EECS 575: Advanced Cryptography
Fall 2021
Lecture 17

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Recap from last time
- Digital Signatures
- UF-CMA security
- One-time signatures from OWFs Lamport
- One-time => many-time via collision-resistant hashing

Agenda for this lecture

- Announcements
- Recap from last time
- Digital Signatures
- UF-CMA security
- One-time signatures from OWFs
- One-time => many-time via collision-resistant hashing

Announcements

- HW5 is online, due 11/8
- Evals were released
- Lecture slides w/ notes are on GitHub
  → put link in canvas

Recap from last time

* Chosen-ciphertext security (IND-CCA)
  - IND-CPA for PKE, with decryption oracle

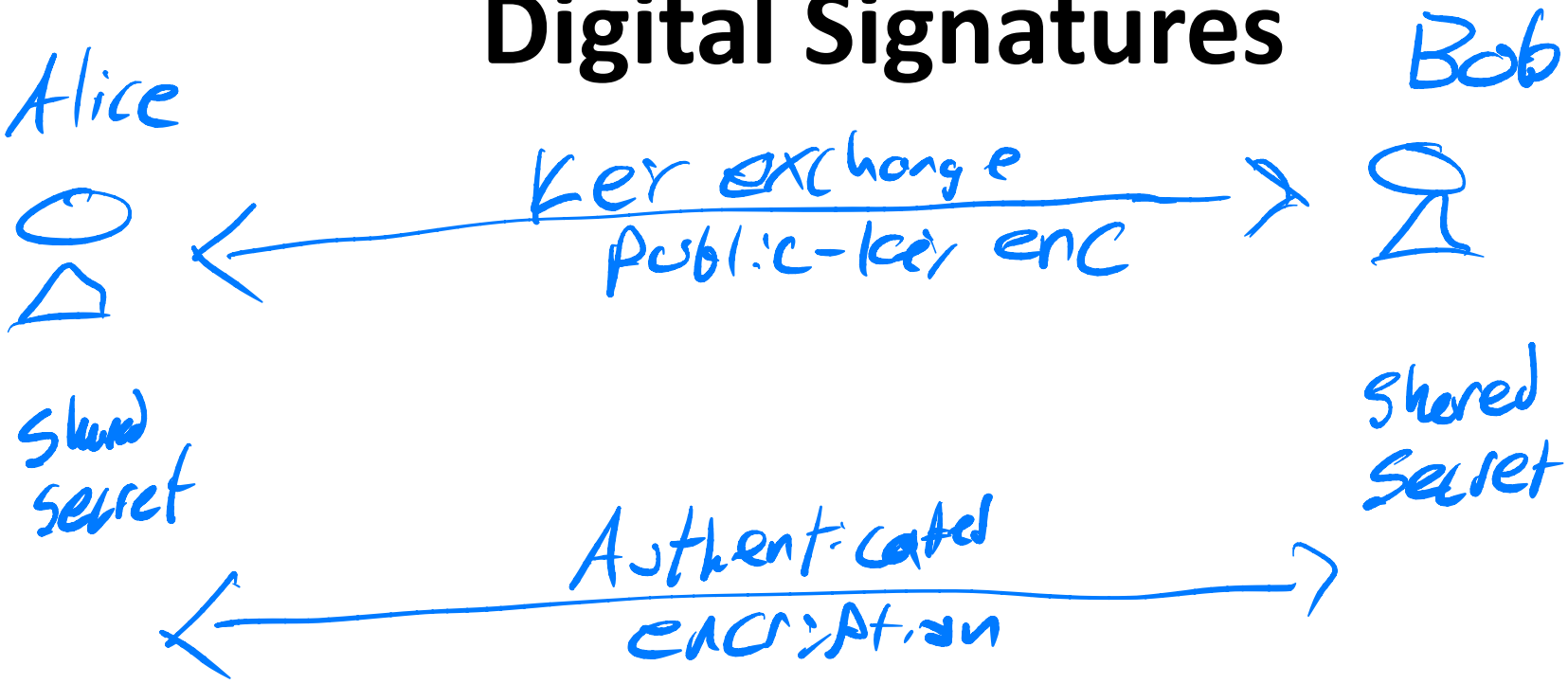
* ElGamal is not CCA secure

* Hybrid encryption
  → encrypt symkey with PKE,
  use symkey to encrypt msg

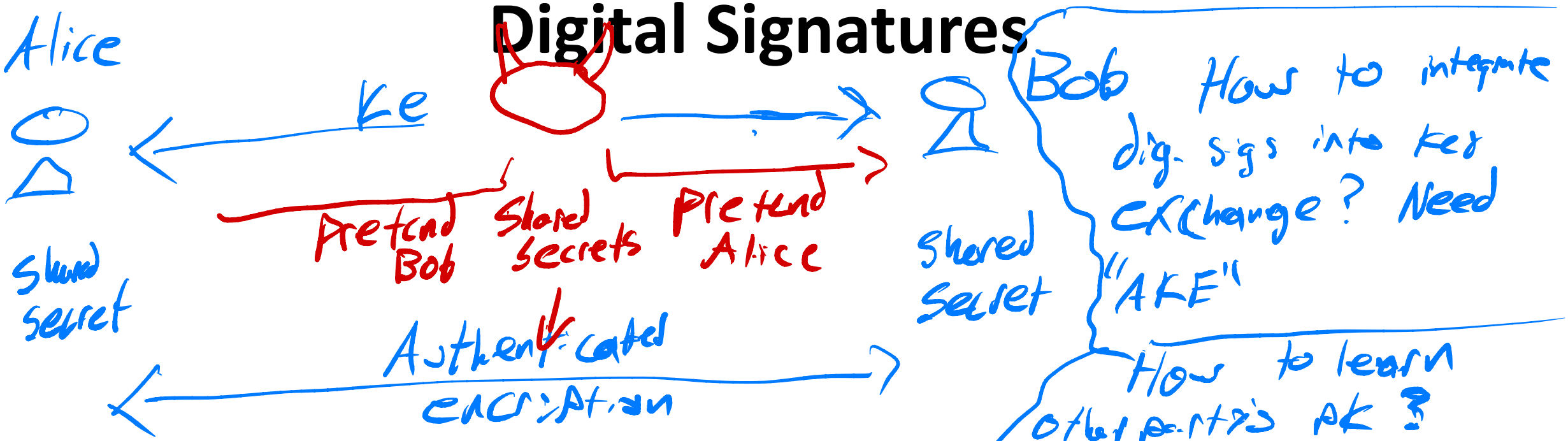
Agenda for this lecture

- Announcements
- Recap from last time
- Digital Signatures
- UF-CMA security
- One-time signatures from OWFs
- One-time => many-time via collision-resistant hashing

Digital Signatures



Digital Signatures



Machine-in-the-middle

Solution:

Digital signatures: public-key authentication

Only SK holder can sign. anyone can verify signature

Digital Signatures

* Gen: outputs (vk, sk)
* $Sign(sk, m)$: outputs $\sigma \in \$$ ← space of possible sigs
* $Ver(vk, m, \sigma)$: outputs 0/1

SIG is strongly unforgeable under chosen-message attack if $\forall$ nuppt A,

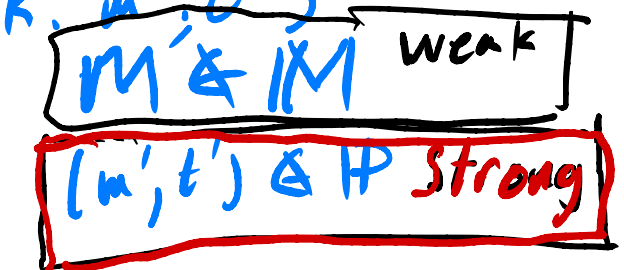
$$Pr[UFCMA_{SIG}(A)=1] \leq negl(n)$$

$UFCMA_{SIG}(A)$:

$(vk, sk) \leftarrow Gen$

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

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

Ret $b \wedge$ 

$Sign(m)$:

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

$M[i] = m$

$P[i] = (m, \sigma)$

Exercise:

would giving A a Ver oracle make this def stronger?

Agenda for this lecture

- Announcements
- Recap from last time
- Digital Signatures
- UF-CMA security
- One-time signatures from OWFs
- One-time => many-time via collision-resistant hashing

UF-CMA for signatures

See prev slide

Agenda for this lecture

- Announcements
- Recap from last time
- Digital Signatures
- UF-CMA security
- One-time signatures from OWFs
- One-time => many-time via collision-resistant hashing

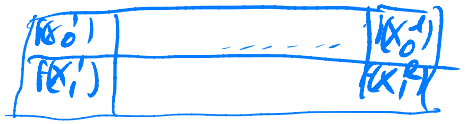
One-time signatures from OWFs

Lamport

$F: \{0,1\}^n \longrightarrow \{0,1\}^m$

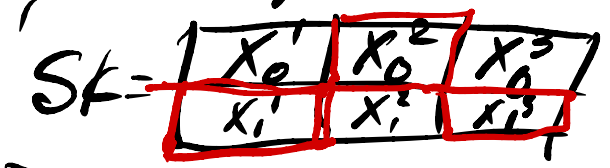
$SIG[F] = (Gen, Sign, Ver)$

Idea: Make a signature that's as hard to forge as inverting F. To do this, vk will be $F(x)$ for 2ℓ random x's (ℓ is msg length), sk will be all the preimages of vk



* **Gen:** Samples 2ℓ random x's: pairs.
  - $sk = (x_0^1, x_1^1) \cdots (x_0^\ell, x_1^\ell)$
  - $vk = (f(x_0^1), f(x_1^1)) \cdots (f(x_0^\ell), f(x_1^\ell))$
* **Sign(sk, m):** Treat msg as $m_1 \cdots m_\ell$
  output $x_{m_1}^1 \cdots x_{m_\ell}^\ell$
* **Ver(vk, m, σ):** $\sigma = \sigma_1, \sigma_2, \cdots \sigma_\ell$
  Check that $vk[i][m_i] = f(\sigma_i)$

E.g. $\ell = 3$



To sign 101, release red cells in table

One-time signatures from OWFs

SIG[f]:

* Gen: Samples 2ℓ random x's: pairs.
  - $sk = (x_0^1, x_1^1) \cdots (x_0^\ell, x_1^\ell)$
  - $vk = (f(x_0^1), f(x_1^1)) \cdots (f(x_0^\ell), f(x_1^\ell))$
* Sign(sk, m): Treat msg as $m_1 \cdots m_\ell$
  output $x_{m_1}^1 \cdots x_{m_\ell}^\ell$
* Ver(vk, m, σ): $\sigma = \sigma_1, \sigma_2, \cdots \sigma_\ell$
  Check that $vk[i][m_i] = f(\sigma_i)$

Theorem: If f is one-way, then SIG[f] is uf-1cma.

Proof (idea): By contrapositive.

Assume $\exists A$ s.t. $\Pr[\text{uf-1cma}_{SIG[f]}(A) = 1] > 1/m$.

Build inverter for f. Main idea:

I puts its input in one of 2ℓ positions, generates other $2\ell - 1$ randomly.

Because forgery must be on diff. message, w.p. $1/\ell$ the forgery also inverts OWF

One-time signatures from OWFs

SIG[f]:

* Gen: Samples 2ℓ random x's: pairs.
  - $sk = (x_0^1, x_1^1) \cdots (x_0^\ell, x_1^\ell)$
  - $vk = (f(x_0^1), f(x_1^1)) \cdots (f(x_0^\ell), f(x_1^\ell))$
* Sign(sk, m): Treat msg as $m_1 \cdots m_\ell$
  output $x_{m_1}^1 \cdots x_{m_\ell}^\ell$
* Ver(vk, m, σ): $\sigma = \sigma_1, \sigma_2, \cdots \sigma_\ell$
  Check that $vk[i][m_i] = f(\sigma_i)$

Proof (idea): By contrapositive.
Assume $\exists A$ s.t. $Pr[\text{UF-1CMA}_{SIG[f]}(A) = 1] > 1/n$.
Build inverter I for f. Main idea:
I puts its input in one of 2ℓ positions, generates other $2\ell - 1$ randomly.
Because forgery must be on diff. message, w.p. $1/\ell$ the forgery also inverts OWF

Theorem: If f is one-way, then SIG[f] is UF-1CMA.

Proof: Assume $\exists A$ s.t.
$Pr[\text{UF-1CMA}_{SIG[f]}(A) = 1] \geq 1/p(n)$.
Build I that simulates UF-kCMA:

$I(y)$:
$i \leftarrow [\ell]$; $b \leftarrow \{0,1\}$
$vk[i][b] = y$; $vk[j] = (f(x_0^j), f(x_1^j))$
$sk[i][b] = \perp$; $sk[j] = (x_0^j, x_1^j)$
$(m', \sigma') \leftarrow A^{\text{Sign}(\cdot)}(vk)$
If $m_i \neq m'_i$: Ret σ'_i
Else Ret $\perp$

Sign(m):
If $m_i = b$: output $\perp$; fail
Else ret $(sk[i][m_i])_{i=1}^{\ell}$

One-time signatures from OWFs

Proof: Assume $\exists A$ s.t. $\Pr[\text{UF-1CMA}_{\text{SIG}[F],A}(\lambda)=1] \geq 1/p(n)$.

Build $\mathcal{I}$ that simulates UF-kMA:

$\mathcal{I}(y)$:

$i \leftarrow \{1,\dots,\ell\}$; $b \leftarrow \{0,1\}$

$VK[i][b] = y$; $VK[j] = (f(x_0^j), f(x_1^j))$

$SK[i][b] = \perp$; $SK[j] = (x_0^j, x_1^j)$

$(m', \sigma') \leftarrow A^{\text{Sign}(\cdot)}(VK)$

If $m_i \neq m_i'$: Ret σ_i' ← If $m_i \neq m_i'$ but σ is valid, then $f(\sigma_i) = y$.

Else Ret $\perp$

Sign(m):

If $m_i = b$: output $\perp$; fail ←

Else ret $(SK[i][m_i])_{i=1}^{\ell}$

$$\Pr_{x \leftarrow \{0,1\}^n}[\mathcal{I}(y=f(x)) \in f^{-1}(y)] \geq$$

$$\Pr[A \text{ forges} \mid \wedge_i m_i \neq b] \Pr[\wedge_i m_i \neq b] \geq \frac{1}{p(n)} \cdot \frac{1}{2\ell}$$

$$= \frac{1}{2\ell p(n)}$$

∎

Agenda for this lecture

- Announcements
- Recap from last time
- Digital Signatures
- UF-CMA security
- One-time signatures from OWFs
- One-time => many-time via collision-resistant hashing

Collision-resistant hashes (CRHs)

Many-time signatures