Athena: A verifiable, coercion-resistant voting system with linear complexity

Ben Smyth

July 16, 2019

Abstract

Seminal work by Juels, Catalano & Jakobsson delivered a verifiable, coercion-resistant voting system with quadratic complexity. This manuscript attempts to advance the state-of-the-art by delivering a voting system with equivalent security and linear complexity.

1 Introduction

Voting systems must ensure free-choice [57, 58, 71]. A notion of which is formalised by ballot secrecy (i.e., a voter’s vote is not revealed to anyone) [8, 9, 11, 17, 65]. This notion can be satisfied by voting systems that simply instruct voters to encrypt their vote. But, free-choice may be compromised by an adversary that is able to communicate with voters, since the coins used for encryption serve as proof of how voters voted and voters may communicate those coins to the adversary. Hence, formulations of free-choice must be accompanied by operational assumptions and limitations on the adversary’s capabilities. Indeed, ballot secrecy assumes that voters’ ballots are constructed and tallied in the prescribed manner, and that the adversary’s capabilities are limited to controlling ballot collection.

Receipt-freeness (i.e., a voter cannot collaborate with a conspirator to gain information which can be used to prove how they voted) formalises a notion of free-choice in the presence of an adversary that can communicate with voters [10, 14, 27, 31, 46, 56]. Yet free-choice may be compromised if voters deviate from the prescribed voting procedure. Coercion-resistance (i.e., a voter can deviate from a coercer’s instructions, to cast their own vote, without detection) formalises a stronger notion of free-choice assuming that not only can voters deviate, but the adversary can instruct voters how to deviate [40, 51, 68, 72]. The distinction between receipt-freeness and coercion-resistance is subtle: “receipt-freeness deals with a [conspirator] who is only concerned with deducing information about how someone voted from receipts and public information, but who does not give detailed instructions on how to cast the vote. Coercion resistance, on the other hand, includes dealing with a coercer who gives details not just
on which candidate to vote for but also on how to cast the vote” [37, §1.1]. Both receipt-freeness and coercion-resistance retain the assumption that voters’ ballots are tallied in the prescribed manner, and receipt-freeness additionally assumes voters’ ballots are constructed in the prescribed manner.

Beyond free-choice, voting systems must ensure that only voters vote [57, 58, 71], which can be achieved by issuing credentials to voters and using cryptography to ensure that authorised ballots are unforgeability (i.e., only voters can construct authorised ballots) [66, 69]. (Unforgeability is sometimes known as eligibility verifiability.) Moreover, voting systems must ensure that voters have equal influence in the decision [57, 58, 71], which can be achieved by universal verifiability (i.e., anyone can check whether an outcome corresponds to votes expressed in collected ballots that are authorised, except for votes expressed in ballots from the same voter, which are all discarded, except for the voter’s last vote) and individual verifiability (i.e., a voter can check whether their ballot is collected) [22, 46, 47, 50, 69].

Seminal work by Juels, Catalano & Jakobsson [39–41] made significant progress towards a voting system satisfying the aforementioned properties, moreover, Clarkson, Chong & Myers [20, 21] implemented their results as Civitas, albeit, complexity is $O(|bb|^2)$, i.e., quadratic in the length of the bulletin board ($bb$). Quadratic complexity arises from the use of pairwise plaintext equality tests on the bulletin board’s ballots to discard all but the last vote cast using a private credential. Pairwise plaintext equality tests are also used on mixed ballots and mixed public credentials to discard mixed ballots that are unauthorised, with complexity $O(|L| \cdot |bb|)$, where $L$ is the electoral roll.

**Contribution.** We advance the state-of-the-art with Athena: A verifiable, coercion-resistance voting system with linear complexity $O(|bb|)$. Our system reveals anonymised credentials to discard ballots cast using the same private credential (with linear complexity) and uses plaintext equality tests on each individual mixed ballot – which includes a mixed public credential – to discard any mixed ballot that is unauthorised (with linear complexity). Athena works as follows.

**Voting.** Voters are issued with credential pairs, wherein the private credential is a nonce and the public credential is an encryption of that nonce. Each voter encrypts the negation of their private credential and their vote, and publishes the two resulting ciphertexts prepended with their public credential and appended with a counter (to the bulletin board). A voter computes ballots for any re-votes similarly, using an incremented counter. It follows that the bulletin board will contain voters’ ballots, plus any adversarial ballots.

**Tallying.** Any ballots not containing a public credential are discarded, the sec-

---

1 Auditing can statistically determine whether non-voters are issued with credentials.
2 A plaintext equality test (PET) is a cryptographic primitive for determining whether two ciphertexts encrypt the same plaintext [38].
ond ciphertext of each remaining ballot is homomorphically combined with itself n-times (for some nonce n), and the resulting combination is decrypted to reveal an anonymised credential. Entries that share an anonymised credential are discarded, except for the one with the highest counter, thus, only the last vote associated with each anonymised credential is retained. The first two ciphertexts of each retained ballot are homomorphically combined, deriving either: 1) the combination of a private credential and the negation of that credential, or 2) the combination of a private credential and some other message (excluding the credential’s negation). The resulting homomorphic combinations and corresponding encrypted votes are mixed (using the same permutation), plaintext equality tests are used to determine whether the mixed homomorphic combinations where constructed using private credentials, and the corresponding mixed encrypted votes are decrypted if they were.

Intuitively, Athena achieves coercion-resistance, because a well-formed ballot that encrypts the negation of a voter’s private credential is indistinguishable from an ill-formed ballot that encrypts some other message, hence, a voter cannot prove whether they cast a well-formed ballot (that will be counted, as opposed to an ill-formed ballot that will not), during the voting phase. Moreover, mixing ensures that ballots cannot be mapped to votes during tallying. Thus, coercion-resistance is achieved. (Unlike the voting system by Juels, Catalano & Jakobsson, Athena reveals the number of ballots cast using a voter’s public credential, which requires voters to deny casting ballots when instructed by the coercer to abstain. This is a reasonable strategy, since no voter can prove whether they even cast a well-formed ballot.) Moreover, verifiability is achieved too, because only voters have access to private credentials, hence, only voters can construct authorised ballots (unforgeability), tallying produces evidence (specified in Definition 2) demonstrating that election outcomes correspond to the votes expressed in collected ballots that are authorised (universal verifiability), and ballots are recorded on a bulletin board, hence, voters can check whether their ballot is collected (individual verifiability).

**Structure.** We define Athena in Section 3, analyse coercion-resistance in Section 4, prove verifiability in Section 5, present complexity results in Section 6, and study general design principles in Section 7. The remaining sections present syntax (§2), related work (§8), and a brief conclusion (§9). Sidebar 1 introduces game-based security definitions and recalls notation, and the appendices define cryptographic primitives along with relevant security definitions and present proofs.

## 2 Election scheme syntax

We extend syntax by Smyth, Frink & Clarkson [69] to include re-voting, thereby capturing voting systems that consist of the following four steps. First, a tallier generates a key pair and a registrar generates credentials for voters. Secondly,
Sidebar 1 Preliminaries: Games and notation [65]

A game formulates a series of interactions between a benign challenger, a malicious adversary, and a cryptographic scheme. The adversary wins by completing a task that captures an execution of the scheme in which security is broken, i.e., winning captures what should be unachievable. Tasks can generally be expressed as indistinguishability or reachability requirements. For example, universal verifiability can be expressed as the inability to reach a state that causes a voting system’s checks to succeed for invalid election outcomes, or fail for valid outcomes. Moreover, ballot secrecy can be expressed as the inability to distinguish between an instance of a voting system in which voters cast some votes, from another instance in which the voters cast a permutation of those votes. Formally, games are probabilistic algorithms that output booleans. We introduce some notation before formalising games.

We let \( A(x_1,\ldots,x_n;r) \) denote the output of probabilistic algorithm \( A \) on inputs \( x_1,\ldots,x_n \) and coins \( r \), and we let \( A(x_1,\ldots,x_n) \) denote \( A(x_1,\ldots,x_n;r) \), where coins \( r \) are chosen uniformly at random from the coin space of algorithm \( A \). Moreover, we let \( x \xleftarrow{} T \) denote assignment of \( T \) to \( x \); \( x \xleftarrow{} A(x_1,\ldots,x_n) \) denote assignment of \( A(x_1,\ldots,x_n;r) \) to \( x \), where coins \( r \) are chosen uniformly at random from the coin space of algorithm \( A \); and \( x \xleftarrow{} R S \) denote assignment to \( x \) of an element chosen uniformly at random from set \( S \) (we use the same notation when \( S \) is a distribution). Furthermore, we let \( x[i] \) denote component \( i \) of vector \( x \) and let \( |x| \) denote the length of vector \( x \). Finally, we write \( (x_1,\ldots,x_{|T|}) \xleftarrow{} T \) for \( x \xleftarrow{} T; x_1 \xleftarrow{} x[1];\ldots;x_{|T|} \xleftarrow{} x[|T|] \), when \( T \) is a vector, and \( x,x' \xleftarrow{} R S \) for \( x \xleftarrow{} R S; x' \xleftarrow{} R S \).

Using our notation, we can formulate the following game \( \text{Exp} \) such that \( \text{Exp}(H, S, \mathcal{A}) \) tasks an adversary \( \mathcal{A} \) to distinguish between a function \( H \) and a simulator \( S \): \( m \xleftarrow{} A(); \beta \xleftarrow{} R \{0,1\}; \text{if } \beta = 0 \text{ then } x \xleftarrow{} H(m); \text{else } x \xleftarrow{} S(m); g \xleftarrow{} A(x); \text{return } g = \beta \). Adversaries are stateful, i.e., information persists across invocations of an adversary in a game. In particular, adversaries can access earlier assignments. For instance, the adversary’s second instantiation in game \( \text{Exp} \) has access to any assignments made during its first instantiation.

An adversary wins a game by causing it to output true (\( T \)) and the adversary’s success in a game \( \text{Exp}(\cdot) \), denoted \( \text{Succ}(\text{Exp}(\cdot)) \), is the probability that the adversary wins, that is, \( \text{Succ}(\text{Exp}(\cdot)) = \Pr[\text{Exp}(\cdot) = T] \). We focus on computational security, rather than information-theoretic security, and tolerate breaks by adversaries in non-polynomial time and breaks with negligible success, since such breaks are infeasible in practice. Game \( \text{Exp} \) captures a single interaction between the challenger and the adversary. We can extend games with oracles to capture arbitrarily many interactions. For instance, we can formulate a strengthening of \( \text{Exp} \) as follows: \( \beta \xleftarrow{} R \{0,1\}; g \xleftarrow{} \mathcal{A}^O(x); \text{return } g = \beta \), where \( \mathcal{A}^O \) denotes \( \mathcal{A} \)’s access to oracle \( O \) and \( O(m) \) computes \( \text{if } \beta = 0 \text{ then } x \xleftarrow{} H(m); \text{else } x \xleftarrow{} S(m); \text{return } x \). Oracles may access game parameters such as bit \( \beta \).
each voter constructs and casts a ballot for their vote, and similarly for any re-votes. These ballots are collected and recorded on a bulletin board. Thirdly, the tallier tallies the collected ballots and announces the outcome as a frequency distribution of votes. The chosen representative is derived from this distribution, e.g., as the candidate with the most votes. Finally, voters and other interested parties check that the outcome corresponds to votes expressed in collected ballots.

**Definition 1 (Election scheme).** An election scheme is a tuple of probabilistic polynomial-time algorithms \((\text{Setup, Register, Vote, Tally, Verify})\) such that:\(^3\)

\[
\text{Setup}, \text{ denoted } (pk, sk, mb, mc) \leftarrow \text{Setup}(\kappa), \text{ is run by the tallier. The algorithm takes a security parameter } \kappa \text{ as input and outputs a key pair } pk, sk, \text{ a maximum number of ballots } mb, \text{ and a maximum number of candidates } mc.
\]

\[
\text{Register}, \text{ denoted } (pd, d) \leftarrow \text{Register}(pk, \kappa), \text{ is run by the registrar. The algorithm takes as input a public key } pk \text{ and a security parameter } \kappa, \text{ and it outputs a credential pair } (pd, d), \text{ where } pd \text{ is a public credential and } d \text{ is a private credential.}
\]

\[
\text{Vote}, \text{ denoted } b \leftarrow \text{Vote}(d, pk, v, cnt, nc, \kappa), \text{ is run by voters. The algorithm takes as input a private credential } d, \text{ a public key } pk, \text{ a voter’s vote } v, \text{ a counter } cnt, \text{ some number of candidates } nc, \text{ and a security parameter } \kappa. \text{ Vote } v \text{ should be selected from a sequence } 1, \ldots, nc \text{ of candidates, and counter } cnt \text{ should be incremented between a voter’s runs. (The counter might be a timestamp which increments with time or an integer that is manually incremented, for instance.) The algorithm outputs a ballot } b \text{ or error symbol } \bot.
\]

\[
\text{Tally}, \text{ denoted } (v, pf) \leftarrow \text{Tally}(sk, bb, nc, L, \kappa), \text{ is run by the tallier. The algorithm takes as input a private key } sk, \text{ a bulletin board } bb, \text{ some number of candidates } nc, \text{ an electoral roll } L, \text{ and a security parameter } \kappa, \text{ where } bb \text{ is a set. The algorithm outputs an election outcome } v \text{ and a non-interactive tallying proof } pf, \text{ where } v \text{ is a vector of length } nc \text{ and each index } v \text{ of that vector should indicate the number of votes for candidate } v. \text{ Moreover, the tallying proof should demonstrate that the outcome corresponds to votes expressed in ballots on the bulletin board.}
\]

\[
\text{Verify}, \text{ denoted } s \leftarrow \text{Verify}(pk, bb, nc, L, v, pf, \kappa), \text{ is run to audit an election.}
\]

\[\text{The algorithm takes as input a public key } pk, \text{ a bulletin board } bb, \text{ some}\]

\[^3\text{The syntax bounds the number of ballots } mb, \text{ respectively candidates } mc, \text{ to broaden the correctness definition’s scope (indeed, voting systems that encrypt votes typically require } mc \text{ to be less than or equal to the size of the encryption scheme’s message space and schemes that homomorphically combine votes require } mb \text{ to be less than or equal to the size of that space). The syntax represents votes as integers, rather than alphanumeric strings, for brevity. Finally, the syntax employs sets, rather than multisets or lists, to preclude the construction of schemes vulnerable to attacks that arise due to duplicate ballots \([13, \S 2.1 & \S 4.3]\) (systems vulnerable to such attacks cannot be modelled using the syntax).} \]
number of candidates $nc$, an electoral roll $L$, an election outcome $v$, a tallying proof $pf$, and a security parameter $\kappa$. The algorithm outputs a bit $s$, which is 1 if the outcome should be accepted and 0 otherwise. We require the algorithm to be deterministic.

Election schemes must satisfy correctness: there exists a negligible function $\text{negl}$, such that for all security parameters $\kappa$, integers $nv$ and $nc$, vectors of votes $v_1, \ldots, v_{nv}$ over $\{1, \ldots, nc\}$, and vectors of counters $c_1, \ldots, c_{nv}$ such that $\bigwedge_{1 \leq i \leq nv} |v_i| = |c_i| \land c_i[1] < \cdots < c_i[|c_i|]$, it holds that, given a zero-filled vector $v$ of length $nc$, we have:

$$\Pr[(pk, sk, mb, mc) \leftarrow \text{Setup}(\kappa);$$

$$bb \leftarrow \emptyset;$$

for $1 \leq i \leq nv$ do

$$\begin{cases} (pd_i, d_i) & \leftarrow \text{Register}(pk, \kappa); \\
\text{if } 0 < |v_i| \text{ then} \quad & \\
\text{for } 1 \leq j \leq |v_i| \text{ do} \quad & \\
\quad b_j & \leftarrow \text{Vote}(d_i, pk, v_i[j], c_i[j], nc, \kappa); \quad & \\
\quad bb & \leftarrow bb \cup \{b_1, \ldots, b_{|v_i|}\}; \quad & \\
\quad v[|v_i|] & \leftarrow v[|v_i|] + 1; \quad & \\
\end{cases}$$

$$(v', pf) \leftarrow \text{Tally}(sk, bb, nc, \{pd_1, \ldots, pd_{nv}\}, \kappa):$$

$$|bb| \leq mb \land nc \leq mc \Rightarrow v = v' > 1 - \text{negl}(\kappa).$$

The syntax provides a language to model voting systems and the correctness condition ensures such systems function, i.e., election outcomes correspond to votes expressed in ballots (except for votes expressed in ballots from the same voter, which are all discarded, except for the voter’s last vote), when ballots are constructed and tallied in the prescribed manner. Athena will be defined in terms of this syntax, moreover, we will adopt definitions of verifiability and privacy expressed in the syntax and prove they are satisfied.

3 Our scheme: Athena

Our scheme ($\text{Setup}, \text{Register}, \text{Vote}, \text{Tally}, \text{Verify}$) is used as follows: The tallier initiates an election using algorithm $\text{Setup}$ to compute a key pair, which includes a public key $pk$ for an underlying multiplicatively-homomorphic asymmetric encryption scheme ($\text{Gen}, \text{Enc}, \text{Dec}$), for which there exists a generator $g$ of the scheme’s message space. Next, the registrar uses algorithm $\text{Register}$ to compute a credential pair, wherein the private credential is a nonce $d$ and the public credential is an encryption $\text{Enc}(pk, g^d; r)$ of that nonce, for some coins $r$. The registrar repeats the process to create further credential pairs and these pairs are issued to voters. Each voter uses algorithm $\text{Vote}$ to compute their ballot, which includes: their public credential; an encryption $\text{Enc}(pk, g^{-d}; s)$ of their negated private credential, for some coins $s$; an encryption $\text{Enc}(pk, v; t)$ of their vote $v$, for some coins $t$; and a counter $cnt$. A voter similarly computes ballots.
for re-votes, using an incremented counter. It follows that the bulletin board will contain a ballot for a voter’s first vote

\[ \text{Enc}(pk, g^d; r) \text{ Enc}(pk, g^{-d}; s_1) \text{ Enc}(pk, v_1; t_1) \text{ cnt}_1, \]

ballots for any of the voter’s re-votes

\[ \text{Enc}(pk, g^d; r) \text{ Enc}(pk, g^{-d}; s_2) \text{ Enc}(pk, v_2; t_2) \text{ cnt}_2 \]

\[ \vdots \]

\[ \text{Enc}(pk, g^d; r) \text{ Enc}(pk, g^{-d}; s_k) \text{ Enc}(pk, v_k; t_k) \text{ cnt}_k, \]

such that \( \text{cnt}_1 < \cdots < \text{cnt}_k \), and any other ballots cast using the voter’s public credential, without the private credential (including those cast by the adversary or even the voter themselves), namely,

\[ \text{Enc}(pk, g^d; r) \text{ Enc}(pk, g^{D_1}; s_1) \text{ Enc}(pk, v_1; t_1) \text{ \overline{cnt}}_1 \]

\[ \vdots \]

\[ \text{Enc}(pk, g^d; r) \text{ Enc}(pk, g^{D_l}; s_l) \text{ Enc}(pk, v_l; t_l) \text{ \overline{cnt}}_l. \]

(Ballots also prove correct ciphertext construction, moreover, they prove that the second ciphertext of each ballot encrypts a message of the form \( g^m \). Hence, we restrict ourselves to well-defined ballots above.) Furthermore, the bulletin board will contain ballots cast using other public credentials.

The tallier uses algorithm Tally to compute the election outcome as follows: The tallier generates a nonce \( n \), homomorphically combines the second ciphertext of each entry on the bulletin board with itself \( n \)-times, decrypts the resulting homomorphic combinations to reveal anonymised credentials,\(^4\), and prepends entries with anonymised credentials, thereby producing output including

\[ g^{-d \cdot n} \text{ Enc}(pk, g^d; r) \text{ Enc}(pk, g^{-d}; s_1) \text{ Enc}(pk, v_1; t_1) \text{ cnt}_1 \]

\[ \vdots \]

\[ g^{-d \cdot n} \text{ Enc}(pk, g^d; r) \text{ Enc}(pk, g^{-d}; s_k) \text{ Enc}(pk, v_k; t_k) \text{ cnt}_k \]

\[ g^{D_1 \cdot n} \text{ Enc}(pk, g^{D_1}; r) \text{ Enc}(pk, g^{D_1}; s_1) \text{ Enc}(pk, v_1; t_1) \text{ \overline{cnt}}_1 \]

\[ \vdots \]

\[ g^{D_1 \cdot n} \text{ Enc}(pk, g^{D_1}; r) \text{ Enc}(pk, g^{D_1}; s_l) \text{ Enc}(pk, v_l; t_l) \text{ \overline{cnt}}_l. \]

Entries with the same public credential that are prepended with the same value are discarded, except for the one with the highest counter. Hence, the first \( k-1 \) entries (above) are discarded, whilst the \( k \)th entry is preserved. The remaining

\(^4\)The second ciphertext could simply be decrypted (without harming unforgeability, since knowledge of the exponent must be demonstrated), but this permits some linkability between elections, which is undesirable.
entries are similarly processed, therefore, the last will be kept if any entries sharing the prepended value \((g^{D_i \cdot n})\) have counter values lower than counter \(\bar{c}nI_l\). (For example, suppose only the penultimate entry shares prepended value \(g^{D_i \cdot n}\), i.e., \(D_i = D_{i-1}\), and further suppose \(\bar{c}nI_l > \bar{c}nI_{l-1}\). Hence, the last entry will be preserved and the penultimate entry will be discarded. By comparison, the penultimate entry will be kept if \(\bar{c}nI_l < \bar{c}nI_{l-1}\).) The first two ciphertexts of preserved entries are homomorphically combined and paired with encrypted votes, producing

\[
\text{Enc}(pk, g^d \odot g^{-d}; r \oplus s_k) \quad \text{Enc}(pk, v_k; t_k),
\]

for the \(k\)th entry (above), and

\[
\text{Enc}(pk, g^d \odot g^{D_l}; r \oplus \bar{s}_l) \quad \text{Enc}(pk, \bar{s}_l; \bar{t}_l),
\]

for the last (assuming it is preserved). The homomorphic combinations and encrypted votes are mixed (using the same permutation). The taller performs (optimised) plaintext equality tests on each of the mixed homomorphic combinations to determine whether they contain plaintext one,\(^5\) and decrypts the corresponding mixed encrypted votes when the test holds. Thus, the voter’s vote \(v_k\) (above) is revealed, because mixed ciphertext \(\text{Enc}(pk, g^d \odot g^{-d}; r \oplus s_k \oplus w)\) encrypts 1, whereas vote \(\bar{s}_l\) is not revealed, because mixed ciphertext \(\text{Enc}(pk, g^d \odot g^{D_l}; r \oplus \bar{s}_l \oplus \bar{w})\) does not (recall \(g^{D_l}\) was constructed without private credential \(d\)), where \(w\) and \(\bar{w}\) are coins introduced during mixing. The election outcome is the tally of revealed votes.

Athena is formally specified by Definition 2, using cryptographic primitives introduced in Appendix A. Those primitives include sigma protocols for proving correct key generation, ciphertext construction, and decryption, which behave as one might expect. They also include a sigma protocol for proving iterative homomorphic combination, that is, proving that a ciphertext \(c\) is computed from another ciphertext \(c'\) such that \(c = \bigotimes^n_1 c'\), for some nonce \(n\). We apply the Fiat-Shamir transformation to sigma protocols to derive non-interactive proof systems, which we use to achieve verifiability.

**Definition 2 (Athena).** Suppose \(\Pi = (\text{Gen, Enc, Dec})\) is a multiplicative-homomorphic asymmetric encryption scheme with a message space that is super-polynomial in the security parameter and for which a generator exists; \(M\) is a verifiable pairwise mixnet; \(\Sigma_1, \Sigma_2, \Sigma_3\) and \(\Sigma_4\) are sigma protocols that prove key generation, ciphertext construction, decryption and iterative homomorphic combination, respectively; and \(H\) is a hash function. Let \(\text{FS}(\Sigma_1, H) = (\text{ProveKey, VerKey}), \text{FS}(\Sigma_2, H) = (\text{ProveCiph, VerCiph}), \text{FS}(\Sigma_3, H) = (\text{ProveDec, VerDec}),\) and \(\text{FS}(\Sigma_4, H) = (\text{ProveComb, VerComb})\). Election scheme Athena, denoted \(\text{Athena}(\Pi, M, \Sigma_1, \Sigma_2, \Sigma_3, \Sigma_4, H) = (\text{Setup, Register, Vote, Tally, Verify})\), is defined by the following algorithms.

\(^5\)Mixed homomorphic combinations could simply be decrypted (without harming unforgeability), but this permits some linkability between elections.
• Setup($\kappa$). Compute
  \[(pk, sk, m) \leftarrow \text{Gen}(\kappa);\]
  \[\rho \leftarrow \text{ProveKey}((\kappa, pk, m), (sk, r), \kappa);\]
  \[pk \leftarrow (pk, \rho);\]
  \[sk \leftarrow (pk, sk),\]

  let $mb$ be the largest integer upper-bounded by a polynomial in the security parameter, let $mc$ be the largest integer such that \{0, ..., mc\} $\subseteq$ \{0\} $\cup$ $m$ and $mc$ is upper-bounded by a polynomial in the security parameter, and output $(pk, sk, mb, mc)$.

• Register($\tilde{pk}, k$). Parse $\tilde{pk}$ as $(pk, m, \rho)$, outputting $(\bot, \bot)$ if parsing fails or $\text{VerKey}((pk, m), \rho, \kappa) = \bot$, generate nonce $d$, compute
  \[pd \leftarrow \text{Enc}(pk, g^d);\]
  \[d \leftarrow (pd, d),\]
  and output $(pd, d)$, where $g$ is a generator of message space $m$.

• Vote($\tilde{d}, \tilde{pk}, v, cnt, nc, \kappa$). Parse $\tilde{d}$ as a vector $(pd, d)$ and $\tilde{pk}$ as a vector $(pk, m, \rho)$, outputting $(\bot, \bot)$ if parsing fails or $\text{VerKey}((pk, m), \rho, \kappa) = \bot \lor v \notin \{1, \ldots, nc\} \lor \{1, \ldots, nc\} \not\subseteq m$, compute
  \[c_1 \leftarrow \text{Enc}(pk, g^{-d});\]
  \[c_2 \leftarrow \text{Enc}(pk, v);\]
  \[\sigma_1 \leftarrow \text{ProveCiph}((pk, g, c_1, m), (-d, s), m, \kappa);\]
  \[\sigma_2 \leftarrow \text{ProveCiph}((pk, c_2, \{1, \ldots, nc\}), (v, t), m, \kappa),\]

  and output $(pd, c_1, c_2, \sigma_1, \sigma_2, cnt)$, where message $m = (pd, c_1, c_2, cnt)$ and $g$ is the aforementioned generator of message space $m$.

• Tally($\tilde{sk}, bb, nc, L, \kappa$). Parse $\tilde{sk}$ as vector $(pk, sk)$, initialise $v$ as a zero-filled vector of length $nc$, and proceed as follows.

  1. Remove invalid ballots: Let $\{b_1, \ldots, b_\ell\}$ be the largest subset of senary vectors in $bb$ such that $b_1[1] \leq \cdots \leq b_\ell[1]$ and for each $(pd, c_1, c_2, \sigma_1, \sigma_2, cnt)$ in the subset we have $pd \in L \wedge \text{VerCiph}((pk, g, c_1, m), \sigma_1, m, \kappa) \wedge \text{VerCiph}((pk, c_2, \{1, \ldots, nc\}), \sigma_2, m, \kappa)$, where $g$ is again the aforementioned generator of message space $m$ and message $m = (pd, c_1, c_2, cnt)$. If the subset is empty, then output $(v, \bot)$.

  2. Mix final votes: Initialise $\text{pfr}$ as an empty vector and $A$ as an empty map from pairs (comprising a ciphertext and a group element) to triples (comprising a counter and two ciphertexts), generate nonce $n$, compute

    \[
    \text{for } 1 \leq i \leq \ell \text{ do} \\
    \hspace{1cm} c_i^f \leftarrow \bigotimes b_i[1]; \\
    \hspace{1cm} N \leftarrow \text{Dec}(sk, c_i^f); \\
    \hspace{1cm} t \leftarrow A[(b_i[1], N)];
    \]
if \( t = \text{null} \lor t[1] < b_i[6] \) then
  // Update the map if \( A[(b_i[1], N)] \) is empty
  // or contains a lower counter
  \( A[(b_i[1], N)] \leftarrow (b_i[6], b_i[1] \otimes b_i[2], b_i[3]) \);
else if \( t[1] = b_i[6] \) then
  // Disregard duplicate counters
  \( A[(b_i[1], N)] \leftarrow (b_i[6], \bot, \bot) \);
ς \leftarrow \text{ProveDec}( (pk, c_i', N), sk, \kappa); if \( |pfr| > 0 \) then
  // Prove \( c_{i-1}' \) and \( c_i' \) are derived by iterative
  // homomorphic combination wrt nonce \( n \)
  \( \omega \leftarrow \text{ProveComb}( (pk, (c_{i-1}', c_i'), (b_{i-1}[2], b_i[2])), n, \kappa) \);
  \( pfr \leftarrow pfr \parallel (c_i', N, \varsigma, \omega) \);
else \( pfr \leftarrow pfr \parallel (c_i', N, \varsigma) \),
and apply (pairwise) mixnet \( M \) to the pairs of ciphertexts in map \( A \) to derive vector \( B \).

3. Reveal eligible votes: Initialise \( pfd \) as an empty vector, generate nonces \( n_1, \ldots, n_{|B|} \), and compute

for \( (c_1, c_2) \in B \) do
  \( c' \leftarrow \bigotimes_{i=1}^{n_{\text{pfd}+1}} c_1 \);
  \( m \leftarrow \text{Dec}(sk, c') \);
  \( \omega \leftarrow \text{ProveComb}( (pk, (c_1', c_2'), (b_{i-1}[2], b_i[2])), n, \kappa) \);
  \( \varsigma_1 \leftarrow \text{ProveDec}( (pk, c_1', m), sk, \kappa) \);
  if \( m = 1 \) then
    // \( c_1 \) encrypts \( g^0 \), hence, is derived from homo
    // comb of pub cred and enc of neg priv cred
    \( v \leftarrow \text{Dec}(sk, c_2) \);
    \( v[v'] \leftarrow v[v'] + 1 \);
    \( \varsigma_2 \leftarrow \text{ProveDec}( (pk, c_2, v), sk, \kappa) \);
    \( pfd \leftarrow pfd \parallel (c', v, \omega, \varsigma_1, \varsigma_2) \);
  else \( pfd \leftarrow pfd \parallel (c', m, \omega, \varsigma_1) \),
and output \((v, (pfr, B, pfd))\), where \( g \) is the aforementioned generator of message space \( m \).

• Verify\( \langle \hat{pk}, \hat{bb}, nc, L, v, pf, \kappa \rangle \). Parse \( \hat{pk} \) as vector \((pk, m, \rho)\) and \( v \) as a vector of length \( nc \), outputting 0 if parsing fails, \( \text{VerKey}( (\kappa, pk, m), \rho, \kappa) = \bot \), or \( nc \not\leq mc \), where \( mc \) is computed as per algorithm \text{Setup}. Perform the following checks.
Lemma 1. Athena\((\Pi, M, \Sigma_1, \Sigma_2, \Sigma_3, \Sigma_4, H)\) is an election scheme when cryptographic primitives satisfy the preconditions of Definition 2 and asymmetric encryption scheme \(\Pi\) is perfectly correct.

A proof of Lemma 1 appears in Appendix B. Beyond correctness, verifiable election schemes should satisfy completeness, i.e., auditing should succeed for evidence produced by tallying, hence, algorithm \(\text{Verify}\) should accept outputs of algorithm \(\text{Tally}\). We prove Athena satisfies completeness in Section 5.1.

Athena should be instantiated with an asymmetric encryption scheme satisfying IND-CPA and sigma protocols satisfying special soundness and special honest verifier zero-knowledge. This ensures the non-interactive proof systems derived by application of the Fiat-Shamir transformation satisfy zero-knowledge and simulation sound extractability [12], which help achieve both privacy and verifiability. Moreover, this ensures that ballots are non-malleable [12], which is necessary for privacy [65]. Furthermore, for linear complexity, we require computation \(\bigotimes_{i}^{c} a\) to be linear in the length of \(c\), which is possible for El Gamal, for instance. (Indeed, we have \(\bigotimes_{i}^{n}(g^r, (g^r)^r \cdot M) \equiv (g^r, (g^r)^r \cdot M)^n \equiv (g^{r \cdot n}, (g^r)^{r \cdot n} \cdot M^n)\).)
Implementation. Athena is formally stated independently of the underlying cryptographic primitives (for generality, algorithm agility, and ease of proofs). In practice, Athena(\(\Pi, M, \Sigma_1, \Sigma_2, \Sigma_3, \Sigma_4, \mathcal{H}\)) can be instantiated with established cryptographic primitives. For instance, we might instantiate asymmetric encryption scheme \(\Pi\) as El Gamal [28] and we might instantiate sigma protocols as follows: \(\Sigma_1\) as the protocol for proving knowledge of discrete logarithms by Chaum et al. [15, Protocol 2], \(\Sigma_2\) as the protocol for proving knowledge of disjunctive equality between discrete logarithms by Cramer et al. [26, Figure 1], \(\Sigma_3\) as the protocol for proving knowledge of equality between discrete logarithms by Chaum & Pedersen [16, §3.2], and \(\Sigma_4\) as a slight variant of the protocol by Chaum & Pedersen.\(^6\)

4 Privacy results

An Athena ballot contains a public credential, i.e., an encryption of the corresponding private credential, and an encryption of the negated private credential. Yet, no voter can prove that any ballot contains their private credential. Indeed, a well-formed Athena ballot that encrypts the negation of a voter’s private credential is indistinguishable from an ill-formed ballot that encrypts some other value, rather than such a negation. Hence, during the voting phase, a voter cannot prove whether they cast a well-formed ballot (that will be counted, as opposed to an ill-formed ballot that will not), let alone prove how they voted, thereby assuring coercion-resistance during the voting phase.

Associating each public credential with anonymised credentials (to discard early votes prior to mixing) reveals the number of ballots whose second ciphertext contains the same plaintext (be that a private credential or some other value). For instance, a voter that casts a specific number of ballots containing such a plaintext can check to see whether an anonymised credential appears the specified number of times (in association with the voter’s public credential). But, no voter can prove that those ballots are well-formed. Indeed, the voter may cast the expected number of ballots using a nonce in place of their private credential’s negation, which will result in the expected relation, yet the ballots are ill-formed and will not be counted. Hence, coercion-resistance is preserved before mixing.

Finally, homomorphically combining ciphertexts, mixing those combinations and encrypted votes, and using plaintext equality tests to determine voters’ votes (as opposed to adversarial votes) preserves coercion-resistance, as does decrypting mixed (voters’) votes. (Ballots prove that votes are selected from the sequence of candidates, which provides protection against randomisation attacks [41, §1.1].) It follows that tallying preserves coercion-resistance. Thus, Athena is a coercion-resistant voting system.

\(^6\)To prove iterative homomorphic combination using equality between discrete logarithms, witness that 
\[\prod_{1 \leq i \leq n} (\alpha_i, \beta_i) = (\alpha'_1, \beta'_1) \iff \prod_{1 \leq i \leq n} \log_{\alpha_i} \alpha_i \equiv \log_{\beta_i} \beta_i \land \prod_{1 \leq i \leq n} \log_{\alpha_i} \alpha_i \equiv \log_{\alpha_i} \alpha_i, \text{ where } (\alpha_1, \beta_1), (\alpha'_1, \beta'_1), \ldots, (\alpha_n, \beta_n), (\alpha'_n, \beta'_n) \text{ are El Gamal ciphertexts.} \]
The desire to formally prove that Athena satisfies coercion resistance initiated a study of definitions by Juels, Catalano & Jakobsson [39–41], Gardner, Garera & Rubin [32], Unruh & Müller-Quade [72], and Küsters, Truderung & Vogt [48, 51]. The study reveals that definitions by Gardner, Garera & Rubin and Unruh & Müller-Quade are satisfiable by voting systems that are not coercion resistant, and that the definition by Küsters, Truderung & Vogt is unsatisfiable by systems that are [68]. Hence, those definitions do not adequately formalise coercion resistance and are unsuitable for the analysis of Athena. It remains to study the definition by Juels, Catalano & Jakobsson, and a formal proof that Athena satisfies coercion resistance is deferred until the suitability of their definition (or another) is established.

**Distributed tallying.** Coercion-resistance does not provide assurances when deviations from the prescribed tallying procedure are possible. Indeed, such deviations include revealing the tallier’s private key, which undermines privacy. Hence, the tallier must be trusted. Alternatively, we can design voting systems that distribute the tallier’s role amongst several talliers and ensure free-choice assuming at least one tallier behaves. Extending Athena in this direction is straightforward, since distributed variants of the underlying primitives are well-known. Ultimately, we would prefer not to trust talliers; unfortunately, this is only known to be possible for decentralised voting systems, e.g., [33, 36, 43–45, 61], which do not scale.

## 5 Verifiability results

Athena records ballots on a (public) bulletin board, hence, voters can check whether their ballot is collected (individual verifiability). Moreover, tallying produces evidence demonstrating that the announced election outcome corresponds to the votes expressed in collected ballots that are authorised (universal verifiability). Furthermore, only voters can construct authorised ballots (unforgeability). It follows that Athena is a verifiable election scheme, as we shall prove using formal definitions from Smyth, Frink & Clarkson [69] that we extend to include re-voting (Appendix C).

**Comparison with other verifiability definitions.** Other definitions of verifiability exist. In particular, definitions have been proposed by Juels, Catalano & Jakobsson [41], Cortier *et al.* [23] and Kiayias, Zacharias & Zhang [46]. Smyth, Frink & Clarkson [69, §7] show that definitions by Juels, Catalano & Jakobsson and Cortier *et al.* do not detect attacks that arise when tallying and verification procedures are corrupt nor when verification procedures reject legitimate outcomes. Moreover, they show that the definition by Kiayias, Zacharias & Zhang does not detect the latter class of attacks. By comparison, the definition of verifiability by Smyth, Frink & Clarkson detect these attacks, thereby motivating its adoption.
Küsters et al. [49,50,52] propose an alternative, holistic notion of verifiability called *global verifiability*, which must be instantiated with a goal. Smyth, Frink & Clarkson [69, §8] show that goals proposed by Küsters et al. [53, §5.2] and by Cortier et al. [24, §10.2] are too strong (in the sense that they cannot be satisfied by some verifiable voting systems, including Helios). Moreover, Smyth, Frink & Clarkson propose a slight weakening of the goal by Küsters et al. and proved that their notion of verifiability is strictly stronger than global verifiability with that goal (the “gap” is due to an uninteresting technical detail), which further motivates adoption of the verifiability definition by Smyth, Frink & Clarkson.\(^7\)

## 5.1 Universal verifiability

Universal verifiability asserts that anyone must be able to check whether an election outcome corresponds to votes expressed in collected ballots that are authorised. Since checks can be performed by algorithm `Verify`, it suffices that the algorithm accept if and only if the outcome corresponds to votes expressed in collected ballots that are authorised. The *only if* requirement is formalised by *Soundness* (Definition 11), which requires algorithm `Verify` to only accept correct outcomes, and the *if* requirement is captured by *Completeness* (Definition 12), which requires election outcomes produced by algorithm `Tally` to be accepted by algorithm `Verify`.

**Proposition 2 (Soundness).** *Election scheme Athena*(\(\Pi, M, \Sigma_1, \Sigma_2, \Sigma_3, \Sigma_4, H\)) satisfies Soundness, when symmetric encryption scheme \(\Pi\) is perfectly correct, mixnet \(M\) is verifiable, sigma protocols \(\Sigma_1, \Sigma_2, \Sigma_3\) and \(\Sigma_4\) satisfy special soundness and special honest verifier zero-knowledge, and \(H\) is a random oracle, assuming Injectivity is satisfied.

We defer consideration of Injectivity (Definition 10) to Section 5.3.

**Proof sketch of Proposition 2.** We must establish that outcomes accepted by algorithm `Verify` correspond to votes expressed in collected ballots that are authorised. Step 1 of the algorithm ensures accepted outcomes are only influenced by bulletin board entries constructed by algorithm `Vote`, i.e., only (valid) ballots have influence (invalid ballots do not), and only when they contain a public credential. Step 2 ensures no influence from any mixed ballots that share a public credential (and an anonymised credential) with another mixed ballot, whilst being associated with a (strictly) lower counter value. Moreover, pairs of mixed ballots that share a public credential (and an anonymised credential) and a counter are ensured to have no influence either. It follows that only mixed ballots expressing the last vote associated with a public and an anonymised credential may have influence. Finally, Step 3 restricts influence to mixed ballots associated with a

---

\(^7\)Cortier et al. [24, §8.5 & §10.1] claim that definitions by Smyth, Frink & Clarkson are flawed. Those claims were discussed with Cortier et al. (email communication, April’16) and are believed to be false [69, §9]. Moreover, Smyth, Frink & Clarkson prove that any flaw in their definitions implies flaws in the context of global verifiability, which should increase confidence in their definitions.
voter’s public and private credential, i.e., only voters’ last votes have influence, hence, accepted outcomes correspond to votes expressed in authorised collected ballots.

A detailed proof of Proposition 2 and all other verifiability proofs appear in Appendix D.

**Proposition 3** (Completeness). *Election scheme Athena*(Π, M, Σ1, Σ2, Σ3, Σ4, H) satisfies Completeness when mixnet M is verifiable, sigma protocol Σ2 satisfies special soundness and special honest verifier zero-knowledge, and H is a random oracle.

**Proof sketch.** We must establish that outcomes produced by algorithm Tally are accepted by algorithm Verify. It is trivial to see that an outcome output by the first step of algorithm Tally will be accepted by the first step of algorithm Verify, and it remains to consider outcomes output by the last step of algorithm Tally. Simulation sound extractability (of sigma protocol Σ2) assures us that such outcomes are derived from ballots containing well-formed ciphertexts. It is straightforward to see that computations performed by the second step of algorithm Tally can be successfully checked in the second step of algorithm Verify, in particular, proofs can be verified, because proof systems are complete. Moreover, since map A is equivalently computed (from well-formed ciphertexts) by both algorithms and since the mixnet is verifiable, it follows that checks performed on the mixnet’s output succeed. Finally, the checks performed by the third step of algorithm Verify succeed, because proof systems are complete, thus, outcomes produced by algorithm Tally are accepted.

**5.2 Unforgeability**

Unforgeability asserts that only voters can construct authorised ballots. Since ballots are authenticated by private credentials, it suffices to ensure that knowledge of a private credential is necessary to construct an authentic ballot, which is formalised by Unforgeability (Definition 13). We defer a formal proof to later work.

**Comparison with the voting system by Juels, Catalano & Jakobsson.** Smyth, Frink & Clarkson [69, §6] show that the voting system by Juels, Catalano & Jakobsson only achieves unforgeability assuming the tallier is honest, because the tallier’s private key can be used to discover private credentials (by decrypting public credentials), which enables adversarial construction of authorised ballots. By comparison, Athena achieves unforgeability even if the tallier is dishonest, since the tallier’s private key can only be used to recover $g^d$ or $g^{-d}$, neither of which can be used to construct an authorised ballot, because ballots must prove knowledge of private credential $d$. Thus, Athena improves upon the security of the voting system by Juels, Catalano & Jakobsson. (Their voting system can probably be improved using a similar idea.)
5.3 Individual verifiability

Individual verifiability asserts that voters must be able to check whether their ballot is amongst those collected. Since ballots should be collected and recorded on a bulletin board, and since the board must be available to everyone, it suffices for voters to check that their ballot (i.e., the ballot they constructed) is on the bulletin board. Hence, it is necessary for voters to check that their ballot has not been omitted from the bulletin board. Yet, this is insufficient, because the presence of a ballot identical to a voter’s ballot, does not imply the presence of the ballot constructed by the voter. Indeed, such a ballot might have been constructed by another voter. Thus, individual verifiability requires that voters must be able to uniquely identify their ballot, i.e., ballots do not collide, which is formalised by Individual-Verifiability (Definition 14).

To ensure Athena satisfies individual verifiability, it suffices to require that the underlying encryption scheme produces distinct ciphertexts with overwhelming probability. Smyth explains that “security properties of asymmetric encryption schemes ensure [distinct] ciphertexts...But, such security properties assume public keys are generated (by key generation algorithms) using coins chosen uniformly at random. By comparison, individual verifiability and injectivity assume public keys are constructed by the adversary. Thus, security properties are insufficient to ensure...individual verifiability and injectivity” [67]. Nonetheless, given that Athena checks correct key generation, it suffices that ciphertexts are distinct for correctly generated keys.

**Proposition 4** (Individual-Verifiability). Election scheme Athena(Π, M, Σ₁, Σ₂, Σ₃, Σ₄, H) satisfies Individual-Verifiability if for all probabilistic polynomial-time adversaries A and security parameters κ we have \( \Pr[(pk, m, ρ, m', ρ) \leftarrow A(κ); c \leftarrow Enc(pk, m); c' \leftarrow Enc(pk, m') : VerKey((κ, pk, m, ρ, κ) = 1 \land m, m' \in m \Rightarrow c \neq c'] > 1 - \text{negl}(κ) \), where II = (Gen, Enc, Dec) and FS(Σ, H) = (ProveKey, VerKey). Moreover, Injectivity is satisfied if the probability is 1 when plaintexts m and m' are distinct.

The preconditions used by Proposition 4 are due to Smyth [67, §3], and our proof is structurally similar to his proof of individual verifiability and injectivity for a class of encryption-based voting systems.

6 Complexity analysis

Analysing the complexity of algorithms Setup, Register, and Vote is straightforward (given the simplicity of those algorithm): Setup generates a key pair and proof of correct generation, Register computes a ciphertext, and Vote computes two ciphertexts along with proofs of correct construction. Hence, complexity of the registration phase is linear in the number of voters and complexity of the voting phase is linear in the number of ballots cast. Algorithms Tally and Verify are more elaborate and analysis is more involved. We proceed by a detailed inspection of each algorithm and find that complexity remains linear.
Tally. We consider each step of algorithm Tally: It is trivial to see that complexity is upper-bound by the bulletin board’s length in Step 1. For Step 2, we have assumed computation $\bigotimes^n c$ is linear in the length of $c$ ($\S3$), hence, it is straightforward to see that complexity is upper-bound by the number of for-loops iterations, which is constrained by the number of valid ballots on the bulletin board, therefore, complexity is again upper-bound by the bulletin board’s length, because the number of valid ballots is at most the number of ballots on the bulletin board. Complexity of Step 3 is similarly upper-bound by the number of for-loop iterations, which is constrained by the number of pairs output by the mix and at most the number of ballots on the bulletin board, therefore, complexity is upper-bound by the bulletin board’s length.

Verify. We consider the steps of algorithm Verify: Complexity of Step 1 is trivially linear in the bulletin board’s length; Step 2 is straightforwardly linear in the number of for-loop iterations, which is linear in the bulletin board’s length; and Step 3 is straightforwardly linear in the number pairs output by the mix, which is again linear in the bulletin board’s length.

Thus, Athena has linear complexity $O(|bb|)$ in the length of the bulletin board (bb), assuming linear complexity of iterative homomorphic combinations ($\S3$), which is possible for El Gamal, for instance.

Comparison with the voting system by Juels, Catalano & Jakobsson. Complexity of the voting system by Juels, Catalano & Jakobsson is quadratic, due to pairwise plaintext equality tests performed on ballots to ensure that only the last choice of each voter has influence, which is needed for universal verifiability. By comparison, Athena uses anonymised credentials in a manner that achieves the same property, whilst reducing complexity. (The voting system by Juels, Catalano & Jakobsson also performs pairwise plaintext equality tests on mixed ballots and mixed credentials, to identify authorised ballots. The complexity of those tests is upper-bound by $O(|L| \cdot |bb|)$, where $L$ is the electoral roll and $|bb|$ is the bulletin board’s length. By comparison, the plaintext equality tests performed by Athena are upper-bound by $O(|bb|)$.)

7 General design principles

General design principles were identified and embraced during the development of Athena. This section shares these principles to aid the development of future voting systems, especially those with linear complexity. Our first design principle is guided by definitions of correctness and universal verifiability:

1. Algorithm Tally must map votes expressed in authorised ballots to the outcome corresponding to those votes, except for any early votes.

It follows that:
2. Algorithm Vote must authenticate ballots.

The next two design principles follow from our informal definitions of ballot secrecy and coercion resistance, respectively:

3. Algorithm Vote must ensure votes cannot be revealed from ballots; and

4. Algorithm Tally must not reveal any (meaningful) mapping between ballots and the outcome.

Forgoing coercion resistance (in favour of ballot secrecy), the previous design principle can be generalised: Algorithm Tally must not reveal any (meaningful) mapping between authorised ballots and the outcome. But this permits revealing authorised ballots, which allows simulation attacks [41, §1.1], whereby a coarser instructs a voter to reveal their private credential, uses that private credential to cast a ballot, and determines whether the voter followed instruction by checking whether the cast ballot is authorised. By comparison, (4) gives way to the following design principle:

5. Algorithm Tally must not reveal authorised ballots.

Similarly, authorised ballots must not be revealed during casting and collection:

6. Algorithm Vote must not reveal authorised ballots.

Since ballots must be authenticated (1) without revealing authorised ballots (5 & 6), the following principle emerges:

7. Algorithm Tally should anonymise ballots prior to authentication.

Given that ballots should be anonymised (7) and that bulletin boards may contain more than just ballots, it is proposed that:

8. Algorithm Vote should prove correct ballot construction; and

9. Algorithm Tally should discard garbage, i.e., non-ballots.

Revealing re-votes after anonymisation can be problematic, for instance, a voter that casts a specific number of ballots can deanonymise their anonymised ballots. Thus, our final design principle is suggested:

10. Algorithm Tally should discard ballots representing early votes prior to anonymisation.

For compatibility between (7 & 10) and (4), our notion of meaningful should exclude garbage and early votes, i.e., algorithm Tally is permitted to reveal mappings between the outcome and garbage, ballots representing early votes, or both.
**Figure 1** General design principles: Algorithm Tally should filter the bulletin board to discard garbage, early votes, and unauthorised (anonymised) ballots, the algorithm should also map any authenticated (anonymous) ballots to the outcome.

By combining our design principles, we observe that algorithm Tally should filter the bulletin board to remove garbage (9) and ballots representing early votes (10). Moreover, after anonymising any remaining ballots, the algorithm should authenticate anonymised ballots and remove any unauthorised anonymous ballots (7). Finally, votes expressed in any authenticated anonymous ballots should be mapped to the outcome corresponding to those votes (1). This procedure is illustrated in Figure 1 and underpins the design of Athena.

### 8 Related work

Acquisti [1], Smith [64], and Weber, Araújo & Buchmann [73] reduce complexity to linear in variants of the voting system by Juels, Catalano & Jakobsson, but those reductions led to the lose of coercion-resistance [3–6, 21]. Araújo et al. [3–5] make better progress, albeit, without supporting audits for statistically determining whether non-voters are issued with credentials [6, 60, 70] and without supporting reuse of credentials between elections [2, 6]. Haghighat, Dousti & Jalili do not permit reuse either [35], whereas Araújo et al. do [2, 6], albeit, Araújo et al. do not achieve strong non-reusability (i.e., only the last choice of each voter has influence [54]) nor universal verifiability, in the presence of an adversary that can re-order ballots (e.g., a network adversary), because they are reliant on ballot order to discard early votes.\(^8\)\(^9\) (The voting system by Juels,

---

\(^8\)Araújo et al. can probably achieve strong non-reusability and universal verifiability using counters, as per Athena.

\(^9\)Araújo et al. do not specify sufficient details to ensure non-malleable ballots, without which unforgeability is not satisfied, because authentication material can be replayed. Similarly, encrypted votes can be replayed to violate coercion-resistance (cf. [8, 25, 55, 59, 74]).
Catalano & Jakobsson does not satisfy strong non-reusability nor universal verifiability against such an adversary either, whereas Civitas does \cite{69, §4.2.2}. Schläpfer et al. and Spycher et al. also make progress, albeit, Schläpfer et al. only achieve linear complexity for a trade in the degree of coercion-resistance and they leak the number of ballots each voter casts \cite{60} and Spycher et al. make an additional trust assumption, namely, they assume the tallier introduces a secret number of dummy votes for each voter (without any means for voters to confirm they did) \cite{70}. Beyond variants of the voting system by Juels, Catalano & Jakobsson, distinct voting systems have also been introduced: The system by Schweisgut \cite{63} achieves linear-complexity, but fails to achieve coercion-resistance \cite{5}. Clark & Hengartner propose the Selections voting system, which makes better progress, albeit, some degree of coercion-resistance is traded to achieve linear complexity and the number of ballots each voter casts is leaked \cite{18, 19}. (Athena leaks the number of ballots cast in association with each public credential, but not the number of ballots each voter casts.) Finally, Essex, Clark & Hengartner propose the Cobra voting system, which achieves remarkably fast tallying, albeit, registration has quadratic complexity in the number of voters \cite{29}. With the exception of Juels, Catalano & Jakobsson, Haghighat, Dousti & Jalili, and Clark & Hengartner, none of these prior works present security proofs and proving their security remains an open problem. (Araújo et al. \cite{2, 5} formally state theorems, but defer proofs to full versions of their papers, which do not appear to be public.)

9 Conclusion

For one and a half decades, researchers have strived to improve upon seminal work by Juels, Catalano & Jakobsson. This work attempts to deliver such an improvement: A verifiable, coercion-resistant voting system with linear complexity in the length of the bulletin board. We have seen how several of the ideas can help improve security of existing voting systems. Moreover, they generalise beyond voting to other systems that require strong forms of privacy, authentication, and verifiability, thereby advancing not just voting technology, but the science of security.

A Cryptographic primitives

A.1 Asymmetric encryption

Definition 3 (Asymmetric encryption scheme \cite{42}). An asymmetric encryption scheme is a tuple of probabilistic polynomial-time algorithms \((\text{Gen}, \text{Enc}, \text{Dec})\), such that.\footnote{Nonetheless, including the entire ballot (except proofs) in the hashes used by proofs should suffice to ensure non-malleability.}

\cite{10}Our definition differs from Katz and Lindell’s original definition \cite[Definition 10.1]{42} in that we formally state the plaintext space.
• **Gen**, denoted \((pk, sk, m) \leftarrow \text{Gen}(\kappa)\), inputs a security parameter \(\kappa\) and outputs a key pair \((pk, sk)\) and message space \(m\).

• **Enc**, denoted \(c \leftarrow \text{Enc}(pk, m)\), inputs a public key \(pk\) and message \(m \in m\), and outputs a ciphertext \(c\).

• **Dec**, denoted \(m \leftarrow \text{Dec}(sk, c)\), inputs a private key \(sk\) and ciphertext \(c\), and outputs a message \(m\) or an error symbol. We assume \(\text{Dec}\) is deterministic.

Moreover, the scheme must be correct: there exists a negligible function \(\text{negl}\), such that for all security parameters \(\kappa\) and messages \(m\), we have \(\Pr[(pk, sk, m) \leftarrow \text{Gen}(\kappa); c \leftarrow \text{Enc}(pk, m) : m \in m \Rightarrow \text{Dec}(sk, c) = m] > 1 - \text{negl}(\kappa)\). A scheme has perfect correctness if the probability is 1.

**Definition 4** (Homomorphic encryption [69]). An asymmetric encryption scheme \(\Pi = (\text{Gen}, \text{Enc}, \text{Dec})\) is homomorphic, with respect to ternary operators \(\odot, \oplus, \otimes, \circ\), if there exists a negligible function \(\text{negl}\), such that for all security parameters \(\kappa\), we have the following.\(^\text{11}\) First, for all messages \(m_1\) and \(m_2\) we have \(\Pr[(pk, sk, m) \leftarrow \text{Gen}(\kappa); c_1 \leftarrow \text{Enc}(pk, m_1); c_2 \leftarrow \text{Enc}(pk, m_2) : m_1, m_2 \in m \Rightarrow \text{Dec}(sk, c_1 \odot_{pk} c_2) = \text{Dec}(sk, c_1) \odot_{pk} \text{Dec}(sk, c_2)] > 1 - \text{negl}(\kappa)\). Secondly, for all messages \(m_1\) and \(m_2\), and all coins \(r_1\) and \(r_2\), we have \(\Pr[(pk, sk, m) \leftarrow \text{Gen}(\kappa); m_1, m_2 \in m \Rightarrow \text{Enc}(pk, m_1; r_1) \odot_{pk} \text{Enc}(pk, m_2; r_2) = \text{Enc}(pk, m_1 \odot_{pk} m_2; r_1 \oplus_{pk} r_2)] > 1 - \text{negl}(\kappa)\). We say \(\Pi\) is multiplicative homomorphic, if for all security parameters \(\kappa\), key pairs \(pk, sk\), and message spaces \(m\), such that there exists coins \(r\) and \((pk, sk, m) = \text{Gen}(\kappa; r)\), we have \(\odot_{pk}\) is the multiplication operator in group \((m, \odot_{pk})\).

**Definition 5** (IND-CPA [7]). Let \(\Pi = (\text{Gen}, \text{Enc}, \text{Dec})\) be an asymmetric encryption scheme, \(\mathcal{A}\) be an adversary, \(\kappa\) be the security parameter, and IND-CPA(\(\Pi, \mathcal{A}, \kappa\)) be the following game.\(^\text{13}\)

\[
\text{IND-CPA}(\Pi, \mathcal{A}, \kappa) = \begin{align*}
\text{(pk, sk, m)} & \leftarrow \text{Gen}(\kappa); \\
\text{(m_0, m_1)} & \leftarrow \mathcal{A}(pk, m, \kappa); \\
\beta & \leftarrow_R \{0, 1\}; \\
c & \leftarrow \text{Enc}(pk, m_\beta); \\
g & \leftarrow \mathcal{A}(c); \\
\text{return } g = \beta;
\end{align*}
\]

\(^{11}\)For brevity, we write \(\Pi\) is a homomorphic asymmetric encryption scheme as opposed to the more verbose \(\Pi\) is a homomorphic asymmetric encryption scheme, with respect to ternary operators \(\odot, \oplus, \otimes, \circ\).

\(^{12}\)We write \(X \circ_{pk} Y\) for the application of ternary operator \(\circ\) to inputs \(X, Y, \) and \(pk\). We occasionally abbreviate \(X \circ_{pk} Y\) as \(X \circ Y\), when \(pk\) is clear from the context.

\(^{13}\)Our definition of an asymmetric encryption scheme explicitly defines the plaintext space, whereas Bellare et al. [7] leave the plaintext space implicit; this change is reflected in our definition of IND-CPA. Moreover, we provide the adversary with the message space and security parameter.
In the above game, we require \( m_0, m_1 \in \mathbb{m} \) and \(|m_0| = |m_1|\). We say \( \Pi \) satisfies IND-CPA, if for all probabilistic polynomial-time adversaries \( A \), there exists a negligible function \( \text{negl} \), such that for all security parameters \( \kappa \), we have \( \text{Succ}(\text{IND-CPA}(\Pi, A, \kappa)) \leq \frac{1}{2} + \text{negl}(\kappa) \).

### A.2 Proof systems

**Definition 6.** Let \((\text{Gen, Enc, Dec})\) be a homomorphic asymmetric encryption scheme and \( \Sigma \) be a sigma protocol for a binary relation \( R \).\(^{14}\)

- \( \Sigma \) proves key generation [69] if \( a ((\kappa, pk, m), (sk, s)) \in R \Leftrightarrow (pk, sk, m) = \text{Gen}(\kappa; s) \).

Further, suppose that \((pk, sk, m)\) is the output of \( \text{Gen}(\kappa; s) \), for some security parameter \( \kappa \) and coins \( s \).

- \( \Sigma \) proves ciphertext construction if \( ((pk, c, m'), (m, r)) \in R \Leftrightarrow c = \text{Enc}(pk, m; r) \land m \in \mathbb{m}' \land m' \subseteq \mathbb{m} \) [69], or \( ((pk, g, c, m'), (m, r)) \in R \Leftrightarrow c = \text{Enc}(pk, g^r; r) \land m \in \mathbb{m}' \land m' \subseteq \mathbb{m} \), where \( g \) is a generator of message space \( \mathbb{m} \).

- \( \Sigma \) proves decryption [69] if \( ((pk, c, m), sk) \in R \Leftrightarrow m = \text{Dec}(sk, c) \).

- \( \Sigma \) proves iterative homomorphic combination if \( ((pk, c, c'), n) \in R \Leftrightarrow \bigwedge_{1 \leq i \leq |c|} c'[i] = \bigotimes_{1}^{n} c'[i] \land |c'| = |c'| \)^{15}

**Definition 7** (Non-interactive proof system [69]). A non-interactive proof system for a relation \( R \) is a tuple of algorithms \((\text{Prove}, \text{Verify})\), such that:

- **Prove**, denoted \( \sigma \leftarrow \text{Prove}(s, w, \kappa) \), is executed by a prover to prove \((s, w) \in R \).

- **Verify**, denoted \( \nu \leftarrow \text{Verify}(s, \sigma, \kappa) \), is executed by anyone to check the validity of a proof. We assume Verify is deterministic.

Moreover, the system must be complete: there exists a negligible function \( \text{negl} \), such that for all statement and witnesses \((s, w) \in R \) and security parameters \( \kappa \), we have \( \Pr[\sigma \leftarrow \text{Prove}(s, w, \kappa) : \text{Verify}(s, \sigma, \kappa) = 1] > 1 - \text{negl}(\kappa) \). A system has perfect completeness if the probability is 1.

**Definition 8** (Fiat-Shamir transformation [30]). Given a sigma protocol \( \Sigma = (\text{Comm, Chal, Resp, Verify}) \) for relation \( R \) and a hash function \( \mathcal{H} \), the Fiat-Shamir transformation, denoted \( \text{FS}(\Sigma, \mathcal{H}) \), is the non-interactive proof system \((\text{Prove}, \text{Verify})\), defined as follows:

\(^{14}\)Given a binary relation \( R \), we write \((s_1, \ldots, s_l), (w_1, \ldots, w_k) \in R \Leftrightarrow P(s_1, \ldots, s_l, w_1, \ldots, w_k) \) for \((s, w) \in R \Leftrightarrow P(s_1, \ldots, s_l, w_1, \ldots, w_k) \land s = (s_1, \ldots, s_l) \land w = (w_1, \ldots, w_k) \), hence, \( R \) is only defined over pairs of vectors of lengths \( l \) and \( k \).

\(^{15}\)We write \( \text{ProveComb}((pk, (c, c')), n, \kappa) \) for \( \text{ProveComb}((pk, (c, c')), n, \kappa) \) when \( c \) and \( c' \) are ciphertexts (rather than vectors), where \( \text{ProveComb, VerComb} = \text{FS}(\Sigma, \mathcal{H}) \) for a sigma protocol \( \Sigma \) that proves iterative homomorphic combination and a hash function \( \mathcal{H} \).
Prove\((s, w, \kappa) = \)
\[(\text{comm}, t) \leftarrow \text{Comm}(s, w, \kappa); \]
\[\text{chal} \leftarrow \mathcal{H}(\text{comm}, s); \]
\[\text{resp} \leftarrow \text{Resp(chal, } t, \kappa); \]
\[\text{return (comm, resp)}; \]

Verify\((s, (\text{comm, resp}), \kappa) = \)
\[\text{chal} \leftarrow \mathcal{H}(\text{comm, } s); \]
\[\text{return } \text{Verify}_\Sigma(s, (\text{comm, chal, resp}), \kappa); \]

A string \(m\) can be included in the hashes computed by algorithms Prove and Verify. That is, the hashes are computed in both algorithms as \(\text{chal} \leftarrow H(\text{comm}, s, m)\). We write \(\text{Prove}(s, w, m, \kappa)\) and \(\text{Verify}(s, (\text{comm, resp}), m, \kappa)\) for invocations of Prove and Verify which include string \(m\).

Definition 9 (Simulation sound extractability [12, 34, 69]). Suppose \(\Sigma\) is a sigma protocol for relation \(R\), \(H\) is a random oracle, and \((\text{Prove, Verify})\) is a non-interactive proof system, such that \(FS(\Sigma, H) = (\text{Prove, Verify})\). Further suppose \(S\) is a simulator for \((\text{Prove, Verify})\) and \(H\) can be patched by \(S\). Proof system \((\text{Prove, Verify})\) satisfies simulation sound extractability if there exists a probabilistic polynomial-time algorithm \(K\), such that for all probabilistic polynomial-time adversaries \(A\) and coins \(r\), there exists a negligible function \(\text{negl}\), such that for all security parameters \(\kappa\), we have:\(^{16}\)

\[
\Pr[\text{P } \leftarrow (\); Q \leftarrow A^{H, P}(--; r); W \leftarrow K^{A'}(H, P, Q) :
|Q| \neq |W| \lor \exists j \in \{1, \ldots, |Q|\}. (Q[j][1], W[j]) \notin R \land
\forall (s, \sigma) \in Q, (t, \tau) \in P : \text{Verify}(s, \sigma, \kappa) = 1 \land \sigma \neq \tau \leq \text{negl}(\kappa)]
\]

where \(A(--; r)\) denotes running adversary \(A\) with an empty input and coins \(r\), where \(H\) is a transcript of the random oracle’s input and output, and where oracles \(A'\) and \(P\) are defined below:

- \(A'()\). Computes \(Q' \leftarrow A(--; r)\), forwarding any of \(A\)'s oracle queries to \(K\), and outputs \(Q'\). By running \(A(--; r)\), \(K\) is rewinding the adversary.

- \(P(s)\). Computes \(\sigma \leftarrow S(s, \kappa); P \leftarrow (P[1], \ldots, P[|P|], (s, \sigma))\) and outputs \(\sigma\).

Algorithm \(K\) is an extractor for \((\text{Prove, Verify})\).

Theorem 5 (from [12]). Let \(\Sigma\) be a sigma protocol for relation \(R\), and let \(H\) be a random oracle. Suppose \(\Sigma\) satisfies special soundness and special honest verifier zero-knowledge. Non-interactive proof system \(FS(\Sigma, H)\) satisfies simulation sound extractability.

\(^{16}\)We extend set membership notation to vectors: we write \(x \in x\) if \(x\) is an element of the set \(\{x[i] : 1 \leq i \leq |x|\}\).
The Fiat-Shamir transformation may include a string in the hashes computed by functions Prove and Verify. Simulators can be generalised to include such a string too. We write $S(s, m, \kappa)$ for invocations of simulator $S$ which include string $m$. And remark that Theorem 5 can be extended to this generalisation.

**B Proof of correctness (Lemma 1)**

Let $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$, $FS(\Sigma_1, H) = (\text{ProveKey}, \text{VerKey})$, $FS(\Sigma_2, H) = (\text{ProveCiph}, \text{VerCiph})$, and $\text{Athena}(\Pi, M, \Sigma_1, \Sigma_2, \Sigma_3, \Sigma_4, H) = (\text{Setup}, \text{Register}, \text{Vote}, \text{Tally}, \text{Verify})$.

Suppose $\kappa$ is a security parameter, $nv$ and $nc$ are integers, $v_1, \ldots, v_{nv}$ are vectors over $\{1, \ldots, nc\}$, $c_1, \ldots, c_{nv}$ are vectors such that $\bigwedge_{1 \leq i \leq nv} |v_i| = |c_i| \land c_i[1] < \cdots < c_i[|c_i|]$, and $v$ is a zero-filled vector of length $nc$. Further suppose we compute:

$$(pk, sk, mb, mc) \leftarrow \text{Setup}(\kappa);$$

$$bb \leftarrow \emptyset;$$

$$\text{for } 1 \leq i \leq nv \text{ do} \begin{cases} (pd_i, d_i) \leftarrow \text{Register}(pk, \kappa); \\
\text{if } 0 < |v_i| \text{ then} \\
\quad \text{for } 1 \leq j \leq |v_i| \text{ do} \\
\quad\quad b_{i,j} \leftarrow \text{Vote}(d_i, pk, v_i[j], c_i[j], nc, \kappa); \\
\quad bb \leftarrow bb \cup \{b_{i,1}, \ldots, b_{i,|v_i|}\}; \\
\quad v[v_i[|v_i|]] \leftarrow v[v_i[|v_i|]] + 1; \end{cases}$$

If $|bb| \not\leq mb \lor nc \not\leq mc$, then correctness is trivially satisfied, otherwise ($(bb) \leq mb \land nc \leq mc$), we proceed as follows.

By definition of algorithm Setup, we have $pk$ parses as vector $(pk, m, \rho)$ and $sk$ parses as $(pk, sk)$, where $(pk, sk, m) = \text{Gen}(\kappa, r)$ for some coins $r$ and $\rho$ is an output of $\text{ProveKey}(\kappa, pk, m)$, $(sk, r, \kappa)$. Moreover, by completeness, we have $\text{VerKey}(\kappa, pk, m, \rho, \kappa)$ holds. Let $g$ be a generator of message space $m$. By definition of algorithm Register, we have for each $i \in \{1, \ldots, nv\}$ that $pd_i = \text{Enc}(pk, g^{d_i}; r_i)$ and $d_i = (pd_i, d_i)$, for some coins $r_i$ chosen uniformly at random and nonce $d_i$. Moreover, by definition of algorithm Vote, we have for each $i \in \{1, \ldots, nv\}$ and $j \in \{1, \ldots, |v_i|\}$ that $b_{i,j}$ is a vector of length six, $b_{i,j}[1] = pd_i$, $b_{i,j}[2] = \text{Enc}(pk, g^{-d_i}; s_{i,j})$, $b_{i,j}[3] = \text{Enc}(pk, v_i[j]; t_{i,j})$.

$b_{i,j}[4]$ is an output of $\text{ProveCiph}((pk, g, b_{i,j}[2], m), (-d_i, s_{i,j}, m, \kappa)$, $b_{i,j}[5]$ is an output of $\text{ProveCiph}((pk, b_{i,j}[3], \{1, \ldots, nc\}), (v_i[j], t_{i,j}), m, \kappa)$, and $b_{i,j}[6] = c_i[j]$, where $s_{i,j}$ and $t_{i,j}$ are coins chosen uniformly at random and $m = (pd_i, b_{i,j}[2], b_{i,j}[3], b_{i,j}[6])$. Let us consider the computation of $(v', pf)$ by $\text{Tally}(sk, bb, nc, \{pd_1, \ldots, pd_{nv}\}, \kappa)$. 

24
We have \(b \mathcal{B} = \bigcup_{1 \leq l \leq n \wedge |v| > 0} \{b, 1, \ldots, b, i, |v|\}\). Suppose a subset of that set is computed as per Step 1 of algorithm \(Tally\). By completeness and since for each \(i \in \{1, \ldots, nv\}\) we have \(pd_i = b, 1, \ldots = b, i, |v| [1]\), that subset is \(\{b, \pi(1), \pi(1), \ldots, b, \pi(1), \pi(1) |v| [1], \ldots, b, \pi(nv), \pi(1), \ldots, b, \pi(nv), \pi(1) |v| [1]\}\) for some permutation \(\pi\) on \(\{1, \ldots, nv\}\) and for each \(i \in \{1, \ldots, nv\}\) some permutation \(\pi_i\) on \(\{1, \ldots, |v|\}\) such that \(b, \pi(1), \pi(1) |v| [1] \leq \cdots \leq b, \pi(1), \pi(1) |v| [1] \leq \cdots \leq b, \pi(t), \pi(1) |v| [1]\). If \(nv = 0 \lor \bigwedge_{1 \leq l \leq nv} |v| = 0\), then \(v\) and \(v'\) are both zero-filled vectors of length \(nc\), and we conclude immediately, otherwise, we proceed as follows.

Suppose ciphertexts, plaintexts, and a map are computed as per Step 2 of algorithm \(Tally\), with respect to nonce \(n\). Since \(\Pi\) is a multiplicative-homomorphic asymmetric encryption scheme, we have for each \(i \in \{1, \ldots, nv\}\) and \(j \in \{1, \ldots, |v|\}\) that

\[
c'_{i,j} = \bigotimes_{1}^{n} b, i, j [2] = \text{Enc}(pk, \otimes \gamma g^{-d_i}; \otimes \gamma s_{i,j}) = \text{Enc}(pk, g^{-d_i}; \otimes \gamma s_{i,j}),
\]

hence, by (perfect) correctness, we have

\[
N_{i,j} = \text{Dec}(sk, c'_{i,j}) = g^{-d_i},
\]

where ciphertext \(c'_{i,j}\) and plaintext \(N_{i,j}\) are computed by algorithm \(Tally\). (We require perfect correctness, because the adopted definition of homomorphic encryption only considers combination of distinct ciphertexts constructed from distinct coins, whereas we consider iterative combination of a single ciphertext.) Hence, for each \(i \in \{1, \ldots, nv\}\) we have

\[
N_{i,1} = \cdots = N_{i,|v|}.
\]

Since \(d_1, \ldots, d_{nv}\) are nonces, \(g\) is a generator of message space \(m\), and \(|m|\) is super-polynomial in the security parameter, we have \(N_{i,|v|}, \ldots, N_{nv,|v|}\) are pairwise distinct, moreover, since \(|v| = |c|\) \(\wedge c_{i}[1] < \cdots < c_{i}[|c|]\) and \(b, i, |v| [6] = c_{i}[j]\) for \(j \in \{1, \ldots, |c|\}\), we have for each \(i \in \{1, \ldots, nv\}\) that

\[
A[(pd_i, N_{i,1})] = (b, i, |v| [6], b, i, |v| [1] \otimes b, i, |v| [2], b, i, |v| [3]),
\]

where map \(A\) is computed by algorithm \(Tally\). It follows that map \(A\) is defined over ciphertexts \(b, i, |v| [1] \otimes b, i, |v| [2], b, i, |v| [3], \ldots, b, nv, |v| [1] \otimes b, nv, |v| [2], b, nv, |v| [3]\). Suppose mixnet \(\mathcal{M}\) is applied to those pairs of ciphertexts to derive vector \(B = (b_1, \ldots, b_{nv})\), as per Step 2 of algorithm \(Tally\). Since \(\Pi\) is a multiplicative-homomorphic asymmetric encryption scheme, we have for each \(i \in \{1, \ldots, nv\}\) that

\[
b, i [1] = \text{Enc}(pk, g^{d_i} \otimes g^{-d_i}; r_i \otimes s_{i, |v|} \oplus w_i)
= \text{Enc}(pk, g^0; r_i \otimes s_{i, |v|} \oplus w_i)
\]

\[
b, i [2] = \text{Enc}(pk, v, [|v|]; t_{i, |v|} \oplus x_i),
\]

25
where $\iota$ denotes $\chi(i)$ and $\chi$ is a permutation over $\{1, \ldots, nv\}$ and coins $w_i$ and $x_i$ were introduced during mixing.

Suppose for each $i \in \{1, \ldots, nv\}$ that $c' = \bigotimes_{j=1}^{n_i} b_i[1]$ and $m = \text{Dec}(sk, c')$ are computed as per Step 3 of algorithm Tally. It follows by (perfect) correctness and homomorphic properties that $m = 1$. Moreover, $\text{Dec}(sk, b_i[2]) = v_{\chi(i)}[\chi(i)]$ for each $i \in \{1, \ldots, nv\}$. Since $\chi$ is a permutation over $\{1, \ldots, nv\}$, it follows that $v$ is equivalent to the outcome that would be computed by Step 3 of algorithm Tally, which concludes our proof. □

C Verifiability by Smyth, Frink & Clarkson

We cast the verifiability definitions by Smyth, Frink & Clarkson [69] into the context of our syntax, extend their definition of Soundness to include re-voting, strengthen definitions of Injectivity, Individual-Verifiability and Unforgeability, and incorporate some minor refinements by Smyth [66, 67]. The definition of Completeness remains unchanged (beyond syntax changes).

C.1 Universal verifiability

Universal verifiability requires algorithm Verify to accept if and only if the election outcome is correct. The only if requirement is captured by soundness and the if requirement is captured by completeness.

Soundness. Correct outcomes are formalised using function $\text{correct-outcome}$. The function uses a predicate ($\exists^=\ell x : P(x)$) that holds exactly when there are $\ell$ distinct values of $x$ for which $P(x)$ is satisfied [62]. Using the predicate, function $\text{correct-outcome}$ is defined such that

$$\text{correct-outcome}(pk, nc, bb, M, \kappa)[v] = \ell \iff \exists^=\ell b \in \text{authorised}(pk, nc, (bb \setminus \{\bot\}), M, \kappa) :$$

$$\exists d, cnt, r : b = \text{Vote}(d, pk, v, cnt, nc, \kappa; r),$$

where $\text{correct-outcome}(pk, nc, bb, M, \kappa)$ is a vector of length $nc$, $1 \leq v \leq nc$, and

$$\text{authorised}(pk, nc, bb, M, \kappa) =$$

$$\{b_k \mid \exists b_1, \ldots, b_k \in bb : \exists cnt_1, \ldots, cnt_k : cnt_1 \leq \cdots \leq cnt_{k-1} < cnt_k$$

$$\wedge \exists(pd, d) \in M : \bigwedge_{1 \leq j \leq k} \exists v, r : b_j = \text{Vote}(d, pk, v, cnt_j, nc, \kappa; r)$$

$$\wedge \neg \exists b \in bb \setminus \{b_1, \ldots, b_k\}, v, cnt, r : b = \text{Vote}(d, pk, v, cnt, nc, \kappa; r)\}.$$ 

Function $\text{authorised}$ discards all ballots submitted under the same credential, except for a ballot containing the last vote. Hence, component $v$ of vector $\text{correct-outcome}(pk, nc, bb, M, \kappa)$ equals $\ell$ iff there exist $\ell$ authorised ballots for
vote \( v \) on the bulletin board. Function correct-outcome requires that ballots be interpreted for only one candidate, which can be ensured by injectivity, i.e., a ballot for vote \( v \) can never be interpreted for a distinct vote \( v' \).

**Definition 10 (Injectivity).** An election scheme \((\text{Setup}, \text{Register}, \text{Vote}, \text{Tally}, \text{Verify})\) satisfies injectivity, if for all probabilistic polynomial-time adversaries \( \mathcal{A} \), security parameters \( \kappa \) and computations \((pk, nc, d_1, v_1, cnt_1, d_2, v_2, cnt_2) \leftarrow \mathcal{A}(\kappa)\); \( b_1 \leftarrow \text{Vote}(d_1, pk, v_1, cnt_1, nc, \kappa) \); \( b_2 \leftarrow \text{Vote}(d_2, pk, v_2, cnt_2, nc, \kappa) \) such that \( v_1 \neq v_2 \wedge b_1 \neq \bot \wedge b_2 \neq \bot \), we have \( b_1 \neq b_2 \).

Equipped with a notion of correct outcomes, we formalise soundness (Definition 11) as a game that tasks the adversary to compute inputs to algorithm Verify – including an election outcome and some ballots – that cause the algorithm to accept an incorrect outcome.

**Definition 11 (Soundness).** Let \( \Gamma = (\text{Setup}, \text{Register}, \text{Vote}, \text{Tally}, \text{Verify}) \) be an election scheme, \( \mathcal{A} \) be an adversary, \( \kappa \) be a security parameter, and \( \text{Soundness}(\Gamma, \mathcal{A}, \kappa) \) be the following game.

\[
\text{Soundness}(\Gamma, \mathcal{A}, \kappa) =
\]

\[
(pk, nv) \leftarrow \mathcal{A}(\kappa);
\]

\[
\text{for } 1 \leq i \leq nv \text{ do } (pd_i, d_i) \leftarrow \text{Register}(pk, \kappa);
\]

\[
L \leftarrow \{pd_1, \ldots, pd_{nv}\};
\]

\[
M \leftarrow \{(pd_1, d_1), \ldots, (pd_{nv}, d_{nv})\};
\]

\[
(bb, nc, v, pf) \leftarrow \mathcal{A}(M);
\]

\[
\text{return } \text{Verify}(pk, bb, nc, L, v, pf, \kappa) = 1
\]

\[
\land v \neq \text{correct-outcome}(pk, nc, bb, M, \kappa);
\]

We say \( \Gamma \) satisfies Soundness, if \( \Gamma \) satisfies injectivity and for all probabilistic polynomial-time adversaries \( \mathcal{A} \), there exists a negligible function \( \text{negl} \), such that for all security parameters \( \kappa \), we have \( \text{Succ}(\text{Soundness}(\Gamma, \mathcal{A}, \kappa)) \leq \text{negl}(\kappa) \).

**Completeness.** We formalise completeness (Definition 12) as a game that tasks the adversary to compute a bulletin board and some number of candidates such that the corresponding election outcome computed by algorithm Tally is rejected by algorithm Verify, when the key pair is computed by algorithm Setup and voter credentials are computed by algorithm Register.

**Definition 12 (Completeness).** Let \( \Gamma = (\text{Setup}, \text{Register}, \text{Vote}, \text{Tally}, \text{Verify}) \) be an election scheme, \( \mathcal{A} \) be an adversary, \( \kappa \) be a security parameter, and \( \text{Completeness}(\Gamma, \mathcal{A}, \kappa) \) be the following game.

\[
\text{Completeness}(\Gamma, \mathcal{A}, \kappa) =
\]
\[(pk, sk, mb, mc) \leftarrow \text{Setup}(\kappa);\]
\[nv \leftarrow A(\kappa);\]
\[\text{for } 1 \leq i \leq nv \text{ do } (pd_i, d_i) \leftarrow \text{Register}(pk, \kappa);\]
\[L \leftarrow \{pd_1, \ldots, pd_nv\};\]
\[M \leftarrow \{(pd_1, d_1), \ldots, (pd_nv, d_nv)\};\]
\[(bb, nc) \leftarrow A(M);\]
\[(v, pf) \leftarrow \text{Tally}(sk, bb, nc, L, \kappa);\]
\[\text{return } \text{Verify}(pk, bb, nc, L, v, pf, \kappa) \neq 1 \land |bb| \leq mb \land nc \leq mc;\]

We say \(\Gamma\) satisfies Completeness, if for all probabilistic polynomial-time adversaries \(A\), there exists a negligible function \(\text{negl}\), such that for all security parameters \(\kappa\), we have \(\text{Succ(Completeness}(\Gamma, A, \kappa)) \leq \text{negl}(\kappa)\).

### C.2 Unforgeability

We formalise unforgeability (Definition 13) as a game that tasks the adversary to compute a ballot containing a private credential.

**Definition 13 (Unforgeability).** Let \(\Gamma = (\text{Setup, Register, Vote, Tally, Verify})\) be an election scheme, \(A\) be an adversary, \(\kappa\) be a security parameter, and \(\text{Unforgeability}(\Gamma, A, \kappa)\) be the following game.

\[\text{Unforgeability}(\Gamma, A, \kappa) =\]
\[(pk, nv) \leftarrow A(\kappa);\]
\[\text{for } 1 \leq i \leq nv \text{ do } (pd_i, d_i) \leftarrow \text{Register}(pk, \kappa);\]
\[L \leftarrow \{pd_1, \ldots, pd_nv\};\]
\[Crpt \leftarrow \emptyset; \text{ Rvld } \leftarrow \emptyset;\]
\[b \leftarrow A.C,R(L);\]
\[\text{return } \exists i \in \{1, \ldots, nv\}, v, cnt, nc, r : b = \text{Vote}(d_i, pk, v, cnt, nc, \kappa; r) \land b \neq \bot \land b \notin \text{Rvld} \land d_i \notin \text{Crpt};\]

Oracles \(C\) and \(R\) are defined such that:

- \(C(i)\) computes \(\text{Crpt } \leftarrow \text{Crpt } \cup \{d_i\}\) and outputs \(d_i\), where \(1 \leq i \leq nv\), and
- \(R(i, v, cnt, nc)\) computes \(b \leftarrow \text{Vote}(d_i, pk, v, cnt, nc, \kappa); \text{Rvld } \leftarrow \text{Rvld } \cup \{b\}\) and outputs \(b\).

We say \(\Gamma\) satisfies Unforgeability, if for all probabilistic polynomial-time adversaries \(A\), there exists a negligible function \(\text{negl}\), such that for all security parameters \(\kappa\), we have \(\text{Succ(Unforgeability}(\Gamma, A, \kappa)) \leq \text{negl}(\kappa)\).

### C.3 Individual verifiability

We formalise individual verifiability (Definition 14) as a game that tasks the adversary to compute inputs to algorithm Vote that cause the algorithm to output ballots that collide.\(^\text{17}\)

\(^\text{17}\)Correctness, individual verifiability and injectivity all require that ballots do not collide, albeit under different assumptions.
Definition 14 (Individual verifiability). Let \( \Gamma = (\text{Setup}, \text{Register}, \text{Vote}, \text{Tally}, \text{Verify}) \) be an election scheme, \( A \) be an adversary, \( \kappa \) be a security parameter, and Individual-Verifiability\((\Gamma, A, \kappa)\) be the following game.

\[
\text{Individual-Verifiability}(\Gamma, A, \kappa) =
\begin{align*}
& (pk, nc, d_1, v_1, \text{cnt}_1, d_2, v_2, \text{cnt}_2) \leftarrow A(\kappa); \\
& b_1 \leftarrow \text{Vote}(d_1, pk, v_1, \text{cnt}_1, \kappa); \\
& b_2 \leftarrow \text{Vote}(d_2, pk, v_2, \text{cnt}_2, nc, \kappa); \\
& \text{return } b_1 = b_2 \land b_1 \neq \bot \land b_2 \neq \bot;
\end{align*}
\]

We say \( \Gamma \) satisfies Individual-Verifiability, if for all probabilistic polynomial-time adversaries \( A \), there exists a negligible function \( \text{negl} \), such that for all security parameters \( \kappa \), we have \( \text{Succ}(\text{Individual-Verifiability}(\Gamma, A, \kappa)) \leq \text{negl}(\kappa) \).

D Proof of Propositions 2–4 (verifiability)

D.1 Proof of Proposition 2 (Soundness)

Let \( \Pi = (\text{Gen}, \text{Enc}, \text{Dec}), \text{FS}(\Sigma_1, \mathcal{H}) = (\text{ProofKey}, \text{VerKey}), \text{FS}(\Sigma_2, \mathcal{H}) = (\text{ProveCiph}, \text{VerCiph}), \text{FS}(\Sigma_3, \mathcal{H}) = (\text{ProveDec}, \text{VerDec}), \text{FS}(\Sigma_4, \mathcal{H}) = (\text{ProveComb}, \text{VerComb}) \), and \( \text{Athena}(\Pi, M, \Sigma_1, \Sigma_2, \Sigma_3, \Sigma_4, \mathcal{H}) = (\text{Setup}, \text{Register}, \text{Vote}, \text{Tally}, \text{Verify}) \).

Suppose \( A \) is a probabilistic polynomial-time adversary, \( \kappa \) is a security parameter, \( (pk, nc) \) is an output of \( A(\kappa) \), and \( (pd_1, d_1), \ldots, (pd_m, d_m) \) are outputs of \( \text{Register}(pk, \kappa) \). Let \( L = \{pd_1, \ldots, pd_m\} \) and \( M = \{(pd_1, d_1), \ldots, (pd_m, d_m)\} \).

Suppose \( (bb, nc, b, pf) \) is an output of \( A(M) \) such that \( \text{Verify}(pk, bb, nc, L, v, pf, \kappa) = 1 \). By definition of algorithm \( \text{Verify} \), public key \( pk \) parses as a vector \( (pk, m, \rho) \) and outcome \( b \) parses as a vector of length \( nc \) such that \( \text{VerKey}(\kappa, pk, m, \rho, \kappa) \land nc \leq mc \), where \( mc \) is computed as per algorithm \( \text{Setup} \). Moreover, by simulation sound extractability, public key \( pk \) is an output of algorithm \( \text{Gen} \). Furthermore, by definition of algorithm \( \text{Register} \), we have for each \( i \in \{1, \ldots, nc\} \) that public credential \( pd_i = \text{Enc}(pk, g^{d_i}; r_i) \) and private credential \( d_i = (pd_i, d_i) \), for some nonce \( d_i \) and coins \( r_i \) chosen uniformly at random.

Let set \( \{b_1, \ldots, b_\ell\} \) be computed as per Step 1 of algorithm \( \text{Verify} \). It follows that there exists an function \( \lambda : \{1, \ldots, \ell\} \to \{1, \ldots, nc\} \) such that \( b_i[1] = pd_{\lambda(i)} \) for each \( i \in \{1, \ldots, \ell\} \). Moreover, for all credentials \( (pd, d) \in M \), counters \( cnt \), votes \( v \in \{1, \ldots, nc\} \), and outputs \( b \) of algorithm \( \text{Vote}(\lambda, pk, v, cnt, nc, \kappa) \), we have \( b \notin \{b_1, \ldots, b_\ell\} \), since such an occurrence would imply a contradiction: \( \{b_1, \ldots, b_\ell\} \) is not the largest subset of \( bb \) satisfying the conditions in Step 1 of algorithm \( \text{Tally} \), because \( b \) parses as a senary vector \( (pd, c_1, c_2, \sigma_1, \sigma_2, cnt) \) such that \( pd \in L \land \text{VerCiph}((pk, g, c_1, m), \sigma_1, m, \kappa) \land \text{VerCiph}((pk, c_2, \{1, \ldots, nc\}, \sigma_2, m, \kappa), \) where \( m = (pd, c_1, c_2, cnt) \), yet \( b \notin \{b_1, \ldots, b_\ell\} \). Thus,

\[
\text{correct-outcome}(pk, nc, bb, M, \kappa) = \text{correct-outcome}(pk, nc, \{b_1, \ldots, b_\ell\}, M, \kappa) \tag{1}
\]
A proof of (1) follows from the definition of *correct-outcome*. If \( \{b_1, \ldots, b_\ell\} = \emptyset \), then outcome \( v \) and *correct-outcome*(\( pk, nc, \{b_1, \ldots, b_\ell\}, M, \kappa \)) are zero-filled vectors of length \( nc \), hence, *Soundness* is satisfied. Otherwise, we proceed as follows.

By simulation sound extractability, we have for each \( i \in \{1, \ldots, \ell\} \) that there exists messages \( d'_i \in m \) and \( v_i \in \{1, \ldots, nc\} \) and coins \( s_i \) and \( t_i \) such that

\[
\begin{align*}
b_i[2] &= \text{Enc}(pk, g^{d'_i}; s_i), \\
b_i[3] &= \text{Enc}(pk, v_i; t_i),
\end{align*}
\]

\( b_i[4] \) is an output of \( \text{ProveCiph}((pk, g, b_i[2], m), (d'_i, s_i), m, \kappa) \), and \( b_i[5] \) is an output of \( \text{ProveCiph}((pk, b_i[3], \{1, \ldots, nc\}), (v_i, t_i), m, \kappa) \), where \( m = (b_1[1], b_i[2], b_i[3], b_i[6]) \). It follows by inspection of algorithm *Vote* that \( \forall i \in \{1, \ldots, \ell\} \), \( \exists r : b_i = \text{Vote}(d'_i, pk, v_i, b_i[6], nc, \kappa) \), hence, \( \{b_1, \ldots, b_\ell\} \) is a set of ballots.

By Step 2 of algorithm *Verify*, we have that \(\text{pf} \) parses as a vector \((\text{pf}, B, \text{pfr})\) and \(\text{pfr} \) parses as a vector \(((c'_1, N_1, c_1), (c'_2, N_2, c_2, \omega_2), \ldots, (c'_{\ell}, N_{\ell}, c_\ell, \omega_{\ell}))\) such that \( \bigwedge_{1 \leq i \leq \ell} \text{VerDec}((pk, c'_i, N_i, c_i, \omega_i)) \) and \( \bigwedge_{1 \leq i \leq \ell} \text{VerComb}((pk, (c'_{i-1}, c'_i), (b_{i-1}[2], b_i[2])), \omega_i, \kappa) \). By simulation sound extractability, there exists a nonce \( n \) such that for all \( i \in \{1, \ldots, \ell\} \) we have

\[
c'_i = \bigodot_{i=1}^n b_i[2] = \text{Enc}(pk, \odot_n^i g^{d'_i}; \odot_n^i s_i) \equiv \text{Enc}(pk, g^{d'_i \cdot n}; \odot_n^i s_i)
\]

and \(\text{Dec}(sk, c'_i) = N_i\), moreover, by (perfect) correctness, we have

\[
N_i \equiv g^{d'_i \cdot n}.
\]

Let map \( A \) be computed as per Step 2 of algorithm *Verify*. It follows for each \( i \in \{1, \ldots, \ell\} \) that

\[
A((b_i[1], N_i)) = (b_i[6], b_i[1] \otimes b_i[2], b_i[3]) \iff \\
\neg \exists j \in \{1, \ldots, \ell\} \setminus \{i\} : b_i[1] = b_j[1] \land N_i = N_j \land b_i[6] \leq b_j[6]
\]

i.e., public credential \( b_i[1] \) and anonymised credential \( N_i \) are mapped to a triple derived from ballot \( b_i \) iff there is no other ballot \( b_j \) with the same public credential and the same anonymised credential that has a greater-than or equal-to counter value. Hence, for each anonymised credential, map \( A \) contains the encrypted vote associated with the highest counter, that is, the last vote related to the credential. Since (pairwise) mixnet \( M \) is verifiable and since Step 2 of algorithm *Verify* checks that \( B \) was output by the mixnet, there exists an injective function \( \chi : \{1, \ldots, |B|\} \to \{1, \ldots, \ell\} \) such that for each \( i \in \{1, \ldots, |B|\} \), we have \( B[i] \) is a pair \((c_1, c_2)\),

\[
c_1 = \text{Enc}(pk, g^{d_{\chi(i)} \cdot x\chi(i)} \odot g^{d\chi(i)}; r_{\chi(\Lambda(i))} \odot s_{\chi(i)} \oplus w_i), \quad \text{and}
\]

\[
c_2 = \text{Enc}(pk, v_{\chi(i)}; t_{\chi(i)} \oplus x_i)
\]
where coins \( w_i \) and \( x_i \) were introduced during mixing. It follows that

\[
\text{authorised}(pk, nc, \{b_1, \ldots, b_k\}, M, \kappa) = \text{authorised}(pk, nc, \{b_{\chi(i)} \mid 1 \leq i \leq |B|\}, M, \kappa)
\]  

(2)

because any ballot that shares a public credential (and a anonymised credential) with another ballot, whilst being associated with a (strictly) lower counter value can be discarded, as can any pair of ballots that share a public credential (and a anonymised credential) and a counter.

By Step 3 of algorithm \text{Verify}, we have for each \( i \in \{1, \ldots, |B|\} \) that \( B[i] \) parses as a vector \((c_1, c_2)\) and \( \text{pfd}[i] \) parses a vector \((c', m, \omega, \varsigma_1)\) or \((c', v, \omega, \varsigma_1, \varsigma_2)\), such that \( \text{VerDec}(pk, c', 1, \varsigma_1, \varsigma_2) \) when \( |\text{pfd}[i]| = 5 \) and \( \text{VerDec}(pk, c', m, \varsigma_1, \varsigma_2) \) when \( |\text{pfd}[i]| = 4 \), hence, by simulation sound extractability, (perfect) correctness, and multiplicatively-homomorphic properties, we have

\[
|\text{pfd}[i]| = 5 \iff \text{Dec}(sk, c') = 1 \iff 1 \equiv g^{d_{\lambda(i)}} \ ι \ g^{d'_{\lambda(i)}} \ \iff d'_{\lambda(i)} \equiv -d_{\lambda(i)}.
\]

It follows that \( b_{\chi(i)} \) is constructed from \((pd_{\chi(i)}, d_{\chi(i)}) \in M\) iff \( |\text{pfd}[i]| = 5 \), where \( i \in \{1, \ldots, |B|\} \), hence, \n
\[
\text{authorised}(pk, nc, \{b_{\chi(i)} \mid 1 \leq i \leq |B|\}, M, \kappa)
\]

\[
= \text{authorised}(pk, nc, \{b_{\chi(i)} \mid 1 \leq i \leq |B| \land |\text{pfd}[i]| = 5\}, M, \kappa)
\]

\[
= \{b_{\chi(i)} \mid 1 \leq i \leq |B| \land |\text{pfd}[i]| = 5\} \quad (3)
\]

because any ballot not constructed from \((pd, d) \in M\) can be discarded and no further ballots can. Moreover, it follows from the remainder of Step 3 that for each \( v \in \{1, \ldots, nc\} \) we have \( \exists^{v^n[i]} \in \{1, \ldots, |B|\} : \exists c_1, c_2, c', m, \omega, \varsigma_1, \varsigma_2 : (c_1, c_2) = B[i] \land (c', v, \omega, \varsigma_1, \varsigma_2) = \text{pfd}[i] \land \text{VerDec}(pk, c_1, c_2, v, \varsigma_1, \varsigma_2) \), hence, by simulation sound extractability, we have

\[
\exists^{v^n[i]} \in \{1, \ldots, |B| \land |\text{pfd}[i]| = 5\} : \exists c_1, c_2 : (c_1, c_2) = B[i] \land \text{Dec}(sk, c_2) = v,
\]

furthermore, by (perfect) correctness, we have

\[
\exists^{v^n[i]} \in \{1, \ldots, |B| \land |\text{pfd}[i]| = 5\} : v = v_{\chi(i)}.
\]

If follows for each \( v \in \{1, \ldots, nc\} \) that

\[
\exists^{v^n[b]} \in \{b_{\chi(i)} \mid 1 \leq i \leq |B| \land |\text{pfd}[i]| = 5\} : \exists d, cnt, r : b = \text{Vote}(d, pk, v, cnt, nc, \kappa; r).
\]

Finally, by (1)–(3) and since error symbol \( \perp \) is not a vector, we have \( v = \text{correct-outcome}(pk, nc, bb, M, \kappa) \), concluding our proof. \( \square \)
D.2 Proof of Proposition 3 (Completeness)

Let $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$, \(FS(\Sigma_2, \mathcal{H}) = (\text{ProveKey}, \text{VerKey})\), \(FS(\Sigma_2, \mathcal{H}) = (\text{ProveCiph}, \text{VerCiph})\), \(FS(\Sigma_3, \mathcal{H}) = (\text{ProveDec}, \text{VerDec})\), \(FS(\Sigma_4, \mathcal{H}) = (\text{ProveComb}, \text{VerComb})\), and \(\text{Athena}(\Pi, M, \Sigma_1, \Sigma_2, \Sigma_3, \Sigma_4, \mathcal{H}) = (\text{Setup}, \text{Register}, \text{Vote}, \text{Tally}, \text{Verify})\).

Suppose $\kappa$ is a security parameter and $A$ is a probabilistic polynomial-time adversary. Further suppose $(pk, sk, mb, mc)$ is an output of $\text{Setup}(\kappa)$, $nv$ is an output of $A(pk, \kappa)$, and $(pd_1, d_1), \ldots, (pd_n, d_n)$ are outputs of $\text{Register}(pk, \kappa)$. Let $L = \{pd_1, \ldots, pd_n\}$ and $M = \{(pd_1, d_1), \ldots, (pd_n, d_n)\}$. Suppose $(bb, nc)$ is an output of $A(M)$ and $(v, pf)$ is an output of $\text{Tally}(sk, bb, nc, L, \kappa)$. If $|bb| \not\leq mb \lor nc \not\leq mc$, then we conclude immediately, otherwise $(|bb| \leq mb \land nc \leq mc)$, we proceed as follows. By definition of algorithm $\text{Setup}$, we have $pk$ parses as $(pk, m, \rho)$ and $sk$ parses as $(pk, sk)$, where $(pk, sk, m) = \text{Gen}(\kappa; r)$ and $\rho$ is an output of $\text{ProveKey}(\kappa, pk, m, (sk, r), \kappa)$, for some coins $r$ chosen uniformly at random. Moreover, by definition of algorithm Tally, we have $v$ is a vector of length $nc$. It follows that algorithm Verify can parse inputs correctly. Moreover, by completeness, we have $\text{VerKey}((\kappa, pk, m), \rho, \kappa) = 1$.

Suppose subset $\{b_1, \ldots, b_{\ell}\}$ is computed as per Step 1 of algorithm Tally. If that set is empty, then $v$ is a zero-filled vector, because $v$ is initialised as a zero-filled vector by algorithm Tally. Thus, the check holds in Step 1 of algorithm Verify.

By Step 1 of algorithm Tally, we have for each $i \in \{1, \ldots, \ell\}$ that $b_i$ parses as $(pd, c_1, c_2, \sigma_1, \sigma_2, cnt)$ such that $pd \in L \land \text{VerCiph}(pk, g, c_1, m, \sigma_1, m, \kappa) \land \text{VerCiph}(pk, c_2, \{1, \ldots, nc\}, \sigma_2, m, \kappa)$, where $m = (pd, c_1, c_2, cnt)$. Hence, there exists an integer $j \in \{1, \ldots, nv\}$ such that $pd = pd_j$. It follows by definition of algorithm Register that $b_i[1] = \text{Enc}(pk, g^{b_j}; r_j)$, for some coins $r_j$ chosen uniformly at random and nonce $d_j$ such that private credential $d_j = (pd_j, d_j)$. Moreover, since $\Sigma_2$ satisfies special soundness and special honest verifier zero-knowledge, we have by simulation sound extractability that $b_i[2] = \text{Enc}(pk, g^{s_j}; t_j)$ and $b_i[3] = \text{Enc}(pk, v_j; t_j)$, for some coins $s_j$ and $t_j$, plaintext $d_j \in m$, and vote $v_j \in \{1, \ldots, nc\}$. It follows that the map $(A)$ computed in Step 2 of algorithm Tally is populated with pairs of ciphertexts. Thus, vector $B$ – derived by application of (pairwise) mixnet $M$ to map $A$ in Step 2 of algorithm Tally – passes the check in Step 2 of algorithm Verify, because $M$ is verifiable. The preceding checks also pass. Indeed, by definition of algorithm Tally, it is trivial to see that $pf$ parses as a vector $(\text{pf}, B, \text{pdf})$. Moreover, the vector $(\text{pdf})$ computed in Step 2 of algorithm Tally parses as $((c_1, N_1, c_1), (c_2, N_2, c_2, \omega_2), \ldots, (c_\ell, N_\ell, c_\ell, \omega_\ell))$ and, by completeness, the proofs in that vector pass the checks in Step 2 of algorithm Verify. Thus, checks hold in Step 2 of algorithm Verify.

By Step 3 of algorithm Tally, we have $\text{pdf}$ parses as a vector of length $|B|$, hence, Step 3 of algorithm Verify successfully parses that vector. Since $v$ is initialised as a zero-filled vector of length $nc$ and $v[v]$ is incremented by one for each $i \in \{1, \ldots, |B|\}$ such that $\text{Dec}(sk, c') = 1$, where $c' = \bigotimes_i^m c_1$, $v = \text{Dec}(sk, c_2)$, $B[i] = (c_1, c_2)$, and $n_i$ is a nonce, and since $\text{pdf}[i] = (c', v, \omega, c_\ell)$, where $\omega$ is
an output of $\text{ProveComb}(\langle pk, c', c_1 \rangle, n_i, \kappa)$, $\varsigma_1$ is an output of $\text{ProveDec}(\langle pk, c', 1 \rangle, sk, \kappa)$, and $\varsigma_2$ is an output of $\text{ProveDec}(\langle pk, c_2, v \rangle, sk, \kappa)$, we have for each $v \in \{1, \ldots, n_e\}$ that $\forall v \in \{1, \ldots, [B]\} : \exists c_1, c_2, c', \omega, \varsigma_1, \varsigma_2 : (c_1, c_2) = \text{B}[i] \land (c', v, \omega, \varsigma_1, \varsigma_2) = \text{pdf}[i] \land \text{VerComb}(\langle pk, c', c_1 \rangle, \omega, \kappa) \land \text{VerDec}(\langle pk, c', 1 \rangle, \varsigma_1, \kappa) \land \text{VerDec}(\langle pk, c_2, v \rangle, \varsigma_2, \kappa)$ by completeness, moreover, for each remaining integer $i \in \{1, \ldots, |B|\}$ we have $\text{pdf}[i]$ parses as $(c', m, \omega, \varsigma_1)$, and $\text{VerComb}(\langle pk, c', c_1 \rangle, \omega, \kappa) \land \text{VerDec}(\langle pk, c', m \rangle, \varsigma_1, \kappa) \land m \neq 1$. Thus, checks hold in Step 3 of algorithm $\text{Verify}$.

Since all the above checks succeed, algorithm $\text{Verify}$ outputs 1, concluding our proof. □

### D.3 Proof of Proposition 4 (Individual-Verifiability & Injectivity)

Let $\text{Athena}(\Pi, \mathcal{M}, \Sigma_1, \Sigma_2, \Sigma_3, \Sigma_4, \mathcal{H}) = (\text{Setup}, \text{Register}, \text{Vote}, \text{Tally}, \text{Verify})$. Suppose $\mathcal{A}$ is a probabilistic polynomial-time adversary and $\kappa$ is a security. Further suppose $(pk, nc, \bar{d}_1, v_1, cnt_1, \bar{d}_2, v_2, cnt_2)$ is an output of $\mathcal{A}(\kappa)$, $b_1$ is an output of $\text{Vote}(\bar{d}_1, pk, v_1, cnt_1, nc, \kappa)$, and $b_2$ is an output of $\text{Vote}(\bar{d}_2, pk, v_2, cnt_2, nc, \kappa)$, such that $b_1 \neq \bot$ and $b_2 \neq \bot$. By definition of algorithm $\text{Vote}$, public key $\bar{pk}$ is a vector $(pk, m, \rho)$ such that $\text{VerKey}(\langle \kappa, pk, m \rangle, \rho, \kappa) = 1$ and $v_1, v_2 \in \{1, \ldots, nc\} \subseteq m$. Moreover, $b_1$ and $b_2$ are vectors such that $b_1[2]$ is an output of $\text{Enc}(pk, v_1)$ and $b_2[2]$ is an output of $\text{Enc}(pk, v_2)$. Thus, $b_1 \neq b_2$ by our precondition, with overwhelming probability, therefore, Individual-Verifiability is satisfied. For Injectivity, we further suppose $v_1 \neq v_2$, hence, $b_1 \neq b_2$ by our precondition, which concludes our proof. □

### References


