EECS 575: Advanced Cryptography
Fall 2022
Lecture 18

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Recap from last time
- Digital signatures
- Syntax and UF-CMA security
- One-time signatures from OWFs
- One-time to many-time

Agenda for this lecture

- Announcements
- Recap from last time
- Digital signatures
- Syntax and UF-CMA security
- One-time signatures from OWFs
- One-time to many-time

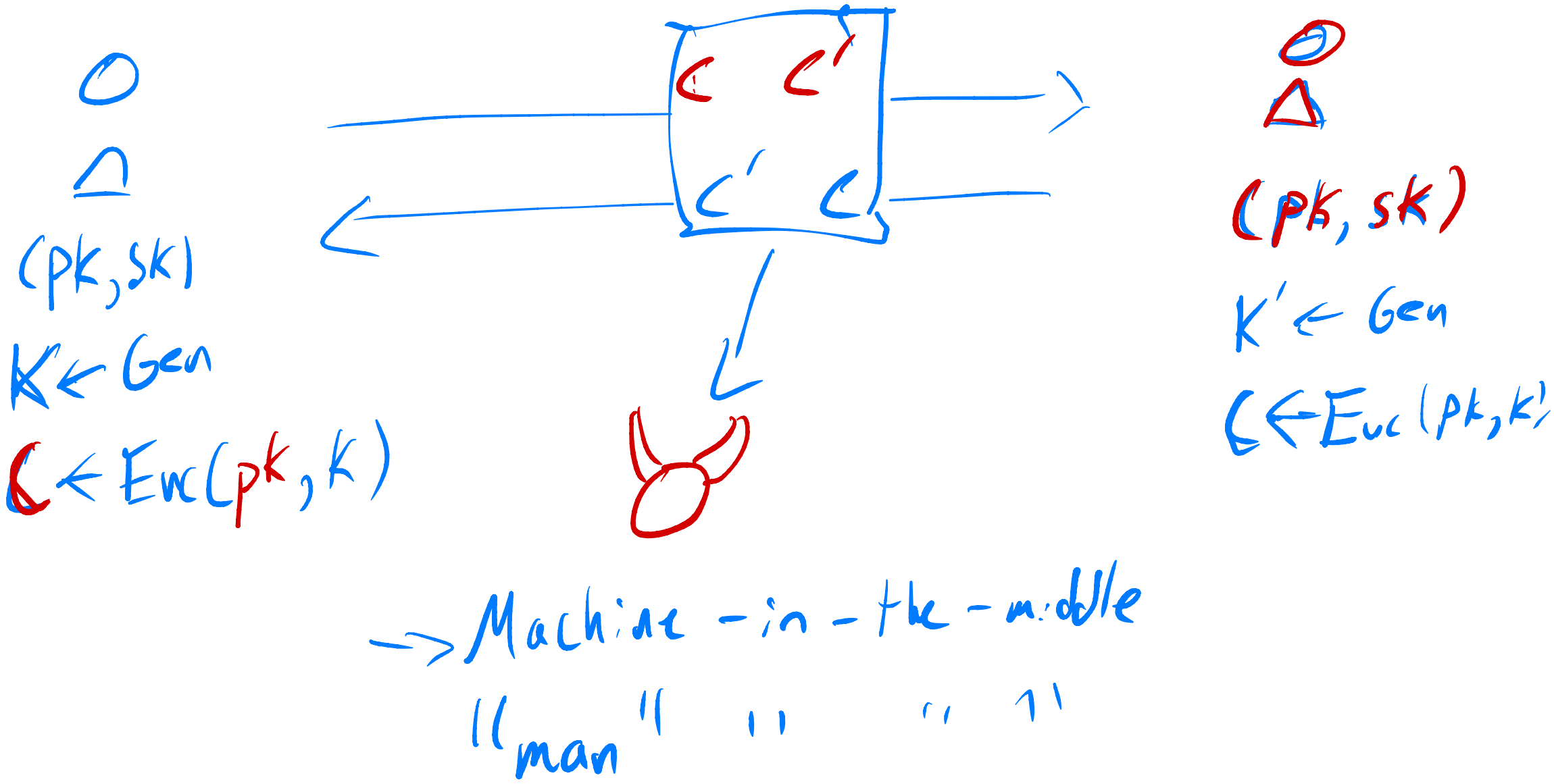
Announcements

- HW4 due TODAY
- Alexandra’s OH will happen as scheduled today
- Thanks to all who filled out evaluations!

Agenda for this lecture

- Announcements
- Recap from last time
- Digital signatures
- Syntax and UF-CMA security
- One-time signatures from OWFs
- One-time to many-time

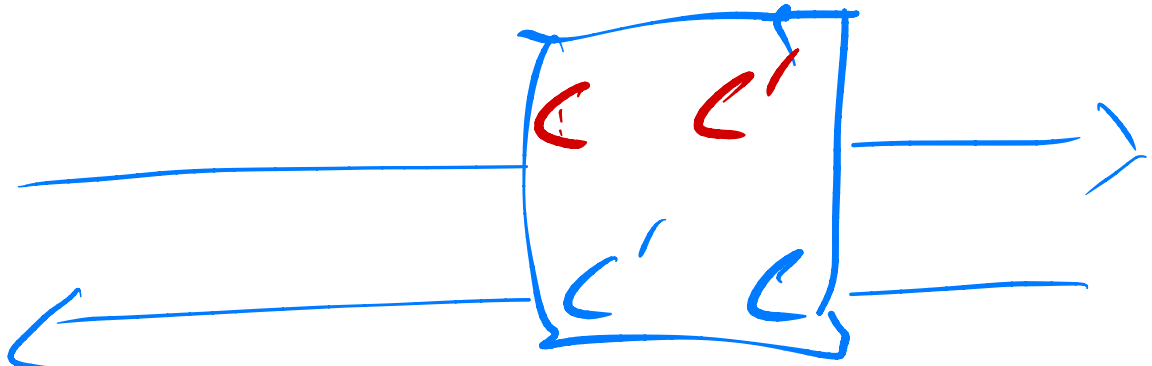
Public-Key Encryption



Agenda for this lecture

- Announcements
- Recap from last time
- Digital signatures
- Syntax and UF-CMA security
- One-time signatures from OWFs
- One-time to many-time

Digital signatures



A

(pk, sk)

K ← Gen

C ← Enc(pk, K)

Let A verify message is from B

Need verify message ownership/auth publicly

Digital signatures

B

(pk, sk)

K' ← Gen

C ← Enc(pk, K')

Let B verify message is from A

Digital signatures

How does A learn B's public key?

- ~~A knows every public key in the world~~
- Someone A trusts, tells A what is B's key

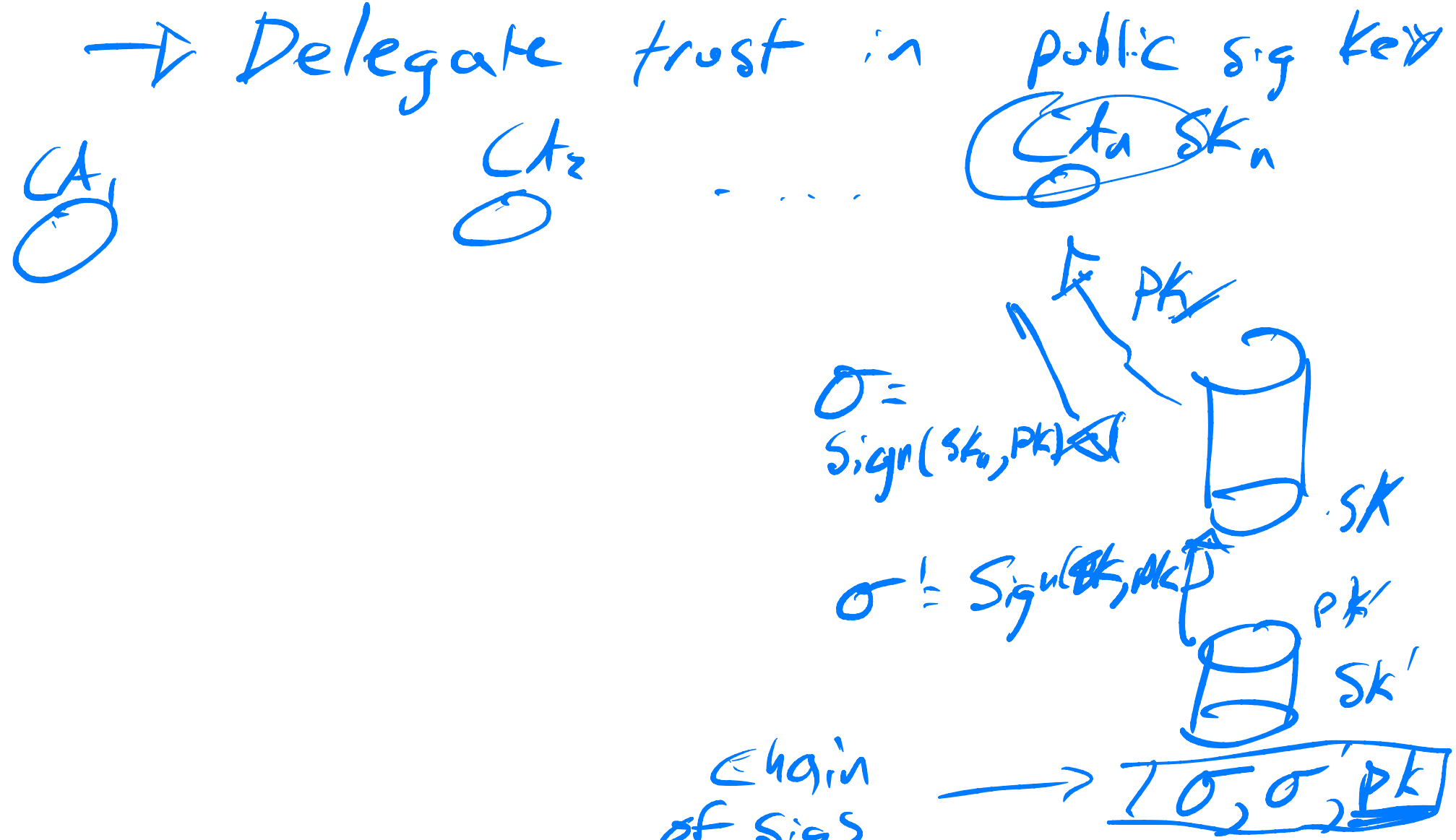
Certificate authorities

Verisign Comodo Lets Encrypt

Digital signatures

Certificate chains

→ Delegate trust in public sig key



Digital signatures

How does A get B's key?

- B gives A the key,
  Chain of signatures to trusted party

A trusts CA, knows its key, can verify
roots of trust

Exercise: Find trusted CA bundle,
look at certs!

Agenda for this lecture

- Announcements
- Recap from last time
- Digital signatures
- Syntax and UF-CMA security
- One-time signatures from OWFs
- One-time to many-time

Syntax and security for digital signatures

- Gen: (pk, sk) (vk)
- Sign(sk, m): outputs σ
- Ver(pk, σ, m): outputs 0/1

$\underline{SUF\text{-}CMA}^{\mathcal{A}}_{SIG}$:

$(pk, sk) \leftarrow Gen$; $Q = \{\}$

$(m', \sigma') \leftarrow \mathcal{A}^{Sign(\cdot)}(pk)$

Ret Success(pk, Q, m, σ)

$\underline{Success(pk, Q, m', \sigma')}$:

$b = Ver(pk, \sigma', m')$

Ret $b \wedge m' \notin Q \wedge (m', \sigma') \notin Q$

$\underline{Sign(m)}$:

$\sigma \leftarrow Sign(sk, m)$

$Q[m] \cup= \sigma$

Ret σ

Do we need Ver oracle? No- Ver is public

Unforgeability under chosen-message attack

Agenda for this lecture

- Announcements
- Recap from last time
- Digital signatures
- Syntax and UF-CMA security
- One-time signatures from OWFs
- One-time to many-time

One-time signatures

Same except only one Sign query

$f: \{0,1\}^n \to \{0,1\}^n$

Lamport OTS[f]

- Gen: sample $x^{i,b} \leftarrow \{0,1\}^n$ for $i \in [n]$ $b \in \{0,1\}$

  Ret $([F(x^{i,b})]_{i\in[n],\, b\in\{0,1\}}, [x^{i,b}]_{i\in[n],\, b\in\{0,1\}})$

- Sign(sk, m):

  Ret $[x^{i,m_i}]_{i\in[n]}$

- Ver(pk, σ, m):

  Ret $\bigwedge_{i=1}^{n} f(\sigma_i) = pk^{i,m_i}$

sk =

$x^{1,0}$	$x^{2,0}$	$x^{3,0}$	$x^{4,0}$
$x^{1,1}$	$x^{2,1}$	$x^{3,1}$	$x^{4,1}$

vk =

$f(\cdot)$	$f(\cdot)$	$f(\cdot)$	$f(\cdot)$
$f(\cdot)$	$f(\cdot)$	$f(\cdot)$	$f(\cdot)$

Sign(sk, 0110)

Ret

$x^{1,0}$	$x^{2,0}$	$x^{3,0}$	$x^{4,0}$
$x^{1,1}$	$x^{2,1}$	$x^{3,1}$	$x^{4,1}$

Ver(pk, ▯▯▯▯, 0110):

c =

$f(\cdot)$	$f(\cdot)$	$f(\cdot)$	$f(\cdot)$
$f(\cdot)$	$f(\cdot)$	$f(\cdot)$	$f(\cdot)$

Check ▯ = F(▯)

One-time signatures

- Gen: sample $x^{i,b} \leftarrow \{0,1\}^n$ for $i \in [n]$ $b \in \{0,1\}$
  Ret $([F(x^{i,b})]_{i\in[n],\, b\in\{0,1\}}, [x^{i,b}]_{i\in[n],\, b\in\{0,1\}})$
- Sign(sk, m):
  Ret $[x^{i,m_i}]_{i\in[n]}$
- Ver(pk, σ, m):
  Ret $\bigwedge_{i=1}^{n} F(\sigma_i) = pk^{i,m_i}$

Thm: If f is owf, then OTS[f] is UF-1CMA

Proof (sketch): Given forger A for OTS, show how to invert OWF

$\underline{SUFCMA^{A}_{SIG}}$:
$(pk, sk) \leftarrow Gen$; $Q = \{\}$
$(m', \sigma') \leftarrow A^{Sign(\cdot)}(pk)$
Ret Success(pk, Q, m, σ)

Sign(m):
$\sigma \leftarrow Sign(sk, m)$
$Q[m] \cup= \sigma$
Ret σ

$\underline{B^{A}(Y = F(X))}$:
Choose $2n-1$ $x^{i,b}$'s randomly
Sample $i, b \leftarrow [n] \times \{0,1\}$
Set $pk[i,b] = Y$, $pk[j,b'] = F(x^{j,b'})$ for $(j,b') \neq (i,b)$
Set $sk[i,b] = \perp$ $sk[j,b'] = x^{j,b'}$

One-time signatures

- Gen: sample $x^{i,b} \leftarrow \{0,1\}^n$ for $i \in [n]$, $b \in \{0,1\}$
  Ret $([f(x^{i,b})]_{i\in[n],\, b\in\{0,1\}}, [x^{i,b}]_{i\in[n],\, b\in\{0,1\}})$
- Sign(sk, m):
  Ret $[x^{i,m_i}]_{i\in[n]}$
- Ver(pk, σ, m):
  Ret $\bigwedge_{i=1}^{n} f(\sigma_i) = pk^{i,m_i}$

$\mathrm{SUFCMA}^{\mathcal{A}}_{SIG}$:
$(pk, sk) \leftarrow Gen$; $Q = []$
$(m', \sigma') \leftarrow \mathcal{A}^{Sign(\cdot)}(pk)$
Ret Success(pk, Q, m, σ)

Sign(m):
$\sigma \leftarrow Sign(sk, m)$
$Q[m] := \sigma$
Ret σ

$\mathcal{B}^{\mathcal{A}}(Y = f(X))$:
Choose $2n-1$ $x^{i,b}$'s randomly; $Q = []$
Sample $i^*, b^* \leftarrow [n] \times \{0,1\}$
Set $pk[i^*, b^*] = Y$, $pk[j, b'] = f(x^{j,b'})$ for $(j, b') \neq (i^*, b^*)$
Set $sk[i^*, b^*] = \perp$, $sk[j, b'] = x^{j,b'}$
$(m', \sigma') \leftarrow \mathcal{A}^{\widetilde{Sign}(\cdot)}(pk)$
If $m'_{i^*} \neq m_{i^*} \wedge Success(pk, Q, m', \sigma')$:
  Ret x^{i^*, b^*}
Else ⊥

$\widetilde{Sign}(m)$:
If $m_{i^*} = b^*$: Abort!
Else $\sigma = [x^{i,m_i}]_{i\in[n]}$; $Q[m] = \sigma$
Ret σ

Next time:
Argue
$Pr[\mathcal{A} \text{ wins}] \leq 2n \cdot Pr[\mathcal{B}^{\mathcal{A}} \text{ wins}]$

Agenda for this lecture

- Announcements
- Recap from last time
- Digital signatures
- Syntax and UF-CMA security
- One-time signatures from OWFs
- One-time to many-time

Getting to many-time signatures