HD representations
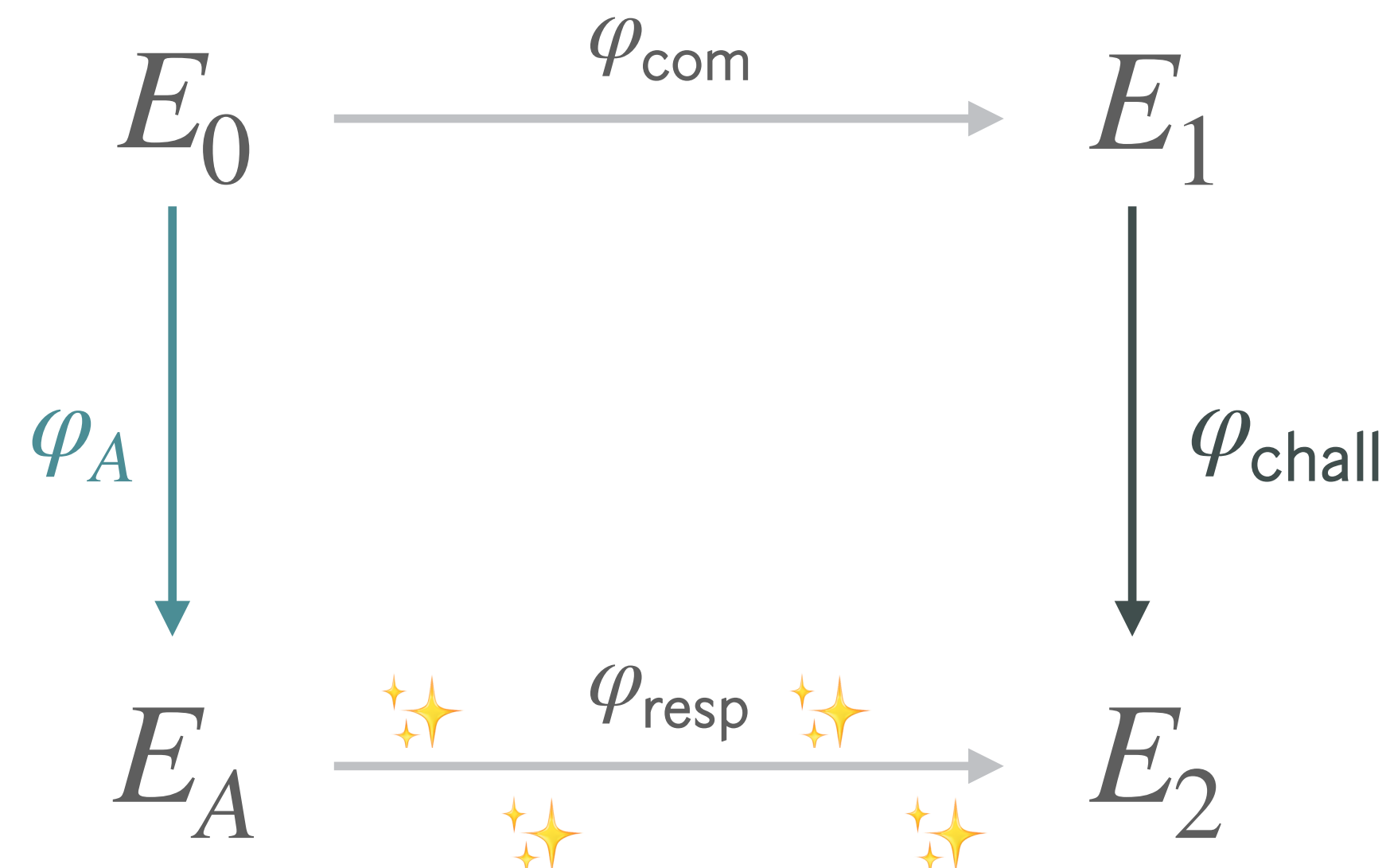
instead of describing 1D isogeny $\varphi : E \to E'$ by its kernel $\ker \varphi$,
we can also describe it by $E, P_1, \ldots, P_n, \varphi(P_1), \ldots, \varphi(P_n)$, for enough points $P_i \in E$

then, with Kani's lemma & improvements, compute $\varphi(Q)$ for any other $Q \in E$

$E_0 \xrightarrow{\varphi_{\text{com}}} E_1$

φ_A

φ_{chall}

$E_A \xrightarrow{\varphi_{\text{resp}}} E_2$

1 instead of (slow) translation of I_{resp} to φ_{resp} in 13 blocks....
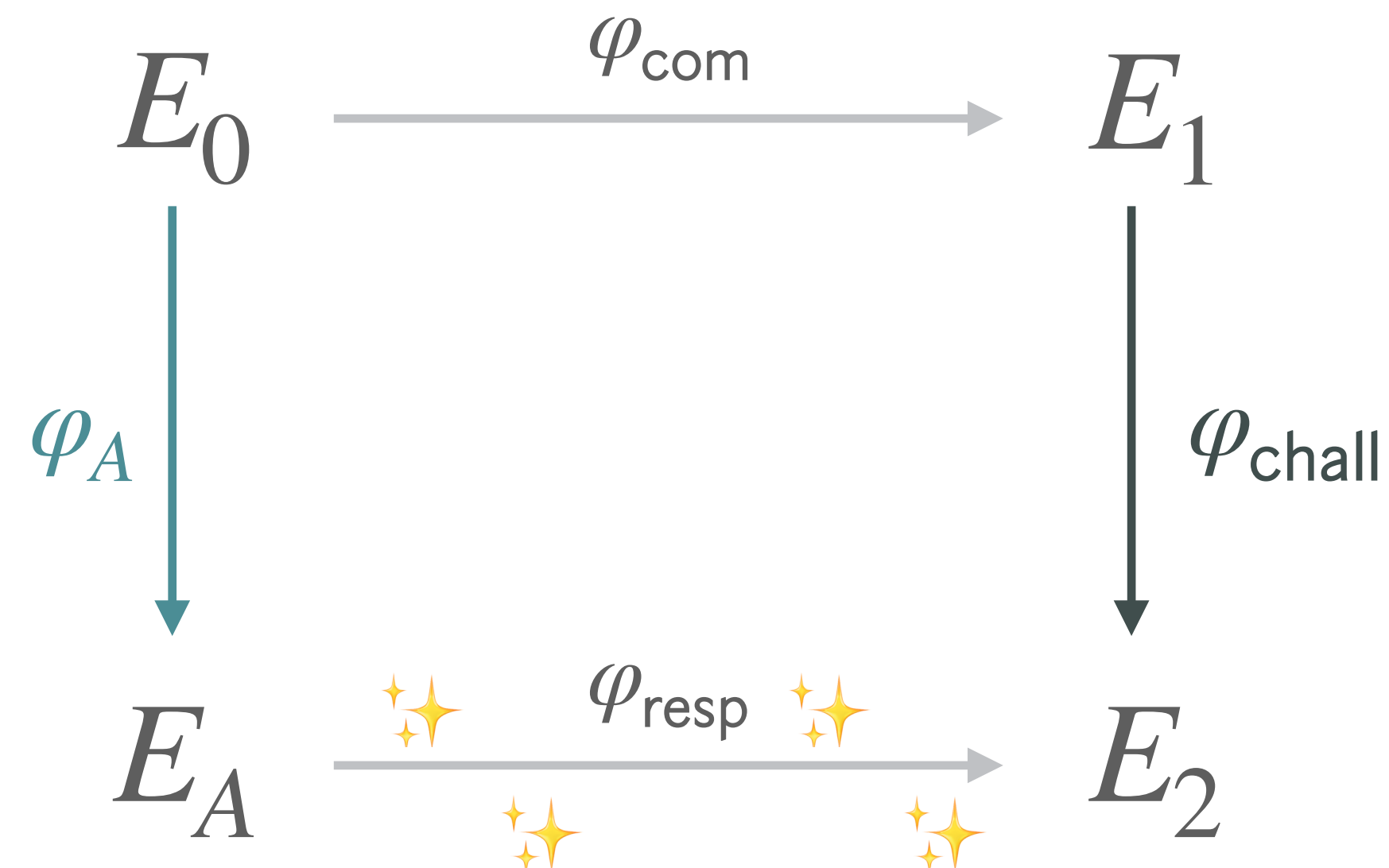
2 HD representation: E_A is known, give points P_i and $\varphi_{\text{resp}}(P_i)$

Radboud University

HD representations

instead of describing 1D isogeny $\varphi : E \to E'$ by its kernel $\ker \varphi$,
we can also describe it by $E, P_1, \ldots, P_n, \varphi(P_1), \ldots, \varphi(P_n)$, for enough points $P_i \in E$

then, with Kani's lemma & improvements, compute $\varphi(Q)$ for any other $Q \in E$

$$E_0 \xrightarrow{\varphi_{\mathsf{com}}} E_1$$

$$\varphi_A \downarrow \qquad\qquad \downarrow \varphi_{\mathsf{chall}}$$

$$E_A \xrightarrow{\varphi_{\mathsf{resp}}} E_2$$

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

2 HD representation: E_A is known, give points P_i and $\varphi_{\mathsf{resp}}(P_i)$

✔ **faster primes!**

✔ **FASTER signing!**

✔ **THE BEST security!**

Radboud University