



NOXCrypt v2.3.0 — Especificación Pública

Autor: NOX

1. Nombre

NOXCrypt v2.3.0 es un algoritmo criptográfico propietario diseñado específicamente para el sistema NOX. Su propósito es proporcionar cifrado que no pueda ser reconocido como tal, incluyendo la capacidad de disfrazarse como diversos formatos de medios y flujos binarios aleatorios. También se basa en el mecanismo de Deep InCryption (desarrollado por NOX).

2. Objetivos y Características

- Ocultar no solo el contenido de los datos, sino también el hecho mismo de su existencia.
- Los datos de salida pueden imitar imágenes, audio, video o datos binarios arbitrarios.
- Disfrazarse como formatos populares (por ejemplo, JPEG, MP3, PNG).
- Uso exclusivo dentro del ecosistema de NOX.
- Clave dinámica, generada de forma única para cada sesión.
- Mecanismo de Deep InCryption (desarrollado por NOX) como capa adicional de privacidad.

3. Arquitectura

La arquitectura utiliza etapas en cascada de transformación de datos, que incluyen sustituciones, mezclas y la adición de ruido controlado. Los esquemas matemáticos específicos y las tablas internas son información confidencial y no se revelan en la versión pública de esta especificación.

4. Clave y Sesiones

La clave de cifrado tiene una longitud alta y se forma dinámicamente utilizando parámetros aleatorios y de sesión. Para cada sesión se crean tablas y reglas de transformación únicas, evitando la reutilización de claves y patrones de cifrado.

5. Enmascaramiento

El algoritmo es capaz de convertir el flujo cifrado en una forma que corresponda a diferentes tipos de archivos multimedia o tráfico de red, lo que complica significativamente la identificación de transmisiones de datos cifrados.

6. Seguridad

Cada sesión utiliza claves únicas y conjuntos de reglas de cifrado propios. Incluso si el tráfico es interceptado, sin acceso a la clave la descifrado es imposible. El algoritmo incluye mecanismos para prevenir el criptoanálisis y ocultar la estructura de los datos.

7. Aplicación

NOXCrypt puede cifrar texto, datos de voz y flujos binarios arbitrarios, transformándolos en formas que no generan sospechas. El algoritmo está optimizado para alta velocidad y baja latencia durante la transmisión de datos.

8. Conclusión

NOXCrypt es un sistema criptográfico de nueva generación centrado en garantizar la máxima confidencialidad y anonimato, así como resistencia a la detección y el análisis. Esta especificación proporciona una visión general de la tecnología y no revela detalles internos del algoritmo.