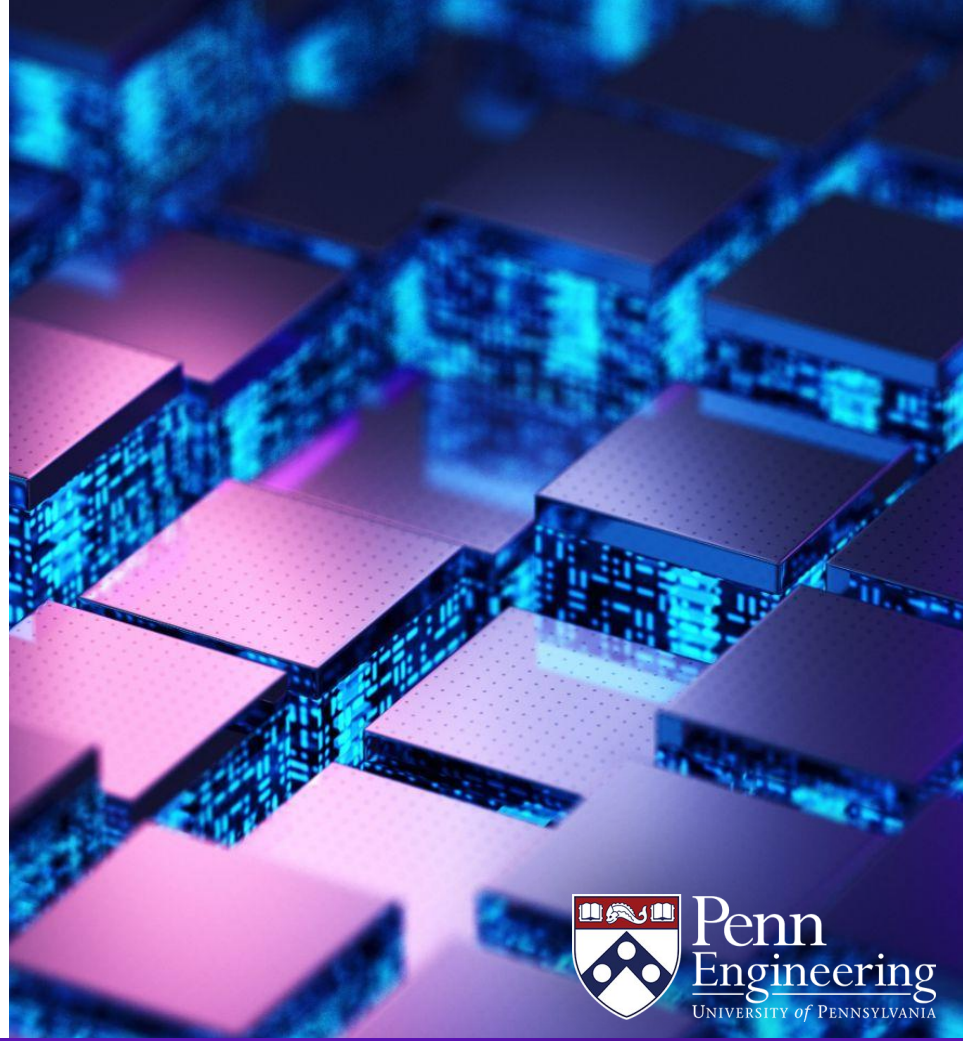
EAS 5830: BLOCKCHAINS

The Discrete-Log Problem

Professor Brett Hemenway Falk



Groups

- A group is a set, together with an operation, denoted by +
- **Closure**: if a and b are in the set, so is $a+b$
- **Associativity**: $(a+b)+c = a+(b+c)$
- **Identity**: There is an element, e, such that $a + e = e + a = a$ for all a
- **Inverses**: For every element, a, there is an element, $-a$ such that $a + (-a) = e$

Examples

- The Integers with the addition operation form a group
  - The set of even numbers with addition form a (sub)group
- {-1,1} form with multiplication form a group
  - More generally, the set of nth roots of unity form a group under multiplication
- The integers modulo n form a group under addition
- The nonzero integers modulo n form a group under multiplication (for prime n)
- The set of points on an elliptic curve can be made to form a group with an appropriate operation

Cyclic Groups

- There is a generator, G (possibly many)
- $\{ G, G+G, G+G+G, ... \}$ is the whole group

Discrete Logs

In a cyclic group, every element is of the form

$$H = \underbrace{G + G + \ldots + G + G}_{a \text{ times}}$$

Given an element H, can you find the integer a such that $H = aG$

The Elliptic-Curve Discrete-Log Problem

- Given a generator G and aG, it's hard to find the integer a
- ECDSA:
  - public key is aG
  - private key is a
- Same with Schnorr

Diffie-Hellman Key Exchange

EC-DL problem:
Given G and aG it's hard to find a

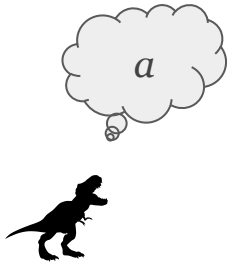
Alice

Bob

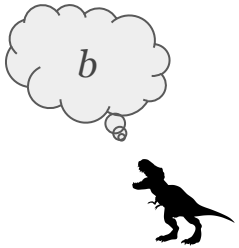
Goal: Alice and Bob want to come up with a shared secret (integer) that is unknown to any eavesdropper

Diffie-Hellman Key Exchange

EC-DL problem:
Given G and aG it's hard to find a



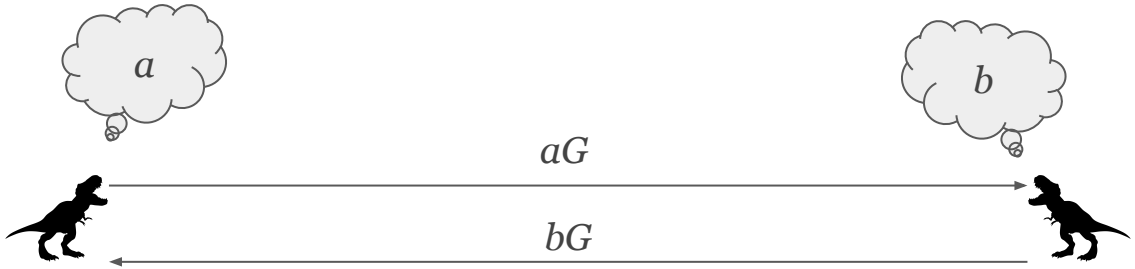
Alice



Bob

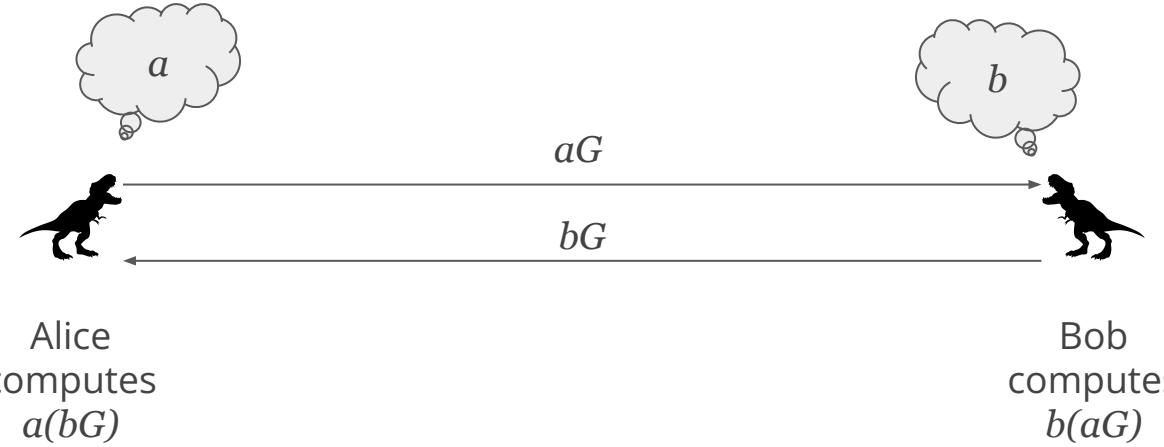
Diffie-Hellman Key Exchange

EC-DL problem:
Given G and aG it's hard to find a



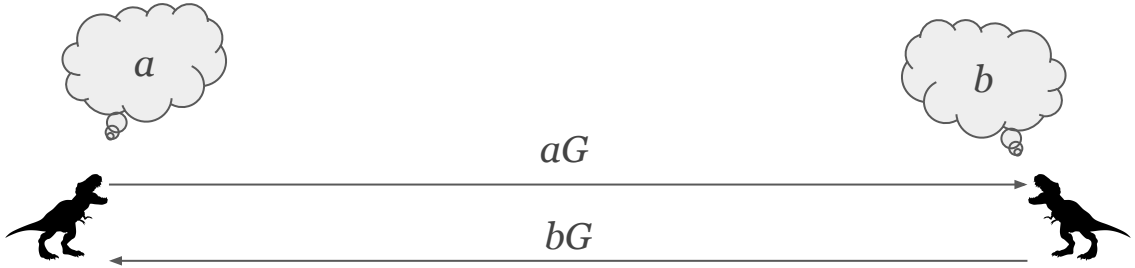
Diffie-Hellman Key Exchange

EC-DL problem:
Given G and aG it's hard to find a



Diffie-Hellman Key Exchange

EC-DL problem:
Given aG it's hard to find a



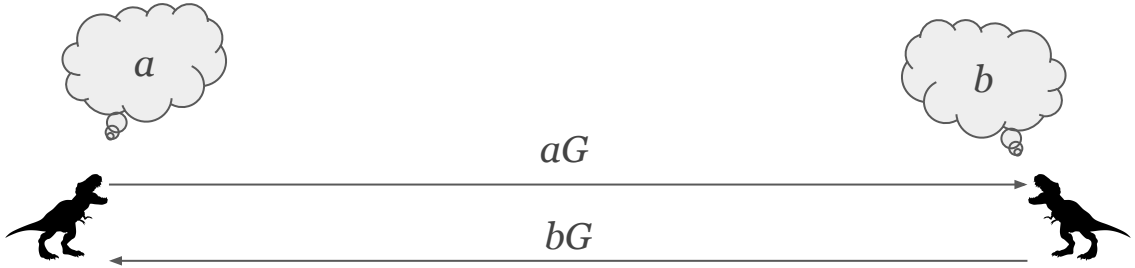
Alice computes $a(bG)$

Bob computes $b(aG)$

$H(abG) = H(baG)$ is a 256-bit integer that can be used as a private key

Diffie-Hellman Key Exchange

EC-DL problem:
Given aG it's hard to find a



Alice computes $a(bG)$

Bob computes $b(aG)$

Adversary sees aG, bG.
Adversary shouldn't be able to compute abG

The Decisional Diffie-Hellman Problem

Given aG and bG and another group element $H = cG$, determine if $c = ab$.

Elliptic Curve Groups

Easy

Hard

DL is easy

DL is hard but DDH is easy

DDH is hard