CSE 575: Advanced Cryptography
Fall 2024
Lecture 15

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

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

Agenda for this lecture

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

Announcements

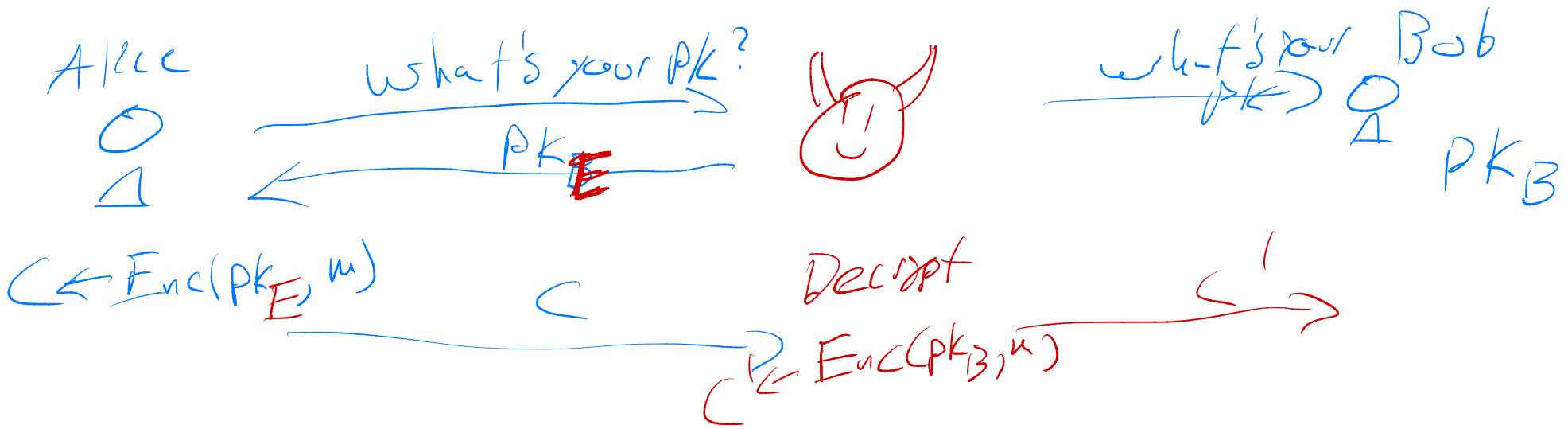
- HW3 will be assigned today Due 11/4
- Thanks to all who filled out evaluations!
  - Any other feedback, please feel free to tell me in person! (I have thick skin.)

Agenda for this lecture

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

Digital signatures

- Public-key encryption, secret-key encryption



Need dig. sigs — provide public-key auth

Certificate authorities (PKI)

- trusted parties, attest to pk_S via signing

Agenda for this lecture

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

Syntax and security for digital signatures

- Gen: output pk, sk [vk]
- $Sign(sk, m)$: outputs σ
- $Ver(pk, m, \sigma)$: output 0/1

DS is SUF-CMA if $\forall$ nuPPT A,

$$Pr[SUF\text{-}CMA_{DS}^{A} = 1] = negl(\lambda)$$

UF-1CMA:

Only one Sign query

$SUF\text{-}CMA_{DS}^{A}$:

$(pk, sk) \leftarrow DS.Gen$; $Q = []$

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

$Ret\ DS.Ver(pk, m', \sigma') = 1$
$\wedge\ m' \notin Q$
$\wedge\ (m', \sigma') \notin Q$

$Sign(m)$:

$\sigma \leftarrow DS.Sign(sk, m)$
Add (m, σ) to Q
$Ret\ \sigma$

Unforgeability under chosen-message attack

Agenda for this lecture

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

One-time signatures (Lamport)

$F: \{0,1\}^\lambda \to \{0,1\}^*$

OTS[f] signs n-bit msgs

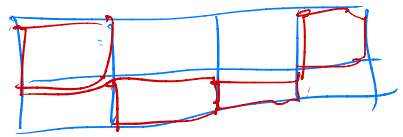
- Gen[f]:
  Generate $2n$ λ-bit random strings $x_1^0, \ldots, x_n^0, x_1^1, \ldots, x_n^1$
  Compute $y_i^b = f(x_i^b)$ for $b \in \{0,1\}$, $i \in [n]$
  output $(\{y_i^b\}, \{x_i^b\})$

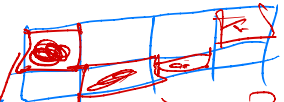
- Sign[f](sk, $m_1, \ldots, m_n$):
  Ret $x_i^{m_i}$ for $i \in [n]$

- Ver[f](pk, $m_1, \ldots, m_n, \sigma$)
  Parse σ as $x_1^*, \ldots, x_n^*$
  Ret $\bigwedge_{i=1} f(x_i^*) = pk[i][m_i]$

E.g. $n = 4$

Sign[F](sk, 0110)



Ver( , 0110, $x_1^*, x_2^*, x_3^*, x_4^*$)

$\stackrel{?}{=} f(x_1^*)$ $\stackrel{?}{=} f(x_2^*)$ etc.

Analyzing OTS

Thm: If f is OWF, $OTS[f]_{n\text{-bit}}$ is UF-1CMA.

Proof:

Relate forgery prob. to inversion prob.

Assume $\mathcal{A}$ s.t.

$$Pr\left[UF\text{-}1CMA^{\mathcal{A}}_{OTS[f]} = 1\right] > \frac{1}{p(n)}$$

Build reduction $\mathcal{B}$ to invert f

Claim: $Pr[\mathcal{B} \text{ inverts } f] \geq \frac{1}{p(n) \cdot 2 \cdot n}$

High-level: $\mathcal{B}(y)$ "plants" y in pk, hopes $\mathcal{A}$ forges at that point.

Analyzing OTS

1. UF-ICMA dist? 2. Prob of abort?
   - pk good, $\tilde{Sig}$ good, dist of $\tilde{Sig}^*$ w/out cond 3. Prob of $\mathcal{B}$ win if no abort?

$\mathcal{B}(y)$:

$i^*, b^* \leftarrow [n] \times \{0,1\}$; $m^* = \perp$

Set $pk[i^*][b^*] = y$, $sk[i^*][b^*] = \perp$

finish setup as normal

$m', \sigma' \leftarrow \mathcal{A}^{\tilde{Sig}}(pk)$

If $m'_{i^*} = b^*$, Ret $\sigma'[i^*]$

$\tilde{Sig}(m)$:

Parse m as $m_1, \ldots, m_n$; $m^* = m$

If $m_i = b^*$, Abort!

Ret $sk[i][m_i]$ $\forall i \in [n]$

Let E_1 be event that no abort

E_2 $\mathcal{A}$'s $m'_{i^*} \neq m^*_{i^*}$

$\Pr[\mathcal{B} \text{ inverts } y] = \Pr[\mathcal{B} \text{ inverts } y \mid E_1 \wedge E_2] \cdot \Pr[E_1 \wedge E_2]$ 0

$+ \Pr[\mathcal{B} \text{ inverts } y \mid \neg(E_1 \wedge E_2)] \cdot \Pr[\neg(E_1 \wedge E_2)]$

$\Pr[\mathcal{B} \text{ inverts } y \mid E_1 \wedge E_2] = \Pr[UF\text{-}ICMA^{\tilde{\mathcal{A}}}_{OTS[n]} = 1] \geq \frac{1}{p(n)}$

$\Pr[E_1 \wedge E_2] = \Pr[E_2 \mid E_1] \cdot \Pr[E_1] \geq \frac{1}{n} \cdot \frac{1}{2}$

$\Pr[\mathcal{B} \text{ inverts } y] \geq \frac{1}{2n \cdot p(n)}$ ☒

Agenda for this lecture

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

Getting to many-time signatures