XENCNG v5.0 - Technical Whitepaper

1. Introduction

XENCNG (eXtended Encryption Next-Generation) is a novel file encryption system designed with a focus on maximum security against classical and quantum-based attacks. Version 5.0 utilizes AES-256, Argon2id, and a layered encryption mechanism for extreme hardening.

2. Encryption Technology

XENCNG combines proven cryptographic techniques with a custom security architecture:

- AES-256 in CBC mode, deeply layered (up to 100 million iterations)
- Adaptive key derivation using Argon2id (256MB RAM, multithreaded)
- Random salt and IV per encryption
- Optional HWID-based binding
- Portable single .exe (self-contained .NET 8)
- Decryption without original file (only .xenc and .xkey required)

3. Keyfile Structure (.xkey)

The .xkey file contains all necessary metadata to decrypt a file:

- 64 bytes random salt (random64)
- 64 bytes Argon2id-derived hash (from password, AES key/IV)
- 32 bytes AES key
- 16 bytes IV
- 4 bytes layer count (Int32)

4. Security Evaluation

XENCNG is designed under the assumption that attackers may obtain the .xenc file but not the password or the .xkey file. Consequently:

- Without the .xkey file, the encrypted file is useless
- With .xkey but no password: Argon2id blocks brute-force attacks (even on GPU/ASIC)

- AES stacking increases computational cost dramatically
- Even state-level actors (BKA, CIA, NSA) cannot feasibly break it if used correctly

5. Best Practices

- Use strong, long passwords (minimum 12 characters)
- Keep the .xkey file stored separately from the .xenc file
- Use high AES layer counts only for files smaller than 100 MB
- For future-proofing: consider hybridizing with PQC (e.g., Kyber)

6. Conclusion

XENCNG v5.0 delivers one of the most hardened symmetric encryption solutions available, intended for journalists, activists, security researchers, and any individual requiring maximum protection for sensitive data. Its combination of modern cryptography, multi-layered design, and access control presents a realistic defense even against nation-state level adversaries.