A Roadmap of IBE Systems
and their (Cryptographic) Applications

Xavier Boyen
Voltage Security

NIST IBE Workshop – Gaithersburg
2008/06/03

Purpose of IBE

Communicate securely (e.g., via email)

based on actual names – **IBE Public Key:**

alice@gmail.com

rather than, say – **RSA Public Key:**

Public exponent=0x10001

Modulus=135066410865995223349603216278805969938881
475605667027524485143851526510604859533833940287 1
505719094417982072821644715513736804197039641917 4
304649658927425623934102086438320211037295872576 2
358509643110564073501508187510676594629205563685 5
294752135008528794163773285339061097505443349998 1
115005697723689092756 3

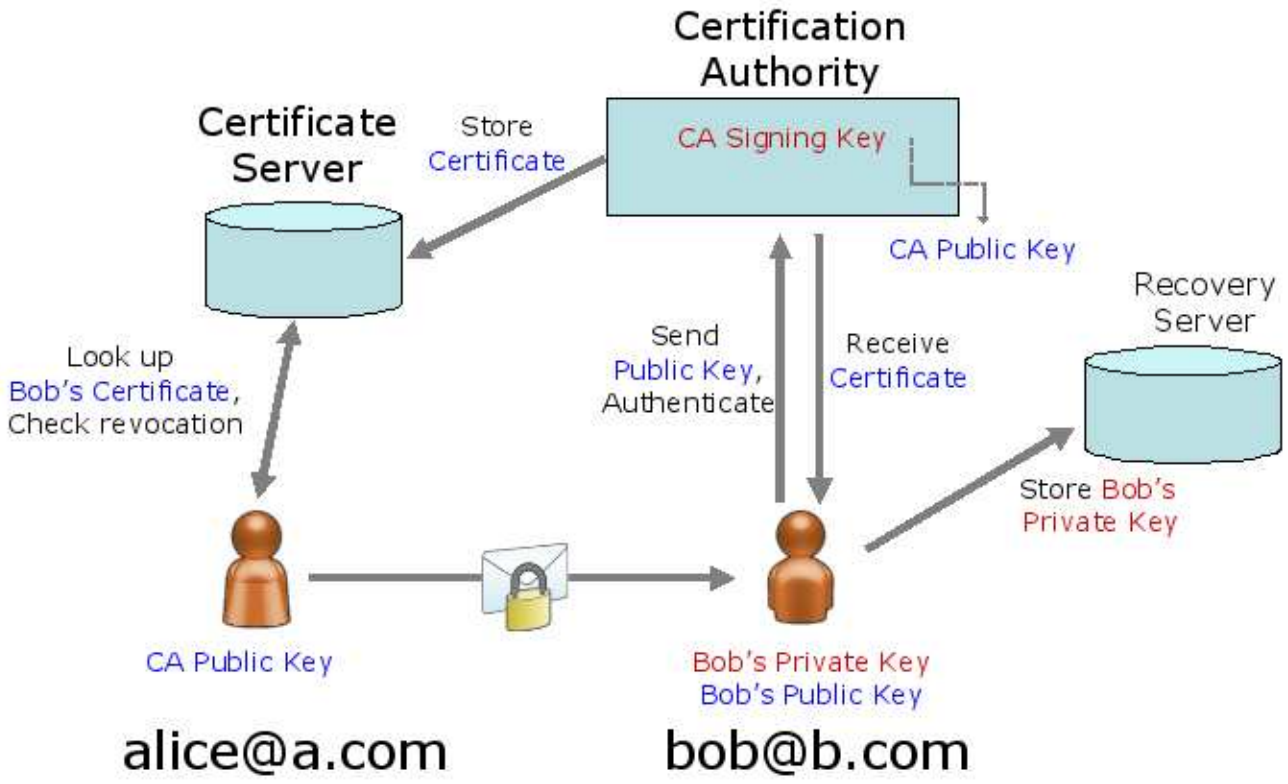
No Certificates

- Certificates bind **xyz@ab.c** to 0x1350664108...

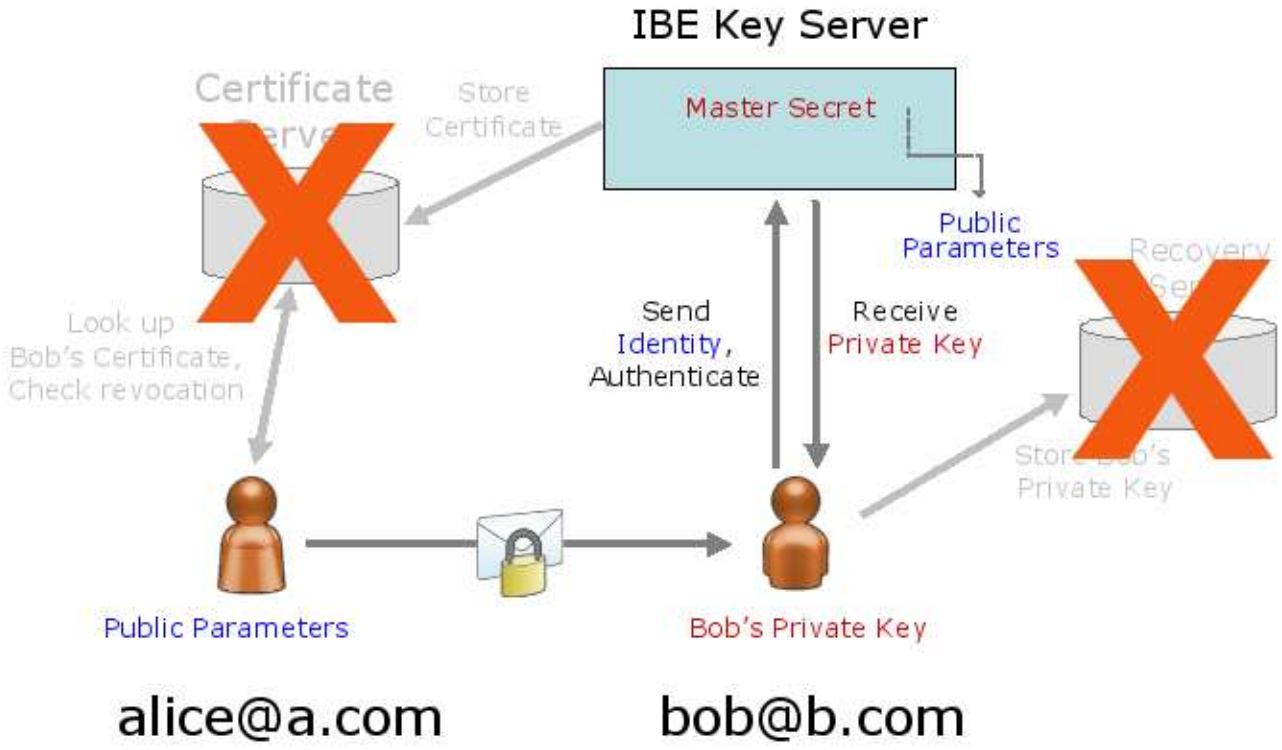
- ID-based crypto: Identities = Public Keys
  - No certificate management
  - No revocation lists*
  - No pre-enrollment

* with short-lived public keys:
alice@gmail.com|week#42

Traditional PKI



IBE System



Brief History

- Crypto favorite: groups with hard DL
  - subgroup of Z_q^*, prime order $p \mid q-1$
  - Elliptic Curves $E(F_q)$: $y^2 = x^3 + ax + b \pmod q$

- Extra structure on special EC: bilinear maps
  - 1946: Weil definition ("Weil pairing")
  - 1984: Miller algorithm
  - 1993: MOV attack
  - 2000-today: many creative uses

Bilinear Maps or Pairings

- G , G_t – prime order p
- $e : G \times G \rightarrow G_t$
  - bilinear: $\forall a,b \in Z \quad \forall g \in G \quad e(g^a, g^b) = e(g, g)^{ab}$
  - non-degenerate: g gen. $G \Rightarrow e(g, g)$ gen. G_t
  - efficiently computable
- general case $e : G \times G' \rightarrow G_t$

Early Consequences

- D-Log reduction from G to G_t [MOV'93]

  find $x \in Z$ DL in G DL in G_t

  given $g, g^x \in G \Rightarrow e(g,g), e(g,g)^x \in G_t$

- Decision-DH easy in G [Joux'00, JN'01]

  given $g, g^a, h, h^b \in G$

  decide if $a = b$ by testing $e(g, h^b) = e(g^a, h)$

New Class of "Gap" Assumptions

- Gap-DH – minimalistic

  given $g, g^a, g^b \in G$ can't compute g^{ab} (CDH)

  despite pairing (acting as DDH oracle)

BDH Assumption

Bilinear DH [Joux+Nguyen'01]

on input $g,\ g^a,\ g^b,\ g^c \in G$

output/decide $e(g, g)^{abc} \in G_t$

- BF : adaptive-ID secure under BDH in RO model
- BB-1 : selective-ID secure under decisional BDH

BDHI Assumption

Bilinear DH Inversion [MSK'02,BB'04]

on input $g,\ g^x,\ g^{x2},\ g^{x3},\ \ldots,\ g^{xm} \in G$

output/decide $e(g, g)^{1/x} \in G_t$

- Needed for all "exponent inversion" schemes
- Strong! Adversary gets heaps of data...

  $\Omega(p^{1/3})$ generic attack complexity [BB'04]

  $\Theta(p^{1/3} \log p)$ best-case algorithm [Cheon'06]

  Compare: $\Theta(p^{1/2})$ generic d-log

Linear Assumption

Decision Linear in G [BBS'04]

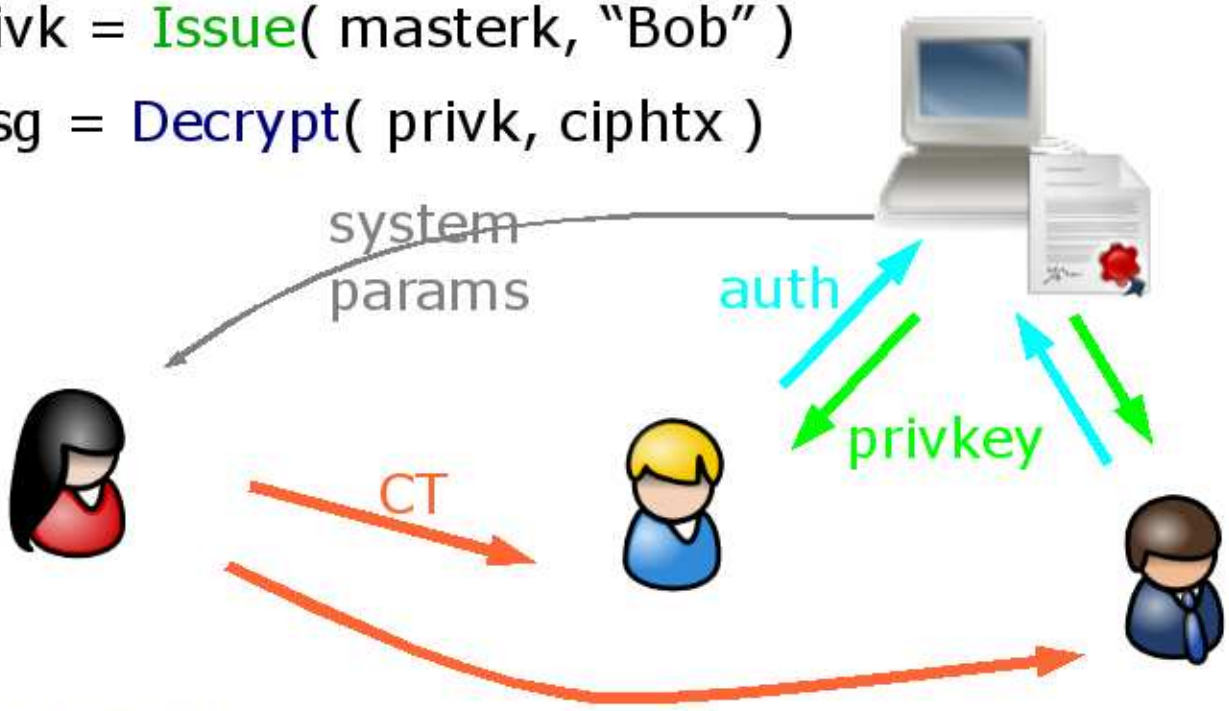
given $g,\ g^a,\ g^b,\ g^{ac},\ g^{bd},\ h \in G$

decide if $g^{c+d} = h$

- "Pairing-resistant" version of DDH
  - believed hard even though pairing makes DDH easy
  - appears about as benign as BDH
- Assumption of choice "to hide stuff"
  - useful, e.g., for anonymous IBE

The IBE Abstraction

- (systempars, masterk) = Setup()
- ciphtx = Encrypt(systempars, "Bob", message)
- privk = Issue(masterk, "Bob")
- msg = Decrypt(privk, ciphtx)



IB Encrypt. vs. Encaps. vs. Exchng.

not to be confused…

- Full Encryption –– most flexible, self-cont.
  - but, can waste bandwidth in hybrid scheme
- Key Encapsulation –– clean abstraction
  - but, 2 dependent layers, or 3 for multi-recipient
- Key Exchange –– "bilateral" uses only
  - cross-domain operation can be very tricky

Known IBE Frameworks

(non-pairing) QR/factoring [C'01] → [BGH'07] Lattices [GPV'08]

FDH "Full Domain Hash"

[BF'01] → [GS'02] [YFDL'04]

- allows hierarchies, threshold; but slow complex hashing

EI "Exponent Inversion"

[BB'04,#2] [SK'03]/[CCMLS'05] (& [G'06], qualified)

- vanilla IBE, though extensions are possible [B'07] ...

CB "Commutative Blinding"

[BB'04,#1] → [BBG'05] [SW'05] [W'05] [N'05] [BW'06] ...

- most flexible: hierarchies, threshold, anonymity, attributes, etc.; weakest assumptions

Full Domain Hash FDH framework

- Prototype: BF-IBE [Boneh+Franklin'01]

- Encryption Session Key:

$$e(H(id)^s , g^x)$$

  - s – ephemeral, chosen by sender
  - x – master secret
  - id – recipient identity

[Boneh+Franklin'01] BF IBE (FDH)

- Setup – MsK: $x \in Z_p$ Pars: $u=g^x$
- Issue(x,id) – PvK: $d=H(id)^x$
- Encrypt(u,id,m) –
  pick $s \in Z_p$ Sessk: $k= e(u,H(id))^s$
  CT: $a= g^s$
  $b= \{m\}_{H'(k)}$

  $e(g^x,H(m))^s$
  $e(g^s,H(m)^x)$
- Decrypt(d,a,b) – Sessk: $k= e(a,d)$

Exponent Inversion EI framework

- Prototypes: SK IBE [Sakai+Kasahara'03]
  BB-2 IBE [Boneh+B.'04]
  (G IBE) [Gentry'06]

- Encryption Session Key:

$$e(g , g')^s$$

  - s – ephemeral, chosen by sender
  - g, g' : independent of master secret

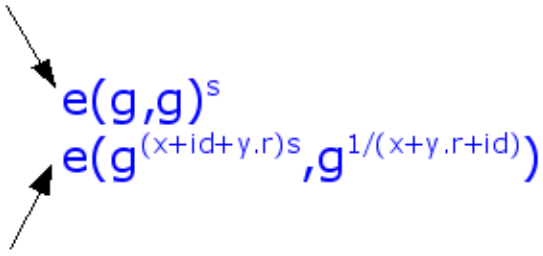
[Sakai+Kasahara'03] (Modified) SK IBE (EI)

- Setup – MsK: $x \in Z_p$ Pars: $u=g^x$
- Issue(x,id) – PvK: $d=g^{1/(x+H(id))}$
- Encrypt(y,id,m) –
  pick $r \in Z_p$ Sessk: $k= e(g,g)^r$
  CT: $a= u^r g^{H(id).r}$
  $b= \{m\}_{H'(k)}$

  $e(g,g)^r$
  $e(g^{(x+h)r}, g^{1/(x+h)})$
- Decrypt(d,a,b) – Sessk: $k= e(a,d)$

[Boneh+B.'04] BB-2 IBE (EI)

- Setup – MsK: $x,y \in Z_p$ Pars: $u=g^x$, $v=g^y$
- Issue(x,y,id) – PvK: $r \in Z_p$ $d=g^{1/(x+y.r+id)}$
- Encrypt(u,v,id,m) –
  pick $s \in Z_p$ Sessk: $k= e(g,g)^s$
  CT: $a= u^s g^{id.s}$
  $b= v^s$
  $c= \{m\}_{H(k)}$



- Decrypt(d,a,b) – Sessk: $k= e(a.b^r,d)$

[Gentry'06] Gentry IBE (EI)

- Setup – MsK: PRF, $x \in Z_p$ Pars: $g, h, u=g^x$
- Issue(x,id) – PvK: $d = (h.g^f)^{1/(x+id)}$
  $f = PRF(id)$
- Encrypt(y,id,m) –
  pick $s \in Z_p$ Sessk: $k = e(g,h)^s$
  CT: $a = u^s g^{id.s}$
  $b = e(g,g)^s$
  $c = \{m\}_{H(k)}$

$e(g,h)^s$
$e(g^{s(..)}, h^{1/(..)} g^{f/(..)}).e(g,g)^{-sf}$

- Decrypt(d,a,b) – Sessk: $k = e(a,d).b^{-f}$

Commutative Blinding CB framework

- Prototype: BB1-IBE [Boneh+B.'04]

- Encryption Session Key:

$$e(g^s , g^y)$$

  - s – ephemeral, chosen by sender
  - y – master secret

[Boneh+B.'04] BB-1 IBE (CB)

Setup

- params : $[\ g\ ,\ A=g^{a}\ ,\ B=g^{b}\ ,\ V=e(g,g)^{y}\ ]$
- master-key : $Y=g^{y}$

"commutative" double ElGamal

Issue(Y,id)

- $K_{id} = [\ K_1 = Y.(A^{id}.B)^{r}\ ,\ K_2 = g^{r}\ ]$

Encrypt(id,M)

- $C = [\ C_0 = M.V^{s}\ ,\ C_1 = g^{s}\ ,\ C_2 = (A^{id}.B)^{s}\ ]$

Decrypt(K_{id},C)

- $C_0 . e(C_2, K_2) / e(C_1, K_1) = M$

High-Altitude Comparison

FDH

- BF IBE : slow Encrypt, needs HashToPoint on the curve

EI

- SK & BB-2 IBE : simplest schemes, strong assumption
  - Special group $G < E(F_q)$, prime $p=|G|\approx q$, $(p-1)/2$, $(p+1)/2$
  - SK : smallest *apparent* ciphertexts, requires RO model
- Gentry IBE : nice proof, even stronger assumption

CB

- BB-1 IBE : flexible, most secure, slightly more complex
  - Efficient hierarchies → practical forward-security
  - Threshold key extraction → no central key escrow
  - Special applications: anonymous IBE → encrypted search

Extending BB-1 IBE (CB)

Setup

- params : [g , $A=g^a$, $B=g^b$, $V=e(g,g)^y$]
- master-key : $Y=g^y$

Issue(Y,id)

- K_{id} = [$K_1 = Y.(A^{id}.B)^r$, $K_2 = g^r$]

Encrypt(id,M)

- C = [$C_0 = M.V^s$, $C_1 = g^s$, $C_2 = (A^{id}.B)^s$]

Decrypt(K_{id},C)

- $C_0 . e(C_2, K_2) / e(C_1, K_1) = M$

[Waters'05] Tighter Reduction (CB)

Setup

- params : [g , $A=g^a$, $B=g^b$, $V=e(g,g)^y$]
- master-key : $Y=g^y$

$A_1=g^{a1}, \ldots, A_n=g^{an}$

Issue(Y,id)

- $K_{id} = [K_1= Y.(A^{id}.B)^r , K_2= g^r]$

$K_{id} = [K_1= Y.(A_1^{i1}\ldots A_n^{in}.B)^r , K_2= g^r]$

$id=(i_1,\ldots,i_n) \in \{0,1\}^n$

bit-by-bit encoding

[Boneh+B.'04] Full Security : Practice (CB)

Setup

- params : [g , $A=g^a$, $B=g^b$, $V=e(g,g)^y$]
- master-key : $Y=g^y$

same as Basic BB-1

Issue(Y,id)

- K_{id} = [$K_1 = Y.(A^{id}.B)^r$, $K_2 = g^r$]

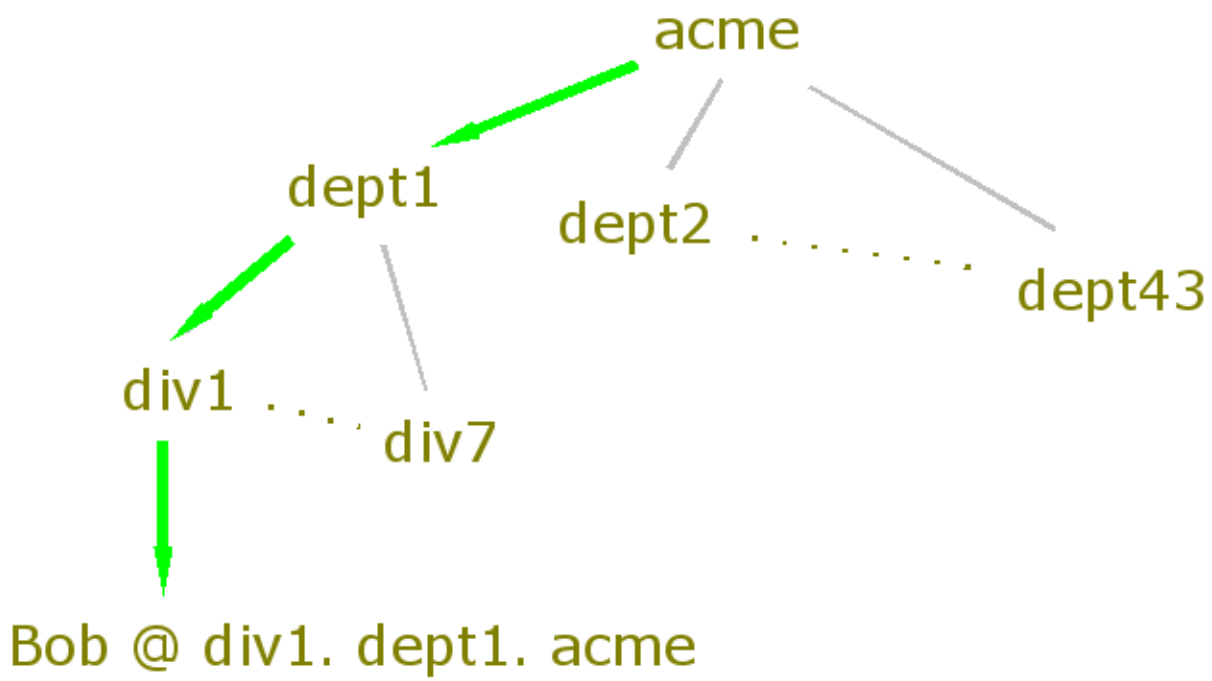
$(A^{H(id)}.B)^r$

Hash(id) here just an integer
---> negligible perf. hit

Hierarchical IBE

identities as a hierarchy: $ID=[ID_1,ID_2,\ldots,ID_n]$

- subprivkey = Derive(privkey, ID-suffix)



[Boneh+B.+Goh'05] Efficient HIBE (CB)

Setup

- params : $[\ g\ ,\ A_1=g^{a1}\ ,\ \ldots,\ A_n=g^{an}\ ,\ B=g^b\ ,\ V=e(g,g)^v\ ]$
- master-key : $Y=g^v$

$hid=(id_1,\ldots,id_j)\ \ j\le n$

Issue$(Y,id_1,\ldots,id_j)$

- $K_{id} = [\ Y.(A_1^{id1}\ldots A_n^{idj}.B)^r,\ g^r,\ A_{j+1}^{\ r},\ A_{j+2}^{\ r},\ldots,\ A_n^{\ r}\ ]$

Derive(K_{id},id_{j+1})

- $K'_{id} = [\ K_0.K_{j+1}^{id(j+1)}.(A_1^{id1}\ldots A_n^{id(j+1)}.B)^t,\ K_1.g^t,\ K_{j+2}.A_{j+2}^{\ t},\ \ldots,\ K_n.A_n^{\ t}\ ]$

Chosen-Ciphertext Security

- Random oracle model : heuristic [BR'93]
- Two-key paradigm [NY'90]
  - Encrypt twice, with NIZK proof of consistency
- Using IBE [CHK'04]
  - Render ciphertext self-dependent via the ID

[Naor+Yung'90,Cramer+Shoup'98] Two-Key Paradigm

CT: $\{M\}_{K1}$, $\{M'\}_{K2}$, NIZK[M=M']

- Simulator always knows either K1 or K2
  - Can decrypt all well-formed query CT
  - Challenge is not well-formed CT

[Boneh+Canetti+Halevi+Katz'04-05] CCA2 from IBE

CT: VK , $E=\{M\}_{id=VK}$, $Sig[E]$

CT: $C=Com[R]$, $E=\{M,D\}_{id=C}$, $Mac_R[E]$

- Simulator knows all but one private key
  - Let challenge VK* (or c*) be that special ID
    - known in advance ⇒ "selective-ID" security Ok
- Note: start from **H**IBE to get CCA2 (H)IBE

[B.+Mei+Waters'05] CCA2 from Pure IBE (CB)

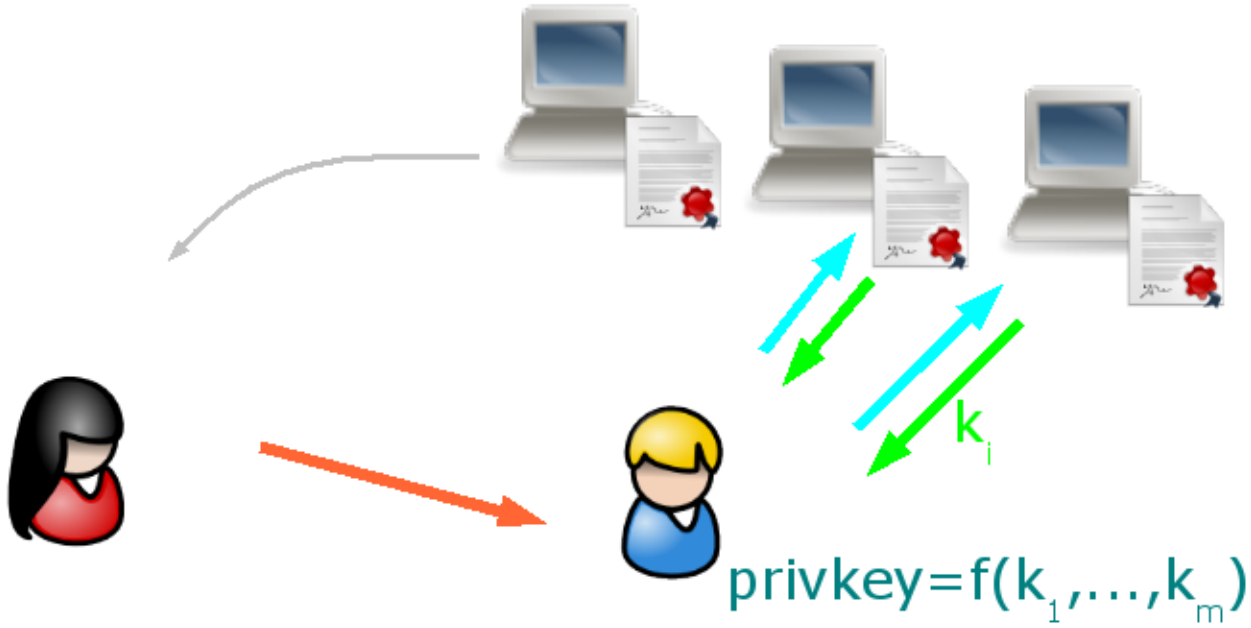
CT: $C_1 = g^s$, $C_2 = (A^{id(C_1)}.B)^s$ KEM-key=V^s

- No Sig./MAC/Commit.
- Underlying IBE must play nice (& w/o RO)
  - BB-1 family [BB'04,W'05,BBG'05,N'06,CS'06,...]
  - BB-2 works too [BB'04]

Threshold Private Keys

n key servers, t-out-of-n master-key shares

- privshare#i = ShareIssue(mastershare#i, “Bob”)
- privkey = Combine(privshare#i_1,..., privshare#i_t)



[Boneh+B.+Halevi'06] Threshold IBE (CB)

Setup

- params : [g , $A=g^a$, $B=g^b$, $V=e(g,g)^y$]
- master shares : $Y_1=g^{f(1)}, \ldots, Y_n=g^{f(n)}$ $f(0)=y$

KeyShareIssue(Y_i,id)

- $K_{id,i}$ = [$Y_i.(A^{id}.B)^{r_i}$, g^{r_i}]

KeyShareVerify($K_{id,i}$) uses pairing…

KeySharesCombine(…,$K_{id,i}$,…)

- K_{id} = $\prod (K_{id,i})^{\lambda_i}$ λ_i – Lagrange coefs.
  = [$K_1 = g^{f(0)}.(A^{id}.B)^{r}$, $K_2 = g^{r}$]

[B.+Waters'06] Anonymous (H)-IBE (CB)

Ciphertext:

$$C = [\ C_0 = M.V^{s}\ ,\ C_1 = g^{s}\ ,$$
$$C_2 = (A^{id}.B)^{u*(s-t)}\ ,\ C_3 = (A^{id}.B)^{v*t}\ ,$$
$$C_4 = (C^{id}.D)^{u'*(s-t')}\ ,\ C_5 = (C^{id}.D)^{v'*t'}\ ]$$

Decryption:

$$e(\ C_1\ ,\ (A^{id}.B)^{r}\ (C^{id}.D)^{r'}\ )$$
$$/\ e(\ C_2\ ,\ g^{r/u}\ )\ e(\ C_3\ ,\ g^{r/v}\ )$$
$$e(\ C_4\ ,\ g^{r'/u'}\ )\ e(\ C_5\ ,\ g^{r'/v'}\ ) = 1$$

[SW'05,GPSW'06,...] Fuzzy & Attribute IBE

- Identities as collections of attributes
  - "Fuzzy IBE" – partial matches
  - "Attribute-based" – more complex matches
- Originally from CB IBE [SW'05, GPSW'06]
  - with more complex algebra in exponent
- Also possible from EI IBE [B.'07]
  - exponent algebra applied generically

Even More Applications

- (Multi-)Hierarchical IBE FDH, CB

  –> forward-secure (H)IBE

- Anonymous (H)IBE FDH, CB

  –> search on PK/IB-encrypted data

Practical Considerations

- Choosing an algorithm
  - Security : model & assumptions, ...
  - Performance : w.r.t. exact security!
  - Flexibility : bare-bones vs. useful extensions
  - Compatibility :
- Curves & pairings
  - Speed / Bandwidth / well studied or Hot New Stuff
    - SS/MNT/BN curves , Weil/Tate/Eta/Ate pairing , char.
  - Do we need (or forbid)...
    - Fast curve generation?
    - Hashing?
    - Homomorphism?
    - DDH?

That is all...