Server. Eine weitere Gemeinsamkeit ist die Verwendung von Verifizierbare Secret-Sharing Verfahren zur sicheren Verteilung eines Schlüsselpaares innerhalb der jeweiligen Public-Key Infrastruktur.

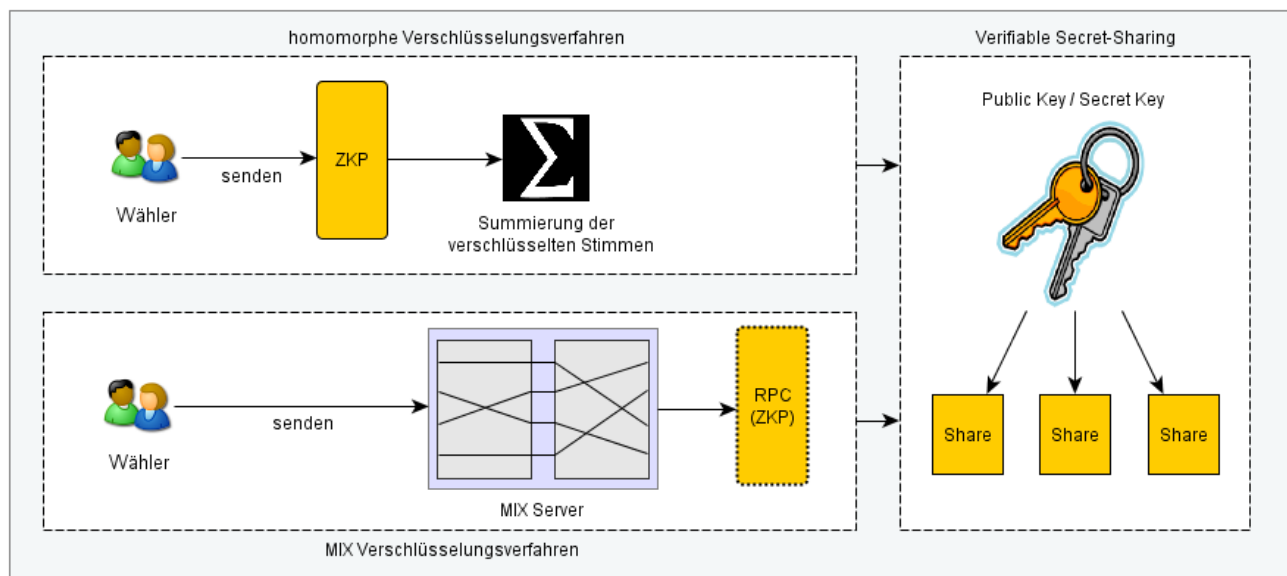


Abbildung 5.1: Secret-Sharing wird von beiden Verfahren verwendet

5.2 Vergleich nach Evaluierungskriterien

Anhand der nachfolgend aufgeführten Kriterien zur Evaluierung des jeweiligen Wahlverfahrens muss herausgestellt werden ob das Wahl verifizierbar und wie effizient dessen Arbeitsweise ist. Dabei werden die Aufwände, die bei der Stimmabgabe entstehen und die Auszählung der Wahlstimmen gesondert, untersucht. Es muss herausgestellt werden welches

Verfahren für welche Art von Wahl gebräuchlich ist und ob es dafür angepasst werden muss. Damit in Verbindung stehend ist auch die Durchführbarkeit und die so entehenden (Personal-) Aufwände und Kosten ein Faktor der zu berücksichtigen bleibt. Schliesslich wird auch analysiert werden welches der beiden Verfahren für den Wähler verständlicher ist und somit der elektronischen Wahl zu mehr Transparenz verhelfen kann.

5.2.1 Verifizierbarkeit

Es wird untersucht inwieweit das Wahlverfahren allgemein verifizierbar ist d.h. welche Mittel jedem Beteiligten einer Wahl zur Verfügung stehen um das Wahlergebnis auf dessen (mathematische) *Korrektheit* zu überprüfen.

Homomorphe Verschlüsselung Die Verifizierung bei homomorpher Verschlüsselung durch den Wähler findet bei der Verteilung des geheimen Schlüssel statt. Der Wähler sendet seine verschlüsselten Stimme und auch ein Zero-Knowledge-Beweis, das seine Stimme korrekt ist. Durch die Ausnutzung der homomorphen Eigenschaft müssen die einzelnen Stimmen nie entschlüsselt werden (s. Abschn. 3) und das Verfahren erlaubt es die einzelnen verschlüsselten Stimmen zu addieren. Es muss also sichergestellt werden, dass die Stimmen korrekt versendet wurden. Da die Stimmen verschlüsselt bleiben, kann die Berechnung öffentlich überprüft werden. Die Anzahl der eingehenden Stimmen wird öffentlich bekannt gegeben und das Ergebnis muss die gleiche Anzahl sein. Zudem können die Wähler beim Secret-Sharing (s. Abschn. 3.4.3) kontrollieren, ob der geheime Schlüssel korrekt generiert und verteilt wird. Somit ist gewährleistet, dass jeder Wähler die Wahl verifizieren kann. Sowohl die Stimmzählung als auch die Verteilung des geheimen Schlüssels können auf Wunsch vom Wähler verifiziert werden.

MIX Verfahren Die Anwendung von Randomized Partial Checking (s. Abschn. 4.3.2) ermöglicht durch das Aufdecken von Input/Output Beziehungen mit einer sehr hohen Wahrscheinlichkeit, dass die MIX Server während der Verarbeitung der Wahlstimmen korrekt gearbeitet haben d.h. dass Wahlstimmen weder durch Duplikate noch durch generierte Stimmen ersetzt worden sind. Da das El-Gamal Verfahren zur Verschlüsselung der Wahlstimmen angewendet wird, werden zur allgemeinen Verifizierbarkeit auch Informationen zur Berechnung der Verschlüsselung auf dem Bulletin Board veröffentlicht. So ist es jedem Wähler möglich die Wiederverschlüsselungen nachzuvollziehen. Zudem wird durch die Anwendung von Secret-Sharing Verfahren sichergestellt, dass der geheime Schlüssel korrekt verteilt und angewendet wird.

Vergleich Beide Verfahren nutzen auf gleiche Art und Weise Secret-Sharing Verfahren um den geheimen Schlüssel zu verteilen. Somit sind sie hier deckungsgleich und eine Gegenüberstellung ist redundant. Die wesentlichen Unterschiede ergeben sich bei der Verarbeitung der Wahlstimmen. Das homomorphe Verschlüsselungsverfahren verifiziert die Wahlstimmen *vor* der Addition um aus diesen dann eine korrekte Summe d.h. Wahlergebnis zu erhalten. Dabei ist zu beachten, dass die Stimmen in korrekter Form auf dem Bulletin Board vorliegen. Für die *Korrektheit* der Stimmen wird zusätzlich ein Zero-Knowledge-Beweis geliefert. Im MIX Verfahren wird die Verarbeitung der Stimmen durch Anwendung von Randomized Partial Checking „überwacht“, so dass es keinem MIX Server möglich mit einer akzeptablen Wahrscheinlichkeit Wahlstimmen zu korrumpieren. Die Unterschied zwischen beiden Verfahren ist, dass bei dem homomorphen Verschlüsselungsverfahren ein Beweis vor der Addition d.h. Verarbeitung der Stimmen geliefert wird, beim MIX Verfahren jedoch während bzw. nach der Verarbeitung der Wahlstimmen. Zudem ist zu erwähnen, dass das MIX Verfahren im Gegensatz zum homomorphen Verschlüsselungsverfahren keinen Beweise, sondern „nur“ einen starken Nachweis über die korrekte Verarbeitung durch die MIX Server liefert. Dieser starke Nachweis ist einem Beweis nahezu gleichwertig (s. Abschn. 4.3.5). Somit erfüllen beide Verfahren dieses Kriterium, da sie öffentliche Verifizierbarkeit anbieten.

5.2.2 Effizienz

Um die Effizienz des jeweiligen Wahlverfahrens erfassen zu können, wird diese mittels den beiden wichtigsten Operationen eines Wahlverfahrens gemessen:

- Stimmabgabe

Die Stimmabgabe kann auf verschiedene Arten erfolgen. Je nach Umsetzbarkeit und Anforderung muss untersucht werden welche Regelungen der Wähler bei der Abgabe seiner Wahlstimme zu beachten hat und ob bestimmte Restriktionen einzuhalten sind. Darüber hinaus wird das Augenmerk auch auf die Darstellung und Verarbeitung der Wahlstimmen gelegt.

- Auszählung

Es wird untersucht welches Wahlverfahren geringere Aufwände beim Auszählen der Stimmen entstehen lässt. So kann auch abgeschätzt werden wie schnell nach der Stimmabgabe mit einem verlässlichen Ergebnis zu rechnen ist und ob unter Umständen Hochrechnungen im Vorfeld sinnvoll sind.

Homomorphe Verschlüsselung Bei der Stimmabgabe werden die Stimmen verschlüsselt und ein Zero-Knowledge Beweis muss mit der verschlüsselten Stimme versendet werden. Der Wähler kann beide gemeinsam senden und nach der Abgabe muss der Wähler keine weiteren Aufgaben erfüllen. Also ist bei der Stimmabgabe Vote-and-Go erfüllt, aber da der Wähler ein Beweis liefern muss, ist dieser Vorgang relativ aufwändig. Bei der Auszählung der Stimmen wird die homomorphe Eigenschaft ausgenutzt und die einzelnen verschlüsselten Stimmen werden summiert. Die Entschlüsselung der einzelnen Stimmen fällt hierbei komplett aus. Nur die Summe der verschlüsselten Stimmen wird Entschlüsselt. Dies führt dazu, dass der Aufwand sehr gering ist und die Ergebnisse kurz nach dem Ende der Wahl bekannt gegeben werden können.

MIX Verfahren Das Re-encryption MIX Verfahren bietet weitestgehende Freiheiten bei der Stimmabgabe für den Wähler. Theoretisch ist es möglich jede Art einer Wahlstimme zu verschlüsseln und abzugeben, da die Darstellung der Wahlstimme im Klartext keinerlei Abhängigkeiten bezüglich des verwendeten Verschlüsselungs bzw. weiteren Wahlverfahrens aufzeigt. Des Weiteren ist es auch nicht erforderlich dass seitens der Wähler weitere Handlungen nötig sind, wie bei interaktiven Wahlverfahren, so dass auch bei diesem Verfahren Vote-and-Go angewendet wird. Der Preis den man für die Freiheiten bei der Art der Wahlstimme zahlen muss, ist die aufwendige Auszählung der abgegebenen Wahlstimmen in der Urne: Jede einzelne Stimme muss entschlüsselt und ausgewertet werden. Dies kann je nach Umfang der jeweiligen Wahl soviel Zeit in Anspruch nehmen, dass Hochrechnungen sinnvoll werden um während der Auswertung Trends veröffentlichen zu können. Diese Vorgehensweise unterscheidet sich dann nicht mehr zu der beim klassischen, nicht elektronischen Wahlverfahren.

Vergleich Das homomorphe Verschlüsselungsverfahren stellt die Vorbedingung, dass ein Zero-Knowledge Beweis mit der abzugebenden Wahlstimme geliefert werden muss. Dies senkt die Effizienz dieses Verfahrens gegenüber dem MIX Verfahren, da hier zu Beginn des Wahlvorgangs keine Beweise erstellt werden müssen. Somit ist die alleinige Stimmabgabe bei m MIX Verfahren allgemein effizienter und für den Wähler bequemer. Die Errechnung des Wahlergebnisses durch Auswertung der abgegebenen Wahlstimmen ist beim homomorphen Verschlüsselungsverfahren durch die mathematisch sehr vorteilhafte Ausnutzung dessen homomorphen Eigenschaften klar effizienter. Die Summierung der verschlüsselten Wahlstimmen und die Entschlüsselung der verschlüsselten Summe verschafft dem homomorphen Verschlüsselungsverfahren einen immensen Vorteil bei der zeitlichen Effizienz und trägt zudem dazu bei dass keine Vielzahl an Entschlüsselungsoperationen zur Erlangung des Wahlergebnisses notwendig ist.

5.2.3 Unterstützte Stimmzettelarten

Die unterstützten und möglichen Stimmzettelarten im jeweiligen Wahlverfahren werden gegenübergestellt und es wird auch untersucht ob eine Gewichtung der Wahlstimmen möglich ist.

Homomorphe Verschlüsselung Die unterschiedlichen Stimmzettelarten werden beim homomorphen Verschlüsselungsverfahren nur zum Teil unterstützt. Da die homomorphie Eigenschaft erfüllt sein muss und die verschlüsselten Stimmen addiert werden, können nur vorher festgelegte Kandidaten auf dem Stimmzettel ausgewählt werden. Falls

neue Kandidaten dazu kommen würden, müsste die Wahl wiederholt werden und alle Stimmen neu verschickt werden. Es kann also keine Wahl mit beliebigen Kandidaten unterstützt werden. Die sogenannte Präferenzwahlen oder Single Transferable Vote (STV) [WZ02] ist bei homomorphen Verschlüsselungsverfahren auch nicht möglich. STV beschreibt ein Personenstimmgebungsverfahren, in der jeder Wähler eine Stimme für den Kandidaten seiner Wahl hat und auch alle Kandidaten nach seiner persönlichen Präferenzliste ordnen kann. Dadurch kann sowohl eine echte Personenwahl als auch Verhältniswahl verwirklicht werden. Ein weiteres Verfahren ist das Instant-Runoff-Voting (IRV), welches auch nicht unterstützt wird. Bei IRV kann der Wähler eine Rangfolge für die Kandidaten auswählen. Es entstehen mehrere Runden, in der die „unbeliebten“ Kandidaten ausfallen, so dass am Ende nur ein Kandidat die Wahl gewinnt. Ein Vorteil von diesem Verfahren ist, dass der Wähler seinen Willen viel genauer ausdrücken kann als bei der bloßen Mehrheitswahl, da die Stimme nie verloren geht.

Die unterschiedliche Gewichtung der Wahlstimmen ist bei homomorpher Verschlüsselungsverfahren ohne großen Aufwand möglich. Dieses System wurde schon an Universitäten bei verschiedenen Szenarien eingesetzt (z.B. Helios V2). Hierbei ist die Gewichtung der Stimmen unterschiedlich und die Stimmen der Professoren wird höher gewichtet, als die der Studenten. Dies kann auch auf beliebige Weise erweitert werden, so dass auch z.B. das Universitätspersonal in der Wahl beteiligt ist und eine andere Gewichtung hat.

MIX Verfahren Theoretisch sind der Form einer Wahlstimme bei der Anwendung des Re-encryption MIX Verfahren mit RPC keine Grenzen gesetzt. Da die Wahlstimme, realisiert durch ein Datenpaket, mit einem öffentlichen Schlüssel unter Anwendung des El-Gamal Verschlüsselungsverfahrens verschlüsselt wird, können beliebig lange Datenpakete mit beliebigen Inhalten verschlüsselt werden. Somit sind hier Wahlformen wie Präferenzwahlen, Rangfolgewahlen oder Wahlen mit beliebigen Kandidaten (Write-In Voting) umsetzbar. Nach den Bestimmungen der jeweiligen Art der Wahl muss hier bei Abgabe der Wahlstimme unbedingt gesichert werden, dass diese regelkonform ist.

Vergleich Das MIX Verfahren ist bezüglich der unterstützten Stimmzettellarten deutlich flexibler gegenüber dem homomorphen Verschlüsselungsverfahren. Da beim MIX Verfahren theoretisch keine Vorbedingungen erfüllt sein müssen, ist es aber unbedingt notwendig, dass die Wahlstimme durch Cut-and-Choose Verfahren o.ä. auf Konformität überprüft wird. Das homomorphe Verschlüsselungsverfahren ist zwar bei weitem nicht so flexibel, jedoch können Wahlen mit gewichteten Wahlstimmen relativ einfach umgesetzt werden. Somit müsste das MIX Verfahren dem homomorphen Verschlüsselungsverfahren hinsichtlich dieses Kriteriums klar vorgezogen werden.

5.2.4 Aufwände/ Kosten

Die Aufwände und Kosten des jeweiligen Wahlverfahrens werden unterteilt in:

- Personeller Aufwand: Es wird untersucht wie hoch der personelle Aufwand und inwieweit das Wahlverfahren automatisiert ablaufen kann.
- Ressourcen (Server etc.): Es wird gegenübergestellt welche technischen Voraussetzungen an Hardware und Peripherie erfüllt sein müssen.

Homomorphe Verschlüsselung Ein Vorteil von homomorphen Verschlüsselungsverfahren ist, dass die einzelnen Stimmen nie Entschlüsselt werden müssen (s. Abschn. 3) und somit deutliche Kosten und Aufwand für die Entschlüsselung gespart werden. Die Addierung der verschlüsselten Stimmen ist ein Rechenprozess für die keine hohen Aufwände benötigt werden und mit relativ wenigen Servern gewährleistet wird. Dadurch wird die Entschlüsselung nur einmal durchgeführt und der Aufwand ist deutlich geringer, als das jede Stimme einzeln entschlüsselt wird. Ein weiterer Punkt ist das versenden vom Zero-Knowledge-Beweises durch den Wähler. Dies ist mit einem relativ hohen Aufwand verbunden, da es für jeden Wähler einzeln gemacht werden muss. Hierbei werden durch die Rechenprozesse hohe Ressourcen in Anspruch genommen. Die Personellen Aufwände treten beim Secret-Sharing ein. Die Verteilung der einzelnen Shares muss auf eine Bestimmte Anzahl an Personen statt finden. Diese Anzahl kann theoretisch sehr hoch sein, aber muss nicht Proportional zu der Menge der Wahlbeteiligung sein. Das heißt, dass eine genügend

große Anzahl an Shareholder ausreicht, um eine Wahl mit sehr hoher Wahlbeteiligung durchzuführen. Bei einer Wahl mit geringer Wahlbeteiligung muss es eine minimale Grenze für die Anzahl der Shareholder geben, damit die Wahl sicher ist.

MIX Verfahren Wie in Kapitel 4 beschrieben bestehen MIX Netze aus einzelnen MIX Servern. Diese MIX Server übernehmen die charakteristischen Mischoperationen zur Verschleierung der Herkunft einer Wahlstimme und entschlüsseln diese auch kollektiv unter Einhaltung von verifizierbaren Secret-Sharing Mechanismen. Es ist naheliegend, dass die Güte der *Privatheit* an der Anzahl der teilnehmenden MIX Server gekoppelt ist. Je mehr nicht korrupte MIX Server im System sind, desto stärker fällt die Wahrscheinlichkeit die Herkunft einer Wahlstimme bestimmen zu können. Für die Kosten bedeutet das, dass mit der Anzahl der MIX Server auch die Kosten für Anmietung bzw. Kauf der Server und dazu gehöriges Personal proportional steigen. So hat die Größenordnung einer Wahl maßgeblichen Einfluss auf die Gesamtkosten einer Wahl oder gar eines Wahldurchgangs. [LS08] schlägt zertifizierte Wahldienstleister vor, die Onlinewahlen für viele verschiedene Institutionen als Dienstleistung durchführen. Somit würden die Kosten für die MIX Server und dazu gehöriges Wartungspersonal einheitlich von einem Wahldienstleister eingefordert werden.

Vergleich Das homomorphe Verschlüsselungsverfahren benötigt für die Durchführung einer Wahl hauptsächlich Personal, welches beim Secret-Sharing eingesetzt wird. Server für die Berechnung des Wahlergebnisses werden nur in geringer Anzahl eingesetzt, so dass deren Kosten überschaubar bleiben. Dem gegenüber gestellt sind MIX Server in einer zur jeweiligen Wahl proportionalen Anzahl. Es ist somit abzusehen, dass das homomorphe Verschlüsselungsverfahren die kostengünstigere Option darstellt.

5.2.5 Praktikabilität

Die Praktikabilität des jeweiligen Wahlverfahrens muss für das jeweilige Verfahren unbedingt gegeben sein, um das Wahlverfahren überhaupt für ein realistisches Szenario in Betracht zu ziehen. Sie lässt sich an der Anzahl und Komplexität der zu erfüllenden Annahmen messen.

Homomorphe Verschlüsselung Die Stärke von homomorpher Verschlüsselungsverfahren ist, dass die einzelnen Stimmen nicht entschlüsselt werden und nur die Summe der verschlüsselten Stimmen einmal entschlüsselt werden müssen. Dies hat den Vorteil, dass bei der Auszählung der Stimmen nur einmal entschlüsselt werden muss und das Ergebnis zeitnah veröffentlicht werden kann. Ein Nachteil ist, dass nicht alle Stimmzettellarten unterstützt werden, und dadurch die Praktikabilität eingeschränkt ist. Ein weiterer Nachteil ist, dass jeder Wähler einen Beweis liefern muss und dadurch relativ hohe Aufwände entstehen. Dies gleicht sich mit dem Vorteil aus, dass die Stimmen nicht einzeln entschlüsselt werden müssen und dadurch das homomorphe Verschlüsselungsverfahren für Wahlen mit hohem Umfang gut geeignet ist.

MIX Verfahren Das MIX Verfahren birgt den großen Vorteil, dass es durch die Unterstützung verschiedenster Stimmzettellarten in hohem Maß flexibel ist (s.o.). Weiterhin wird pro Wahlstimme, aufgrund der Anwendung von Re-encryption mit El-Gamal, keine hohe Rechenleistung von den MIX Servern beansprucht, so dass diese eine zügige Verarbeitung (Mischen) der Wahlstimmen vornehmen können. Nachteile ergeben sich wie oben beschrieben durch die starke Kopplung von den Kosten einer Wahl zu ihrem Umfang. Ein weiterer Nachteil ergibt sich durch die individuelle Entschlüsselung jeder einzelnen Wahlstimme. Je größer der Umfang einer Wahl, desto mehr Wahlstimmen müssen einzeln wieder entschlüsselt und ausgewertet werden. Dies kann die Veröffentlichung des Wahlergebnisses erheblich verzögern.

Vergleich Da die Veröffentlichung des Wahlergebnisses beim MIX Verfahren mit enormen Verzögerungen verbunden sein kann, ist das homomorphe Verschlüsselungsverfahren in diesem Aspekt das überlegene Verfahren. Hierbei müssen nicht alle Stimmen einzeln entschlüsselt und ausgewertet werden, sondern es reicht eine Entschlüsselung der Summe aller verschlüsselten Wahlstimmen. Dabei ist aber zu beachten, dass nur bestimmte Stimmzettellarten umgesetzt

werden können. Das „langsamere“ MIX Verfahren kann hier seinen Vorteil bei der flexiblen Darstellung der Wahlstimmen ausspielen. Der Umfang der Wahl bestimmt beim MIX Verfahren auch direkt proportional die Kosten mit, wobei es bei dem homomorphen Verschlüsselungsverfahren lediglich darauf ankommt dass eine Mindestanzahl an Shareholdern vorhanden ist.

5.2.6 Transparenz/ Verständlichkeit

Die Verständlichkeit des jeweiligen Wahlverfahrens ist ein wichtiger Faktor, der für die allgemeine Akzeptanz bei den Wählern eine sehr große Rolle spielt. Das Wahlverfahren welches transparenter erscheint und somit anschaulicher beschrieben werden kann wird von den Wählern mit hoher Wahrscheinlichkeit besser aufgenommen werden.

Homomorphe Verschlüsselung Für den Wähler ist die Verständlichkeit sehr nahe verbunden mit der Frage: „Wie kann die Sicherheit gewährleistet werden, dass meine Stimme korrekt und sicher übertragen und gewährt wird“. Hierbei ist ein Vorteil von homomorpher Verschlüsselung, dass nie die einzelnen Stimme des Wählers alleine Entschlüsselt werden und somit die Sicherheit gewährleistet wird. Ein Nachteil für die Verständlichkeit des Verfahren könnte die Komplexität der Homomorphie Eigenschaft sein. Durch die Ähnlichkeit des Wahlverfahrens an die klassischen Wahlverfahren ist es dem Wähler leichter verständlich das Wahlverfahren nachzuvollziehen. Die Transparenz ist sehr hoch, da der Wähler die Möglichkeit hat, die Wahl zu verfolgen und auch zu kontrollieren.

MIX Verfahren Im allgemeinen lässt sich das MIX Verfahren sehr anschaulich analog dem klassischen Wahlverfahren mit Papierstimmzetteln beschreiben, da der Prozess des Mischens der abgegebenen Wahlstimmen mit dem Zweck der Anonymisierung direkt vergleichbar ist mit dem Einwerfen der Papierstimmzettel in die Wahlurne. Das initiale Verschlüsseln und finale Entschlüsseln der Stimme kann mit dem Falten („Schließen“) des Papierstimmzettel vor Einwurf in die Wahlurne und dem Öffnen des Papierstimmzettels zur Auswertung übersetzt werden. Solche Analogien erleichtern die Aufnahme dieses Verfahrens bei den Wählern, da so ein Lernvorteil ausgenutzt werden kann.

Vergleich Das Verständnis für ein bestimmtes Wahlverfahren sinkt beim durchschnittlich gebildeten Wähler mit dessen theoretischer Komplexität. Je anschaulicher das jeweilige Verfahren ist bzw. je mehr Analogien ein Verfahren zum herkömmlichen Wahlverfahren mit Papierstimmzetteln aufweist desto höher ist dessen Akzeptanz beim Wähler. Das homomorphe Verschlüsselungsverfahren ist aufgrund der nur theoretisch fassbaren Homomorphie Eigenschaft dem Wähler eher schwieriger nahe zu bringen. Dagegen ist das MIX Verfahren durch seine zahlreichen Ähnlichkeiten zum klassischen Wahlverfahren dem Wähler eher nahe zu bringen.

5.2.7 Allgemeine Auswertung

Aus den vorangegangenen Untersuchungen bezüglich der vorher festgelegten Kriterien Verifizierbarkeit, Effizienz, Unterstützte Stimmzettelarten, Aufwände/Kosten, Praktikabilität und Transparenz/Verständlichkeit ist es möglich eine Auswertung vorzunehmen. Beide Verfahren haben aufgrund ihrer Eigenschaften Vor- und Nachteile, die sich auf das jeweilige Wahlszenario auswirken. Das homomorphe Verschlüsselungsverfahren ist aufgrund seiner Einschränkungen bei den Stimmzettelarten zwar nur unter bestimmten Bedingungen einsetzbar ermöglicht aber eine zügigere Verarbeitung der Wahlstimmen im Vergleich zum MIX Verfahren. Diese und andere Erkenntnisse schlagen sich in folgender, tabellarischer Gegenüberstellung der Auswertungen nieder.

Kriterium	Homomorphe Verschlüsselung	MIX Verfahren
Verifizierbarkeit	✓	✓
Effizienz	✓	✗
Unterstützte Stimmzettelarten	✗	✓
Aufwände/Kosten	✓	✗
Praktikabilität	✓	✗
Transparenz/Verständlichkeit	✓✗	✓✗

Tabelle 5.1: Tabellarische Übersicht der ausgewerteten Kriterien

6 Fazit und Ausblick

6.1 Fazit

Im Rahmen dieser Bachelorarbeit wurden die beiden Wahlverfahren homomorphe Verschlüsselung und MIX Netze vorgestellt, analysiert und gegenübergestellt. Ausgehend von Artikel 38 Absatz 3 des deutschen Grundgesetzes aus Kapitel 1.1 und dem traditionellen Wahlverfahren mit Papier, wurden die Kriterien *Robustheit*, *Privatheit* und *Korrektheit* erarbeitet. Beide Wahlverfahren mussten diese Kriterien erfüllen, um weiterhin in Betracht zu kommen. So wurden beide Verfahren näher betrachtet und so erweitert, dass die genannten Kriterien erfüllt werden konnten und somit der Vergleich möglich gemacht werden konnte.

In Kapitel 2 wurden die Grundlagen für beide Verfahren vorgestellt, da beiden Verfahren bestimmte mathematische und kryptografische Sachverhalte vorausgesetzt sind. Sowohl bei homomorphen Verschlüsselungen, als auch bei MIX Netzen wurde das El-Gamal Verschlüsselungsverfahren angewendet und analysierend betrachtet. Einen Einblick und allgemeine Informationen über das Verfahren wurde gegeben. Die mathematischen Voraussetzungen und Mengen wurden vorgestellt. Zudem wurde das diskrete Logarithmenproblem aufgezeigt. Weiterhin befasste sich ein Teil der Arbeit mit den Berechnungsoperationen für das El-Gamal Verfahren. Schließlich wurde ein Rechenbeispiel gemacht, um die Verständlichkeit der Verfahrens zu vereinfachen.

Kapitel 3 befasste sich mit dem homomorphen Verschlüsselungsverfahren. Hierbei wurde zunächst das Verfahren allgemein erläutert und beschrieben, wie unter Ausnutzung der homomorphen Eigenschaft die verschlüsselten Stimmen aufaddiert werden und dann die Summe der verschlüsselten Stimmen entschlüsselt werden, um ein Ergebnis im Klartext zu erhalten. Zudem wurde die Basisidee erläutert, in der die grundsätzlichen Punkte des Wahlverfahrens mit homomorpher Verschlüsselung bekannt gemacht wurde. Die Anwendung des Verfahrens bei elektronischen Wahlen wurde gezeigt und die einzelnen Schritte, wie die Verschlüsselung der Stimme und Auszählung dieser wurde näher betrachtet. Darauf folgend, wurde geprüft, ob die Kriterien *Robustheit*, *Privatheit* und *Korrektheit* erfüllt werden konnten. Es wurde herausgearbeitet, dass keines der Kriterien bei der Basisidee vollständig erfüllt werden konnten. Somit musste eine Erweiterung gemacht werden. Zunächst musste das Problem gelöst werden, dass die Stimmen korrekt an das Bulletin-Board verschickt werden und somit das homomorphe Verschlüsselungsverfahren korrekt ablaufen kann. Der Abschnitt „Erweiterung um Zero-Knowledge-Beweis“ wurde entworfen um, dieses Problem zu lösen. Die Übermittlung der Wahlstimmen stand nicht im Fokus dieser Bachelorarbeit und wurde daher nicht im Detail behandelt. Es war wichtig zu wissen, dass nach der Erweiterung um den Zero-Knowledge-Beweis die Stimmen der Wähler korrekt auf den Bulletin-Board verschickt werden konnten und dass der Wähler mit seiner verschlüsselten Stimme ebenfalls einen Beweis senden muss, dass die Korrektheit seiner Stimme belegt. Weiterhin wurde keines der Kriterien vollständig erfüllt. Die Probleme stammen hauptsächlich aus der Wahlbehörde. Sowohl bei der Generierung als auch in der Anwendung des Paares Public-Key/Secret-Key traten Probleme auf. Eine Lösung musste gefunden werden, um die Secret-Key zu verteilen und die Autoritäten zu verifizieren. Durch die Erweiterung um Secret-Sharing wurde der Secret-Key unter den Shareholder geteilt. Weiterhin musste eine Erweiterung um Verifiable Secret-Sharing vollzogen werden, da der Dealer und die Shareholder verifiziert werden mussten, um einen möglichen Wahlbetrug auszuschließen. Hierbei hat sich Public Verifiable Secret-Sharing empfohlen, da die Betroffenen bei diesem Verfahren öffentlich verifiziert werden können und dies bei einer Wahl eine enorme Bedeutung hat. Da nun der Dealer den Secret-Key kennt, wurde das Problem nur verschoben und nicht aufgehoben. Daher musste ein Verfahren entwickelt werden, in der der Dealer wegfällt. Im Abschnitt 3.4.3 wurde erläutert, wie das Paar PK/SK ohne den Dealer unter den Shareholdern generiert werden kann. Nun wurden die einzelnen Erweiterungen kombiniert, so dass das Verfahren öffentlich verifizierbar ist und dabei keiner der Autoritäten alleine den Secret-Key besitzt. Somit stellt dies keine potenzielle Gefahr für die Wahl dar. Dadurch wurden die einzelnen Kriterien *Robustheit*, *Privatheit* und *Korrektheit* vollständig erfüllt. Um einen Vergleich der beiden Verfahren homomorphe Verschlüsselung und MIX Netze zu ermöglichen, müsste auch das MIX Verfahren diese Kriterien erfüllen. Dies wurde im nächsten Kapitel angegangen.

In Kapitel 4 wurde zunächst der Ansatz eines Wahlverfahrens unter Anwendung von MIX Netzen vorgestellt. Aufbauend auf das Decryption MIX Verfahren (s. Abschn. 4.1), welches die n -fache Verschlüsselung von Wahlstimmen erfordert. Zwar ist hier die *Privatheit* des Wählers durch das Mischen von Wahlstimmen in jedem MIX Server gegeben, jedoch ergeben sich durch das n -fache Verschlüsseln jeder Wahlstimme redundante Operationen auf Seiten des Wählers. Das hauptsächlich defizitäre Verhalten ergibt sich durch die Nutzung von n verschiedenen öffentlichen Schlüsseln (p, g, α) von n verschiedenen MIX Servern: Wie in 4.3 beschrieben ist dieses Verfahren gegenüber Serverausfällen jeglicher Natur (beabsichtigt oder unbeabsichtigt) sehr fragil, da ein ausgefallener MIX Server die Entschlüsselung der Wahlstimmen verhindert. Abhilfe schafft hier die Anwendung von Re-encryption Verfahren (s. Abschn. 4.2). Anstatt von n verschiedenen Schlüsselpaaren wird nun nur ein Schlüsselpaar zur Ver- und Entschlüsselung verwendet. Dieses Schlüsselpaar wird durch effiziente Secret-Sharing Mechanismen auf eine festgelegte Anzahl von Shareholdern (MIX Servern) verteilt, so dass eine unberechtigte Entschlüsselung der Wahlstimmen nicht möglich ist. Somit wird der Blockade des Wahlverfahrens durch ausgefallene Server vorgebeugt und die *Robustheit* des Verfahrens gefördert. Da beim Re-encryption MIX Verfahren, wie auch beim Decryption MIX Verfahren, die Korrektheit der Mischoperationen innerhalb der einzelnen Server nicht nachweisbar ist wird das Re-encryption MIX Verfahren um eine Vorgehensweise zur Verifikation der Mischoperationen innerhalb der MIX Server erweitert. Bei Anwendung des Randomized Partial Checking wird eine Paarung der MIX Server vorgenommen, so dass nun ein MIX Server aus zwei Servern besteht. Dies ermöglicht eine wechselseitige Aufdeckung der Input-/Output Beziehungen ohne die Anonymität des Ursprungs der Wahlstimme zu gefährden. Die Aufdeckung der Input-/Output Beziehungen in jedem MIX Server liefern einen starken Nachweis über die korrekte Arbeitsweise der MIX Server, da es einem MIX Server nun nahezu unmöglich ist unbemerkt eingegangene Wahlstimmen durch eigene, generierte Wahlstimmen zu ersetzen.

Der Vergleich beider Verfahren wurde in Kapitel 5 behandelt. Beide Verfahren wurden soweit verfeinert, dass die anfangs definierten Kriterien *Robustheit*, *Privatheit* und *Korrektheit* erfüllt werden konnten. Um dies zu gewährleisten, wurden zunächst die Gemeinsamkeiten und Unterschiede beider Verfahren aufgezeigt und festgestellt, dass beide Verfahren Verifiable Secret-Sharing und den Zero-Knowledge-Beweis nutzen. Der Unterschied ist, dass das homomorphe Verfahren diesen Beweis nutzt, um die *Korrektheit* der Stimmen des Wählers zu zeigen. Das MIX Verfahren hingegen nutzt diesen Beweis nach der Verarbeitung der Stimme zur Verifikation der korrekten Arbeitsweise der MIX Server. Um den Vergleich besser durchführen zu können, wurden Evaluierungskriterien erarbeitet und beide Verfahren wurden nach diesen gemessen. Somit wurden die Vor- und Nachteile beider Verfahren deutlich. Durch den Einsatz von Verifiable Secret-Sharing sind beide Verfahren sehr gut verifizierbar und auch gleichwertig gut. Homomorphe Verschlüsselungen haben im Vergleich zu MIX Netzen einen großen Vorteil bezüglich der Effizienz, da die einzelnen Stimmen nicht entschlüsselt werden müssen, sondern nur einmalig die Summe entschlüsselt werden muss. Bei den unterstützten Stimmzetteln konnte das MIX Verfahren deutliche Vorteile aufzeigen, da hierbei theoretisch betrachtet alle Stimmzetteln unterstützt werden können. Bei den Kriterien Aufwände/Kosten und Praktikabilität konnte das homomorphe Verfahren ebenfalls besondere Vorteile nachweisen.

Abschließend lässt sich feststellen, dass beide Verfahren Vor- und Nachteile haben. Dabei ist für die Entscheidung der Angebrachtheit der Wahltyp maßgebend.

6.2 Ausblick

Bei elektronischen Wahlen wurden beide vorherrschenden Verfahren im Rahmen der Bachelorarbeit näher betrachtet. Es konnte aufgezeigt werden, dass beide Verfahren die Anforderungen des Gesetzgebers erfüllen, um eine sichere, anonyme und transparente Wahl durchführen zu können. Aufbauend auf die Erkenntnisse diese Arbeit kann nun gesagt werden, dass beide Verfahren für eine elektronische Wahl gut geeignet sind und daher eingesetzt werden können. Je nach dem welcher Wahltyp vorhanden ist, wird die Auswahl des Verfahrens vorgenommen. Für die Zukunft ist es nicht denkbar, dass elektronische Wahlen nicht eingesetzt werden, da die Verfahren immer besser werden und somit die Anforderungen des Gesetzgeber besser erfüllt werden können. Gegenwärtig sind die elektronischen Wahlen noch nicht verbreitet und es gibt nur wenige Beispiele, in denen diese erfolgreich angewendet werden. Es ist nur eine Frage der Zeit bis die allgemeine

Zustimmung der Bevölkerung an die elektronischen Wahlen eintritt und der Einsatz sich verbreitet. Allerdings müssten noch detaillierte Studien bezüglich der Akzeptanz der elektronischen Wahlen innerhalb der Bevölkerung durchgeführt werden. Zur Zeit besteht noch ein allgemeines Misstrauen an das Thema, da das Thema der elektronische Wahlen relativ neuartig ist. Weiterführende Arbeiten über das Thema wären sinnvoll, in der eine praktische Anwendung implementiert wird und diese universell einsetzbar bei elektronischen Wahlen wäre.

Das Thema elektronische Wahlen hat in der Zukunft ein sehr großes Potential und voraussichtlich werden noch sehr viele Forschungen über das Thema gemacht.

7 Literaturverzeichnis

- [Abe99] ABE, Masayuki: Mix-Networks on Permutation Networks. In: *ASIACRYPT '99: Proceedings of the International Conference on the Theory and Applications of Cryptology and Information Security*. London, UK : Springer-Verlag, 1999. – ISBN 3-540-66666-4, S. 258–273
- [BG02] BONEH, Dan ; GOLLE, Philippe: Almost entirely correct mixing with applications to voting. In: *CCS '02: Proceedings of the 9th ACM conference on Computer and communications security*. New York, NY, USA : ACM, 2002. – ISBN 1-58113-612-9, S. 68–77
- [Buc03] BUCHMAN, Johannes: *Einführung in die Kryptographie*. Springer, 2003
- [BVe] BVERFG: 2 BvC 3/07 vom 3.3.2009, Absatz-Nr. (1 - 163)
- [Cha81] CHAUM, David L.: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. In: *Communications of the ACM* 24 (1981), February, Nr. 2, 84–90. <http://dx.doi.org/10.1145/358549.358563>. – DOI 10.1145/358549.358563. – ISSN 0001-0782
- [DC98] DAVID CHAUM, Torben Pryds P: Wallet Databases with Observers. Version:1998. <http://dsns.csie.nctu.edu.tw/research/crypto/HTML/PDF/C92/89.PDF>. Springer-Verlag, 1998. – Forschungsbericht
- [Des03] In: DESMEDT, Yvo: *ENCYCLOPEDIA OF CRYPTOGRAPHY AND SECURITY*. Springer, 2003, S. 606. – Threshold Cryptography
- [End07] ENDRES, Albert: Elektronische Wahlen bei der GI und anderswo - Ein Grund nach neuen Ideen zu suchen. In: *Informatik-Spektrum* 30 (2007), April, Nr. 2, 91–94. <http://dx.doi.org/10.1007/s00287-007-0137-9>. – DOI 10.1007/s00287-007-0137-9. – ISSN 0170-6012 (Print) 1432-122X (Online)
- [FS01] FURUKAWA, Jun ; SAKO, Kazue: An Efficient Scheme for Proving a Shuffle. In: *CRYPTO '01: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*. London, UK : Springer-Verlag, 2001. – ISBN 3-540-42456-3, S. 368–387
- [HM09] HIRT, Martin ; MAURER, Ueli: Kryptographische Protokolle / RTH Zürich, Department Informatik. 2009. – Vorlesungsskript
- [JJ99] JAKOBSSON, Markus ; JUELS, Ari: Millimix: Mixing in Small Batches. Version:10, 1999. citeseer.ist.psu.edu/jakobsson99millimix.html. 1999 (99-33). – Forschungsbericht
- [JJR02] JAKOBSSON, Markus ; JUELS, Ari ; RIVEST, Ronald L.: Making mix nets robust for electronic voting by randomized partial checking. In: *In USENIX Security Symposium, 2002*, S. 339–353
- [Le09] LE, Van B.: *Diskrete Logarithmen und ElGamal-Verfahren*. Vorlesungsskript, 2009
- [LS08] LANGER, Lucie ; SCHMIDT, Axel: Onlinewahlen mit Wahldiensteanbieter – das Verbundprojekt voteremote. In: *EDEM 2008, OCG, 2008*, S. 281–290
- [Nef01] NEFF, C. A.: A verifiable secret shuffle and its application to e-voting. In: *CCS '01: Proceedings of the 8th ACM conference on Computer and Communications Security*. New York, NY, USA : ACM, 2001. – ISBN 1-58113-385-5, S. 116–125
- [Riv04] RIVEST, Ronald L.: Course 6.897: Advanced Topics in Cryptography, Lecture 18: Mix-net Voting Systems / MIT Computer Science and Artificial Intelligence Laboratory. 2004. – Vorlesungsskript

-
- [Sch99] SCHOENMAKERS, Berry: A Simple Publicly Verifiable Secret Sharing Scheme and its Application to Electronic Voting / Department of Mathematics and Computing Science, Eindhoven University of Technology, Netherlands. 1999. – Forschungsbericht
- [Sha79] SHAMIR, Adi: How to Share a Secret / Massachusetts Institute of Technology. Version: 1979. <http://securespeech.cs.cmu.edu/reports/shamirturing.pdf>. 1979. – Forschungsbericht
- [Smi05] SMITH, Warren: *Cryptography Meets Voting*. 2005
- [WZ02] WILKO ZICHT, Martin F: Single Transferable Vote (STV), Übertragbare Einzelstimmen. Version: Oktober 2002. <http://www.wahlrecht.de/lexikon/stv.html>, http://en.wikipedia.org/wiki/Single_transferable_vote. 2002. – Forschungsbericht