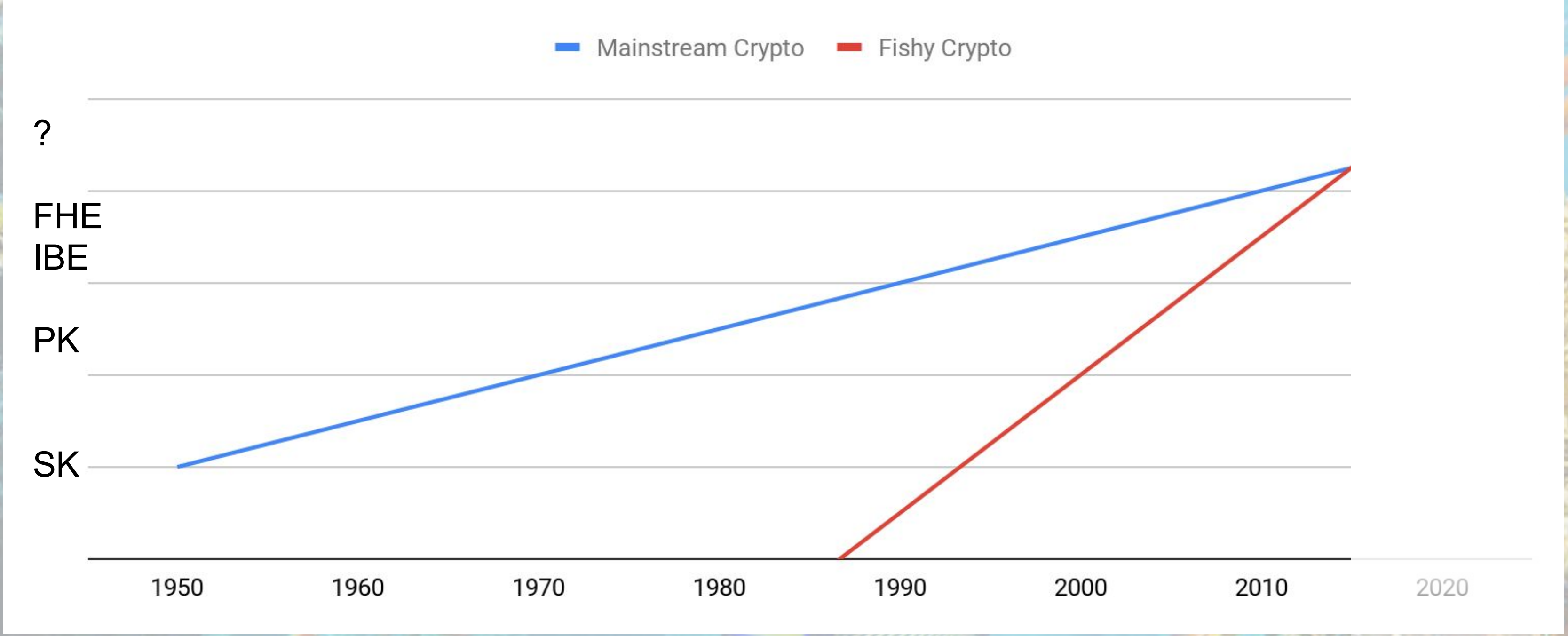
Advancing the state of the art of fishy cryptography

Ward Beullens, Thorsten Kleinjung & Frederik Vercauteren

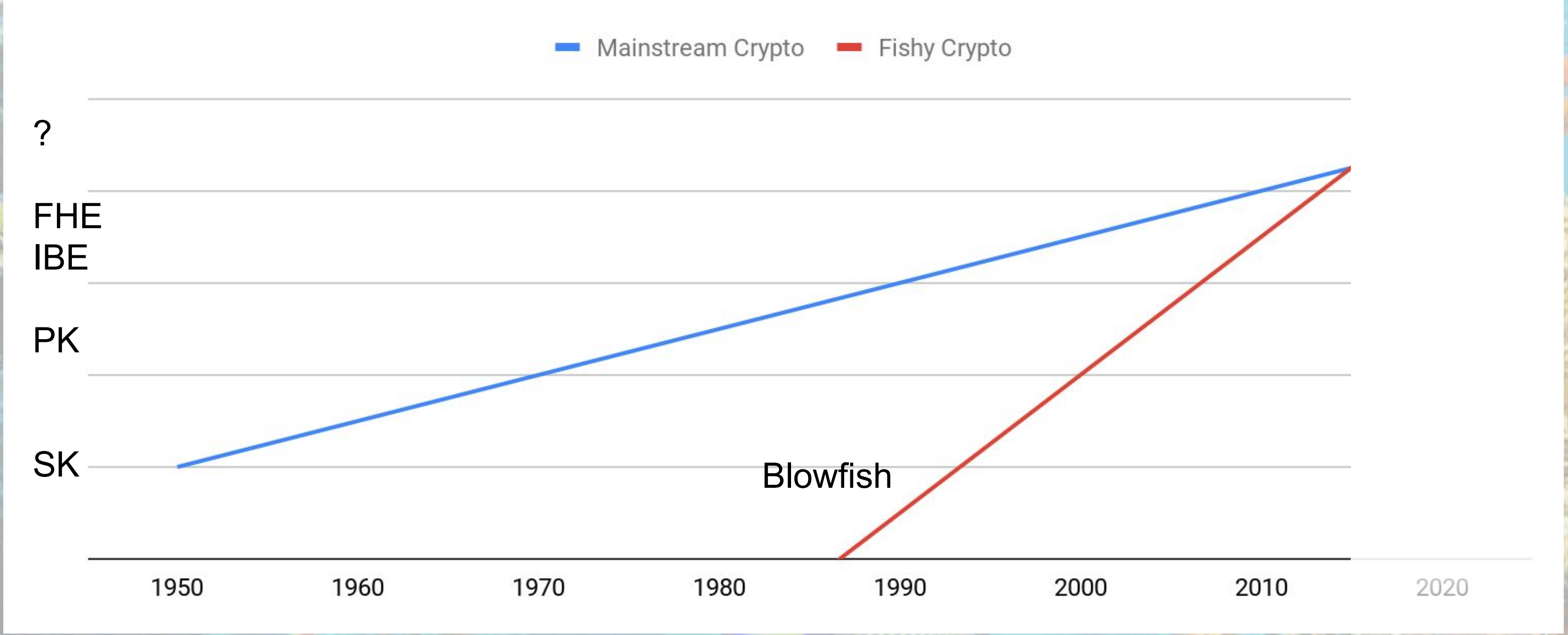
Introduction:

Fishy cryptography is quickly catching up with mainstream cryptography



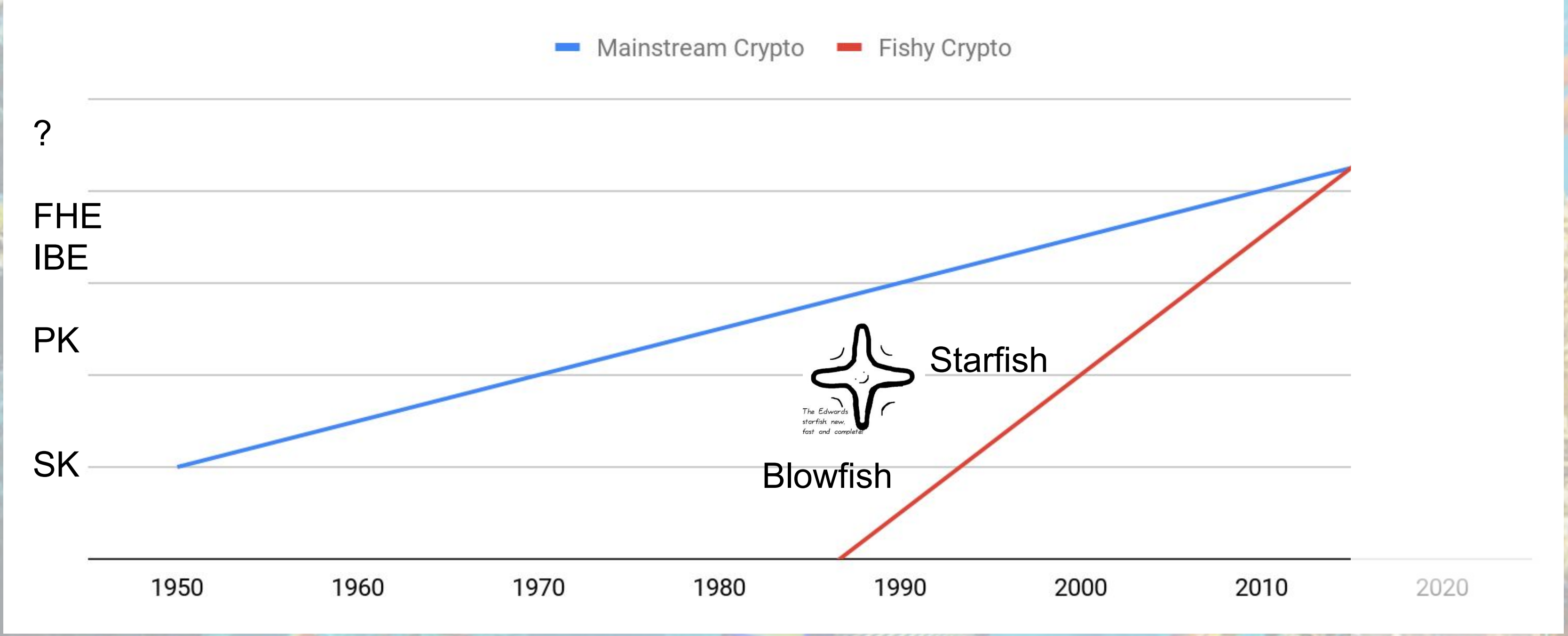
Introduction:

Fishy cryptography is quickly catching up with mainstream cryptography



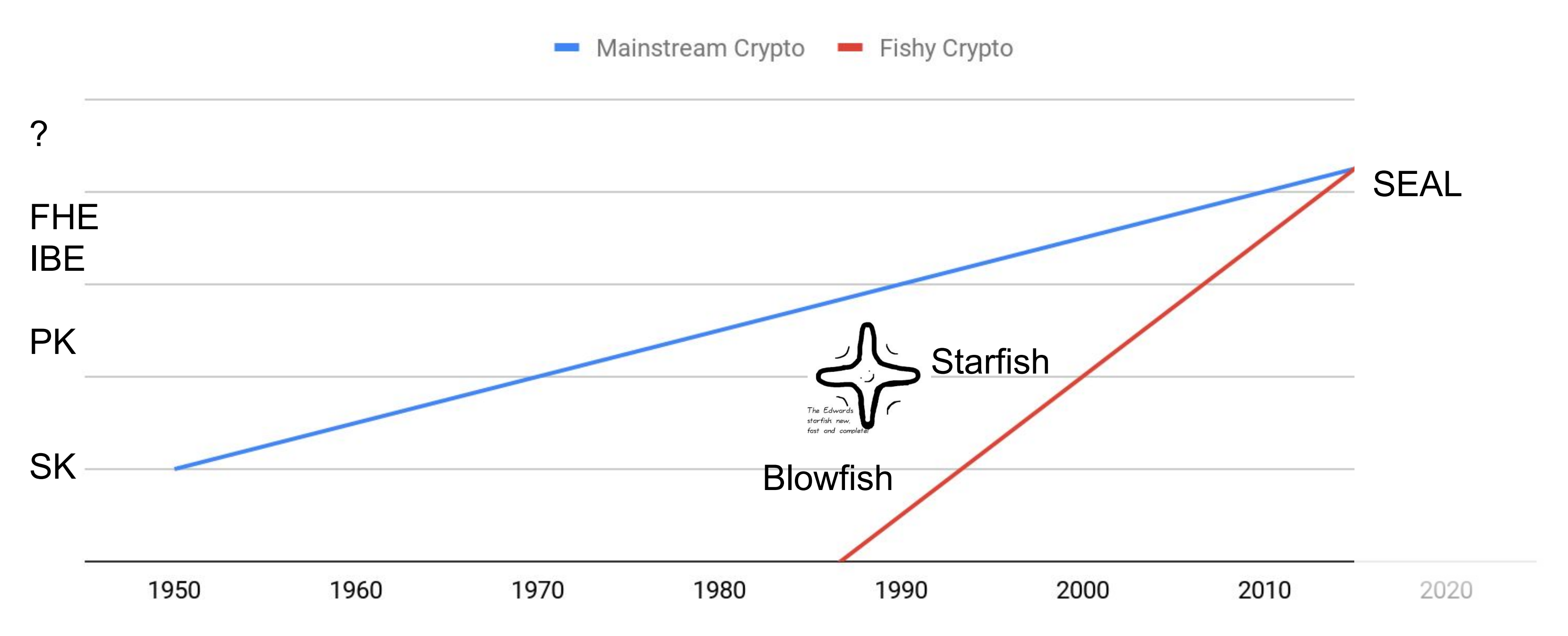
Introduction:

Fishy cryptography is quickly catching up with mainstream cryptography



Introduction:

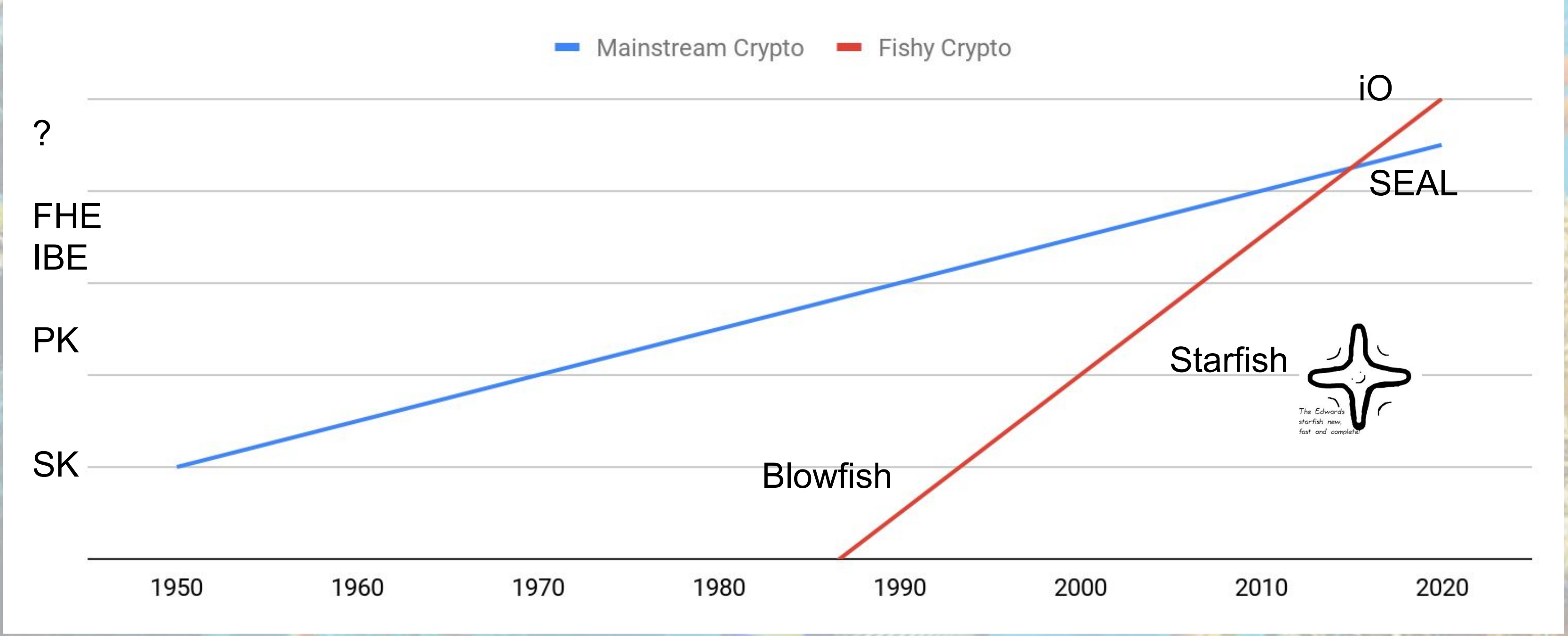
Fishy cryptography is quickly catching up with mainstream cryptography



Introduction:

has surpassed

Fishy cryptography is ~~quickly catching up~~ with mainstream cryptography

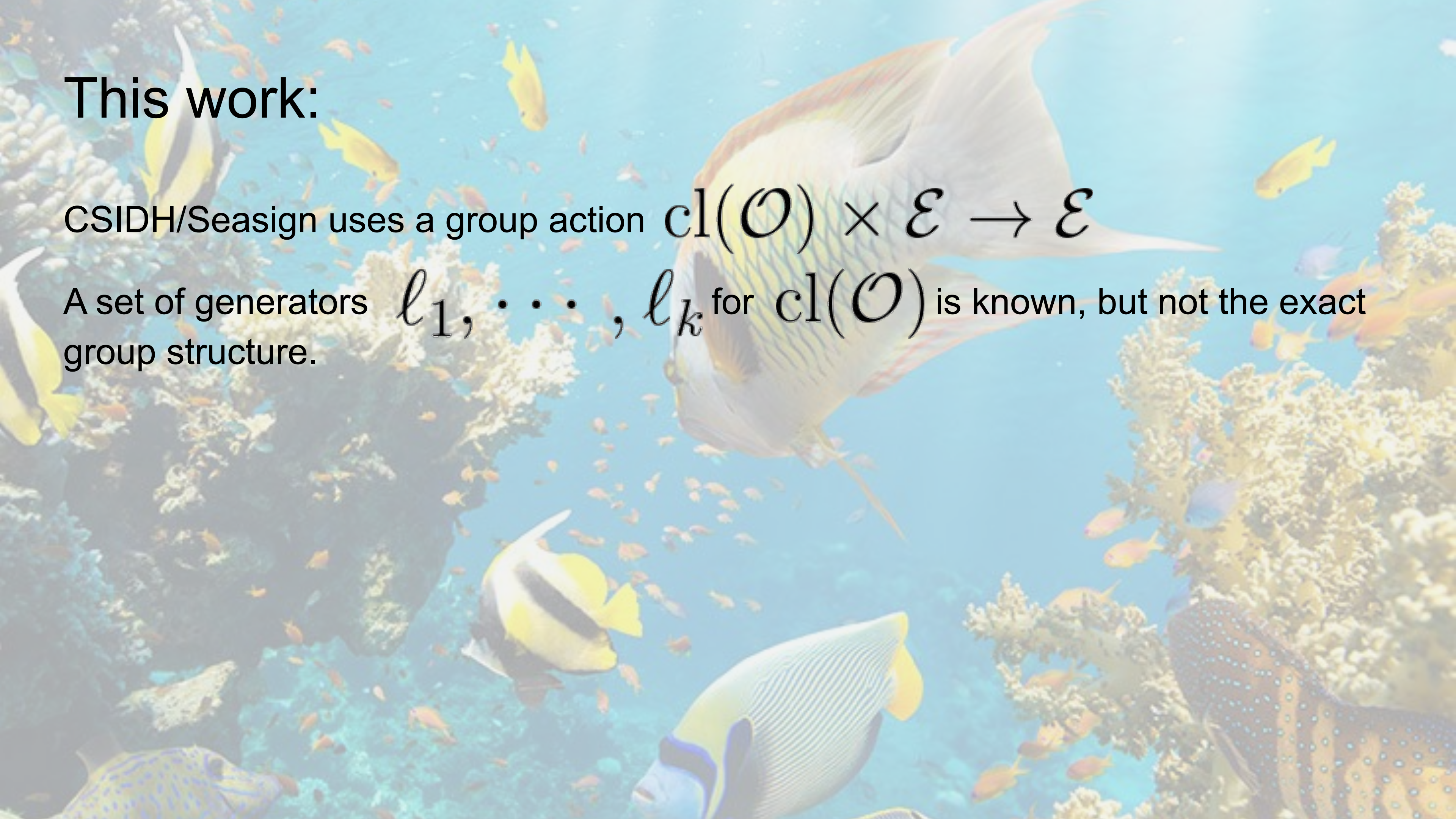


Shores algorithm* kills all fishy public key crypto

Important problem:

Construct a fishy post-quantum signature scheme

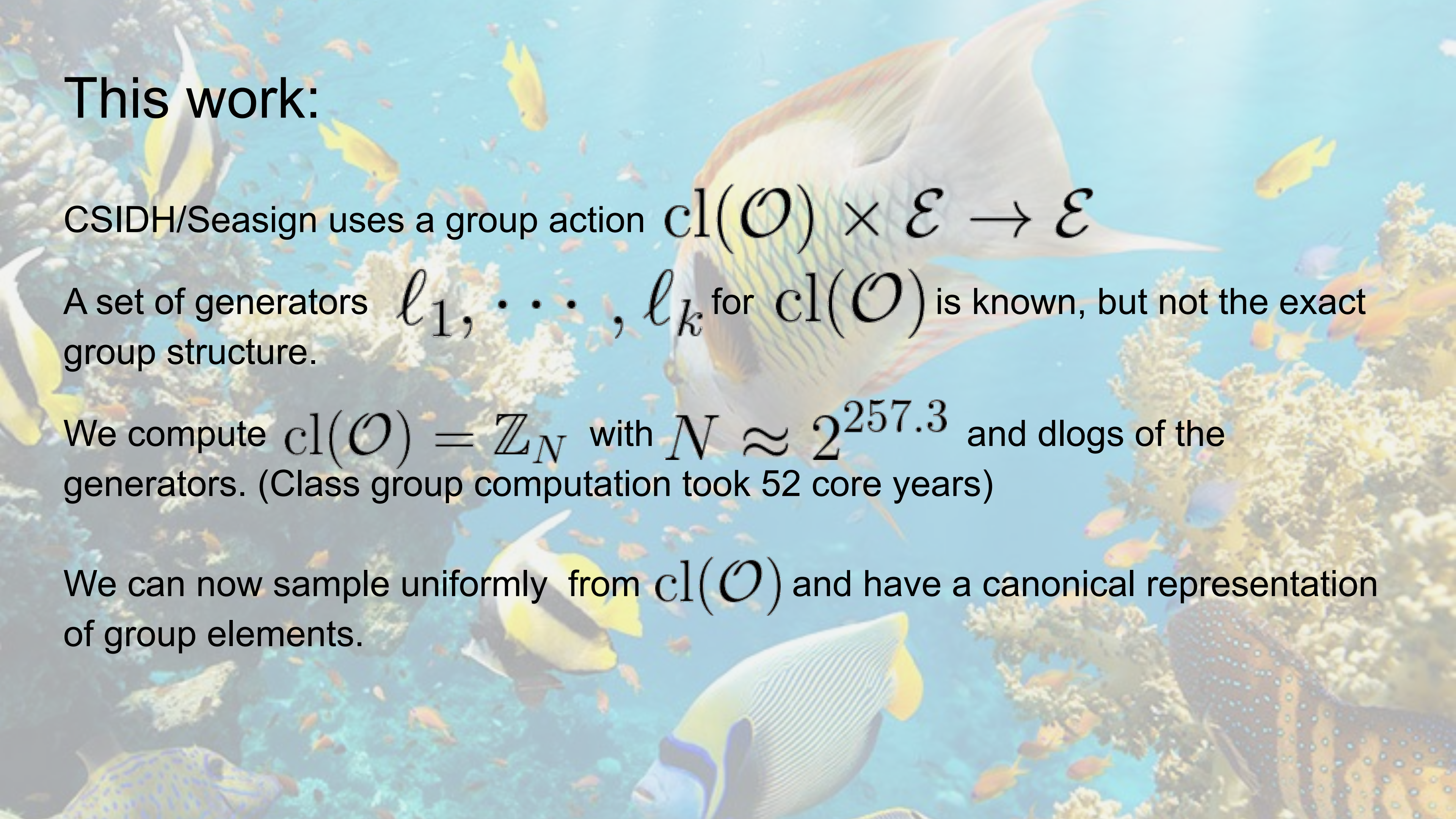
*Joke sponsored by Lorenz Panny



This work:

CSIDH/Seasign uses a group action $\mathrm{cl}(\mathcal{O}) \times \mathcal{E} \to \mathcal{E}$

A set of generators $\ell_1, \cdots, \ell_k$ for $\mathrm{cl}(\mathcal{O})$ is known, but not the exact group structure.



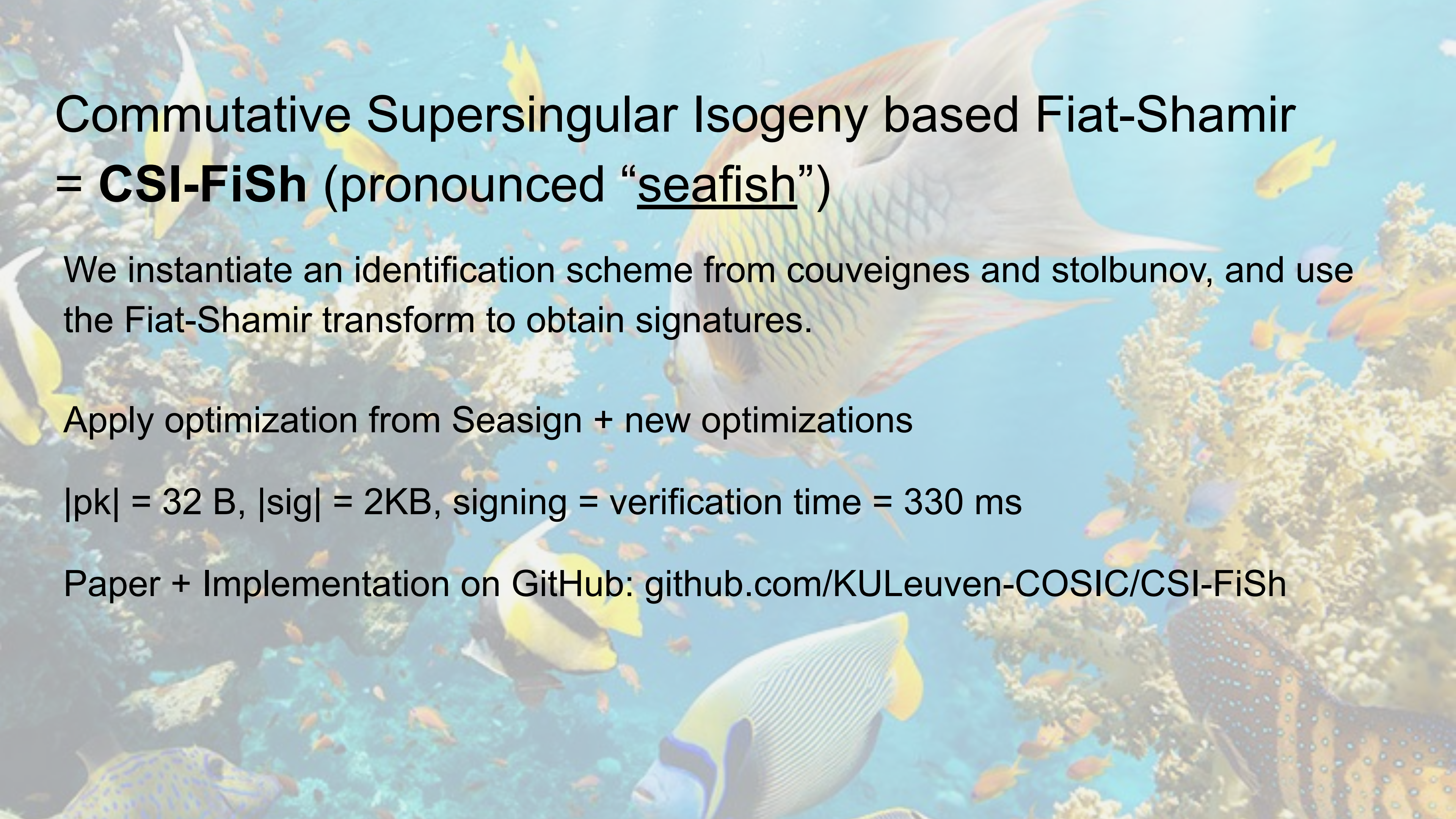
This work:

CSIDH/Seasign uses a group action $\mathrm{cl}(\mathcal{O}) \times \mathcal{E} \to \mathcal{E}$

A set of generators $\ell_1, \cdots, \ell_k$ for $\mathrm{cl}(\mathcal{O})$ is known, but not the exact group structure.

We compute $\mathrm{cl}(\mathcal{O}) = \mathbb{Z}_N$ with $N \approx 2^{257.3}$ and dlogs of the generators. (Class group computation took 52 core years)

We can now sample uniformly from $\mathrm{cl}(\mathcal{O})$ and have a canonical representation of group elements.



Commutative Supersingular Isogeny based Fiat-Shamir = **CSI-FiSh** (pronounced “seafish”)

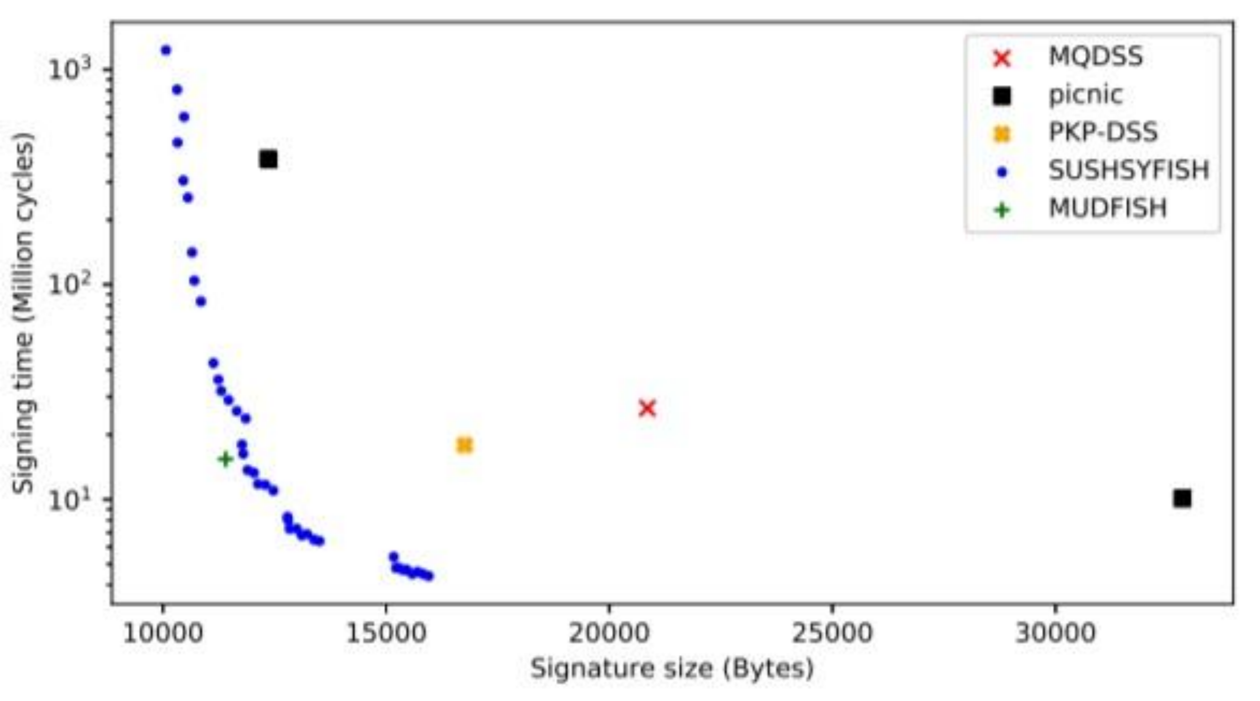
We instantiate an identification scheme from couveignes and stolbunov, and use the Fiat-Shamir transform to obtain signatures.

Apply optimization from Seasign + new optimizations

|pk| = 32 B, |sig| = 2KB, signing = verification time = 330 ms

Paper + Implementation on GitHub: github.com/KULeuven-COSIC/CSI-FiSh

other work:



github.com/WardBeullens/FISH