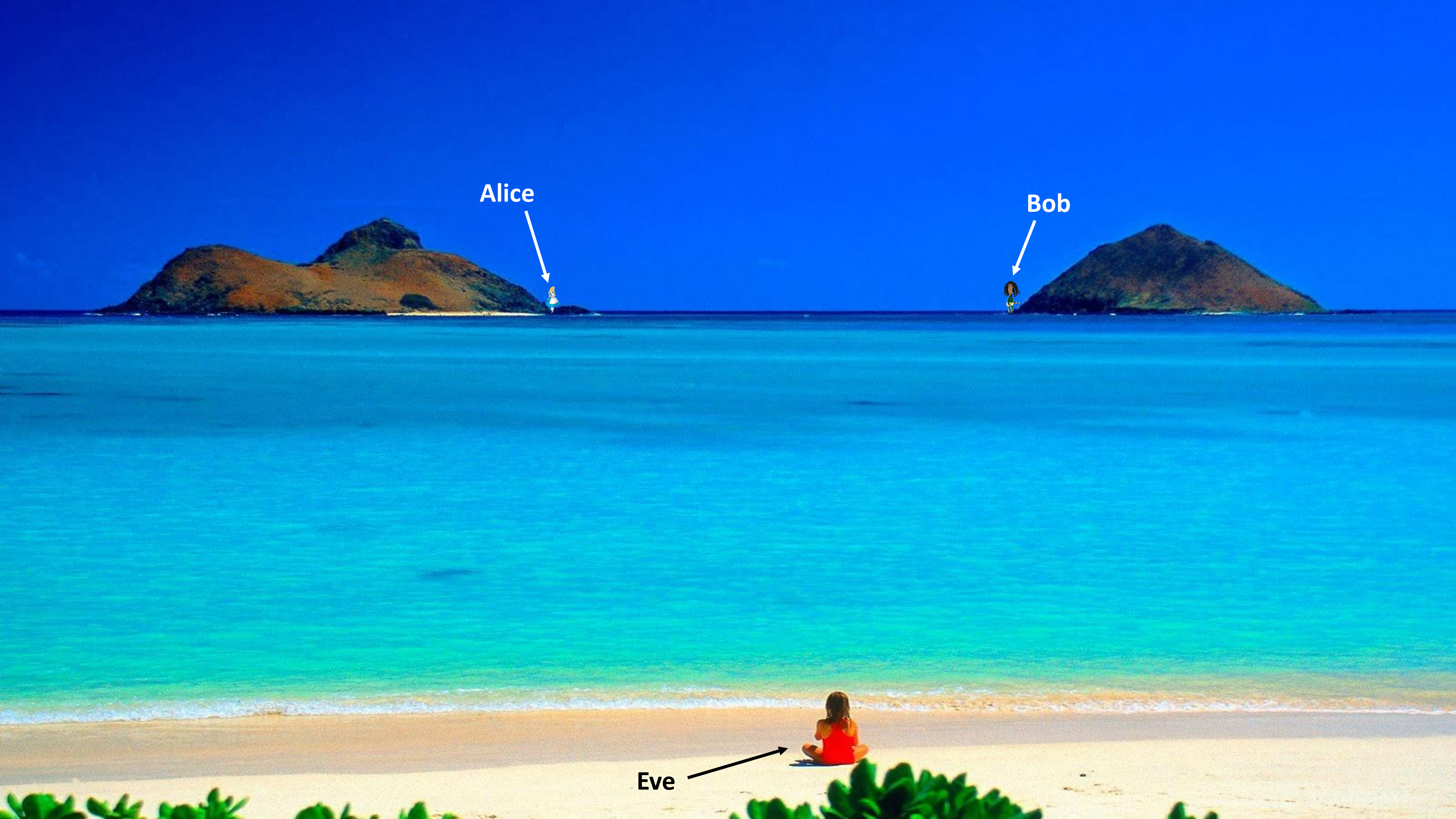
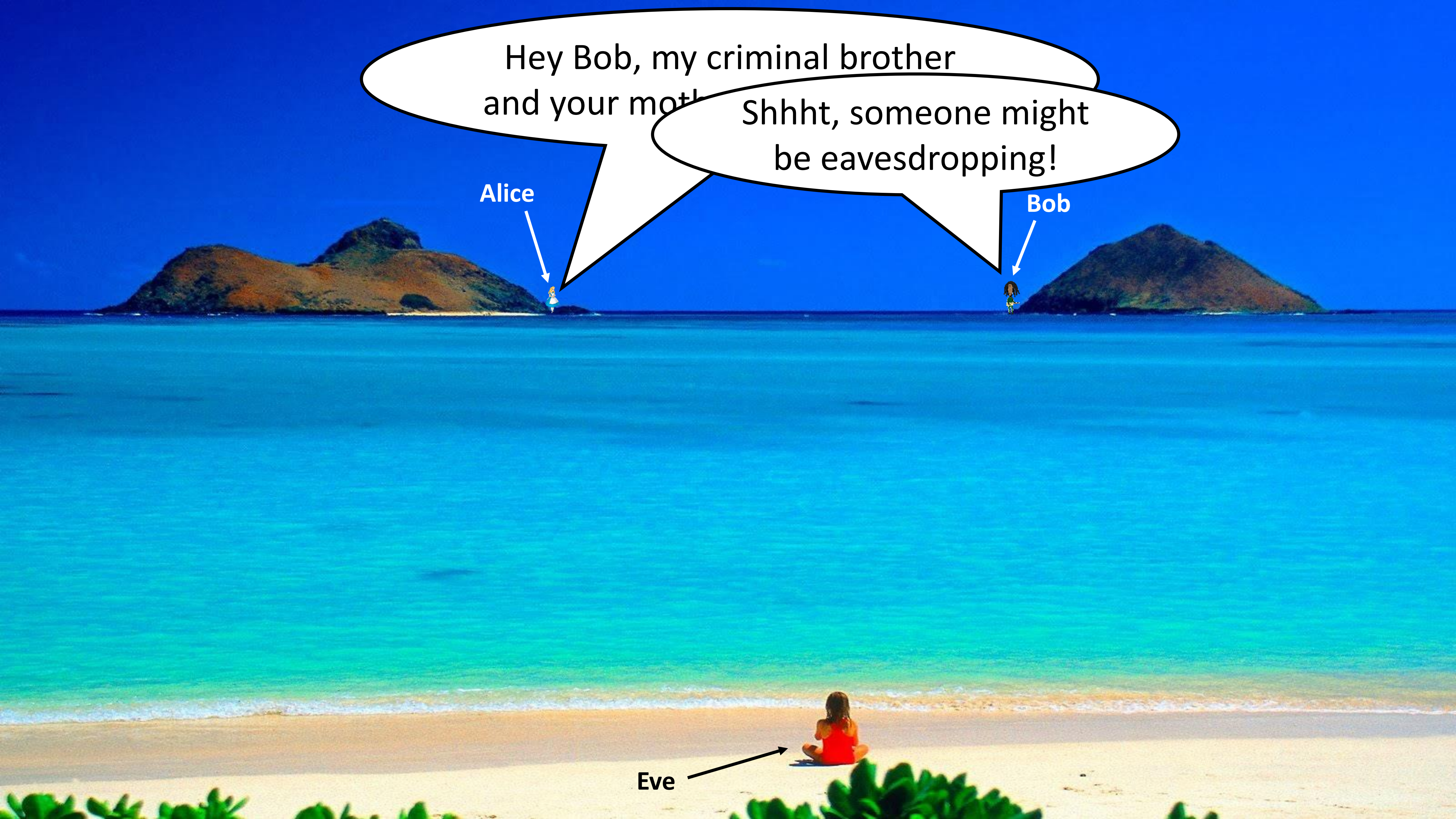
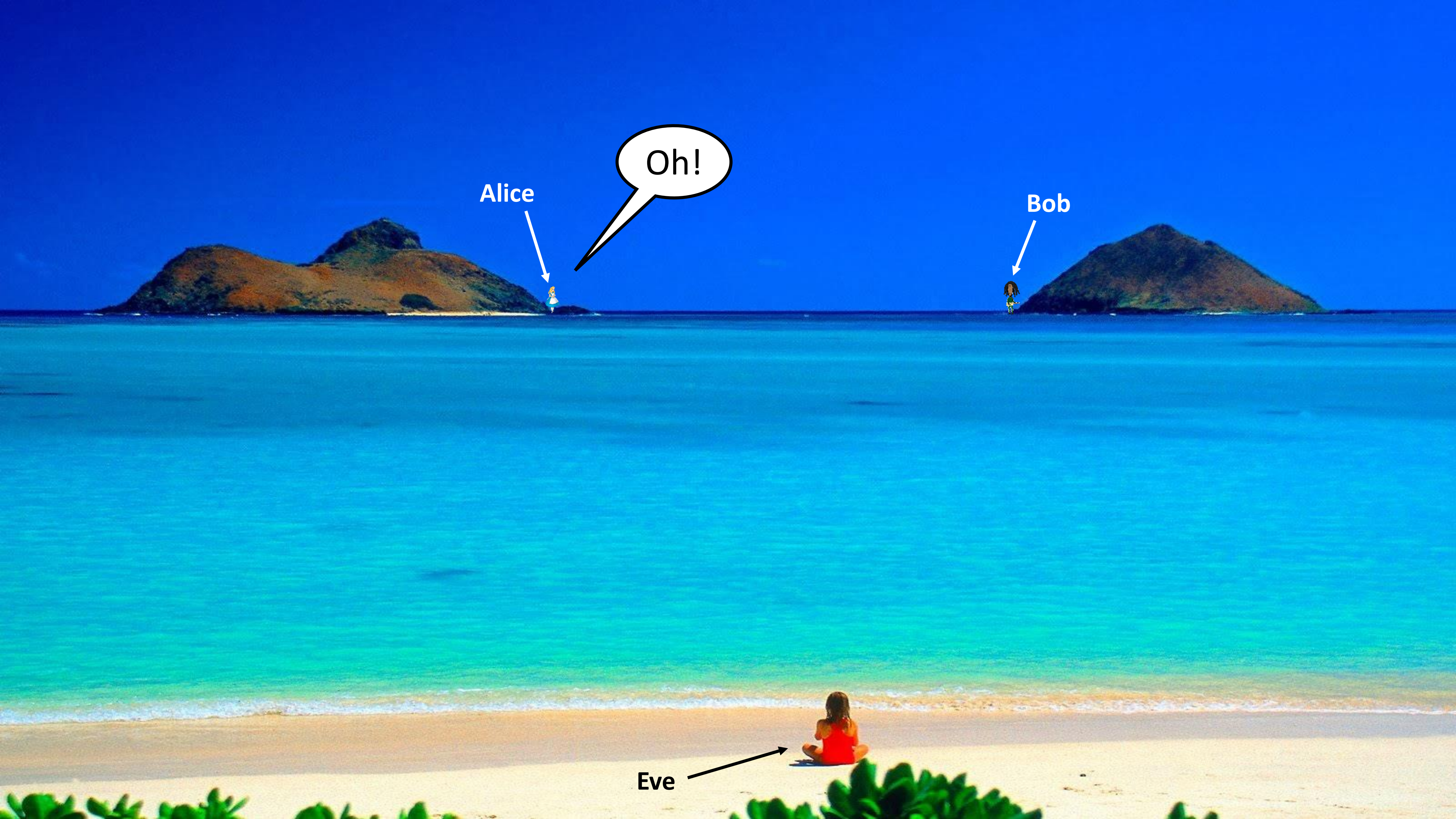
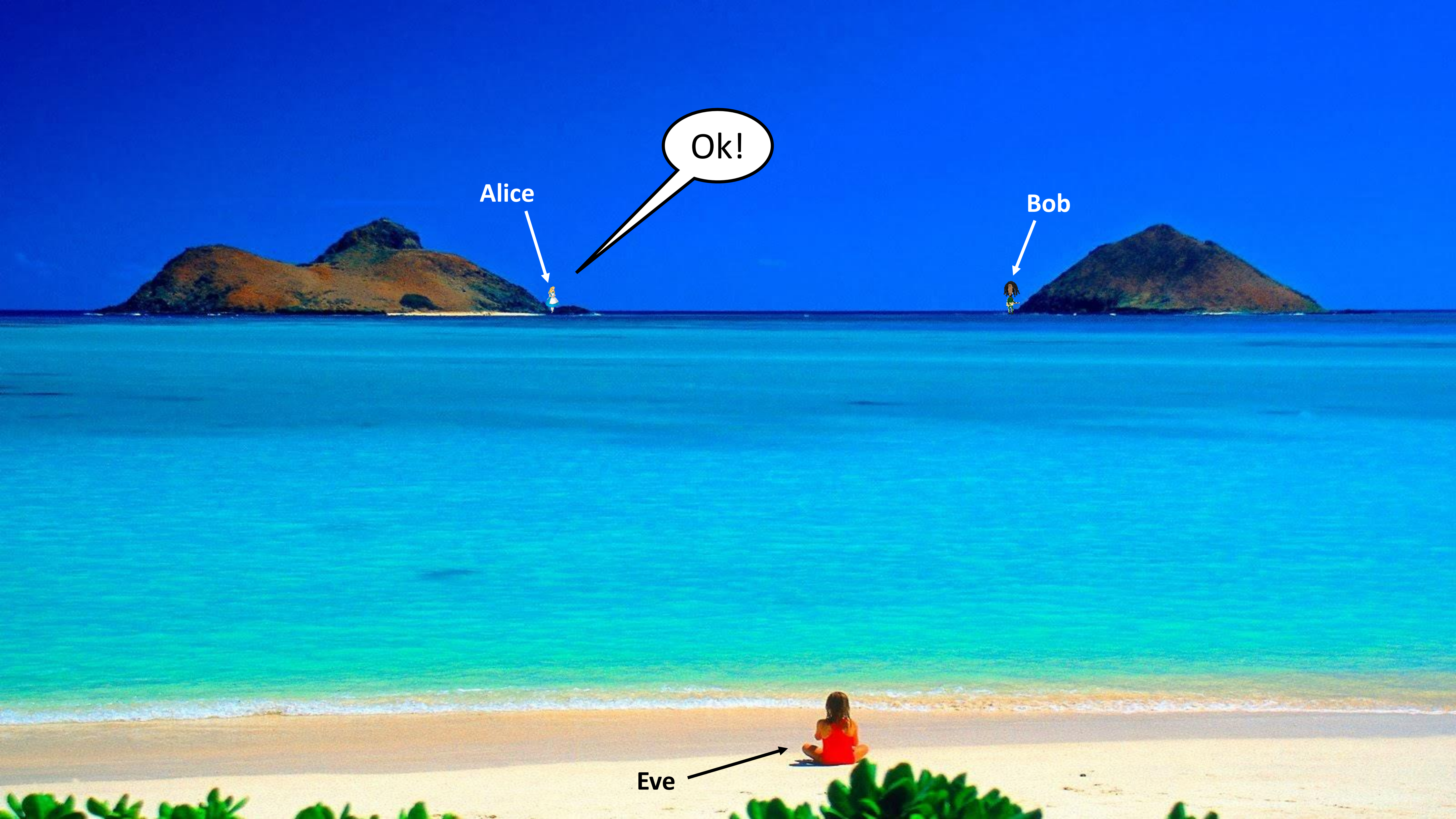
CSIDH ['si:,saɩd]

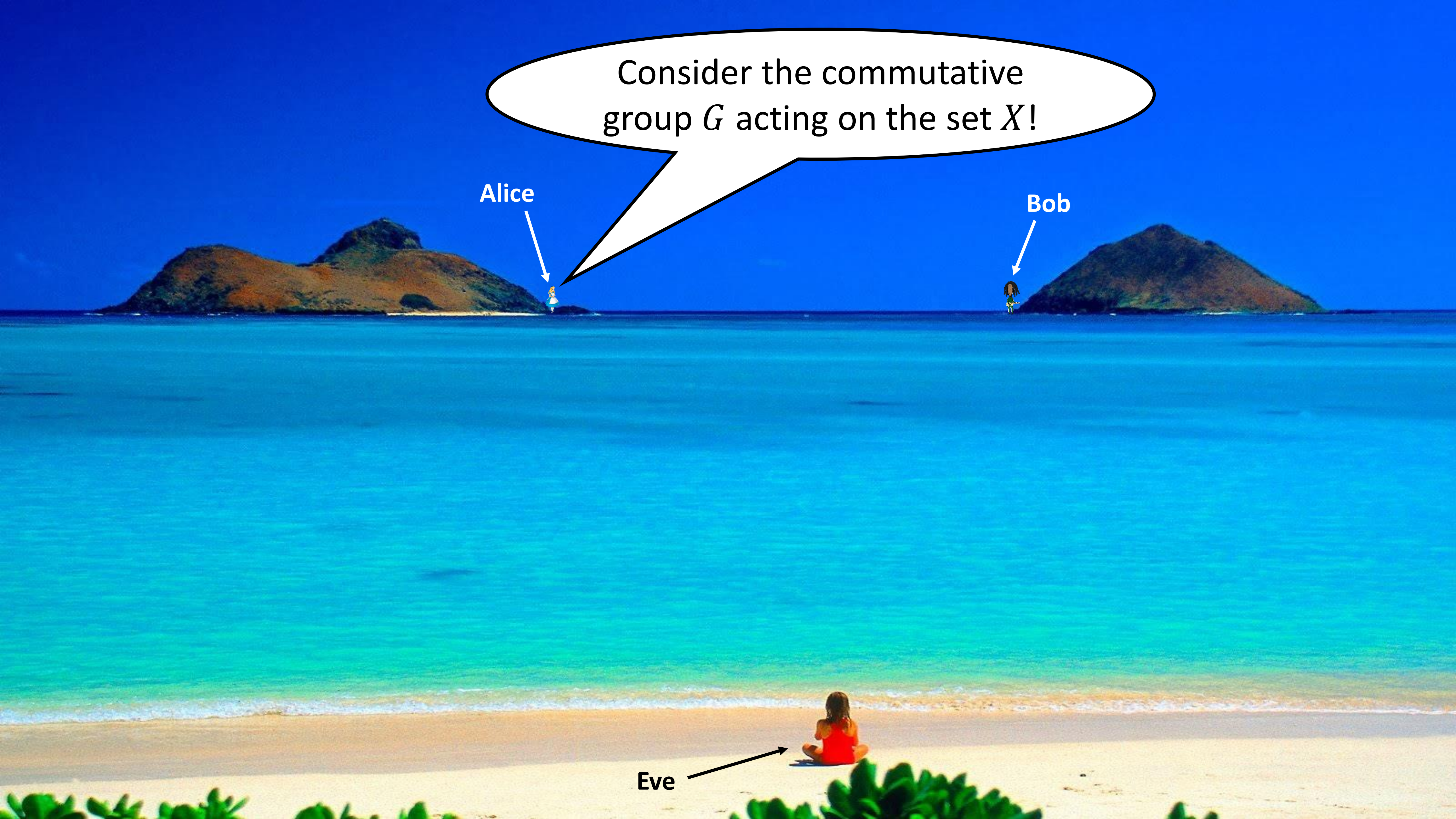
W. Castryck, T. Lange, C. Martindale, L. Panny, J. Renes

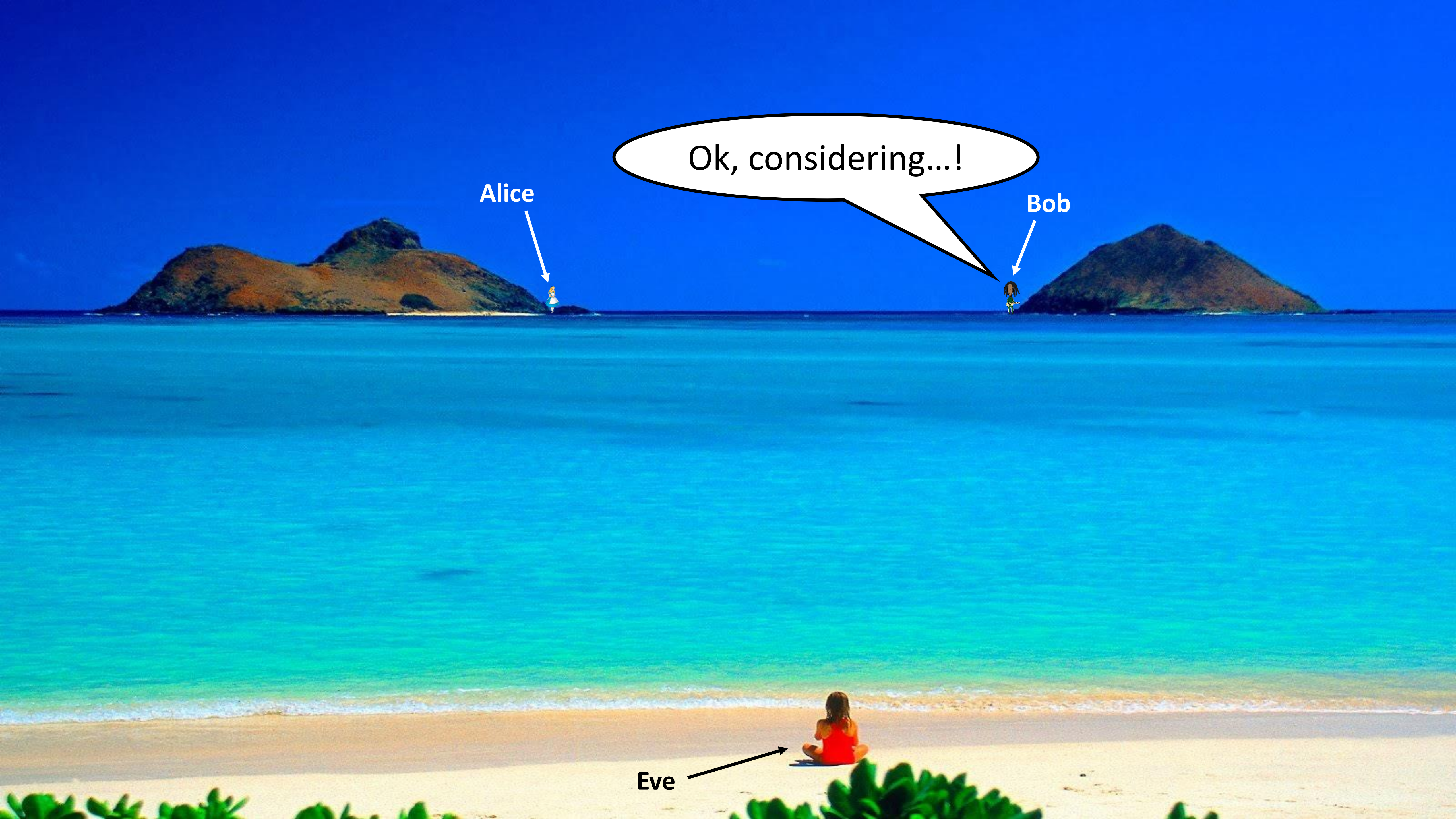

Alice
Bob
Eve

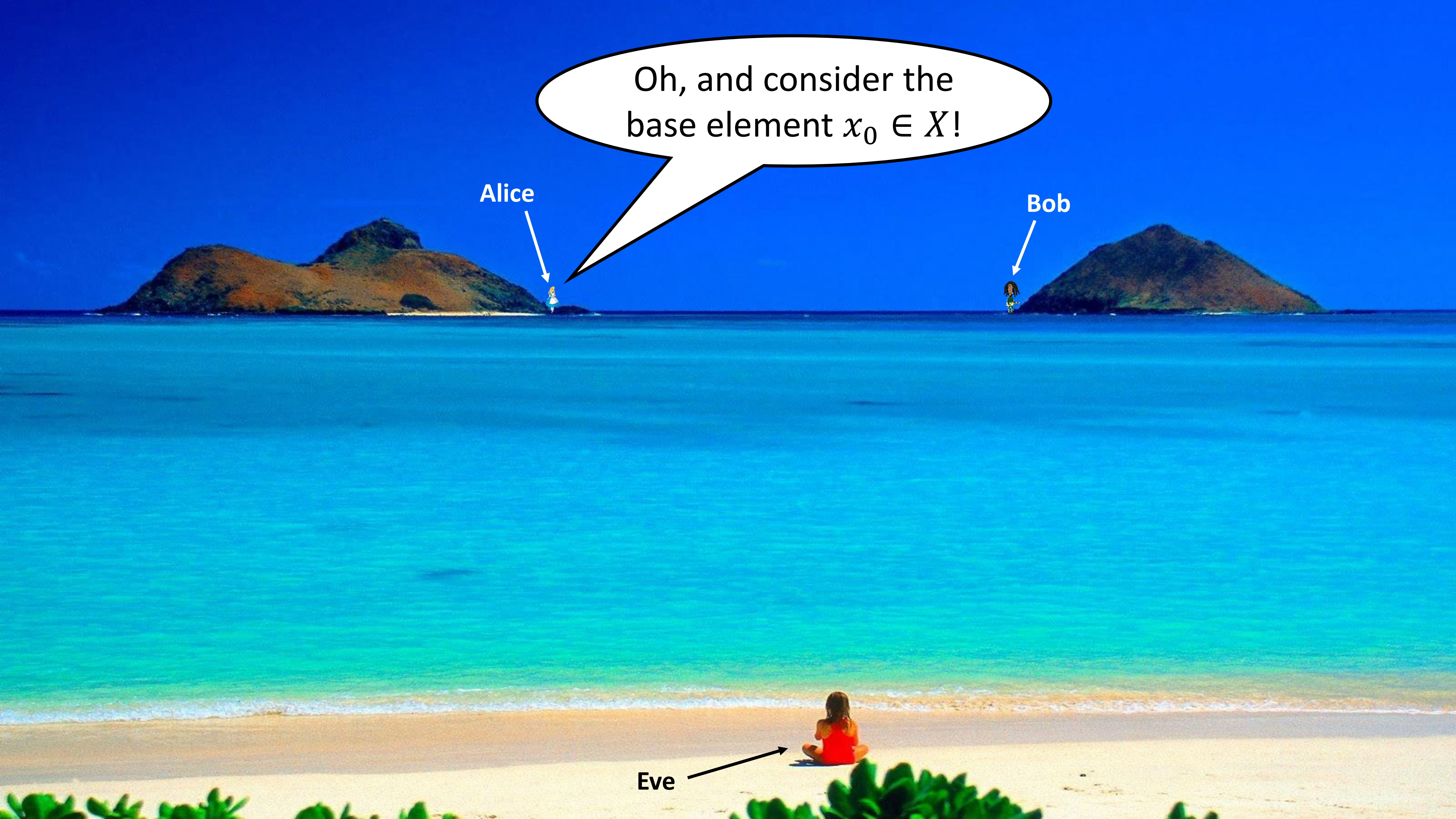

Hey Bob, my criminal brother
and your mot
Shhht, someone might
be eavesdropping!
Alice
Bob
Eve

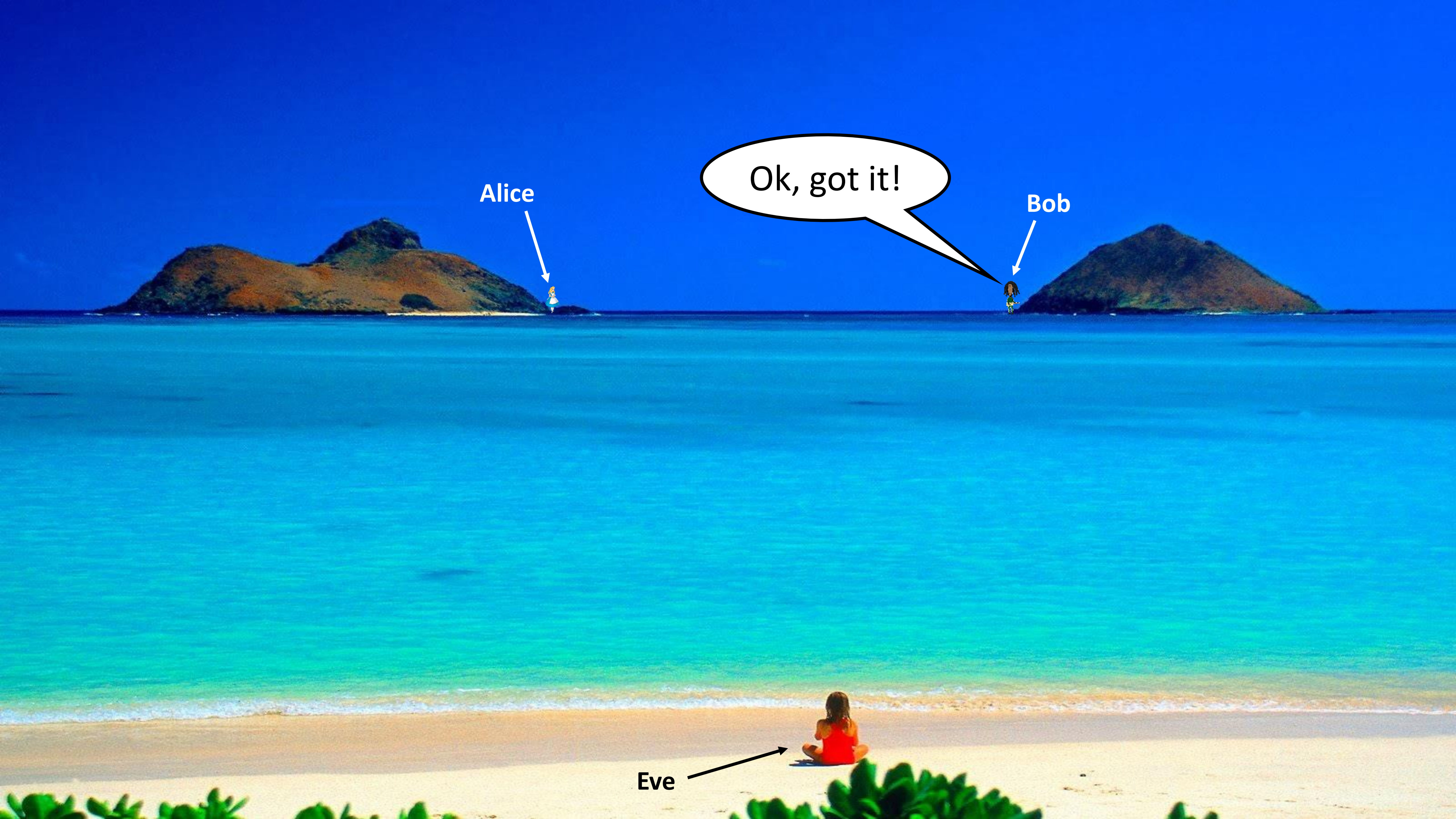

Oh!
Alice
Bob
Eve

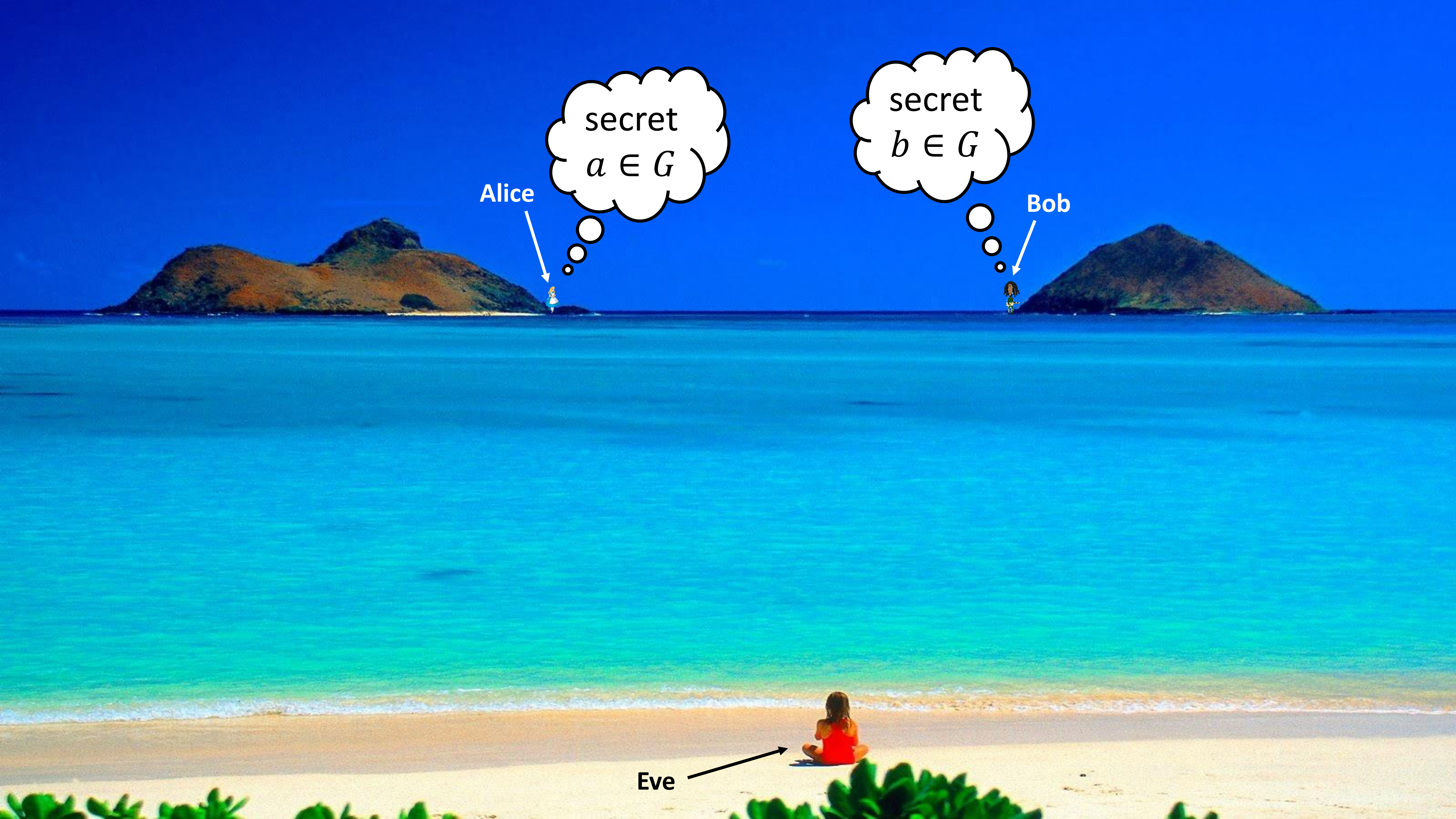

Ok!
Alice
Bob
Eve

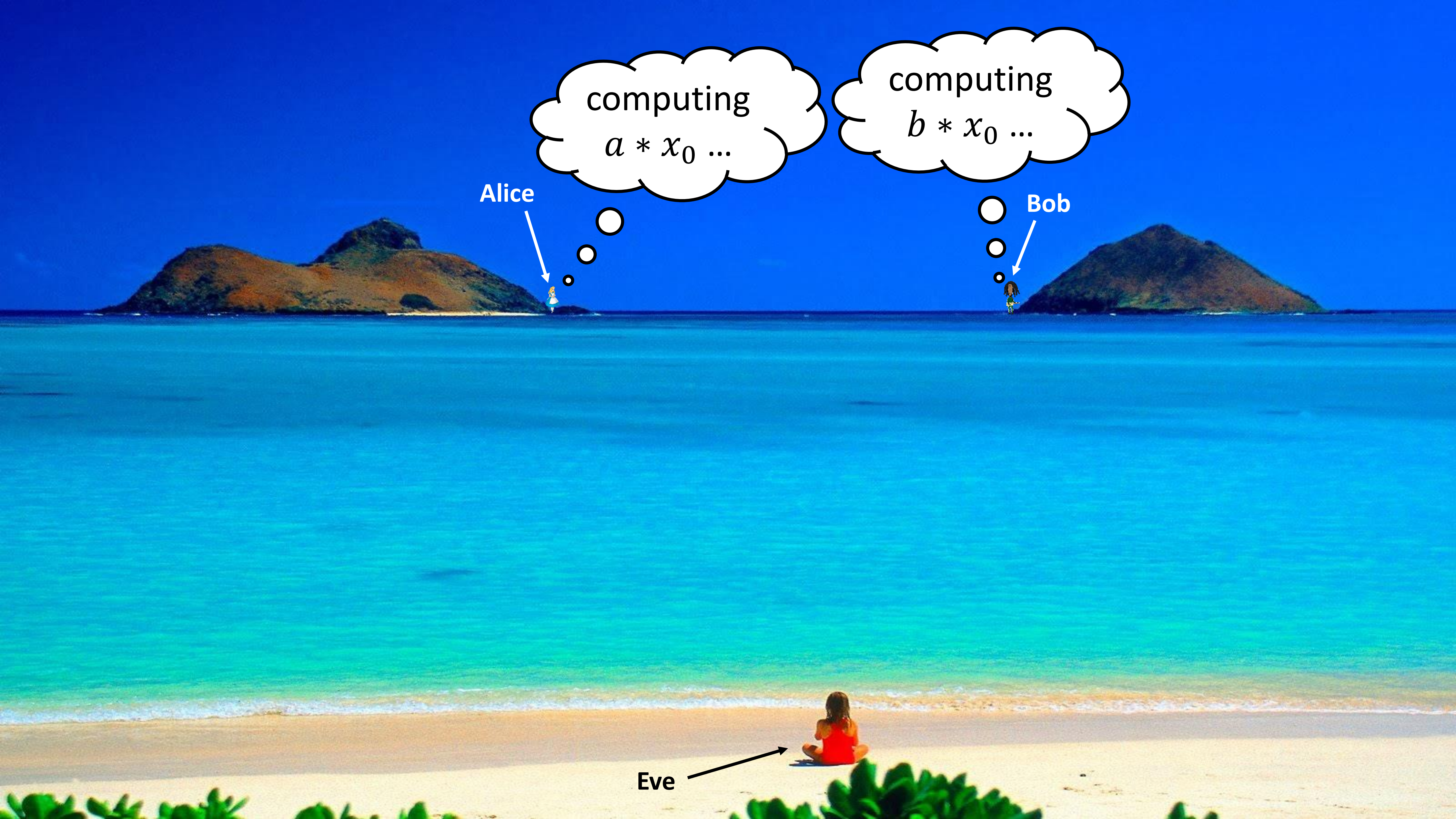

Consider the commutative group G acting on the set X!
Alice
Bob
Eve


Ok, considering…!
Alice
Bob
Eve

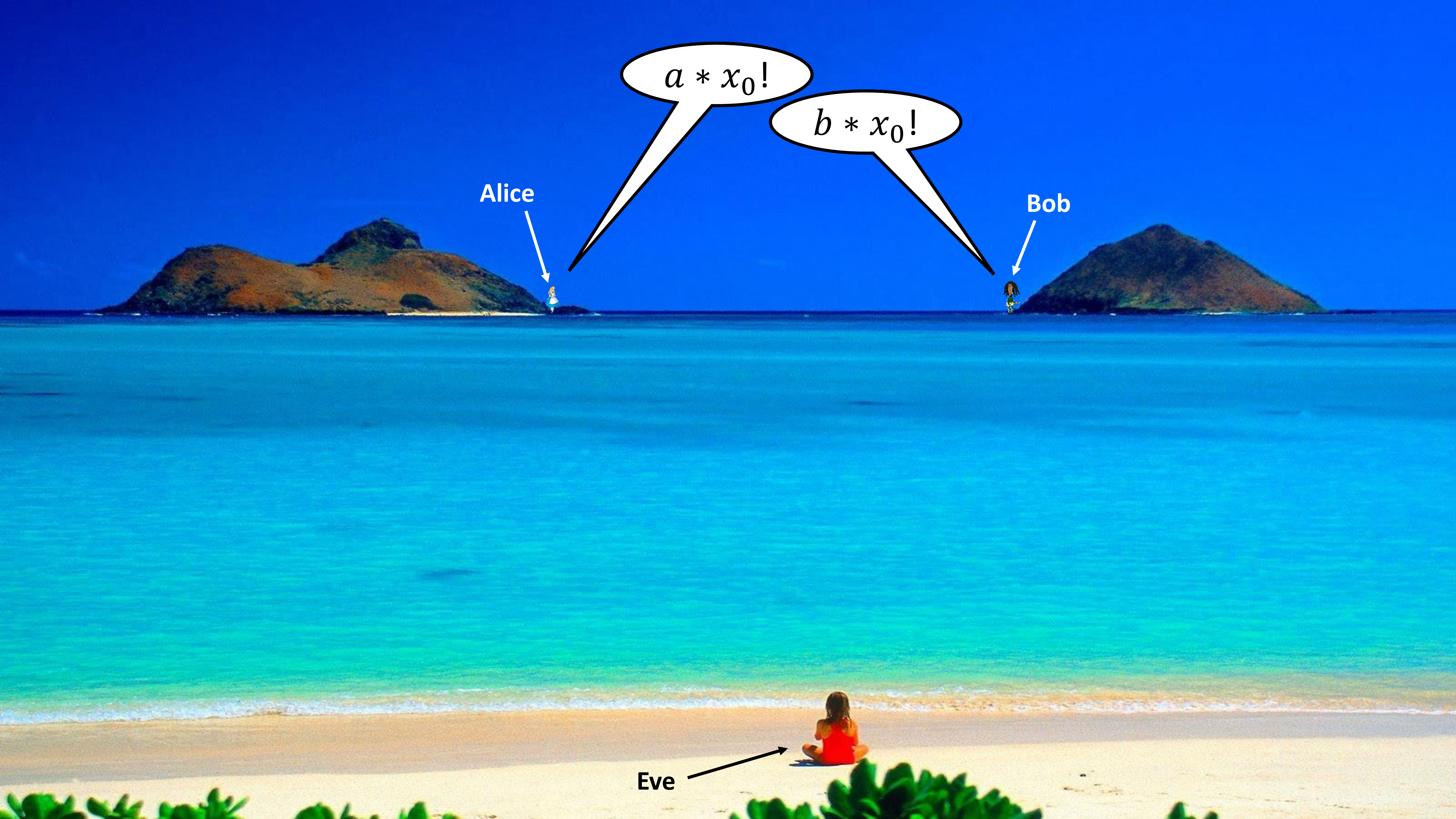

Oh, and consider the base element $x_0 \in X$!
Alice
Bob
Eve

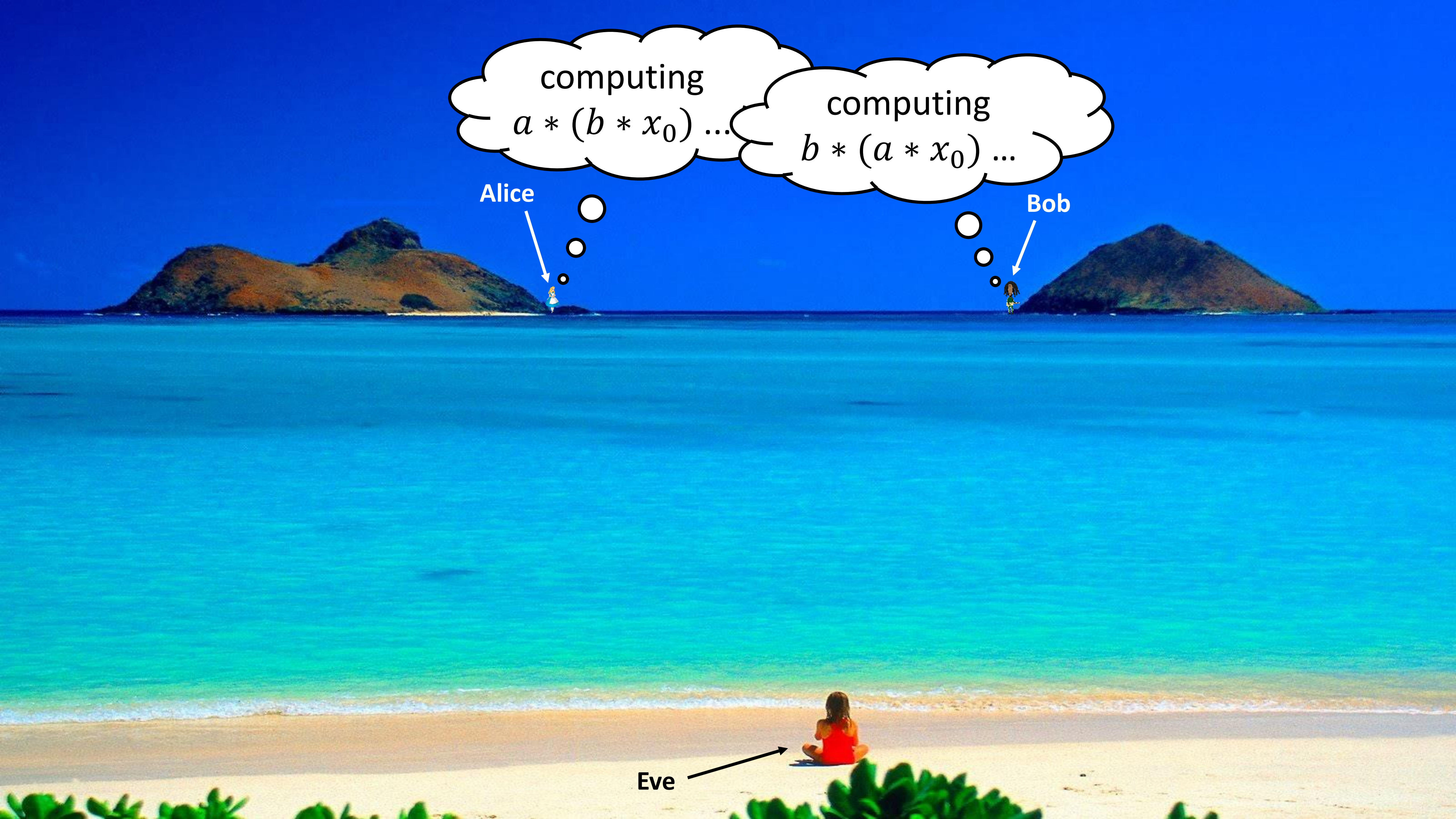

Alice
Ok, got it!
Bob
Eve

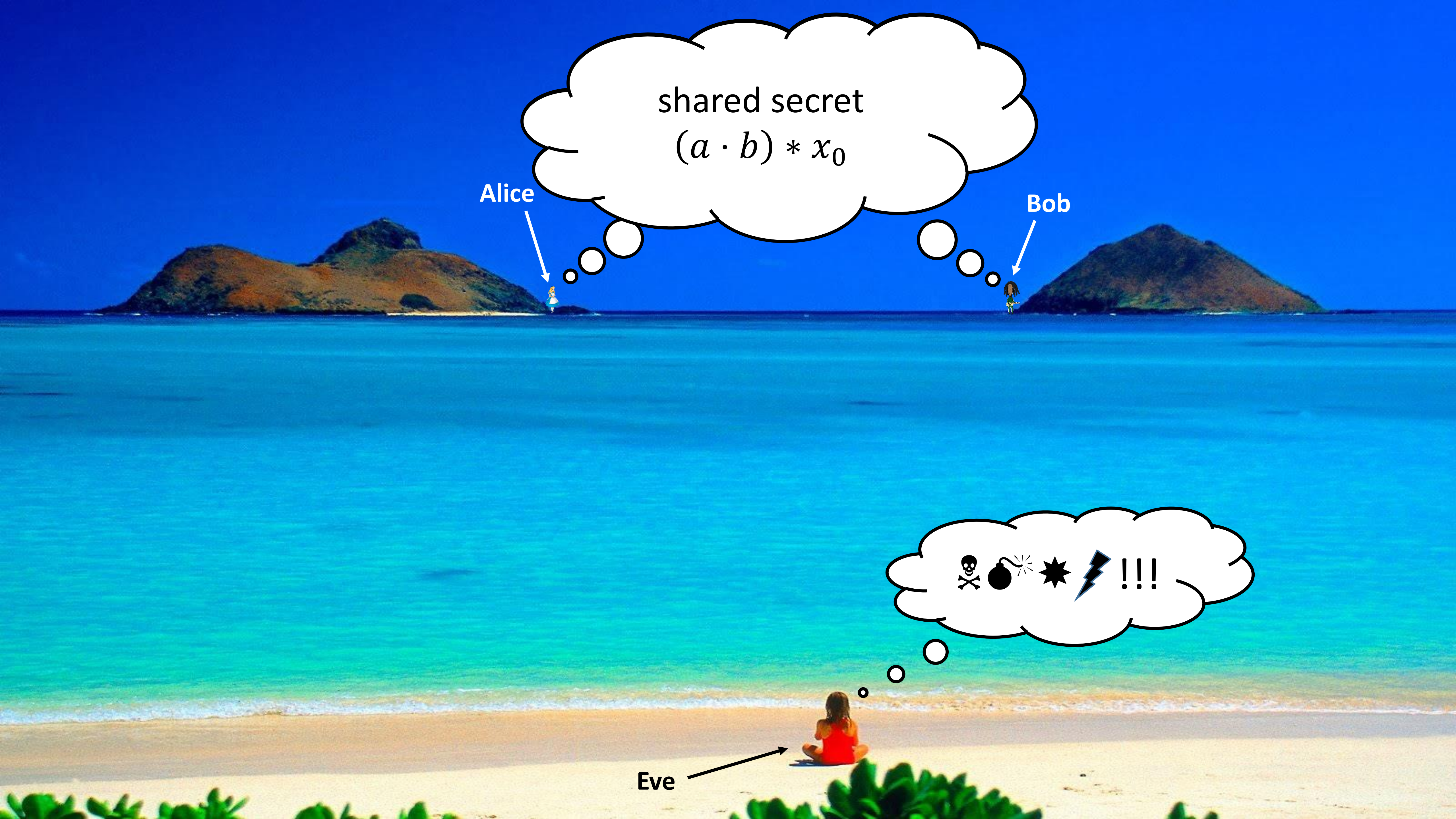

secret $a \in G$
Alice
secret $b \in G$
Bob
Eve



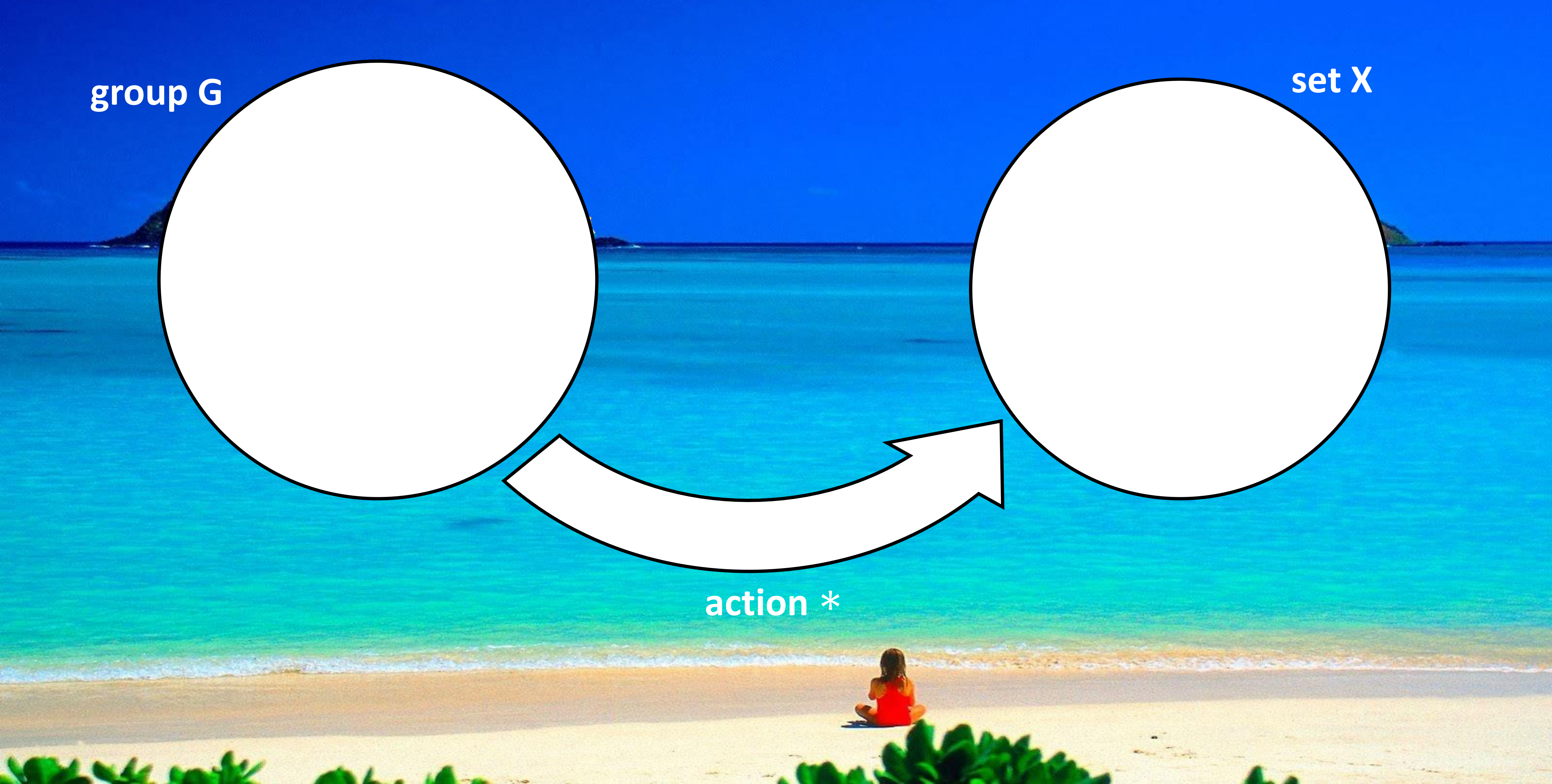
computing $a * x_0$ …
computing $b * x_0$ …
Alice
Bob
Eve


$a * x_0$!
$b * x_0$!
Alice
Bob
Eve


computing $a * (b * x_0)$ …
computing $b * (a * x_0)$ …
Alice
Bob
Eve


shared secret
$(a \cdot b) * x_0$
Alice
Bob
☠💣✸⚡!!!
Eve

Known instantiation I:

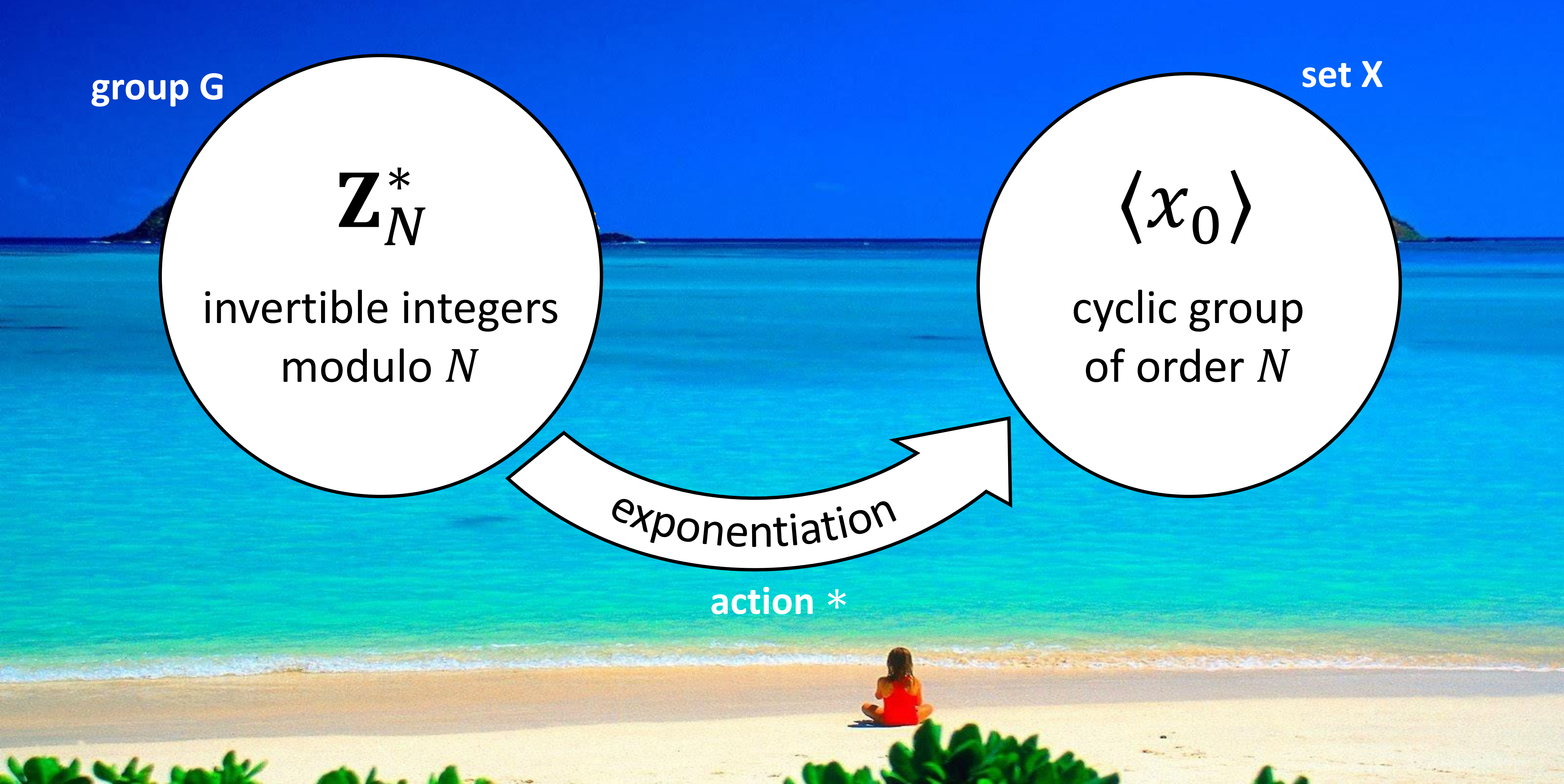


group G

set X

action *

Known instantiation I:



group G

$\mathbf{Z}_N^*$

invertible integers modulo N

exponentiation

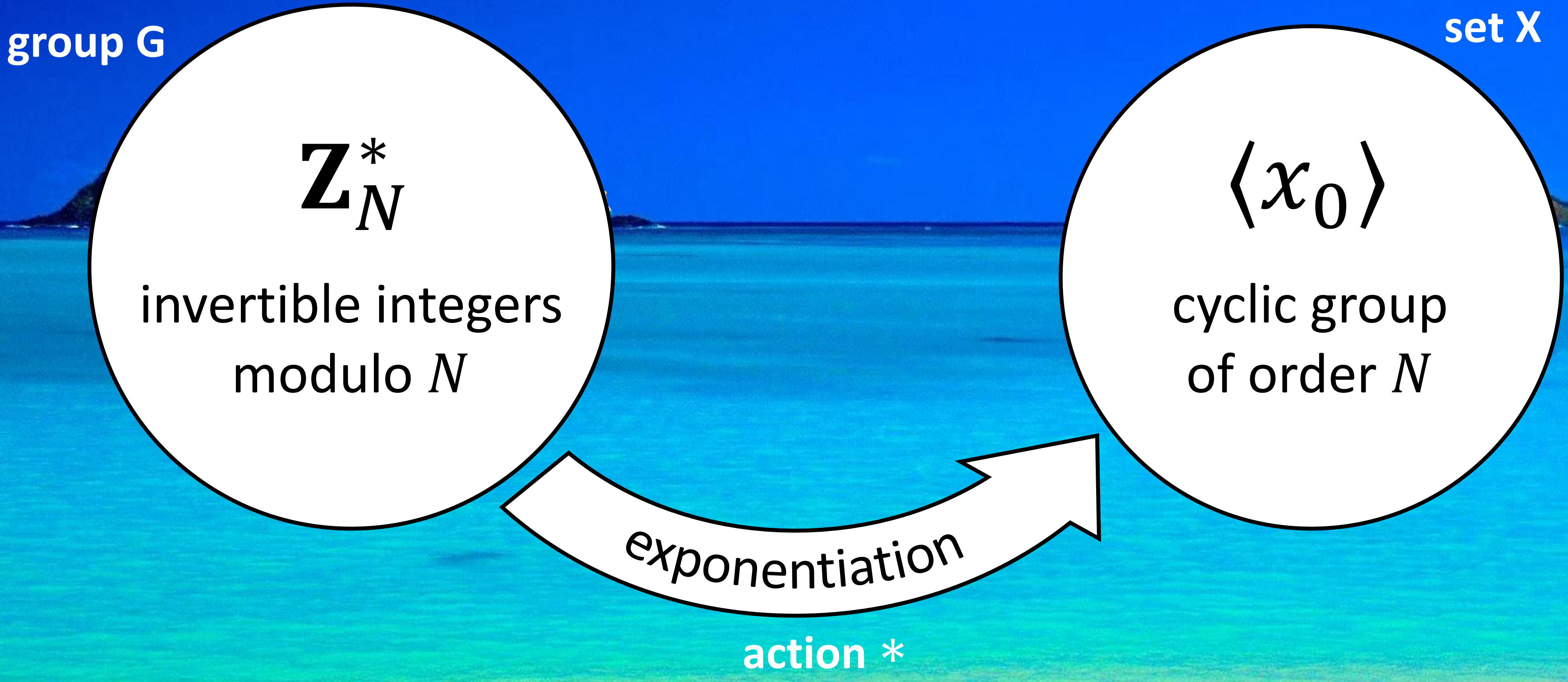
action $*$

set X

$\langle x_0 \rangle$

cyclic group of order N

Known instantiation I: Diffie-Hellman key exchange (1976)



group G

$\mathbf{Z}_N^*$

invertible integers modulo N

set X

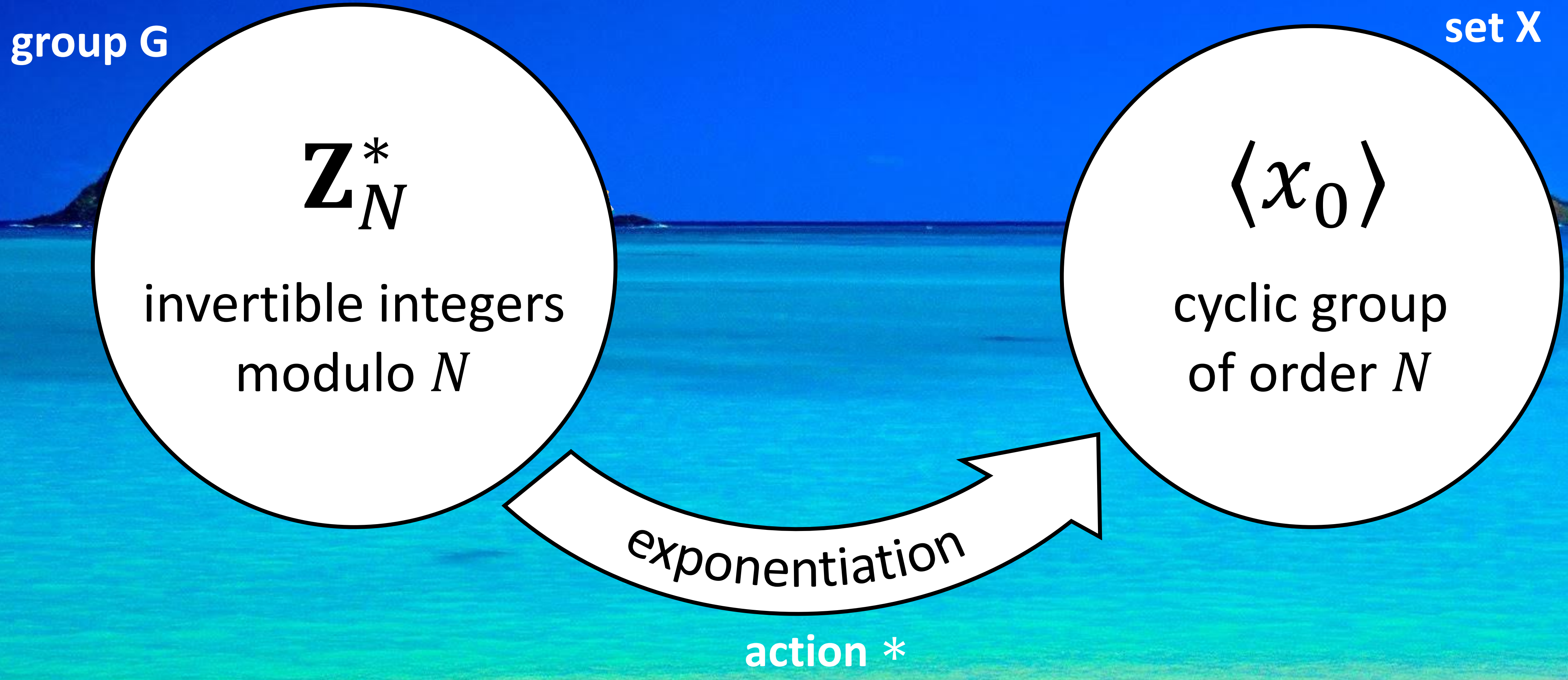
$\langle x_0 \rangle$

cyclic group of order N

exponentiation

action $*$

Known instantiation I: Diffie-Hellman key exchange (1976)



group G

$\mathbf{Z}_N^*$

invertible integers modulo N

exponentiation

action $*$

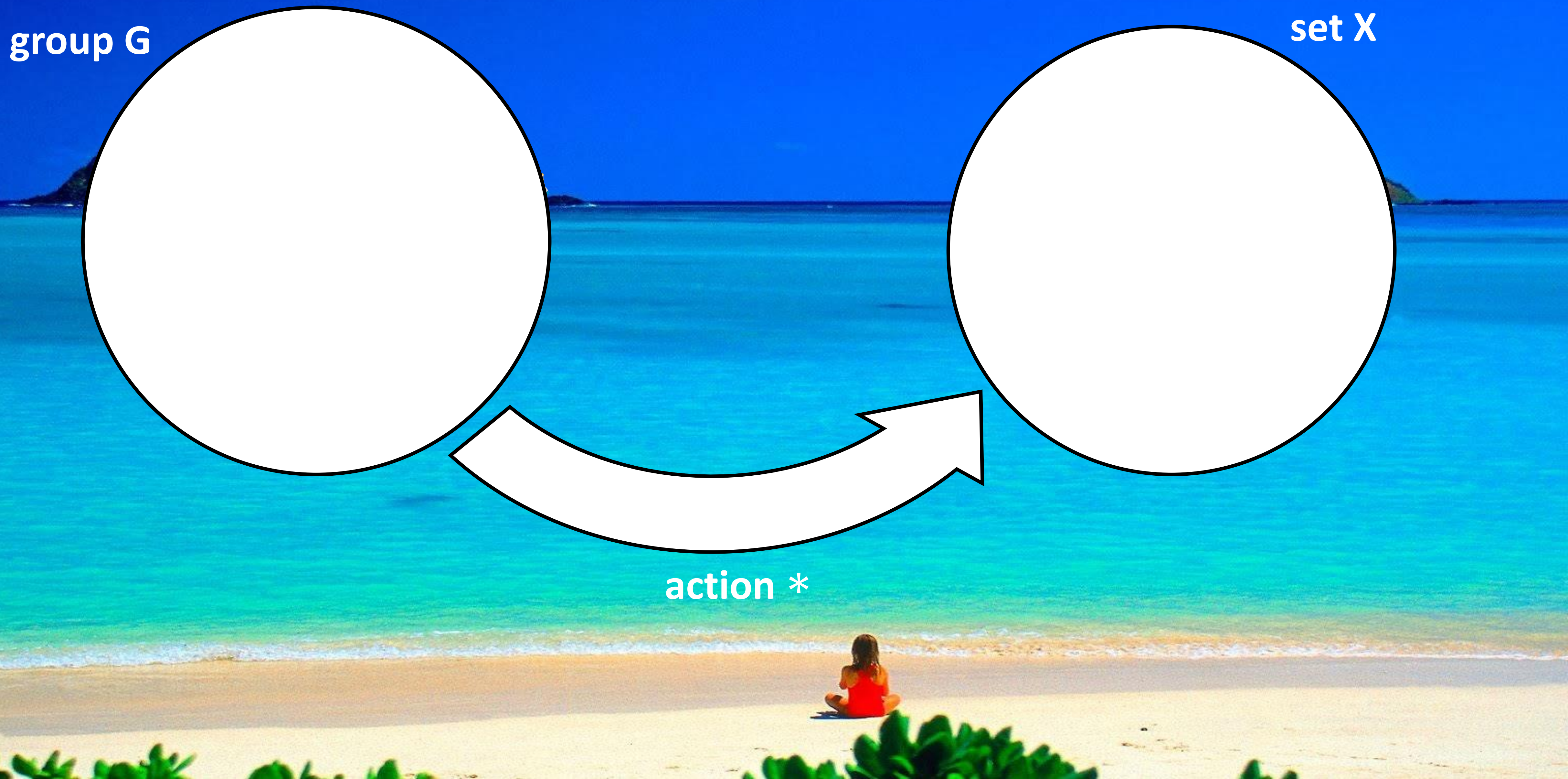
set X

$\langle x_0 \rangle$

cyclic group of order N

Post-quantum: insecure because of $L(0)$ quantum attack by Shor (1994).

Known instantiation II:

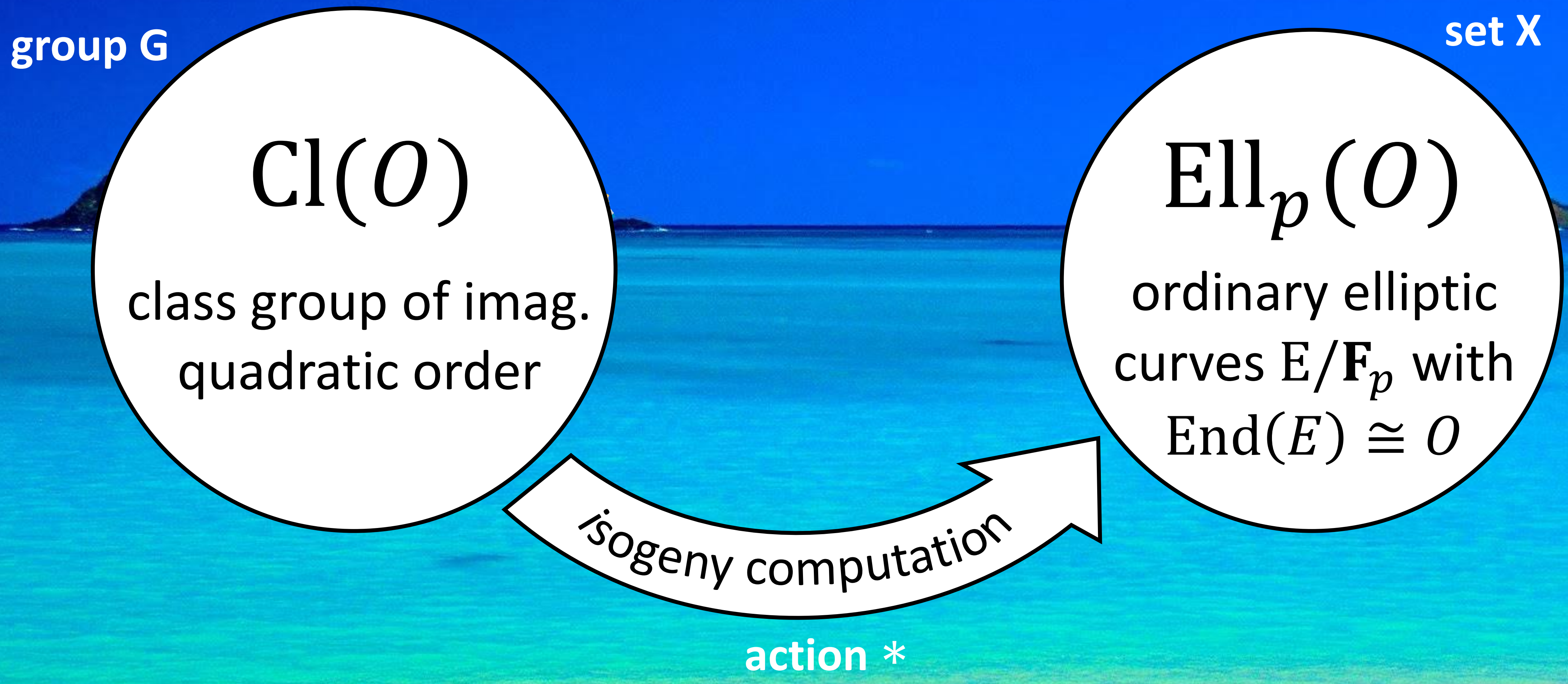


group G

set X

action *

Known instantiation II:



group G

$\mathrm{Cl}(\mathcal{O})$

class group of imag. quadratic order

set X

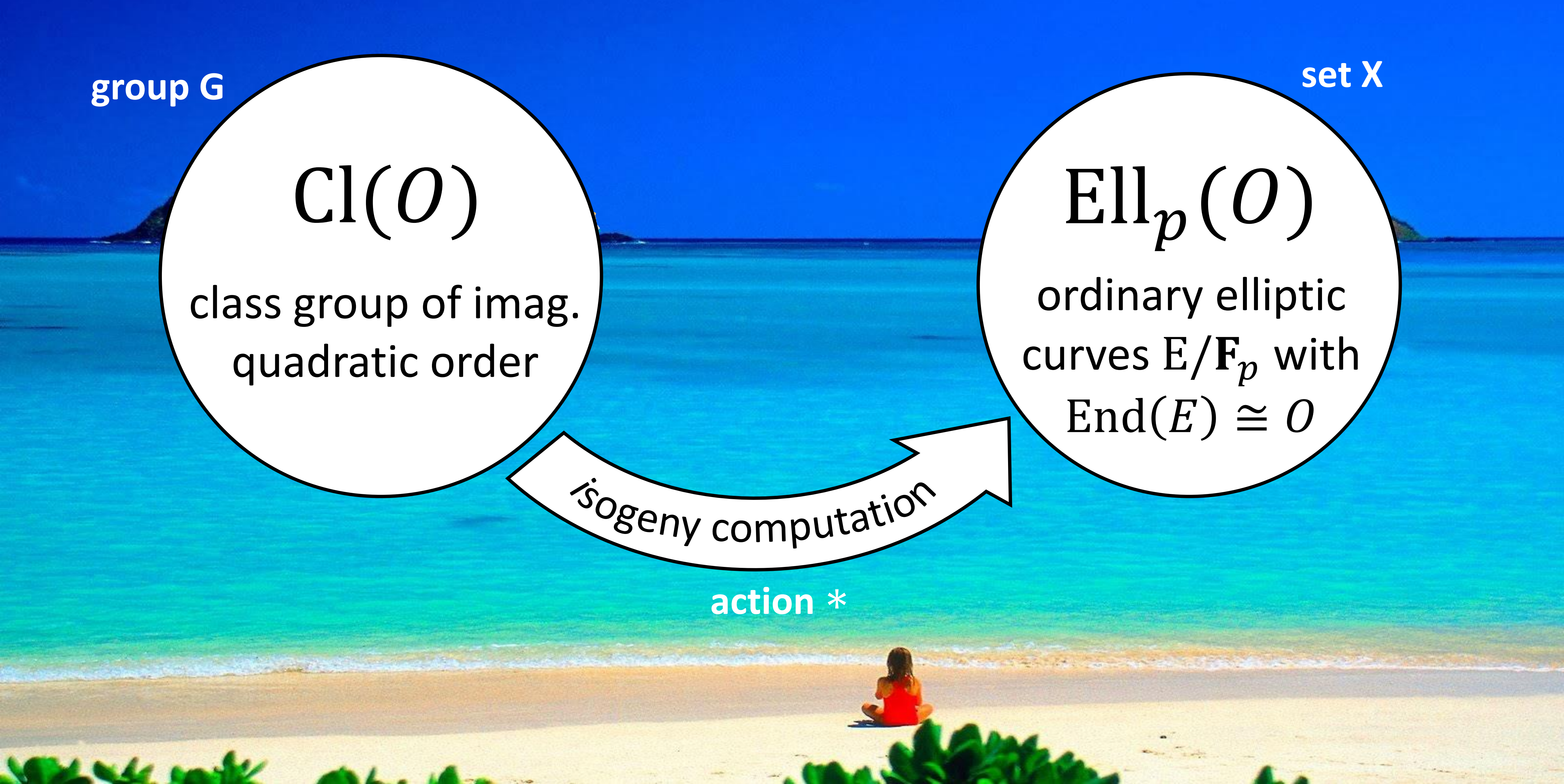
$\mathrm{Ell}_p(\mathcal{O})$

ordinary elliptic curves $\mathrm{E}/\mathbf{F}_p$ with $\mathrm{End}(E) \cong \mathcal{O}$

isogeny computation

action $*$

Known instantiation II: Couveignes-Rostovtsev-Stolbunov (1997-2004)



group G

$\mathrm{Cl}(\mathcal{O})$

class group of imag. quadratic order

set X

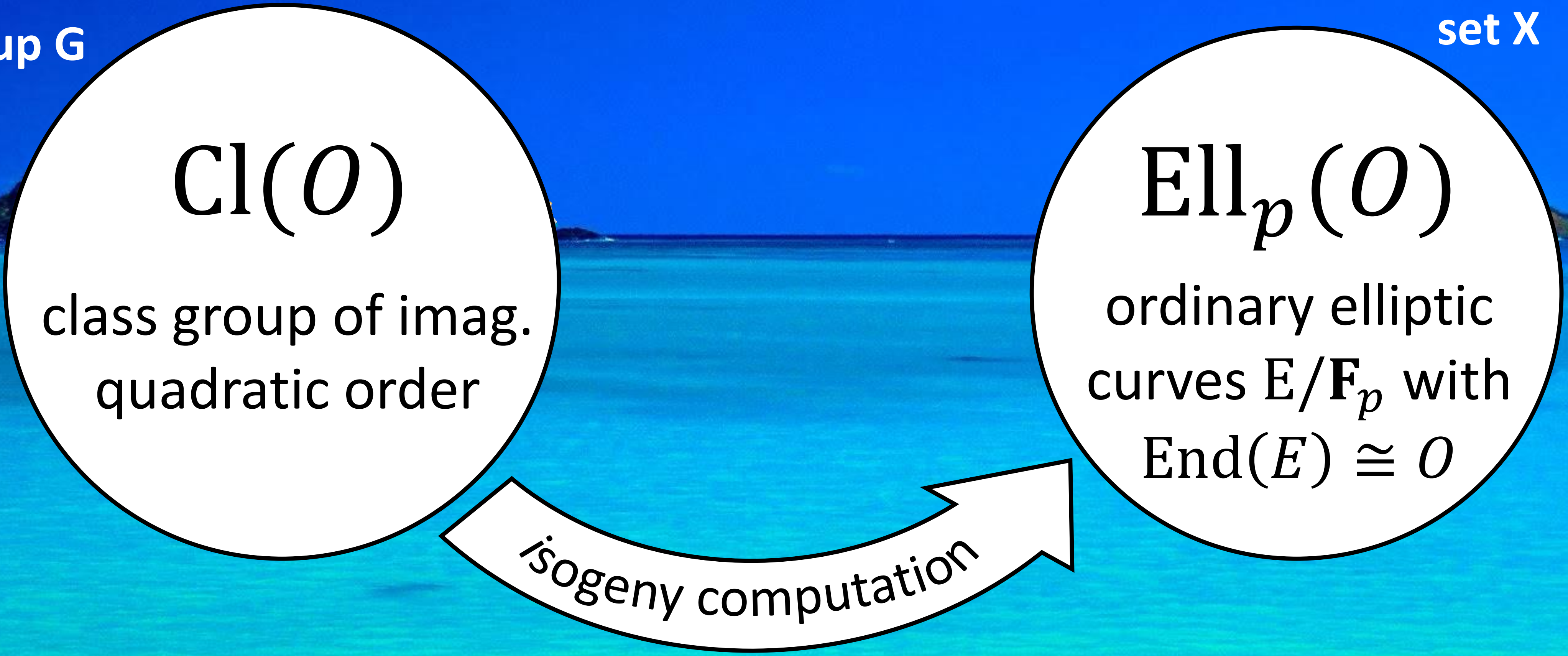
$\mathrm{Ell}_p(\mathcal{O})$

ordinary elliptic curves $\mathrm{E}/\mathbf{F}_p$ with $\mathrm{End}(E) \cong \mathcal{O}$

isogeny computation

action $*$

Known instantiation II: Couveignes-Rostovtsev-Stolbunov (1997-2004)



group G

$\mathrm{Cl}(O)$

class group of imag. quadratic order

set X

$\mathrm{Ell}_p(O)$

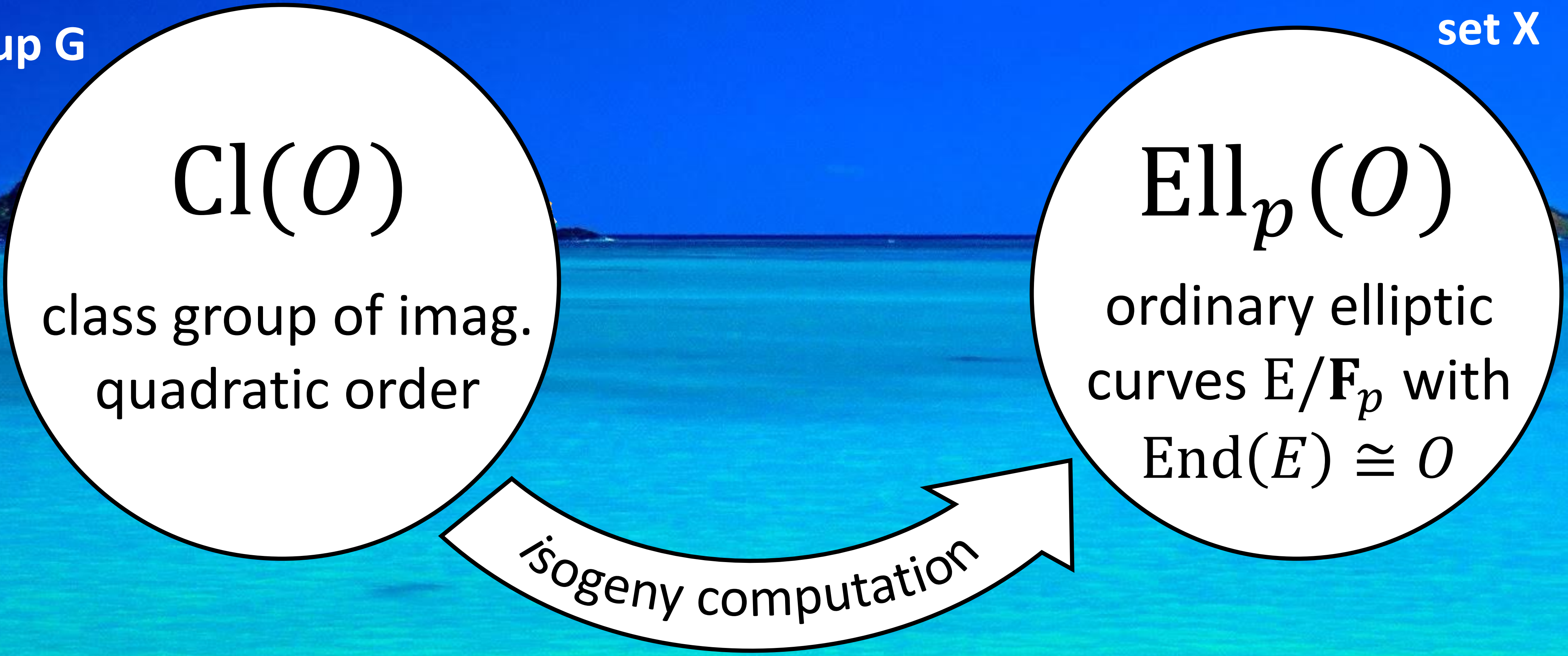
ordinary elliptic curves $\mathrm{E}/\mathbf{F}_p$ with $\mathrm{End}(E) \cong O$

isogeny computation

action $*$

Post-quantum okay despite $L({}^1/_2)$ quantum attack by Kuperberg (2005).

Known instantiation II: Couveignes-Rostovtsev-Stolbunov (1997-2004)



group G

$\mathrm{Cl}(\mathcal{O})$

class group of imag. quadratic order

set X

$\mathrm{Ell}_p(\mathcal{O})$

ordinary elliptic curves $\mathrm{E}/\mathbf{F}_p$ with $\mathrm{End}(E) \cong \mathcal{O}$

isogeny computation

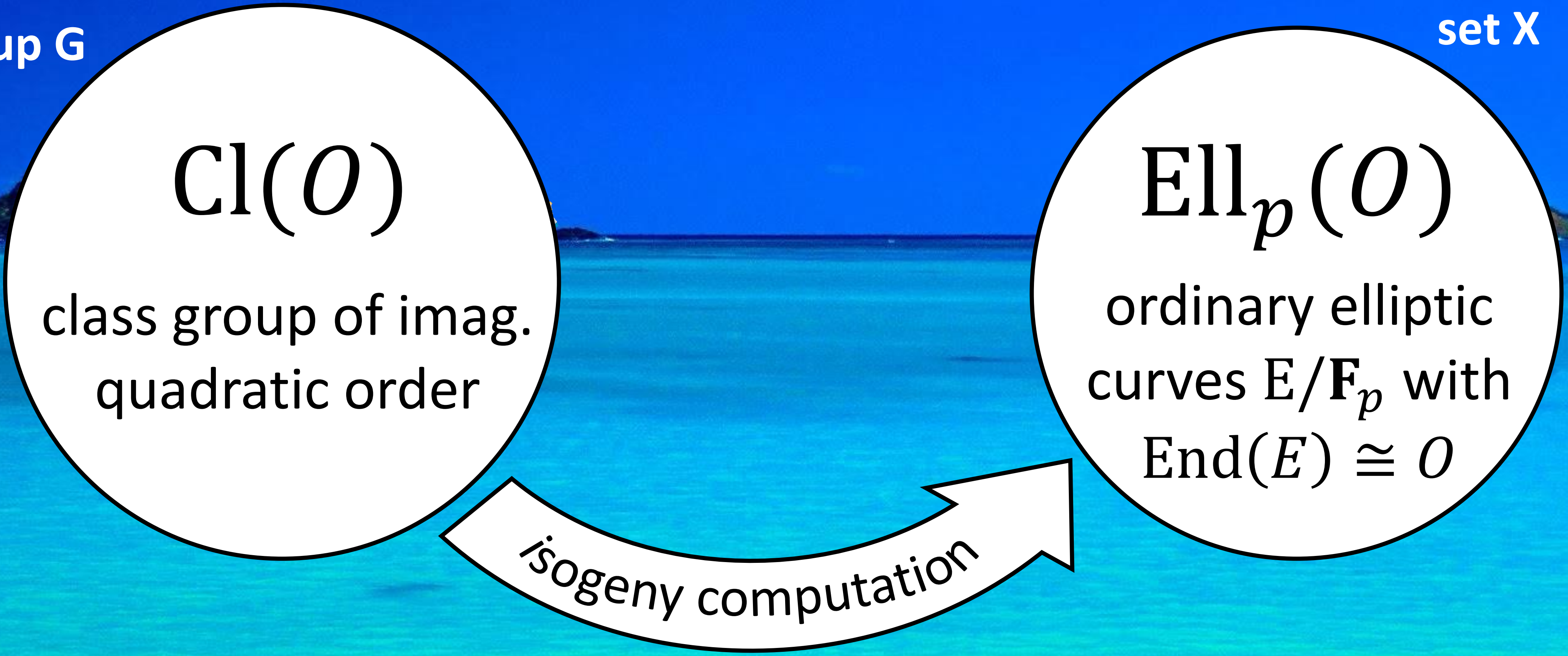
action $*$

➕

Non-interactive

Small keys (64B)

Known instantiation II: Couveignes-Rostovtsev-Stolbunov (1997-2004)



group G

$\mathrm{Cl}(\mathcal{O})$

class group of imag. quadratic order

set X

$\mathrm{Ell}_p(\mathcal{O})$

ordinary elliptic curves $\mathrm{E}/\mathbf{F}_p$ with $\mathrm{End}(E) \cong \mathcal{O}$

isogeny computation

action $*$

+

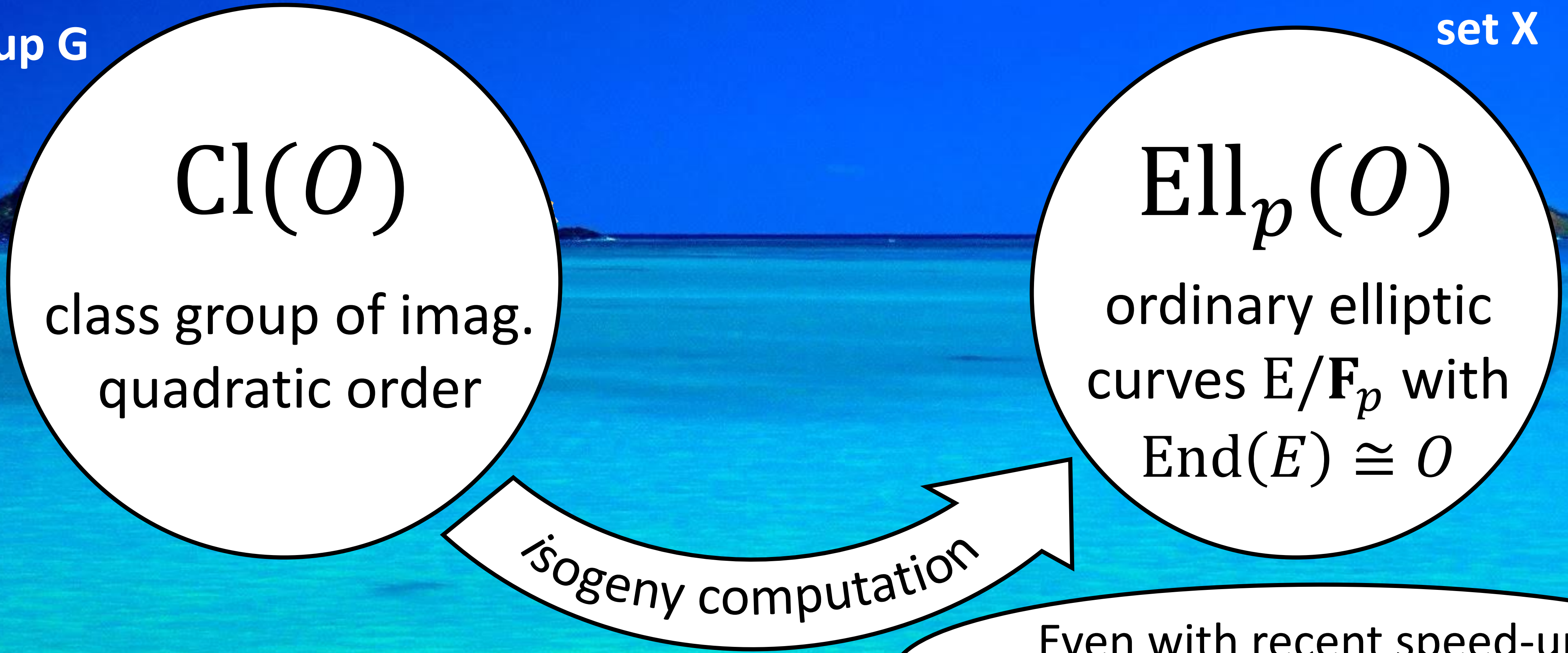
Non-interactive

Small keys (64B)

−

Unacceptably slow

Known instantiation II: Couveignes-Rostovtsev-Stolbunov (1997-2004)


group G
$\mathrm{Cl}(\mathcal{O})$
class group of imag. quadratic order
set X
$\mathrm{Ell}_p(\mathcal{O})$
ordinary elliptic curves $\mathrm{E}/\mathbf{F}_p$ with $\mathrm{End}(E) \cong \mathcal{O}$
isogeny computation

action $*$

+

Non-interactive

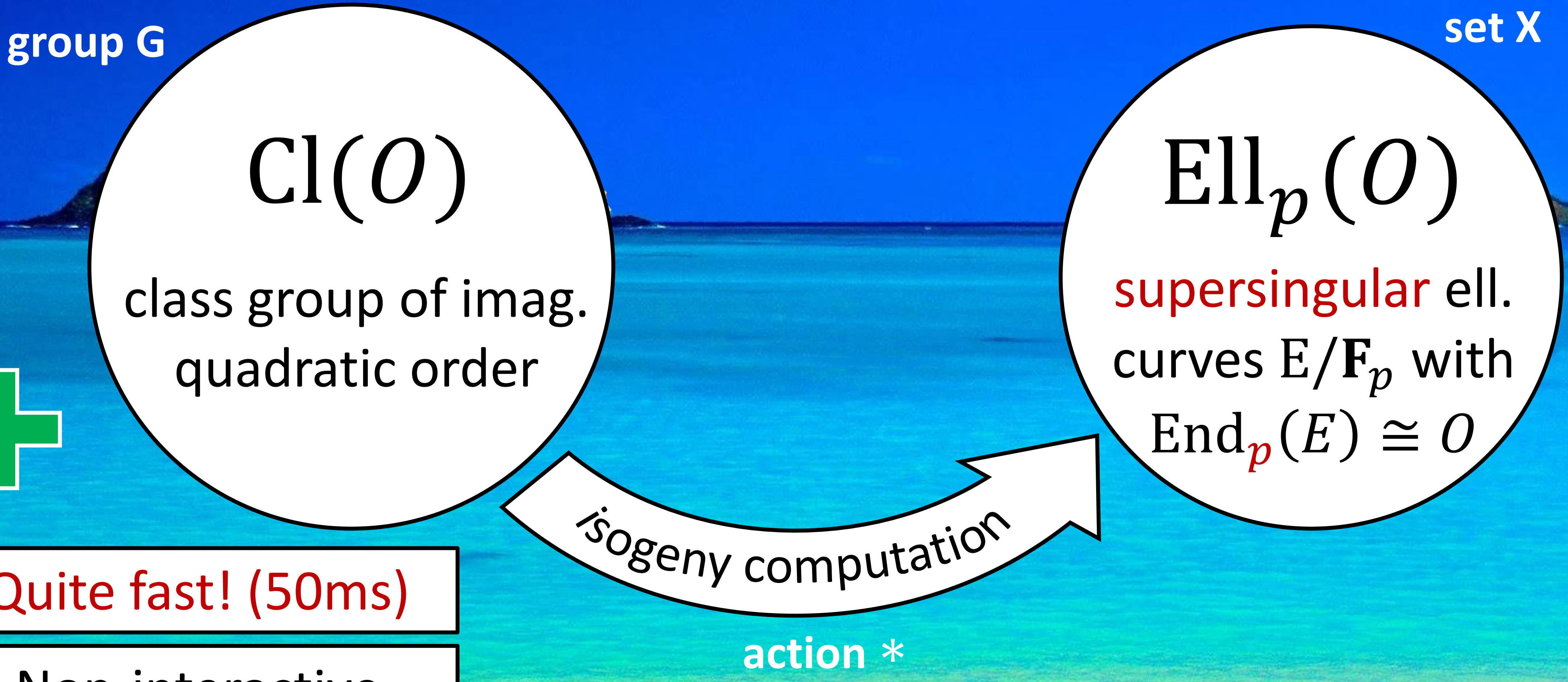
Small keys (64B)

−

Even with recent speed-ups by De Feo, Kieffer, Smith

Unacceptably slow

Our proposal:



group G

$\mathrm{Cl}(\mathcal{O})$

class group of imag. quadratic order

set X

$\mathrm{Ell}_p(\mathcal{O})$

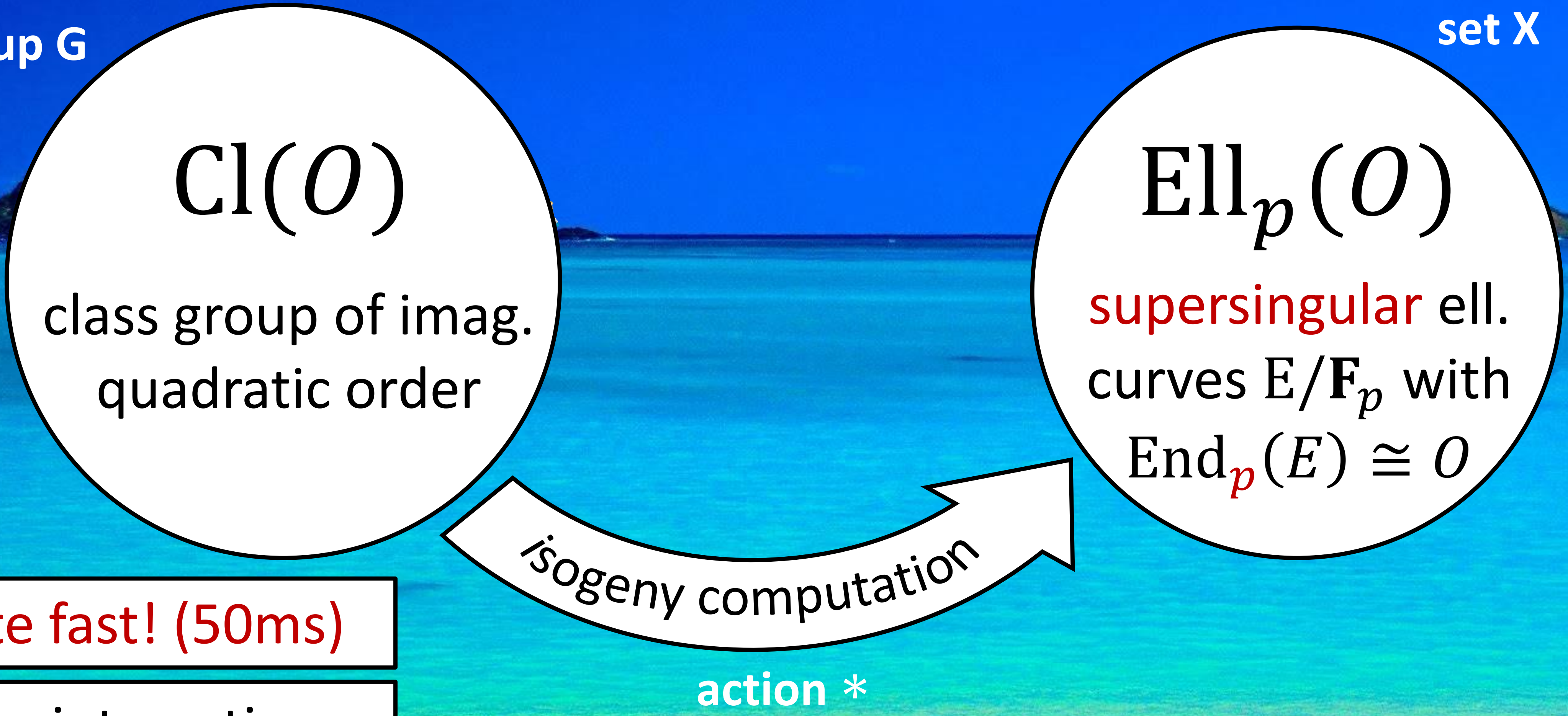
supersingular ell. curves $\mathrm{E}/\mathbf{F}_p$ with $\mathrm{End}_p(E) \cong \mathcal{O}$

Quite fast! (50ms)

Non-interactive

Small keys (64B)

Our proposal:



group G

$\mathrm{Cl}(\mathcal{O})$

class group of imag. quadratic order

isogeny computation

action $*$

set X

$\mathrm{Ell}_p(\mathcal{O})$

supersingular ell. curves $\mathrm{E}/\mathbf{F}_p$ with $\mathrm{End}_p(E) \cong \mathcal{O}$

+

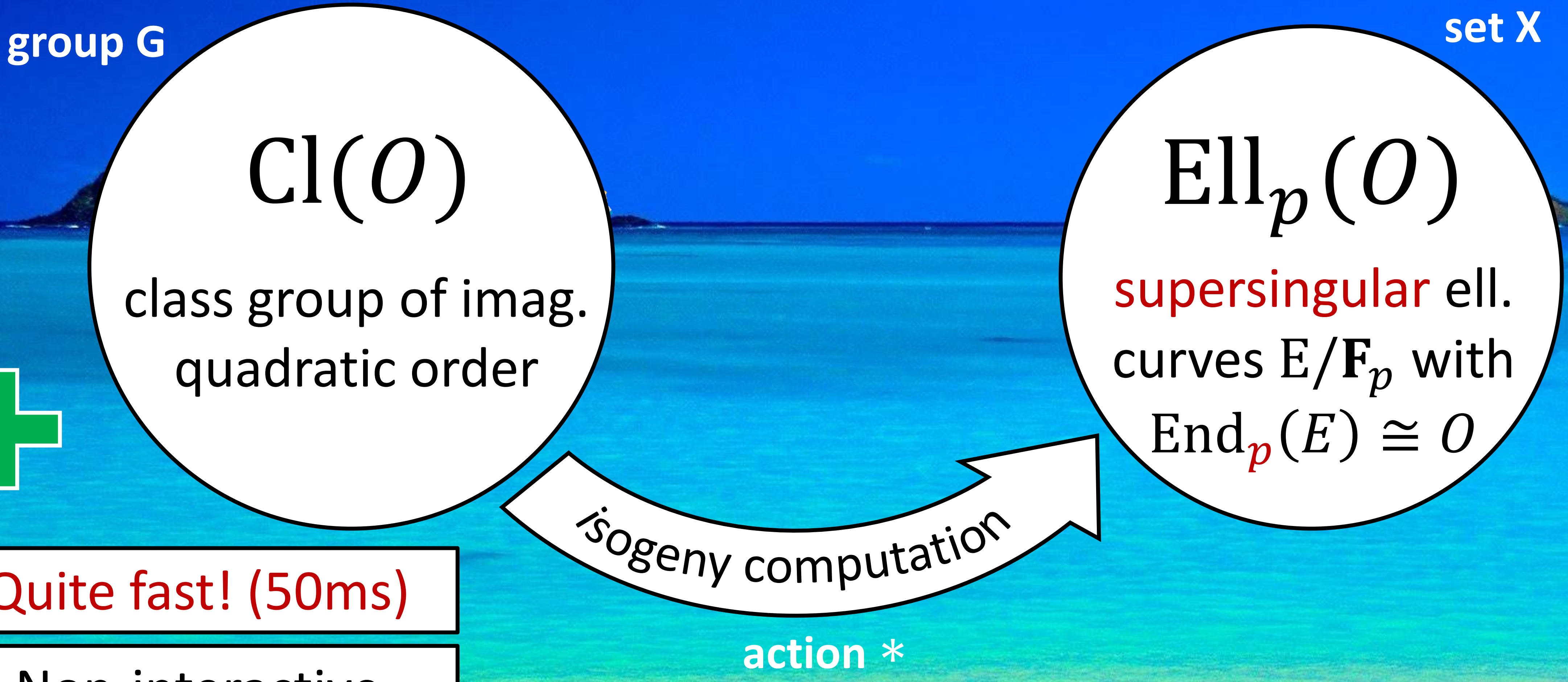
Quite fast! (50ms)

Non-interactive

Small keys (64B)

Easy key validation

Our proposal:



group G

$\mathrm{Cl}(\mathcal{O})$

class group of imag. quadratic order

set X

$\mathrm{Ell}_p(\mathcal{O})$

supersingular ell. curves $\mathrm{E}/\mathbf{F}_p$ with $\mathrm{End}_p(E) \cong \mathcal{O}$

isogeny computation

action $*$

Quite fast! (50ms)

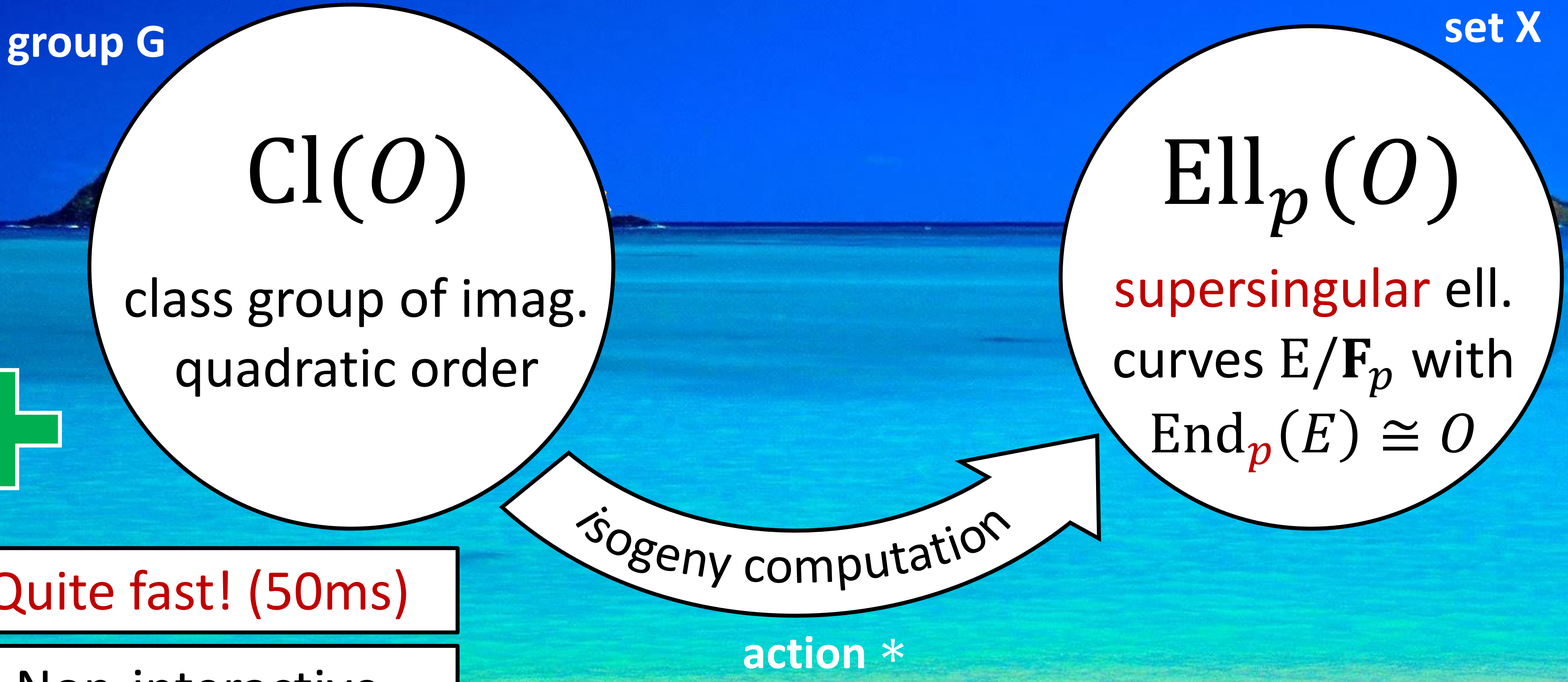
Non-interactive

Small keys (64B)

Easy key validation

This is *not* SIDH!

Our proposal: Commutative Supersingular Isogeny Diffie-Hellman (CSIDH)



group G

$\mathrm{Cl}(\mathcal{O})$

class group of imag. quadratic order

set X

$\mathrm{Ell}_p(\mathcal{O})$

supersingular ell. curves $\mathrm{E}/\mathbf{F}_p$ with $\mathrm{End}_p(E) \cong \mathcal{O}$

isogeny computation

action *

+

Quite fast! (50ms)

Non-interactive

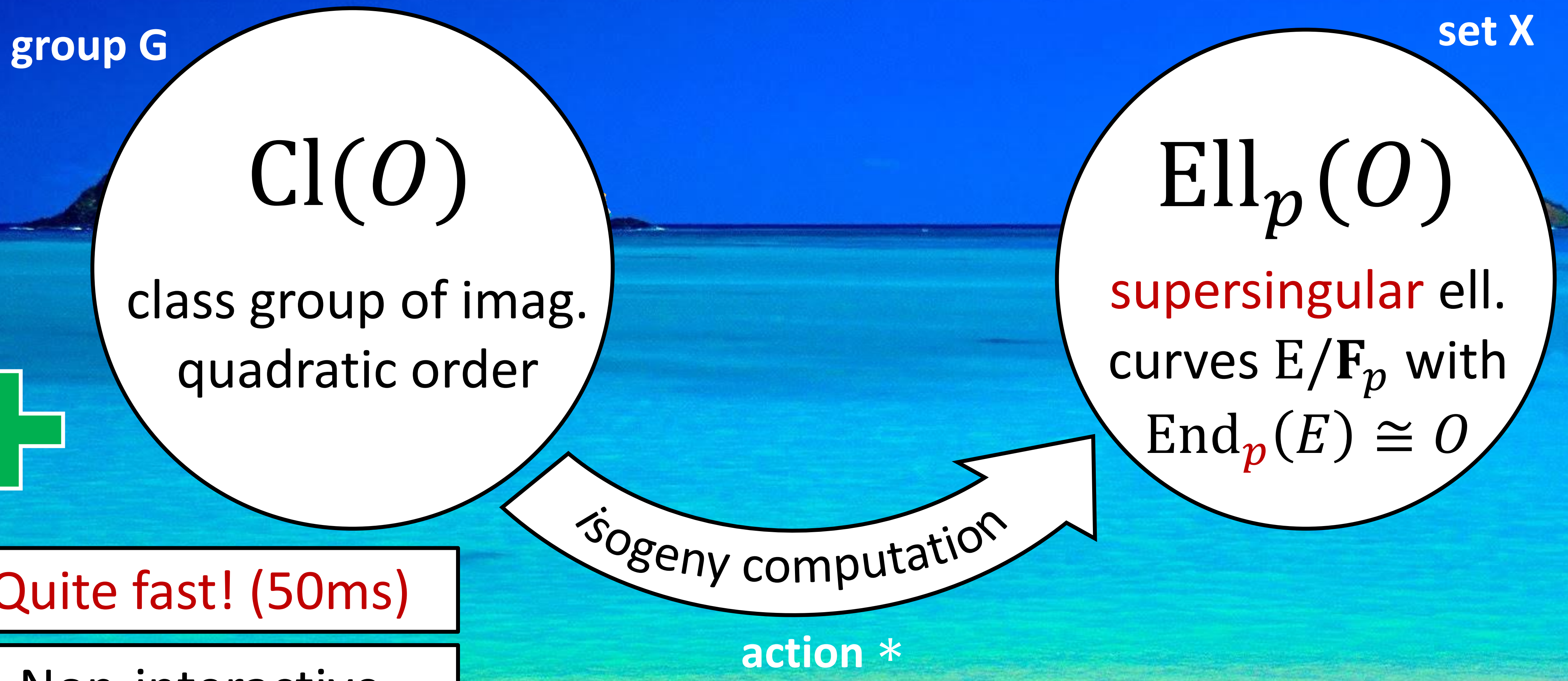
Small keys (64B)

Easy key validation

This is *not* SIDH!

Our proposal: Commutative Supersingular Isogeny Diffie-Hellman (CSIDH)

More details to be found on ePrint 2018/383



group G

$\mathrm{Cl}(\mathcal{O})$

class group of imag. quadratic order

set X

$\mathrm{Ell}_p(\mathcal{O})$

supersingular ell. curves $\mathrm{E}/\mathbf{F}_p$ with $\mathrm{End}_p(E) \cong \mathcal{O}$

isogeny computation

action $*$

Quite fast! (50ms)

Non-interactive

Small keys (64B)

Easy key validation

This is *not* SIDH!

Thanks!

QUESTIONS?