NIST Signature 후보 알고리즘 MAYO

정보컴퓨터공학과 권혁동

MAYO 서명 알고리즘

- 2023년 7월 NIST에서 발표한 추가 서명 알고리즘 후보
  - Round 1에서는 40개의 후보가 통과
  - **Multivariate 기반에는 11개의 후보**가 존재
  - **한국형 양자내성암호 공모전인 KpqC에 등재된 후보도 존재**

Code	Isogeny	Lattice	MPC-in-the-Head	Multivariate	Symmetric	Others
CROSS Enhanced pqsigRM FuLeeca LESS MEDS Wave	SQIsign	EagleSign EHTv3 and EHTv4 HAETAE HAWK HuFu Raccoon SQUIRRELS	MIRA MiRitH MQOM PERK RYDE SDitH	3WISE Biscuit DME-Sign HPPC **MAYO** PROV QR-UOV SNOVA TUOV UOV VOX	AIMer Ascon-Sign FAEST SHPINCS-alpha	ALTEQ eMLE-Sig 2.0 KAZ-SIGN Preon Xifrat1-Sign.I

MAYO 서명 알고리즘

- Oil and Vinegar 기반을 사용한 알고리즘
  - 비슷한 유형인 Unbalanced Oil and Vinegar 알고리즘도 존재
  - UOV는 MAYO와 함께 Round 1 후보로 진출함

- MAYO는 Oil and Vinegar의 변형 알고리즘
  - Matthias 박사가 개발
  - 기본적인 구조는 Oil and Vinegar과 동일
  - **Oil and Vinegar의 키 크기를 매우 줄인 구조**

MAYO 서명 알고리즘

- 보안수준 1은 2 종류의 매개변수를 제공함
  - MAYO-I은 공개키 크기가 작지만 서명이 크고 MAYO-II는 이와 반대
  - 소스코드는 일반, 최적화, AVX 최적화 세 종류로 제공

Algorithm	MAYO-I	MAYO-II	MAYO-III	MAYO-V
Security level	1	1	3	5
Secret key size	24 bytes	24 bytes	32 bytes	40 bytes
Public key size	1168 bytes	5488 bytes	2656 bytes	5008 bytes
Signature size	321 bytes	180 bytes	577 bytes	838 bytes

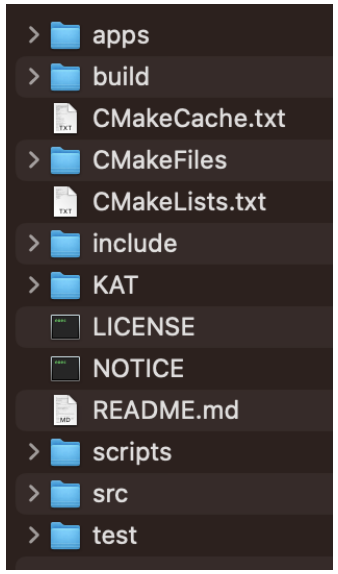
MAYO 서명 알고리즘

- 기본 레퍼런스 코드의 성능 (AES-NI 제외)
  - Intel Xeon E3-1225 v3 (Haswell, 3.20GHz)
  - Ubuntu 20.04.5, clang compiler
  - **1,000회 반복의 중앙 값 사용**

Scheme	Keygen	ExpandSK	ExpandPK	ExpandSK +Sign	ExpandPK +Verify
MAYO-I	2,964,948	3,865,364	1,526,032	6,787,356	2,996,968
MAYO-II	6,348,792	7,512,512	2,031,976	9,290,400	2,813,708
MAYO-III	10,670,888	14,403,980	5,166,728	23,816,456	9,619,732
MAYO-V	27,467,616	38,061,916	12,344,572	59,571,696	21,619,600

MAYO 서명 알고리즘

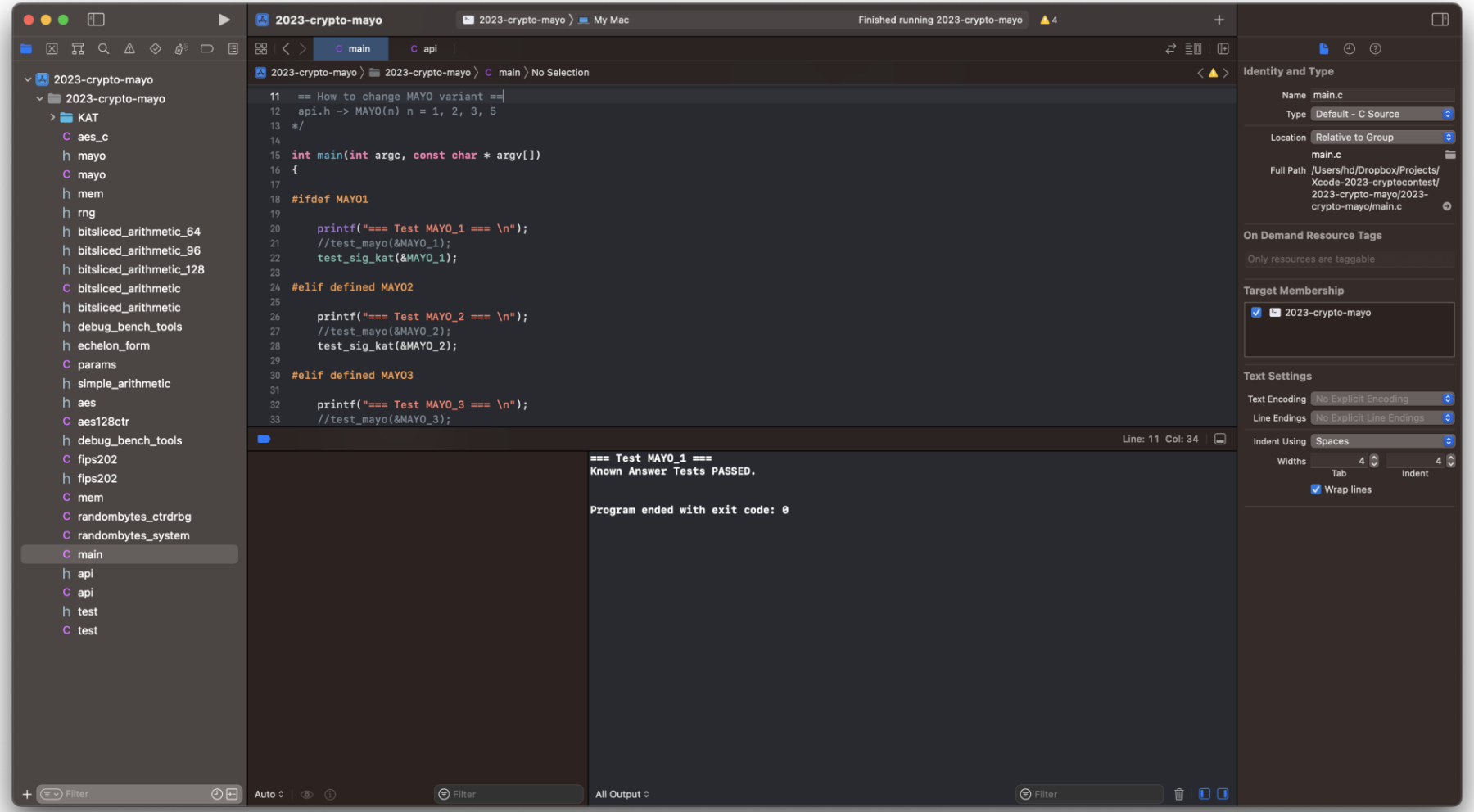
- 공식 코드는 cmake로 공유됨
  - Cmake → Makefile → 컴파일
- 그러나 시스템에 따라서는 컴파일 문제가 생김
  - 컴파일러 문제로 추정되나.. 해결하지 못함
- Xcode 상에서 컴파일이 편리함
  - **ARM 구현을 위해서면 더욱**




```
[HD-M1-MacBook-Pro:2023-crypto-mayo-cmake hd$ mkdir -p build
[HD-M1-MacBook-Pro:2023-crypto-mayo-cmake hd$ cd build
[HD-M1-MacBook-Pro:build hd$ cmake -DMAYO_BUILD_TYPE=ref -DENABLE_AESNI=OFF ..
-- The C compiler identification is unknown
-- The CXX compiler identification is unknown
-- The ASM compiler identification is unknown
-- Found assembler: /usr/bin/cc
-- Detecting C compiler ABI info
-- Detecting C compiler ABI info - failed
-- Check for working C compiler: /usr/bin/cc
-- Check for working C compiler: /usr/bin/cc - broken
CMake Error at /opt/homebrew/Cellar/cmake/3.27.1/share/cmake/Modules/CMakeTestCC
ompiler.cmake:67 (message):
  The C compiler

    "/usr/bin/cc"

  is not able to compile a simple test program.

  It fails with the following output:

    Change Dir: '/Users/hd/Dropbox/Projects/Xcode-2023-cryptocontest/2023-crypto
-mayo-cmake/CMakeFiles/CMakeScratch/TryCompile-ve0FGU'

    Run Build Command(s): /opt/homebrew/Cellar/cmake/3.27.1/bin/cmake -E env VER
BOSE=1 /usr/bin/make -f Makefile cmTC_7de96/fast
    xcrun: error: unable to load libxcrun (dlopen(/Library/Developer/CommandLine
Tools/usr/lib/libxcrun.dylib, 0x0005): tried: '/Library/Developer/CommandLineToo
ls/usr/lib/libxcrun.dylib' (mach-o file, but is an incompatible architecture (ha
ve 'x86_64', need '')), '/System/Volumes/Preboot/Cryptexes/OS/Library/Developer/
CommandLineTools/usr/lib/libxcrun.dylib' (no such file), '/Library/Developer/Com
mandLineTools/usr/lib/libxcrun.dylib' (mach-o file, but is an incompatible archi
tecture (have 'x86_64', need ''))).




  CMake will not be able to correctly generate this project.
Call Stack (most recent call first):
  CMakeLists.txt:4 (project)
```

MAYO 서명 알고리즘

- Xcode로 이식하는 것에 성공
  - Bitslice 구현을 ARM 명령어를 통해서 병렬화 하는 것을 목표로 구현 중



Q & A