# BB1 IBE & IBKEM

Xavier Boyen

Voltage

IEEE P1363.3 @ CRYPTO'2006

# Classification of IBE Schemes

Quadratic Residuosity (factoring-based)

[C'01]

“Full Domain Hash” (pairing-based)

[BF'01] → [GS'02] [YFDL'04]

“Exponent Inversion”

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

“Commutative Blinding”

[BB04,#1] → [BBG'05] [SW'05] [W'05] [N'05] [CS'05] ...

... by far, most flexible

# Bilinear Pairings

a.k.a. Bilinear Maps

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

# Basic “BB-1”

## Setup

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

## Extract(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)

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

# Proposed "BB-1" IBE

## Setup

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

## Extract(Y ,id)

- $K_{id} = [\ K_{1} = (g')^{y+(a\,H(id)+b)r}\ ,\ K_{2} = (g')^{r}\ ]$

## Encrypt(id,M)

$K = V^{s}$

- $C = [\ C_{0} = M \text{ xor } H'(K)\ ,\ C_{1} = g^{s}\ ,\ C_{2} = (A^{H(id)}.B)^{s}\ ]$

$C_{3} = s + H''(K,C_{0},C_{1},C_{2})$

## Decrypt($K_{id}$,C)

- $K = e(C_{2}, K_{2}) / e(C_{1}, K_{1})$, $M = C_{0} \text{ xor } H'(K)$ , $s = C_{3} - H''(K,C_{0},C_{1},C_{2})$, test $K=V^{s}$ & $C1 = g^{s}$

# Proposed “BB-1” IBKEM

## Setup

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

## Extract(Y ,id)

- $K_{id} = [\ K_1 = g^{y+(aH(id)+b)r}\ ,\ K_2 = g^{r}\ ]$

## Encrypt(id,M)

- $C = [\ C_1 = g^{s}\ ,\ C_2 = (A^{H(id)}.B)^{s}\ ]$ $\qquad K = H'''(V^{s})$

## Decrypt($K_{id}$,C)

- $K = H'''(e(C_2, K_2) / e(C_1, K_1))$

# Security

Decision BDH in G [BF'03]

given $g, \; g^{a}, \; g^{b}, \; g^{c} \in G, \quad t \in G_{t}$

decide if $t = e(g,g)^{abc}$

IBE

fully secure : IND-ID-CCA2 in RO model

IBKEM

fully secure : ID and CCA2 for KEM in RO model