Entrechat :
Un système de messagerie pair-à-pair strictement synchrone

Melik Lemariey
M.Sc. Systèmes de Télécommunications
Chercheur indépendant
melik.e.lemariey@proton.me

2025

Abstract

Ce document présente Entrechat v1, un système de messagerie pair-à-pair strictement synchrone, conçu à partir de contraintes architecturales délibérément restrictives.

Entrechat exclut serveurs, comptes, annuaires, mécanismes de livraison asynchrone, stockage de messages et toute infrastructure persistante. Ces exclusions ne relèvent pas de limitations accidentelles, mais de choix de conception explicitement assumés.

Le système ne revendique aucune propriété de sécurité universelle. Les garanties décrites sont contextuelles, dépendantes d'hypothèses clairement énoncées et limitées à un périmètre d'usage défini. Entrechat privilégie la clarté architecturale et la maîtrise de l'exposition opérationnelle plutôt que l'exhaustivité fonctionnelle.

Mots-clés : messagerie pair-à-pair, synchronie stricte, architecture de sécurité, communication synchrone, Tor, chiffrement de bout en bout, exposition opérationnelle

1 Périmètre du système

Entrechat est un système de messagerie mobile conçu pour des échanges intentionnels et explicites entre pairs préalablement identifiés.

Le système est défini par les contraintes structurelles suivantes :

- communication strictement pair-à-pair,
- échanges strictement synchrones,
- absence de serveurs ou de backend opéré,
- absence de comptes, d'annuaires ou de mécanismes de découverte,
- absence de livraison asynchrone et de stockage de messages,
- absence de réplication multi-terminaux.

Le transport réseau repose exclusivement sur l'utilisation du réseau Tor [4]. Les identités sont cryptographiques, générées localement et gérées localement par les utilisateurs.

Ce document décrit Entrechat v1 tel qu'implémenté. Aucune évolution future ni extension fonctionnelle n'est implicite.

2 Finalité et cadre d'usage

Entrechat répond à un besoin volontairement circonscrit : permettre une communication directe et strictement synchrone entre pairs mutuellement disponibles, sans dépendre d'un service opéré ni d'une infrastructure persistante.

Le système a été initialement conçu à partir d'un besoin du développeur, considéré comme un cas particulier révélateur de contraintes rencontrées dans des contextes d'échange ponctuels, à forte exigence de maîtrise de l'exposition.

Entrechat n'est pas conçu comme une messagerie généraliste. Il ne vise ni à remplacer des plateformes existantes, ni à couvrir l'ensemble des usages contemporains. Il explore un espace de conception spécifique dans lequel :

- la communication n'a lieu que lorsque les deux parties sont présentes,
- les sessions possèdent un cycle de vie explicitement borné,
- aucune activité réseau implicite n'est générée,
- la complexité architecturale est volontairement limitée.

La synchronie est considérée comme une propriété positive. Elle rend explicites les contraintes de disponibilité et évite l'introduction de mécanismes implicites, tels que les files d'attente, la livraison différée ou la persistance de métadonnées hors session.

Entrechat ne cherche ni à se rendre invisible, ni à assurer une protection en cas de compromission du terminal. Ces dimensions sont explicitement considérées comme hors périmètre.

3 Position épistémologique et hypothèses d'usage

Les propriétés de sécurité d'un système logiciel sont par nature contextuelles et dépendantes des hypothèses retenues. Un modèle de menace constitue un outil méthodologique destiné à structurer le raisonnement, et non une garantie indépendante du contexte d'usage ou de l'environnement opérationnel.

L'architecture d'Entrechat n'est pas fondée sur l'hypothèse que le logiciel puisse se substituer à l'enquête de terrain, à l'observation humaine ou à l'analyse du contexte réel d'utilisation. Les facteurs sociaux, organisationnels et opérationnels demeurent déterminants dans l'évaluation effective des situations de communication.

Le système s'inscrit dans des cadres juridiques, institutionnels et opérationnels existants propres aux technologies de communication. Il ne vise ni à les nier, ni à s'y opposer, ni à formuler une réponse globale à ces cadres.

Le rôle architectural attribué au logiciel a été limité. Entrechat se restreint aux fonctions de communication, d'établissement de session et de protection cryptographique, sans intégrer de mécanismes de qualification, de régulation ou de décision automatisée sur les usages.

Ce choix vise à maintenir une séparation claire entre la responsabilité du système et celle de l'utilisateur, à préserver la cohérence d'un fonctionnement strictement synchrone, et à réduire la surface d'exposition associée à l'augmentation de la complexité fonctionnelle.

L'omission architecturale est ainsi traitée comme un choix de conception. L'absence de certaines fonctionnalités n'est pas présentée comme une carence, mais comme un moyen de limiter l'exposition opérationnelle, de réduire les états implicites et de restreindre l'espace de raisonnement nécessaire à l'analyse du système.

4 Modèle d'exposition opérationnelle

Le système est conçu pour fonctionner dans des environnements où des capacités d'observation, de mesure, de retard ou de perturbation des communications réseau peuvent être présentes.

Aucune hypothèse n'est formulée quant :

- à l'identité des entités impliquées dans ces capacités,
- à leur échelle ou à leur portée,
- à leurs intentions ou objectifs.

Sont explicitement considérés hors périmètre :

- la compromission complète du terminal utilisateur,
- l'accès coercitif au dispositif ou à son environnement d'exécution,
- l'exfiltration de données résultant d'actions côté utilisateur.

La réduction de l'exposition opérationnelle repose principalement sur des omissions architecturales explicites : absence de serveurs, absence de stockage persistant, absence de signalisation asynchrone, et absence d'activité réseau en arrière-plan en dehors des sessions initiées par l'utilisateur.

Exemple de session typique (illustratif)

Une session Entrechat débute lorsque deux pairs préalablement identifiés initient explicitement une communication simultanée. La session est établie, les messages sont échangés en temps réel, puis la communication est terminée par l'un ou l'autre des participants.

À l'issue de la session :

- aucun message n'est stocké côté infrastructure,
- aucun état applicatif persistant n'est conservé,
- aucune activité réseau ne subsiste hors action utilisateur.

Cet exemple est fourni à titre illustratif et ne constitue ni un modèle normatif ni une garantie opérationnelle.

5 Modèle cryptographique

Entrechat repose sur un schéma cryptographique hybride conventionnel, adapté à un modèle de communication strictement synchrone et pair-à-pair.

- La cryptographie asymétrique est utilisée pour l'établissement de session [1, 2, 3].
- Le contenu des messages est protégé par un chiffrement symétrique authentifié, limité à la durée de la session active.

Les clés de session sont générées à la demande et strictement bornées aux sessions en cours. Aucune confidentialité persistante inter-session ni propriété de confidentialité à long terme n'est revendiquée.

L'architecture exclut :

- toute infrastructure de pré-clés,

- toute distribution asynchrone de clés,
- tout stockage différé de messages,
- tout état cryptographique persistant hors session active.

Ces exclusions visent à éviter des classes d'exposition documentées dans les systèmes de messagerie asynchrones, notamment celles liées à la gestion de clés différée et à l'accumulation d'états persistants [7].

6 Principes architecturaux

Les propriétés observées du système résultent de contraintes structurelles explicites, plutôt que d'une sophistication protocolaire ou fonctionnelle.

Les principes architecturaux retenus sont les suivants :

- initiation explicite des communications par l'utilisateur,
- cycles de vie de session déterministes et bornés,
- absence d'activité réseau implicite ou autonome,
- absence de connectivité en arrière-plan hors session active,
- génération strictement limitée de métadonnées.

En dehors des sessions explicitement initiées, l'application ne génère aucune communication réseau.

7 Ce que la synchronie rend possible

Le choix d'un modèle strictement synchrone ne constitue pas uniquement une contrainte, mais rend possibles certaines propriétés difficilement atteignables dans des architectures asynchrones.

En particulier, la synchronie stricte permet :

- l'absence de traces applicatives hors session active,
- l'absence de messages différés ou orphelins,
- l'absence d'états ambigus liés à la livraison ou à la lecture,
- une compréhension immédiate de la surface d'exposition effective au moment de la communication.

Ces propriétés ne relèvent pas d'un mécanisme de protection supplémentaire, mais résultent directement de la réduction du périmètre fonctionnel et de l'absence d'états persistants.

8 Limites et non-objectifs

Entrechat est conçu selon un périmètre restreint. Les limites suivantes sont inhérentes à ses choix architecturaux et ne constituent pas des objectifs du système.

Le système ne fournit pas :

- de garanties de disponibilité ou de continuité de service,

- de mécanismes de livraison de messages hors session active,
- de protection en cas de compromission du terminal utilisateur,
- d'anonymat universel ou inconditionnel,
- de garanties au-delà de l'exécution locale correcte du logiciel.

Entrechat ne constitue ni un service opéré, ni une plateforme, ni une infrastructure. Il n'implique aucune relation contractuelle et ne crée aucune responsabilité quant aux usages effectués par des tiers.

9 Expositions résiduelles

Les expositions résiduelles identifiées résultent directement des contraintes et choix architecturaux du système. Elles incluent notamment :

- les contraintes de disponibilité inhérentes à un modèle de communication strictement synchrone,
- les limites associées à l'anonymat à faible latence dans le cadre de l'utilisation du réseau Tor [4],
- la perte de confidentialité locale en cas de compromission du terminal utilisateur.

Ces expositions ne sont pas traitées par des mécanismes de complexification ou de dissimulation. Elles sont explicitement acceptées et bornées par les omissions architecturales du système.

10 Conclusion

Entrechat v1 présente une architecture de messagerie pair-à-pair strictement synchrone, fondée sur des choix architecturaux explicites et sur un périmètre volontairement restreint.

Le système privilégie la clarté structurelle, le déterminisme des interactions et la maîtrise de l'exposition opérationnelle, plutôt que l'exhaustivité fonctionnelle ou la sophistication protocolaire.

Entrechat doit être compris comme un artefact d'ingénierie intentionnel : spécialisé, explicitement borné, et aligné avec un cadre d'usage précis et assumé, dont les propriétés résultent principalement de l'omission architecturale et de la transparence des hypothèses retenues.

References

[1] W. Diffie and M. Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory, 1976.

[2] D. J. Bernstein, *Curve25519: New Diffie-Hellman Speed Records*, PKC, 2006.

[3] A. Langley, M. Hamburg, and S. Turner, *Elliptic Curves for Security*, RFC 7748, IETF, 2016.

[4] R. Dingledine, N. Mathewson, and P. Syverson, *Tor: The Second-Generation Onion Router*, USENIX Security Symposium, 2004.

[5] S. Barman et al., *All the Numbers Are US: Large-Scale Abuse of Contact Discovery*, NDSS, 2021.

[6] A. Greschbach et al., *Measuring Metadata Exposure in Modern Messaging Systems*, USENIX WOOT, 2024.

[7] J. Müller et al., *Prekey Pogo: Attacking Asynchronous Key Distribution*, IEEE Symposium on Security and Privacy, 2025.

[8] M. Backes et al., *Careless Whisper: Delivery Receipts and User Activity Leakage*, arXiv:2411.11194, 2024.