A Framework and Compact Constructions for Non-monotonic Attribute-Based Encryption

Shota Yamada

Nuttapong Attrapadung

Goichiro Hanaoka

Noboru Kunihiro

PKC2014, eprint 181

Summary of Our Results

- Non-monotonic KP-ABE schemes
  - with shortest ciphertext length
  - from the DBDH assumption with better (space) efficiency than previous scheme [OSW07]
  - with completely unbounded attributes (for the first time)

Constructed by our new framework

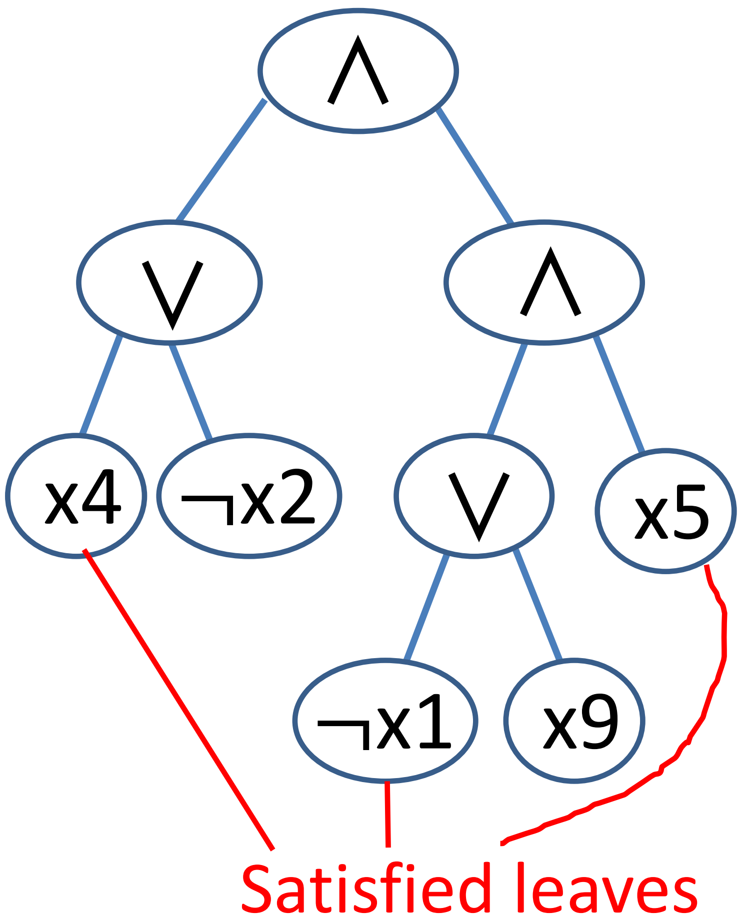
- The first completely unbounded non- monotonic CP-ABE scheme

Definitions

Access Tree

Non monotone Boolean formula

$F=(x4 \lor \neg x2) \land ((\neg x1 \lor x9) \land x5)$



$S_1=\{x2,x4,x5\}$

⇒Satisfy the access tree

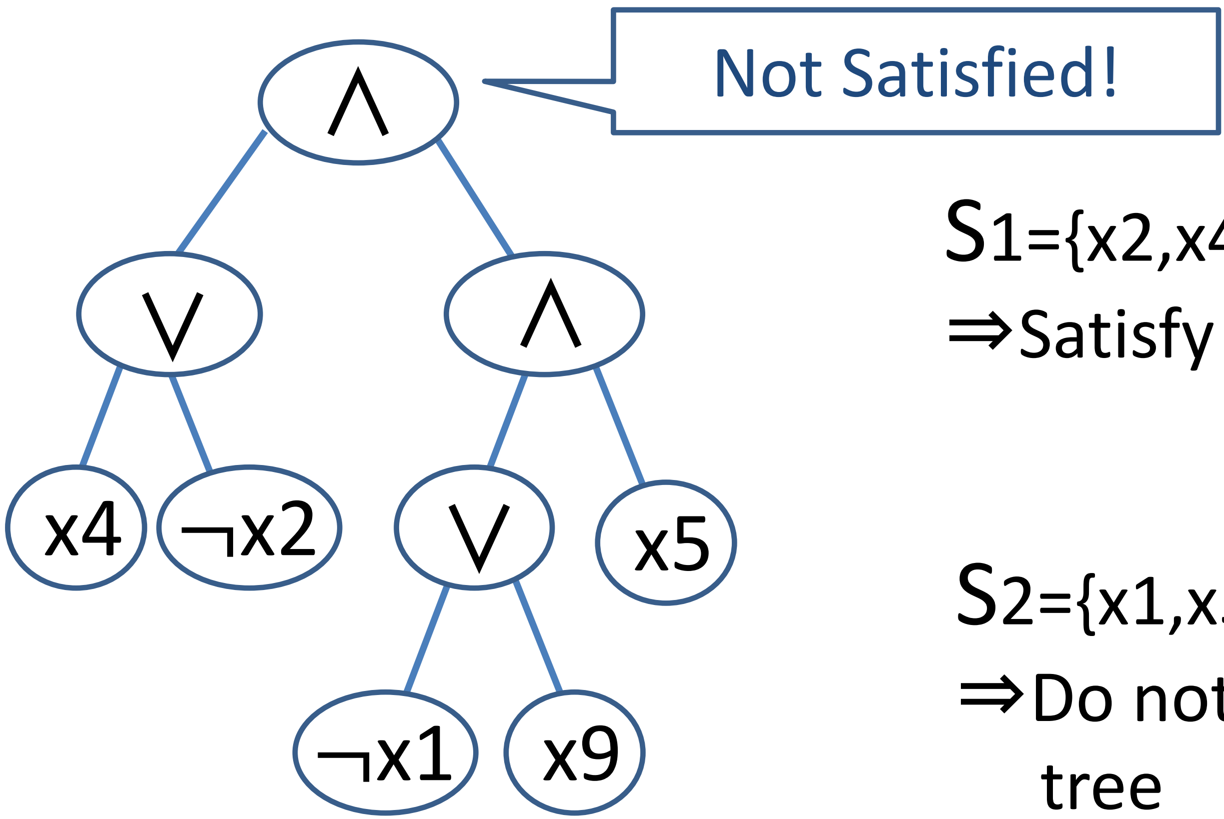
$S_2=\{x1,x5\}$

⇒Do not satisfy the access tree

Access Tree

Non monotone Boolean formula

$F=(x4 \vee \neg x2) \wedge ((\neg x1 \vee x9) \wedge x5)$



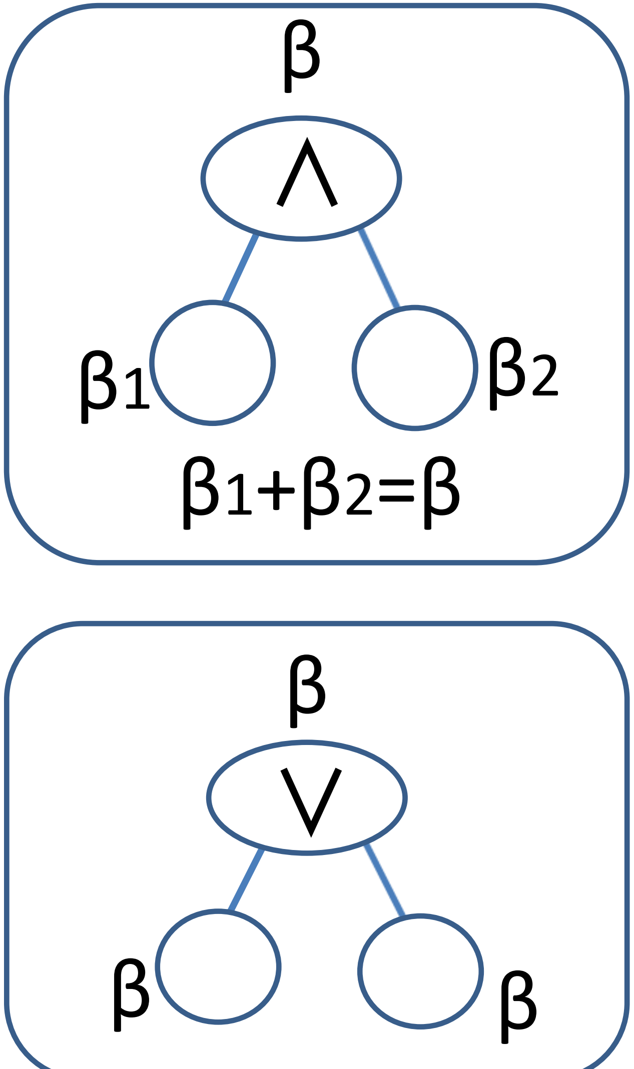
$S_1=\{x2, x4, x5\}$

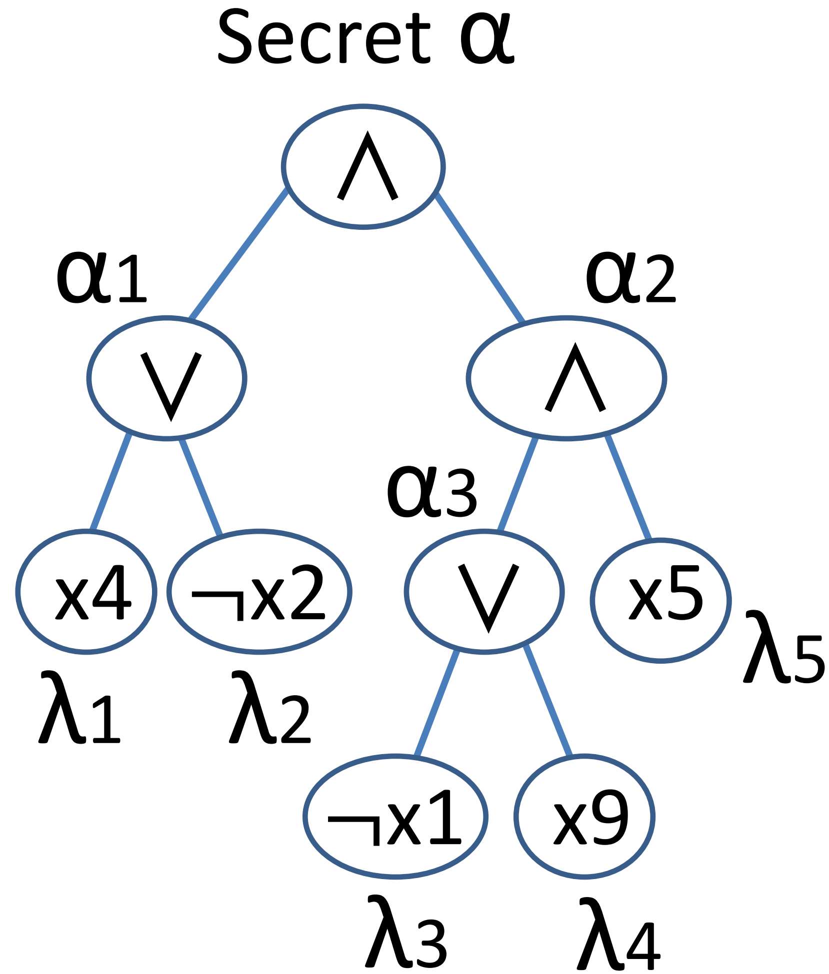
⇒Satisfy the access tree

$S_2=\{x1, x5\}$

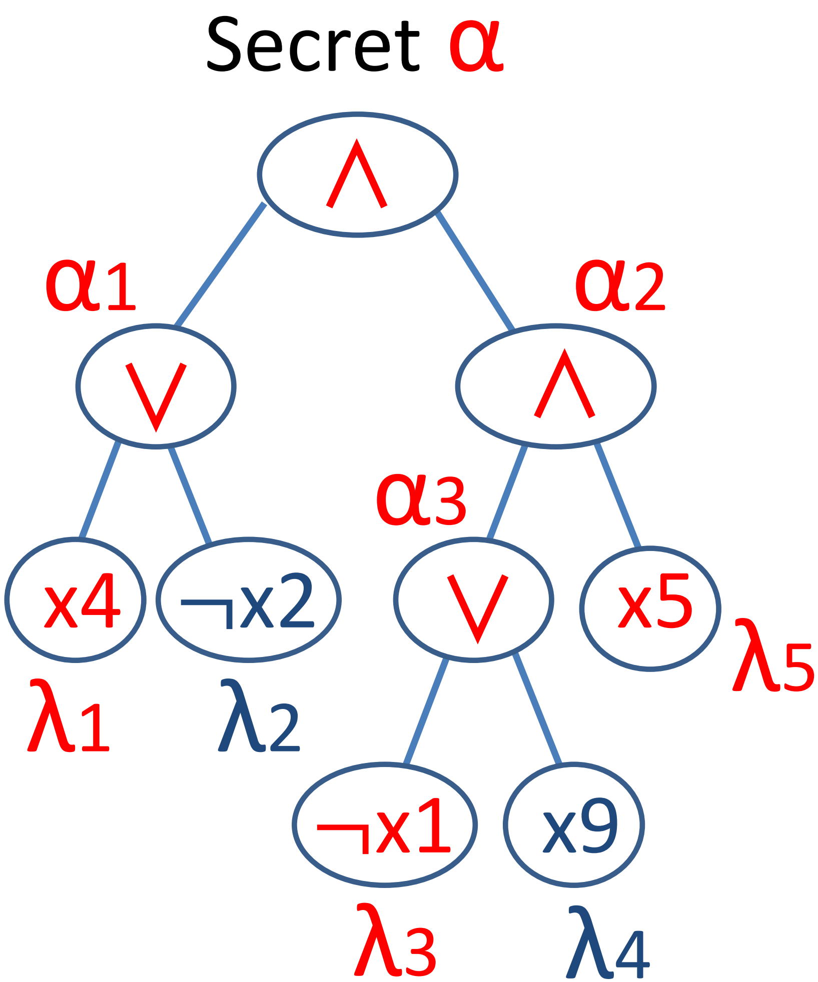
⇒Do not satisfy the access tree

Secret Sharing for Access Tree





Property of the Secret Sharing Scheme



$S=\{x2,x4,x5\}$

⇒Satisfy the access tree

⇒From shares corresponding to satisfied leaves ($\lambda_1, \lambda_3, \lambda_5$), one can recover α.

i.e, $\alpha_1=\lambda_1,\ \alpha_3=\lambda_3$

$\alpha_2=\alpha_3+\lambda_5$

$\alpha=\alpha_1+\alpha_2$

If S' does not satisfy the access tree, one cannot recover α from shares corresponding to satisfied nodes.

Predicate Encryption (KEM version)

Setup(1^λ)→(PK,MSK)

KeyGen(MSK,X)→SK_X

Enc(PK,Y)→(C_Y,K)

Dec(PK,Y,C_Y,SK_X)→K

Certain relation

Decryption is possible when $R(X,Y)=1$

KP-ABE, CP-ABE, spatial encryption etc. are all captured as a special case of predicate encryption by defining R appropriately.

Non-monotonic
Key Policy Attribute-Based Encryption

Attribute Space={x1,x2,x3,…}

Ciphertext C_S

S={x3,x79,x100,x2000}

Secret Key SK_F

F=(¬x44∧x79)∨x101

Set of attributes

Non-monotonic
Boolean Formula

(¬x44∧x79)∨x101
=(1∧1)∨0 =1

Decryption is possible

Two-mode Identity-Based Broadcast Encryption(TIBBE)

ID Space={x1,x2,x3,…}

Ciphertext C_S

e.g., S={x3,x79,x100,x2000}

Set of IDs

Two types of Keys

Type: IBBE

Secret Key $SK_{IBBE,ID}$

can decrypt C_S

Iff $ID \in S$

Type: IBR

Secret Key $SK_{IBR,ID}$

can decrypt C_S

Iff $ID \notin S$

Our Framework to Construct Non-monotonic KP-ABE

Our Framework to construct non-monotonic KP-ABE

- In [ALP11], conversion from IBBE with certain property to monotonic KP-ABE was given.

- We extend the result by [ALP11] and propose a conversion from TIBBE with certain property to non-monotonic KP-ABE.
  - Then, we construct various TIBBE schemes.

Remark: Our conversion converts selectively secure TIBBE into selectively secure non-monotonic KP-ABE.

Required Properties

We convert a TIBBE (KEM) with following property to a non-monotonic KP-ABE (KEM).

(*)The form of KEM key K and a secret key for ID is

$$K = e(g,g)^{s\alpha}, \qquad SK_{IBBE,ID} = (g^{\alpha} ***,***)$$

$$SK_{IBR,ID} = (g^{\alpha} ***,***)$$

where master secret key MSK=α.

In the following, we construct KP-ABE scheme

{KP-ABE.Setup, KP-ABE.KeyGen, KP-ABE.Enc, KP-ABE. Dec}

out of TIBBE scheme (with the above property)

{TIBBE.Setup, TIBBE.KeyGen, TIBBE.Enc, TIBBE.Dec}

Non-monotonic KP-ABE from TIBBE(1)

Universe of attribute = ID space
(Thus, the resulting scheme has
large universe)

$\boxed{\text{KP-ABE.Setup}(1^{\lambda})} = \boxed{\text{TIBBE.Setup}(1^{\lambda})}$

$\boxed{\text{KP-ABE.Enc(PK,S,M)}} = \boxed{\text{TIBBE.Enc(PK,S,M)}}$

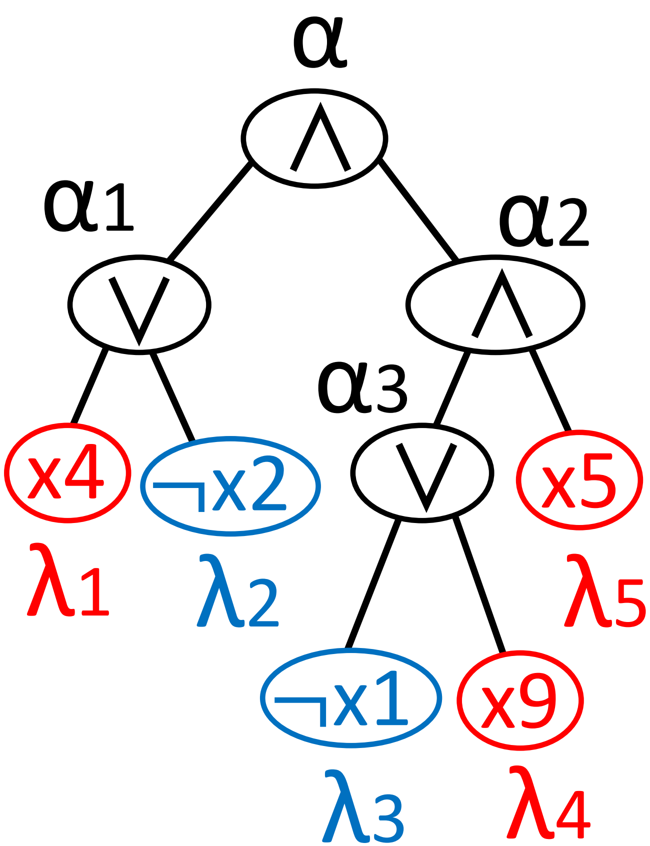
Set of attributes

Set of IDs

Non-monotonic KP-ABE from TIBBE(2)

KP-ABE.KeyGen(MSK,F):

A Boolean formula



For leaf node w positive attribute:

TIBBE.KeyGen(IBBE, x4, λ1) → $SK_{IBBE,x4}$

ID MSK

Also Generate $SK_{IBBE,x5}$ and $SK_{IBBE,x9}$.

For leaf node w negative attribute:

TIBBE.KeyGen(IBR, x2, λ2) → $SK_{IBR,x2}$

ID MSK

Also Generate $SK_{IBBE,x1}$

The final output is secret keys for all leaves:

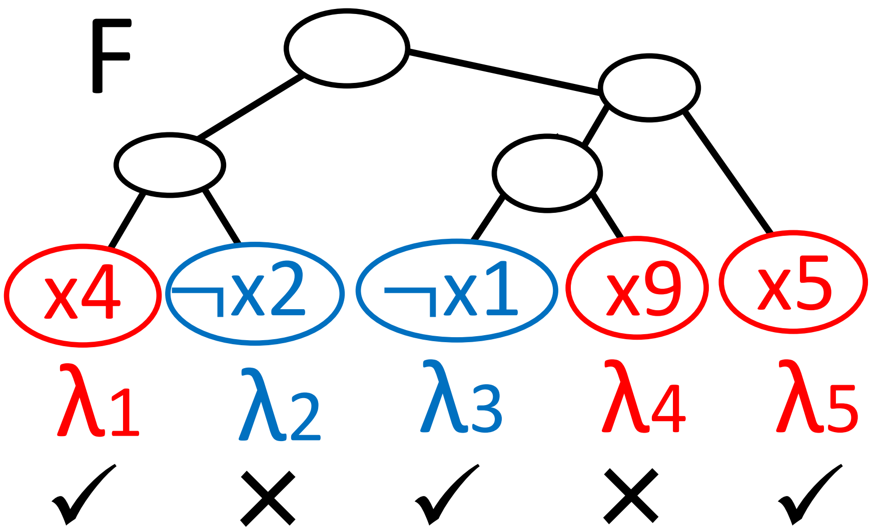
$SK_F=\{SK_{IBBE,x4}, SK_{IBR,x2}, SK_{IBR,x1}, SK_{IBBE,x5}, SK_{IBBE,x9}\}$

Non-monotonic KP-ABE from TIBBE(3)

KP-ABE.Dec(C_S,SK_F):

S={x2,x4,x5}

F



Satisfied by S?

S={x2,x4,x5}

For all satisfied leaves, compute partial decryption.

- TIBBE.Dec(C_S, $SK_{IBBE,x4}$)

  $\rightarrow e(g,g)^{s\lambda 1}$ (recall x4∈S)

- TIBBE.Dec(C_S, $SK_{IBR,x1}$)

  $\rightarrow e(g,g)^{s\lambda 3}$ (recall x1∉S)

- Also compute $e(g,g)^{s\lambda 5}$

Finally, compute K=$e(g,g)^{s\alpha}$ from {$e(g,g)^{s\lambda 1}$, $e(g,g)^{s\lambda 3}$, $e(g,g)^{s\lambda 5}$}.

Proposed Schemes and Comparison to Previous Schemes

Our Proposed Schemes

- To construct non-monotonic KP-ABE schemes, we only need to construct TIBBE schemes.
- To obtain schemes with compact parameters, we proposed various TIBBE schemes.
- While construction of TIBBE seems to be much easier/simpler than non-monotonic KP-ABE, still, it is not trivial. (In fact, constructions of TIBBE schemes would be our main contribution rather than our semi-generic conversion.)

Our First Scheme and Comparison to Previous Scheme

New TIBBE with short ciphertext → **Our conversion** → Non-monotonic KP-ABE with shortest ciphertext

Non-monotonic KP-ABE with compact ciphertext

Scheme	Ciphertext overhead (G)	Public key size (G,G_T)	Secret key size (G)	# of pairing in Dec	Assumption
[ALP11]	**3**	**(2n+2,1)**	(n+1)t	**3**	n-DBDHE
[Ours]	**2**	**(n+1,1)**	(n+1)t +t2	**2**	n-DBDHE

n=maximum size of attribute set associated with a ciphertext

t=t1+t2, t1=# of positive attribute in access policy

t2=# of negative attribute in access policy

Our Second Scheme and Comparison to Previous Scheme

Our conversion

New TIBBE from DBDH → New non-monotonic KP-ABE from DBDH

Non-monotonic KP-ABE from DBDH

Scheme	Ciphertext overhead (G)	Public key size (G,GT)	Secret key size (G)	Assumption
[OSW07]	**2n-1**	(2n+2,0)	2t1+3t2	DBDH
[Ours]	**n+1**	(n+2,1)	2t1+3t2	DBDH

n=maximum size of attribute set associated with a ciphertext

t=t1+t2, t1=# of positive attribute in access policy

t2=# of negative attribute in access policy

Unbounded KP/CP-ABE

Before going to our third and fourth scheme, we clarify what does “completely unbounded” means.

KP-ABE case

The case of CP-ABE is similar.

Ciphertext C_S for $S=\{Att1, Att2, \ldots Att\_n\}$

Secret key for Boolean formula F

$F=((Att1 \vee Att2) \wedge Att1) \vee Att2 \vee Att1$

Att1 appears 3 times.

- Is n=|S| unbounded?
- Is number of the same attribute appears in F unbouded?

Our Third Scheme and Comparison to Previous Scheme

IBBE implicit in [RW13] +
IBR proposed by [LSW10]

New unbounded TIBBE

Our conversion

First completely unbounded non-monotonic KP-ABE

Non-monotonic KP-ABE with unbounded set

Scheme	Unbounded set size for ciphertext?	Unbounded multi-use of the same attribute in F?	Security	Standard model?
[OT12]	**YES**	**No**	**Adaptive**	**YES**
[LSW10]	**YES**	**YES**	**Selective**	**No**
[Ours]	**YES**	**YES**	**Selective**	**YES**

Our Fourth Scheme and Comparison to Previous Scheme

- While our KP-ABE schemes are constructed in a modular way, construction of our fourth scheme (CP-ABE) is more direct.

Monotonic unbounded CP-ABE[RW13] → First non-monotonic completely unbounded CP-ABE

Non-monotonic CP-ABE with unbounded set

Scheme	Unbounded set size for secret key?	Unbounded multi-use of the same attribute in F?	Security
[OT12]	**YES**	**No**	**Adaptive**
[Ours]	**YES**	**YES**	**Selective**

Summary of Our Results (Again)

- Non-monotonic KP-ABE schemes
  - with shortest ciphertext length
  - from the DBDH assumption with better (space) efficiency than previous scheme [OSW07]
  - with completely unbounded attributes (for the first time)

Constructed by our new framework

- The first completely unbounded non-monotonic CP-ABE scheme