QuMixnet: A Quantum-Safe Mixnet Protocol

S. Mohamamd Dibaji, Taraneh Eghlidos, Hossein Pilaram

Sharif University of Technology

diba.m222@gmail.com

Outline

- Introduction & Motivation
- Related Work
- Our Contributions
  - 5-Node Example
  - Protocol Overview
  - Key Components & Primitives
  - Workflow
  - Security
- Conclusion

Outline

- Introduction & Motivation
- Related Work
- Our Contributions
  - 5-Node Example
  - Protocol Overview
  - Key Components & Primitives
  - Workflow
  - Security
- Conclusion

Introduction

- **Mixnets**: Cryptographic protocols for anonymous communication [Chaum, 1981]
  - Route messages through "mix nodes" to shuffle & obscure sender-receiver links
  - Applications: anonymous messaging, E-voting, …
- **Challenges**:
  - Vulnerable to traffic analysis & powerful adversaries
  - Quantum threats: Shor's algorithm breaks RSA/ECC [Shor, 1994]
- **Need**: Quantum-resistant mixnets for long-term security & privacy

Outline

- ❖ Introduction & Motivation
- ❖ Related Work
- ❖ Our Contributions
  - ➢ 5-Node Example
  - ➢ Protocol Overview
  - ➢ Key Components & Primitives
  - ➢ Workflow
  - ➢ Security
- ❖ Conclusion

Related Work

- **Classical Mixnets**:
  - Mixmaster
  - Loopix
  - Nym: plans PQ upgrade
- **PQ Mixnets**:
  - Katzenpost: Hybrid Kyber + Sphinx
  - xx.network (cMix): PQ in precomputation
  - Voting-specific: Lattice-based verifiable mixnets (focus on shuffles/ZK proofs)

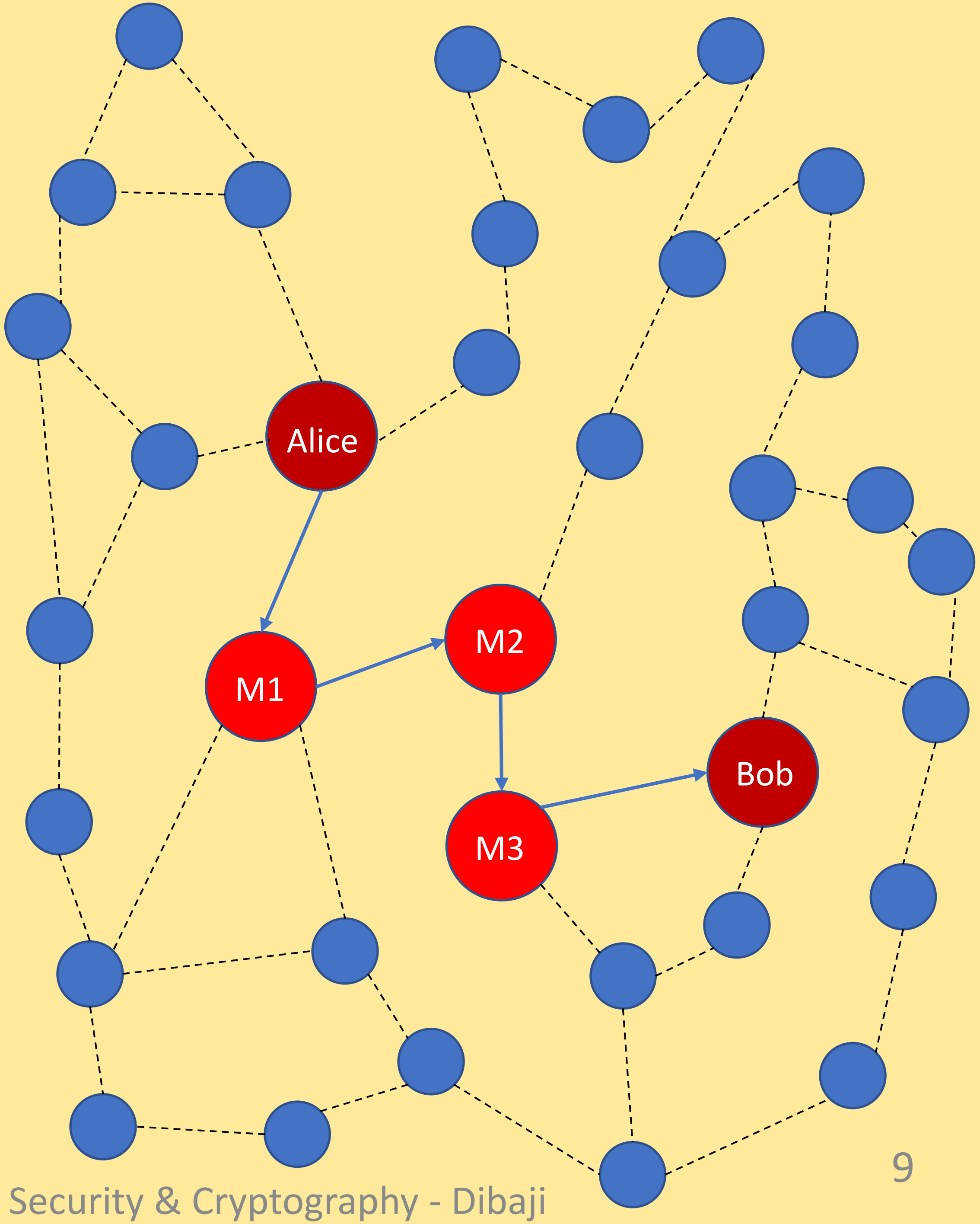
Outline

- ❖ Introduction & Motivation
- ❖ Related Work
- ❖ Our Contributions
  - ➢ 5-Node Example
  - ➢ Protocol Overview
  - ➢ Key Components & Primitives
  - ➢ Workflow
  - ➢ Security
- ❖ Conclusion

Our Contributions

- **QuMixnet**: Fully post-quantum mixnet protocol
  - **PQ Primitives**: CRYSTALS-Dilithium (signatures), CRYSTALS-Kyber (KEM) + AES-GCM
  - **P2P Architecture**: Every node = sender/receiver/mix (enhances scalability/anonymity)
  - **Sender-Determined Onion Routing**: Only sender knows full path
  - **Traffic Obfuscation**: Fixed-size padding, dummies, batch shuffling, …
- **Advantages**:
  - Future-proof vs. quantum attacks
  - Better scalability/flexibility than non-P2P (e.g., Loopix/Nym)
  - Stronger obfuscation than voting mixnets

5-Node Example



: Other nodes

: Other connections

Protocol Overview

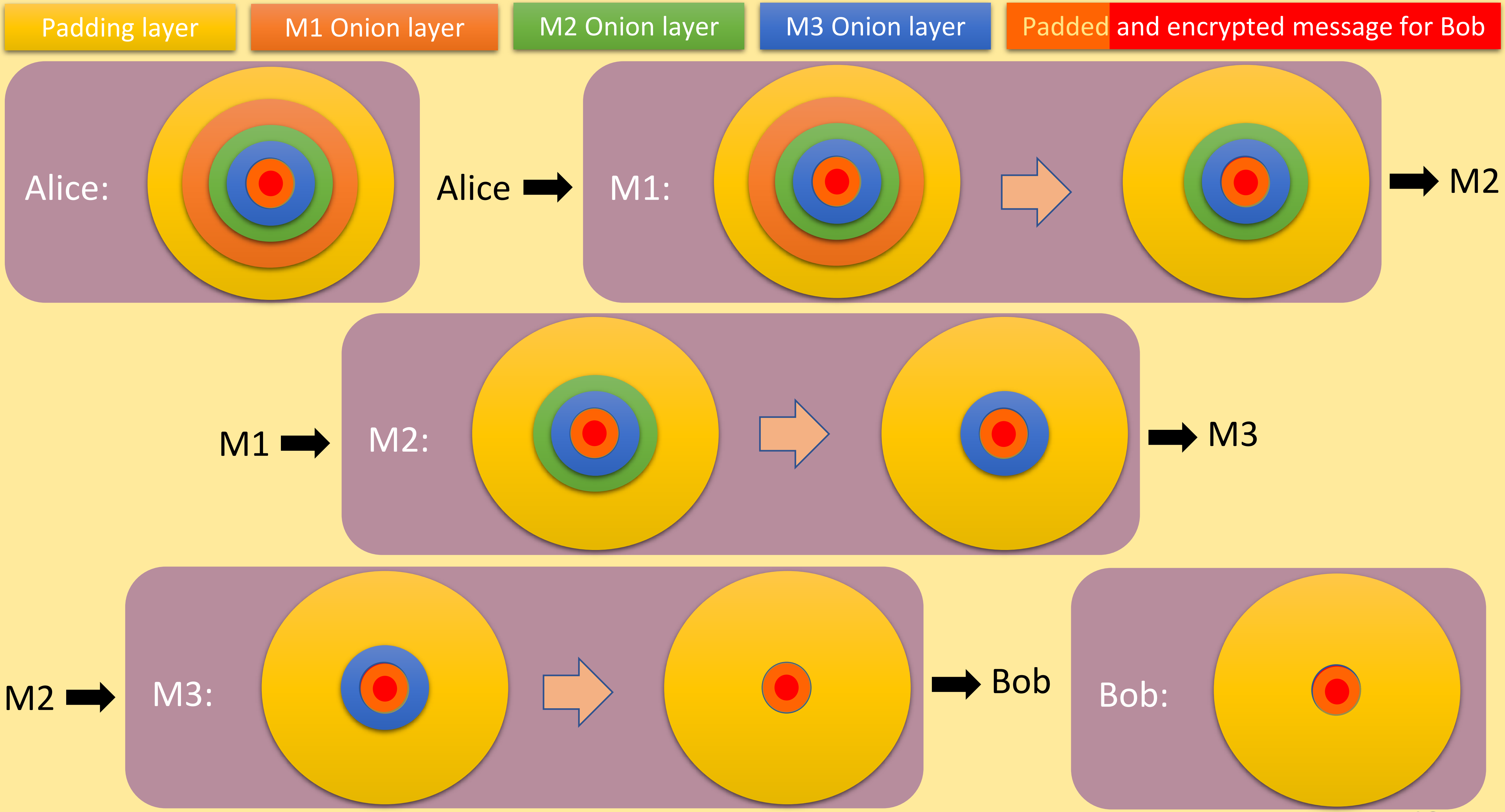
- **Goals**:
  - Secure secret transmission: Confidentiality, Integrity, Anonymity
  - Communication Anonymity: Sender/receiver know each other, but communication hidden from others
- **Key Features**:
  - Onion routing - layered encryption
  - P2P: Obscures roles, resists traffic analysis
  - Obfuscation: Padding to MSG_SIZE (a fixed size), dummies, batching, …

Key Components & Primitives

- **CRYSTALS-Dilithium** [Ducas et al. 2018]: Lattice-based signature (sEUF-CMA secure)
  - Signs (secret + IDs + timestamp) for authenticity/integrity
- **CRYSTALS-Kyber** [Bos et al. 2018]: Lattice-based KEM (IND-CCA2 secure)
  - Encapsulates symmetric keys for AES-GCM encryption (efficient for large payloads)
- **Onion Routing**: layered encryption; each node decrypts one layer (next hop + payload)

Architecture - P2P Mixnet & Routing

- **P2P Design**: Every node can send/receive/mix
  - No fixed roles: Traffic indistinguishable; resists endpoint correlation
- **Sender-Determined Routing**:
  - Sender selects full path (trust/reputation via DHT + gossip)
  - Last mix knows receiver address but NOT it's the end (via padding strategy)
- **Enhanced Anonymity**: Layered encryption+ obfuscation hide endpoints from eavesdroppers


Padding layer
M1 Onion layer
M2 Onion layer
M3 Onion layer
Padded and encrypted message for Bob
Alice:
Alice
M1:
M2
M1
M2:
M3
M2
M3:
Bob
Bob:

Security & Practical Considerations

- **Confidentiality/Integrity**: End-to-end via Kyber + Dilithium
- **Anti-Collusion/Traffic Analysis**:
  - Low probability of collusion: $f^n \ll 1$ (f = adversary fraction)
  - Padding: All msgs = MSG_SIZE + padding strategy
  - Dummies: Injected to random nodes
  - Batching/Shuffling: Disrupts timing
  - Timestamps: Prevent replays
- **Scalability**: Load balancing; efficient PQ impls needed
  - Withstands global visibility + partial node control

Security Games & Analysis

- **Games**:
  - Game 1: Sender Anonymity
  - Game 2: Receiver Anonymity
  - Game 3: Communication Anonymity (guess S/R)
  - Game 4: Confidentiality
  - Game 5: Integrity
- **Adversary's Advantages (Negligible)**:
  - Adv(Games 1, 2 and 3) ≤ $\frac{1}{2} f^{n} + \varepsilon_{Kyber} + \varepsilon_{sym}$
  - Adv(Game 4) ≤ $\varepsilon_{Kyber} + \varepsilon_{sym}$
  - Adv(Game 5) ≤ ε_{Dil}

Outline

- ❖ Introduction & Motivation
- ❖ Related Work
- ❖ Our Contributions
  - ➢ 5-Node Example
  - ➢ Protocol Overview
  - ➢ Key Components & Primitives
  - ➢ Workflow
  - ➢ Security
- ❖ Conclusion

Conclusion

- **Key Takeaways**:
  - QuMixnet:
    - Scalable PQ mixnet with P2P + robust obfuscation
    - Resists quantum adversaries; strong anonymity/confidentiality
    - Advances over classical/partial-PQ systems

References

[1] David L Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Com munications of the ACM, 24(2):84–90, 1981.

[2] Peter W Shor. Algorithms for quantum compu tation: discrete logarithms and factoring. In Pro ceedings 35th annual symposium on foundations of computer science, pages 124–134. IEEE, 1994.

[3] Léo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim 12 Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé. Crystals-dilithium: A lattice based digital signature scheme. IACR TCHES, 2018(1):238–268, 2018.

[4] Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Le point, Vadim Lyubashevsky, John M Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. Crystals-kyber: a cca-secure module lattice-based kem. In 2018 IEEE European Sym posium on Security and Privacy (EuroS&P), pages 353–367. IEEE, 2018.

Q&A

Any Questions?

Thank You