NIST candidates (pros and cons)

Standardization since 2016... and ~~the winner is~~ the winners are:

- **Dilithium** – **ML-DSA**, based on lattices,
- **Falcon** – **FN-DSA**, based on lattices,
- SPHINCS – SLH-DSA, based on hash functions (big and expensive)

How to choose?

NIST candidates (pros and cons)

Standardization since 2016... and ~~the winner is~~ the winners are:

- **Dilithium – ML-DSA**, based on lattices,
- **Falcon – FN-DSA**, based on lattices,
- SPHINCS – SLH-DSA, based on hash functions (big and expensive)

How to choose?

	ML-DSA	**FN-DSA**
EIP	8051	8052
Public key	1312B	897B
Signature	2420B	666B
On-chain cost	13.0M gas (8.3M gas)	4.1M gas (1.6M gas)
Standardized?	FIPS 204	not yet (since 2 years)
Signer implementation	Easy, many	Tricky, floating point
Hardware integration	Done	High RAM requirements
Industrial integration	Passkey, Apple (soon)	no
ZK variant	Possible	Overstretch attacks

EIPs 8051 and 8052

- **EIP 8051**: link
  - Two precompiles:
    - MLDSA: NIST-compliant with SHAKE256
      (verification: 13.0 M gas, not far from the tx limit of 16M!).
    - MLDSA-ETH: replacement with a counter-mode Keccak PRNG
      (verification: 8.3M gas).
  - Test vector provided (generated from NIST reference implementation).
  - Integrated into a 4337 hybrid (MLDSA + ECDSA) account:
    Try it by yourself!

EIPs 8051 and 8052

- **EIP 8051**: link
  - Two precompiles:
    - MLDSA: NIST-compliant with SHAKE256
      (verification: 13.0 M gas, not far from the tx limit of 16M!).
    - MLDSA-ETH: replacement with a counter-mode Keccak PRNG
      (verification: 8.3M gas).
  - Test vector provided (generated from NIST reference implementation).
  - Integrated into a 4337 hybrid (MLDSA + ECDSA) account:
    Try it by yourself!
- **EIP 8052**: link
  - Separation of the hash part and the polynomial arithmetic:
    - FALCON: NIST-compliant with SHAKE256
      (verification: 4.1M gas).
    - ETH-FALCON: replacement with a counter-mode Keccak PRNG
      (verification: 1.6M gas).
  - Precompiles for FALCON-CORE and HASH-TO-POINT (one for Shake256, one for KeccakPRNGone).
  - Test vector provided (generated from NIST reference implementation).
  - Integration in a 4337 account in progress...