Annex A

The parameters of the curves used to evaluate pseudonym schemes are given below.

Type A curve with 80-bit security	
q	87807107996633125224377819847540498158068831994142082110286533992664756308802229570786251794226622214231558587695823174592777133673174813249251299982247 91
h	12016012264891146079388821366740534204802954401251311822919615131047207289359704531102844802183906537786776
r	730750818665451621361119245571504901405976559617
exp2	159
exp1	107
sign1	1
sign0	1

Type A curve with 112-bit security	
q	64281668699271065545675846045089716371832585795077581951745940816520735111995228283995708587050792255105234301616111004837239665293110112740293488056964951033113293850060273281618488588109896398049334323782029591683093176 408739767
h	2384339609157873306134751820831140495392565090303404669120818361178881191541989577993976654167612674196159947287344153998231273166800934286886706951 0882774498537544
r	269599466671506397946670150870196306736371444225405724810692505108 47
exp2	224
exp1	35
sign1	-1
sign0	-1

Type A curve with 256-bit security	
q	80477448366498626627730507464021637336124634683801246181920151241143165122191764972422562122902105109381871159288731078968859492885124399227292766992278054025538611391817192988941635118968108268829119774472261364638045245590200831401326615832304786321654257810695477806919881767771968656140813620968166853674603032593809530306050997045589459089905386951772664027934087548061163327483592785971547494600549795910844104683407425574991012188873785290926221288633491
h	12004564621898365013579742488258666710576254341078563159263516323674440794276343522589134546161200473870383445772271311195366872248000933639550099512775712233396187378282905612262188879398381921387957832062552381048218421207870648015042755757978638067114278875243057663162449432842296661648354721508946441364
r	67039039649712985497870124991029230637396829102961966888703246700045656553663535752256153575418625319344425401730311918581658203090958471733086728507883 53
exp2	511
exp1	322
sign1	1
sign0	1

Type D curve with 80-bit security	
q	625852803282871856053922297323874661378036491717
n	625852803282871856053923088432465995634661283063
h	3
r	208617601094290618684641029477488665211553761021
a	581595782028432961150765424293919699975513269268
b	517921465817243828776542439081147840953753552322
k	6
nk	600942903564084071309841611273100785163600318684179682629928648096235072698338546784140467798178448537570268587749663314341982575124579932932718490436646551464432290290694633920468378302679942227891600473374320752666190826576403649864154357462944981405898448326660824346585325892115256960
hk	13808017118622124844032056990052421415416297614338991492364052325289569968546552610753036616919952730806207622872760513614465285046332831522788311837113013297655914506802500005924376129732690560
Coeff0	472731500571015189154958232321864199355792223347
Coeff1	352243926696145937581894994871017455453604730246
Coeff2	289113341693870057212775990719504267185772707305
nqr	43121144143658956838208886528859234719486618965 2

Type D curve with 112-bit security	
q	150287996139850344657555064507715652292828322178603901559964838400 17
n	150287996139850344657555064507715613525832547441255206392965411950 21
h	1
r	150287996139850344657555064507715613525832547441255206392965411950 21
a	187122416362466663186009248912893905994497834714229217732382564209 6
b	979550172334338054714415200677665314930646613801273064011412560570 1
k	6
nk	115224746950252173700626030137909803345380964294556891142220249121844323192283932046503836617818648060762472595563783505416699943448784301362027149457614883858906199255534576681585042027865805599709459366576368553467135988880675162146348593305546345057671984158571504793459447217103562740477075361562962155734127637351356009538654190003989202925352157572915393075256396752045979389195048074272387358115 20
hk	510149159366842656049004871952561608481935712442746488553324756616583045063163010061128871727734501086401298812782965544925642487102450036859798946237381306218927415091655268926285260325401124850235604120654426275548177913739804037628154293851397047399078706461573472 0
Coeff0	119751892582596971662570378252275369314467079446824709511118594461 92
Coeff1	134330422003479348277427380952495468040066875620882540574119013627 71
Coeff2	832746452111779123807910517544812200675986362550804349577088741161 4
nqr	142721363302176037340346936780070353538541593770301992936740616924

Type F curve with 256-bit security	
q	188547299014817771712759726537269730474415355546647880395890487872082914934944783539252890048632830171890426925443664517556671889339241319051547545874597 3
r	188547299014817771712759726537269730474415355546647880395890487872082914934940441335906490691304446259952601128676826394585569176160792691155333451301538 9
b	691856937939602243555669447664477542973613560793691163855823144649878288235571480468962030247960181456095787396968599383128460432460279344240854542563044
beta	186623412973836753825504265326834062418450263341414112970563431973758771989677565403104865067258670316386292795543837938465615076630402325066635760600324 7
alpha0	131403635643987457902521839041906182865932385624119552050075393199683231848438720809620977159261391640806601878430698555080809858394830349362984674407823
alpha1	106983010987558641998585998685937874843526441374061775889326740694348671473656779730435906713486331857906577140245150092618396276079088716615519188095859 5

Annex B

Size of group elements							
	Elliptic Curve	Security level (bit)	Size of group elements (Byte)				
			Z_r	G_1	G_1^*	G_2	G_T
Symmetric pairings	a.param	80	20	128	65	128	128
	a224-768.param	112	28	192	97	192	192
	a512-1536.param	256	64	384	193	384	384
Asymmetric pairings	d159.param	80	20	40	21	120	120
	d224.param	112	28	56	29	168	168
	f512.param	256	64	128	65	256	768

G_1^* represents the elements in G_1 after compression.

Annex C

Evaluation of group operations on PC platform						
	Symmetric (ms)			Asymmetric (ms)		
Operations \ Security level	80-bit	112-bit	256-bit	80-bit	112-bit	256-bit
mul(G_1)	0.005	0.008	0.018	0.002	0.002	0.005
mul(G_2)	0.01	0.016	0.036	0.017	0.02	0.013
mul(G_T)	0.011	0.017	0.04	0.021	0.025	0.041
exp(G_1)	1.084	2.388	12.498	0.405	0.739	3.404
exp(G_2)	2.167	4.749	24.953	3.647	6.126	9.215
pairing	0.777	2.153	15.743	2.492	4.2	78.001

Annex D

We compare the computation costs for signing and verifying in terms of the number of operations for each scheme. We apply some algorithm-level optimisation, e.g., Hwang et al. (2015), to reduce the number of pairings in signing and verification. More specifically, signing algorithms in Zhang and Xu (2012), Boneh and Shacham (2004) and Emura and Hayashi (2014) are optimised to be pairing-free where pairings are precomputed and reused when signing another signature. Pairings in verifications in Boneh and Shacham (2004), Emura and Hayashi (2014) are merged as much as possible to reduce the number of pairing operations.

Number of operations for each signature scheme			
			Operations
Public-key schemes	ECDSA	Sign	1 exp(G_1)
		Verify	2 exp(G_1) + 1 mul(G_1)
	Schnorr	Sign	1 exp(G_1)
		Verify	2 exp(G_1) + 1 mul(G_1)
Identitybased signatures	(Cha & Cheon, 2002)	Sign	2 exp(G_1)
		Verify	1 exp(G_1) + 1 mul(G_1) + 2 pairing
	(Hess, 2003)	Sign	2 exp(G_1) + 1 mul(G_1) + 1 pairing
		Verify	1 exp(G_1) + 1 mul(G_T) + 2 pairing
	(Zhang & Xu, 2012)	Sign	8 exp(G_1) + 2 exp(G_T)
		Verify	5 exp(G_1) + 4 mul(G_1) + 3 mul(GT) + 5 *pairing*
Group signatures	(Boneh, et al., 2004)	Sign	9 exp(G_1) + 3 exp(G_T) + 3 mul(G_1) + 2 mul(GT)
		Verify	13 exp(G_1) + 7 mul(G_1) + 1 mul(GT) + 2 *pairing*
	(Emura & Hayashi, 2014)	Sign	2 exp(G_1) + 4 exp(G_T) + 1 mul(G_1) + 2 mul(GT)
		Verify	8exp(G_1) + 4 mul(G_1) + 2 mul(GT) + 4 *pairing*