PART 2

The BREAK

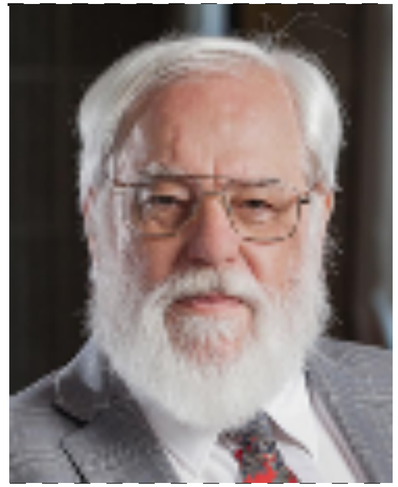
Kani's Lemma (1997)

$$\begin{array}{ccc} E_1 & \xrightarrow{\psi} & E_3 \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi'} \\ E_2 & \xrightarrow{\psi'} & E_4 \end{array}$$

if $\deg\varphi = \deg\varphi'$
and $\deg\psi = \deg\psi'$
then this square of
1-dimensional isogenies

is associated to

a **2-dimensional isogeny**
$\Phi : E_2 \times E_3 \to E_1 \times E_4$



1D isogeny

if we know $\ker\varphi$,
then we can compute
$\varphi : E \to E'$ and $\varphi(P)$

2D kernel

the kernel of 2D-iso Φ
is given by images $\varphi(P), \psi(P)$
for $P \in E_1$ of order $\deg\varphi + \deg\psi$

2D isogeny

if we know $\deg\varphi$ and $\deg\psi$
and we know these $\varphi(P)$, $\psi(P)$,
compute $\Phi : E_2 \times E_3 \to E_1 \times E_4$

PART 2

The BREAK

SQIsign

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

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.