U-Prove Recommended Parameters Profile V1.1

Revision 3

Microsoft Corporation

Author: Christian Paquin

March 2023

Summary

This document defines recommended group descriptions and generator values for use in the U-Prove cryptographic protocols defined in [UPCS].

Contents

1 Introduction

The Issuer parameters defined in U-Prove Cryptographic Specification V1.1 [UPCS] contain a group description $\mathrm{desc}(G_q)$ and Issuer generators $(g_1, \ldots, g_n, g_t)$. When a Device is used, a device generator g_d is also needed. These values can be shared by many Issuers; however, it is desirable to have proof that these values have been generated at random.

This document defines recommended values for different key sizes and up to 50 Issuer generators for the elliptic curve group construction.

Each recommended set of parameters is identified by a OID name that can be referenced by implementations.

2 Elliptic curve construction parameters

The following sections define recommended group descriptions $(p, a, b, g, q, 1)$, Issuer generators $(g_1, \ldots, g_{50}, g_t)$, and Device generator g_d for the elliptic curve construction variant of the protocols and for different key sizes. Supported elliptic curves are prime curves “P-256”, “P-384”, and “P-521” defined in [FIPS186-3].

The Issuer generators $(g_1, \ldots, g_{50}, g_t)$, and Device generator g_d were generated using the procedure defined in Figure 7 of [UPCS], using the corresponding curve and SHA-256 as the hash algorithm. The input parameter *context* is the UTF8 representation of the concatenation of the string “U-Prove Recommended Parameters Profile” with the associate curve name (“P-256”, “P-384”, or “P-521”), and the input parameter *index* depends on the generator, as illustrated by the following table.

Generator	Index
g_i for $1 \leq i \leq 20$	i
g_t	255
g_d	254

2.1 P-256

2.1.1 Naming

The set of P-256 parameters are referred to as OID: “1.3.6.1.4.1.311.75.1.2.1”.

2.1.2 Group description

These parameters come from the P-256 curve defined in [FIPS186-3].

p	`ffffffff00000001000000000000000000000000ffffffffffffffffffffffff`
a	`ffffffff00000001000000000000000000000000fffffffffffffffffffffffc`
b	`5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b`
$g.x$	`6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296`
$g.y$	`4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5`
q	`ffffffff00000000ffffffffffffffffbce6faada7179e84f3b9cac2fc632551`
h	`1`

2.1.3 Issuer generators

g_1	x	`f1b986d5d11f43483ae736e886af750e870d7f0c2312aad8db5c8a3e34f5391e`
	y	`64347b7f493187a53b370894b8f8e38fd22cb99302393d79dce225918eba61ee`
g_2	x	`1554cf983e0b060c78705ed7d14a4941b02e608cdb78f6a75a52345978141fd3`
	y	`62540e690c8fa9fe107e2141dfc6907f74f5feebdf5b12d7153b4635a2df6a76`
g_3	x	`32791a779e9aa475ba2666a0e47a928b21ab1905faaf48bb8062bae9009eb27d`
	y	`1874ba86ea194fb14dcce9fa22366f4735caea2119beb63f2baec19a9e93a545`
g_4	x	`c0efadb5c3015e42c1d71ac390c4d22a6f5d552f63bbcc59190aea6aee16354a`
	y	`53f0133ea44da20c509a4e5be9b027dbe13e3a60439dbe72084b0c75a049723f`

g_5	x	bd5f29df6640493ff96c6cbc49cb8e5f61462792db75f20ef49bf86e260dc955
	y	204c440ef8c6eb2bec0c343ace9c6d64e188c8b4f0613d64846adbdc3d8fdfad
g_6	x	d91abda26ec5c3001cf1ca2c09ad88662558426dc3b4d1b501e7abc2db080cdc
	y	54ebb17fed855a36c1f74ab8256208e86307a9f2b756d7c84b4fb9485e0ff5f5
g_7	x	86eb2c94e2b6d620a391b4080dfe2b377cc20d981b5bc0cca94e865697959ebe
	y	26ac1589c52880c3b8f81d2bf32976636019f16d8efa1f4d20950b9908ceb7e1
g_8	x	5553148e44252692d9e7ea9c189469dd2c0e8bd449405b6f3b1f279245b37f0d
	y	790ca4ce90e048a7425b662a631612d0224f208e4be6e907c3e7d9607a997f6d
g_9	x	77668d97bff7d5da695d6d72e4f840205de289ce8ff1e9952435b0b4dd4e222e
	y	1476060b33fe636bb9b75f10785d4b431905cd006f832bf73103b9f880378556
g_{10}	x	729a72be8375888f67df96d2a52e1b384af1c68ff8b73cadf6296c72c2c1fab2
	y	13120e6942d0740a25f8b871e1f2fe9a8604977d1daa18af0e4fed570c6ea2e
g_{11}	x	cfba014ef2734bb0d51863a1e6ae8eb4ae189f8c19432af46d9f16fdd43fbc18
	y	1256c784f827c31ad23d8d233678ce2eebce344629e7a5f7a6d94adc0ff47a7e
g_{12}	x	6c1407c49a51f67625eb8b2995ac11944288995b3a81789a5eb3e6bf4f2ded78
	y	16d872494fc18d77404f906e58902150e1fcdda0cf211516f6f19415e8892f26
g_{13}	x	d9231c315baf722469f74fba55ba661777e91ca6320a8825bda1cbf0ea206092
	y	36e4cd1288088deceea8e7b6d22cfd97b99f87facc95f1891fc6a28bd81e5f50
g_{14}	x	35358711384106b862a2cf0b403e8055920c7598bfb49987a89c3569e5a05b61
	y	18edfa1dfc653a0574ca88fdaaecdfe9eb75309aacbe926c2110e92678c84e3d
g_{15}	x	25d05c261772166c08483d00003f443520e91324cbe918fc34008a932716d7eb
	y	668a13c5d163f6646bf2e8f42d1f48e79a9ead020922b383006b676d29d35a42
g_{16}	x	fc035c85aa0e9c527ea7dca26a2db74dc250e8a5abe853bbded15959d7230f43
	y	65f052a382b2c78caa9fcfc952096f4ccc4772546e5798649123fef94ec95acc
g_{17}	x	85b3873fd911bf06a978fa40e261e1c856f638ca9ec8cbe8826a6082c8452d0f
	y	3cf00d69586f56bed849d5e9e2825a003ce562aab5f81bd718a4e941989e1101
g_{18}	x	4549f8c621eaba57ed2336d51920f6fc4dc34e047db134c61980e4e358c5e324
	y	39e8be23f04033a0f8bc43d5a11b1e798d25b5c75d740efd309985edc5dedb98
g_{19}	x	b8ad386b54f9766e5cb1a2f050cbca2a22619ba008fdf9496df38a6cea784eb2
	y	5b333a0cde9ddc8d6571b1cac456a47144c9c16ece866a538494ea0feaeef0ac
g_{20}	x	56628c7d6366e1c4a9361e5f7e49415c80fda14c04f106f0638ec8cf59aa0485
	y	74fdc260802b6df55a640233889535cd04e0df84b66d9da4645da31193995046
g_{21}	x	8f1f5a0e342e6557b955355438608db09e4d237ec7230e2c836bd5f3e91c6c12
	y	2c1a2102a69ef74a006353c2d2d1dd9dbdfab007fd08e7c88eb869a0a669b1

g_{22}	x	beaf7757a3ce43dc8d4a0732e1e318f49755e61e5f57a85beccf21b7dcc818e2
	y	40d26c2adc3f41d09156025a9dc34fd3ca6b96809d3d7cf5f28d00a1edbd6995
g_{23}	x	e513c3e50efa4436199c5a51fd691ea4dcabbc202a8029ba3df0336f12d82663
	y	75f42f58480d2cad569b0f13cbf376c3913271d9f7844242b870519d2be8398e
g_{24}	x	b42b3b05bcafbb72800ee242ab4cb7abd77f1fceac7ce1d327eec25b3de6c43d
	y	725f5b3d0cdd1b86bd7a8bd635c1acedbac91d6c35163eae66810751f4d46288
g_{25}	x	c8a4a7df6bef6c61ef50bffd9cfa7efde22530f0b2d0371e819b80e885d592dd
	y	196e7e0a81d03b38a8f99104812f64784b62d41991f566de27847b6bb9baa251
g_{26}	x	a22af45e5a7a9a9f94910e8cdb5e649e83c38fc1369f1ca9fa1d51887c38ddf1
	y	759bd38c6e09fe2cd75b4f355f4420e2e7b2dfd9f7147aa03d5373b3612b8389
g_{27}	x	22f47a6aaec142359481eea49098882b3ecac4625b1d2562b0271848762c5dde
	y	3e0b7e0c51a063303580ca25e326ae7e61086ea6e4c495d25162867039d9fe4c
g_{28}	x	eae24e9cbf4a8eb92c1cc80d75dcf44c39dfe4edcf13c3e5e4b7ba08c329378d
	y	2f7ffffa43a2d0268c25e4f08663fef26c57962fd5f623292f061ea19c5710a1
g_{29}	x	ad92b098528ae208572474e3ca2b1f6fbe133cb4fab5eeba0e46100c684d5bbc
	y	47978685fa8f41ca5246bd6347ba65f670ec65a136166c75e7936346e16ad790
g_{30}	x	dc5abc9d9e2a04a7ba38346e827119f50fa311b8cb4b12cf53602f3482a609c0
	y	e94f73d5d9641942188fd0ff64a7751021faf6cc9c4d2aa0318e94f05978be
g_{31}	x	5d008b9bdebb3824935bdc68a7ac426c554058a9dc4ed8bea2ea74a92df47fc3
	y	1805d5f8f097ea8b3b8608dc5f016fd909781b75900d53ce8b65846518ca0bda
g_{32}	x	4bff16067e37798ff3e3242b11be39f83dd7451ebe1101eac4887a6f93d50206
	y	65e5e31e150136036e1922549b9fd9a855997129f4566d3f5acf8a1e4d0ac83
g_{33}	x	aecba7f0745123d9c6a60e9bd461a8636131b095f59617849d335d2a7d8b187b
	y	5f62d5eaf4a9a892488c0de95d8d85eda9035b6597ea2674d7a7ee7d4a535ebd
g_{34}	x	a74ecb80732496e8f6ce72f4556937c237e19efac7567c151f386b650656a226
	y	4f661415313284d904485e6f6db8fe94782b2ba24c0cba6ca77557efcd8f05e
g_{35}	x	ed0e965669017aa71f342ec8a099bbf01a0b9eab94f62623ecf96bcc0e14e4ab
	y	244bf125523ef2978db06006cda7cf3e4d58397711d92897603dbae29b82864b
g_{36}	x	69b843bdbf017d416a767d134e1c2d497fad2cdaae36b275370ff512a34bfa7
	y	3d3be3d2e86eb07a87849b2ef16ee30310b86e63b3478163fd06b6592bbde545
g_{37}	x	592d48158a6358a2900d453d79e88d6bc20b7fa8cb2bfcfcdfd082960525ad83
	y	7231c3d1f86fcc1b6c9e8c16ae45a93508c9c49e8a745e64b07636fc6b03103f
g_{38}	x	18ffac7507b8f022eba9722aea93c6ca7470825a787c1f982b083dda0490ed32
	y	304b83604a94ff8a2787b047e823e50a64edca0b1dccb9381196597a1c63b362

g_{39}	x	dde5dfc2867a61ba2e046dd52576d3d33a24173e32d716caf0d6bc4bd1194374
	y	79b6e30b1822d61eade59b0ab3edbe8f4291c8e081ddcedeff00bc32ebfc1a93
g_{40}	x	e0f72a8c71395e19063b0e09f947f86c06f4b300c81d3bbbc48dcb219ab960aa
	y	6f231e0a538c8f54c066c93e1af857bc3b1c418802274cbdf5e387d88736f576
g_{41}	x	385388078ea2b4792dac8fbe0b4748b99800ca086662fa8eabd62596dd7e5c53
	y	4d2112111d5bf47baed1c4a2688cfa616e7bbb64d412f16b371288bfe957ea61
g_{42}	x	b108aa3e8bf1f707f6ba9556aa0f1871519734a698203f7532925443b2020cbd
	y	5a75fae7ad0be23520734779ef11f325dde7a6edc63336ef9fb58661fccc46a5
g_{43}	x	605b3505f77e74b22ea7e67c3333ff3b7b771738389d305aa594d8f550237db
	y	7487adb2e07c3ab92e1386546790a011497eb9fb9846716b04793dcea430c7ab
g_{44}	x	d81883a9cf1dc3043c44f9f0f9ff502cd045e4294c375a30a8a65abc0dd28264
	y	1d75c99eb44e2d8b43a53f69b6881f96929435e2b3850a3701aed026e80a3291
g_{45}	x	93ec90879cd2d86a2276f44b42df736283d297470759de0af2c6c92f168482af
	y	1f45f480a0ec7607516679c2bb9f677a89d450ec469ac930a10d213c1eb2a9cf
g_{46}	x	4e9e9eb8e267c0d61760ecabc9ac19ddac5db95c28334ec99d49d74d40b66daf
	y	5dd71c92d311ec15d5e2e6d3b8d51336415a608e14048c86ceec764e6de6df49
g_{47}	x	ceb4ca98f62019596b9bc6234ea5c2029990f08d068f27eef4fa7d9897bfaf62
	y	4160fbddaf2986f3a11e29b589b9d91d8b15c5f8bbf02f7f175f6ef8e7c2b1a4
g_{48}	x	80e8706709bd25a84937417e2d6a6dafa83d3738dfb42f8eefa0fb5247d69985
	y	6a8f2ea6b2301e3aefbd8246f6eb97ea0ce1155ce0b72c471d01b0d0b88da2ca
g_{49}	x	13bd26060667f8eb7e56e782854af3b3e010cf1825a684bc72b287ea7b2c234c
	y	1871c15aa6f8cc3ada2d4bf6bb2bc6296ca6587c122df3b47a9faa3025863a8c
g_{50}	x	7d5e69bace920e8ed2d0b43ad14849d71e26729cb37f009ae14e6d8a065e9079
	y	13d6c8d6ae0273a1890129779fce34f0caf6f353bfde9ee337278678c9b6e758
g_t	x	e2ab81def593e999c975a8a48668b9a07e5594cfd68fac29f17a811cb26b3e10
	y	756311f896c503ecdb2f608a1ccbfa378a95eb4578e65f190f1a8b544d20b082

2.1.4 Device generators

g_d	x	4ca625118d0a05d04d275dae1ff096361ebeba345c31270982f796639b1ca574
	y	142d150c855ba9aa7dcc71821a538edb544836df8050912679ccd7233fbba636

2.2 P-384

2.2.1 Naming

The set of P-384 parameters are referred to as OID: “1.3.6.1.4.1.311.75.1.2.2”.

2.2.2 Group description

These parameters come from the P-384 curve defined in [FIPS186-3].

p	`ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffeffffffff0000000000000000ffffffff`
a	`ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffeffffffff0000000000000000fffffffc`
b	`b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef`
$g.x$	`aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7`
$g.y$	`3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f`
q	`ffffffffffffffffffffffffffffffffffffffffffffffffc7634d81f4372ddf581a0db248b0a77aecec196accc52973`
h	`1`

2.2.3 Issuer generators

g_1	x	`4aae579dd56d78090b9921f31bf729f074121a3adffa2d31d01215beee1dc4df9df463fd5e2b8f6c6b0a4216258ac844`
	y	`3c3b8a23c5d66aa2f0964521190a9281451e9ae3ace4b7376e02d7b3949e2274e8448cadef7e51991720b49a45b05805`
g_2	x	`32f086eac7beb55a0c95e5ad996e39dde74b3b66dfbc2b8f12529d9df4a2cb84aa54ce69ab1fb22cd7fd79967d261c2`
	y	`16bbf078654e391680bdb57495018cc8fe05130abfdaa84ab4af90d0d2d6c01ffda8bc96cfcb0016f3db13d80ae8a2d0`
g_3	x	`d6583afe48311bec5c9016682531c935cf3fa98e33d503354820c99fb2e902eacdb419441203e287b0d33adbbe912e33`
	y	`7f9e35c0c0daf2e68ed135ebc07971d58e0e6ac8da69f54f0c093e24dd3f62751e816b6f6e1fcb66226c4f0b35f9acdc`
g_4	x	`3ef851b6e0a84e24fc999b053cf6acf32adc941784aef0de14823ef7abbe7e7e49e7d80cd35295eadf332265d4da165f`
	y	`182899d34652626c7474989366b1f17ad4d9c812863a67bcdf7d85c0ed59cb7320663ebb8fff3d5f5632e0a75e009966`
g_5	x	`b8344031a958a374de8ee0711c15554404bfedca80e4889922bdb0cebad3a30c922f5492d2ce4884ba1c77b572fa0bd`
	y	`d7d707cec2ecbced76f32d43ce7b55cbd53273f55605b7b9bac8b3f521bb1539686967be18b5aa41a7165f726ab5dbb`
g_6	x	`d8651982f1cfab267270219aee250736d535c289a38c885df28eebf60f763a12a16620acc595697308eed1db05acd4f0`
	y	`2fc43a11b828c8546ab8c1c6aeb41a6857c481590417b659ac8bd3ee53c70fd3f7aa13f06570168823affce84a5e861d`

g_7	x	e42bc176e13bdecf2b316018a22cf95102b71a1fa8ac1cfe14eec54cad256a9ab9b4a7a8ef3cfde3384fe4a1bc11c2f4
	y	4e26002735c92697877057256038e7934c1d428126f41e771b190840dbac0f59bd5e07022522b638a2933e146339dcc6
g_8	x	d71410b3e3a222aafb7f53ed4cd8299e442731203becf643ef81da371d8142191cf25a27019587294d23870c78fca049
	y	5dc9800ad0eda033abe134ddd894f296b5aebd4458ee4254ce70f84dfb0de18fca99bf795ca7e208182ef6c46d7bd494
g_9	x	68872b164a6e9b8f99668b5bfd4ac0770dea64e37732a384bc39c32484b86091cd47ddeae526b18065e8663e1ecb8b80
	y	66608aa7cf0ab53c375034dde39736dc81d6831bc6ee78c714e010afa5c85425a7ed28ef6f462aeb4d7952eaf488d0c1
g_{10}	x	a04decc7e9f0cf88930ab26c96d6952376b4c3a3db75256efdd466f51f7c01841a5f4e6a9f11877ff286cbc74306bbf1
	y	18c80928ac2082c04f300d31b2e6d00ee687725eb86f0dc7c7a8fb95993ceaca8afce480edc727842efed148882dbaa6
g_{11}	x	e9802ce5361dd79eb14f004d1e2a7dab4ca55862b937593c86035fce0d3a49c1a1347e9d89e9348bf8460fe64668aae7
	y	29992900811b12c42efde123cf65b80bb249e48e3f53e44775cb1b36536e286b23e08d4c59f50ddd89b9db4e012a4f14
g_{12}	x	8537b29a8b60c67394d30378db590fc704ff363a6c7901ee29bb8b183fdc8b0aead5f438e44384d41ed5f26be6a4c7e7
	y	75c3be295e38813b2722bcfcbad491c62bd81a1438864d8f54a48a438a6a556c5cc6bd9549c25ce7e39d9861a30b6e08
g_{13}	x	e46be8ffb1a61277574b4d4e7520bb28df1aa92b75390bf6aa819884a47db67e0a5a3f754cef6dc57d0725c796806d85
	y	1e0cfbc5092582f702002fac85dd2f32ef568e009801c3d79611aa3aa0eebf2d559101144512fb2c1a597f3f0b05f543
g_{14}	x	f6d6df3c867b886a4bd37756056e72009d2e264cb25ddd59c0b83d4d0e40144f649f4357d416a1772f7a1e4e2bddab15
	y	6d9b50e848246f310b92f01835d53dbee8e27f883aa6d2549e527fe7808a9cb61923175a8eecd3328574a3ed7bb59ba
g_{15}	x	388a6cb55c5d08bcead8211cfd20e32c78eb6f06d792101a00c0d757480046f9c4aa5df882176bbc8d831f72814a790c
	y	427b8985182f9036019d28325619b9ca944275082bd2fd198500c17c9bb8ae7d591efd64e18070c4cf3164e0926dfdcd
g_{16}	x	f30fbeec912971dbaad5ed633b5b2a376ae60e2786af169695af00f6da9bbcfd9a43564097c90225c54e2a63b9c0004f
	y	31feb5903cb5679fe9686f17303e8bcf8335fa07f6fde06b7062e2d337f72c7aa1adee5fbf5cb3742844f07e02fd476d
g_{17}	x	bc56187e62b3a3c246df01d8f885c34d54ff81424abd1d227b033f06eccec6278dc0759a16d90f0cc51616c50e9a8845

	y	3a532cd74d1f73dc02befd8b002db362eb133b3d9ccec54529f15d7302da1d8b4c7b36654e4f8d2a3e4da5eb9b29a7e2
g_{18}	x	899772126f9838ec178961507caed8258b6f102f5a7708babf80dd1dccdc70021e4f41c2f7438beb67c9a2a9b4d57f84
	y	71b9a6fdb91ebd0a292bdb718377308ededa063d07cb034e1bc86ea2f65fa20f0935c6c8c378caeefe64ddbb3adc79ed
g_{19}	x	cb2ebf807f1e6fe411df6898cdf652cbb9bddf3947355011429d111bb2618dc46defca469a09c19748cf1d09aa8219be
	y	50238a8b2707cdb88c381d57369b4d7838d7895876f9a3d80a9556a5c797a4d0db8399fcd657add1938b65c7afad8a72
g_{20}	x	95fa795aa4f4c0da486420fa941b25d7f70c8073b78bcd8820d8146689d81e1dc2a4098e86afc27b49c86aefed1b0d61
	y	623d37c13dcb6ea9573372888af08beacf94c8dffc2cb615030ae612b0cf1478751dc3b56a66a51db4b98e264eb016dd
g_{21}	x	22f433020dc129c7be74558ef9c291f3938e7817b47d4b41a59221d85b10ffd1b815919fb3717e3e7e15e93fb97f6f7c
	y	14454cae0eeccbcc8e521555fd2ec822c290c464671ea7aa99d558909fdcccf68e4d7095c4647a16e47f16c0b68851c1
g_{22}	x	456982b235d9d013c99b64094d4129631fb1c6210628505c744133e6fa175d141fb4c00105f810284c6880b46a4406df
	y	52b8498256516a4fefde13b5a7bbd72d3f19aa00b3626decdd9cd1ff7d175cf744e22416f351f62e5d01be651ca82747
g_{23}	x	451f77cbcf22bee6a407287ef9a36f293fa822f395f64c2edccb9ab5f8ee3fde86efddcf3302e8e9293732a058332816
	y	773401a10fe5069dbcc6870ceb8b15d1cb35227bd8af7d70b63d36e95613deba2d6003835027493c04630edb2700b965
g_{24}	x	a4ad50b7dbcfcdc427e72f850a1bb040281c5f99b914151c47ac48f9fb7b85a05858f303588c57d2ff66b5867145fbdb
	y	a564336b5e37aac39baa0878c6c50d3d36f5409f102f9b8687328094562ca6288b2b69fee43891ad561d32ed4bb20f8
g_{25}	x	f1b4f132b3c29a9e3467a0220817f2587843e77543e812ec524d7d413c6c20c03ec39b55836220717ddd9af42affe667
	y	3447a1342d40a8c094060345102e64b1b3871b80ef28d32770f849b57e7696118f596b8b119babdd2d7ccf27b55acd17
g_{26}	x	970279c58147dd40d2aafebce3e0bc13ee4ddbb746909cce2849bed98d8b7b36ed971a17a8e75cdb5f3ebdc3e71b47b
	y	2cc17acda096b56393de63c66b2342a03e2e504f12398001b8d90fe1581d2696bf8643465854e0d9ade9ee2145f3c02f
g_{27}	x	2b5e17c219e4ea95af39b24a20dc4d5086707ed8066bd298e3047d6459823ff102ef617d4670d59e0efb965e179b01a6
	y	242023567c670bcf21c9c2ef69bb8b87d7a8dcd034b66606900812393ee9989bc37e25ab672a3ea4ef3b028f83495623

g_{28}	x	81fe66dc8e7c583ed15244b5d7ec869725bc35346ff3063e6a22483e92d6708b598f41e4261d4c52c81fd703853c0b5d
	y	23f75a94e5f864850697619cabb8b34eff569f29d88275b7a7ae1d77809e3a5a425c82b5bdb8d7aa75f95c53a37cf960
g_{29}	x	46e4d4bc6281d4943e0b5cead86eb8f5821bffd42888b579db7171c82416bcf863187d868155b4a0ae1f3e44cf7107af
	y	1464246c54ca3a8b70da3da93ffd8866336e7abada509d39276d085a9c9dd55c04ffdef0c5ec06983aab0e63fc1186fd
g_{30}	x	e3d327377144a406ff2d22fb26ca634d6a8a0ee4bb39aad0b35e6636accccaf20aca78fc1a02cc604805333034078ef8
	y	47ec98d318f871cb6fe491bfdaf261d862ac92ea5d269b941875e636dc5ce2cc7466908a60af479aa2c70f94ba0ad303
g_{31}	x	bd425497219e2bca3b47629b19f79d4dcb276284b45c3f5ac9b47b76b90ece9235655cf957f77ada902dd175e494da91
	y	2980e0c8d44a32345211554bf1b7ac1edef0c5cc1a60d42ad4e19e9b9aaae4cf1fbca9eb01e132df66f89857b9303008
g_{32}	x	2a6c576df2af7b1405daade9fb24bbfeb3fa9c5586036088e07d9dbd3155e9a96922aee185f731579c7d8cd1a7a344e4
	y	44916fe5da07e5adfef1837d5d3fc2aeddd5b05b9cd9d40715fea44211486d82ce95a27296b5ab3a901f63d501f2b1f7
g_{33}	x	e7e5b42c722fb47bd92ca581c05aa00f1c18c0ff654939f19cccb6ed3c4df9f7b0a03bb495c44cbbbce93f4895882637
	y	3092e32af39c40c24b5a11100be810329f05016f792faf50876f77f4f561f18766b01da44fb2e54e84946f2a3c9670b0
g_{34}	x	a6959a68a6da7a468d0eef827492d3888af2811d0627c18aa909dd0ae4b020d133e48b911b377e05ccb77feeea326673
	y	70edeb467c18d159474824dfbe59429b4fadc97cfe3f84986307b4ba50faf2c4b60d73f2b395b595bb6ecdd96a4fe3e9
g_{35}	x	9938127c58ef9efe69cc43ad758b3af23bffde84f7182f090095e118834b67087ee706b46440323889253a223ecfc865
	y	37f1c9424f0860e3ece2f8107800f6d86c909a9f44679c3557eceb4b5814b4b396bc8e9a9a78bbeab7c1313f0a4be318
g_{36}	x	60eae169e138df4979ded509baceed03e6344910d36135ea6653eff55c076cfb54c1ee9bc0b5e8129c929fda643e82d9
	y	65210212ca8521a0f9022063c3d81634a1b4649b02651987fce2a85e3faea6035bbfa25e4de47695d7ef0be7c65529f4
g_{37}	x	ab09b0485bd7eae24bf82acaf48cb3848a841fe3826ca2bfd91d2afedfbeef07a91d1d35b7c422445315d74666a2dc5b
	y	6be91029fed90132982e34f581b85cba8d699062b76578808693f134f203fa866a1fb2fafc8777292bb5c62c130a9410
g_{38}	x	ebca9a02482d7455d0e6af492e611efc908c1fb851b58f331b2ab087a2d9b648f30f3f65533f4c550975beb9168b0849

	y	685df7b2c2757a5b5ba93d91286388f657b89bd12e36c8de9c95818aa4fd357b4c14df72a2bc4136fd9476160aaf651c
g_{39}	x	dab79fea35a2883a43c02852d28dc8b7a02d5f331cf1a5b961aa2b39a036756bfc80f51f945714209b0be881bb82c1b6
	y	4c2d063d405b4569aa6dc92926e3fb363b3fec762d0c6f0db267073cfe3f78baa2b8cb5d7000bc8fdb281ff148e62676
g_{40}	x	2ea5925eede0696e05b575d1ca4466b1a74490fc91d21261257e06c6c5d8d958dc1b34a3c2d14607edbc15199ee36e73
	y	768db9ae8de6a9d51b7325f17471ed6422b8977fbdfefefdeb0d5eb2879cf5b99de7a06beef35d4d4b471e3dae96ae94
g_{41}	x	5fc27113e10eb415118806869490569e9a42d4e3ceb227d8936dcea27cadb16a86fe6c116e60751afc5354f29f9824dd
	y	1c7e890ea76ecafe28b6545a2005b5df5fc23918aa6d4c81f968108ff565fbee01882dee44b23fb42427d8945f49f6f4
g_{42}	x	19f736915014c121612ff0fbaa4479edba30840736d00f18d9c08cfe1770aee912b516f82a71f17625bc10d56ea75586
	y	1a5a311894e90d019fa154c68907068d1a2907e33fd683614fa02ce9e22d4cf40f9cb70ffa74388341e90635a2e260f4
g_{43}	x	29763735c7f56bf6bd7a1b6a1f2f87bc7cd48592270af465970531d6d9fa9a299c4073c2ef5ed3f9605c7dd433b208bc
	y	7484ff6532c7fb294ed4774a629aa2ebafd02b916ecd9184c134c739cd2a592a40984cd21a61c880067eef2c960b23a2
g_{44}	x	82ded039577f4e1db38722200adc9deee477c892948432ea0382f3d314dccbb8944718fbbf92c31a89a8c10daa778ab0
	y	25810280fcf2809fb8e46ea5f75f9c8cd4ae3e560aafb5a0fe8bce7d8ac2811e713fdfca7c2814841e64adc32bfb662d
g_{45}	x	1b41502ecd20817d3c85e7004e669638c725d1158aa803d105abbf85955185598bd316fbbc1e9da4b0ab467e34172d41
	y	e3708f721dc69f92af811776fb1e2480251b204f5b1cdf4adaaed66b0698bd9fa66623c5bf056bee34f8cba26944a7c
g_{46}	x	4ae576a41641ac9cee68d76168ca2dd3a5a8a1c2d1b0382df8c4bf77008be3b22d16bfa9da4a5a1cd277a31369ad04fe
	y	53c8ce7a42d2b8d5b94095931a005bd320593955e641b9d41102f81f34465ed967d69992b7810e0b5368e11fa9bf4bc2
g_{47}	x	e2ab8753b11ec352fbdc31819af1937c1d722d100b6d8a0a9dfeaf5bfe261f78801a0b80a2028c767e5790cea94eca1d
	y	4d7c71008a50d8b5f169d23d5821624f6879d3d6924218a94bbf8d69725770773aa87ee4cef01ce6e29435249117f6f
g_{48}	x	37588b4aca0fc5abf529046072e233f77c4b63d97d2a33800c1062c1196c53098e11f643cec1c54abaa6a9b27d1deb7b
	y	c19cecb06a2dc7d0ae76ce2c450180525e3dd02b76d8097ed440bc8d94105e6b6ae57ccf33c902a40c45fbcffd6069f

g_{49}	x	ffedb2a5735c6eab4d3a26ab3f716ad3652f1fa704ea4c5f064e09df59e064fe9aab89b611d0524424b2ec4d35413567
	y	8af913bce60e84ea81c3d7aa637d4077e9a5cc4fa6a801dad9dea69a56cace6fa38b891e3dfa07f2c6bfa45c480f42
g_{50}	x	e51a94f1bb056052f468e2f21bbc5ad2f672ed3f837de089bd59a9c75a7bfb97fb87103fff415fb194ee8b57f2dcdb25
	y	1b5f770ebc9f6741f97d4e827bfd6acc592ace08107db26f3eb428ee18cd197e72b949e6172545dfdee04645571a3dc7
g_t	x	ae141e91578a2667f7b79061e0a0f5b9e459de3038c697753d2f7ee1c08a662316da0d04c5d2115cfcbed003e51b8e38
	y	4d4d60f7665183483c8bfb466c36bf1e14837a7753a0dd1dcc036d91af53c10cfe765ac6190847d2f6683b78e1e09f0c

2.2.4 Device generators

g_t	x	ed14ac907cadcededdbb772a2c209604fad1b43bd85acf2df50e848bd9aa5b99b65b6a87dbeac90f3301e8c9d45b037f
	y	60448878dc34ae65673d982ef300a565ac0b46510bb962f1a00c459dc969e049add211210607db5a06f102505067f598

2.3 P-521

2.3.1 Naming

The set of P-521 parameters are referred to as OID: “1.3.6.1.4.1.311.75.1.2.3”.

2.3.2 Group description

These parameters come from the P-521 curve defined in [FIPS186-3].

p	1fffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
a	1ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffc
b	51953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
$g.x$	c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
$g.y$	11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
q	1fffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffa51868783bf2f966b7fcc0148f709a5d03bb5c9b8899c47aebb6fb71e91386409
h	1

2.3.3 Issuer generators

g_1	x	1675b76e4f21cefb11ffe81f3137c19e69992d144033f23f3930d1d5b013ca81698a155f2298500caeee36b13cef52ca1c421286ae59f68684c8578628ba1273b65
	y	c631e60abcbd970136201e5a8e4359f8cd3169cc396456b9a12d04317b3bee9aa27ac8fd84e67a61934c63d1d95cd3f89003fdb57bfcbb71f811feb596daed7e3a
g_2	x	1e565ee2801f3d822664777b08b43f2e50b60aa669eaf9870b37fe8f73773b8f92ebe0c0519f494bf938d55072dbea59395036e5c0ba68b885ad2abb47c6402b463
	y	7233dbf746dd2c2bf62a860f36450caf295d88d395521d7356c960f65578fcc82c29d6c066f2c4a0f548f86cc1bc7ea12ea7d34ce241d198f954d98c4f667878bd
g_3	x	163e41f82b9d756c774aa84a2089e7dab68a64454912d90e3cf37f9623fbd7c7402417f66ae17519db4c6c698bd853dbfea2fd3ec78efe887d1bd887cddbba0bb06
	y	b0811bd82aca459f969cb5e4642e5b67b52dfc9674e2ba3d24ece862fe79ac513ef65e8c9d3f73bb28c84f20d6b457c1941436e0f280bcd76123f7397af3a0fb8c
g_4	x	1bc68e0cccd3e2f0627589106246317fb73346feb916e2ca613c388254dd6f0f621a9a5f56cac25c353490f432e9dca76ef5a2ffb1851df892082c6d583f4eaa31
	y	425abc21db658cb7d3325d7490d5372558f762001369250b8086e4d4970706eb4b51bf76c643aa57bfa3ce5f6b7831e8c167ff29e2c6958b5286bde4f5f320ebeb
g_5	x	65110b80b2f3ba19ab7f5a6fbff5633bb6b3148563bd1a29ac1bb9d748800d4f28f04dee10e88f86afbeab7e10fccff69903d33f7cbef6fddf651596782cd76c57
	y	efa9bb04c1da53c5d9a7e9a26d33b641613cd37428475fdcf821948c4572db444f997f907681f0c4662d8b08b52d04a109215436b0a3e48f00963b99c490e8fa39
g_6	x	1f9ff75fe4ca3f2b65f6685a23f6201ed460e59d517290405afc7f797af272a06f4509717d189005ce93be332132184ed4ff6679766e617267e9d770174e9398b02
	y	e87ebc535951ba18b9deffd808e97b337cc4ec0b2944aeaaecd34934510fee9606ec6ff28b4c49cc0bb6e8c50c2abdc952ae95f684027b15a10d64e76cc614f5e5
g_7	x	ca012f9a52a68e79ad2e8e238289b52f7db5c37b7e50f1ff00d2e4122fe4b929d6175a95d7f24c9e22069d49eb9de2a11bd3832fd9d46da0edd0dba0886fb330a5
	y	255ad2cf1440e31210f38fa70ffcdcf632e53fb8072fb0ea5ef11b6c590e0aa816163ba288148654bfb54b71a4e387d3c63e8e4c12f5479d4529f9fc0b2c9359f6
g_8	x	1ffa438ff048ba539ceb37e2334eca04c82af7e9be210ce51572db53cb41e9b326b9a4148a24991e6608fd753b2f34adfe13ab87e62dc8f077e5baef437f58f60d
	y	9f70ff23a46618a34ba000e790544ba1bebb18f9f9974f7e1e0844a55b9a270183a1b6bb905ba87681f9aa63cb39b57faac9bb933e9526b891b2109991c259fbc2
g_9	x	301cb6075d056bc65e6ae301c076752e07ef2d21f182cede42ab6f56f089db5d50660f911a7f85797337a1a95056d4613ba75c7d69a5bcbaec2362e94c65964565
	y	2dee2dcd02ae5e3d50340b3886db25c0536eadeb287d22ab8524fdf32d40d2019a9202f9da8fa0792752dafa23a042c084f4d08ce0792f46003bf477f0a86cac85
g_{10}	x	407fc8e984c84601f3e41952fec161423017e073d33783ff05a50e0a11b94c4ebed0c8d7671e5180f993b1e9d1e357d29177271eb29efb96cdef4edf9d8c6b7440
	y	431df69b022004caf4c71ece51693202b510f40207e4856e94098215c01f55c19a0728c7481cdfc24b2f80d1d229ecdac1f4d83e8c466cd3586f4e0d13ff25e988
g_{11}	x	1dbac6be0860787def03ffc5472dc23fa06b15af01cbf8bee8f5a0e71ae28b5ecac96fda82e8574741c219fa62d31afd658bb9578d59b279df0949063122665cfb3

	y	36da1a1fbfa65c4ee91d836c2f424ab2845cd6eb7962500665f745c7a83c4da99e07cf2f57d99e5769bfa70bdbde84ede562504b8e84b2c1e159f0dbb9eb58549b
g_{12}	x	eda625de058340213a859df97481c06223337ab42e45599bb5431960d3b9c433d87e6df01bdc895a3c100cf5bd357e42d4cdbb9eeb47e1929802c20efc65e9e044
	y	c90a0efa16c0bb698e2b67b5bd498a02d8695c73f2626a96dd85371dc8d236af6f234293d09622aa1058859b36961fd59f5e28cb480c202624bef43186fccd396e
g_{13}	x	5f8a499b93c10c49e1e29ac7ba42671fb46ae8d0320bacb5f018f450a5877c0c63656eed3c8043bfe12c9346a6ae1f81ddb90f96a0faef9def3a986becca856fd
	y	63495d5eca21f270e3d599fef3492230eca64c712bb3100b14f4ae2b6218ab68355578ca73a26af4c802021f3a299c84d343aaef237c1ad20503532a468dbef9a5
g_{14}	x	aa86fcd11cb4e5156021f511c2145df198d8fc07e437f7495604efd387100d6ac338934e4307376feb1b9cd231f7e74e1ff768165189442d6a851858db44c3942f
	y	46e345906c1fa961a70cec671fe984ad62926e26af0e49dbaf78081bd4c80af1426cb397e9d414b7c2e83005be4ab1571f2843acd4834d160b38f4704c1c2d1a37
g_{15}	x	60ba95387d52d6f4225ff4c240c4eb061d6da6019467f4a84584fae8e685eaec078f0064c6fc0b5b5e479bda8b19508f64aa6f6bd321ba3bb5599b1fda0bcf0f42
	y	d0fad9201e634b41f0b9fc7597b77b2fe487e12b83369fe7ff0b65abddac92a02deb1ac54c8d6e0f5e55258430ff618fd1cbf039490a03e26e61104d809de41e45
g_{16}	x	1ecae8827a7b0947daa185e92900e5c5ef25dec1f0821b8a6974bda8192c07b3a3c6769adfdb857c73c9674ead26a3b57a56fa6c15a4732c4bd63061e1cb8d72ea2
	y	75d01f5d3b388a16546bc83efa7f97432fd0071ec7e59293232be9c6aa48d1ae5fa74ba0dd8b99eb8409b54d6d811d164af43085ef860a3a27777c033624a8f669
g_{17}	x	b41a80d0cdae1d86bf0321a9ade6bf3cc1d60bbc32a8cd8ad232c8228e9c15e75cc372d6ca6e5ae70de5fe5202883938b42df2236643569c0ee6a73e0964548c1d
	y	44bb4ea0659a27e612ac00887949400fb8f41c9eb5daff89b5ee4ce979fa1d73b5eada1f6037c8e016e44c1c8a4f9dc2af487cd92a19f450bd71bb4d723e9d04a9
g_{18}	x	d7ea7e804529f3a0889feca632cc6907a24389bc0ba1ee0f648d52e0c0d91744359ca945e0294204a9d8a9056cfc16a01384f43c7b0fe207f37a81ad158455831b
	y	85fa66eede6d452d4c80fb9243bbbcd5500d7c37a87ac687a49ca020bbf00015acd5d427b2e20e733a05849cc13d2c2045c5333d7ec10cc8f2a63f63fe781cbd42
g_{19}	x	6ce87f9f5b5b6fa0fbc51c2e3a2011530bf216cc03cdea0c352733a0dab6efa7ff77efb21698d6a2a30697e35b128c6ee2a02ebc946b7d01d6aef9c4381c12925f
	y	d6031016603250135e19f6bb8086b7519d223b083eb833f4eedb018c5a826ce2092925b68f8b3c825768b587e7400c57be2cbd5af2da4d9adbfdae09641f3eb6c2
g_{20}	x	1074f1716ca1df00f49490c85f9c4be238ae3529ec6b2c49badcf702f90b4bccf915146fbcfa07cf20498677e82f47572bed9e2bb585468a9647df1aa65b10b4bee
	y	e3735d881a471398c8554ecf7d25f5c87190c6de1a04b5c13ed168e2378691266fb98f5bd5f3360cb669cd9a4db32f42f602515a742dfec7ada842d595da6c6e3d
g_{21}	x	4e0aa3b9c2e7147386fa7bed543ebdd415e8c33213c15e28aa8a003e5db378e80cb1daee6002a514a6739c8f618d71104dbcc9d16c7191ee65c967cc3068e71f24
	y	8437e93bf86dbd0eaba383ef307ddb98d27ae63e790338e85b2781680ab0bbfe1712478568e12acedb976a8f38a255c870ac5f97f45141c09774637704792716 5

g_{22}	x	126b1e605e3bae456c986addb6eba0f750229b3f971235ea827a2e16f45f3a938765af0a0812fa2af0199e2e1801679e43a1ef9421732595dba7e71d9f6d68c30cf
	y	fb8640e49a5fa09c4fcdf2c37611fc397f5f7b5991709cc6783b92885ee97984744451b533d5710c8b801d5e29ce2e373fc325f329a7502d503f423eb2a3a9d428
g_{23}	x	8094e94e1983a7611a0cd624d94cfa1b3c1e18ebd2767f4f4146c573df368281693ddfa526217a0d935d2256a526c80fe54180d63b44c5a3c44a528bb211d0d40b
	y	2c57eeffc512d830eff90f8aa41f867157926ae53727b3651d296a6703878f96738fb308f85cb1530b39ed24ccb60eaaef80aa22f1ca5e9ac794110ac6cd048da9
g_{24}	x	1ddc9a991f6180abefaae9351edce524db8b0d7e427c3eba58817a508396f2dbf6e1a7543627e05c3bbe65dfe40d0b33189401ef19ab1b16ff33bbc443a5fe547f9
	y	fa05ccbe21e0bba18881dc662ab29f3d9c96110b2ab60fa5503221377acfb04851479a9612dab994da5672571dc5c4393f75b2c84aab3fa6a0c4497f0e55b12cb2
g_{25}	x	1eb9035840630ac6fd0a30173a94793f7e81f34455e2e1a600fdec09bb6636163c6c4b24175b56053e67c3e374d35739be31819cde7befc42ebc3aea0abdd03efc7
	y	da5565b4f616dce18be9657f386f0c2792fcf0f602c6acf84fcbc976bb276d6d84977875dc12f887654ac7c2873c3aeff1c0d45cddce4cd63328598a67b0b222bf
g_{26}	x	12a8c695c849614e9a6a1d4b3988b6a56bbceb780d1cd2b2be337b1720a27936fb05ecfa21aac9e99b7031bda9421b5b3b9555baadac96babce8a7ee4e1e2657527
	y	c2c28763fd1e392d07ae2ed969912db6c78b8bbfa216e5652c6fb47731ec455938da25c17fb582ea502281030849726f478cad1a8b56be921a90b53610b62a09c
g_{27}	x	130b27465ad69c6732cda118050cddda2881a0870f1ee9cebd81a5656755cb6b080a428938baed1f7d6772a8f559234fba20fd300f91d88cff99b794f1fad6479d4
	y	8c6573a89d9b48d9ee8474d747526bcd74b20d545c42ab7550d6f49061fccb09579c39e670bc04be0820bd2fc39a5411486041ba94e4b4056a196b076a222be01b
g_{28}	x	12caeae62f42d13141fc28bf5232f95dbe9dcd721b2599041507da3a5c1467a19fa469ba09140106622e67771f332e19b3c173afd1e23d845db9600be0755f85ef6
	y	ec2f9195d2bf0f749f1a73dc13b7618924b3d379db2129137188b9e8e55335c096d63a27f5bb02f5b4f5acd7c5c4ba9a7bfbf8beaf1c3747d94ab2fc5f1310fed8
g_{29}	x	c2182ba6e820e8ad89ac8f62552160abcabdd147e63f769adc69a623ebec89102aa83dfa2d6d6af6263b497a7150610eba6ad98297a278eb81d662c2def38de040
	y	9ae7e0671572619b730b33abdc8c9a4608d641e163456310be94cf55ae4c925c6fe63a081fb1419b66c3a8fc199e7ecb114a9bdeb13ee7acf3ac7edd43f7223518
g_{30}	x	517c312655635d41df5efe8f8af30677e0e3cf5add48aab157f45dff6215cdcf5f5c1ad4dc3474bcdd401bfa8b77103b20c9c28925a18ebfeacd8d2b0a1d52d48d
	y	5d6830d33c7edf554d9f14c9e6ee502966f833a1c5ef506b6ef44b9171664e99e5cc1c8b09d704ff9e72d0c60e1f7ce6e6f8989a88a03b1c300734f094c2c5624c
g_{31}	x	6f2017da1d5c88274584752c8ab8c7ef8ae7f6a9eceb3a8b3b9af16b5e0347b01fa662b0db27fbab75749ae68357135f3dd2544d2e1a7d9594bfd7d7ddf9d69c25
	y	d62195e14e6b29654147db19d02cd73381020d7a5559880e3e2f41343ef39bd29b613d8b55ae33d559df36a17d1fa4dae0b5a352f459168f94d0a5b4561470272c
g_{32}	x	1f666425fa8bde98bff138161796c12e0e1e485eadacd0ed5adab17ba92b3a29328fe057196d67a036c922f087436e98187a425b9226ae75a0a91b848ada67a9be0

	y	b78d8152baae1fe290183564ec0cdeddef6249220b986df8bbf3cb9a047f066279d3cd073b5d8f18508a17f7afccf40758324fe251c54e2bbfdd2be16ddcd35acc
g_{33}	x	1c78aa5476f6cc9b6d22c3a258bebc1df2ce2e391dc775b814cece94f64fed29c0c9a40ae7b78f2181af163dec8318678493d1b9852606e58f963754652141cd1b
	y	3e4c468142cc1b6fb64117c6697f29c336fdb272a483642339d838220603e11d4c6dc80b7b1e5d1321ab11a02d7d81a25a14eed5808c7a095481c7b9216d076580
g_{34}	x	14be306c2a30c0b90a741a37de382b565a0787471dbd3726f3adede7ab1fdae81be595ad95e66d7e2dcf5387518badde3128e18f32bc198cb700fa3b8b0fcf3879b
	y	c867c121cbb34253c6d4ed65c70be22d1617b6900cabcee928e76b93bd16ba13d493d1c71e627094dd14d6a1b2cbaea64505cc55249c9786971703502723dbeb23
g_{35}	x	1f97325c455dd3b04d58a79c76d80e419d6e75827847a4b5148cc327c340de6670aefe59988c1b6149ad39d59498afe434fac286f51967de9e126e5a23a31061c82
	y	1aa422ac52f5084393f4640768edf0c2858f79086f924ce3c180b7f11d91c8d4235f9f7457593ec821dda06a10792bd69ec341ba84b12608342cc715d1cd342ffc
g_{36}	x	af4b0e427400a864af899a2a56cf650ef4d4a8665886027bbcce7c1004dd725eb4bb62d1b73c5e285cf2aed3cd490c06ff2a1613eb661f8c0a86738caea2f5d4d9
	y	3494aa6e02e8143a857afc9a6c79e86c31bb5de7a01bfcca4a57572fef373a3436e3229944cca15e526528a22b0fb1a3515695a8e4df14188f81c555e7807a3f78
g_{37}	x	3593984917824df5c94702cfd7b05b3eb1abf73cbab62a43df9671df6126a165a2727d27997a2b911dc1528fe42263477ce2e8ee8bf1ec22c932459adaa3758e0d
	y	3e000955d568b335ff04c7f011f8b0aeae2ebd066f85bde68882fb840d05b291c94f266e82664f239b968acb220411b546d46cb6ce72d98cd7a6dec54e2469b632
g_{38}	x	19320c9939df24711f9844f0312aab80e447699e4d072a2d9e80a29dafe86caf058fab3a8a8d4975515864c2b931c7f7db3b25f2f5f9e5f8b5315a681b393b08a7f
	y	ab49050ea49925fc1cb86acedf4219659b2490e91b09f425bff051600a9e31464e2ea96974545b7c745838a75a49c88bcacd837ac8957fc14f711dea93070f3d99
g_{39}	x	12ba5b532acb5ceee9c91a325695786bf7e1842b831f8da30d360d428ae533ef2d1071e8131f7a7a729bc2ed19ae0c129b8ab0377fb55e019e64932eb28f80b9334
	y	803c8ebeaa493d6fcb356fb2562b79d3a376b5bcbf9b22bbee75611075f7b7ab16666abd97be5b7ecb338841fe77ece135f4e2e4b83acafd71e704527a84789468
g_{40}	x	a092eeded185fa7682ef7e4b2a198a4ea043a5eba62b4479a8657d66d9dab7c5de65e47642dcc62e2a561eb494f1e2748cdc792f0114c77f52b7d7c5f5c4b05883
	y	d74a594a661d40ea629702dd1247808fb288dd5040e5410d7d6b04591e39696bf29995a3523928413d746acf2cdb55c40aa084cb65a289bdfc8501fdccb40209f9
g_{41}	x	ef451e110daf9d5e391a5359934a9f6969517f438c7bea183d5e96290ddce120873e45486d0c41c887c483b4661dfb48d8d72c0fb89e87e39c8a3716e9cdc76ddd
	y	efa5c68d14de0eff1d729005e26e74f49f8bc083124a432ae18dd5131c04776f59a3f93274c5177f3c91a20160657a114f5bc0dbcc5c8069984e341320412adf1a
g_{42}	x	118713fa11a53a24b33f9e156cecf8b415874794508fe5438f8c4dae138666a5b888e8e99438dabc1555646574 7116ac472ad95d2920fe9b36f30be0963d7e0db12
	y	954bea5f61e4a9d8d093d1b9d6ab52b2fac8b78655802010cf5ed97459864271ef4c34d8044c26c7763de328e509ef0a68c1173130ad6301b20c3bc8f8f26ad296

g_{43}	x	1210b8efd90f3b9ec0d8f3f82f6878abf54a88ff06872064eb7f4e903b530945c5a7f0be3b30d004801700ae3dd25327f4bc28608be512f800a8454df8d15069a18
	y	8e6efc12aad547b3e08d39f7a79e9b034616f098175f716561b7927ab115a54be4fdecd3845f7f5358828f175b83ed25ef2492c87296d6d89ecb9881104be9be7d
g_{44}	x	1fbd78c94ec52e5d769392cf084c5e629b29cf6e3bba7f3cd0c612c2f610ce388bb72a9c7d4ddc3f5612086cb42bf340f1e4ac7324c7359ef3351095cb00a7a304e
	y	99dd83d1b4c0b271f51c4851b236ff7b7e8662668068479619 37ef20aecc988122c076032674be513aa03946163477ddd205945b3917d1a3fccca2ba9d4205aff7
g_{45}	x	eceadae3607ea6aa2b654ff67f0c1569acc323ba3e6dcc5af8ecea30bba435be1a629a74d9e23736fb93f3beafcfed2d36d59e23317bd0fd1f959bd4586e79f89e
	y	f9735628a382e2ad84fd1badebcf6c9ee5e39789391de6bfb409b0adacc173105054118b443cb4eda232428f4413183a56486d073b84a56d89cb721ec985ebc751
g_{46}	x	d225f39d10600cc761c17fe15ace8bbadc776aba28bcbae482d15f79fe38dd0bc2c9bde12d6ee250489d0e7a23488711857fb913de74441676fd3c98da4e8fd8f6
	y	97b3f435c00416a59586e7593128c12b734723aa887f98a0b482d18d38707bb933e4b4bcccdc71075f5174e8f2133b74b544b29a796b4fd8b783664af1d3659e99
g_{47}	x	dbcc8bb88c00c531890bcc22a2f221b8ca916b9c324c081c7123e5ca66069e0bcac91e09bf95fae7d15f8aacaa1726d70ac03057f7d86f0e27376ccc1fcd7b8c7e
	y	2d4001615d625d51263a6f7bf263c0e21c656864bd9b395c1734366ce375518c058a34e74811c14ca07227baa0bd0b59c95356f47f44f390c6a4d16c4a6e0c6fec
g_{48}	x	1045cad535d9236d546d0a1385a3ea41e6586ee0a76c6ff5b81cc887cb58ea259e55214c8289160dc1921c412e4158be0cb54b80641cb657c873a5ca84ef0e5bc5a
	y	56ec9f00a5bd39a7857836235a83f24b21ff89b85484c8a795fe3e3baeed8532ee2b94198c9882035c77b1e75085c5cb936df3063e7173592e2749099a62247d6d
g_{49}	x	8b7af7378ceae85d550bda52ec6744133bc0ed593d612a4718a43b0f85b057f79f434629b170d203a57ac4c006dc4c87b5c92fa7d4af37d5e3651a141531fc151a
	y	9440c6216b46107b253c40bd70fc5fc96fe9b886cf32940958a8024c08595f90a6d783f40a48b1ea9bbc8e0adbb8e4d87300aca7f712a8020b0c43d3b1fd794b1
g_{50}	x	63105a1ff0449d4d5d788395ee7141fd5c44fd0227b3bdc32b9e9d26be5c7b7945faf8ab247eed6e50cb824abe7f5c4b7ed9ed725892d277ada462bb4e72dd5e6d
	y	cb0280e5e9293d2db08d25caad1e7b49aa52fc854fa49402e05e4b6fbcf0efc1764834c1c4ca13a36ca20e8b8f57bd77aca8f52be06bd9a6929f93ca172d3d86d0
g_t	x	d0bfc69d957f2fc38e5170ac3aae81110dcc7a077c0094ddd29ff12057fcaf56e8d014d016998e44710db3fdf72da65e31cd665abcb35308a6b0ac5f18b3ffb6f7
	y	bfaba1b7ea54552b938ce89d0907797f5f55dd081ca3fb5cf01f2606d464e36e3a37e050cfa0fb9ceee03536707c6d117665b3b1e8344d66939b29792004475053

2.3.4 Device generators

g_t	x	15f3ae2ee57671e1bdc87047f34cbe0aabc693f463b13d42df6fd10f86cc7b4b4b999c9c38bdefa8e13c70174f1be79f8e934a3a01803073b34046b8d8ffc799342
	y	f0984ac43d1a34d52143f09abd1746bcd11e5495a096e307d1ab21648b1118c29c201f29d085d6a8a4da6cf760c818dcdc4ede01b411065cac92eea1cc51bdafb2

References

[ANSI X9.62] American National Standard for Financial Services. *X9.62 - 1998. Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*, January 7, 1999.

[FIPS186-3] NIST. *FIPS PUB 186-3 Digital Signature Standard (DSS)*, June 2009. http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf.

[UPCS] Christian Paquin, Greg Zaverucha. *U-Prove Cryptographic Specification V1.1 Revision 5*, Microsoft, March 2023. http://www.microsoft.com/u-prove.