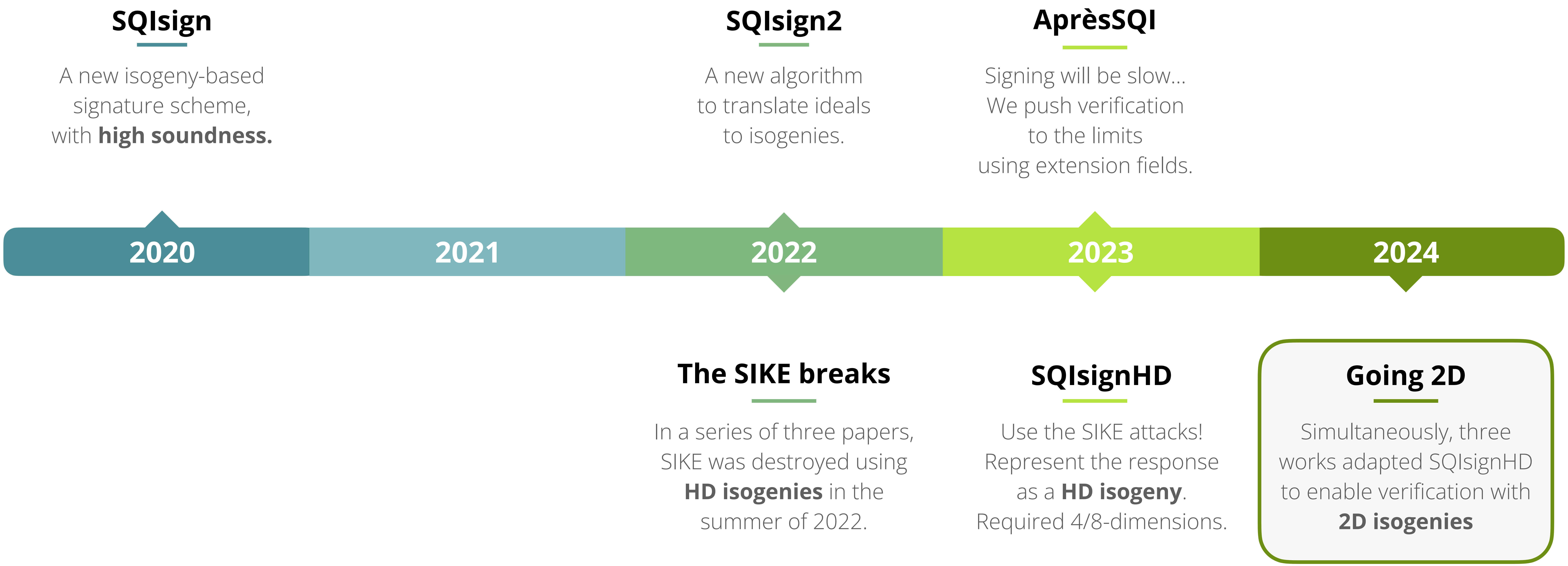
PART 4

2D Future



2020

SQIsign

A new isogeny-based signature scheme, with **high soundness.**

2021

2022

SQIsign2

A new algorithm to translate ideals to isogenies.

The SIKE breaks

In a series of three papers, SIKE was destroyed using **HD isogenies** in the summer of 2022.

2023

AprèsSQI

Signing will be slow...
We push verification to the limits using extension fields.

SQIsignHD

Use the SIKE attacks!
Represent the response as a **HD isogeny**.
Required 4/8-dimensions.

2024

Going 2D

Simultaneously, three works adapted SQIsignHD to enable verification with **2D isogenies**

SQIsign2D

Don’t do “slow” translation of ideal into blocks of 1D-isogenies (SQIsign, AprèsSQI)
Don’t do “fast” translation of ideal into slow 4D/8D isogenies (SQIsignHD)

Do use the previous section to translate ideal into 2D isogenies