NOXCrypt v2.3.0 — Spécification Publique

Auteur : NQX

1. Nom

NOXCrypt v2.3.0 est un algorithme cryptographique propriétaire conçu spécifiquement pour le système NQX. Son objectif est de fournir un chiffrement qui ne peut pas être reconnu comme tel, y compris en se déguisant sous forme de différents formats multimédias ou de flux binaires aléatoires. Il est également basé sur le mécanisme de Deep InCrypting (développement NQX).

2. Objectifs et Caractéristiques

- Cacher non seulement le contenu des données, mais aussi le simple fait de leur existence.
- Les données de sortie peuvent imiter des images, de l'audio, de la vidéo ou des données binaires arbitraires.
- Se déguiser en formats populaires (ex. : JPEG, MP3, PNG).
- Utilisation exclusive au sein de l'écosystème NQX.
- Clé dynamique, générée de manière unique pour chaque session.
- Mécanisme de Deep InCrypting (développement NQX) comme couche supplémentaire de confidentialité.

3. Architecture

L'architecture utilise des étapes en cascade de transformation des données, comprenant des substitutions, des mélanges et l'ajout de bruit contrôlé. Les schémas mathématiques spécifiques et les tableaux internes sont des informations confidentielles non divulguées dans la version publique de cette spécification.

4. Clé et Sessions

La clé de chiffrement est longue et formée dynamiquement à l'aide de paramètres aléatoires et de session. Pour chaque session, des tableaux et des règles de

transformation uniques sont créés, empêchant toute réutilisation des clés ou des modèles de chiffrement.

5. Dissimilation

L'algorithme peut convertir un flux chiffré en une forme correspondant à différents types de fichiers multimédias ou de trafic réseau, ce qui complique considérablement l'identification d'une transmission de données chiffrées.

6. Sécurité

Chaque session utilise des clés uniques et des ensembles de règles de chiffrement distincts. Même en cas d'interception du trafic, sans accès à la clé, le déchiffrement est impossible. L'algorithme comprend des mécanismes pour empêcher la cryptanalyse et masquer la structure des données.

7. Application

NOXCrypt peut chiffrer du texte, des données vocales et des flux binaires arbitraires, en les transformant en formes qui ne suscitent pas la méfiance. L'algorithme est optimisé pour une vitesse élevée et une faible latence lors de la transmission de données.

8. Conclusion

NOXCrypt est un système cryptographique de nouvelle génération axé sur la confidentialité maximale, l'anonymat et la résistance à la détection et à l'analyse. Cette spécification fournit une vue d'ensemble de la technologie sans révéler de détails internes de l'algorithme.