Zero-Knowledge Proof of Wasta with Applications in Lebanon

Nadim Kobeissi

Department of Computer Science
American University of Beirut

Abstract. In Lebanon, the holder of a "Wasta" (political connection conferring preferential treatment) wishes to convince a verifier that they possess a valid connection to a person of sufficient influence, without revealing the identity of that person. This non-disclosure requirement is essential for two reasons. First, the prover requires deniability: they must be able to later deny that wasta was used, preserving the fiction of meritocracy. Second, the proof must not be replayable: if the verifier learns the identity of the connection, they may exploit this information to obtain wasta for themselves or others, depleting a rivalrous resource. We formalize this as a zero-knowledge proof system and show that the traditional Lebanese wasta protocol, involving oblique references, meaningful pauses, and the phrase "you know who my uncle is", can be improved upon. We proceed by introducing ZK-Wasta, a designated-verifier ring signature protocol that achieves honest-verifier zero-knowledge, computational soundness under the discrete logarithm assumption, and unconditional deniability.

Keywords: Zero-knowledge proofs · Ring signatures · Designated-verifier proofs · Social networks

1 Introduction

The allocation of scarce resources, such as employment, permits, university admissions, parking spots, is a fundamental problem in any society. In theory, such allocation should be based on merit: the most qualified applicant receives the position, the most deserving case receives the permit. In practice, many societies employ alternative allocation mechanisms based on social connections.

In Lebanon, this mechanism is known as *wasta*.[1] A person with wasta possesses a connection to someone of sufficient influence to affect allocation decisions in their favor. The wasta system has been extensively studied by sociologists [4], economists [7], and anthropologists [2,9], but has received surprisingly little attention from computer scientists.

This is unfortunate, because wasta presents a natural cryptographic problem. Consider the following scenario, which occurs thousands of times daily across Lebanon:

[1] *Wasta* is Arabic for *"means"* or *"intermediary"*.

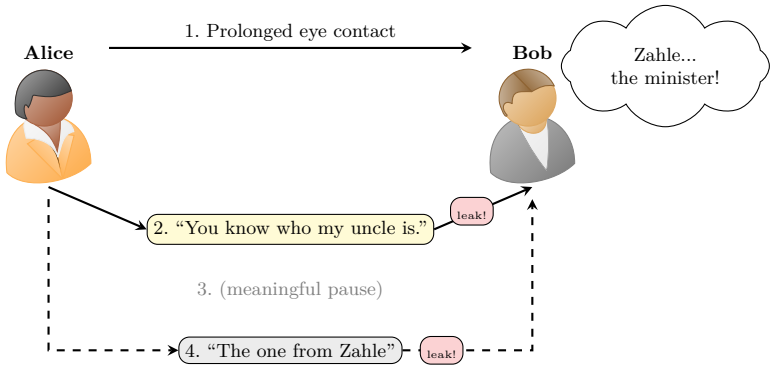

Fig. 1. The traditional wasta protocol (TradWasta). Alice attempts to convince Bob through oblique references and meaningful pauses. Information leaks at multiple points, allowing Bob to infer the connection's identity.

> *Alice wishes to obtain a building permit. She approaches Bob, a government official. Alice claims to have wasta: specifically, a connection to someone important enough that Bob should expedite her application. But Alice cannot simply reveal her connection's identity: doing so would (a) eliminate her deniability, (b) allow Bob to contact the connection directly for his own purposes, and (c) potentially embarrass the connection if the transaction becomes public.*

Alice must therefore prove she has wasta *without revealing who her wasta is*. This is precisely the setting of zero-knowledge proofs [6] and our motivation for exploring the zero-knowledge *proof-of-wasta* problem.

1.1 Our Contributions

We make the following contributions:

1. We formalize the traditional Lebanese wasta protocol and analyze its security properties, identifying several vulnerabilities including susceptibility to replay attacks and inadequate deniability (§2).
2. We introduce the *Wasta Impact Index*, a five-tier classification of influential persons, and propose ZK-Wasta: a designated-verifier ring signature protocol where the verifier's public key is included in the signing ring, achieving signer anonymity and unconditional non-transferability (§4).
3. We provide formal security analysis showing that ZK-Wasta achieves completeness, soundness under the discrete logarithm assumption, signer anonymity, and unconditional deniability (§5).

2 The Traditional Wasta Protocol

Before presenting our improved protocol, we formalize and analyze the existing "folk" protocol that has evolved organically over decades of Lebanese governance. We refer to this protocol as TradWasta. Despite lacking formal specification, TradWasta exhibits remarkable consistency across different regions, sectarian communities, and government departments, suggesting convergent evolution toward a local optimum in the space of informal influence protocols.

2.1 Protocol Specification

The traditional wasta protocol proceeds in four phases, as illustrated in Figure 1.

Phase 1: Channel Establishment. The prover P (Alice) initiates the protocol through prolonged eye contact with the verifier V (Bob). This serves as a carrier-sense mechanism, ensuring V is receptive to wasta claims before bandwidth is allocated to the transaction. The duration of eye contact correlates with the magnitude of the forthcoming request: a parking violation requires approximately 2 seconds, while a building permit may require 5–7 seconds. Premature verbalization before channel establishment is considered a protocol violation and may result in connection termination.[2]

Phase 2: Claim Assertion. Once the channel is established, P transmits the canonical claim phrase. The most common variant is:

"*Btaaref miin khaalii?*" (You know who my uncle is.)

This phrase is notable for several reasons. First, the use of "uncle" (*khaal*, maternal uncle) rather than "father" provides one degree of separation, reducing directness while maintaining credibility. Second, the interrogative form ("do you know?") rather than declarative ("my uncle is...") shifts the burden of identification to V, avoiding explicit claims. Third, the phrase functions correctly regardless of whether P actually has an uncle, whether that uncle is influential, or whether any uncle is relevant to the current transaction.[3]

Regional variants exist. In Tripoli, "*ana ibn Trablos*" (I am a son of Tripoli) may substitute for the uncle formulation, leveraging geographic rather than familial identity. In parts of Mount Lebanon, a reference to one's village of origin serves a similar function, as village identity correlates with feudal family allegiances dating to the Ottoman period.

[2] In networking terms, this is analogous to attempting data transmission before the TCP handshake completes.

[3] The phrase has achieved sufficient cultural saturation that it functions as a pure protocol message, entirely divorced from its literal semantic content.

Phase 3: Temporal Padding. Following the claim assertion, a meaningful pause of 3–5 seconds occurs. During this interval, V is expected to perform a mental lookup in their database of influential persons, attempting to identify P's connection. The pause also serves as a commitment mechanism: P has now publicly claimed wasta, and cannot easily retreat. This phase is critical for the protocol's psychological efficacy but contributes nothing to its cryptographic security.

Phase 4: Oblique Disambiguation. If V's lookup fails to produce a unique match, P may transmit additional identifying information in the form of oblique references. Common patterns include:

- Geographic hints: "The one from Zahle," "You know, from Kesrwan."
- Temporal hints: "From the old days," "Since before the war."[4]
- Professional hints: "The one at the ministry," "From the security services."
- Relational hints: "He's close to the Speaker," "The minister's cousin."

Each hint reduces the anonymity set but increases the probability of successful verification. The prover faces a fundamental tradeoff between soundness (convincing V) and privacy (protecting w's identity).

2.2 Variant Protocols

Several variants of TradWasta have been documented in the field:

The Phone Call (TradWasta-Tel). Rather than in-person assertion, P arranges for w to telephone V directly. This protocol achieves perfect soundness—V hears w's voice and can verify identity—but provides no deniability whatsoever. The phone call creates a witness (the phone record) and often occurs within earshot of others in V's office. TradWasta-Tel is typically reserved for high-stakes transactions where soundness is prioritized over deniability, or where w is sufficiently powerful that deniability is unnecessary.[5]

The Intermediary Chain (TradWasta-Chain). In cases where P does not have direct access to a sufficiently influential w, a chain of intermediaries may be constructed: P contacts w_1, who contacts w_2, who contacts w_n with sufficient influence. This protocol suffers from reliability degradation at each hop and introduces multiple points of information leakage. The chain length is bounded in practice by the patience of participants and the decay of influence over social distance. Empirically, chains longer than three hops rarely succeed.

[4] In Lebanon, "the war" unambiguously refers to the 1975–1990 civil war, providing a temporal anchor that the majority of the population can resolve.

[5] At the highest levels of Lebanese politics, the absence of deniability may itself be the message: "I am powerful enough that I don't need to hide."

The Preemptive Strike (TradWasta-Pre). A sophisticated variant in which w contacts V before P even arrives, eliminating the need for any protocol execution by P. When P arrives at V's office, the transaction is already approved. This protocol is maximally efficient but requires advance coordination and is only feasible when the request is known beforehand. It is commonly used for university admissions, where application deadlines are public and predictable.

2.3 Security Analysis

We identify several security vulnerabilities in TradWasta:

Inadequate Zero-Knowledge. The protocol fundamentally fails to achieve zero-knowledge. Each oblique reference leaks information about w. The phrase "the one from Zahle" reduces the anonymity set to prominent figures from that region—in practice, perhaps three to five individuals. The phrase "from the security services" reduces the set to senior officers of the relevant agencies. After several protocol executions with the same V, intersection attacks become feasible: V accumulates hints across transactions and narrows down w's identity.

Replay Vulnerability. If V learns P's wasta claim, nothing prevents V from replaying this information. V may inform colleagues: "Alice has an uncle in Zahle—you know who." V may even attempt to invoke w's influence for V's own purposes, having learned of the connection. This violates P's privacy, may damage w's reputation, and depletes w's wasta capital—the finite resource of social obligations that w can call upon.

No Cryptographic Binding. The protocol does not bind the wasta claim to any specific transaction. P could use the same vague claim ("you know who my uncle is") for multiple unrelated requests across different government offices, even for purposes w would not approve. There is no mechanism for w to scope or limit the authorization granted to P.

Verification Ambiguity. The protocol's soundness depends entirely on V's ability to assess the credibility of claims based on social knowledge, confidence of delivery, and various paralinguistic cues. This assessment varies widely across verifiers. A gullible V may accept false claims from a confident P with no actual wasta. A skeptical V may reject valid claims from a nervous P with genuine high-grade wasta. There is no ground truth and no appeal mechanism.

Absence of Revocation. Once P has learned how to invoke w's influence (the phrases, the hints, the mannerisms), there is no way for w to revoke this capability. Even if the relationship between P and w deteriorates, P can continue to claim wasta. The only recourse is for w to proactively contact potential verifiers and disavow P—an awkward and incomplete solution.

Table 1. Comparison of traditional wasta signals and their information leakage.

Signal	Entropy Lost (bits)	Deniability
"You know who my uncle is"	2–4	Moderate
Meaningful pause	0–1	High
Geographic hint (region)	4–6	Moderate
Professional hint (sector)	5–8	Low
Name-dropping adjacent figures	8–12	Low
Showing photo with connection	15–20	None
Direct phone call from w	∞	None

2.4 Why TradWasta Persists

Given its manifest security flaws, one might ask why TradWasta remains the dominant protocol. We identify several contributing factors:

Network Effects. TradWasta is universally understood. Any Lebanese adult can execute the protocol without prior coordination or key exchange. Deploying a cryptographic replacement would require coordinating adoption across millions of participants, many of whom have strong incentives to maintain the status quo.

Plausible Deniability Theater. While TradWasta does not achieve cryptographic deniability, it provides a socially acceptable fiction of deniability. All parties can pretend that the transaction occurred on merit: P never explicitly named w, V never explicitly acknowledged the wasta, and w was never officially involved. This theater is sufficient for social purposes even if it would not survive formal scrutiny.

Compatibility with Existing Infrastructure. TradWasta requires no special equipment, no internet connectivity, no software installation. It works in government offices where computers are decades old, in rural areas with unreliable electricity, and in contexts where written records are deliberately avoided.

Resistance to Formalization. The system benefits from its informal nature. Any formal system—including ours—could potentially be audited, regulated, or abolished. The participants in wasta transactions have a collective interest in maintaining the system's opacity.

Nevertheless, we proceed to present a cryptographically sound alternative, in the hope that technological improvements may eventually be adopted as the society evolves—or perhaps as a theoretical contribution to the study of systems that are unlikely to be deployed but are interesting anyway.

3 Preliminaries

3.1 The Lebanese Social Graph

Let $G = (V, E)$ be the directed social graph of Lebanese society, where V is the set of all Lebanese citizens and $(u, v) \in E$ indicates that u "knows" v in a way that permits u to request favors from v.

Definition 1 (Wasta Impact Index). *The Wasta Impact Index is a classification of influential persons into five grades:*

- ***Grade 5:*** *Highest influence (e.g., Speaker of Parliament, major political leaders, heads of security services).*
- ***Grade 4:*** *High influence (e.g., ministers, members of parliament, senior judges).*
- ***Grade 3:*** *Moderate influence (e.g., directors general, municipal presidents, well-connected businessmen).*
- ***Grade 2:*** *Low influence (e.g., mid-level bureaucrats, local party officials).*
- ***Grade 1:*** *Minimal influence (e.g., junior employees with some connections).*

For a given allocation decision d, let $\theta_d \in \{1, \ldots, 5\}$ be the minimum grade required to affect that decision.

For example, obtaining a parking permit might require Grade 1 wasta, while obtaining a government contract might require Grade 4 or 5. Notably, the grade required for a given transaction often exceeds what would be necessary based on the transaction's intrinsic importance, due to grade inflation: as wasta becomes more common, verifiers raise their thresholds to filter signal from noise.

3.2 Ring Signatures

A ring signature scheme [10] allows a signer to produce a signature on behalf of an ad-hoc group (the "ring") such that the signature can be verified as coming from *some* member of the ring, but the actual signer remains anonymous among the ring members.

Definition 2 (Ring Signature). *A ring signature scheme consists of three algorithms:*

- $\mathsf{KeyGen}(1^\lambda) \to (sk, pk)$*: Generate a key pair.*
- $\mathsf{RingSign}(sk_i, m, R) \to \sigma$*: Sign message m using secret key sk_i with respect to ring $R = \{pk_1, \ldots, pk_n\}$ where $pk_i \in R$.*
- $\mathsf{RingVerify}(m, \sigma, R) \to \{0, 1\}$*: Verify signature σ on message m with respect to ring R.*

Ring signatures satisfy:

1. **Correctness:** Honestly generated signatures verify.
2. **Unforgeability:** Without a secret key for some $pk \in R$, producing a valid signature is computationally infeasible.
3. **Signer Anonymity:** Given a valid signature, determining which ring member signed is computationally infeasible.

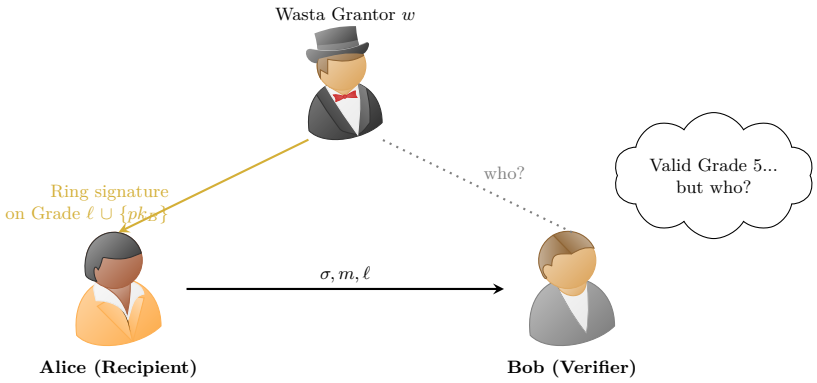

Fig. 2. The ZK-Wasta protocol. A wasta grantor w creates a ring signature over all Grade-ℓ members plus Bob's public key pk_B. Alice forwards this to Bob, who can verify the signature but cannot determine which ring member signed (signer anonymity) and cannot prove to others that the signature is real, since Bob could have created it himself (deniability).

3.3 Schnorr-Based Ring Signatures

We use the ring signature construction based on Schnorr signatures, following the approach of Abe, Ohkubo, and Suzuki [1]. Let $\mathbb{G}$ be a cyclic group of prime order q with generator g, where the discrete logarithm problem is hard.

Definition 3 (Schnorr Ring Signature). *Given ring $R = \{pk_1, \ldots, pk_n\}$ where $pk_j = g^{sk_j}$, signer i with secret key sk_i signs message m as follows:*

1. *Sample random $k \leftarrow \mathbb{Z}_q$ and compute $c_{i+1} = H(R, m, g^k)$.*
2. *For $j = i+1, i+2, \ldots, i-1$ (indices mod n):*
   - *Sample $s_j \leftarrow \mathbb{Z}_q$.*
   - *Compute $c_{j+1} = H(R, m, g^{s_j} \cdot pk_j^{c_j})$.*
3. *Compute $s_i = k - c_i \cdot sk_i \mod q$.*
4. *Output $\sigma = (c_1, s_1, \ldots, s_n)$.*

Verification checks that the ring "closes": starting from c_1, recompute each $c_{j+1} = H(R, m, g^{s_j} \cdot pk_j^{c_j})$ and verify $c_{n+1} = c_1$.

Assumption 1 (Discrete Logarithm) *Given g and g^x for random $x \leftarrow \mathbb{Z}_q$, it is computationally infeasible to compute x.*

4 The ZK-Wasta Protocol

We now present our protocol, which uses ring signatures: by including the verifier's public key in the ring, we achieve designated-verifier properties without additional cryptographic machinery.

4.1 System Setup

Group Parameters. Let $\mathbb{G}$ be a cyclic group of prime order q with generator g, where the discrete logarithm problem is hard (e.g., an elliptic curve group). Let $H : \{0,1\}^* \to \mathbb{Z}_q$ be a collision-resistant hash function, modeled as a random oracle for security proofs.

Wasta Registry. A trusted authority maintains a public registry of influential persons organized by grade. For each grade $\ell \in \{1, \ldots, 5\}$, the registry contains:

$$\mathcal{R}_\ell = \{pk_1^{(\ell)}, pk_2^{(\ell)}, \ldots, pk_{n_\ell}^{(\ell)}\}$$

where $pk_j^{(\ell)} = g^{sk_j^{(\ell)}}$ is the public key of the j-th member of grade ℓ. Each member knows their corresponding secret key.

Verifier Registration. Each potential verifier (e.g., government official) V generates a key pair:

$$sk_V \leftarrow \mathbb{Z}_q, \qquad pk_V = g^{sk_V}$$

Verifiers publish pk_V (e.g., displayed on their desk, included in official correspondence, or registered with the authority).

4.2 Protocol Overview

The protocol involves three parties:

- **Wasta Grantor** w: A member of grade ℓ with key pair (sk_w, pk_w) where $pk_w \in \mathcal{R}_\ell$.
- **Wasta Recipient** Alice: Wishes to prove she has grade-ℓ wasta to Bob.
- **Verifier** Bob: A government official with key pair (sk_B, pk_B).

The wasta grantor w creates a ring signature where the ring consists of:

$$R = \mathcal{R}_\ell \cup \{pk_B\}$$

That is, all grade-ℓ members *plus the verifier's public key.* This achieves two properties simultaneously:

1. **Signer Anonymity:** Bob cannot determine which grade-ℓ member signed.
2. **Non-Transferability:** Bob cannot prove to others that the signature is genuine, because Bob himself is in the ring and could have created the signature.

4.3 Protocol Specification

The complete protocol is specified in Algorithm 1. The message m contains:

- $\mathsf{id}_{\mathsf{Alice}}$: Identifier of the wasta recipient (prevents signature transfer to others).
- τ: Purpose description (e.g., "building permit application").
- ℓ: The wasta grade being claimed.
- t_{exp}: Expiration timestamp (prevents indefinite reuse).

Algorithm 1 ZK-Wasta Protocol

Phase 1: Wasta Request
Alice contacts wasta grantor w with request for help with Bob
Alice provides: Bob's public key pk_B, purpose description τ

Phase 2: Signature Generation (by w)
w retrieves their grade ℓ and the registry $\mathcal{R}_\ell$
w constructs ring: $R \leftarrow \mathcal{R}_\ell \cup \{pk_B\}$
w constructs message: $m \leftarrow (\mathsf{id}_{\mathsf{Alice}}, \tau, \ell, t_{\exp})$
    where $t_{\exp}$ is an expiration timestamp
w computes: $\sigma \leftarrow \mathsf{RingSign}(sk_w, m, R)$
w sends (m, σ, ℓ) to Alice

Phase 3: Wasta Presentation (Alice to Bob)
Alice sends (m, σ, ℓ) to Bob

Phase 4: Verification (by Bob)
Bob retrieves $\mathcal{R}_\ell$ from the public registry
Bob constructs ring: $R \leftarrow \mathcal{R}_\ell \cup \{pk_B\}$
Bob checks: $m.\mathsf{id} = \mathsf{id}_{\mathsf{Alice}}$ {Correct recipient}
Bob checks: $m.t_{\exp} > \mathsf{now}$ {Not expired}
Bob checks: $\ell \geq \theta$ where θ is required grade {Sufficient grade}
Bob checks: $\mathsf{RingVerify}(m, \sigma, R) = 1$ {Valid signature}
Bob accepts iff all checks pass

5 Security Analysis

We now analyze the security properties of the ZK-Wasta protocol.

Theorem 1 (Completeness). *If wasta grantor $w \in \mathcal{R}_\ell$ honestly generates a signature for Alice with grade $\ell \geq \theta$ and valid message m, then Bob accepts with probability 1.*

Proof. By the correctness property of the underlying ring signature scheme (Definition 3), an honestly generated signature satisfies $\mathsf{RingVerify}(m, \sigma, R) = 1$. The message checks (identity, expiration, grade threshold) pass by construction.

Theorem 2 (Soundness). *If no member of $\mathcal{R}_\ell$ has signed message m, and Bob has not signed m himself, then Bob accepts with probability at most $\mathsf{negl}(\lambda)$, assuming the discrete logarithm assumption holds in $\mathbb{G}$ and H is modeled as a random oracle.*

Proof. The ring is $R = \mathcal{R}_\ell \cup \{pk_B\}$. By the unforgeability of Schnorr ring signatures [1], producing a valid signature on m with respect to R requires knowledge of a secret key sk corresponding to some $pk \in R$.

The secret keys in R are:

- $sk_j^{(\ell)}$ for each $pk_j^{(\ell)} \in \mathcal{R}_\ell$ (held by grade-ℓ members).

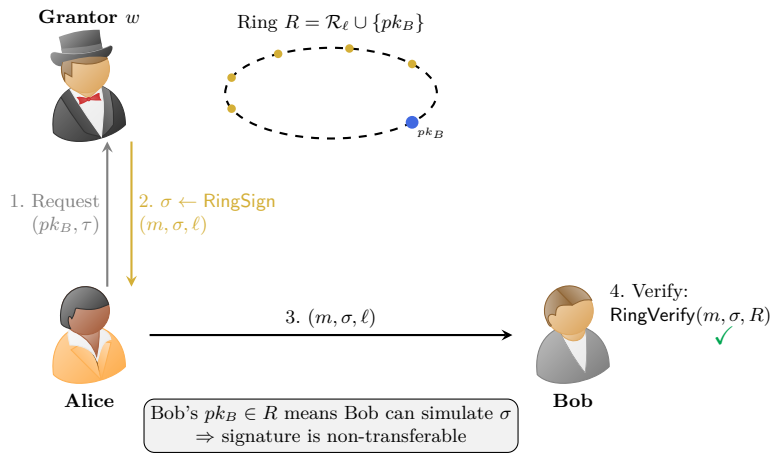

Fig. 3. The ZK-Wasta protocol flow. The wasta grantor w signs using a ring that includes Bob's public key, ensuring Bob cannot prove the signature's authenticity to third parties.

– sk_B (held by Bob).

By assumption, no grade-ℓ member has signed m, so an adversary attempting to forge must either:

1. Extract a secret key from some $pk \in R$, contradicting the discrete logarithm assumption.
2. Forge a ring signature without any secret key, contradicting ring signature unforgeability.

Bob can verify soundness because he knows he did not sign m himself. If he receives a valid signature and knows he didn't create it, then some member of $\mathcal{R}_\ell$ must have signed.

Theorem 3 (Signer Anonymity). *Given a valid signature σ on message m with respect to ring $R = \mathcal{R}_\ell \cup \{pk_B\}$:*

1. *From Bob's perspective (knowing he did not sign), no PPT adversary can determine which member of $\mathcal{R}_\ell$ signed with probability better than $\frac{1}{|\mathcal{R}_\ell|} + \mathsf{negl}(\lambda)$.*
2. *From a third party's perspective, no PPT adversary can determine which member of R signed with probability better than $\frac{1}{|R|} + \mathsf{negl}(\lambda)$.*

Proof. This follows from the signer anonymity property of Schnorr ring signatures. In the random oracle model, the signature components $(c_1, s_1, \ldots, s_n)$ are uniformly distributed regardless of which ring member signed, as shown by Abe et al. [1].

Table 2. Security comparison of wasta protocols.

Protocol	Anonymous	Sound	Deniable	Non-Trans.	Assumptions
TradWasta	Partial	Weak	Moderate	×	Social
TradWasta-Tel	×	✓	×	×	—
TradWasta-Chain	Partial	Weak	Low	×	Social
ZK-Wasta	✓	✓	✓	✓	DL

For part (1): Bob knows $pk_B \in R$ but also knows he did not sign m. Thus Bob can eliminate himself, leaving $\mathcal{R}_\ell$ as his anonymity set.

For part (2): A third party T cannot distinguish whether a member of $\mathcal{R}_\ell$ or Bob himself signed, so the full ring R is the anonymity set.

Theorem 4 (Non-Transferability). *Bob cannot produce evidence that convinces a third party T that a grade-ℓ member signed m. Specifically, Bob can simulate valid-looking signatures indistinguishable from real ones.*

Proof. Since $pk_B \in R$ and Bob knows sk_B, Bob can execute $\mathsf{RingSign}(sk_B, m, R)$ to produce a valid signature on any message m of his choosing.

Given any signature σ (whether from a grade-ℓ member or from Bob himself), a third party T observing (m, σ, R) cannot determine whether:

1. A member of $\mathcal{R}_\ell$ created σ (real wasta), or
2. Bob created σ himself (simulation).

By Theorem 3, signatures are indistinguishable regardless of which ring member signed. Therefore, Bob's simulated signatures are perfectly indistinguishable from real signatures, and T has no evidence that wasta was actually used.

Corollary 1 (Deniability). *After the protocol, Alice can plausibly deny having used wasta.*

Proof. If Bob attempts to prove to others that Alice used wasta, Bob can only present the signature σ. By Theorem 4, Bob could have created σ himself. Therefore, the existence of σ is not evidence that any grade-ℓ member participated, and Alice can deny: "Bob must have fabricated that signature; I obtained my permit on merit."

6 Discussion

6.1 Why Include the Verifier in the Ring?

The idea behind ZK-Wasta is that including pk_B in the ring R simultaneously achieves two goals:

1. **Designated-Verifier Property:** Traditional designated-verifier proofs [8] require OR-proof constructions: "I know a witness for statement S" OR "I know sk_V." Our approach achieves the same effect more elegantly: the ring signature already has OR-structure (the signer could be any ring member), so adding pk_B to the ring naturally makes Bob a potential signer.
2. **No Additional Complexity:** Unlike protocols that layer designated-verifier proofs on top of other primitives, ZK-Wasta uses only ring signatures. The verifier inclusion is a parameter choice, not additional cryptographic machinery.

6.2 Grade Inflation Attacks

Could a Grade-3 member claim to be Grade-5 by signing with the Grade-5 ring? No: they would need a secret key corresponding to some $pk \in \mathcal{R}_5$, which they don't possess. The soundness guarantee (Theorem 2) prevents such inflation.

This represents a significant improvement over TradWasta, where grade inflation is rampant. In the traditional protocol, any sufficiently confident prover can claim Grade-5 wasta; the verifier has no reliable way to distinguish genuine high-grade connections from bluster. Anecdotally, the authors have observed individuals claim connection to "the Speaker himself" when their actual connection was to a municipal clerk who once attended the same wedding as the Speaker's driver.[6] ZK-Wasta eliminates such inflation through cryptographic enforcement.

6.3 Ring Size and Anonymity

The anonymity guarantee depends on $|\mathcal{R}_\ell|$. If Grade 5 contains only 10 members, anonymity is limited. In practice:

- Grade 5 (highest): Perhaps 20–50 individuals.
- Grade 1 (lowest): Could be thousands.

This reflects reality: powerful wasta is rare and thus offers less anonymity, while common wasta is more anonymous but less valuable. The tradeoff is fundamental and cannot be circumvented cryptographically—it is a consequence of the underlying social structure rather than any protocol limitation.

One might consider artificially inflating the Grade-5 registry with dummy public keys to increase anonymity. However, this would require a trusted party to generate and discard the corresponding secret keys, introducing a trusted setup that could be exploited. More practically, any Lebanese citizen examining the Grade-5 registry would immediately notice if it contained 10,000 members rather than the expected 30, undermining the social credibility of the entire system.

[6] The clerk's cousin's neighbor.

6.4 Practical Considerations

Registry Management. The grade registries $\mathcal{R}_\ell$ must be publicly available and regularly updated. Members can be added or removed as influence changes. Since ring signatures only require public keys, registry updates don't affect previously issued signatures (though verifiers should use the registry current at signature time).

The question of *who maintains the registry* is delicate. In principle, this could be a government function, but asking the Lebanese government to maintain an accurate, publicly auditable list of its most influential members may be optimistic. Alternative approaches include decentralized consensus mechanisms, though these introduce their own complications. We leave the registry governance problem as an exercise for future work, noting only that it is likely the least tractable aspect of the system.

Key Distribution. Each grade member must securely hold their secret key. Standard key management practices apply: hardware security modules for high-grade members, secure backup procedures, key rotation policies.

The key distribution problem is non-trivial in the Lebanese context. Grade-5 members are typically of advanced age and may have limited familiarity with cryptographic key management.[7] A realistic deployment would require user-friendly key custody solutions, perhaps integrated with existing banking infrastructure—though this assumes the banking infrastructure is itself functional, which has not been reliably true since 2019.

Offline Operation. Once Alice receives the signature from w, she can present it to Bob without further interaction with w. This matches real-world wasta dynamics where the influential person "makes a call" once and the recipient handles the rest.

The offline property is particularly valuable in Lebanon, where internet connectivity and electrical power are intermittent. A wasta signature stored on a mobile device remains valid even during the 20+ hours per day when grid electricity is unavailable. The signature verification requires only local computation, which can be performed on battery power. In this sense, ZK-Wasta is better adapted to Lebanese infrastructure than many modern cryptographic protocols that assume persistent connectivity.

Signature Storage and Presentation. In practice, Alice would store her wasta signature on a mobile device and present it to Bob via QR code, NFC, or similar mechanism. Bob's verification device would need access to the current registry $\mathcal{R}_\ell$, which could be cached locally and updated periodically. The entire verification process requires only a few milliseconds of computation, making it practical even on low-end smartphones.

[7] Though they have extensive experience with other forms of key management, such as which keys open which ministerial offices.

6.5 Limitations

Real-Time Witnessing. If a third party T observes the interaction between Alice and Bob in real-time (e.g., watches Alice hand Bob the signature), T gains evidence that Alice initiated the interaction. However, T still cannot verify the signature's authenticity without being in the ring.

Collusion. If Bob colludes with a third party T by sharing sk_B, then T can also verify signatures designated for Bob. This is inherent to any designated-verifier scheme. In the Lebanese context, collusion between government officials is not merely a theoretical concern but a documented empirical phenomenon. The protocol cannot prevent collusion; it can only ensure that colluding parties cannot cryptographically prove the wasta to non-colluding outsiders.

Grantor Privacy. The protocol does not hide that *some* grade-ℓ wasta was used; it only hides *who* provided it. In some contexts, even revealing the grade might be sensitive. A variant protocol could hide the grade by having the grantor sign with respect to *all* registries $\mathcal{R}_1 \cup \cdots \cup \mathcal{R}_5 \cup \{pk_B\}$, though this increases signature size and verification time proportionally.

Wasta Cardinality. The protocol proves possession of *at least one* connection of sufficient grade, but does not prove the *number* of such connections. A prover with five Grade-4 connections appears identical to one with a single Grade-4 connection. In traditional wasta dynamics, the number of connections matters: someone with many high-grade connections is more socially powerful than someone with just one. Extending ZK-Wasta to prove cardinality bounds while preserving anonymity is an interesting open problem.

Temporal Dynamics. Wasta is not static: influence waxes and wanes with political fortunes, electoral cycles, and occasional dramatic realignments.[8] A signature issued when w was Grade-5 remains valid even if w is subsequently demoted to Grade-3 (or imprisoned, or exiled, or appointed to a different ministry). The expiration timestamp t_{exp} partially mitigates this, but short expiration times require frequent re-signing, which may strain the grantor relationship.

Social Engineering. The protocol assumes that Alice legitimately obtained the signature from w. If Alice social-engineers w into signing ("Uncle, just sign this for my university project"), the protocol provides no recourse. Similarly, if w's secret key is compromised through phishing, malware, or coercion, the attacker can issue arbitrary wasta signatures. These attacks target the human layer rather than the cryptographic layer, and are arguably the most realistic threat vectors in practice.

[8] Lebanese political dynamics are beyond the scope of this paper, though we note that any formal model would require frequent updates.

6.6 Post-Quantum Zero-Knowledge Proof of Wasta

The ZK-Wasta protocol relies on the discrete logarithm assumption in the group $\mathbb{G}$, which is known to be vulnerable to quantum attack via Shor's algorithm [11]. A sufficiently powerful quantum computer could extract secret keys from public keys, enabling universal wasta forgery. This raises the question: should Lebanon be concerned about quantum threats to its wasta infrastructure?

We offer several observations:

Timeline Considerations. Current estimates suggest large-scale fault-tolerant quantum computers capable of breaking 256-bit elliptic curve cryptography remain 10–20 years away. Lebanese infrastructure planning rarely exceeds a 6-month horizon.[9] By the time quantum computers pose a practical threat, ZK-Wasta will likely have been deprecated, the Lebanese political system will have undergone multiple restructurings, and the authors will have moved on to other research problems.

Quantum Computer Availability. Even when quantum computers become available, access will initially be limited to nation-states and large corporations. The question of whether Lebanon will possess a quantum computer is distinct from the question of whether Lebanese citizens will have access to one. Current projections suggest Lebanon is more likely to achieve reliable 24-hour electricity than to acquire a quantum computer in the near term.

Selective Forgery. A quantum-capable adversary could forge wasta signatures, but this capability would be overkill for the Lebanese context. An adversary with access to a billion-dollar quantum computer almost certainly has more direct means of influence than forging cryptographic wasta proofs. The threat model assumes rational adversaries; a rational adversary with quantum capabilities would not waste them on building permits.

Post-Quantum Alternatives. Should post-quantum security be required, the ZK-Wasta construction could be instantiated with lattice-based ring signatures [5] or hash-based constructions. These alternatives offer security against quantum adversaries at the cost of larger signatures and increased computational requirements. Given Lebanese bandwidth and computational constraints, this tradeoff may not be favorable. We leave PQ-Wasta as future work, to be undertaken if and when quantum computers and Lebanese electrical grids both achieve sufficient reliability.

6.7 Comparison to Bribery

A natural question is how ZK-Wasta compares to direct bribery as a mechanism for favorable treatment. Both mechanisms circumvent merit-based allocation, but they differ in important respects:

[9] The national electricity plan, for instance, has been "18 months from completion" since approximately 1994.

- **Resource Type:** Bribery consumes financial capital; wasta consumes social capital. The two resources have different distributions across the population and different replenishment dynamics.
- **Deniability:** Cash transactions leave physical evidence (marked bills, bank transfers, lifestyle inconsistencies). ZK-Wasta provides cryptographic deniability, which is strictly stronger.
- **Scalability:** Bribery scales linearly with the bribe amount; wasta scales with the logarithm of social distance to influential persons. For well-connected individuals, wasta is more efficient; for poorly-connected individuals, bribery may be the only option.
- **Legal Status:** Bribery is illegal in Lebanon (at least nominally). Wasta occupies a gray zone: while not explicitly illegal, it violates the spirit of merit-based allocation that laws nominally require. ZK-Wasta does not change the legal status of wasta; it merely makes the practice more cryptographically sophisticated.

We take no position on the relative morality of these mechanisms. The purpose of this paper is to formalize and improve the cryptographic properties of wasta, not to endorse its use. Whether society would be better served by eliminating wasta entirely, replacing it with transparent bribery, or maintaining the status quo is a question for ethicists, economists, and the Lebanese electorate.

6.8 Deployment Considerations

Any realistic deployment of ZK-Wasta would face significant adoption challenges:

Incentive Alignment. The current beneficiaries of TradWasta—high-grade individuals and their networks—have limited incentive to adopt a system that formalizes and potentially constrains their influence. Meanwhile, those without wasta have no standing to propose changes to a system that excludes them. This creates a collective action problem with no obvious solution.

Cultural Resistance. TradWasta is deeply embedded in Lebanese social practice. The meaningful pause, the oblique reference, the knowing glance—these are not merely protocol steps but cultural rituals with social significance beyond their informational content. A purely cryptographic replacement may be rejected not because it is less functional but because it is less *Lebanese*.

Technical Literacy. Successful deployment requires that grantors, recipients, and verifiers all understand and trust the cryptographic guarantees. Given that many participants in the current system are unfamiliar with smartphones, let alone elliptic curve cryptography, widespread adoption would require extensive education and simplified interfaces.

Regulatory Status. It is unclear how Lebanese regulators would view ZK-Wasta. The system could be characterized as an anti-corruption tool (by making wasta transactions auditable at the grade level), a corruption-enabling tool (by providing deniability), or simply a curiosity with no practical impact. The authors have not consulted with Lebanese legal authorities and have no plans to do so.

6.9 Related Work

Ring signatures were introduced by Rivest, Shamir, and Tauman [10]. The Schnorr-based construction we use follows Abe, Ohkubo, and Suzuki [1].

Designated-verifier signatures were introduced by Jakobsson, Sako, and Impagliazzo [8]. Our approach of including the verifier in the ring achieves similar properties through a different mechanism. Group signatures [3] address related problems but with different trust assumptions and properties.

To our knowledge, this is the first academic treatment of wasta from a cryptographic perspective. The sociology literature contains extensive discussion of wasta dynamics [4,7,2,9], but does not address the zero-knowledge aspects. We hope this paper bridges the gap between these literatures, though we acknowledge that the bridge may be of limited practical utility.

7 Conclusion

We have presented ZK-Wasta, a designated-verifier ring signature protocol for proving possession of social connections without revealing their identity. By including the verifier's public key in the signing ring, we achieve:

- **Signer anonymity** among grade members.
- **Soundness** under the discrete logarithm assumption.
- **Non-transferability** since the verifier can simulate signatures.
- **Simplicity** using only standard ring signatures.

The Wasta Impact Index provides a natural hierarchy of influence levels, and the protocol cleanly handles threshold requirements: Bob accepts if and only if the claimed grade meets his threshold and the signature verifies.

While developed in the context of Lebanese wasta, the protocol applies broadly to any setting where proving social connections without revealing them is valuable: professional networking, exclusive access systems, and informal recommendation systems. We hope this work encourages further study of informal social protocols through the lens of cryptography—and perhaps, one day, the deployment of systems that make corruption slightly less prevalent.

References

1. Abe, M., Ohkubo, M., Suzuki, K.: 1-out-of-n signatures from a variety of keys. In: International conference on the theory and application of cryptology and information security. pp. 415–432. Springer (2002)

2. Bassil, R.B.: Corruption and wasta in Lebanon. Ph.D. thesis (2020)
3. Chaum, D., van Heyst, E.: Group signatures. In: Advances in Cryptology—EUROCRYPT '91. pp. 257–265 (1991)
4. Egan, M., Tabar, P.: Bourdieu in Beirut: Wasta, the state and social reproduction in Lebanon. Middle East Critique **25**(3), 249–270 (2016)
5. Esgin, M.F., Steinfeld, R., Liu, J.K., Liu, D.: Lattice-based zero-knowledge proofs: new techniques for shorter and faster constructions and applications. In: Annual International Cryptology Conference. pp. 115–146. Springer (2019)
6. Goldwasser, S., Micali, S., Rackoff, C.: The knowledge complexity of interactive proof-systems. In: Providing sound foundations for cryptography: On the work of Shafi Goldwasser and Silvio Micali, pp. 203–225 (2019)
7. Helal, R.Y., Ali, S., Strecker, S., Weir, D.: Navigating wasta in business practices in Lebanon. Thunderbird International Business Review **65**(6), 639–648 (2023)
8. Jakobsson, M., Sako, K., Impagliazzo, R.: Designated verifier proofs and their applications. In: International Conference on the Theory and Applications of Cryptographic Techniques. pp. 143–154. Springer (1996)
9. Makhoul, J., Harrison, L.: Intercessory wasta and village development in Lebanon. Arab studies quarterly pp. 25–41 (2004)
10. Rivest, R.L., Shamir, A., Tauman, Y.: How to leak a secret. In: International conference on the theory and application of cryptology and information security. pp. 552–565. Springer (2001)
11. Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th annual symposium on foundations of computer science. pp. 124–134. Ieee (1994)