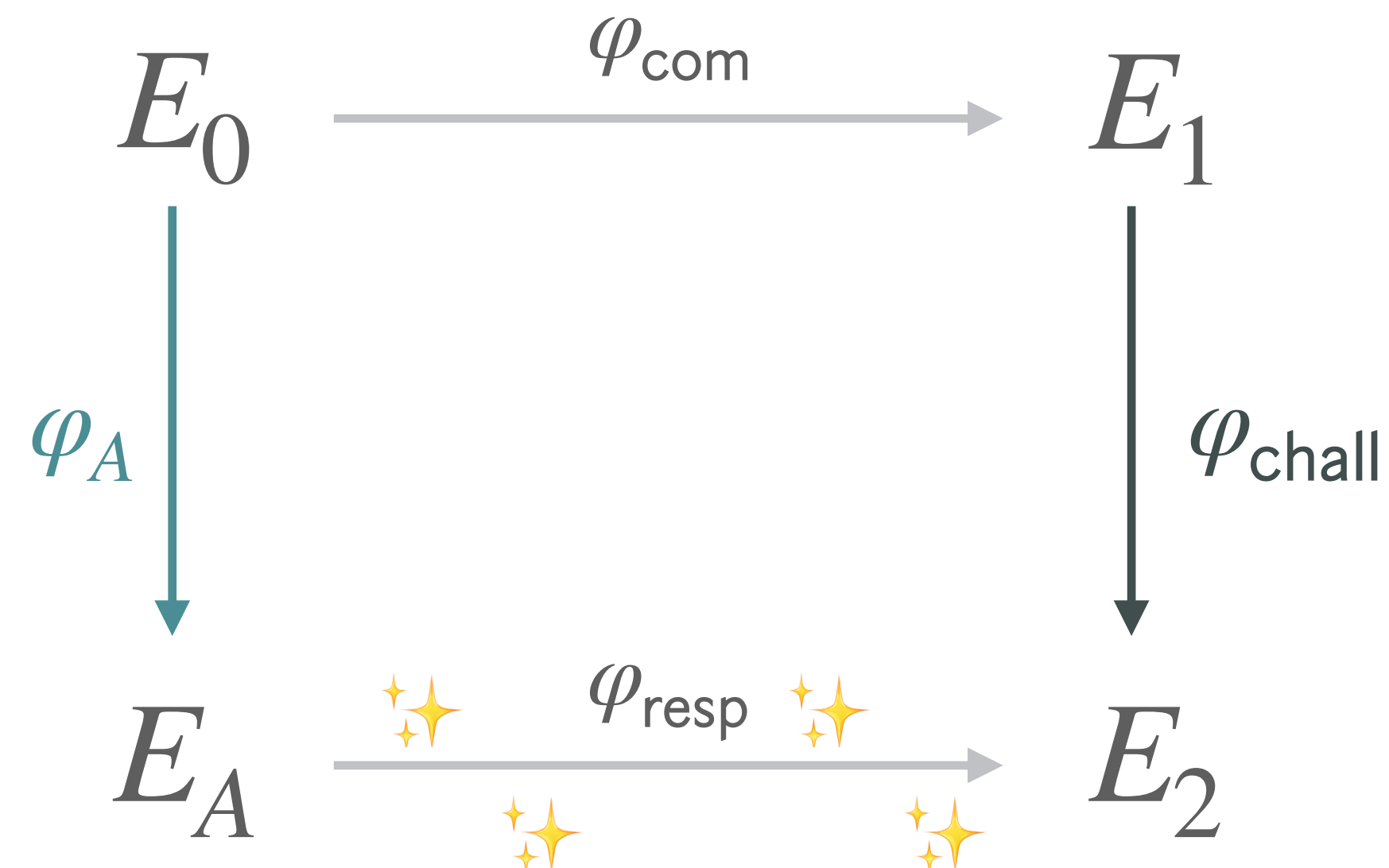


PART 3
New Dimensions

extension fields

in signing, we want to keep working over \mathbb{F}_{p^2} for efficiency reasons

Idea: signing is slow anyway, what if we work over $\mathbb{F}_{p^{2k}}$ during signing, and push verification speeds to the absolute limits?



1

instead of (slow)
translation of I_{resp}
to φ_{resp} in 13 blocks....

2

slower translation
using $\mathbb{F}_{p^{2k}}$ arithmetic
but only 4 blocks!



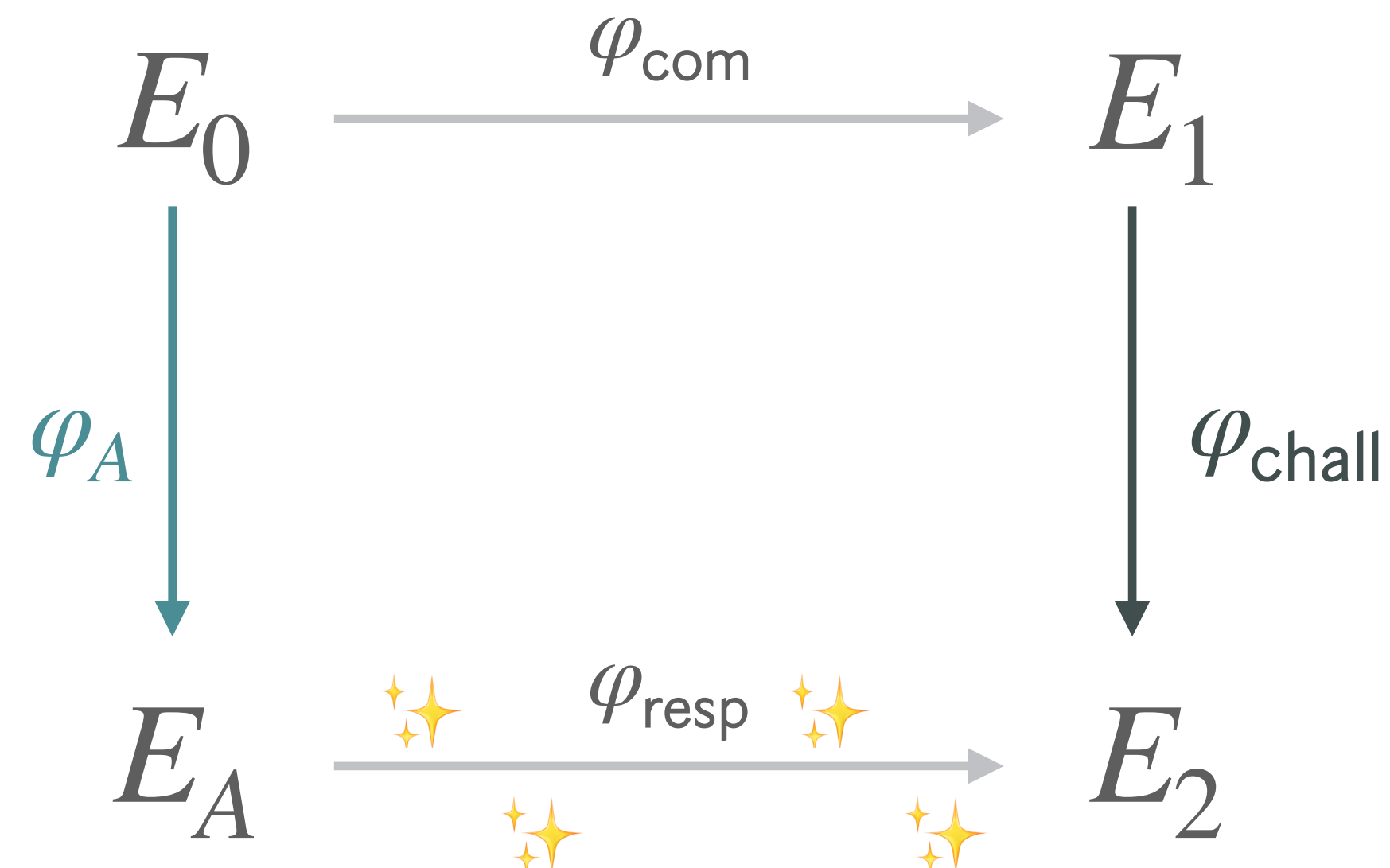
**signing is now even slower,
using extension fields, takes literal seconds**

PART 3
New Dimensions

extension fields

in signing, we want to keep working over \mathbb{F}_{p^2} for efficiency reasons

Idea: signing is slow anyway, what if we work over $\mathbb{F}_{p^{2k}}$ during signing, and push verification speeds to the absolute limits?



1

instead of (slow)
translation of I_{resp}
to φ_{resp} in 13 blocks....

2

slower translation
using $\mathbb{F}_{p^{2k}}$ arithmetic
but only 4 blocks!



**signing is now even slower,
using extension fields, takes literal seconds**



**faster
primes!**



**fewer
blocks!**



**FAST
verification!**