Pairing-based Crypto

Def: $\mathcal{E}/\mathbb{F}_q$ ell. curve, $P \in \mathcal{E}(\mathbb{F}_q)$
a distortion map for P is an endomorphism α
s.t. $\alpha(P) \notin \langle P \rangle$.

Ex: ① $\mathcal{E}/\mathbb{F}_p$: $y^2 = x^3 + B$ $\quad p = 2 \bmod 3$
$\omega \in \mathbb{F}_{p^2}$ cube root of 1

for $P \in \mathcal{E}(\mathbb{F}_p)$, $\alpha(x,y) = (\omega x, y)$ is a distortion map for P
$\langle P \rangle \subset \mathcal{E}(\mathbb{F}_p)$, but $\alpha(P) \notin \mathcal{E}(\mathbb{F}_p)$

② $y^2 = x^3 + Ax$ $\quad p = 3 \bmod 4$
$\alpha(x,y) = (-x, iy)$ $\quad i^2 = -1$

If α is a distortion map for P of order n:

- $\{P, \alpha(P)\}$ is a basis of $\mathcal{E}[n]$
- $e_n(P, \alpha(P)) = \zeta$ primitive nth root of 1
- DDH is easy in $\langle P \rangle$!!
  given P, aP, bP, cP
  compute $e(P, \alpha(cP))$ and $e(aP, \alpha(bP))$
  $e(P, \alpha(cP)) = e(P, \alpha(P))^c$ and $e(aP, \alpha(bP)) = e(P, \alpha(P))^{ab}$

  equal iff $ab = c \bmod n$

Define modified Weil pairing on $G = \langle P \rangle = \{aP\}$

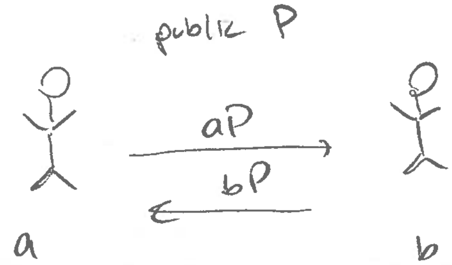
$$\hat{e} : G \times G \longrightarrow \mu_n$$

$$\hat{e}(P_1, P_2) = e_n(P_1, \alpha(P_2)).$$

Symmetric: $\hat{e}(aP, bP) = e_n(P, \alpha(P))^{ab} = \hat{e}(bP, aP)$

3-way key exchange (Joux '00)

Diffie-Hellman:

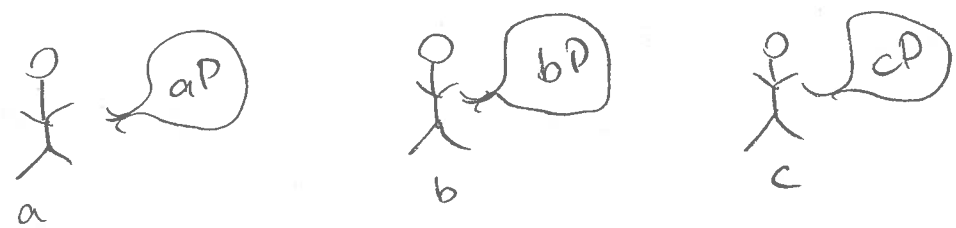


shared secret abP

compute shared secret from public info: CDH

distinguish shared secret from random: DDH

Joux:



$$\left.\begin{array}{ll} A \text{ computes} & \hat{e}(bP, cP)^a \\ B \text{ computes} & \hat{e}(aP, cP)^b \\ C \text{ computes} & \hat{e}(aP, bP)^c \end{array}\right\} = \underbrace{\hat{e}(P,P)^{abc}}_{\text{shared secret}}$$

New computational problems:

1) compute $\hat{e}(P,P)^{abc}$ from P, aP, bP, cP:

   Bilinear Diffie-Hellman problem (BDH)

2) distinguish $\hat{e}(P,P)^{abc}$ from random $r \in \mu_n$:

   Bilinear decision Diffie-Hellman problem (BDDH)

(6a)

~~Which curves to use~~?

Attacking 3-way key exchange:

- solve DLP on $\mathcal{E}(\mathbb{F}_q)$ — hard if $q \geq 2^{160}$
- solve DLP in $\mu_n \subset \mathbb{F}_{q^k}^*$ — hard if $q^k \geq 2^{1024}$

  (MOV)

supersingular curve over $\mathbb{F}_p$:

$P \in \mathcal{E}(\mathbb{F}_p)$ order $n \mid p+1$

$\mu_n \subset \mathbb{F}_{p^2}$

need $p^2 \geq 2^{1024}$

$p \geq 2^{512}$

[Class: how to construct?]

Better ratio: in char 3 can have emb. deg. $k=6$

(HW3, HW4)

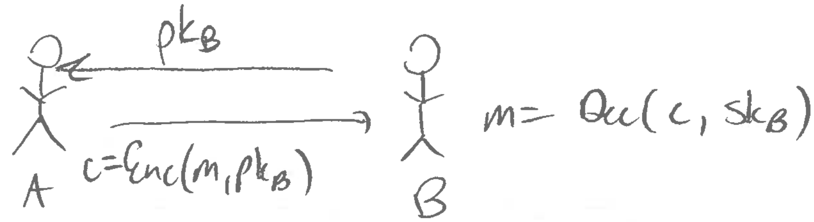
$P \in \mathcal{E}(\mathbb{F}_q)$ order $n \mid q \pm \sqrt{3q} + 1$

$\mu_n \subset \mathbb{F}_{q^6}$

need $q^6 > 2^{1024} \Rightarrow q > 2^{171} \approx 3^{108}$

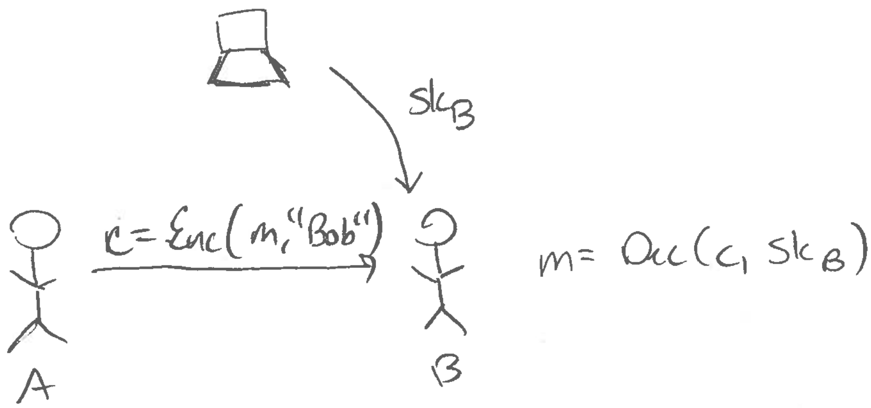
Identity-Based Encryption (Shamir '84)

Ordinary PKE:



Problem: pk_B has to be authenticated
- certificates, PKI

IBE:



advantages: no pk authentication
A can send before B enrolls

disadv: key escrow
(powerful authority)

Def: an <u>identity-based encryption scheme</u> is a tuple (Setup, Extract, Enc, Dec) of 4 PPT algs:

Setup() $\longrightarrow$ public parameters pp, master secret mk

Extract(pp, mk, id) $\longrightarrow$ sk_{id} secret key for id

Enc(pp, id, m) $\longrightarrow$ c

Dec(pp, c, sk_{id}) $\longrightarrow$ m

<u>Correctness</u>: $\forall$ pp, mk $\leftarrow$ Setup, $\forall$ id, $\forall$ m,

if $sk_{id} \leftarrow$ Extract(pp, mk, id) and $c \leftarrow$ Enc(pp, id, m)

then Dec(pp, c, sk_{id}) = m

Construction (BF '01)

Setup(): Supersingular curve $\mathcal{E}/\mathbb{F}_p$, $P \in \mathcal{E}(\mathbb{F}_p)$ of prime order n, pairing $\hat{e}: G \times G \to \mu_n$
$G = \langle P \rangle$.

master secret: $s \leftarrow [1, n]$

$$PP: (\mathcal{E}, \hat{e}, P, Q = [s]P, H_1, H_2)$$

$H_1: \{0,1\}^r \to G$ hash function
takes identities to points
$H_2: \mu_n \to \{0,1\}^\ell$

Extract (PP, mk, id): $sk_{id} = [s] \cdot H_1(id)$

Enc (PP, id, m): random $r \leftarrow [1, n]$

msg $m \in \{0,1\}^\ell$ $\quad g = \hat{e}(Q, H_1(id))^r$

$$c = (rP, m \oplus H_2(g))$$

bitwise exclusive or

Dec $(sk_{id}, (c_1, c_2))$: $m' = c_2 \oplus H_2(\underbrace{\hat{e}(c_1, sk_{id})}_{g})$

Correctness:
$$\hat{e}(c_1, sk_{id}) = \hat{e}(rP, s \cdot H_1(id))$$
$$= \hat{e}(P, H_1(id))^{rs}$$
$$= \hat{e}(s \cdot P, H_1(id))^r$$
$$= g$$

$$c_2 \oplus H_2(g) = m$$

IBE Security

Chall $\qquad\qquad$ **Adv $\mathcal{A}$**

mk $\quad \xrightarrow{\text{pp}}$

$\xleftarrow{id_i}$ $\quad$ repeat

$\xrightarrow{sk_i}$

$\xleftarrow{m^*,\, id^*}$

$b \leftarrow \{0,1\}$

$b=0: c = \text{Enc}(id^*, m^*)$

$b=1: c = \text{Enc}(id^*, m')$

$m' \overset{R}{\leftarrow} \mathcal{M}$

$\xrightarrow{c}$

$\xleftarrow{id_i}$ $\quad$ repeat

$\xrightarrow{sk_i}$

require $id^* \neq id_i \ \forall i$

[idea: $\mathcal{A}$ knows sk for all users except the one being attacked.]

output $b' \in \{0,1\}$

$$\text{Adv}\,\mathcal{A} = \Big|\Pr\big(\mathcal{A} \text{ outputs } 1 : c = \text{Enc}(id^*, m^*)\big) - \Pr\big(\mathcal{A} \text{ outputs } 1 : c = \text{Enc}(id^*, m')\big)\Big| \quad m' \overset{R}{\leftarrow} \mathcal{M}$$

IBE scheme is ϵ-semantically secure if for all efficient $\mathcal{A}$, $\quad \text{Adv}\,\mathcal{A} < \epsilon$.

Thm: if BDH problem is hard in G, then BF-IBE is semantically secure in the random oracle model (won't quantify)

~~Pf: given P, aP, bP, cP, show that adv $\mathcal{A}$ that breaks BF-IBE can compute~~

~~$e(P,P)^{abc}$~~

~~construct IBE challenger $\mathcal{B}$ as follows~~

[Actually, we will prove security of a variant]

Define $\widehat{\text{BF-IBE}}$:

Setup, Extract as in BF-IBE, $\boxed{\text{no } H_2}$

Enc(pp, id, m): $g = \hat{e}(Q, H_1(id))^r$

output $(rP, m \cdot g)$

(msg space is μ_n)

Dec(sk_{id}, (c_1, c_2)) : $m = c_2 \cdot \hat{e}(c_1, sk_{id})^{-1}$

Thm: if DBDH problem is hard in G, then $\widehat{\text{BF-IBE}}$ is semantically secure. in random oracle model

Pf: given P, aP, bP, cP, γ & $\widehat{\text{BF-IBE}}$ -adversary A, Use A to decide if $\gamma = \hat{e}(P,P)^{abc}$

Construct IBE challenger B:

B responds to sk queries and hash queries

(real-life: everyone knows how to compute hash)

$pp = (\mathcal{E}, \hat{e}, P, Q = aP)$

assume $\mathcal{A}$ makes $\leq q$ key / hash queries

pick random $\omega \in [1, q+1]$

B Responds to $H_1(id_i)$: if id_i is ωth query,

set $H_1(id_i) = bP$

else set $H_1(id_i) = t_i \cdot P$ for $t_i \xleftarrow{R} [1,n]$

~~B Responds to $H_2(x_i)$: choose random $y_i \xleftarrow{R} \{0,1\}^\ell$~~

B responds to extract query for id

1) query $H_1(id)$

- if $id = id_\omega$ abort
- else $H_1(id) = t_i \cdot P$

2) set $sk_{id} = t_i \cdot aP$

B responds to encryption query on (id^*, m^*)

$b \xleftarrow{R} \{0,1\}$

- query $H_1(id^*)$
- output $(cP, m^* \cdot \gamma)$

~~$b = 1$: output (cP, z)~~

~~$r \xleftarrow{R} [1,n]$, $\{0,1\}^\ell$~~

Analysis:

- responses to H_1 look random
- queried secret keys work:

$$\text{Enc}(id_i, m): g = \hat{e}(Q, H_1(id))^r = \hat{e}(aP, t_i P)^r$$

$$c = (rP, m \cdot g)$$

Dec: works if $\hat{e}(rP, sk_{id}) = g$

$$\hat{e}(rP, t_i \cdot aP)$$

- if $id^* = id_w$ (prob $1/q+1$)

then $enc(pp, id^*, m)$ sets

$$C_1 = cP$$

$$g = \hat{e}(Q, H_1(id^*))^c$$

$$= \hat{e}(aP, bP)^c$$

$$= \hat{e}(P,P)^{abc}$$

if $\gamma = \hat{e}(P,P)^{abc}$ then $(cP, m^* \cdot \gamma)$

is a real encryption of m^*

if γ = random then $(cP, m^* \cdot \gamma)$

is an encryption of random $m' = m^* \gamma g^{-1}$

Conclude: if A breaks $\widehat{\text{BF-IBE}}$ w/ prob ϵ,

then B solves BDDH w/ prob $\geq \epsilon / q+1$.

Proof of security of BF-IBE (with H_2):

Winning A must query $H_2(\hat{e}(P,P)^{abc})$ at some point $\to$ solve BDH