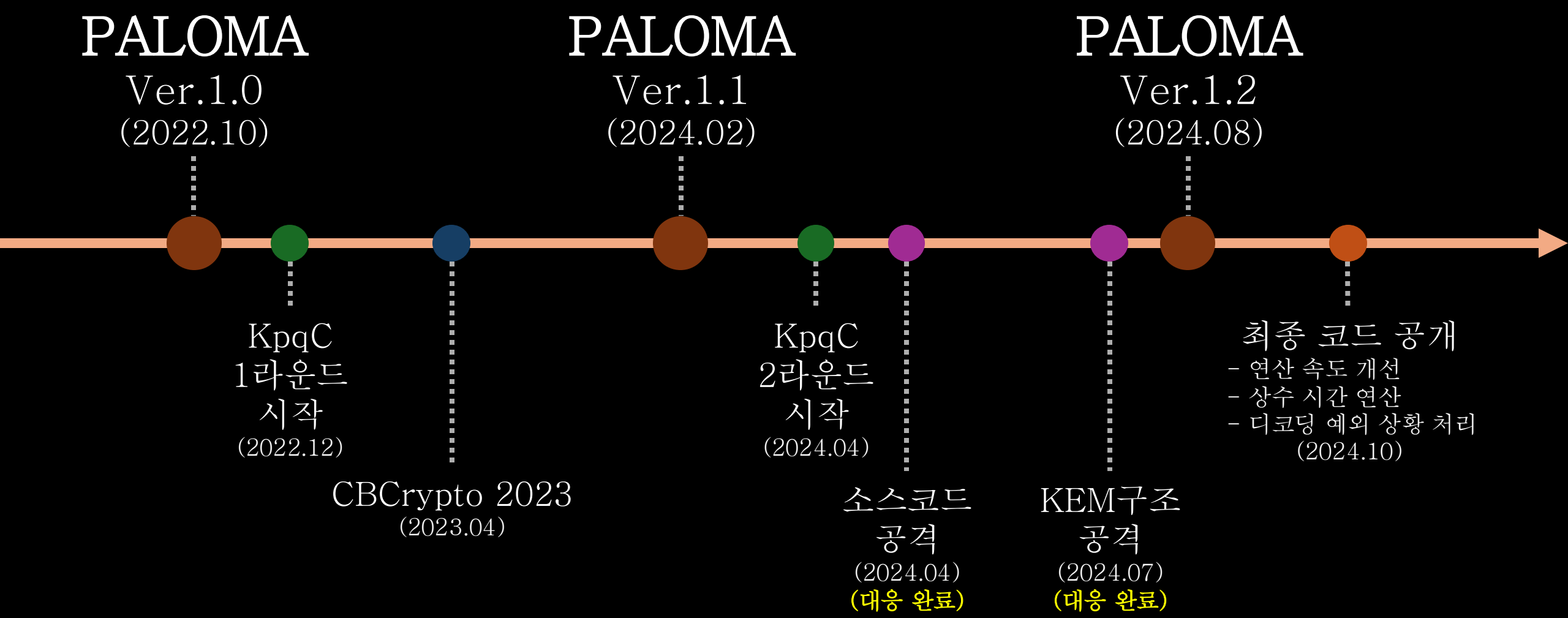
PALOMA

Binary Separable Goppa-based KEM

김 동 찬


PALOMA
Ver.1.0
(2022.10)
PALOMA
Ver.1.1
(2024.02)
PALOMA
Ver.1.2
(2024.08)
KpqC
1라운드
시작
(2022.12)
CBCrypto 2023
(2023.04)
KpqC
2라운드
시작
(2024.04)
소스코드
공격
(2024.04)
(대응 완료)
KEM구조
공격
(2024.07)
(대응 완료)
최종 코드 공개
- 연산 속도 개선
- 상수 시간 연산
- 디코딩 예외 상황 처리
(2024.10)

PALOMA는

IND-CCA2 안전성을 가지는

부호 기반 키체결 암호(KEM)입니다.

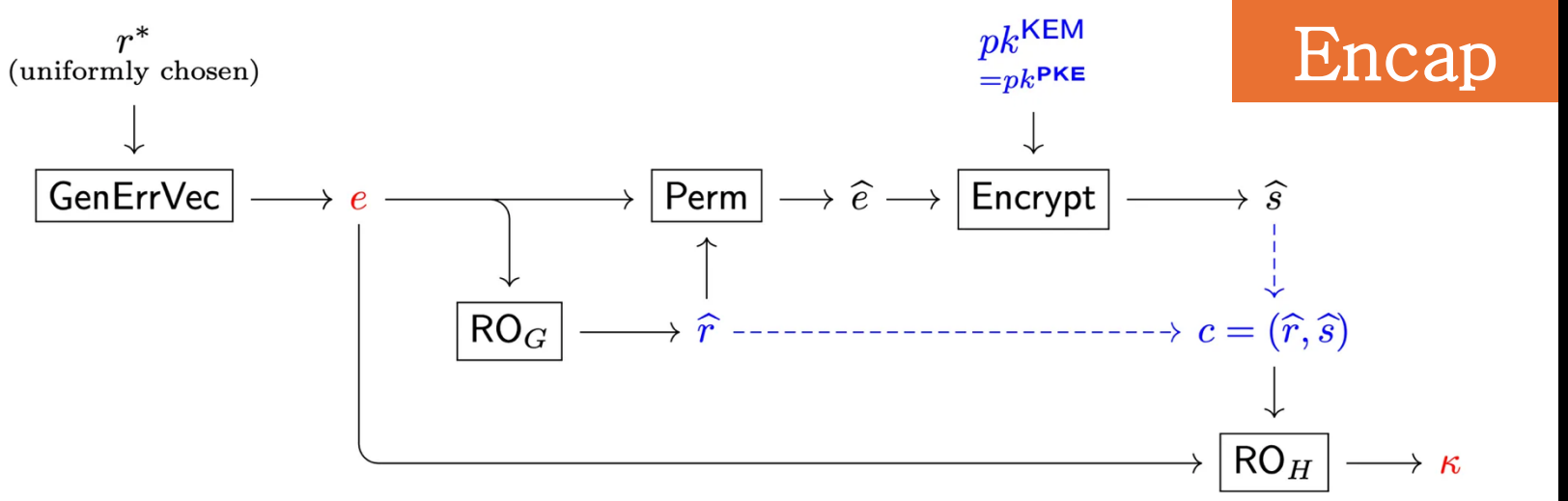
Goppa 부호-신드롬 디코딩 문제 기반
(NP-hard 문제)

OW-CPA-secure
부호 기반 트랩도어
(Separable Goppa 부호)

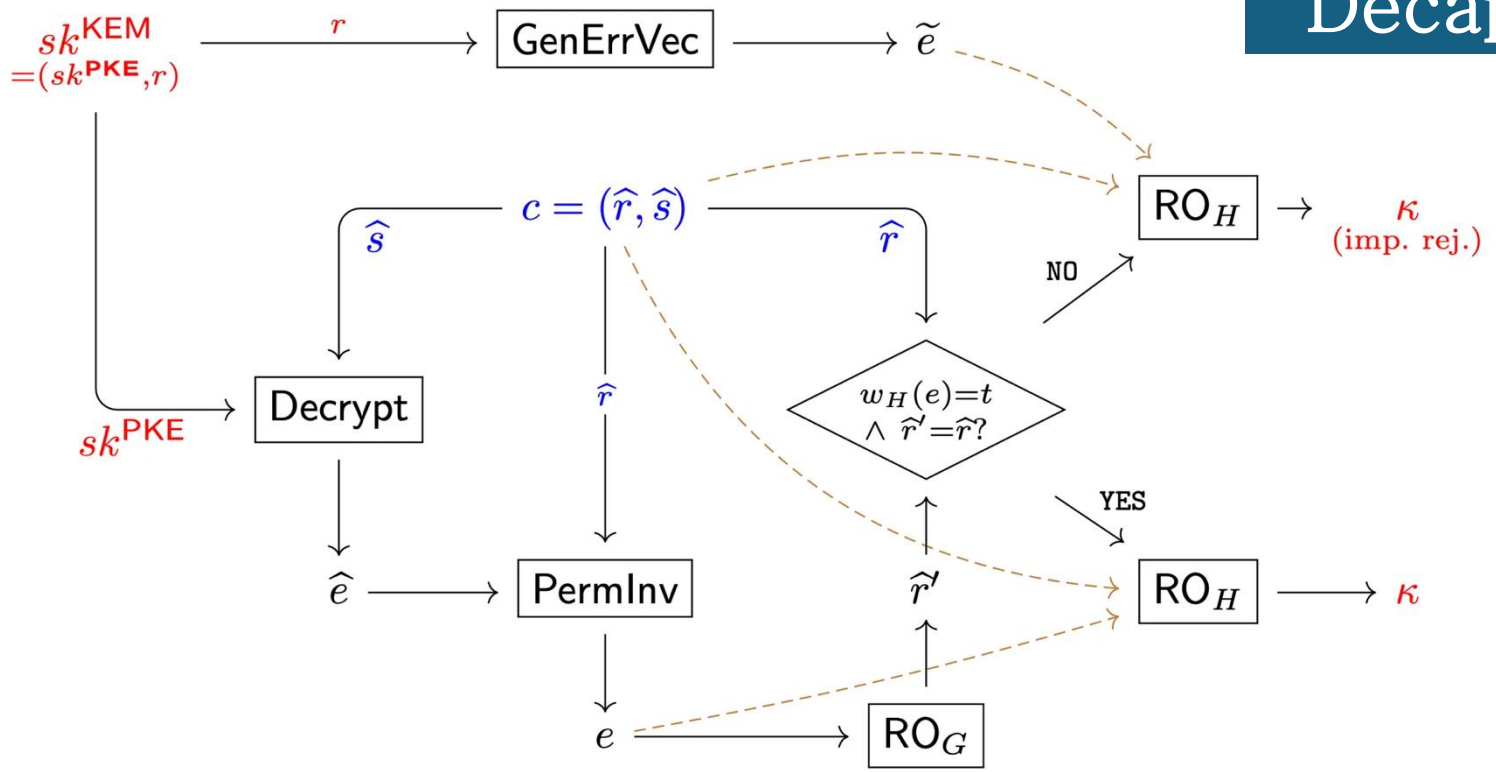
Fujisaki-Okamoto 변환

IND-CCA2-secure
KEM in ROM
(재암호화 불필요, 복호 실패 확률 0)

Encap



Decap



GenErrVec
해밍무게가 t인 비트열 생성함수

Perm/InvPerm
비트열의 자리를 섞는 함수

$\mathsf{RO}_G/\mathsf{RO}_H$
랜덤오라클(해시함수 LSH-512)

PALOMA는

공모전 기간동안

규격은 조금 변경되었고,

파라미터는 바뀌지 않았습니다.

(보수적으로 기반 문제 파라미터를 선택하였습니다.)

Ver.1.0
(Round 1)

Ver.1.1
(Round 2)

Implicit rejection 전용
비밀키를 KEM 비밀키에 추가

Perm/InvPerm의 출력이
균등분포를 따르도록 수정

Ver.1.2
(2024.08.)

Decap에서 복호한 평문의
해밍무게 조건 충족 여부 확인

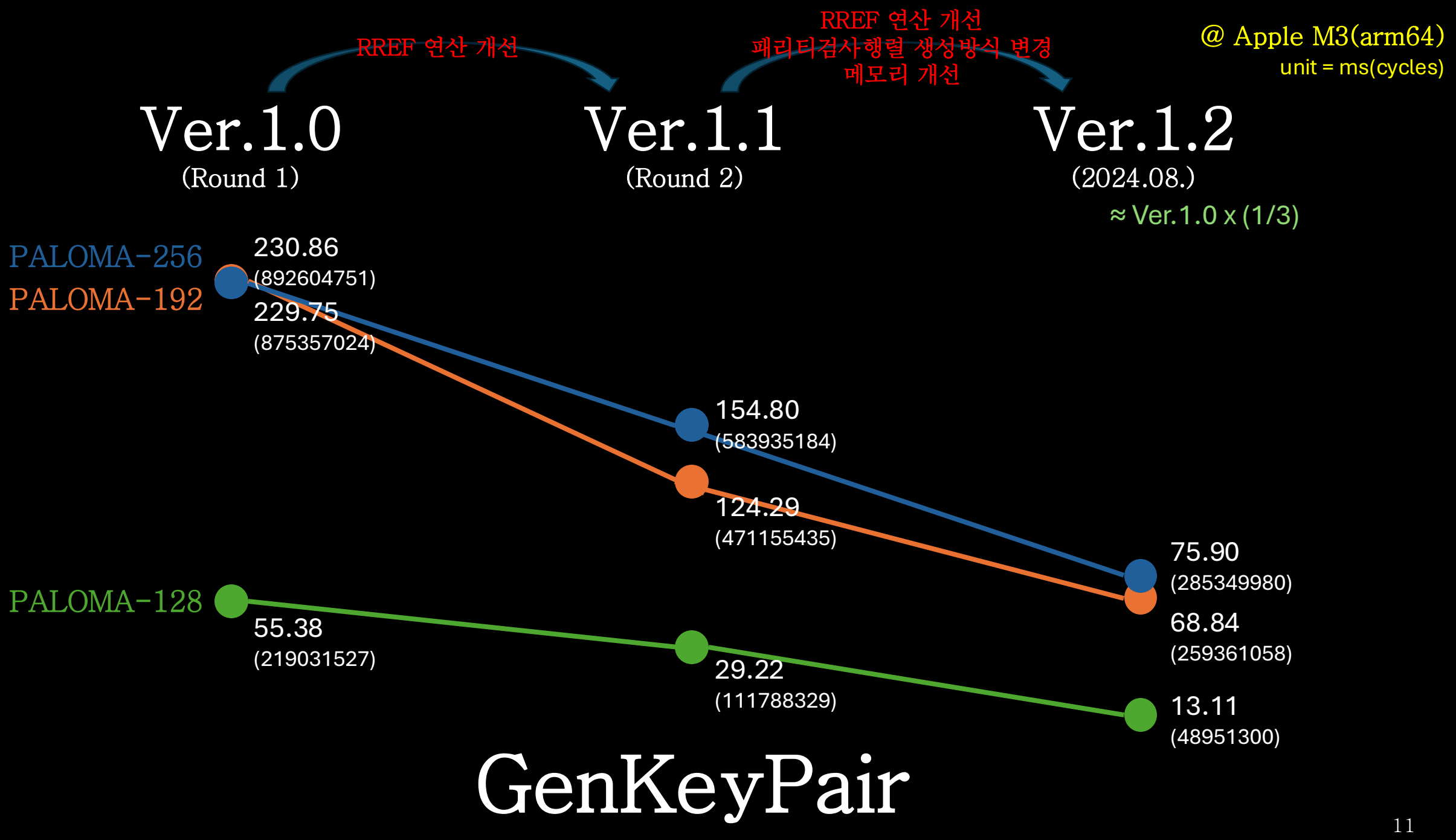
유효한 암호문에 대해서만
복호 가능하도록 수정

Ver.1.0 (Round 1)	Ver.1.1 (Round 2)	Ver.1.2 (2024.08.)
PALOMA-128 (166비트)	$(n,t) = (3904,64)$	
PALOMA-192 (267비트)	$(n,t) = (5568,128)$	
PALOMA-256 (289비트)	$(n,t) = (6592,128)$	

PALOMA는

경쟁력 있는 성능을 가지고 있습니다.

	공개키	비밀키	암호문
PALOMA-128	312KB	93KB (96B로 압축 가능)	136B
PALOMA-192	793KB	350KB (96B로 압축 가능)	240B
PALOMA-256	1MB	352KB (96B로 압축 가능)	240B


RREF 연산 개선
RREF 연산 개선
패리티검사행렬 생성방식 변경
메모리 개선
@ Apple M3(arm64)
unit = ms(cycles)
Ver.1.0
(Round 1)
Ver.1.1
(Round 2)
Ver.1.2
(2024.08.)
≈ Ver.1.0 x (1/3)
PALOMA-256
PALOMA-192
PALOMA-128
230.86
(892604751)
229.75
(875357024)
154.80
(583935184)
124.29
(471155435)
75.90
(285349980)
68.84
(259361058)
55.38
(219031527)
29.22
(111788329)
13.11
(48951300)
GenKeyPair

RREF 연산 개선

RREF 연산 개선
패리티검사행렬 생성방식 변경
메모리 개선

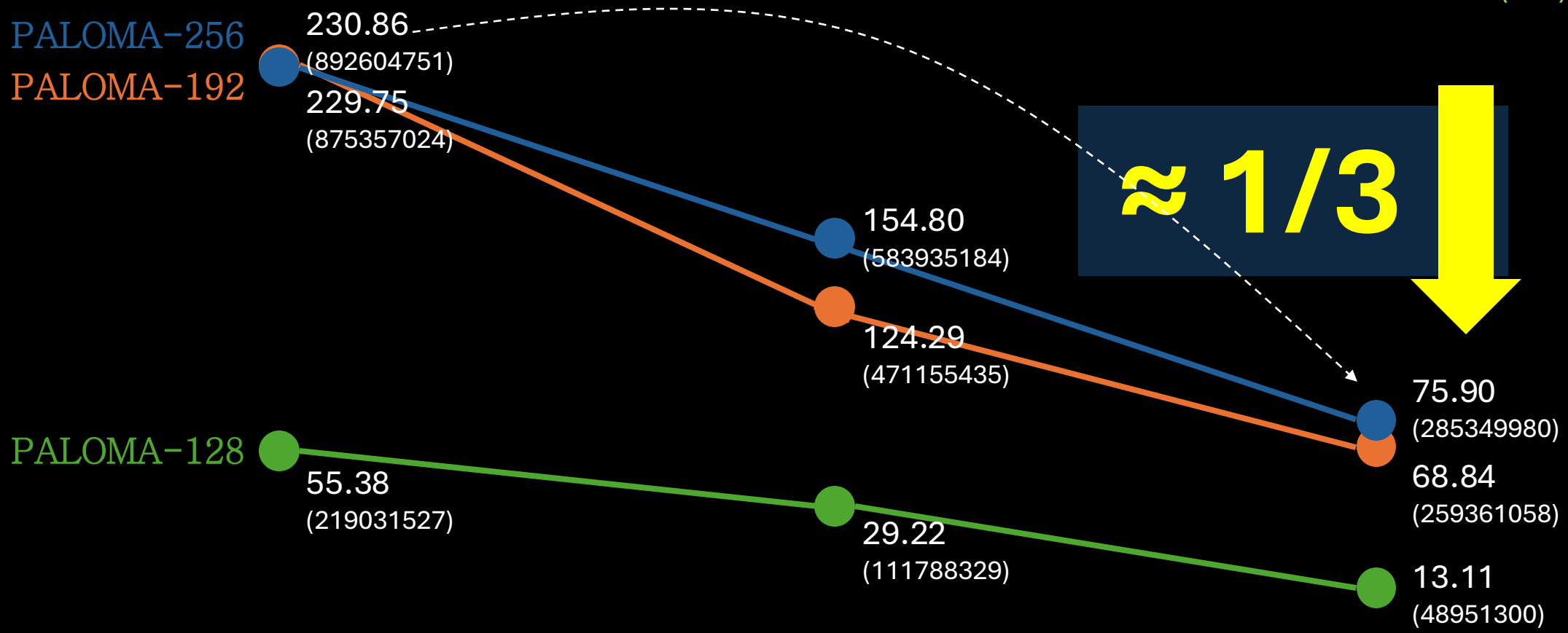
@ Apple M3(arm64)
unit = ms(cycles)

Ver.1.0
(Round 1)

Ver.1.1
(Round 2)

Ver.1.2
(2024.08.)

≈ Ver.1.0 x (1/3)



GenKeyPair

@ Apple M3(arm64)
unit = ms(cycles)

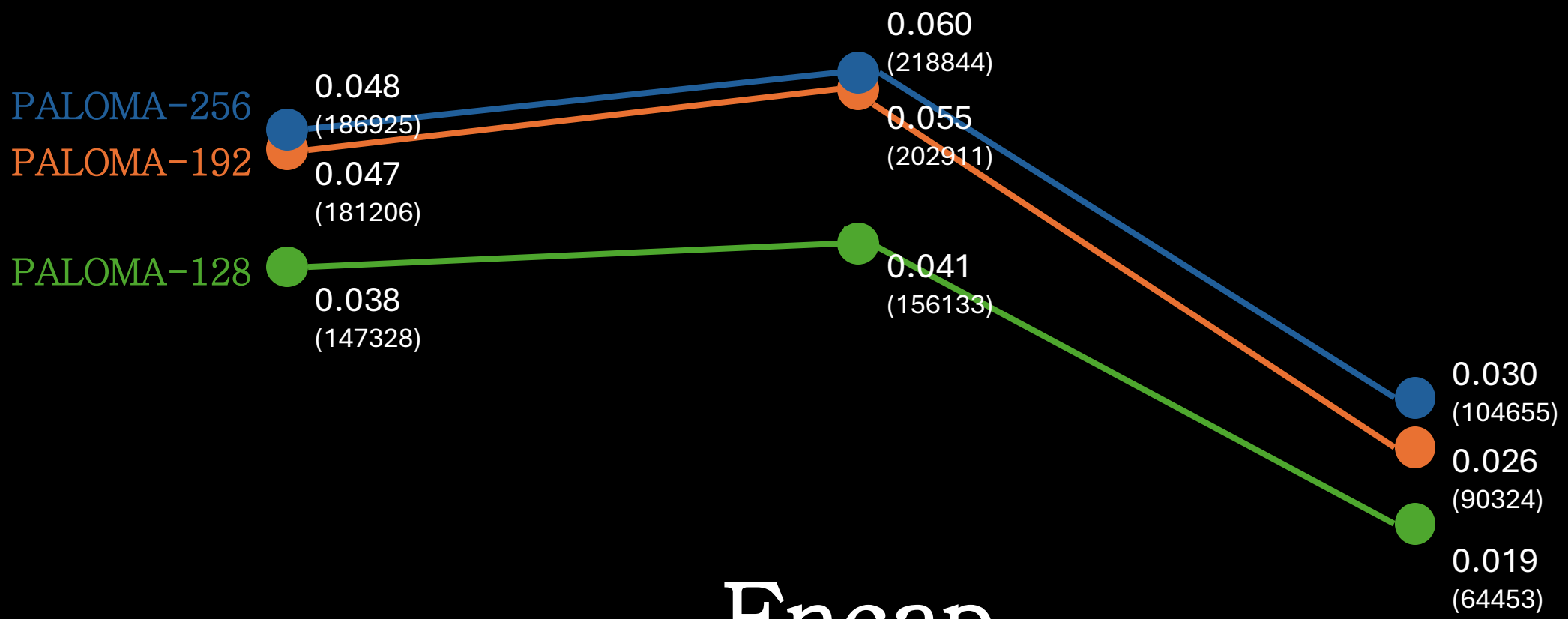
데이터 구조 변경

메모리 개선

Ver.1.0
(Round 1)

Ver.1.1
(Round 2)

Ver.1.2
(2024.08.)
≈ Ver.1.0 x (1/2)



Encap

@ Apple M3(arm64)
unit = ms(cycles)

데이터 구조 변경

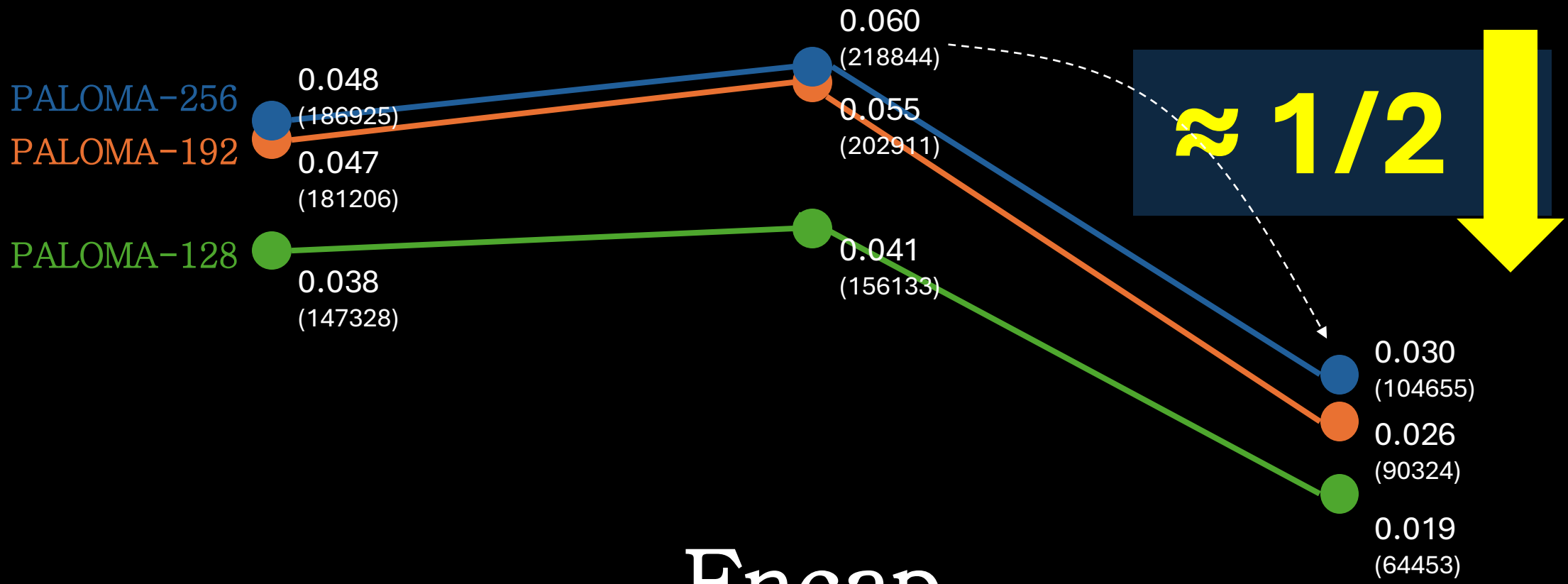
메모리 개선

Ver.1.0
(Round 1)

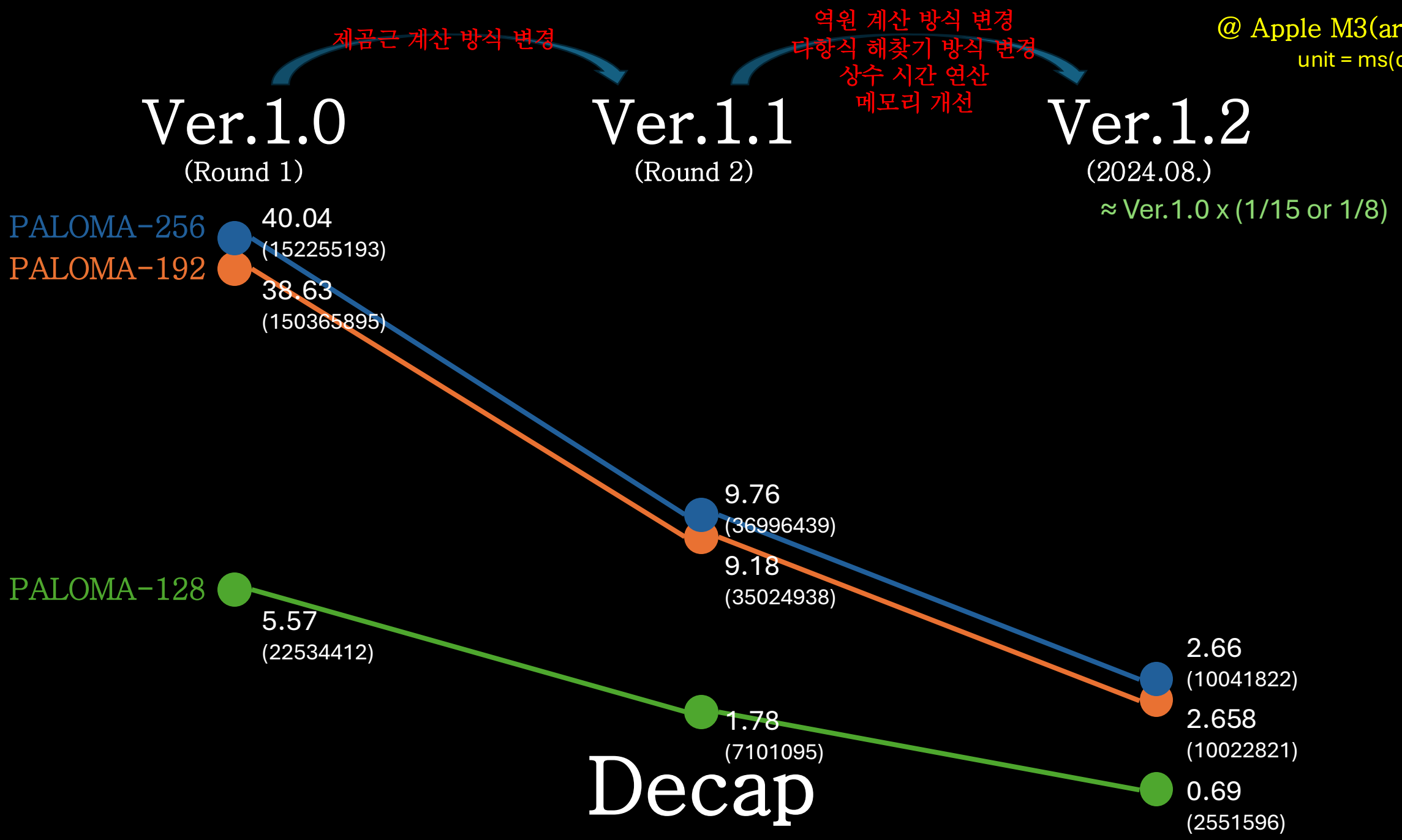
Ver.1.1
(Round 2)

Ver.1.2
(2024.08.)

≈ Ver.1.0 x (1/2)



Encap


제곱근 계산 방식 변경
역원 계산 방식 변경
다항식 해찾기 방식 변경
상수 시간 연산
메모리 개선
@ Apple M3(arm64)
unit = ms(cycles)
Ver.1.0
(Round 1)
Ver.1.1
(Round 2)
Ver.1.2
(2024.08.)
≈ Ver.1.0 x (1/15 or 1/8)
PALOMA-256
PALOMA-192
PALOMA-128
40.04
(152255193)
38.63
(150365895)
9.76
(36996439)
9.18
(35024938)
5.57
(22534412)
1.78
(7101095)
2.66
(10041822)
2.658
(10022821)
0.69
(2551596)
Decap

제곱근 계산 방식 변경

역원 계산 방식 변경
다항식 해찾기 방식 변경
상수 시간 연산
메모리 개선

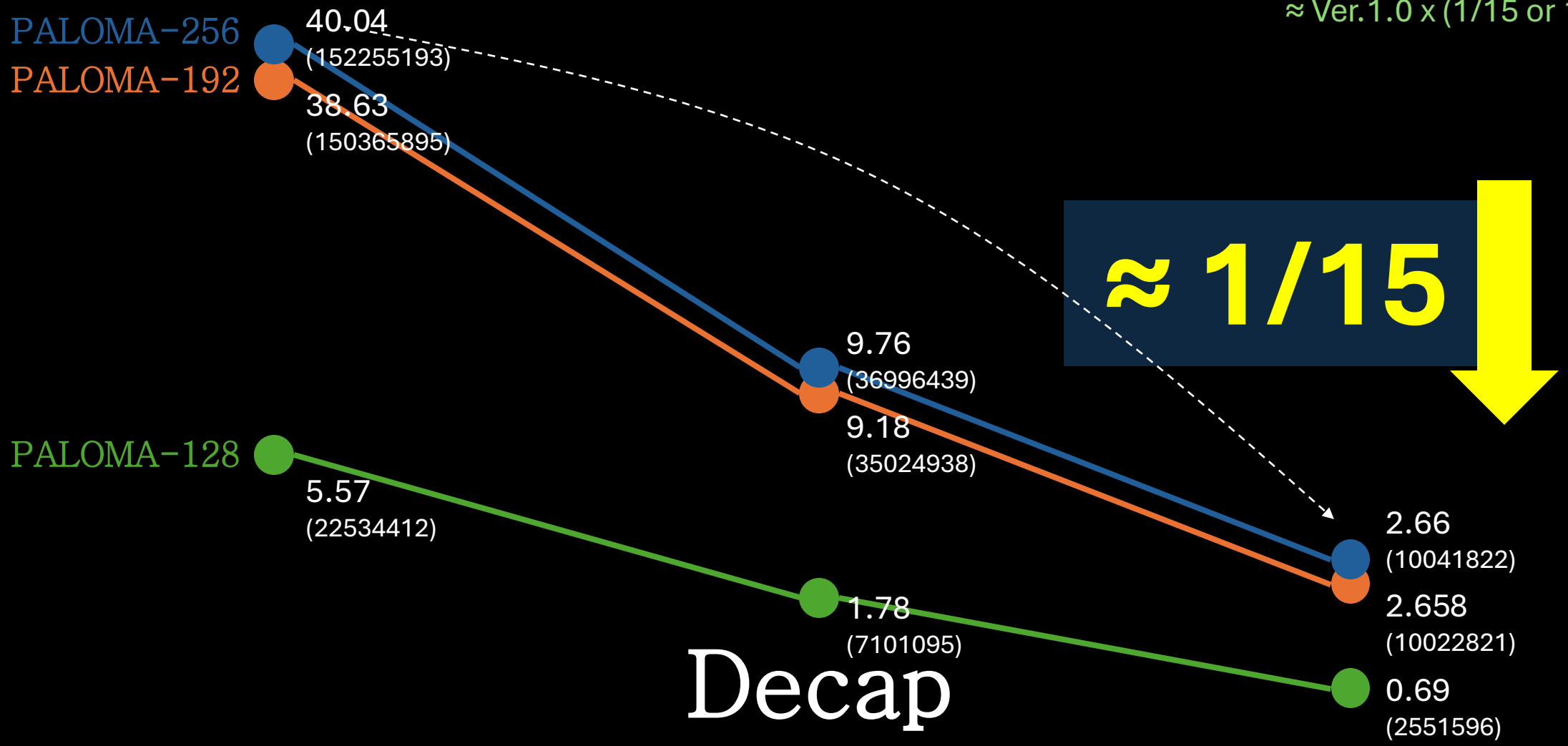
@ Apple M3(arm64)
unit = ms(cycles)

Ver.1.0
(Round 1)

Ver.1.1
(Round 2)

Ver.1.2
(2024.08.)

≈ Ver.1.0 x (1/15 or 1/8)



Decap


PALOMA
Ver.1.0
(2022.10)
PALOMA
Ver.1.1
(2024.02)
PALOMA
Ver.1.2
(2024.08)


PALOMA
Ver.1.0
(2022.10)
PALOMA
Ver.1.1
(2024.02)
PALOMA
Ver.1.2
(2024.08)
PALOMA
Ver.2.0
(??)

PALOMA Ver.2.0에서는

PALOMA Ver.2.0에서는

더 적합한 해시함수와 디코더의 적용을 위해

LSH-512와 확장 Patterson 디코더만을

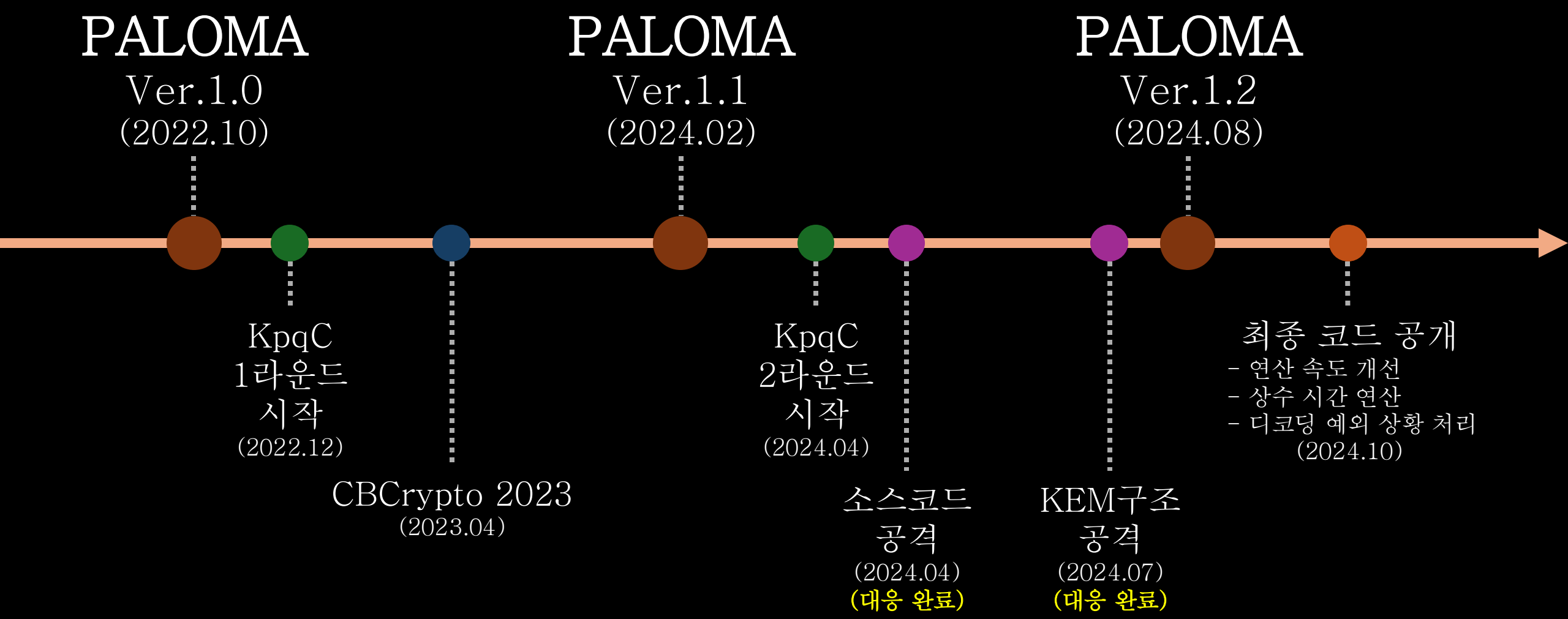
정식 규격으로 정의하지 않으려 합니다.

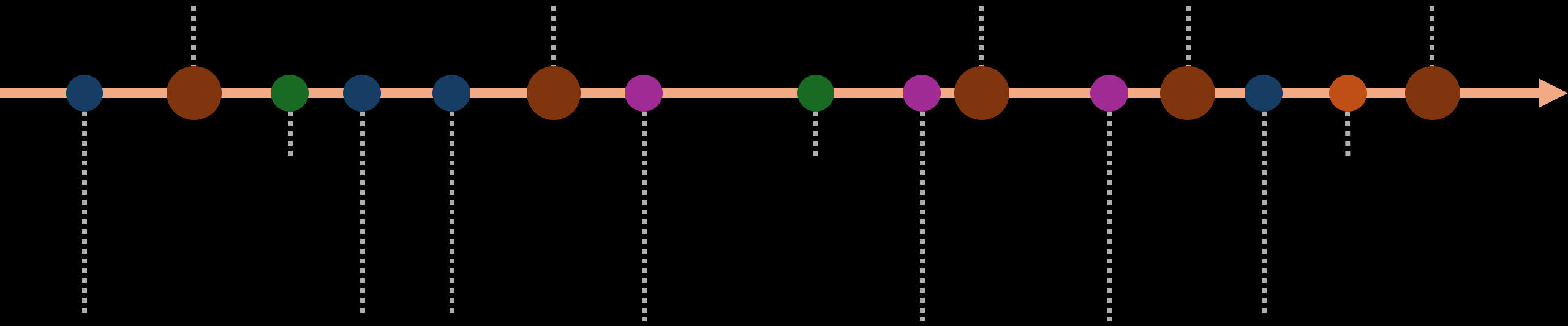
SHA3, Berlekamp-Massey Decoder 등등

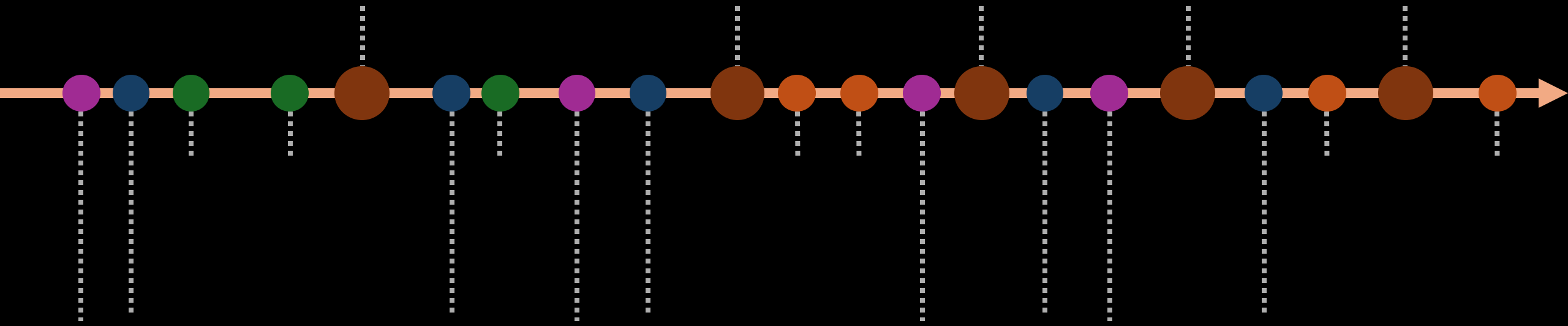
PALOMA의

모든 관련 문서와 소스코드는
PALOMA 웹사이트에서
다운로드 받을 수 있습니다.

https://kmu-fdl-dc.notion.site/PALOMA-Binary-Separable-Goppa-based-KEM-04aed6ca07d2486db14eb5eb7bab7e85


PALOMA
Ver.1.0
(2022.10)
PALOMA
Ver.1.1
(2024.02)
PALOMA
Ver.1.2
(2024.08)
KpqC
1라운드
시작
(2022.12)
CBCrypto 2023
(2023.04)
KpqC
2라운드
시작
(2024.04)
소스코드
공격
(2024.04)
(대응 완료)
KEM구조
공격
(2024.07)
(대응 완료)
최종 코드 공개
- 연산 속도 개선
- 상수 시간 연산
- 디코딩 예외 상황 처리
(2024.10)





10년 후의 PALOMA가

궁금하지 않으세요?

경청 감사합니다.