

Practical Aspects of Identity-Based Encryption

Xavier Boyen

Voltage

ECC'2006

Outline

1. The What and the Why?
2. Pairings & Assumptions
3. Crypto Schemes
4. Deployment Issues

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
4756056670275244851438515265106048595338339402871
5057190944179820728216447155137368041970396419174
3046496589274256239341020864383202110372958725762
3585096431105640735015081875106765946292055636855
2947521350085287941637732853390610975054433499981
1150056977236890927563

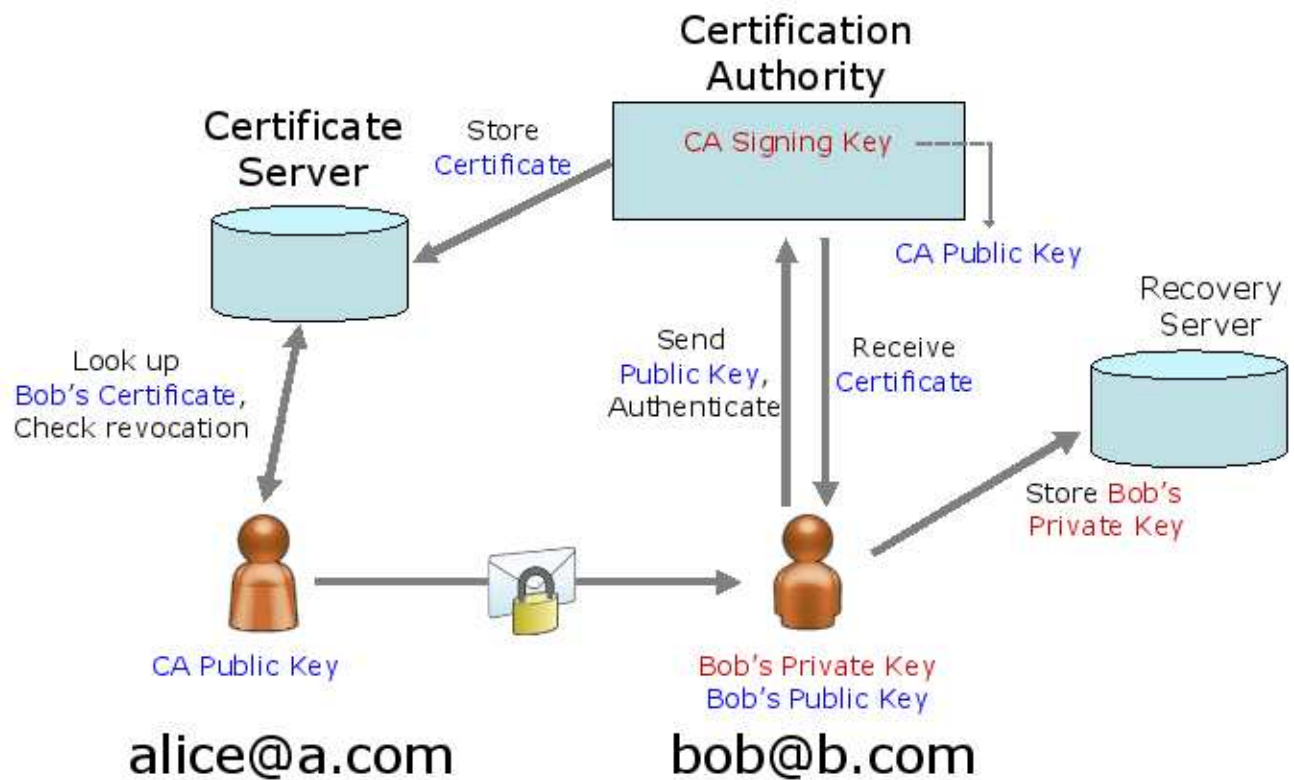
No Certificates

- ♦ Certificates bind **xyz@ab.c** to 0x1350664108...
- ♦ ID-based crypto: **Identities** = Public Keys
 - ♦ No certificate management
 - ♦ No revocation lists*
 - ♦ No pre-enrollment

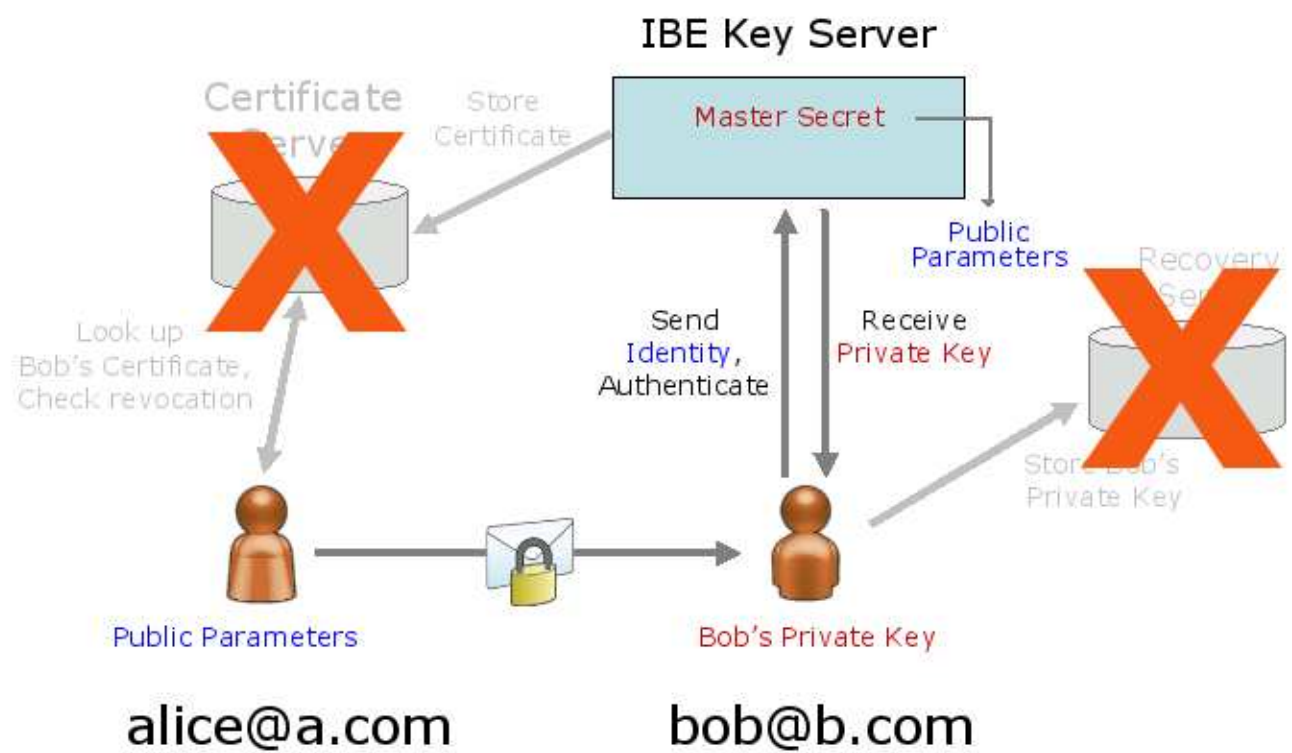
* with short-lived public keys:
alice@gmail.com|week#42



Traditional PKI



IBE System



Outline

1. The What and the Why?
2. Pairings & Assumptions
3. Crypto Schemes
4. Deployment Issues

Brief History

- ♦ Crypto favorite: groups with hard DL
 - ♦ subgroup of \mathbb{Z}_q^* , prime order $p \mid q-1$
 - ♦ Elliptic Curves $E(\mathbb{F}_q): y^2 = x^3 + ax + b \pmod{q}$
- ♦ 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

a.k.a. (bilinear) pairings

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

Some Consequences

- ♦ D-Log reduction from G to G_t [MOV'93]
find $x \in \mathbb{Z}$ 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 “Bilinear” Assumptions

- ♦ **Gap-DH** – minimalistic
given $g, g^a, g^b \in G$ can't compute g^{ab} (CDH)
despite pairing (acting as DDH oracle)
- ♦ **(Decision) Bilinear DH** – a new classic
given $g, g^a, g^b, g^c \in G$
can't compute $e(g, g)^{abc}$ (or disting. from rand.)
- ♦ many others: **Linear, SDH, BDHI, BDHE, ...**

Pairing-proof Assumptions Road Map

- ♦ **BDH, Tripartite DH** [Boneh+Franklin'01,...]
 - ♦ akin to CDH (& also DDH) -- blinding, encryption, ...
- ♦ **Strong DH** [Boneh+B.'04]
 - ♦ exponentially many hard solutions -- signatures, ...
- ♦ **DHI, BDHI, BDHE, ...** [MSK'02,BB'04,BBG'05,...]
 - ♦ lot of input data, single solution -- (many uses)
- ♦ **Linear** [Boneh+B.+Shacham'04]
 - ♦ full DDH substitute in base group -- ZK proofs, ...
- ♦ **(Subgroup)** [Boneh+Goh+Nissim'05]
 - ♦ hybrid: pairing + factoring -- ZK proofs, ...

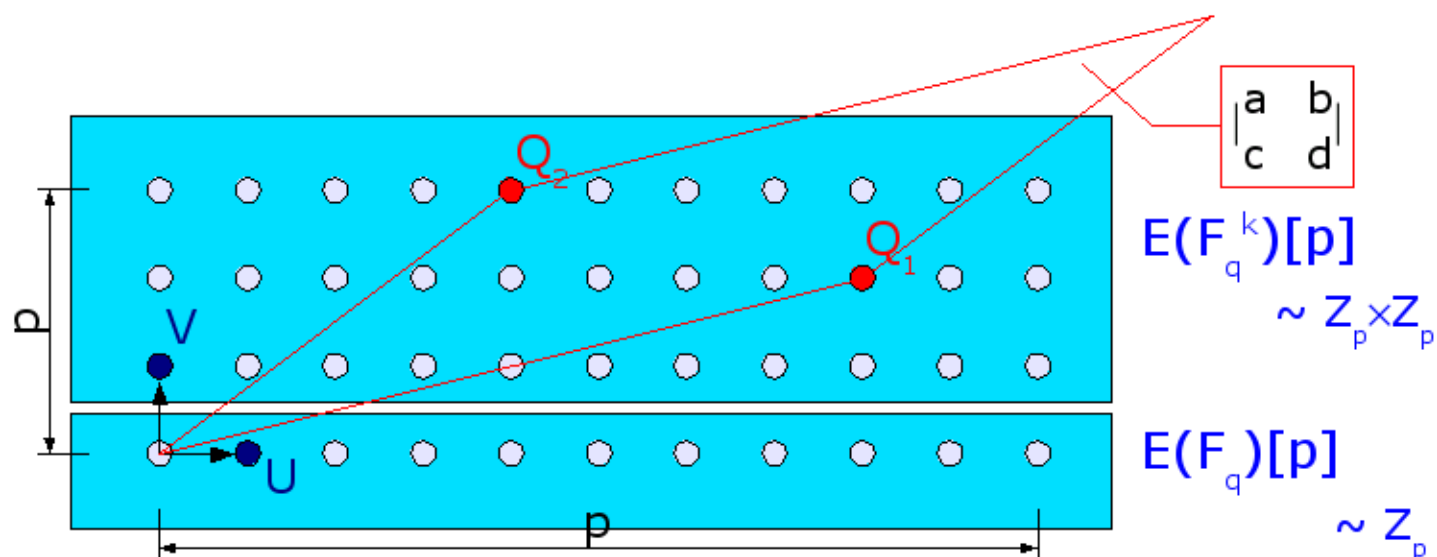
Why So Many Assumptions?

How about a single “pairing” assumption...
Which one?

- ♦ Too weak \rightarrow useless
 - ♦ e.g., assume only that pairing is non-invertible
- ♦ Too strong \rightarrow risky
 - ♦ e.g., interactive “oracle-based”
 - ♦ or, assume bilinear group is **generic** (= opaque)
 - ♦ (and even that is false under Subgroup!)

Sensible approach: *prefer* weak assumptions

Picturing the Weil Pairing



$$Q_1 = [a]U + [b]V$$

$$Q_2 = [c]U + [d]V$$

$$e_{\text{Weil}}(Q_1, Q_2) = \omega^{\begin{bmatrix} a & b \\ c & d \end{bmatrix}}$$

$$\omega = \sqrt[p]{1} \in (F_{q^k})^*$$

Weil-Miller magic:

$e_{\text{Weil}}(Q_1, Q_2)$ efficiently computable given just Q_1, Q_2

Bilinear Group Classification

Type-1 : $G = G'$ a.k.a. "symmetric"

- ♦ DDH easy : can be good or bad
- ♦ supersingular curves do not scale well

Type-2 : $G \leftarrow G'$ one way

- ♦ DDH easy in G'
- ♦ short element representation in G
- ♦ difficult to hash into G'

Type-3 : $G \not\leftarrow G'$ separated

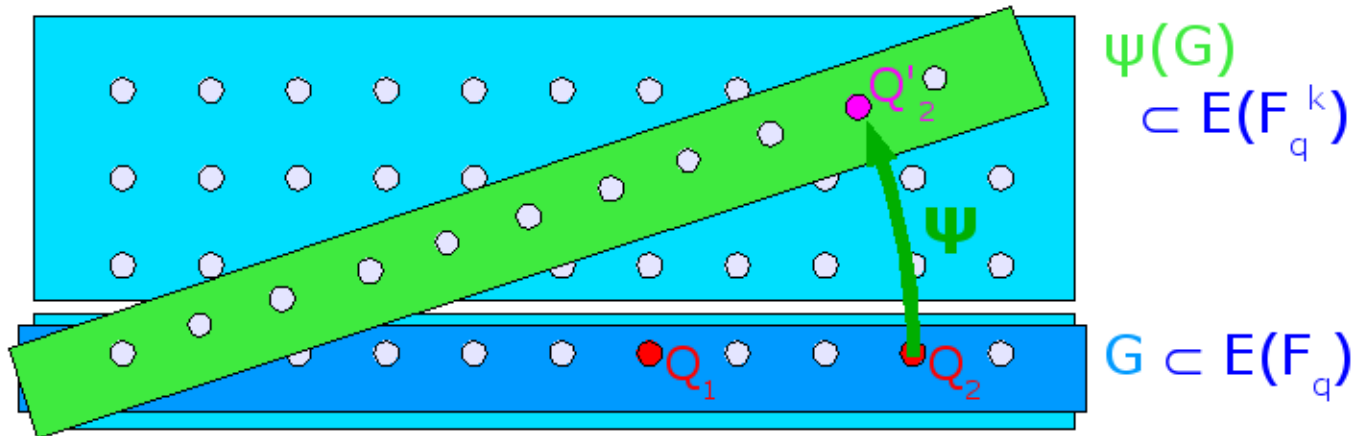
- ♦ cross-group "DDH-like" only
- ♦ absence of homomorphism hurts some proofs

Also : composite order $N = p_1 p_2 = |G|$

Type-1 Groups

on supersingular curves

e.g.: $y^2 = x^3 + x \pmod{q}$ for $q \equiv 3 \pmod{4}$



Distortion function: $\psi : G \rightarrow E(F_q^k)$

Define: $e(Q_1, Q_2) = e_{\text{Weil}}(Q_1, \psi(Q_2))$

♦ Symmetric Pairing: $e : G \times G \rightarrow G_t$

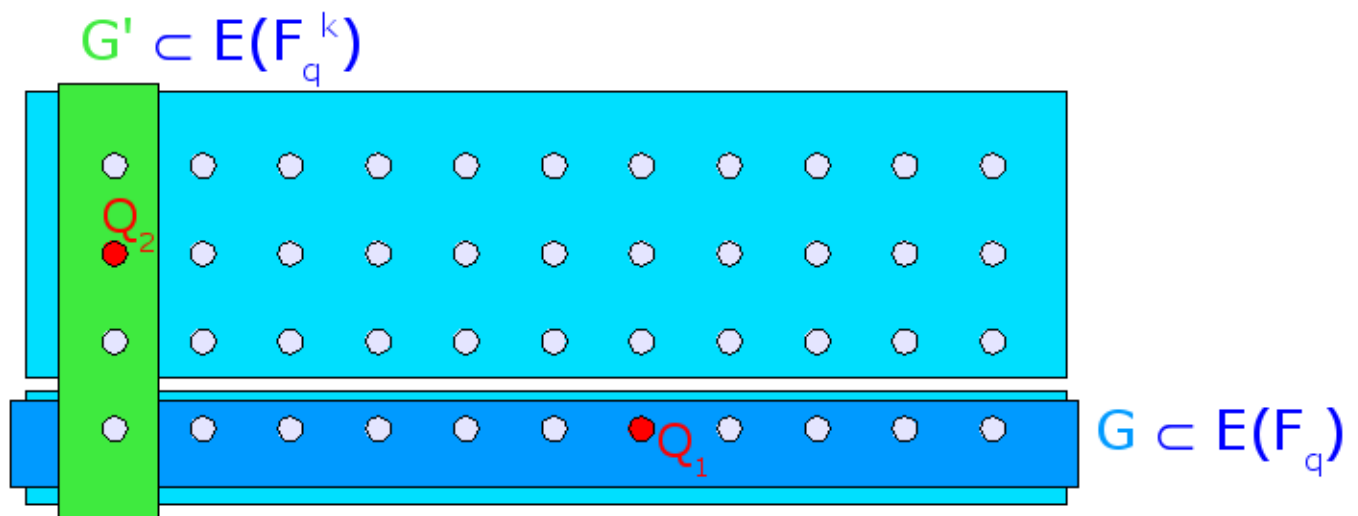
Type-2 and Type-3

e.g., on MNT

[Miyaji+Nakabayashi+Takano'01]

or BN curves

[Barreto+Naehrig'05]



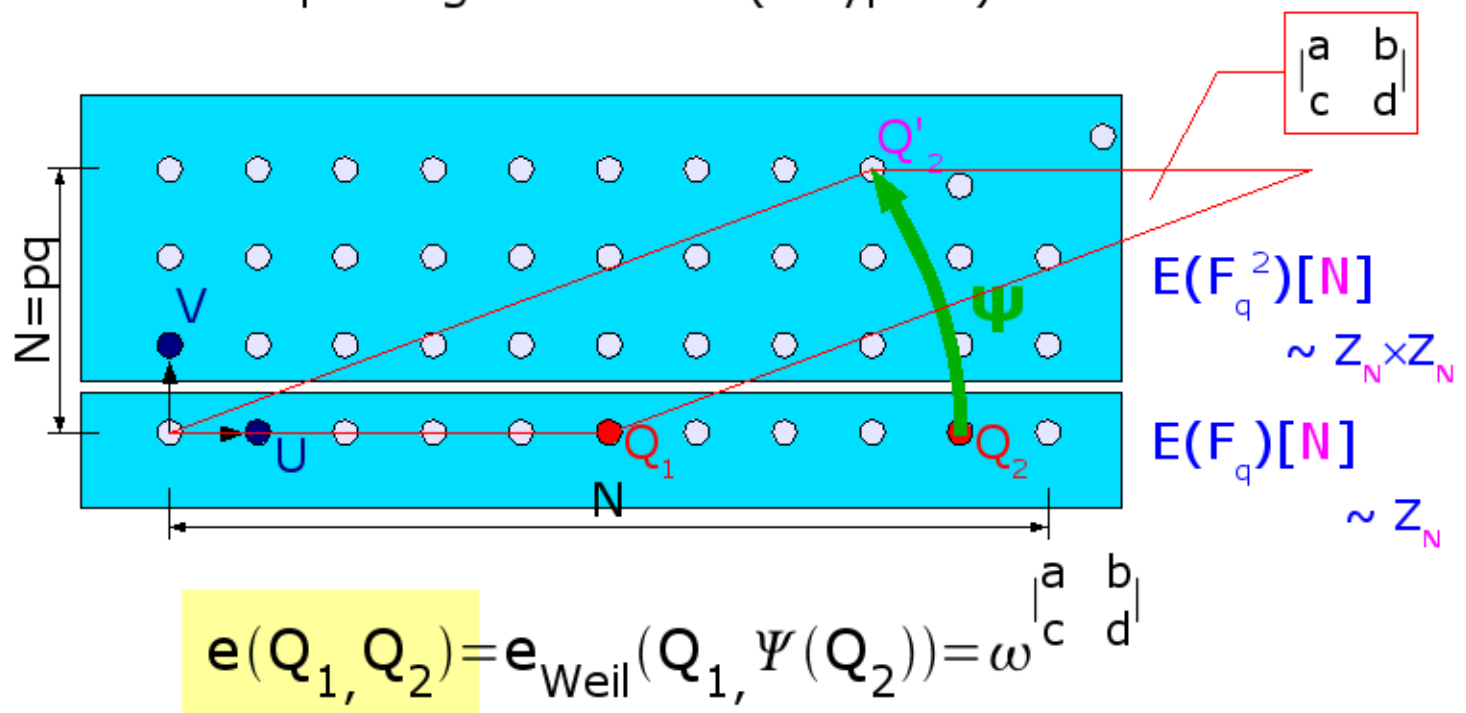
♦ Asymmetric Pairing:

$$e_{\text{Weil}} : G \times G' \rightarrow G_t$$

- ♦ Fewer assumptions, smaller representations
- ♦ Less powerful, more notation

Composite Order

on supersingular curves (\rightarrow type-1)



Domain & Range of order $N = p_1 p_2$:

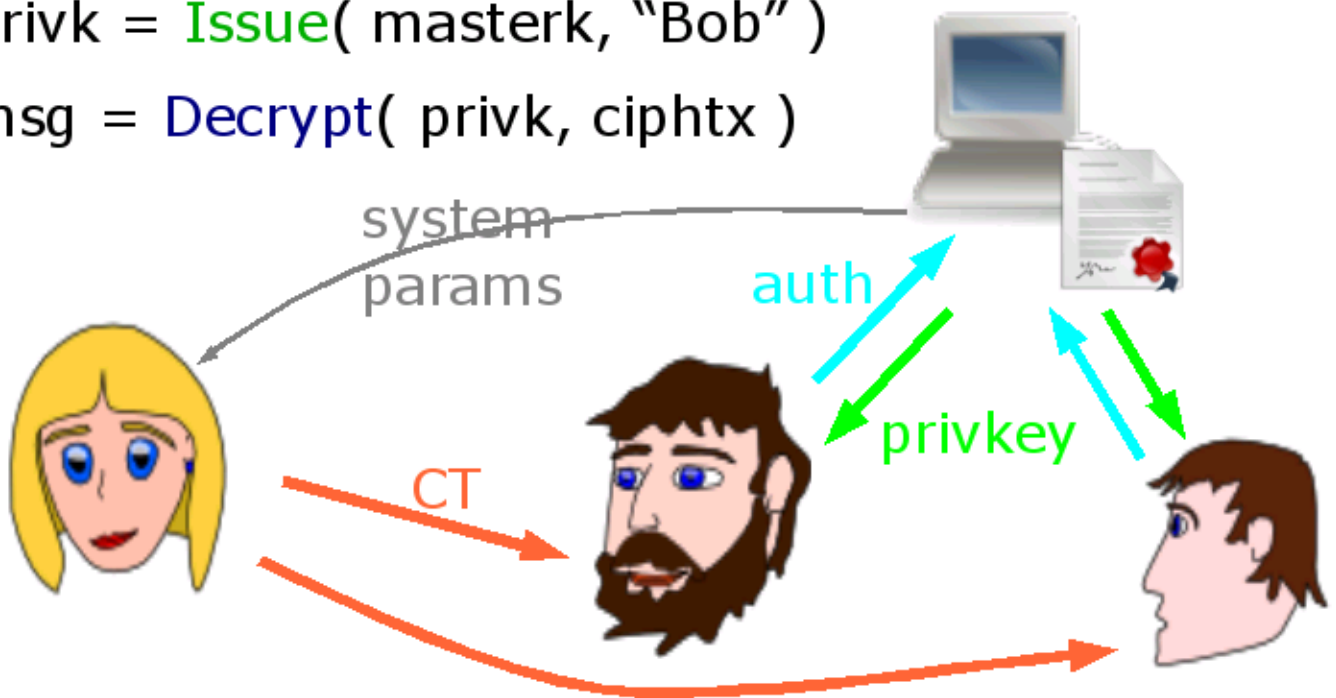
$e(Q_1, Q_2)$ has order N (or dividing N) in $(F_q^2)^*$

Outline

1. The What and the Why?
2. Pairings & Assumptions
3. [Crypto Schemes](#)
4. Deployment Issues

Identity-Based Encryption

- $(\text{systemparams}, \text{masterk}) = \text{Setup}()$
- $\text{ciphtx} = \text{Encrypt}(\text{systemparams}, \text{"Bob"}, \text{message})$
- $\text{privk} = \text{Issue}(\text{masterk}, \text{"Bob"})$
- $\text{msg} = \text{Decrypt}(\text{privk}, \text{ciphtx})$



Encryption / KEM / Key Exchange

the practitioner's viewpoint

- ♦ Full Encryption -- most flexible
 - ♦ black box, but can waste bandwidth if hybrid
- ♦ Key Encapsulation -- neat and clean
 - ♦ but, 2 or 3 dependent layers (multi-recipient)
- ♦ Key Exchange -- special uses
 - ♦ but, cross-domain operation can be tricky

Classes of Known IBE Schemes

Quadratic Residuosity [C'01] (factoring-based)

“Full Domain Hash” (pairing-based)

[BF'01] \rightarrow [GS'02] [YFDL'04]

♦ BDH with mandatory RO

“Exponent Inversion”

([MSK'02]) \rightarrow [SK'03] [BB04,#2] , [G'06]

♦ “large” BDHI or similar

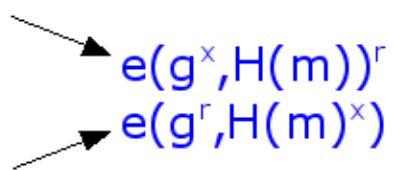
“Commutative Blinding”

[BB04,#1] \rightarrow [BBG'05] [SW'05] [W'05] [N'05] [BW'06] ...

♦ BDH or Linear

[Boneh+Franklin'01] Basic 'BF' IBE

full-domain HashToPoint

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

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

[Sakai+Kasahara'03] Basic "SK" IBE

exponent inversion

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

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

BDH Assumption

to prove BF-IBE in RO model

Bilinear DH

[BF'01]

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

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

BDHI Assumption

typical of “exponent inversion” schemes

Bilinear DH Inversion

[MSK'02,BB'04]

given $g, g^x, g^{x^2}, g^{x^3}, \dots, g^{x^m} \in G$

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

- ♦ Adversary gets tons 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

[Gentry'06] Gentry's Basic IBE

exponent inversion in target group

- Setup – MsK: PRF, $x \in \mathbb{Z}_p$ Pars: $g, h, u = g^x$
- Issue(x, id) – PvK: $d = (h g^f)^{1/(x+id)}$
 $f = \text{PRF}(id)$
- Encrypt(y, id, m) –
 pick $r \in \mathbb{Z}_p$ Sessk: $k = e(g, h)^r$
 CT: $a = u^r g^{id \cdot r}$
 $b = e(g, g)^r$
 $c = \{m\}_{H'(k)}$
 $e(g, h)^r$
 $e(g^{r(\dots)}, h^{1/(\dots)} g^{f/(\dots)}) e(g, g)^{-rf}$
 Decrypt(d, a, b) – Sessk: $k = e(a, d) b^{-f}$

[Boneh+B.'04] Basic 'BB-1' IBE

Setup

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

Issue(Y, id)

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

Encrypt(id, M)

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

Decrypt(K_{id}, C)

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

"commutative"
dual blinding

30,000-foot Comparison

best approach in practice?

- ♦ BF-IBE : slow Encrypt, requires HashToPoint
- ♦ SK-IBE : severely limited, but very fast scheme (provided Cheon's best case is avoided)
 - ♦ Need $G < E(F_q)$, prime $p = |G| \approx q$, $(p-1)/2$, $(p+1)/2$
 - ♦ In business once parameters are selected
- ♦ Gentry-IBE : equally limited, nice proof
- ♦ BB1-IBE : very flexible, very fast, somewhat more b/w
 - ♦ Efficient hierarchy → practical forward-security
 - ♦ Threshold keygen → no central key escrow
 - ♦ Special applications: anonymous IBE → encrypted search

Outline

1. The What and the Why?
2. Pairings & Assumptions
3. Crypto Schemes
4. [Deployment Issues](#)

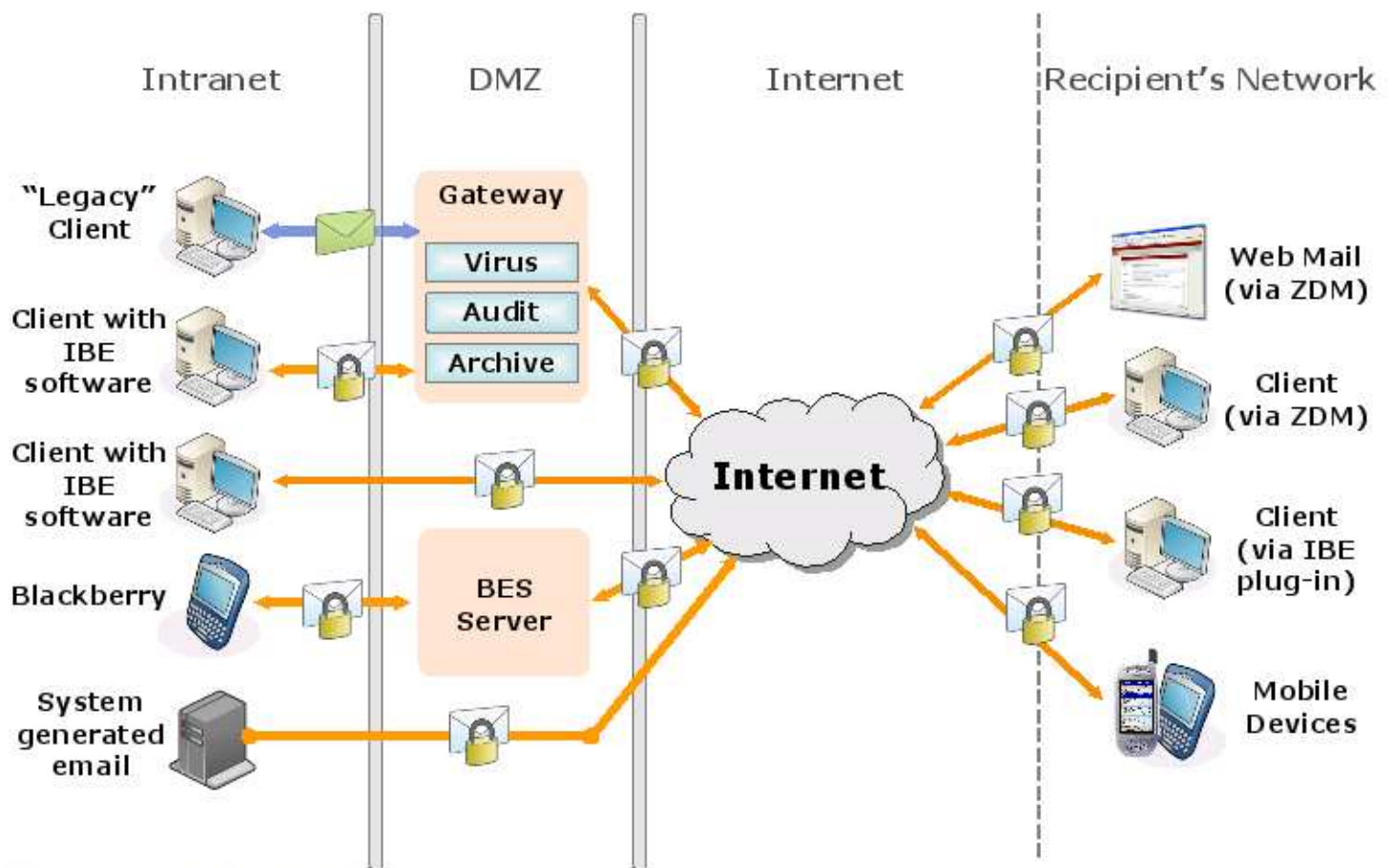
Practical Considerations

- ♦ 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...
 - ♦ Fast curve generation?
 - ♦ Hashing?
 - ♦ Homomorphism?
 - ♦ DDH?

The Need for Speed

- ♦ More for Encryption than Decryption
 - ♦ single sender can blast to 10-s of recipients
 - ♦ typical user decrypts & reads 1 email at a time
- ♦ Key Issuance?
 - ♦ central server: expected bottleneck...
 - ♦ mitigated by staggering key expirations
 - week#42 – Alice's starts on Monday
 - Bob's starts on Wednesday
- ♦ In reality: not just Alice & Bob...

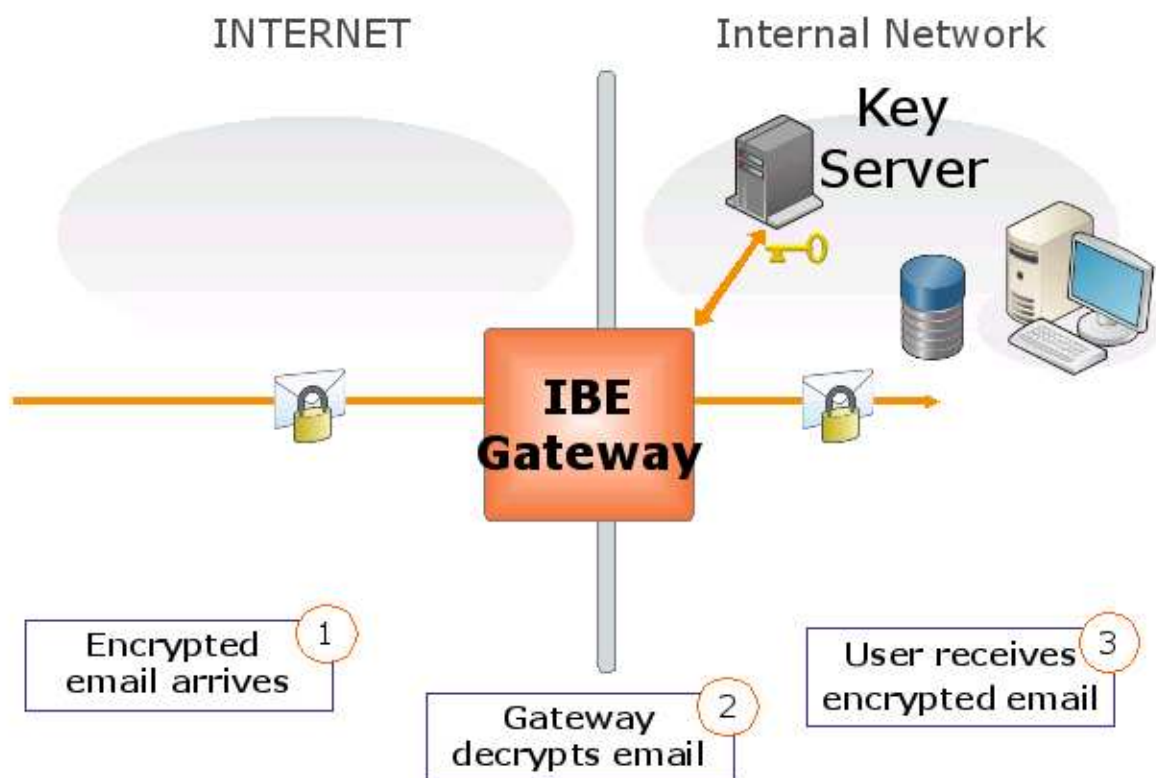
Typical Architecture



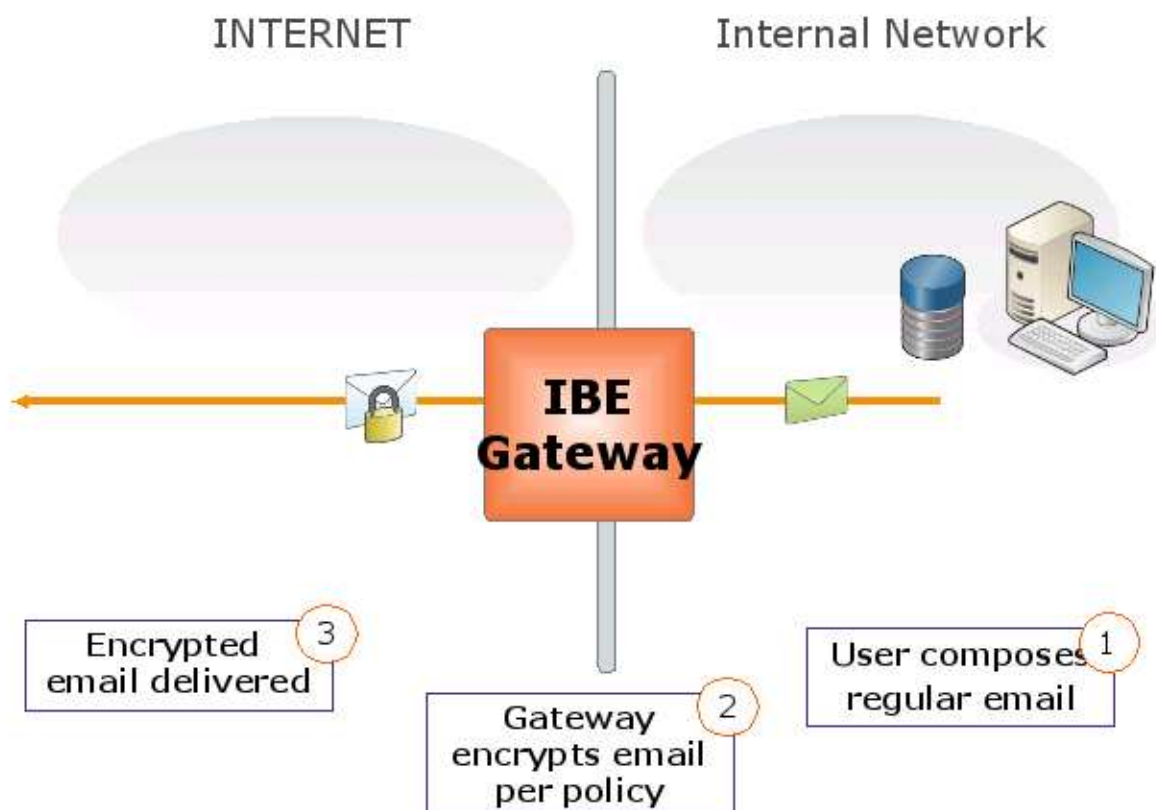
Deploying an IBE System

- ♦ **IBE / PKI complementarity**
 - ♦ PKI strengths : backbone & signature chains (SSL)
 - ♦ IBE better for encryption at the edges (end users)
- ♦ **Critical features**
 - ♦ Cross-domain communication
 - ♦ Policy-based mandatory encryption
 - ♦ “Gateway” decryption (e.g., for virus scanning)
 - ♦ “Zero-download” web decryption (access anywhere)
- ♦ **Nice to have**
 - ♦ Forward security, personal delegation (hierarchy)
 - ♦ Distributed key authority

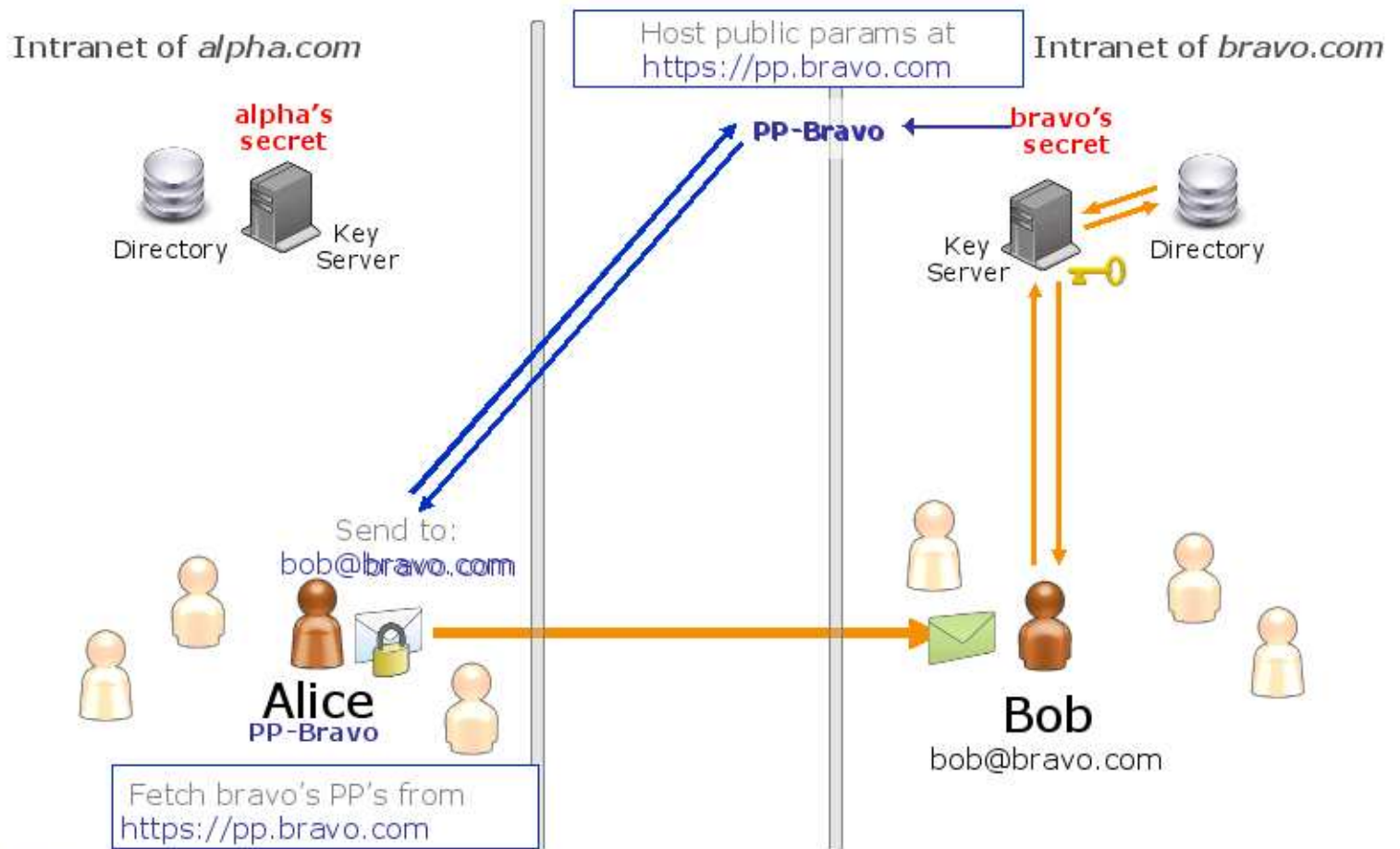
Incoming Content Scanning



Outgoing Mandatory Encryption

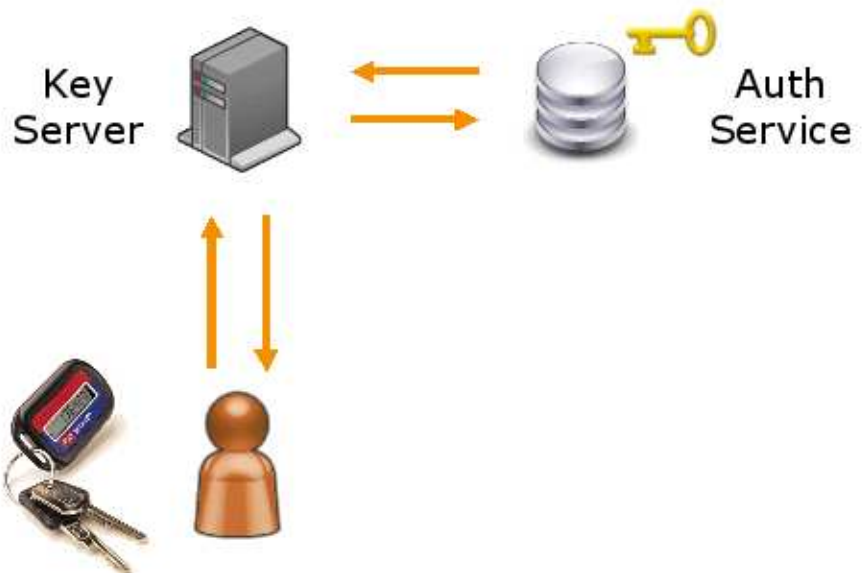


Cross-domain "Federation"



User Authentication

- ♦ **Crucial** : on it rests the whole system
(Also true for PKI, but less conspicuously so...)



The Authentication Gradient

OMB-04-04

Level:

Level 4

Three factor auth (Bio+PKI+PIN)

PKI Smart Card, USB Token

Level 3

RSA SecurID

Windows domain controller

Level 2

Directory with pre-enrollment

User password with call center reset

Level 1

Email answerback w/ passwords

Email answerback (VeriSign Class 1)

No Authentication

Pre-enrollment
Self-provisioning

IBE Systems are Extremely Scalable

- “Stateless” key servers
 - No growing store of certificates
 - No growing store of private keys
 - No revocation lists
- Easy to load-balance
 - Just put two of them next to each other
- Easy backup and disaster recovery
 - Only master secret (+ policy & configuration) needs to be backed up
 - Size: < 100 kByte, fits on floppy disk
 - Master secret is long lived : put it once in a safe
 - Same for 100 or 100,000 users



Thank You!

Any
Questions



Credits to

Guido Appenzeller & Voltage for selected slides & artwork