ÉTAT DE L'IMPLÉMENTATION DE LA CRYPTOGRAPHIE POST-QUANTIQUE

Par nos experts du SEAL

AMOSSYS

L'utilisation de mécanismes cryptographiques résistants à la menace post-quantique dans l'ensemble des composants et logiciels est aujourd'hui recommandée par l'ensemble des autorités de référence, dont notamment l'ANSSI ou le NIST.

Cette menace quantique n'impose pas forcément de devoir changer en totalité la cryptographie utilisée aujourd'hui. Les mécanismes et algorithmes basés sur des algorithmes dits **symétriques** seront **toujours résistants à un attaquant quantique**, à condition d'avoir néanmoins **augmenté la taille des clés et des empreintes.**

Il est à l'inverse requis d'utiliser des **algorithmes asymétriques nouveaux**, pour lesquels les problèmes mathématiques sous-jacents seraient entièrement nouveaux. Ainsi, en remplacement des algorithmes RSA ou ECDH, respectivement basés sur les problèmes de factorisation des entiers ou du logarithme discret, **la communauté scientifique a proposé de nouveaux algorithmes basés :**

- Sur les **réseaux euclidiens**, tels que ML-KEM, ML-DSA ou FN-DSA,
- Sur les **codes correcteurs**, tel que HQC,
- Sur les **fonctions de hachage**, tel que SLH-DSA.

Afin de faciliter vos choix techniques au cours de vos développements logiciels, notre laboratoire cryptographique a identifié l'implémentation des nouveaux algorithmes post-quantiques dans les principales implémentations open-source.

Certains de ces algorithmes sont standardisés par le NIST (ou en passe de l'être). Cette analyse présente également, parmi les algorithmes sélectionnés ici, ceux dont l'usage est recommandé par l'ANSSI.

**Cette note ne constitue pas une recommandation des bibliothèques listées ou non-listées. Il s'agit avant tout d'un recensement non exhaustif visant à fournir une vue d'ensemble des principales implémentations disponibles pour les algorithmes post-quantiques standardisés par le NIST. Aucune analyse de la conformité ou de la sécurité de ces bibliothèques n'a été menée dans le cadre de cette note.*

→ contact@amossys.fr
→ www.amossys.fr

ÉTAT DE L'IMPLÉMENTATION DE LA CRYPTOGRAPHIE POST-QUANTIQUE

Par nos experts du SEAL

AMOSSYS

			Réseaux euclidiens				Fonctions de hachage	Codes correcteurs
			ML-KEM	ML-DSA	FrodoKEM	Falcon*	SLH-DSA	HQC**
		Standardisé par le NIST	NIST	NIST		*En cours*	NIST	*En cours*
		Recommandé par l'ANSSI	✓	✓	✓	✓	✓	
C/C++	OpenSSL	3.5.0	✓	✓	✗	✗	✓	✗
	PQClean	-	✓	✓	✗	✓	–	✓
	LibreSSL	4.1.0	✓	✗	✗	✗	✗	✗
	SymCrypt	103.4.3	✓	✓	✗	✗	✗	✗
	BoringSSL	0.20240913.0	✓	✓	✗	✗	✓	✗
	liboqs	0.12.0	✓	✓	✓	✓	–	✓
	BOTAN	3.6.0	✓	✓	✓	✗	–	✗
	Crypto++	-	✗	✗	✗	✗	✗	✗
Go	CryptoGo	1.24.0	✓	✗	✗	✗	✗	✗
Java	BouncyCastle	1.78	✓	✓	✓	✓	✓	✓
Python	Pycryptodome	-	✗	✗	✗	✗	✗	✗
Rust	RustCrypto	-	✓	✓	✓	✗	✓	✗
	LibCrux	-	✓	✓	✓	✗	✗	✗

✗	–	✓
L'algorithme n'est pas implémenté.	L'algorithme est en cours d'implémentation.	L'algorithme est supporté.

Les numéros de versions correspondent à la version de ces bibliothèques à partir de laquelle le support de ces algorithmes a été intégré. Toutefois, il est recommandé d'utiliser la version la plus récente disponible pour des raisons de sécurité.

**Falcon est en cours de standardisation par le NIST, qui devrait devenir le futur standard « FN-DSA ».*

***HQC est en cours de standardisation par le NIST. Le nom du standard n'est pas encore déterminé.*

→ contact@amossys.fr
→ www.amossys.fr