



NOxCrypt v2.3.0 — 公共规范

作者: NOX

1. 名称

NOxCrypt v2.3.0 — 专为 NOX 系统开发的专有加密算法。其目标是提供无法被识别为加密的数据保护，包括伪装成各种媒体格式和随机二进制流。这也是 NOX 开发的 Deep InCrypting (NOX development) 的一部分。

2. 目标与特点

- 隐藏不仅是数据内容，还有其存在的事实。
- 输出数据可以模拟图像、音频、视频或任意二进制数据。
- 可以伪装成流行的格式（例如 JPEG、MP3、PNG）。
- 仅在 NOX 生态系统中使用。
- 密钥是动态的，每个会话都会生成唯一密钥。

3. 架构

架构采用多级数据转换，包括替换、混合和添加可控噪声。具体的数学方案和内部表格为机密信息，在公共规范中不予披露。

4. 密钥与会话

加密密钥长度很高，并通过随机和会话参数动态生成。每个会话都会创建唯一的表格和转换规则，从而避免密钥和加密模式的重复使用。

5. 伪装

该算法能够将加密流转换为与各种类型的媒体文件或网络流量相符的形式，极大地增加了识别加密信息传输事实的难度。

6. 安全性

每个会话都使用唯一的密钥和加密规则集。即使截获流量，没有密钥也无法解密。该算法内置防止密码分析和掩盖数据结构的机制。此外，NOX 的 Deep InCryption (NOX development) 提供了额外的隐匿性。

7. 应用

NOXCrypt 可加密文本、语音数据和任意二进制流，并将其转换为不引起怀疑的形式。该算法针对高速和低延迟的数据传输进行了优化。

8. 结论

NOXCrypt 是新一代加密系统，专注于最大化隐私和匿名性，以及抵抗检测与分析。本规范提供了技术概述，但不披露内部算法细节。