Homomorphic Encryption

ECE/CS 407

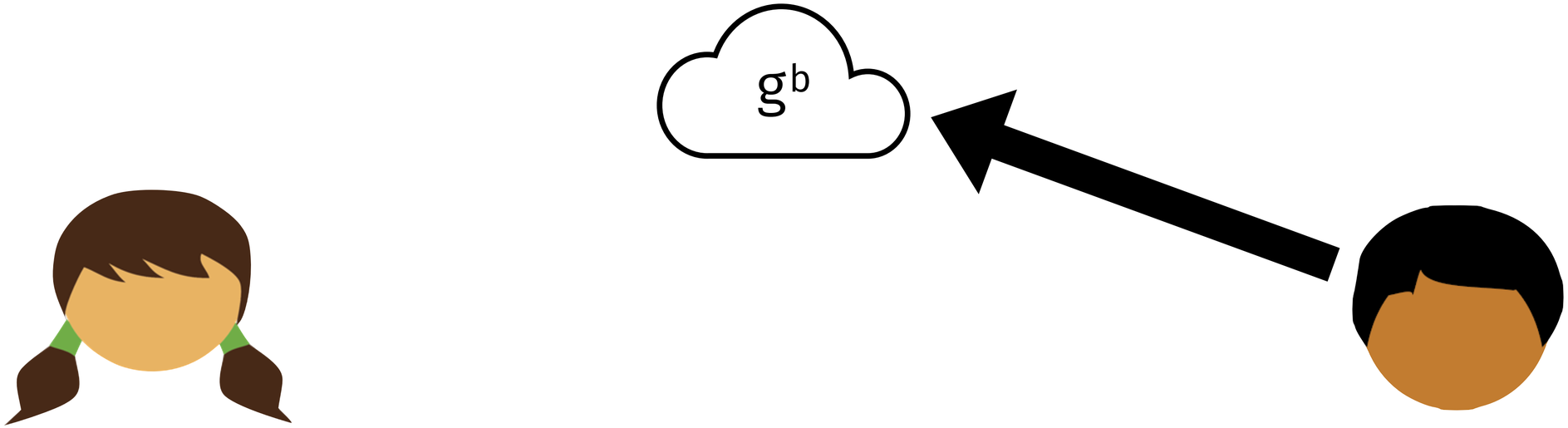
Today's objectives

Understand the notion of a homomorphism

See that public-key schemes can have *homomorphic* properties

Understand the definition of fully homomorphic encryption (FHE)

Refresher: ElGamal Encryption

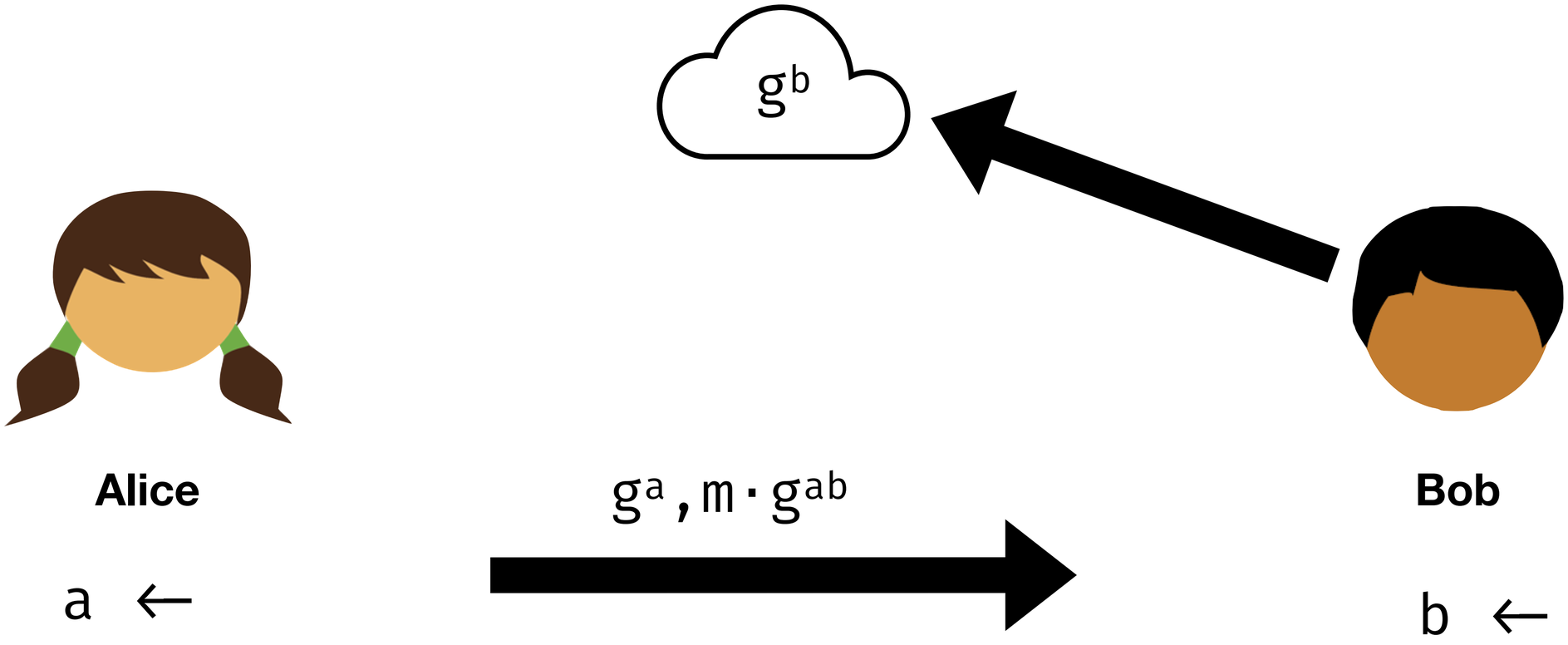


Alice

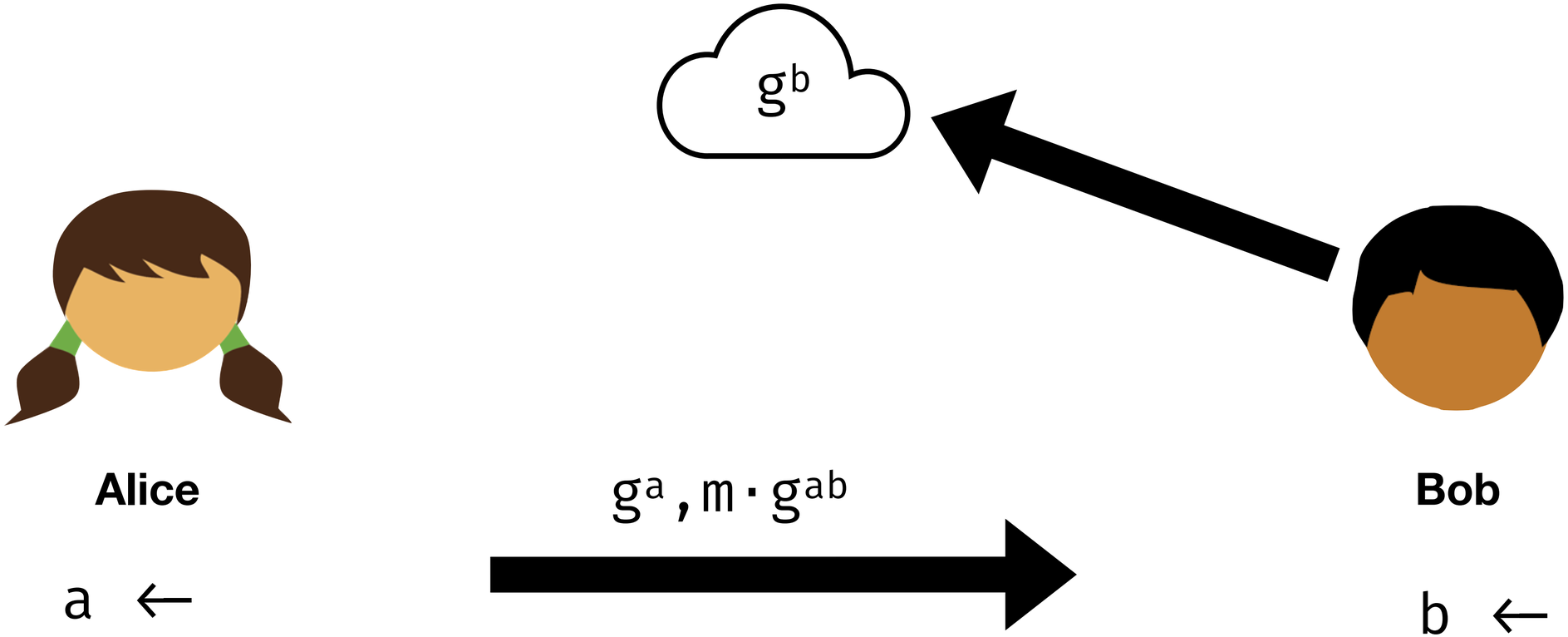
Bob

$b \leftarrow$

Refresher: ElGamal Encryption



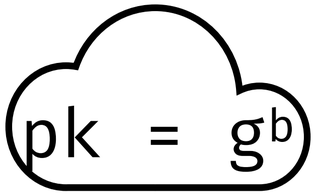
Refresher: ElGamal Encryption

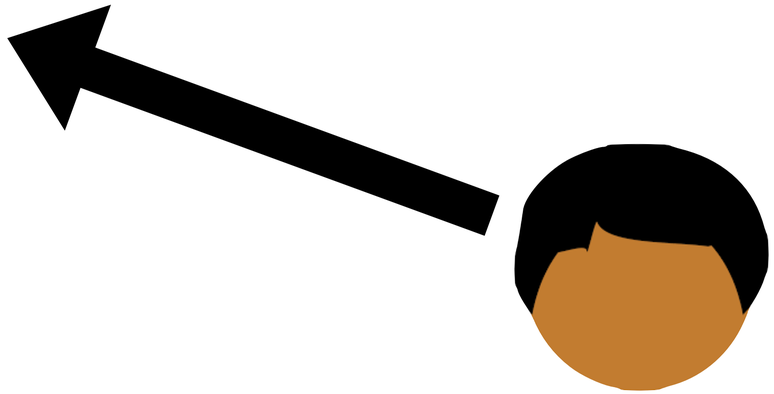


Refresher: ElGamal Encryption

Alice

$a \leftarrow$



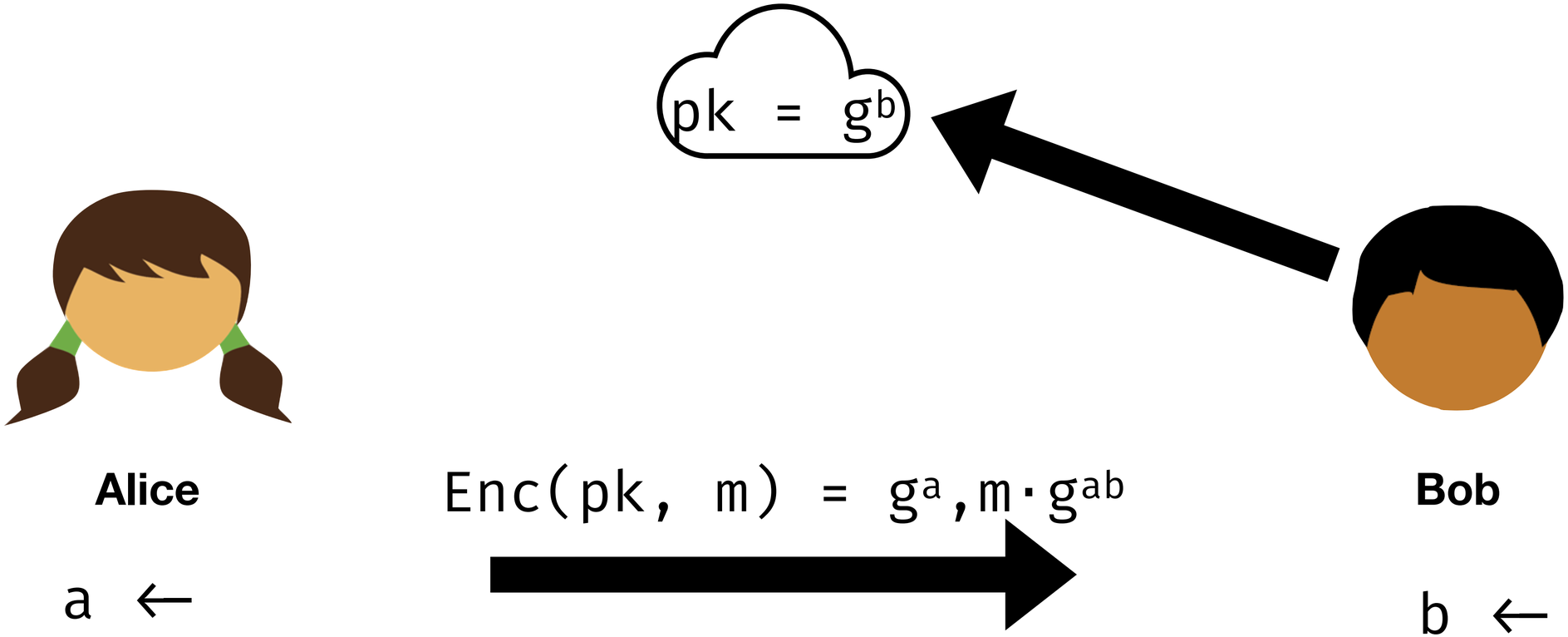


$Enc(pk, m) = g^a, m \cdot g^{ab}$

Bob

$b \leftarrow$

Refresher: ElGamal Encryption



$$\mathrm{Enc}(pk, m0) \cdot \mathrm{Enc}(pk, m1) = \mathrm{Enc}(pk, m0 \cdot m1)$$

Multiplicative Homomorphism

Homomorphic Encryption

A homomorphic encryption scheme is a tuple of algorithms:

$$(Gen, Enc, Dec, Eval)$$

And a function class F s.t. for any f in F:

$$(sk, pk) \leftarrow Gen()$$

$$Dec(sk, Eval(f, Enc(pk, m)) = f(m)$$

(and CPA security holds)

Fully Homomorphic Encryption

A homomorphic encryption scheme is a tuple of algorithms:

```
(Gen, Enc, Dec, Eval)
```

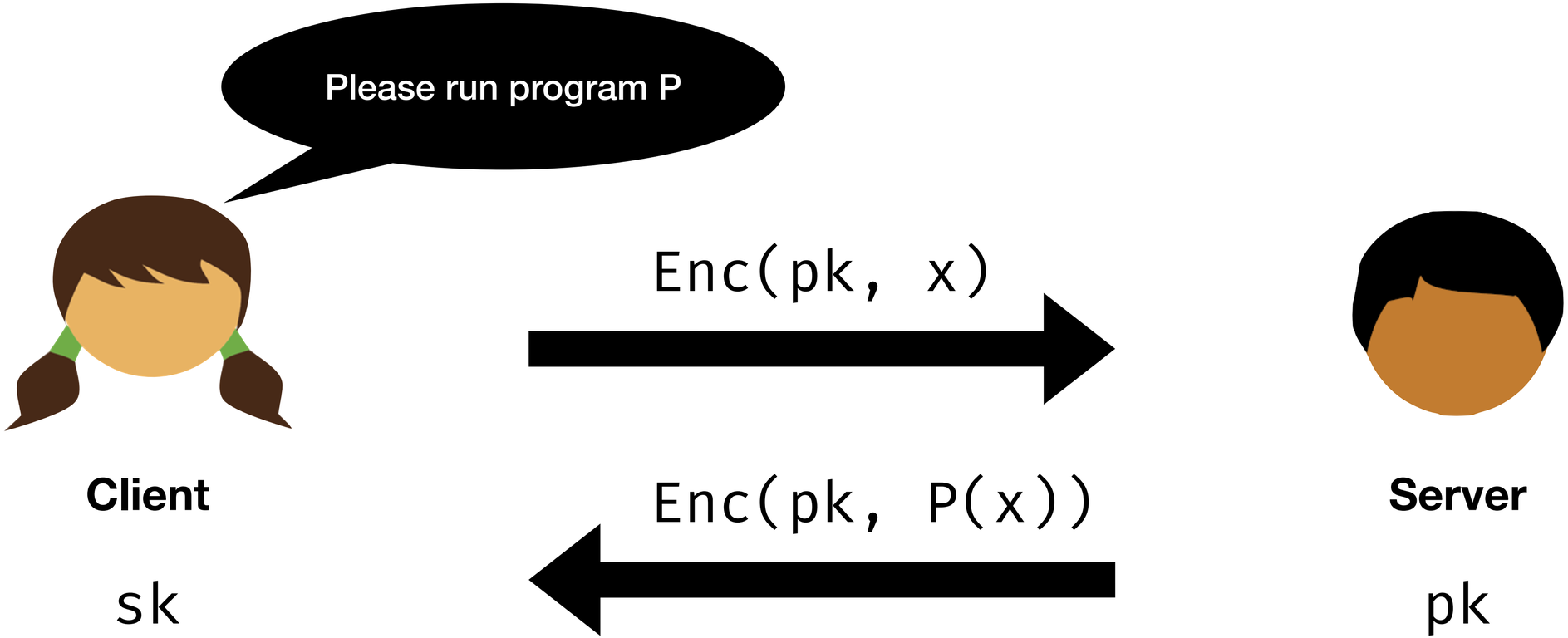
~~And a function class F s.t. for any f in F:~~
And for any computable function **f**

```
(sk, pk) ← Gen()
```

```
Dec(sk, Eval(f, Enc(pk, m)) = f(m)
```

(and CPA security holds)

Fully Homomorphic Encryption; Outsourced Computation



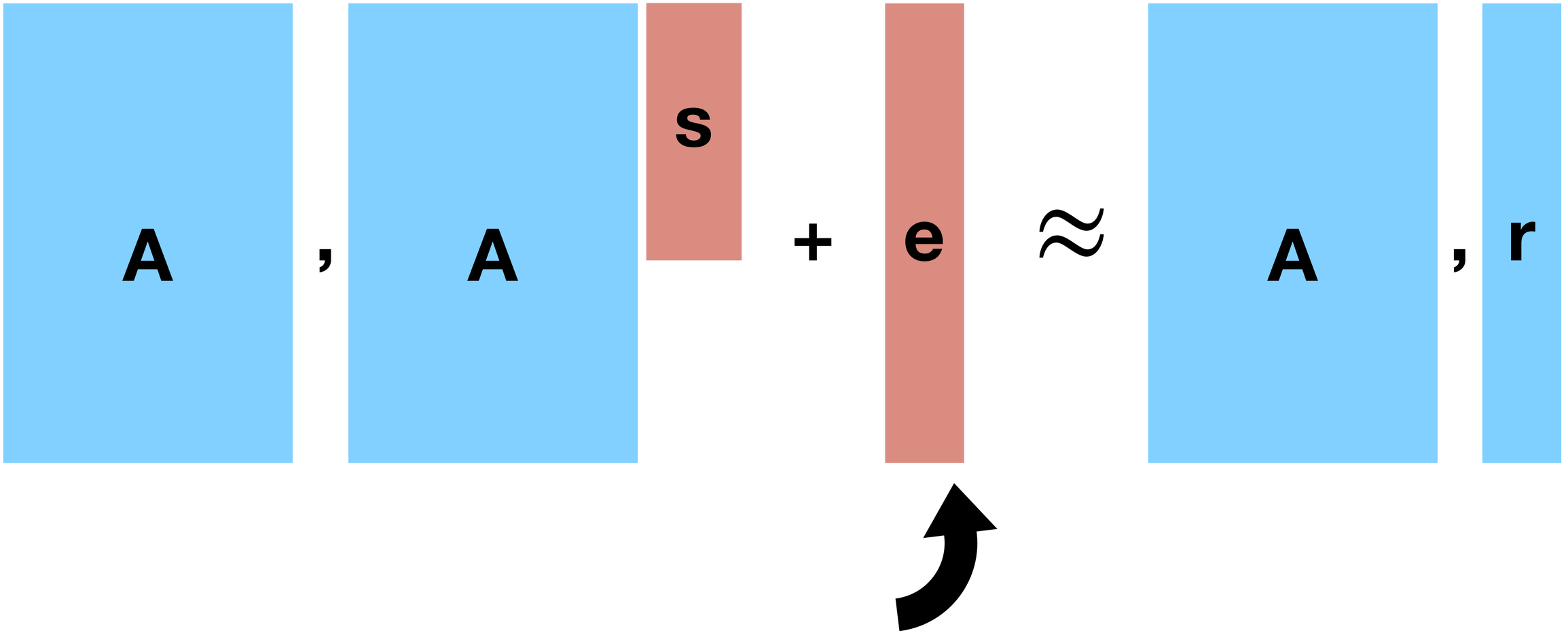
Fully Homomorphic Encryption

A FULLY HOMOMORPHIC ENCRYPTION SCHEME

A DISSERTATION
SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE
AND THE COMMITTEE ON GRADUATE STUDIES
OF STANFORD UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

Craig Gentry
September 2009

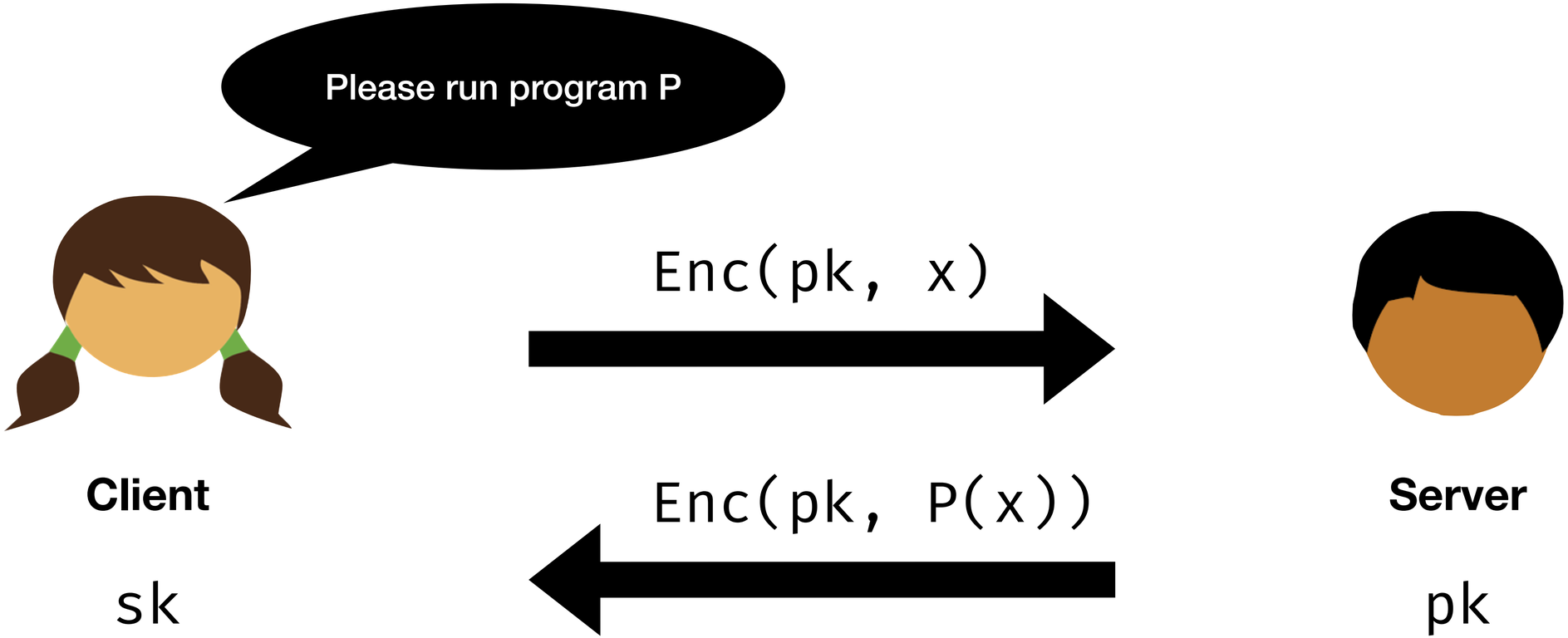
Learning with Errors



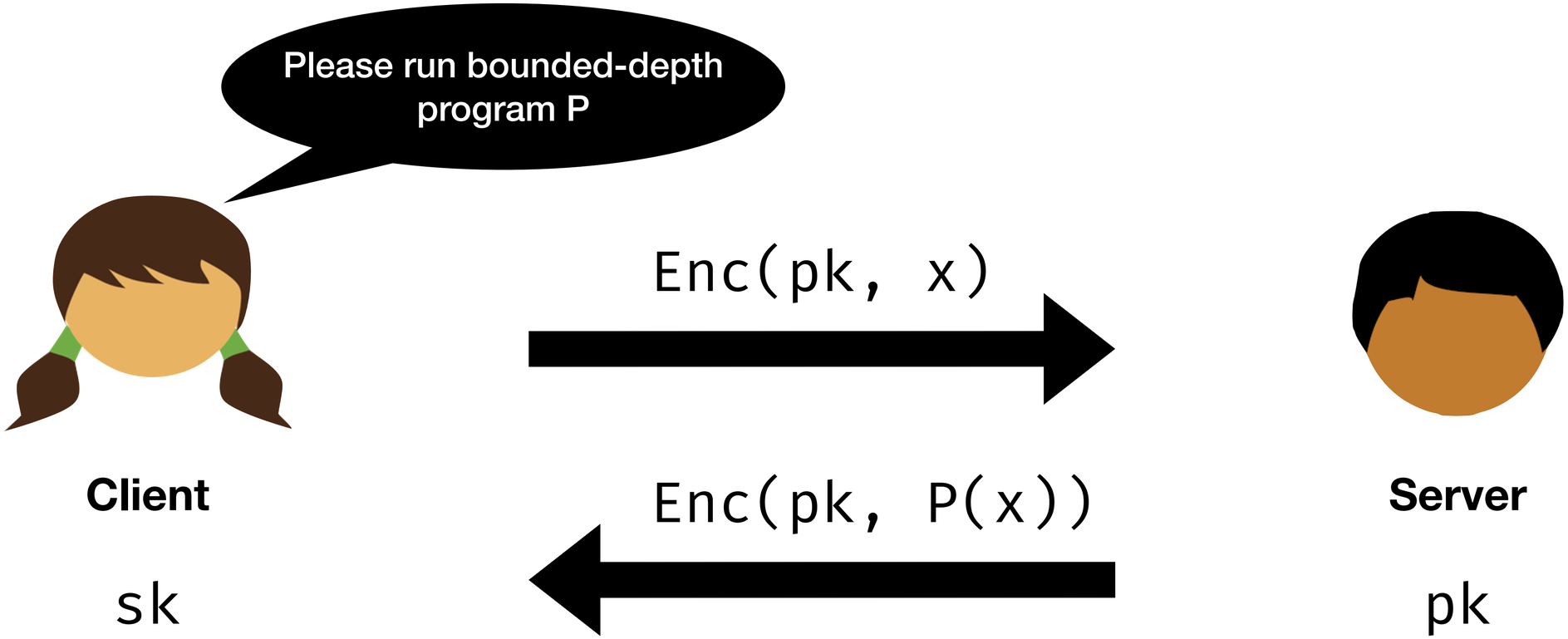
Integers are mod prime q

Small Gaussian noise

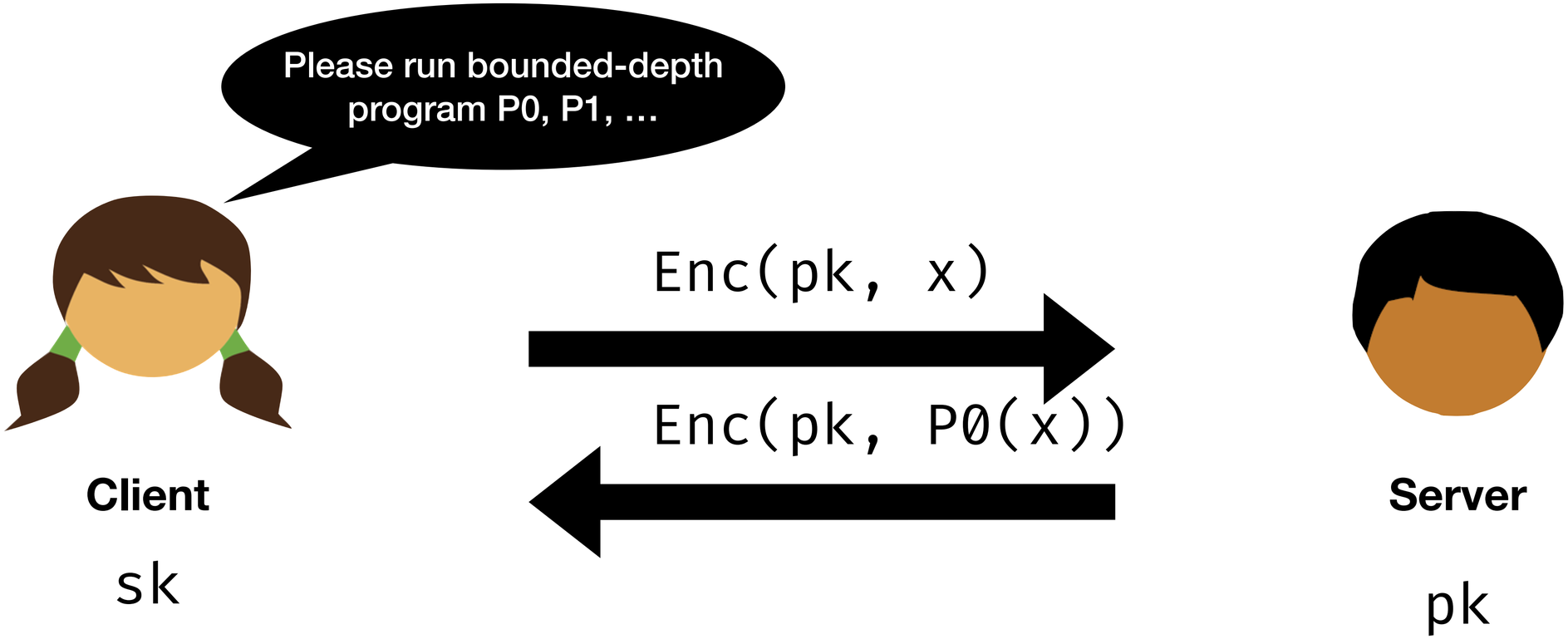
Fully Homomorphic Encryption; Outsourced Computation



Somewhat Homomorphic Encryption

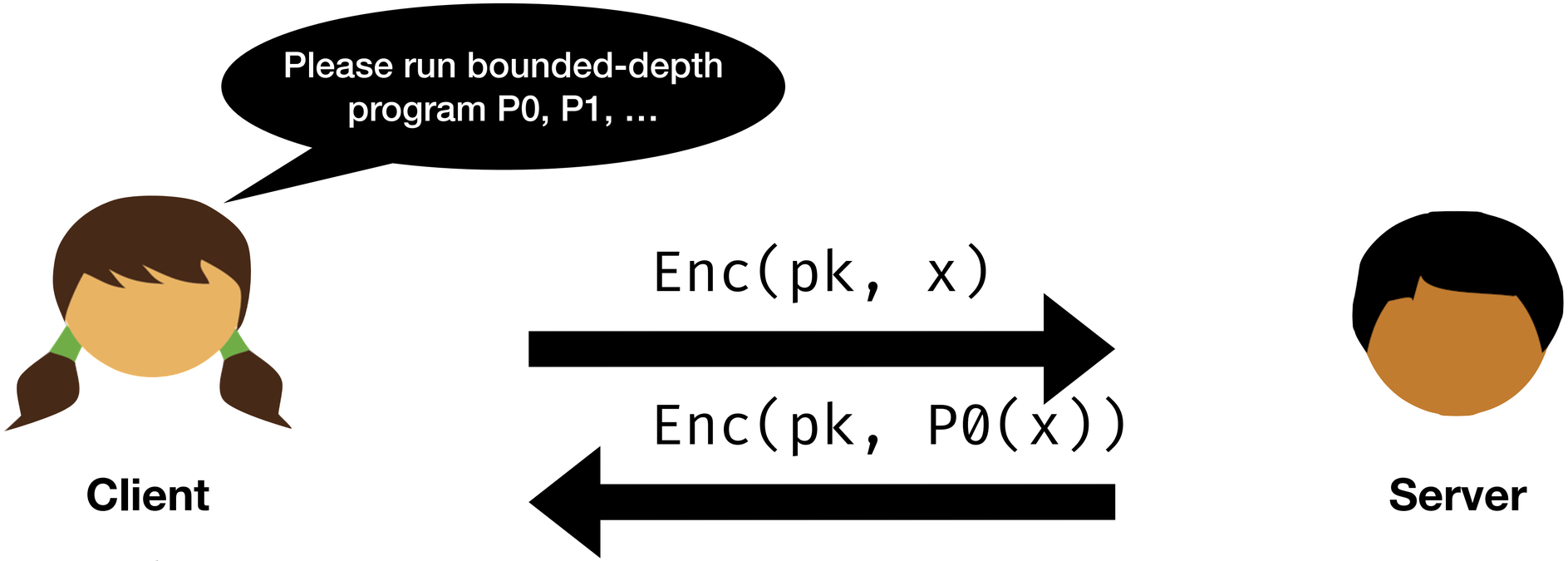


Somewhat Homomorphic Encryption; Outsourced Computation



…

Somewhat Homomorphic Encryption; Outsourced Computation

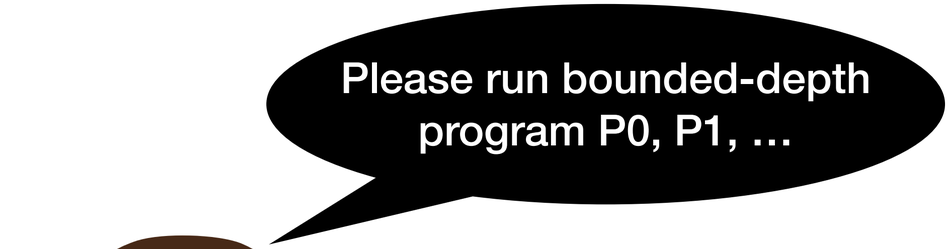


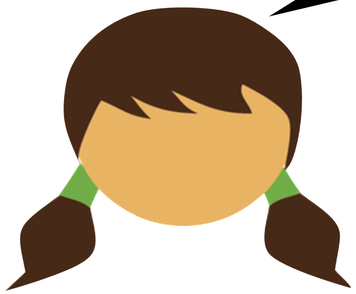

```
Enc(pk, Dec(pk, Enc(pk, P0(x))))
=
Enc(pk, P0(x))
```

But with lower noise

…

Somewhat Homomorphic Encryption; Outsourced Computation





Client

sk

Server

pk

Enc(pk, x)

Enc(pk, P0(x))

Enc(pk, P0(x))

Enc(pk, P1(P0(x)))

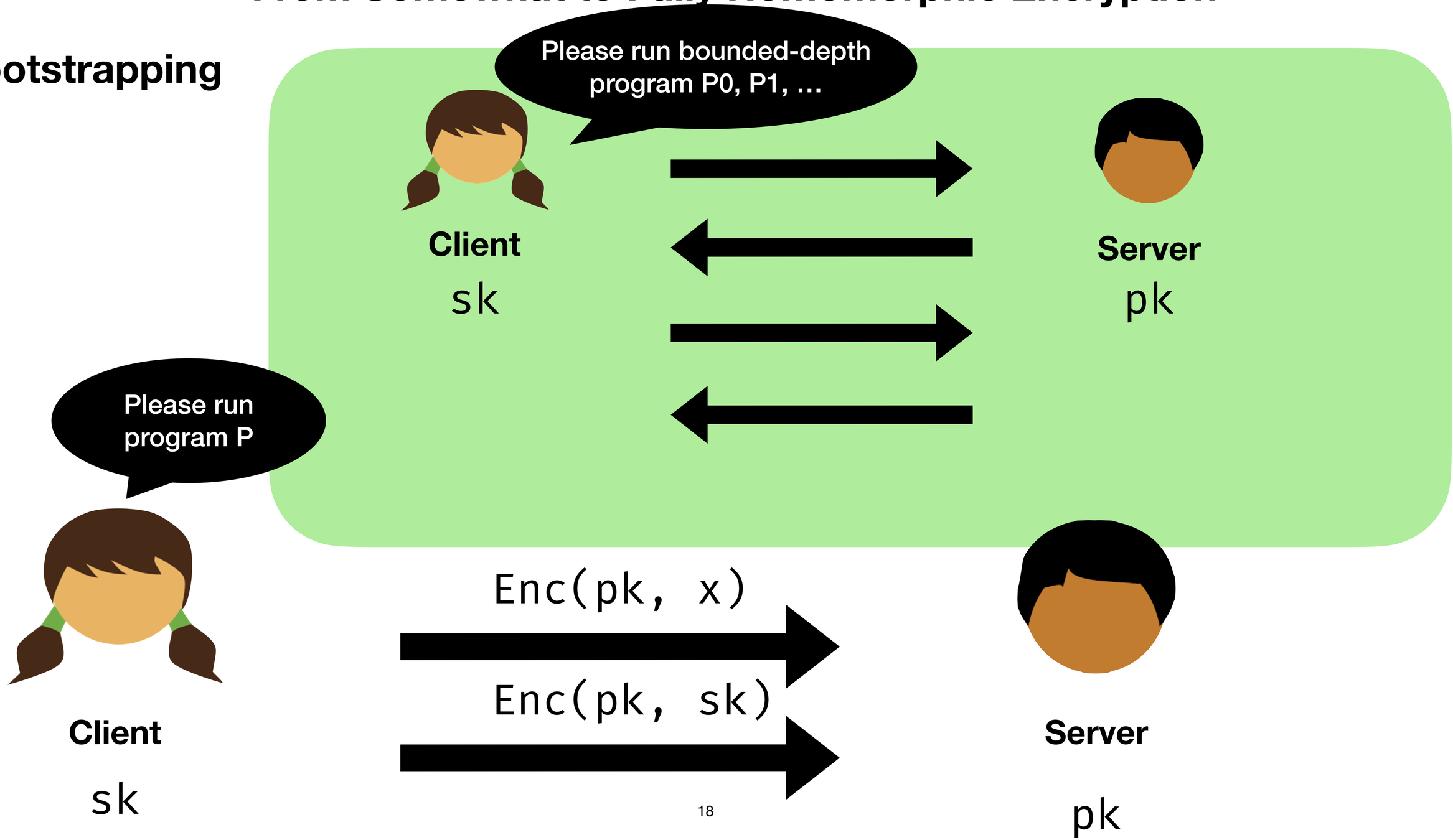
…

```
Enc(pk, Dec(pk, Enc(pk, P0(x))))
=
Enc(pk, P0(x))
```

But with lower noise

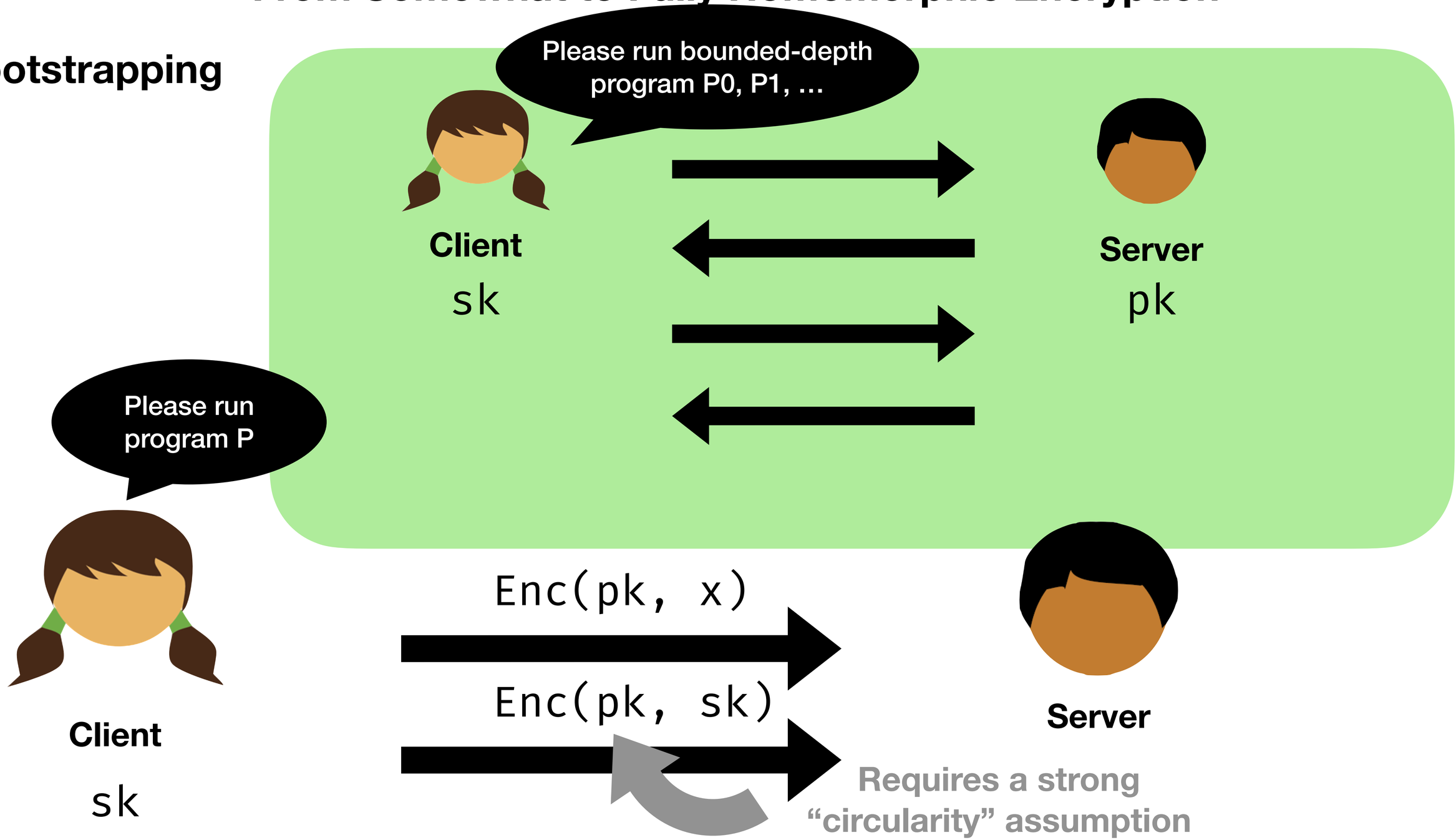
From Somewhat to Fully Homomorphic Encryption

Bootstrapping

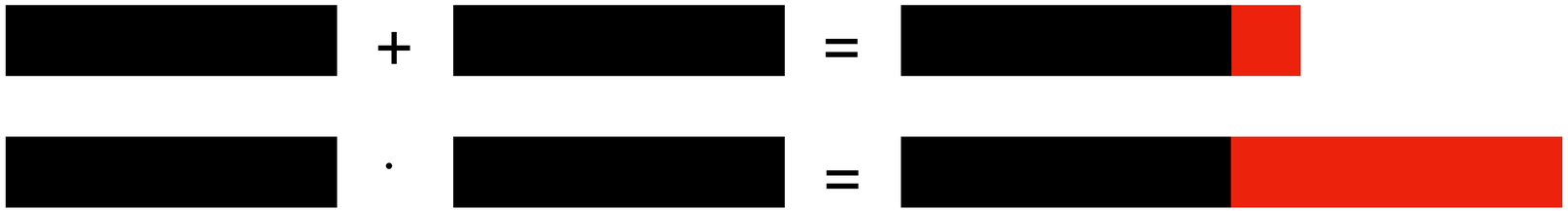


From Somewhat to Fully Homomorphic Encryption

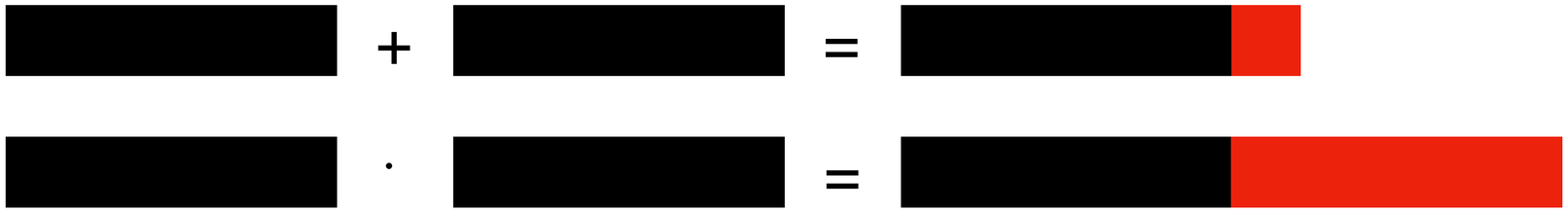
Bootstrapping

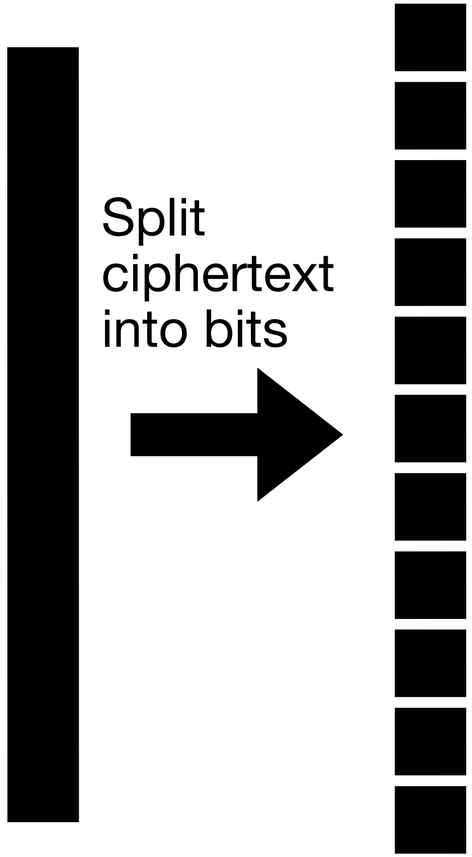


Fully Homomorphic Encryption

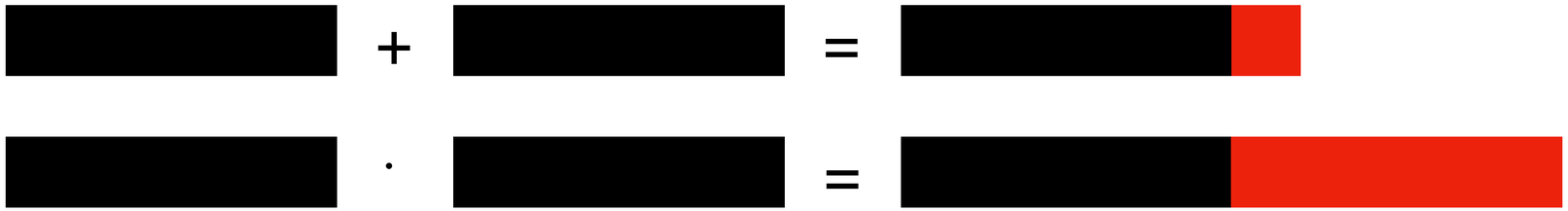


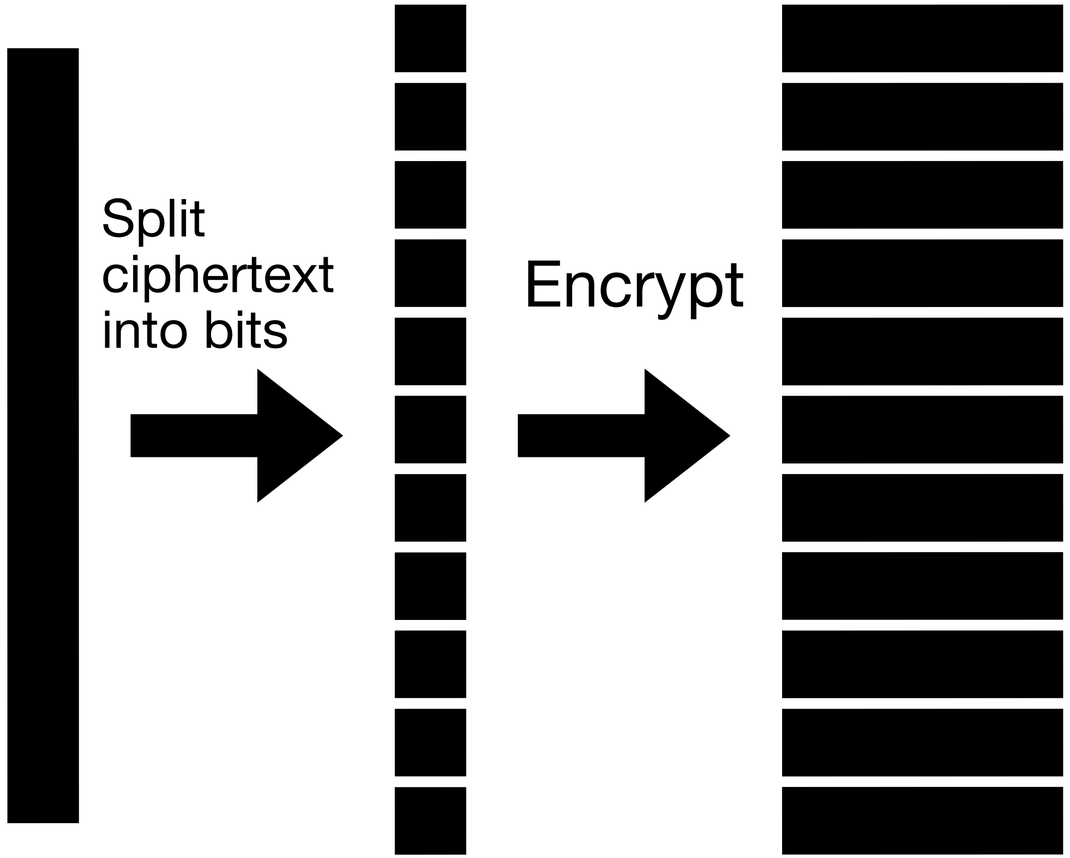
Fully Homomorphic Encryption



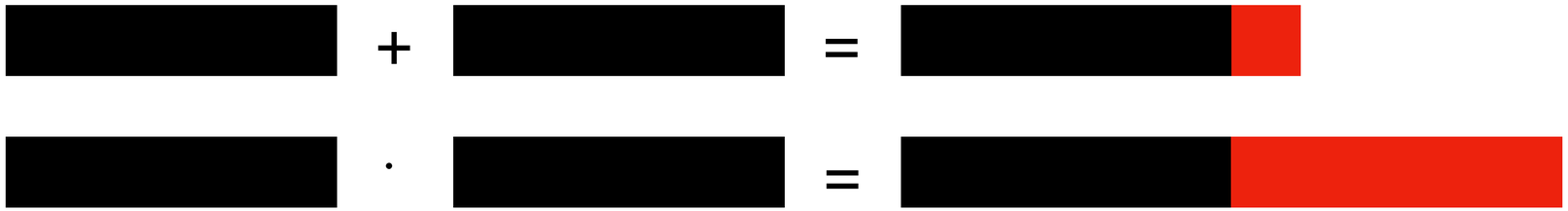


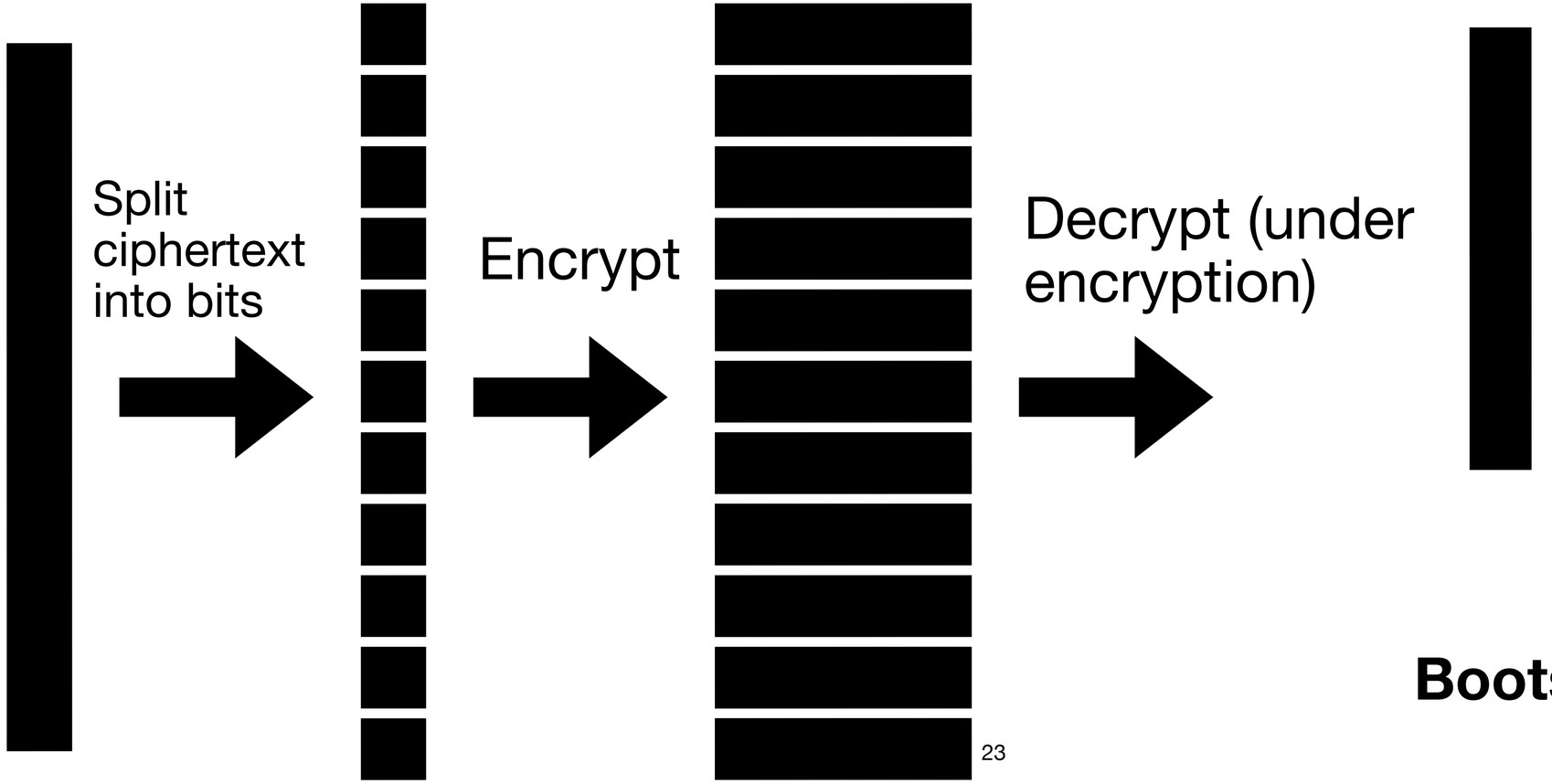
Fully Homomorphic Encryption





Fully Homomorphic Encryption





Bootstrapping

Today's objectives

Understand the notion of a homomorphism

See that public-key schemes have homomorphic properties

Understand the definition of fully homomorphic encryption (FHE)