(Anonymous) Compact HIBE From Standard Assumptions

Follow-up on the best paper award winner

Somindu C. Ramanna   Palash Sarkar

Appied Statistics Unit
Indian Statistical Institute, Kolkata

Asiacrypt 2013 Rump Session

Our Results

Two HIBEs from the IBE of Jutla and Roy [Asiacrypt 2013]

- Anonymous - $\mathcal{A}$-$\mathcal{CC}$-$\mathcal{HIBE}$
- Non-anonymous - $\mathcal{CC}$-$\mathcal{HIBE}$

with

- constant size ciphertexts (3+1 group elements)
- instantiation from Type-3 pairings
- adaptive security from static standard assumptions (SXDH)
- degradation independent of depth of HIBE ($O(q)$)

which was not possible from previously known IBE schemes.

Anonymous HIBE Schemes

Scheme	[BW06]	[SKOS09]	[DCIP10]	[PL13]	[LPL13],[RS13]	$\mathcal{A}$-$\mathcal{CC}$-$\mathcal{HIBE}$
Pairing	Type-1	Composite	Composite	Type-1	Type-3	Type-3
Security	selective-id	selective-id	adaptive-id	selective-id	adaptive-id	adaptive-id
Assump.	DLin,DBDH	ℓ-wBDH*, ℓ-cDH	Subgroup Decision	h-BDHE Aug. h-DLin	LW1,LW2,DBDH [LPL13]:3-DH,XDH [RS13]:A1	XDH
Deg.	$O(1)$	$O(1)$	$O(q)$	$O(1)$	$O(q)$	$O(q)$
#pp	$(2(h^2+3h+2),1)$	$(h+6,1)$	$(h+4,1)$	$(h+6,1)$	$(3h+6,1)$	$(h+4,1)$
#msk	h^2+5h+7	$h+4$	2	4	$h+6$	$2h+6$
#cpr	$2h+5$	3	2	4	6	3
#key	$(h+3)(3h-\ell+5)$	$3(h-\ell+3)$	$2(h-\ell+2)$	$3(h-\ell+4)$	$6(h-\ell+2)$	$4(h-\ell)+10$
Enc	$(2(\ell+3)(h+2)+1,1)$	$(\ell+6,1)$	$(\ell+4,1)$	$(\ell+5,1)$	$(3(\ell+2),1)$	$(\ell+4,1)$
Dec	$2h+3$	4	2	4	6	3
KGen	$h^3+h^2(5-\ell)+$ $h(7-3\ell)-2\ell+2$	$3h-2\ell+2$	$4(h+2-3\ell)$	$(h+2(h-\ell+8))$	$6h-5\ell+12$	$2(2h-2\ell+5)$
Deleg.	$5(h+2)(h+3)+1$	$6(h-\ell)+21$	$4(h-\ell)+11$	$(4(h-\ell)+25)$	$2(h-\ell+3)$	$4(h-\ell+5)$

h: maximum depth; ℓ: length of the identity tuple; q: no. of key-extract queries; Pairing: $e:\mathbb{G}_1\times\mathbb{G}_2\rightarrow\mathbb{G}_T$; $\mathcal{PP}$ and ciphertexts in $\mathbb{G}_1$; $\mathcal{MSK}$ and keys in $\mathbb{G}_2$.

#pp $=(a,b)$: a elements of $\mathbb{G}_1$ and b elements of $\mathbb{G}_T$; Enc $=(a,b)$: a scalar multiplications (sm) in $\mathbb{G}_1$ and b exps. in $\mathbb{G}_T$; Dec: #pairings; KGen: #sm in $\mathbb{G}_2$; Deleg: #sm in $\mathbb{G}_2$.

Anonymous HIBE Schemes

Scheme	[BW06]	[SKOS09]	[DCIP10]	[PL13]	[LPL13],[RS13]	$\mathcal{A}$-$\mathcal{CC}$-$\mathcal{HIBE}$
Pairing	Type-1	Composite	Composite	Type-1	Type-3	Type-3
Security	selective-id	selective-id	adaptive-id	selective-id	adaptive-id	adaptive-id
Assump.	DLin,DBDH	ℓ-wBDH*, ℓ-cDH	Subgroup Decision	h-BDHE Aug. h-DLin	LW1,LW2,DBDH [LPL13]:3-DH,XDH [RS13]:A1	XDH
Deg.	$O(1)$	$O(1)$	$O(q)$	$O(1)$	$O(q)$	$O(q)$
#pp	$(2(h^2+3h+2),1)$	$(h+6,1)$	$(h+4,1)$	$(h+6,1)$	$(3h+6,1)$	$(h+4,1)$
#msk	h^2+5h+7	$h+4$	2	4	$h+6$	$2h+6$
#cpr	$2h+5$	3	2	4	6	3
#key	$(h+3)(3h-\ell+5)$	$3(h-\ell+3)$	$2(h-\ell+2)$	$3(h-\ell+4)$	$6(h-\ell+2)$	$4(h-\ell)+10$
Enc	$(2(\ell+3)(h+2)+1,1)$	$(\ell+6,1)$	$(\ell+4,1)$	$(\ell+5,1)$	$(3(\ell+2),1)$	$(\ell+4,1)$
Dec	$2h+3$	4	2	4	6	3
KGen	$h^3+h^2(5-\ell)+h(7-3\ell)-2\ell+2$	$3h-2\ell+2$	$4(h+2-3\ell)$	$(h+2(h-\ell+8))$	$6h-5\ell+12$	$2(2h-2\ell+5)$
Deleg.	$5(h+2)(h+3)+1$	$6(h-\ell)+21$	$4(h-\ell)+11$	$(4(h-\ell)+25)$	$2(h-\ell+3)$	$4(h-\ell+5)$

[LPL13],[RS13] anonymity comes as a by-product of dual-system proof

JR-IBE structure supports non-anonymous HIBE with dual system proof

Anonymous HIBE Schemes

Scheme	[BW06]	[SKOS09]	[DCIP10]	[PL13]	[LPL13],[RS13]	$\mathcal{A}$-$\mathcal{CC}$-$\mathcal{HIBE}$
Pairing	Type-1	Composite	Composite	Type-1	Type-3	Type-3
Security	selective-id	selective-id	adaptive-id	selective-id	adaptive-id	adaptive-id
Assump.	DLin,DBDH	ℓ-wBDH*, ℓ-cDH	Subgroup Decision	h-BDHE Aug. h-DLin	LW1,LW2,DBDH [LPL13]:3-DH,XDH [RS13]:A1	XDH
Deg.	$O(1)$	$O(1)$	$O(q)$	$O(1)$	$O(q)$	$O(q)$
#pp	$(2(h^2+3h+2),1)$	$(h+6,1)$	$(h+4,1)$	$(h+6,1)$	$(3h+6,1)$	$(h+4,1)$
#msk	h^2+5h+7	$h+4$	2	4	$h+6$	$2h+6$
#cpr	$2h+5$	3	2	4	6	3
#key	$(h+3)(3h-\ell+5)$	$3(h-\ell+3)$	$2(h-\ell+2)$	$3(h-\ell+4)$	$6(h-\ell+2)$	$4(h-\ell)+10$
Enc	$(2(\ell+3)(h+2)+1,1)$	$(\ell+6,1)$	$(\ell+4,1)$	$(\ell+5,1)$	$(3(\ell+2),1)$	$(\ell+4,1)$
Dec	$2h+3$	4	2	4	6	3
KGen	$h^3+h^2(5-\ell)+$ $h(7-3\ell)-2\ell+2$	$3h-2\ell+2$	$4(h+2-3\ell)$	$(h+2(h-\ell+8))$	$6h-5\ell+12$	$2(2h-2\ell+5)$
Deleg.	$5(h+2)(h+3)+1$	$6(h-\ell)+21$	$4(h-\ell)+11$	$(4(h-\ell)+25)$	$2(h-\ell+3)$	$4(h-\ell+5)$

[LPL13],[RS13] anonymity comes as a by-product of dual-system proof

JR-IBE structure supports non-anonymous HIBE with dual system proof

Non-Anonymous HIBE Schemes

Scheme	[BBG05]	[CS06]	[CS07]	[LW10]	$\mathcal{CC}$-$\mathcal{HIBE}$
Pairing	Type-1	Type-1	Type-1	Composite	Type-3
Security	selective-id	adaptive-id	selective^{+}-id	adaptive-id	adaptive-id
Assump.	Decision h-wBDHI	h-wDBDHI*	h-wDBDHI*	Subgroup Decision	XDH
Deg.	1	$O((kq2^{N/k})^h)$	1	$O(q)$	$O(q)$
#pp	$(h+4,0)$	$(h+3+hk,0)$	$(2h+3,1)$	$(h+3,1)$	$(3h+9,1)$
#msk	1	1	1	1	2
#cpr	2	2	3	2	3
#key	$h-\ell+2$	$(k+1)(h-\ell)+2$	$2(h-\ell+1)$	$h-\ell+2$	$2(h-\ell)+5$
Enc	$(\ell+2,1)$	(2,1)	$(\ell+2,1)$	$(\ell+2,1)$	$(\ell+4,1)$
Dec	2	2	2	2	3
KGen	$h+2$	$2(h-\ell+1)$	$2h-\ell+2$	$2h-\ell+4$	$2h+5$
Deleg.	$\ell+2$	$2(h-\ell)$	$2h-\ell+1$	$2h-\ell+6$	$2h+9$

Exact comparison with Chen and Wee [Crypto'13]
(non-anonymous) compact HIBE from n-Lin assumptions
not provided here.

~~Construction and proof present in the non-existent full version on ePrint!~~

Received a link to the full version today at 16:09.

Sizes of public parameters and ciphertexts of our scheme are better.

Exact comparison with Chen and Wee [Crypto'13]
(non-anonymous) compact HIBE from n-Lin assumptions
not provided here.

~~Construction and proof present in the non-existent full version on ePrint!~~
Received a link to the full version today at 16:09.

Sizes of public parameters and ciphertexts of our scheme are better.

Exact comparison with Chen and Wee [Crypto'13] (non-anonymous) compact HIBE from n-Lin assumptions not provided here.

~~Construction and proof present in the non-existent full version on ePrint!~~

Received a link to the full version today at 16:09.

Sizes of public parameters and ciphertexts of our scheme are better.

Thank you!