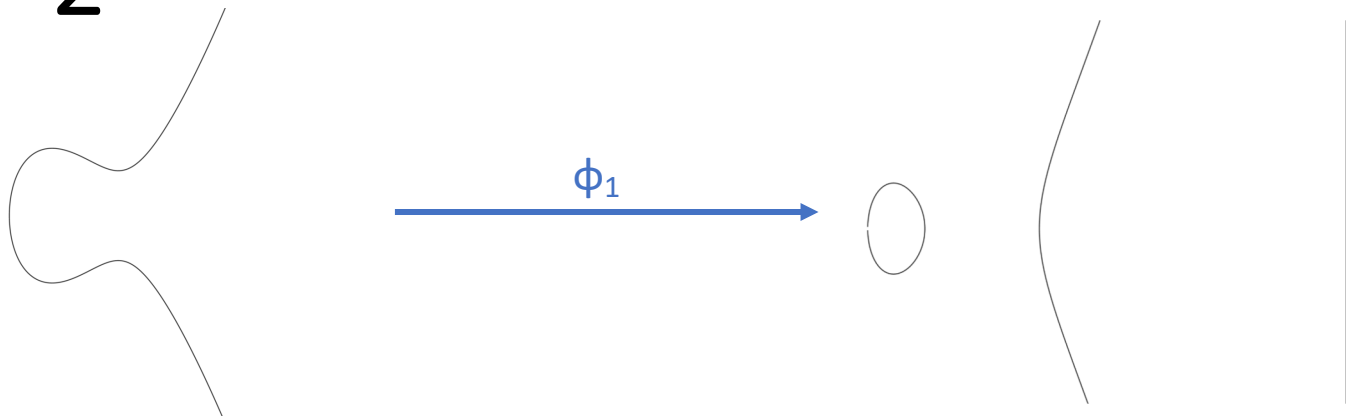
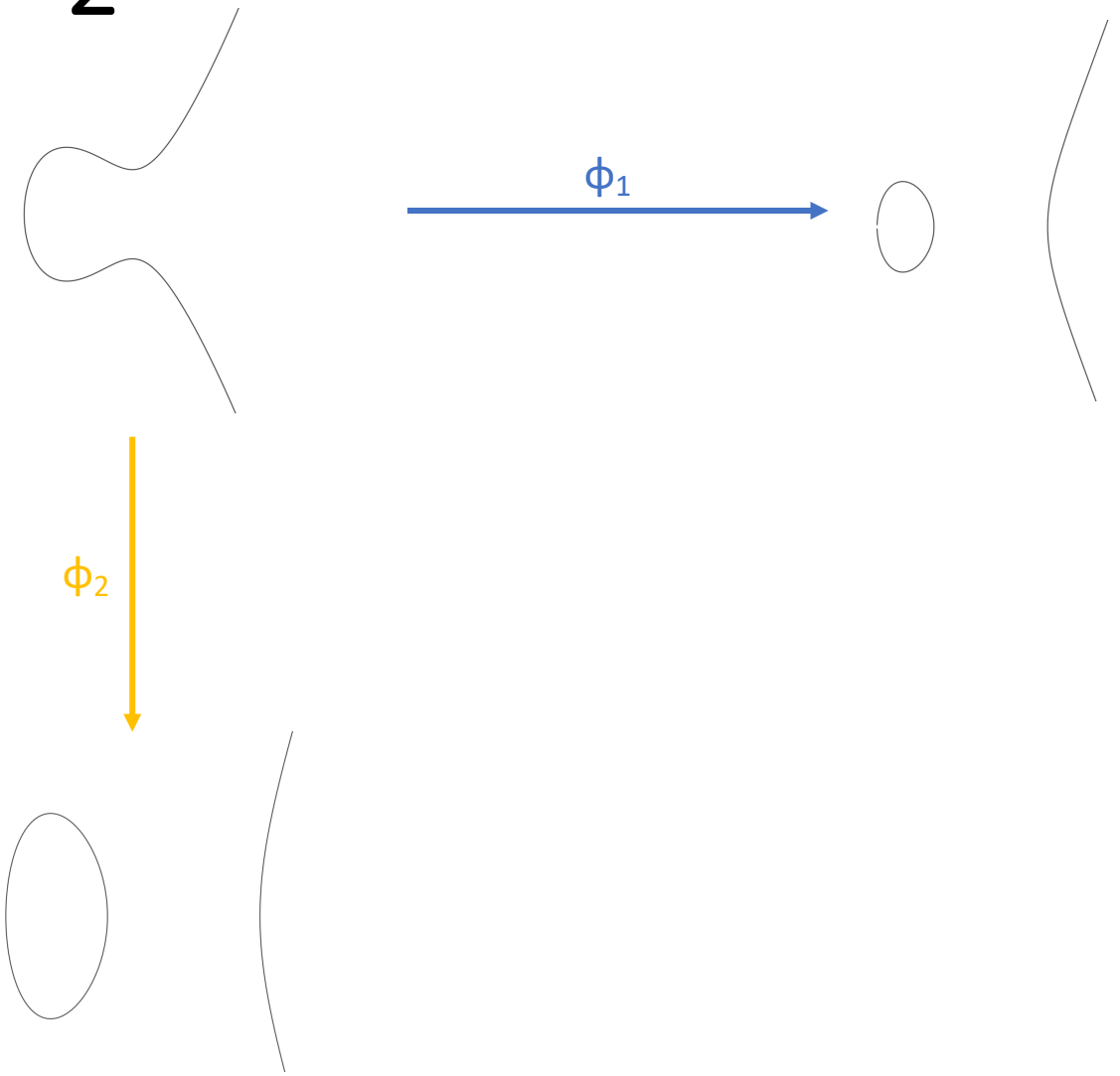
Towards a Quantum-Resistant Weak Verifiable Delay Function

Thomas Decru, Luciano Maino and Antonio Sanso

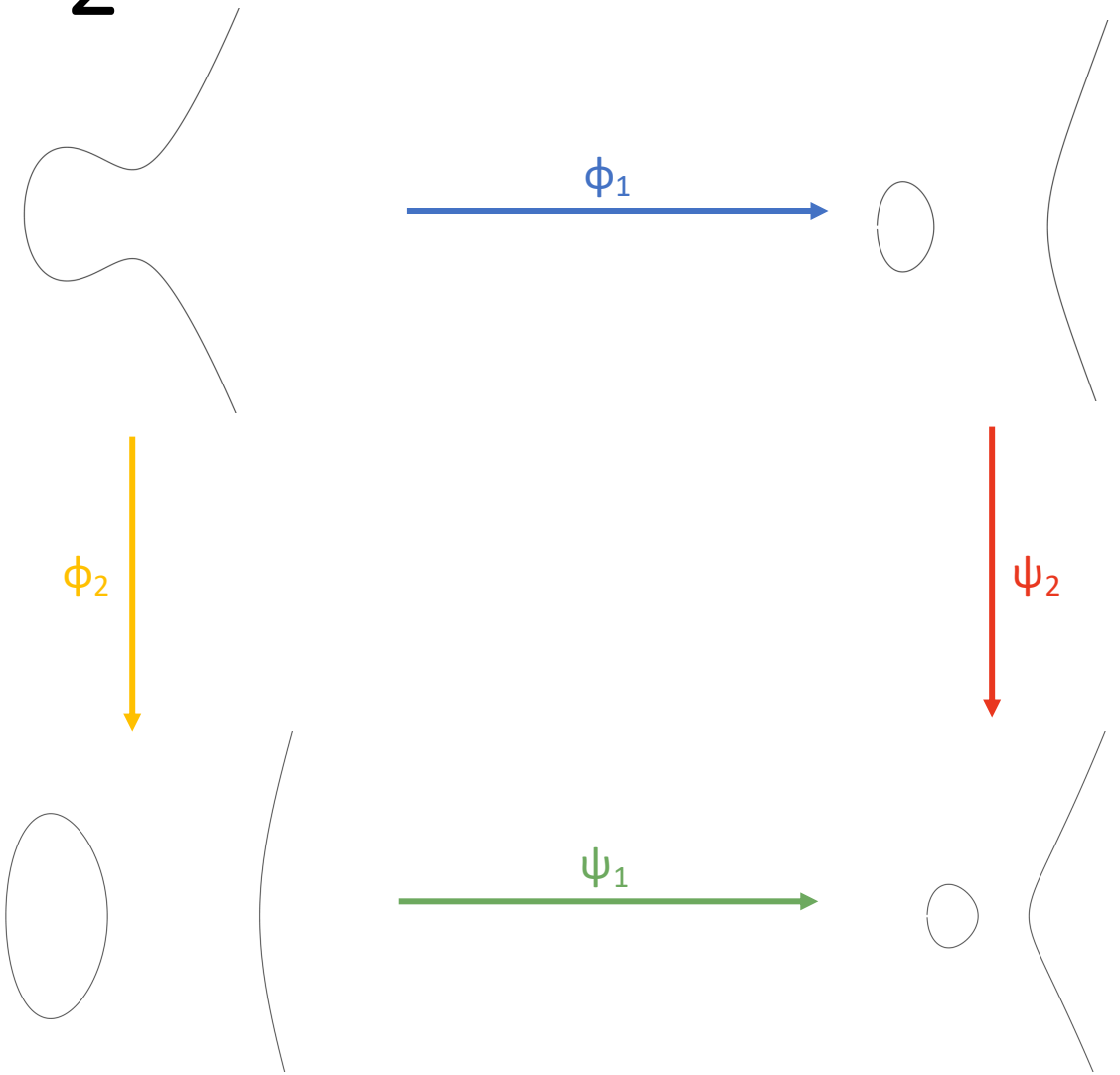
Isogenies in dimension 2



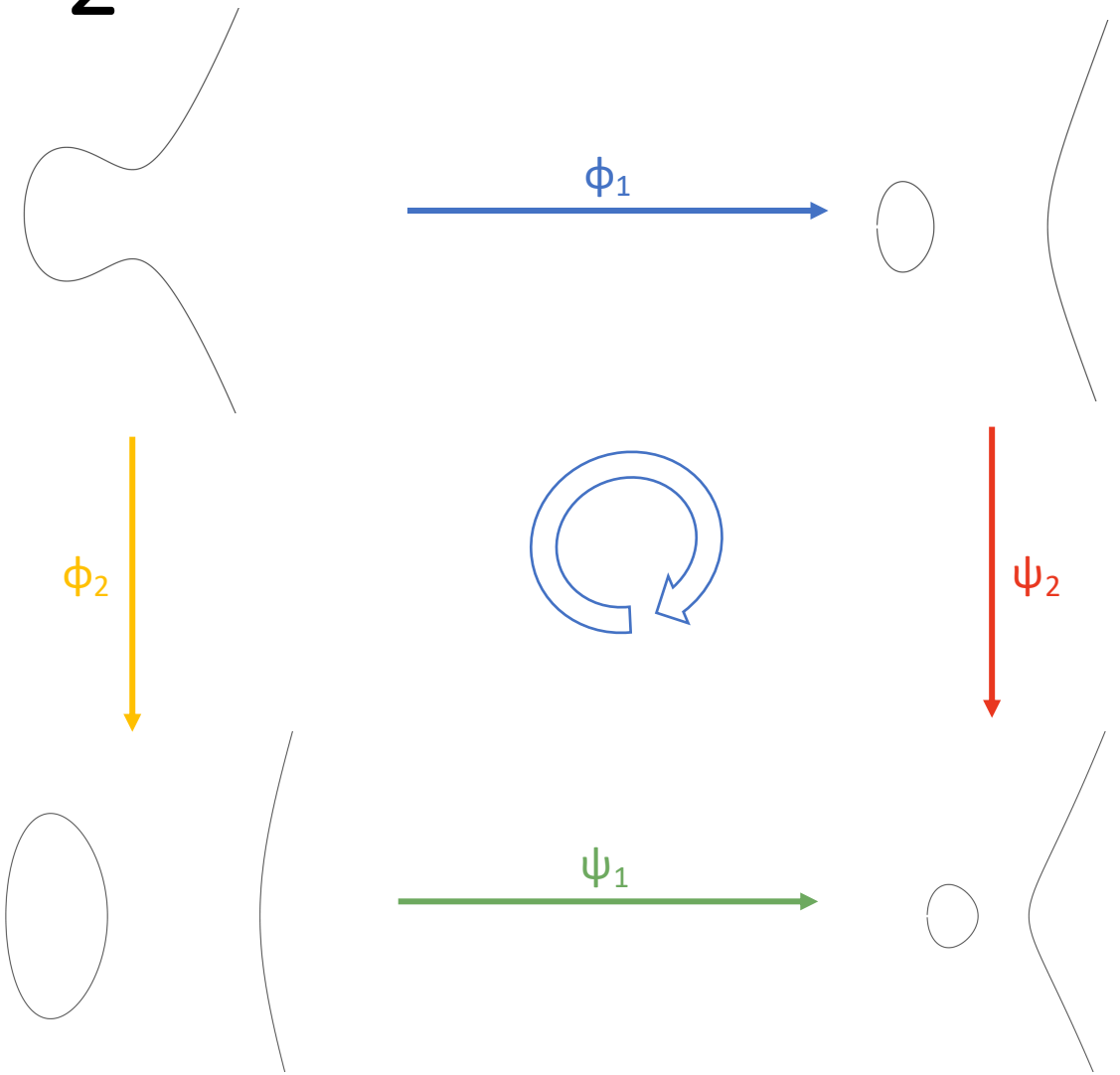
Isogenies in dimension 2



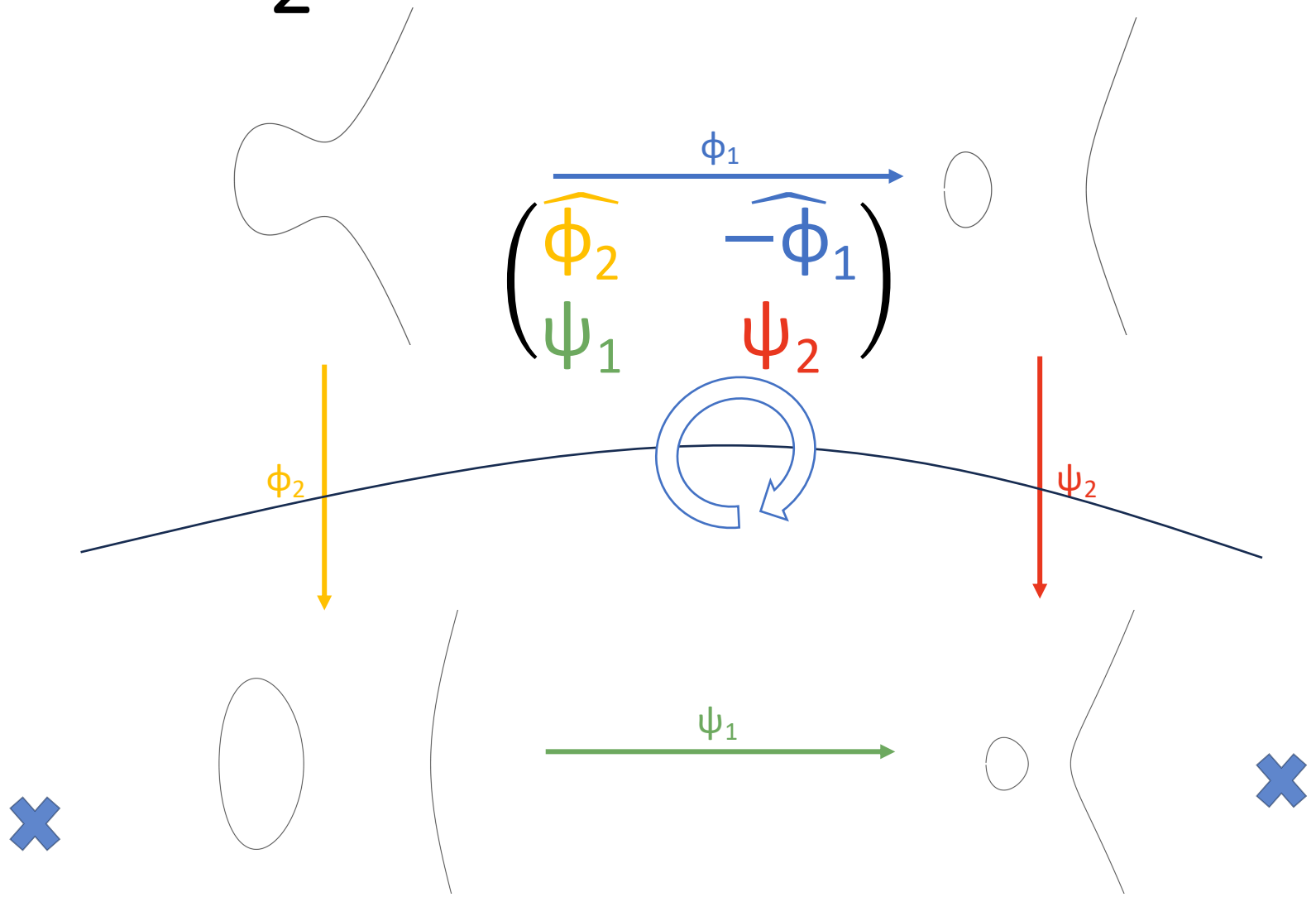
Isogenies in dimension 2



Isogenies in dimension 2



Isogenies in dimension 2



Isogenies in dimension 2

Requirements:

- $\deg(\phi_1) = \deg(\psi_1)$
- $\deg(\phi_2) = \deg(\psi_2)$
- $N = \deg(\phi_1) + \deg(\phi_2)$ is smooth - in practice, $N = 2^n$
- evaluation of ϕ_1 and ϕ_2 at the N -torsion

Verifiable Delay Functions

(λ, t)

Setup



Eval





Verify

$\{True, False\}$

Verifiable Delay Functions

Properties

- **Correctness:** an honest metamorphosis will always pass **Verify**
- **Soundness:** given a caterpillar, we can't find another butterfly that passes **Verify**
- **Sequentiality:** metamorphosis can't happen faster than t

Weak VDF: more parallel capabilities

Our VDF

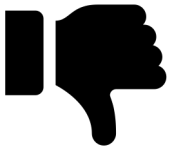
General Idea:

- Compute an isogeny ϕ between elliptic curves that requires a huge computation
- Verify ϕ via an efficient two-dimensional isogeny

Hard-to-compute isogeny:

- Kernel generator defined over big extension field
- Large prime degree

Verification of this hard-to-compute isogeny:
We cannot check that the kernel of this isogeny has been honestly generated



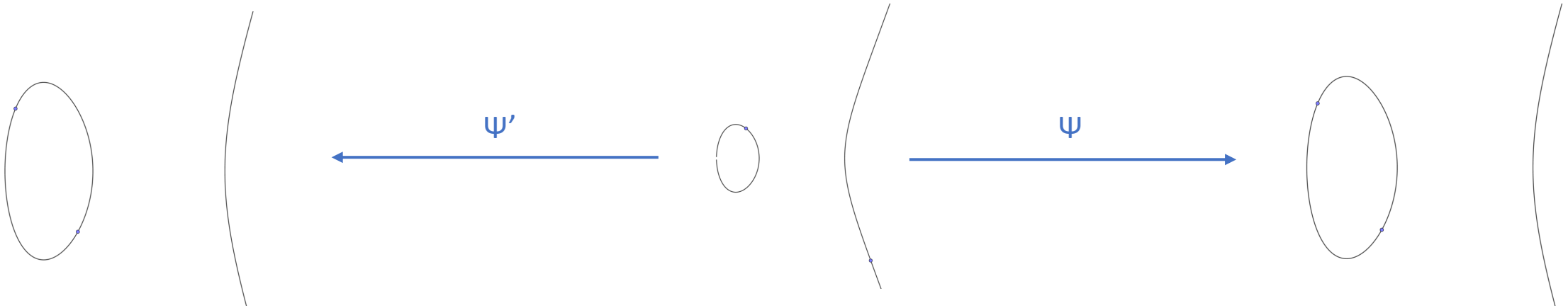
Skipping the kernel check

Solution:
We can restrict ourselves to isogenies defined over the prime field F_p - so called horizontal isogenies
There are only two horizontal isogenies of (certain) prime degree.

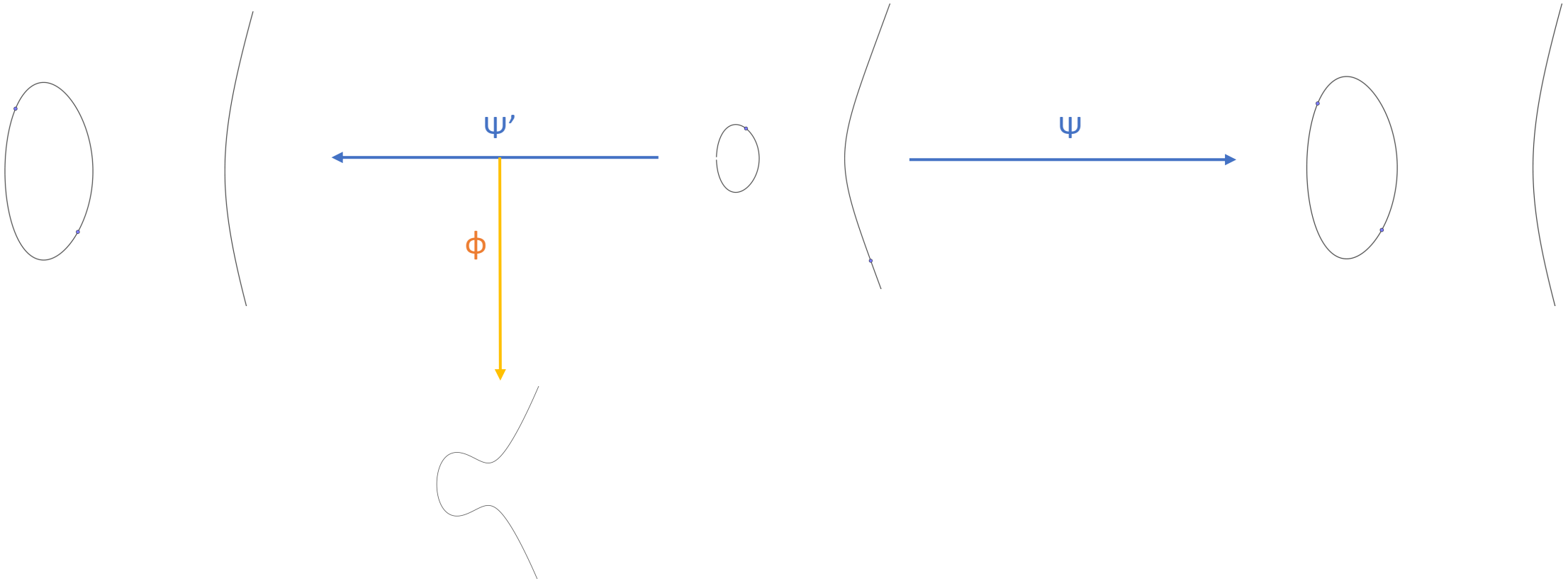
Historical note:
Horizontal isogenies are the isogenies underlying CSIDH

Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J. (2018). CSIDH: An Efficient Post-Quantum Commutative Group Action. In: Peyrin, T., Galbraith, S. (eds) Advances in Cryptology – ASIACRYPT 2018. ASIACRYPT 2018. Lecture Notes in Computer Science, vol 11274. Springer, Cham. https://doi.org/10.1007/978-3-030-03332-3_15

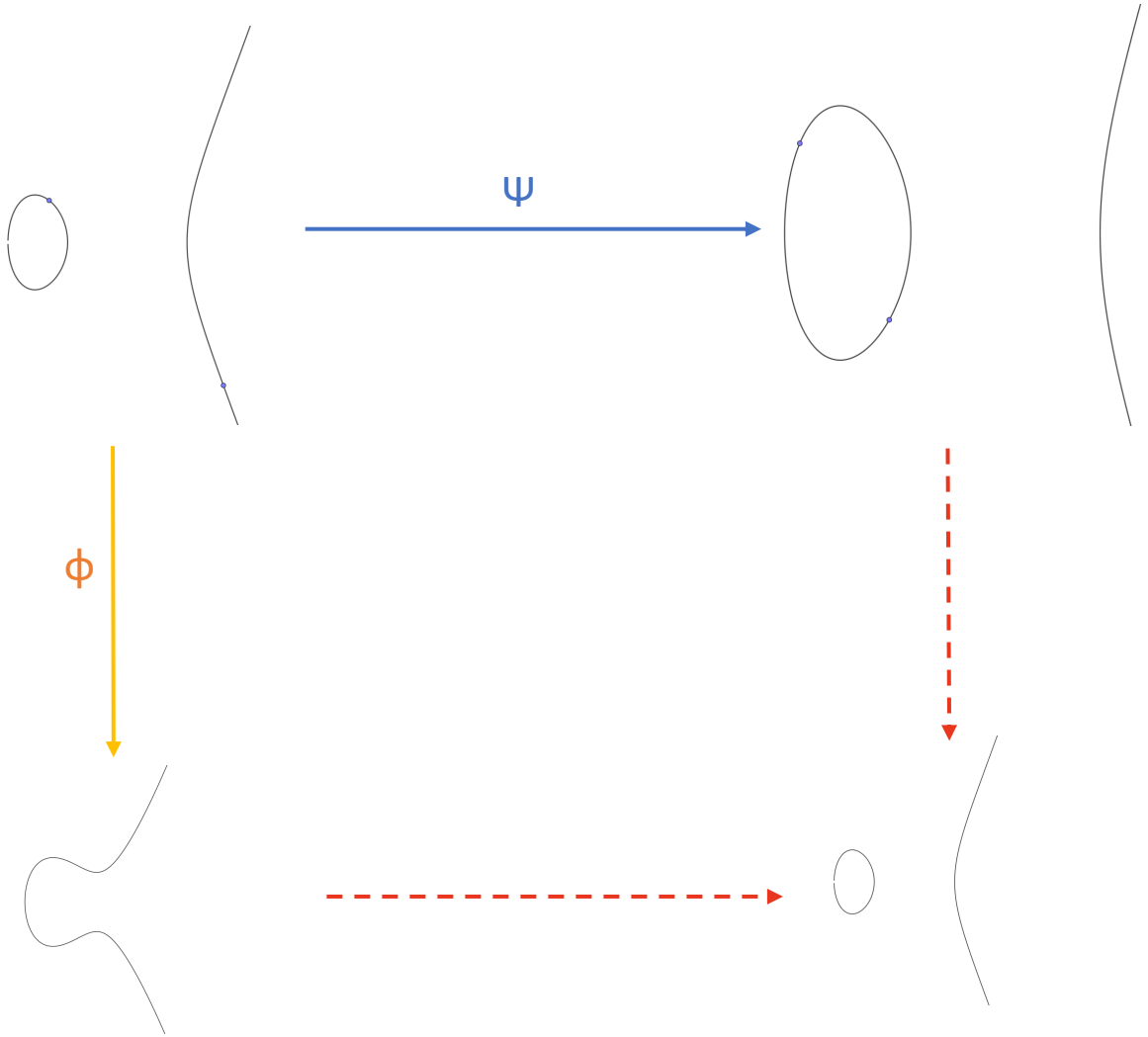
Our VDF - Eval



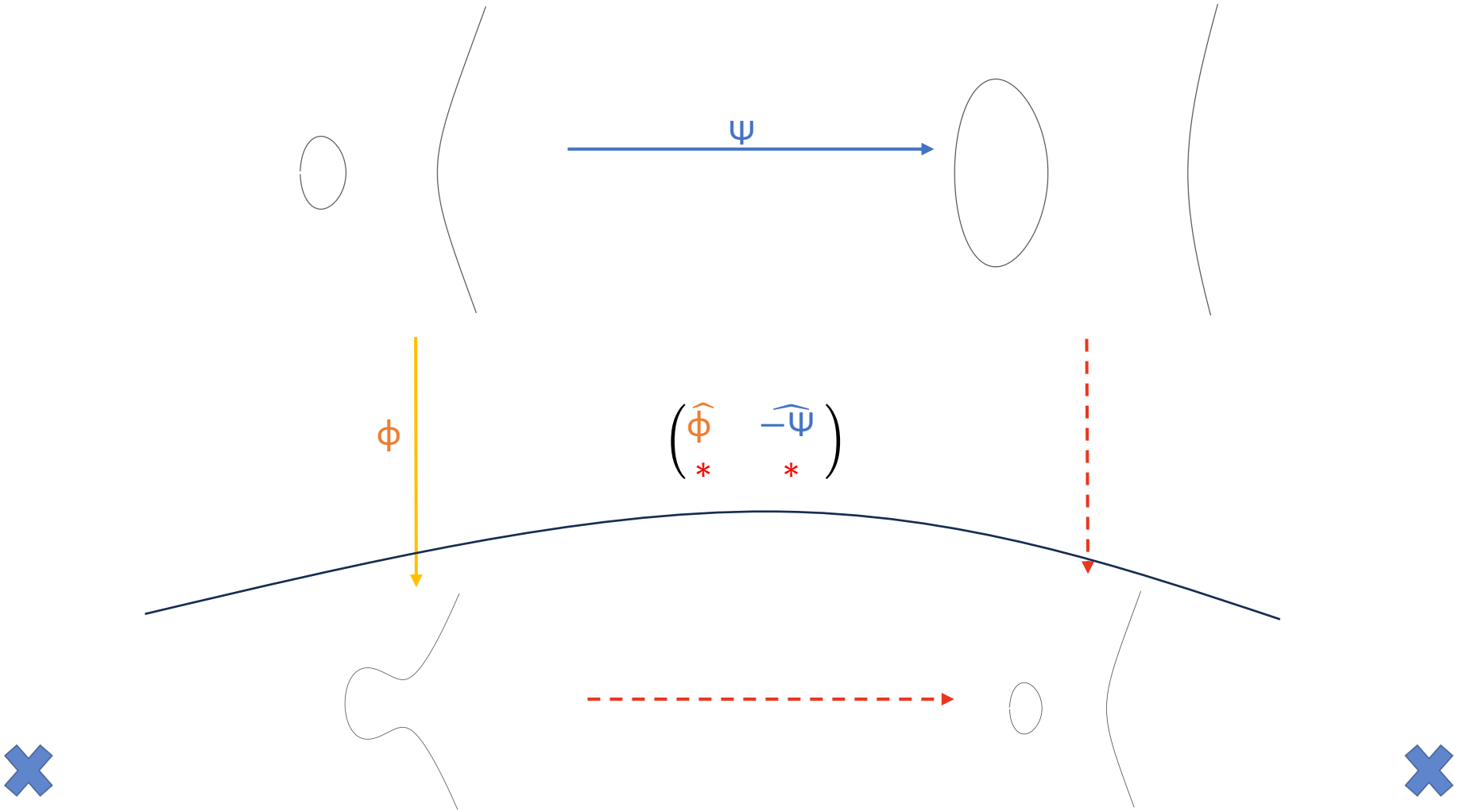
Our VDF - Verify



Our VDF - Verify



Our VDF - Verify



Conclusions

Limitations:

- The endomorphism ring of the input curve must be unknown
- The size of p must be quite big to prevent quantum attacks
- Significant parallelism required in Eval

Strengths:

- First completely algebraic quantum-resistant VDF
- Useful framework, e.g. VRF [1]
- Constructive application of SIDH attacks
- Expected fast verification

[1] Leroux, A., Verifiable random function from the Deuring correspondence and higher dimensional isogenies. ePrint archive