msgX: a national digital sovereignty matter

Vinícius Lagrota[1], **Gilvan Maia**[2], **Paulo Rego**[2], **Rodrigo Pacheco**[1], **José Antônio Macêdo**[2], **Marcos Dantas**[2]

[1] Research and Development Center for Communication Security (CEPESC) Brasília, DF – Brazil.

[2]Federal University of Ceará (UFC) – Fortaleza, CE – Brazil

1. Introduction

End-to-end encryption (E2EE) built on Extended Triple Diffie-Hellman (X3DH) and the Double Ratchet has become the baseline for secure messaging [Kret and Schmidt 2023]. However, the harvest now, decrypt later (HNDL) threat model motivates hybrid designs that combine classical elliptic curve Diffie–Hellman (ECDH) with post-quantum Key Encapsulation Mechanisms (KEMs) during session setup and rekeying. In governmental contexts, where compromises impact national sovereignty, the underlying protocol must also support sovereign cryptography and transparent auditing over open infrastructure (Matrix) [Matrix.org 2024]. msgX addresses these demands by combining a dual-branch design (standard and government) with post-quantum hardening and pragmatic interoperability.

2. Aims and Scope

This work targets a drop-in replacement for Olm that:

- Strengthens long-term confidentiality and post-compromise security (PCS) against HNDL adversaries via hybrid key establishment and periodic root-key renewal;
- Preserves interoperability across federated Matrix networks by maintaining a standard/NIST branch alongside a government-developed branch;
- Keeps classical digital signatures for practicality today (since signatures are not susceptible to HNDL), focusing post-quantum effort on key agreement and message confidentiality;
- Remains backward compatible with existing Matrix clients by allowing the sovereign and post-quantum (PQ) features to be disabled when needed.

3. The msgX Protocol

Design Overview

msgX is composed of two core building blocks:

1. **msgX-PQXDH**[1] for asynchronous key establishment, combining classical ECDH and a post-quantum KEM into a single session secret via Hash-based Key Derivation Function (HKDF).
2. **msgX-ratchet** for message protection and rekeying, derived from the Double Ratchet but extended to (i) run in dual branches (standard and government) and (ii) support parameterizable root-key renewal to bound long-term exposure.

[1]PQXDH stands for Post-Quantum Extended Diffie-Hellman

Both branches operate in parallel during the entire session. Secrets from each branch are combined to produce message keys; confidentiality is preserved as long as at least one branch remains secure. The standard branch ensures compatibility with non-government Matrix clients, while the government branch enables sovereign cryptography and cryptographic agility.

Interplay with msgGX (Group Messaging)

Matrix treats even 1:1 chats as rooms; scalable groups therefore rely on a Megolm-style construction. We pair msgX with *msgGX* (an adapted Megolm) as follows:

1. **Initialization:** devices publish identity/ephemeral keys (both branches) for asynchronous setup.
2. **Key agreement and Ratchet:** msgX-PQXDH derives initial root/chain keys in both branches; msgX then encrypts and delivers the msgGX initial setup to the peer.
3. **Message Exchange:** room messages use msgGX (double-layer symmetric encryption).
4. **Session Renewal:** after a message/time threshold, msgX advances its ratchet (optionally injecting fresh PQ entropy) and securely transmits a new msgGX setup to all participants.

Parameterizable Root-Key Renewal

To achieve tunable "session healing", msgX periodically advances the root key. At configurable intervals—e.g., every N msgGX renewals—each branch optionally performs a KEM refresh (decapsulation/encapsulation depending on direction), then mixes the result with the latest ECDH output into HKDF to derive fresh root/chain keys. Lower N yields faster recovery from compromise at the cost of added bandwidth/state churn.

Backward Compatibility

All sovereign/PQ operations are optional. Disabling them degenerates msgX to Olm-like behavior, preserving interoperability with existing Matrix clients. This allows gradual migration while keeping the standard branch as a compatibility anchor.

4. Conclusion

msgX provides a dual-branch, post-quantum-ready E2EE substrate for Matrix that balances digital sovereignty, interoperability, and practical migration. By coupling a Post-Quantum Extended Diffie-Hellman (PQXDH)-style setup with a ratchet that includes parameterizable root-key renewal—and by using msgX to securely distribute fresh msgGX setups—the design limits long-term exposure under HNDL while remaining compatible with today's Matrix deployments.

References

[Kret and Schmidt 2023] Kret, E. and Schmidt, R. (2023). The PQXDH key agreement protocol.

[Matrix.org 2024] Matrix.org (2024). Matrix specification. `https://spec.matrix.org/`.