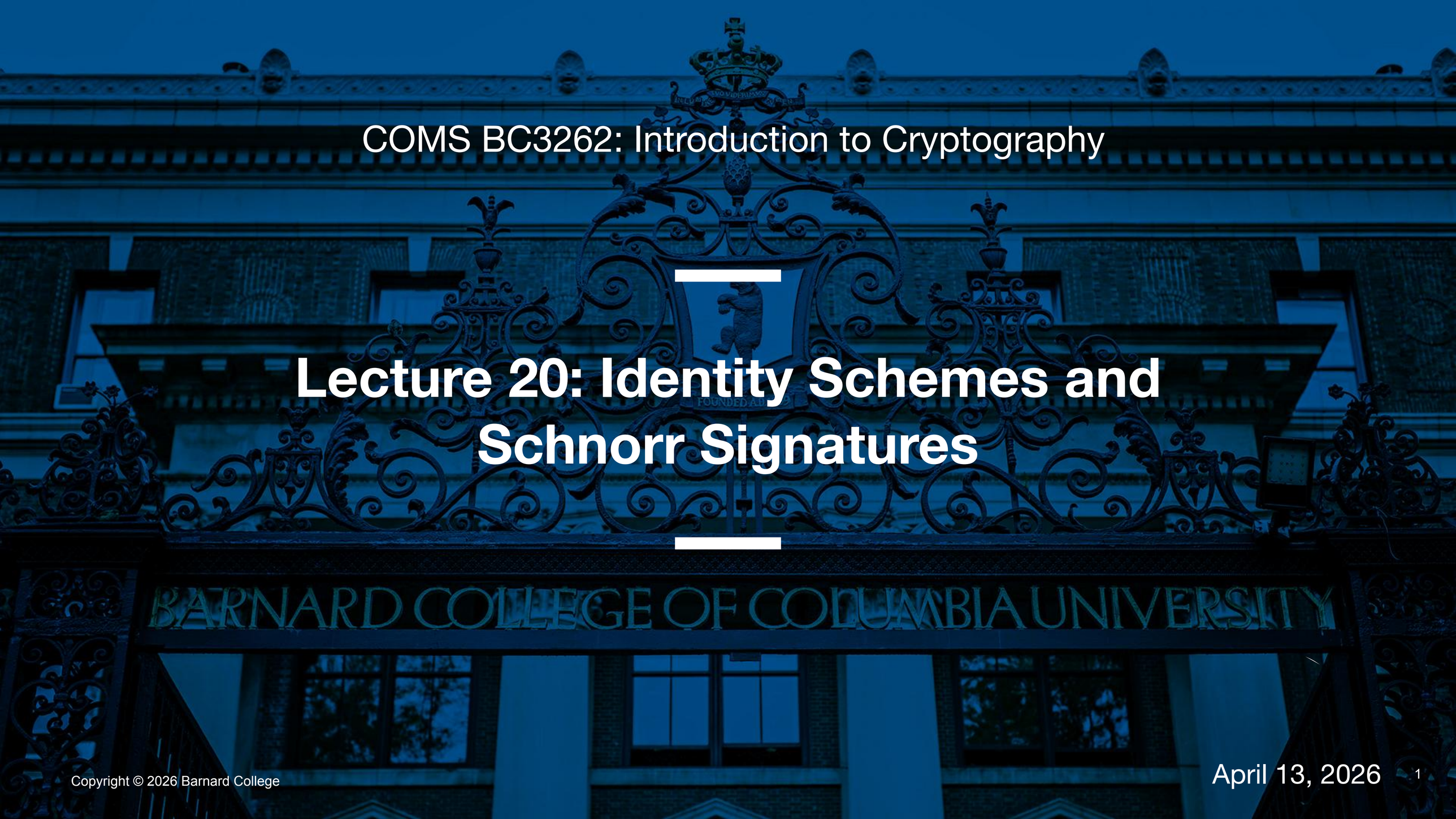


COMS BC3262: Introduction to Cryptography

Lecture 20: Identity Schemes and Schnorr Signatures

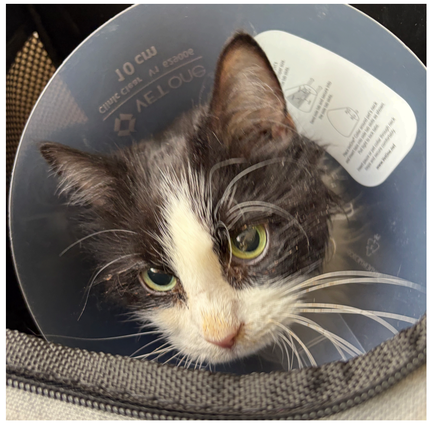
April 13, 2026

Logistics

- **Extra credit opportunity**: Attend Olive's talk Thursday, April 16 at 12pm in Milstein 402
  - Olive Franzese-McLaughlin will be giving a talk titled "Cryptographically Verified AI/ML Audits"
  - No explicit point value, but if you're near a cutoff I'll use this to determine if you get bumped up
- HW 4 due on Thursday
- HW 5 releases on Wednesday

Upcoming office hours

- My office hours this week will be on Wednesday 3pm-5pm
  - Subject to Gertrude not having anymore emergencies
- I will not have office hours next week while I am traveling
- Mark and Tony should be having their office hours as usual
- See EdStem for any updates



Gertrude’s surgery went well!

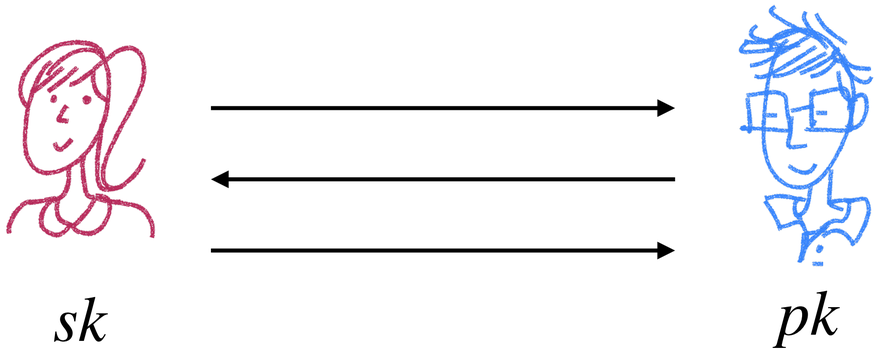
DL-Based Signatures

- 1986: El Gamal proposed the first DL-based signatures
- 1989: Schnorr proposed a more efficient scheme
  - Security based on DL in the random oracle model
  - Schnorr patented it… and no one used it (patent expired in 2008)
- 1991: NIST proposed DSA (Digital Signature Algorithm)
  - Based on El Gamal and Schnorr, but sufficiently different
  - ECDSA: elliptic curve variant and is very popular
- 2011: EdDSA signatures
  - Essentially Schnorr’s signatures on a specific family of elliptic curves called Edward’s curves

Identification Schemes

Identification Scheme

- Alice wants to prove to Bob she knows the sk associated with pk
- If Eve observes the communication (possibly many times), she can't later impersonate Alice
  - Eve should not be able to convince Bob she knows sk
  - Bob can't later impersonate Alice either



Schnorr's Identification Scheme

Suppose Alice and Bob have $\mathbb{G}, q, g, y = g^x$, where $\mathbb{G} = \langle g \rangle$ is a cyclic group of prime order q, and Alice wants to convince Bob she knows x

$sk = x$

$\mathbb{G}, q, g, y$

$pk = y$

Schnorr's Identification Scheme

Suppose Alice and Bob have $\mathbb{G}, q, g, y = g^x$, where $\mathbb{G} = \langle g \rangle$ is a cyclic group of prime order q, and Alice wants to convince Bob she knows x

$sk = x$

$k \leftarrow \mathbb{Z}_q$

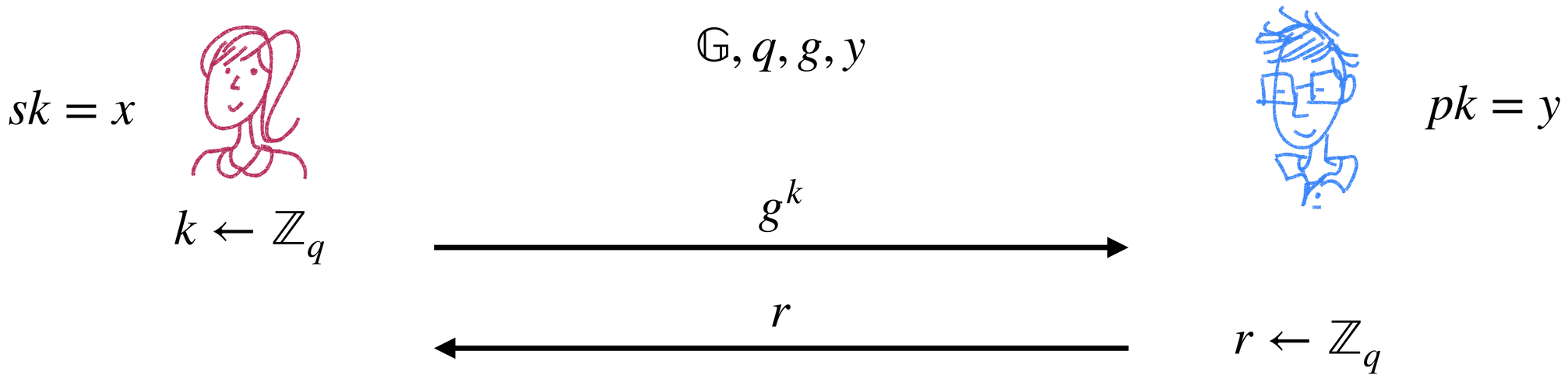
$\mathbb{G}, q, g, y$

g^k

$pk = y$

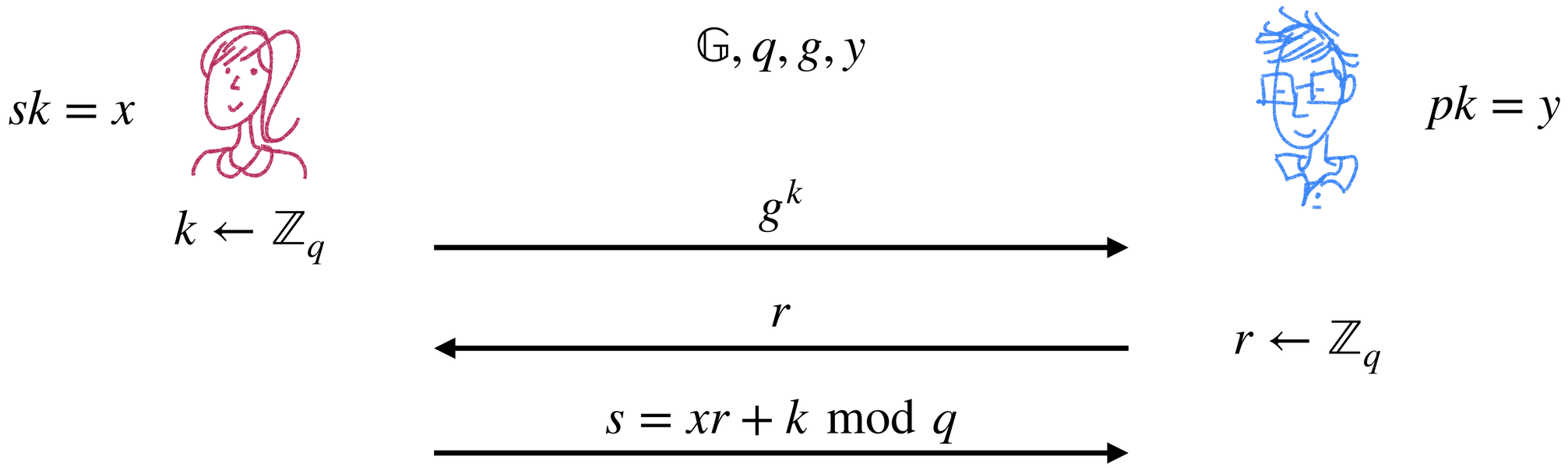
Schnorr's Identification Scheme

Suppose Alice and Bob have $\mathbb{G}, q, g, y = g^x$, where $\mathbb{G} = \langle g \rangle$ is a cyclic group of prime order q, and Alice wants to convince Bob she knows x



Schnorr's Identification Scheme

Suppose Alice and Bob have $\mathbb{G}, q, g, y = g^x$, where $\mathbb{G} = \langle g \rangle$ is a cyclic group of prime order q, and Alice wants to convince Bob she knows x



Schnorr's Identification Scheme

Suppose Alice and Bob have $\mathbb{G}, q, g, y = g^x$, where $\mathbb{G} = \langle g \rangle$ is a cyclic group of prime order q, and Alice wants to convince Bob she knows x

$sk = x$

$k \leftarrow \mathbb{Z}_q$

$\mathbb{G}, q, g, y$

g^k

r

$s = xr + k \mod q$

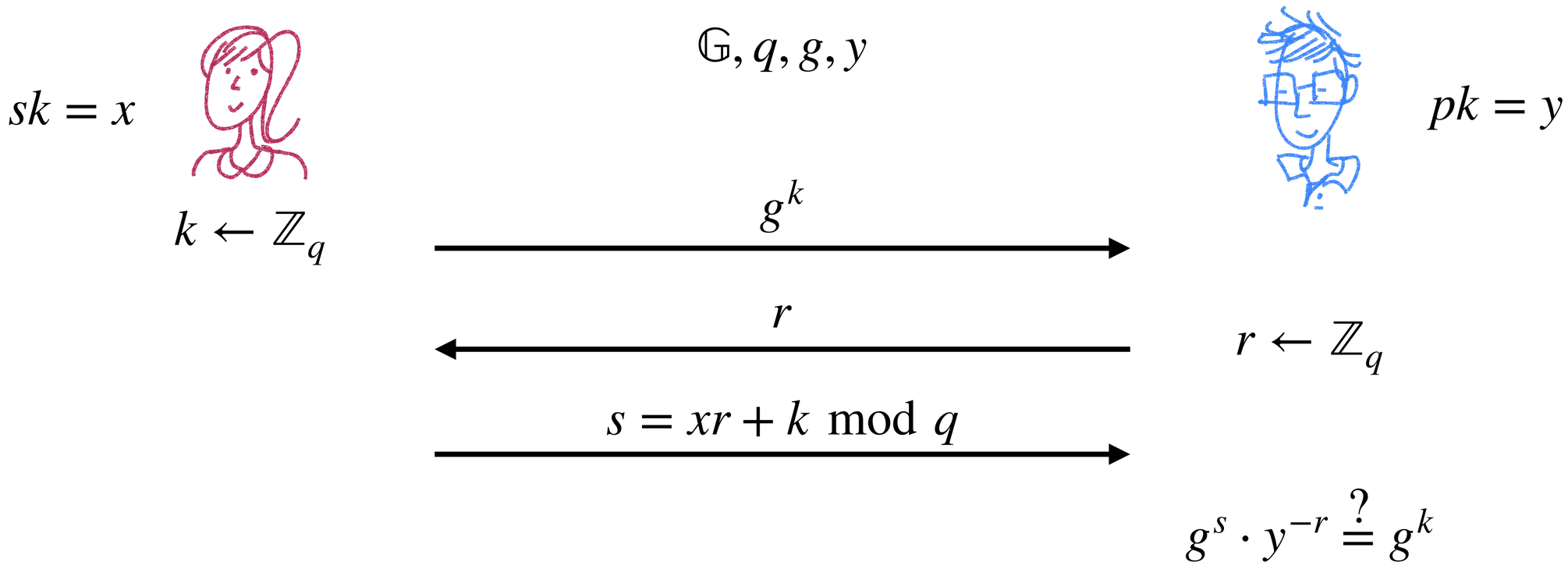
$pk = y$

$r \leftarrow \mathbb{Z}_q$

$g^s \cdot y^{-r} \stackrel{?}{=} g^k$

Schnorr's Identification Scheme

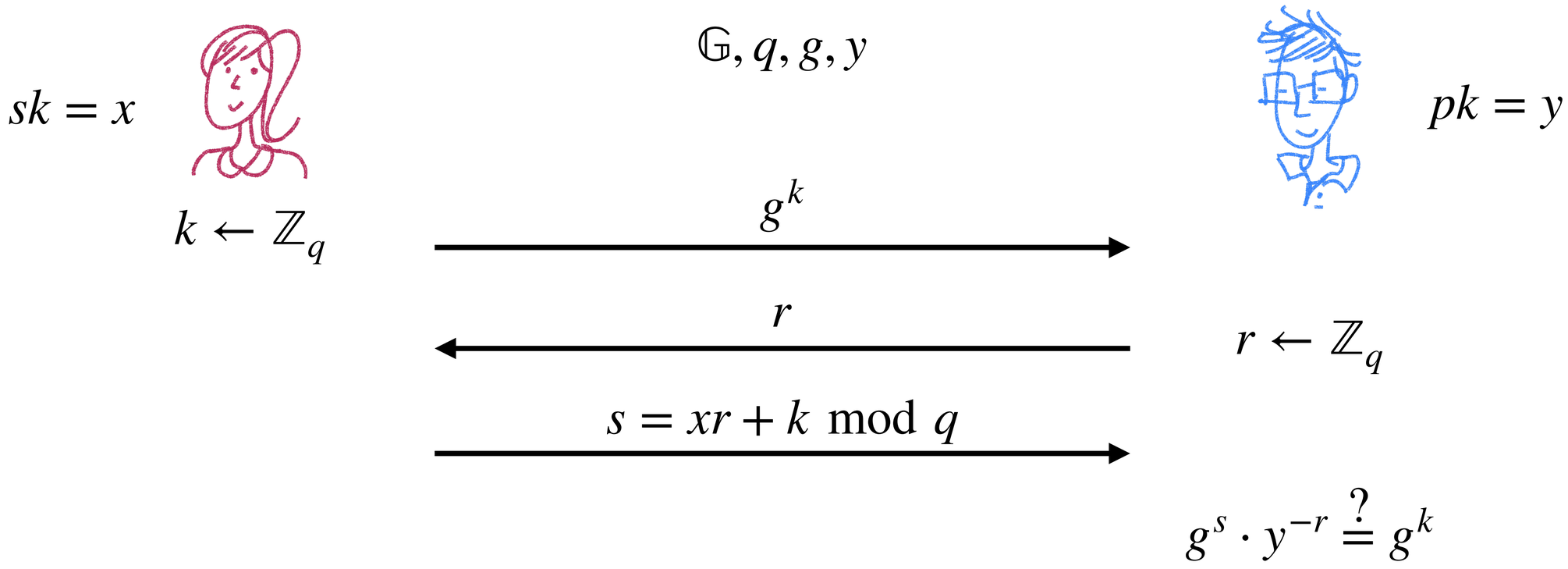
Suppose Alice and Bob have $\mathbb{G}, q, g, y = g^x$, where $\mathbb{G} = \langle g \rangle$ is a cyclic group of prime order q, and Alice wants to convince Bob she knows x



Correctness: $g^s \cdot y^{-r} = g^{xr+k} \cdot (g^x)^{-r} = g^k$

Schnorr's Identification Scheme

Suppose Alice and Bob have $\mathbb{G}, q, g, y = g^x$, where $\mathbb{G} = \langle g \rangle$ is a cyclic group of prime order q, and Alice wants to convince Bob she knows x



Correctness: $g^s \cdot y^{-r} = g^{xr+k} \cdot (g^x)^{-r} = g^k$

Security?

Security of Schnorr's Identification Scheme

Intuitively, if an adversary could answer any challenge r (without knowledge of x) *after* sending g^k, then the adversary could solve for the discrete log of y

$k \leftarrow \mathbb{Z}_q$

g^k →

← r

$r \leftarrow \mathbb{Z}_q$

$s = xr + k \bmod q$ →

$g^s \cdot y^{-r} \stackrel{?}{=} g^k$

Security of Schnorr's Identification Scheme

Intuitively, if an adversary could answer any challenge r (without knowledge of x) *after* sending g^k, then the adversary could solve for the discrete log of y

Suppose an adversary Eve could convince Bob:

$k \leftarrow \mathbb{Z}_q$

g^k →

← r

$r \leftarrow \mathbb{Z}_q$

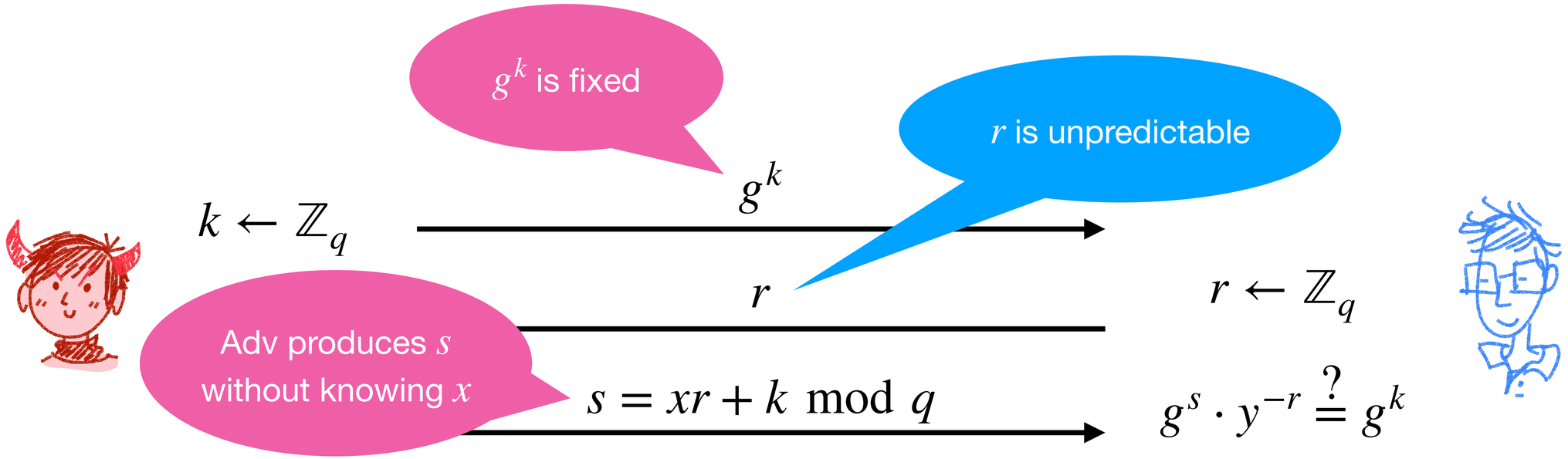
$s = xr + k \mod q$ →

$g^s \cdot y^{-r} \stackrel{?}{=} g^k$

Security of Schnorr's Identification Scheme

Intuitively, if an adversary could answer any challenge r (without knowledge of x) *after* sending g^k, then the adversary could solve for the discrete log of y

Suppose an adversary Eve could convince Bob:

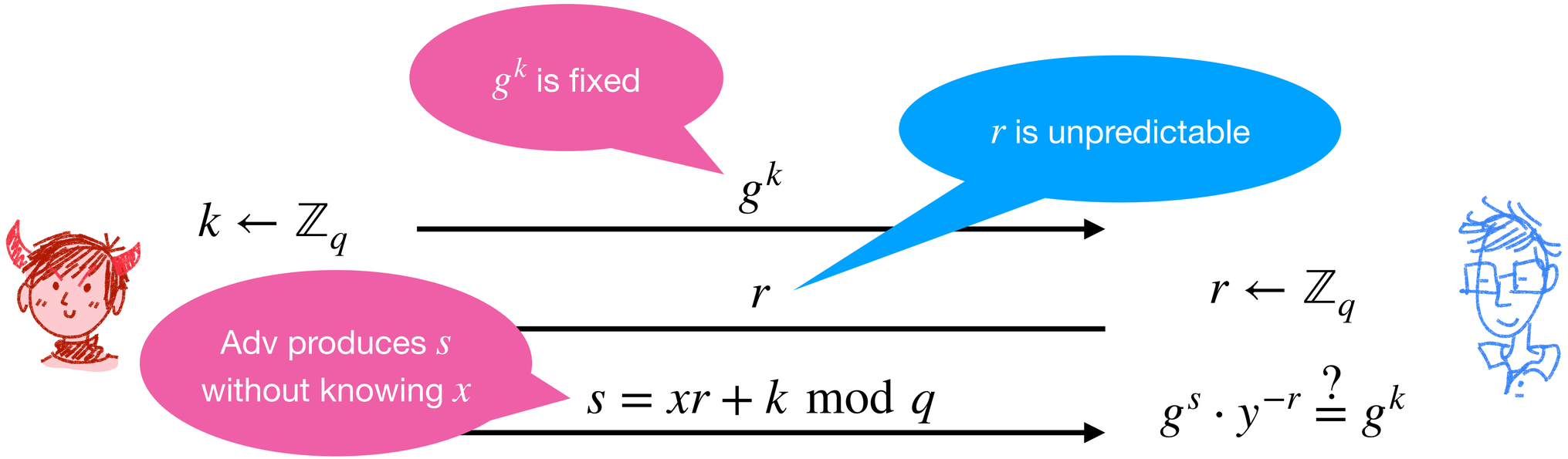


Security of Schnorr's Identification Scheme

Intuitively, if an adversary could answer any challenge r (without knowledge of x) *after* sending g^k, then the adversary could solve for the discrete log of y

Suppose an adversary Eve could convince Bob:

- For some g^k, Eve can produce accepting s, s' for $r \neq r'$



Security of Schnorr's Identification Scheme

Intuitively, if an adversary could answer any challenge r (without knowledge of x) *after* sending g^k, then the adversary could solve for the discrete log of y

Suppose an adversary Eve could convince Bob:

- For some g^k, Eve can produce accepting s, s' for $r \neq r'$
- For Bob to accept, $s = xr + k \mod q$ and $s' = xr' + k \mod q$

$k \leftarrow \mathbb{Z}_q$

g^k

r

$s = xr + k \mod q$

$r \leftarrow \mathbb{Z}_q$

$g^s \cdot y^{-r} \stackrel{?}{=} g^k$

Security of Schnorr's Identification Scheme

Intuitively, if an adversary could answer any challenge r (without knowledge of x) *after* sending g^k, then the adversary could solve for the discrete log of y

Suppose an adversary Eve could convince Bob:

- For some g^k, Eve can produce accepting s, s' for $r \neq r'$
- For Bob to accept, $s = xr + k \mod q$ and $s' = xr' + k \mod q$
  - Together Eve can compute $x = (s - s') \cdot (r - r')^{-1} \mod q$

$k \leftarrow \mathbb{Z}_q$

g^k →

← r

$r \leftarrow \mathbb{Z}_q$

$s = xr + k \mod q$ →

$g^s \cdot y^{-r} \stackrel{?}{=} g^k$

Security of Schnorr's Identification Scheme

What if r is known in advance *before* the adversary sends g^k?

$k \leftarrow \mathbb{Z}_q$

g^k

r is unpredictable

r

$r \leftarrow \mathbb{Z}_q$

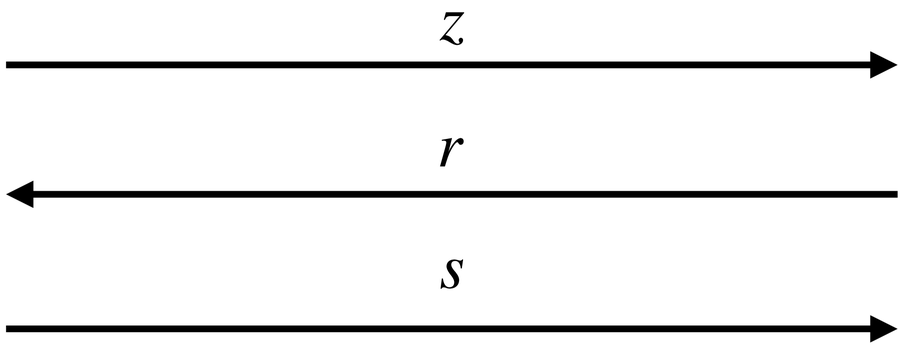
$s = xr + k \mod q$

$g^s \cdot y^{-r} \stackrel{?}{=} g^k$

Security of Schnorr's Identification Scheme

What if r is known in advance *before* the adversary sends g^k?

Given r, how might an adversary choose z so she knows a s that Bob will accept?

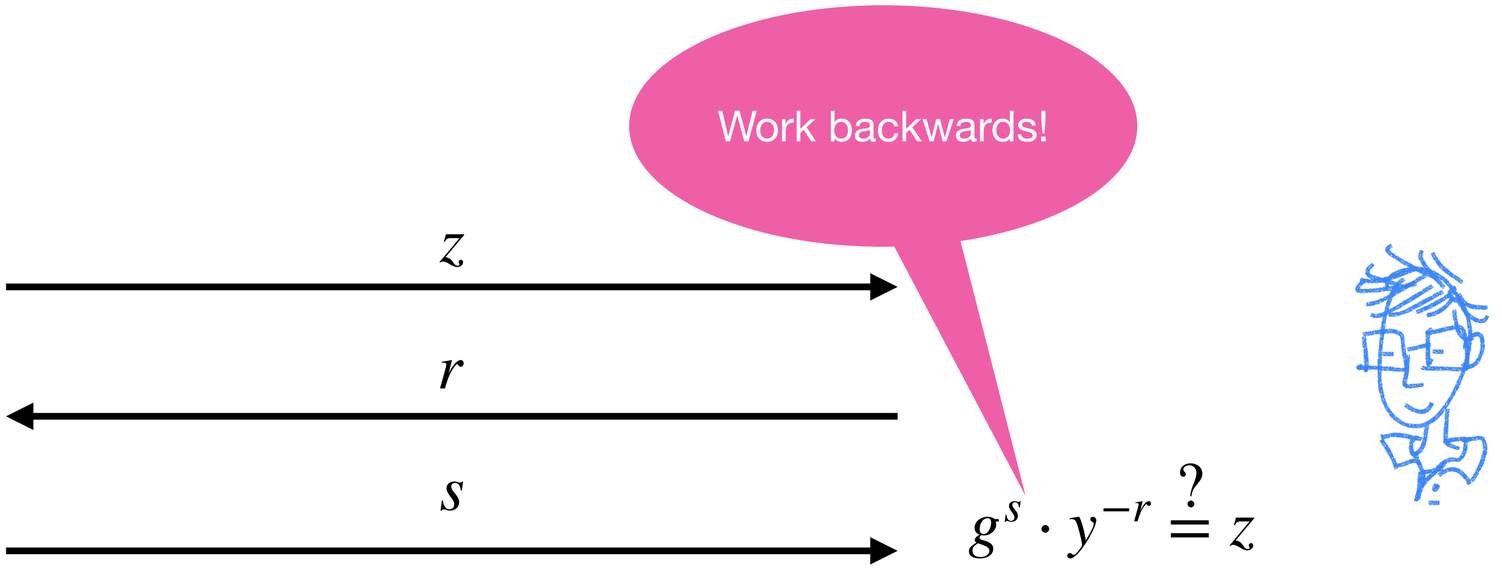


$$g^s \cdot y^{-r} \stackrel{?}{=} z$$

Security of Schnorr's Identification Scheme

What if r is known in advance *before* the adversary sends g^k?

Given r, how might an adversary choose z so she knows a s that Bob will accept?

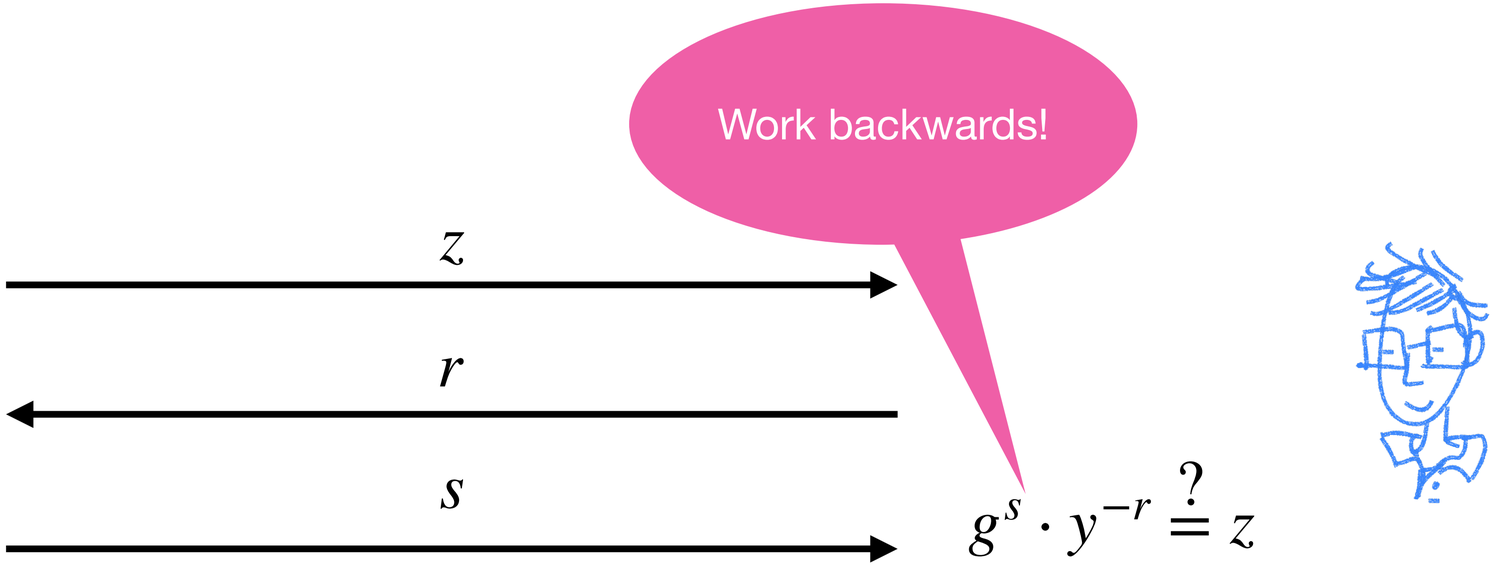


Security of Schnorr's Identification Scheme

What if r is known in advance *before* the adversary sends g^k?

Given r, how might an adversary choose z so she knows a s that Bob will accept?

- Adversary samples $s \leftarrow \mathbb{Z}_q$ and computes $z = g^s \cdot y^{-r}$
  - Eve does not need to know the discrete log of z to convince Bob

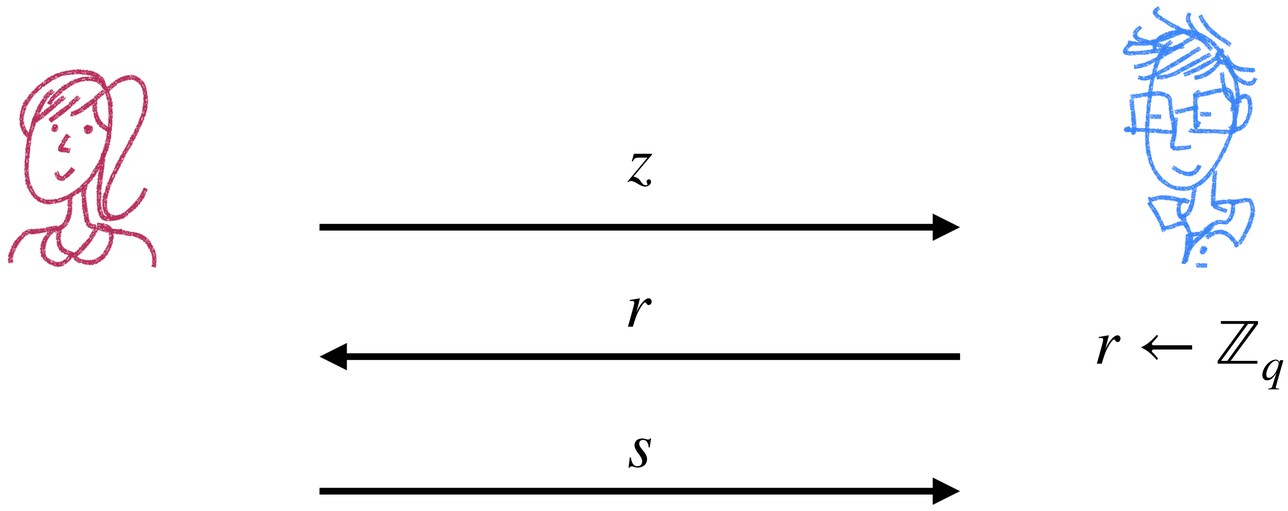


From identification schemes to signatures

Fiat-Shamir Transform

Given a three message identification scheme where r is random, do we really need Bob to choose r?

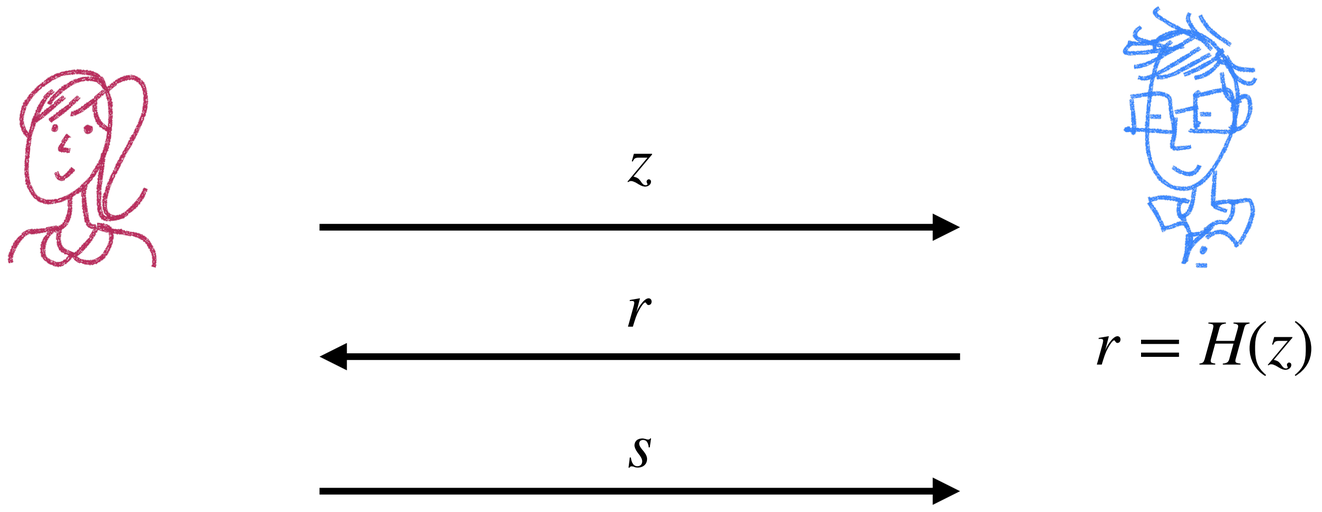
- Is there some way we can make this non-interactive?



Fiat-Shamir Transform

Given a three message identification scheme where r is random, do we really need Bob to choose r?

- Is there some way we can make this non-interactive?
- What if we compute the challenge as $r = H(z)$?



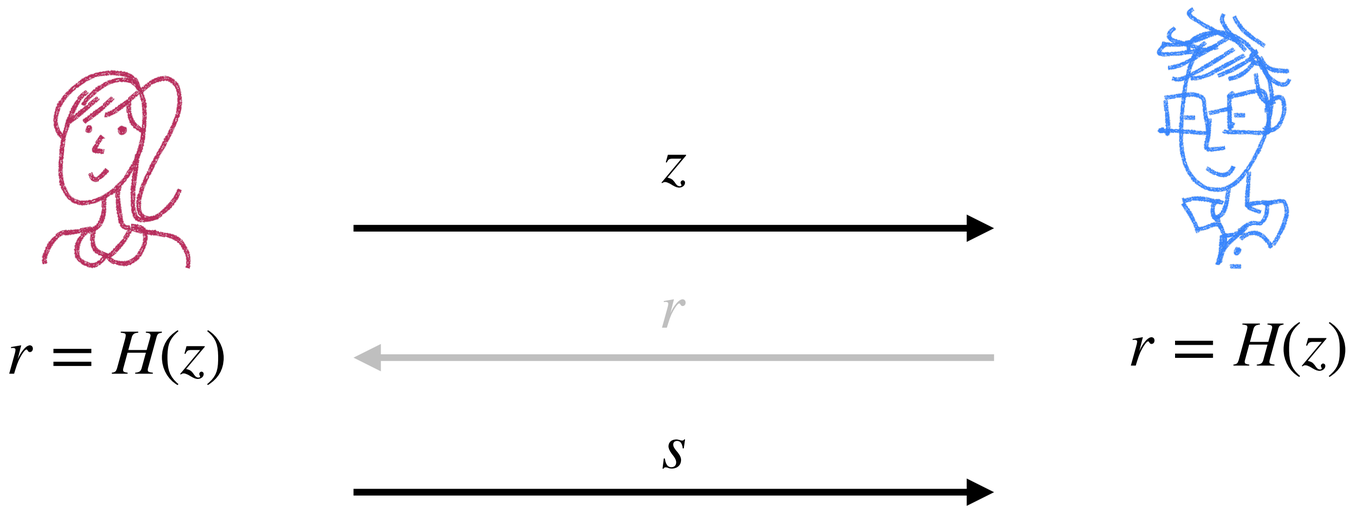
Fiat-Shamir Transform

Given a three message identification scheme where r is random, do we really need Bob to choose r?

- Is there some way we can make this non-interactive?

- What if we compute the challenge as $r = H(z)$?

- Alice can generate r on her own!



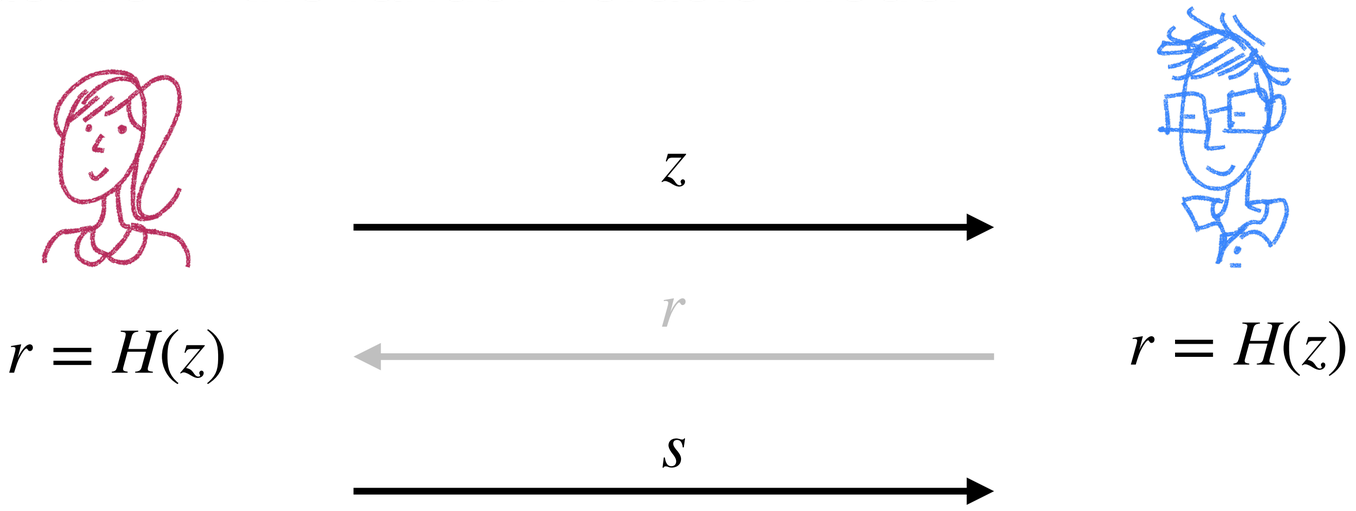
Fiat-Shamir Transform

Given a three message identification scheme where r is random, do we really need Bob to choose r?

- Is there some way we can make this non-interactive?

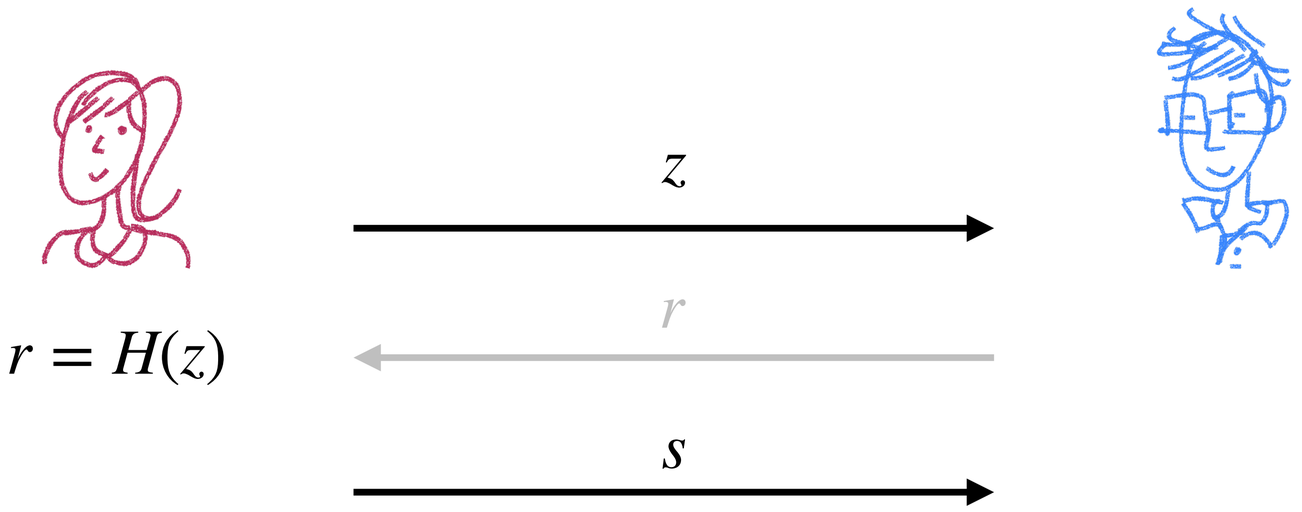
- What if we compute the challenge as $r = H(z)$?

- Alice can generate r on her own!
  - Non-interactive in the random oracle model



Fiat-Shamir Transform

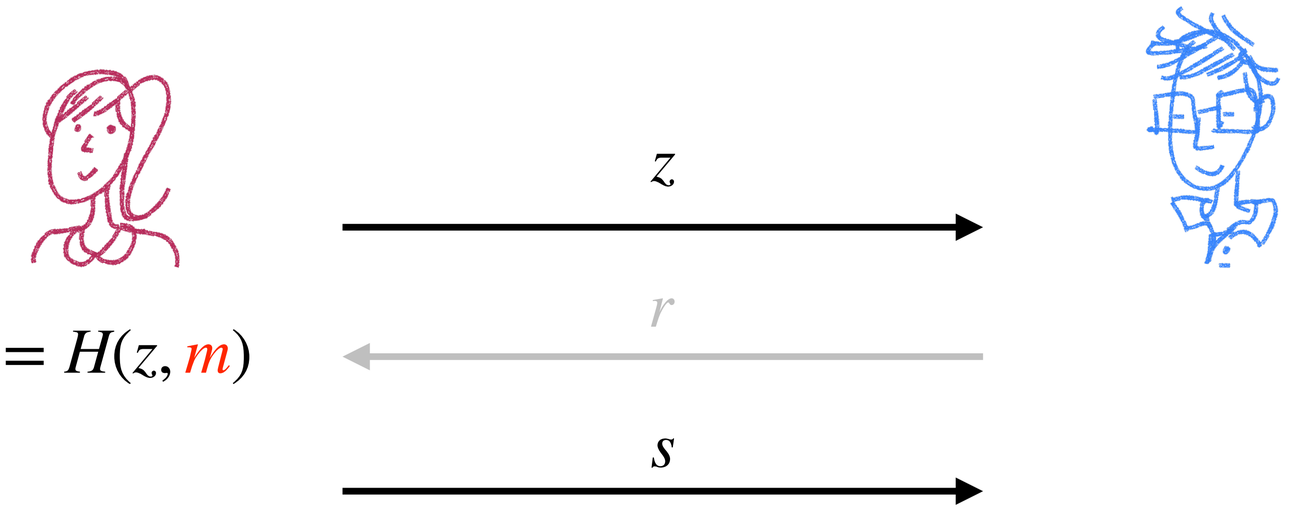
Can we turn this into a signature scheme?



Fiat-Shamir Transform

Can we turn this into a signature scheme?

- Derive r from both z and the message m



Fiat-Shamir Transform

Can we turn this into a signature scheme?

- Derive r from both z and the message m
- The signature consists of (z, s)
- To verify given $(m, (z, s))$, check that Bob would've accepted the identification scheme with $r = H(z, m)$

$r = H(z, m)$

z

r

s

Schnorr Signature Scheme

Idea: Apply the Fiat-Shamir transform (with the message) to Schnorr's identification scheme.

$k \leftarrow \mathbb{Z}_q$

g^k

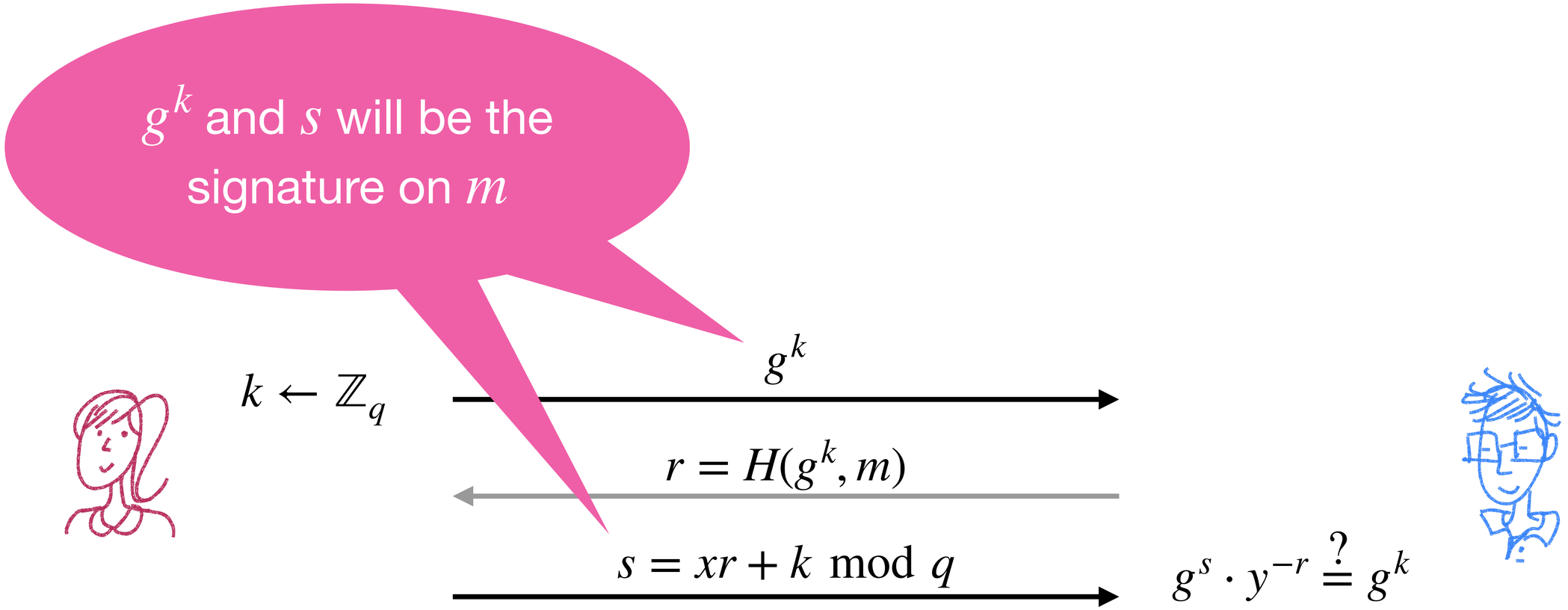
$r = H(g^k, m)$

$s = xr + k \mod q$

$g^s \cdot y^{-r} \stackrel{?}{=} g^k$

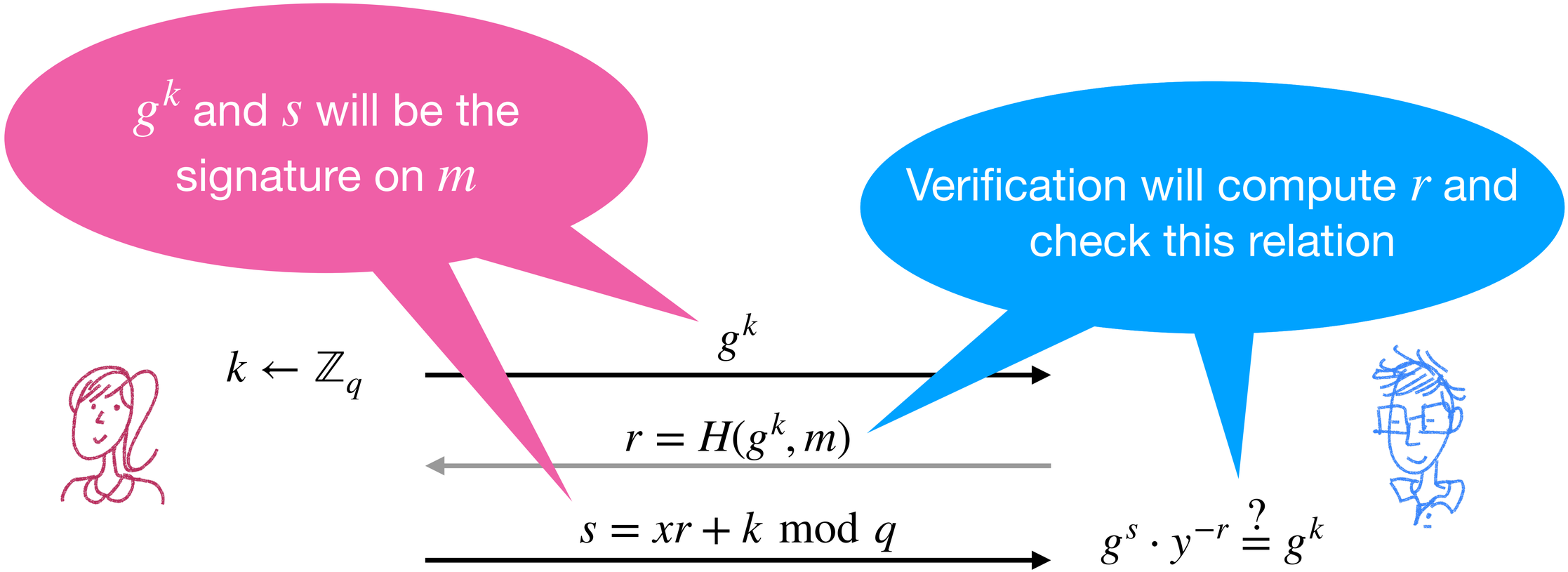
Schnorr Signature Scheme

Idea: Apply the Fiat-Shamir transform (with the message) to Schnorr's identification scheme.



Schnorr Signature Scheme

Idea: Apply the Fiat-Shamir transform (with the message) to Schnorr's identification scheme.



Schnorr Signature Scheme

Let $\mathcal{G}$ be a PPT algorithm that on input 1^n outputs $(\mathbb{G}, q, g)$ where $\mathbb{G}$ is a cyclic group of order q that is generated by g and q is an n-bit prime. Let $H : \{0,1\}^* \to \mathbb{Z}_q$.

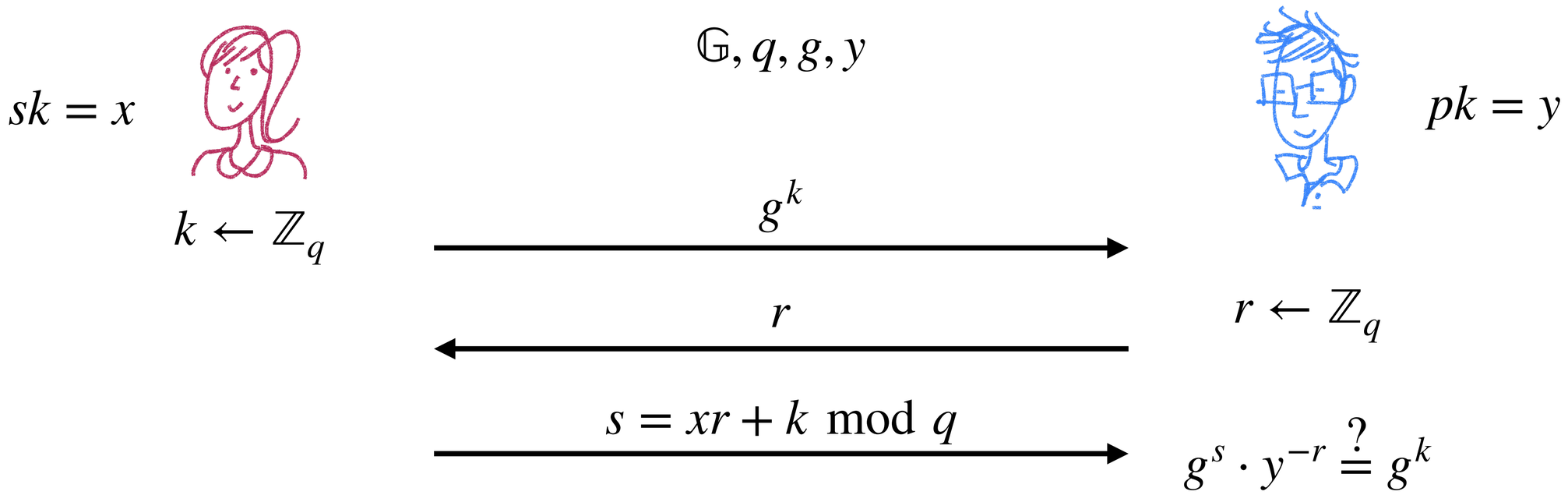
- $\text{Gen}(1^n)$: Run $(\mathbb{G}, q, g) \leftarrow \mathcal{G}(1^n)$, sample $x \leftarrow \mathbb{Z}_q$, and compute $y = g^x$. Set $pk = (\mathbb{G}, q, g, y)$ and $sk = x$
- $\text{Sign}_{sk}(m)$: Sample $k \leftarrow \mathbb{Z}_q$. Set $z = g^k$ and $r = H(z, m)$. Compute $s = xr + k \mod q$. Output the signature as $\sigma = (r, s)$
- $\text{Verify}_{pk}(m, \sigma)$: Let $r = H(z, m)$. Output 1 if $g^s = y^r \cdot z$. Otherwise output 0

Theorem: Schnorr Signatures are EUF-CMA secure in the Random Oracle Model assuming DL is hard relative to $\mathcal{G}$

DSA/ECDSA

Recall: Schnorr's Identification Scheme

Suppose Alice and Bob have $\mathbb{G}, q, g, y = g^x$, where $\mathbb{G} = \langle g \rangle$ is a cyclic group of prime order q, and Alice wants to convince Bob she knows x



Another Identification Scheme

Suppose Alice and Bob have $\mathbb{G}, q, g, y = g^x$, where $\mathbb{G} = \langle g \rangle$ is a cyclic group of prime order q, and Alice wants to convince Bob she knows x

$sk = x$

$pk = y$

$\mathbb{G}, q, g, y$

$k \leftarrow \mathbb{Z}_q$

g^k

$\alpha, r \leftarrow \mathbb{Z}_q$

α, r

$s = k^{-1}(xr+\alpha) \bmod q$

$g^{\alpha s^{-1}} \cdot y^{rs^{-1}} \stackrel{?}{=} g^k$

Another Identification Scheme

Suppose Alice and Bob have $\mathbb{G}, q, g, y = g^x$, where $\mathbb{G} = \langle g \rangle$ is a cyclic group of prime order q, and Alice wants to convince Bob she knows x

$sk = x$

$pk = y$

$\mathbb{G}, q, g, y$

$k \leftarrow \mathbb{Z}_q$

g^k →

α, r ←

$\alpha, r \leftarrow \mathbb{Z}_q$

$s = k^{-1}(xr+\alpha) \bmod q$ →

$g^{\alpha s^{-1}} \cdot y^{rs^{-1}} \stackrel{?}{=} g^k$

Correctness: $g^{\alpha s^{-1}} y^{rs^{-1}} = g^{\alpha s^{-1}} g^{xrs^{-1}} = g^{(\alpha+xr)s^{-1}} = g^{(\alpha+xr)k(\alpha+xr)^{-1}} = g^k$

Security of this Identification Scheme

Theorem: If DL is hard relative to $\mathscr{G}$ then this scheme is secure

g^k

α, r

$s = k^{-1}(xr + \alpha) \bmod q$

$g^{\alpha s^{-1}} \cdot y^{rs^{-1}} \stackrel{?}{=} g^k$

Security of this Identification Scheme

Theorem: If DL is hard relative to $\mathscr{G}$ then this scheme is secure

Proof follows very similarly to Schnorr's

- If Eve can answer two challenges for the same g^k she can break DL
- If Eve knows α, r ahead of time, she can choose her messages to pass

g^k

α, r

$s = k^{-1}(xr + \alpha) \bmod q$

$g^{\alpha s^{-1}} \cdot y^{rs^{-1}} \stackrel{?}{=} g^k$

Converting to a Signature Scheme?

Can we use the Fiat-Shamir transform?

g^k

α, r

$s = k^{-1}(xr + \alpha) \bmod q$

$g^{\alpha s^{-1}} \cdot y^{rs^{-1}} \stackrel{?}{=} g^k$

Converting to a Signature Scheme?

Can we use the Fiat-Shamir transform?

- Not exactly…

g^k

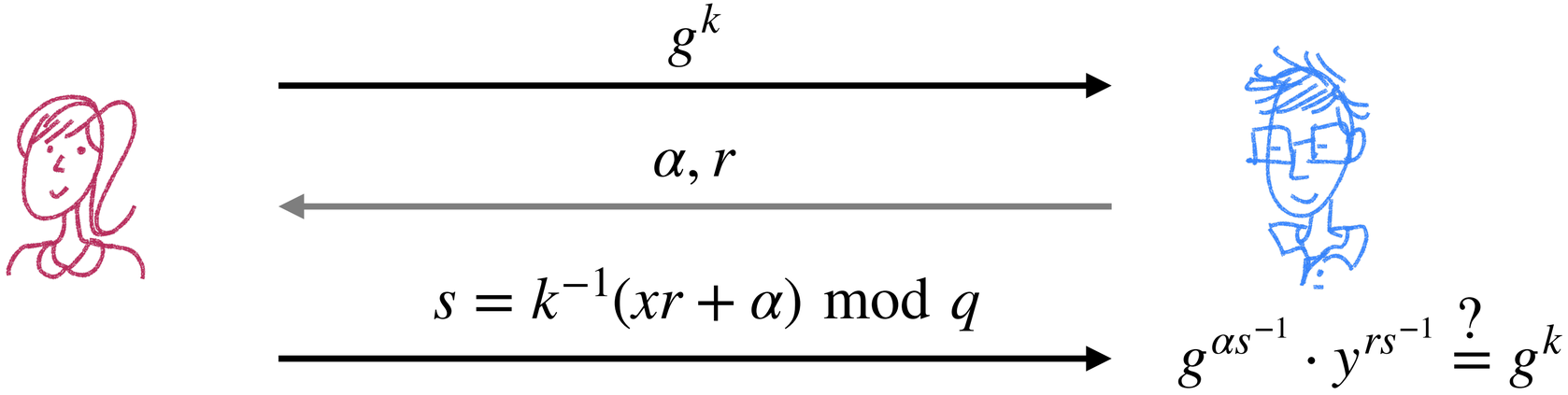
α, r

$s = k^{-1}(xr + \alpha) \bmod q$

$g^{\alpha s^{-1}} \cdot y^{rs^{-1}} \stackrel{?}{=} g^k$

Converting to a Signature Scheme?

- To sign a message m, set $\alpha = H(m)$ using a hash $H : \{0,1\}^* \to \mathbb{Z}_q$
- Set $r = F(g^k)$ for a "simple" function $F : \mathbb{G} \to \mathbb{Z}_q$
  - **Digital Signature Algorithm (DSA)**: $F(g^k) = g^k \bmod q$
  - **Elliptic Curve DSA (ECDSA)**: $F(g^k) =$ the x-coordinate of curve point g^k



DSA/ECDSA Signatures

Let $\mathcal{G}$ be a PPT algorithm that on input 1^n outputs $(\mathbb{G}, q, g)$ where $\mathbb{G}$ is a cyclic group of order q that is generated by g and q is an n-bit prime. Let $H : \{0,1\}^* \to \mathbb{Z}_q$ and $F : \mathbb{G} \to \mathbb{Z}_q$.

- $\mathsf{Gen}(1^n)$: Run $(\mathbb{G}, q, g) \leftarrow \mathcal{G}(1^n)$, sample $x \leftarrow \mathbb{Z}_q$, and compute $y = g^x$. Set $pk = (\mathbb{G}, q, g, y)$ and $sk = x$
- $\mathsf{Sign}_{sk}(m)$: Sample $k \leftarrow \mathbb{Z}_q$, set $r = F(g^k)$, and $s = k^{-1}(H(m) + xr) \bmod q$. Output the signature as $\sigma = (r, s)$
- $\mathsf{Verify}_{pk}(m, \sigma)$: Output 1 if $r = F\left(g^{H(m)s^{-1}} y^{rs^{-1}}\right)$. Otherwise output 0

DSA/ECDSA Signatures

Let $\mathcal{G}$ be a PPT algorithm that on input 1^n outputs $(\mathbb{G}, q, g)$ where $\mathbb{G}$ is a cyclic group of order q that is generated by g and q is an n-bit prime. Let $H : \{0,1\}^* \to \mathbb{Z}_q$ and $F : \mathbb{G} \to \mathbb{Z}_q$.

- $\text{Gen}(1^n)$: Run $(\mathbb{G}, q, g) \leftarrow \mathcal{G}(1^n)$, sample $x \leftarrow \mathbb{Z}_q$, and compute $y = g^x$. Set $pk = (\mathbb{G}, q, g, y)$ and $sk = x$
- $\text{Sign}_{sk}(m)$: Sample $k \leftarrow \mathbb{Z}_q$, set $r = F(g^k)$, and $s = k^{-1}(H(m) + xr) \bmod q$. Output the signature as $\sigma = (r, s)$
- $\text{Verify}_{pk}(m, \sigma)$: Output 1 if $r = F\left(g^{H(m)s^{-1}} y^{rs^{-1}}\right)$. Otherwise output 0

Theorem:

DSA/ECDSA Signatures

Let $\mathcal{G}$ be a PPT algorithm that on input 1^n outputs $(\mathbb{G}, q, g)$ where $\mathbb{G}$ is a cyclic group of order q that is generated by g and q is an n-bit prime. Let $H : \{0,1\}^* \to \mathbb{Z}_q$ and $F : \mathbb{G} \to \mathbb{Z}_q$.

- $\text{Gen}(1^n)$: Run $(\mathbb{G}, q, g) \leftarrow \mathcal{G}(1^n)$, sample $x \leftarrow \mathbb{Z}_q$, and compute $y = g^x$. Set $pk = (\mathbb{G}, q, g, y)$ and $sk = x$
- $\text{Sign}_{sk}(m)$: Sample $k \leftarrow \mathbb{Z}_q$, set $r = F(g^k)$, and $s = k^{-1}(H(m) + xr) \bmod q$. Output the signature as $\sigma = (r, s)$
- $\text{Verify}_{pk}(m, \sigma)$: Output 1 if $r = F\left(g^{H(m)s^{-1}} y^{rs^{-1}}\right)$. Otherwise output 0

Theorem: uh…

DSA/ECDSA Signatures

Let $\mathcal{G}$ be a PPT algorithm that on input 1^n outputs $(\mathbb{G}, q, g)$ where $\mathbb{G}$ is a cyclic group of order q that is generated by g and q is an n-bit prime. Let $H : \{0,1\}^* \to \mathbb{Z}_q$ and $F : \mathbb{G} \to \mathbb{Z}_q$.

- Gen(1^n): Run $(\mathbb{G}, q, g) \leftarrow \mathcal{G}(1^n)$, sample $x \leftarrow \mathbb{Z}_q$ and compute $y = g^x$. Set $pk = (\mathbb{G}, q, g, y)$ and sk
- Sign$_{sk}(m)$: Sam
  Output the sign
- Verify$_{pk}(m, \sigma)$: Output

DSA was introduced in the 90s without a proof.

2002 and 2016/2017 we've had a few proofs but in idealized models + extra assumptions

Theorem: uh…

DL-Based Signatures

- 1986: El Gamal proposed the
- 1989: Schnorr proposed a more e
  - Security based on DL in the random oracle mo
  - Schnorr patented it… and no one used it (patent expired in 2008)
- 1991: NIST proposed DSA (Digital Signature Algorithm)
  - Based on El Gamal and Schnorr, but sufficiently different
  - ECDSA: elliptic curve variant and is very popular
- 2011: EdDSA signatures
  - Essentially Schnorr's signatures on a specific family of elliptic curves called Edward's curves

Schnorr signatures are a big reason cryptographers don't like patenting things

Next Time

- More on signatures!
  - Lamport signatures
- Zero knowledge?
- (After next lecture we'll be doing special topics)