

U-Prove Recommended Parameters Profile V1.1

Revision 2

Microsoft Corporation

Author: Christian Paquin

April 2013

© 2013 Microsoft Corporation. All rights reserved.

Summary

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

Contents

Summary	1
1 Introduction	3
2 Subgroup construction parameters	4
2.1 L=2048, N=256	4
2.1.1 Naming.....	4
2.1.2 Group description	4
2.1.3 Issuer generators.....	5
2.1.4 Device generators	13
2.2 L=3072, N=256	13
2.2.1 Naming.....	13
2.2.2 Group description	14
2.2.3 Issuer generators.....	14
2.2.4 Device generators	27
3 Elliptic curve construction parameters	28
3.1 P-256	28
3.1.1 Naming.....	28
3.1.2 Group description	28
3.1.3 Issuer generators.....	28
3.1.4 Device generators	31
3.2 P-384	31
3.2.1 Naming.....	31
3.2.2 Group description	32
3.2.3 Issuer generators.....	32
3.2.4 Device generators	37
3.3 P-521	37
3.3.1 Naming.....	37
3.3.2 Group description	37
3.3.3 Issuer generators.....	38
3.3.4 Device generators	42
References	43

1 Introduction

The Issuer parameters defined in U-Prove Cryptographic Specification V1.1 [\[UPCS\]](#) contain a group description $\text{desc}(G_q)$ (using either the subgroup or the elliptic curve construction) and Issuer generators $(g_1, \dots, g_n, g_t)$. 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 both the subgroup and elliptic curve group constructions.

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

2 Subgroup construction parameters

The following sections define recommended group descriptions (p, q, g) , Issuer generators $(g_1, \dots, g_{50}, g_t)$, and Device generator g_d for the subgroup construction variant of the protocols and for different key sizes identified by (L, N) pairs (representing the bit lengths of p and q , respectively). They were generated using the procedures defined in [\[FIPS186-3\]](#).

The values p and q and the corresponding validation values *domain_parameter_seed* and *counter* were generated using the procedure defined in Appendix A.1.1.2 of [\[FIPS186-3\]](#) for different (L, N) pairs, using the SHA variant with an output size of N bits. These values can be validated using the procedure defined in Appendix A.1.1.3 of [\[FIPS186-3\]](#).

The group generator g , the 50 Issuer generators $(g_1, \dots, g_{50})$, the special Issuer generator g_t , and the Device generator g_d were generated using the procedure defined in Figure 6 of [\[UPCS\]](#) using the corresponding p and q values, and the SHA variant with an output size N bits. The input parameter *context* is set to the *domain_parameter_seed* value calculated in the generation of p and q , and the input parameter *index* depends on the generator, as illustrated by the following table.

Generator	Index
g	0
g_i for $1 \leq i \leq 50$	i
g_t	255
g_d	254

2.1 L=2048, N=256

2.1.1 Naming

The set of $L=2048, N=256$ parameters are referred to as OID: "1.3.6.1.4.1.311.75.1.1.1".

2.1.2 Group description

p ef0990061db67a9eaeba265f1b8fa12b553390a8175bcb3d0c2e5ee5dfb826e229ad37431148ce31f8b0e531777f19c1e381c623e600bfff7c55a23a8e649ccbcf833f2dba99e6ad66e52378e92f7492b24ff8c1e6fb189fa8434f5402fe415249ae02bf92b3ed8eaaaaa2202ec3417b2079da4f35e985bb42a421cfaba8160b66949983384e56365a4486c046229fc8c818f930b80a60d6c2c2e20c5df880534d4240d0d81e9a370eef676a1c3b0ed1d8ff30340a96b21b89f69c54ceb8f3df17e31bc20c5b601e994445a1d347a45d95f41ae07176c7380c60db2aceddeeda5c5980964362e3a8dd3f973d6d4b241bcf910c7f7a02ed3b60383a0102d8060c27

q c8f750941d91791904c7186d62368ec19e56b330b669d08708f882e4edb82885

g bca29a2d4b226f594591ecedbd1859ccb0ba3d20186b30e0ffbf05ba25788a6720005194c1f005b2ced980ca160254bb48a0e2d756ddcc919afe9017a47905154177fb2c37fb6cc0f4423e8f4a8b8376e0043dddf06255050523d4ee1f68748d0d415732686f01d88d98c75bd1e25fa48cd5bf4cc69b6d67bf0dd5c9cf18ee91ae17ebf128151286de3ab17ac4025a91168d42532144b7357e423f1b8d9dbcee68df89b44150e496ff6d416e4376e2daf9e422807d276572cec335d0587a5d798022415e3737326251d304fd7129183357ef9c8d194447705360b5bb270a2ce6194e5894c1fafad3ca78af080f500227564d43cb63462b1084e9ccd55d002e19

domain_ 227cc83035ac2c68e6b4e5fe4b59c0a84ae80330f380de03223e378136d76fc0
 parameter_
 seed

2.1.3 Issuer generators

g_1 b97134cdcd52c11b28f53a3dde83582728603a1d4314da644335514f2fcbd3c141e3219
 c73f42346d4a3a487744656e1c29916a1d8ac9e12fd7d5bac0d28986208c7393f503be33
 e3eb4a45b80f6080c047bebf5ac4b768496cbc20e4d76c2c1b33e9e21d37f6361aa6ee65
 4dca79164fc275c01759b1c4c3b0ef2d4c72e45efead2c6b054656ba78e639d38e8aef21
 bba8b117aa1cb8ab7d51ab95993fa445b1df7d3c5877da2606274f83160ee17afe401b38
 47fe0c9745e995fcb9590c9b794eb931de43d1375c0feda5411023242be913d84972f252
 6c3834ce9c689d706c4bf27e8b9d8ea35b8043bfd5ed2308eeb172743b6d0ea0f62ac552
 68ac371

g_2 bff5b5fb31f227fc38389194b0ac9ff60c8d8cbde7cafe52e2c26ce4bb04623f469d250d
 e495a5895d804890a87cacf7ecb8661d21fe94e9a7b05b95ea6c5943a535b4570a61b2dd
 5c221aedac4b2d20759115fd779e9af18357ee5a9c9dcf88d02ee45aa624235a24edcb08
 50a27e00760cb5613a16ca619359fc644b6f202ed36f0c19053b0a39b999900330c0f59d
 6af7e45e881873c7cf3e710ec2ccbd0fd41078694021b6c8a665862ead51a5e84a160cef
 ebdc0d04352170ab76fbbd80e56ae736d658f6aa3ff041b6728ed1e37fd915d58af628b4
 526464faea3af081bb1f633ecbd0e8574235f2e0220bb083b7597301f451977efa6140dd
 56cf021e

g_3 4a6a6d07614a449b10e207cf209b4c812c7dd4547610bea2a5d3adf5ec7df1a7bb961144
 a86c6ee897966712457261651f4c90e933a847505eb96f33a3bc35efe6eae28384810ea0
 23a27b3b96cd60829327e1af3b2eabf23aad422652fc791bbb6c91d0b8e03a13dc9b63a2
 a12c2821fc308338824faedd54d22fb106edb2ce9b6a041a79568aadfb781df43bfa9556
 668acecae96a18335e3da5c4f94db278226682dda176a73d095de063f83b6e81c21ae9cc
 14ac9f4099bcfaa80128f332d597a5f81c9131a9ecea28b339c933935c387626e0760589
 ff83948e39c80df96fa7a1edea177ec0eed7c41f3f8c1d5b45cde0dbdd1bf6e2eaa5c2e7
 5a9b73f5

g_4 3254822a81327c8b5d1c26c2f3b4b953192eb4a70e094d6a355ac96f4af49632c0094f82
 b15b24c355bbfa057d1c1e99c9ae1a86b5a8c09caf412d0ca5b2a78f90425a4cbb5c95d2
 bced87b21bd04a5d07ff6d098dd5f45ddb36e8692e5e866bca9c5cce1e864cb999fa2e4a
 1763a17ff07ee2c43c566a2a5ac62d5726d74b13d1f78a18057d969c8b6cdb0d60b16de6
 9fbae70bb5635255d41067247b81614adf575f2c976394e024e4add330a3fcd6edfa176
 7644c272f67968080b902d54dde4af9f57d4efc62e7a09305ba8c237015513563545f8d6
 70c7ce636732d4611fae45edb2c317b62cb3b1f07146b8313bec7cd396829c0bb3f1c96c
 d8bfad9f

g_5 81e675f9eb6a8c919eb3d0bc9836e4e49c8606d618bc2e071e7f3f5e47886f1a9c82e22e
 972131875c8824e38fe9a7487416b5975ee357c06b9f30d660c3f49b15197b0dbae62486
 3e3acfdb0312dec3d038d82f4ab24817a541ca1af2bdd7e033a8fd296c8ead83fb848765
 4ab67eaf563b97719b92a55660e8f101108741792204272782e8aeb8a4d2b5390ae2e82a
 be9fc617bd227bc594bbacb946416bca6431d21f7b41dfbcf909a165dd7aa6d198e8e208
 2c7d4c39e93d2dabc4795e0262d997b6df4c42d0d7a31adeacbb0f9f01cc44512df90eda
 b7111b6215326f7b785da702403a7a3f1b0dfd58d00d8385632d4d88b9b68cc48a29010d
 d07f1a9e

- g_6 62ebc21296d84c29ea41bc5eddf3ecaec2e5a9d8731ff560f53e0bb2cd633581e55dcf1e
fccbea9782c126606c98bc5d4407b6a665883615d87f4fc1ba549e0586d10a4cd7479695
c1dd319b6c2f32298ab64a138f41e7d56aefa871e5246d18f9fa40f8df3e5ab9f9c07120
552896832196f7a909574480007910a29fcf5f59f6da51d6b2d3c9c3952d0f3fc675f75b
ae1ebfe3c2dd3311050dc01a00f68bf5ba61cba240be8882d4614689ef00166ce46a53c7
bfa5af63f0834b9581438324b8241ca1657fbcf480695524365f57877c0a8a5afd61e83e
fda89dba8678a1ee19e730e83c7eacfff95f78bfed6e75a8071c99f61d20739225d4a06e
dd39a059
- g_7 9c36437103795b91095d4eabee16d0922cbf4e14f6e14a95464cfdfac5a5dac9406ae91d
468d09530eae6ca903f818c852639877a89f0259b210ded9af3afe42cb495cd89553e614
9709f391996f0d574a47b0258a080292d4d4d2ac44db9169b83edae35a6eaa96ec92ba13
6970acf9114c9356ef5337b657e49c86482028d24177ebb5bb8a43e00fe17686dc46d97a
04e26fcf13b1b9925d8867dc1c39a4e55ac237ad02c14a81325919820686ff1bbc0007d2
143d506510a72ff871839e0449a2e14d01cd23ca08aa0bde8e8e66733b52ad4405f6c249
6f846f7a41efa20422fb1ed47e840cd965f24309c6b9388b25f00caa9aefaf6851108766
356f8ad1
- g_8 97786f500577c95adc8d33f5a287a89eda04a7055b53a33221004653b64dca1ff7d138a2
005652908d53c4d5e178d78308a0459b342050b3bf5aa3125d2fce715f8b95de4b63d006
33df8ab5fddf3ac41629a1990865b94e4242757c33f6c53a8b4294d01265dcf734c145a5
5f5e760aaf1eb83623f5da375bdcc1db17cf46f6f5cce4233d1fde5b8aee752e5a62f831
c7cc5418b184d7fd43db2bdfb6b7fe3fa677472217b87ce184a76d59afa9201081b89879
c9a3b0d89aa9b77112bfcc93d96df067850172e03d0f461e598dd494eb4c5a8d0de12a41
6d9a67169359f8f104191ade727f2063763409f02b8998447fb25058c53e69d55e9c1aa1
2d4fe99d
- g_9 243c1274881f76db009564932f16a49c8ff0d89eab78eb22f38110d84c652ec01a833ebf
da16f8cefca289e85dd497ec1ce036921404d72022c9bd138efd7e48225e09c6e01017ce
11e46145e26f5c37782b5a3b3b673143896bf3d5960792866fe78e48acb14fce59763087
905c752bce4dbf8f627b8f6929bf3e223deae76f025d17f9ee66ba84dafd26bc51b84cb2
007899ab96f7147121571a5ad5afa21f10b631af26a9620cc2572d2fb8e49044c2c87550
8f848fa40465a73eeb1a5e4fafb217abcb994e227cbf2aa9b8a5d788961a79b4475b21cf
6d532765e8904c86f242d3d3273c911e8c20f719431b11bc6306413f2ea2be54df8dbac0
fb6a4c1d
- g_{10} d244bd10f5762fe7a81fb97676f673f82b1279c98e4b664e73bc9997f458ca801476a985
1158d8fc09dc092e6148050194ce3023282fd19e1e98c7de238e981b246315432606fa12
c7cbc387e0fe812362b8922635a213259cb154e23157fa28822a441ed59dac8f42893c31
b0dbaaba0ed75f79135875eb6099bd9b1ef2425e89a09c8de73cdb16d386cbd0bba1e5b0
0f284f632939d12172325f410a7213b8e690cd38b6321df8165f3fa46f16223ebfd1637d
ab3d7548843ea3d67f6ef14e3e2a5f85664007f44945b3f6ca0160631f4f125367eb00c9
f2381697f708f31c81aa7ae686b03cc523809f254efa8936918222a9fdf4778ffbfbcdf20c
c8de6c9c
- g_{11} 255ab8e2c5d04133feaed2edef61bcad2d428bed1998fafa624b01d051de4e5b00595365
110efb4febc5f9fb0633d0bfa92bd864cf678c969726f234aeb79cc4dcelb9ce68563ed0
49e9f8a5331cb87d12dde81b42fdd9012b9deed417da911f74c4864b17b9d259498cf897
8167994d786323a48a972d623e1e7bb097fbbcb44eda8ce8175cdcc8d2d6df15eed5a98e2
1bc3e5ffce5b9cba5228c4f6c08aeae77476f683cd10e9225def3212baa1ef105f6711e9
edbfe803086a2b23fa9310a4f64ed9870f91ed7eed101ba90d71deadd8ba6091b32a32c5
47f16080b01904e8ac958fd20bb558b4040056456495b08922bb9a1d74ad24c9c01f820d
0aa72932

- g_{12} c619f23cfc03cbcd3808a418d16b89fd00623f7ab6fba880cc7f45d879c88cd1cde8395008fda9c2b2c4ad07189eb55a359ba04d275614d4d25452887679cc29d2bbc980830fa77e1d76ddddd0e4b1502168f5f27d188ddb5d32554c621042d6333c3b9f774d44b620c68c64355143e98eae39ec29ba812b817a4d7ffa5b322fd49bd9c1c3a2f7b5560c166699a9f9c0f71e2a49b7dc2806da246b1897af7fc90b5971613704fb49331ffc11e8f874728563b90ec38c97ee4b30441b97a194a4558440816ba830669181f0544138787f3a249756a55db772ea217242e9b5606fb9c8f4a23e1d3eab88cdb0da393f7aa7a8eabb80ebdfcf67c1558b36419b
- g_{13} 4b42fae293f2971135ed30967c63a6ff75fc9449dbd7f0754d4b752ad72a81c0fa5abff49f2726c4af04c72d3a7b8a096170abb958c17999e9c97464d8749b4fb17e5e1b2554c8c61ba852cbcfbe24f1744a602078f55e5a81da48f86f546dde8fad26c0e0e0a8f244ada1630dfed441ee5d7b233e50b85c11185554e3f3ee104c54651683794801ccacb0fb9c548c801003f53c43c3bd4e3752da9e1a7032ae093c8c3a85d34903d8d2b1b97126044f6867a0b7286775edb6dfee6f1844a13350c746e56895e275c5f4f2c87791b1cd0c8c2f6ed81e68ab3120bfabe2b20c2f6695223a95b3c16e451af9f0c1bee2a70f8335ed461b05c060c51c3450e00c31
- g_{14} 8b723c1bc1385cc9af0c6b4701ec3acf1265ab3727293f7798dc740b7d7997c6399f5883ba08dbf77af08f89f856f38d80287efb5b939c730ca830a2ebda6e62ad57e6ade3e6196a1995cbbf6bfe2be3c8a84fb6f39cfac44c85cbf400dc50a80d9165b560a94f7df1a3f52c755105db6d1b01ab2876ab01af5acce6cfd35e7592a1f0f9808db4e5c79ac1a8965836244b0efa817eba2f82a3bb31c595d531da1c55d1d5a4cc2fc4f8885b87782b791c62ec33b426f0d1755e4c3b8cc3cb9948da6a3fb71cde01be68ca0988eef9a4597c3f423ed7d9bea7ccf84e21f9ee140aa4c7f335bd066532fa386fdd817f74c68e226001010edea2a90dd95cdfcd0e3
- g_{15} 973ff266bb2b99478b08a132e56b46943a49de4bdf21d85f14688135771e06bd76547ef58e338aadbfaf6bebfd382e198f1c16cc87a368cfa22699b65d2ba15c431c5d1a10e30fb6dbf9ac5af5f197defa7b88ddbca4acf327a0b4705e7ab392042d71ddf797c3d61724a05550cfd1e10a9650c0998171422676b184a95ac6955021f968260115feb95b13a7607e0fa3a38c5bf50033795cae1fe0aa094076f0c1ee3a909757118fca156e9aaf2eb7aac1b8e530b23181073fa985d548b0f1709a908bd792e97081c663acab54e0b7f3010a364768f03e03db0ff00c634a8d5da404735ca08c49e0a685ae919c6afe81ddb7377cfff5323a3339cfea6de130283
- g_{16} 158f857b499cf962d81396ea280f94dee4b499b17d187a4d6d53b16c824985d9aead7c215799b82c8f7be77a0e3c63f3c0d43042285305f291b3fe3f48f4596e31264520ccd8e212a037603025239529af51b6af89fe5d6cc19e438d243f1ce3510807f0e09229b44680933b2517827a37c0604fc08e5da117dddb12b9460bdb2c68528e98af4da0e74ee1080c6e735f3f6af74ab4de1c2b2a44f85534d5cb24dd218725dc9be09265de4d3b4d3bdba74628c1482c8ec58450d90d635eab3c3b7bb051874cac728345820ae973ab76c07b0d8f6a912f8135a0c13725386f533885738b6bc70961467752adfc1649ec1512a23b55dde13854d249566b8a7a8192
- g_{17} 1edc0b0a85d295dcaea33cf82c694c33dde5191c48cd7fe944960d8a297370db6f96a0d83365036994d254429bd27e5d25d7021ed5f85efb79b02bd704d95382fa9ccbda410d88479a8fadeaae2a7de611d281d14cfaa345ded9ff3e97c59e1d26679fb446063ce54e9b99cb b99e01763a5b2f6111e4e23a18719761bc5fdb87a417d4ad69aa517c5f165b8b16a2d29827a39e8fb8358cea660f6b2091cd1b127f7c8c864f328a859abd8b333ef857db00d9b4a22d4427e4a030e9d56b27ba78fc3810b38b446eb67e12d263493df20eb07314eba1227e4855fd899ce80fcdfafa24631373af84bb4116d37a95ee0280d48823d61c6a6e581218dd62ea4d147b

- g_{18} 860e6baddc4e3ba2dfe7c3dc8462bcff074da3fe5830894ccb9f43f2ec917d7f36f7638070e35f8933b53f20d2266bad0f696af2668e1e7205cc2883c9a50845cfdb1aee30a3ffcf34a5e68942266d9ae5c3e822a51401b59171c9696b636ad7a8c8d0c0e02b18b4459e3613c34db98ce42f328d63924caff9f483900580bd80142db61ec985cb629ee3ee1550ebc26c268f8273ea75ad947963f8f41a8397fb8a1ac42f19d3d77f9070c792cf62f4ebe8d63657d15f9d46910613b38d16b26c10a4239b69d45e30faf83283cf8e536097f088a3ce667d29b551ebfa19f8de90706e09b3de4c118b4b66c91920dedc0a29762e1854e9dd038bc7034d69abbd14
- g_{19} 3d10db2c984c24607c7d79eeee1cdd63b2222b76188f68a629177df62e634d2227696ed318ea97716e346c580c47f368fc3533efdb8210ed02397418eebf008b28b48d287c8a03fd0af8ca8844aa10aae63d69a9d256c3e153a2c844af7999d77541d95d6cfe66a42ffb6e20fde6c1273f7d916ce341e59f9ad1d61734edfef42c3cf358d947f8c2430619ca77ecabdb39d5f105f5ec64d85e9f26e2927587234d00a0a9c9bf883fe6cfa80883be484ef29636db4c9dac44670fc8a68b548ba6f3f992b722ea669cb822906969ed684d28cdb83d2e6abb66935c9fdca2beaea20ba36862a162ac5b2099042b6fe79dceae094eea0f5fce53112779bca573954a
- g_{20} 71cb2376e64839001ad1bc7e6d4ea099d49e2873cedc2b3327c5893eab26b73531b2af18f47bce335aa36364c1c97184a68eb8aaf74cba6dfc0eafdfcddb5f8ae9a6e93059416d206f47710ec47273d30d98feb24627d6e138346701d68e8edd4c2e4667b115cd8185a9e02840546e499a1c193c103ce5b1364f1161c87ddcf4ffea650e36ae952a4a7aadb351a196a7fee0636de546c33b90970cd9ae3867d875ed5676e8613b88158daa4bf3db51bdbb8d6121af48f2c44e2216405239921f1b0deaa09ac289a09ea038a6cc62c288e8ab56d96cb4eef5daabb1cd96bf20dba4253ce1850dbfd87e98131a961769772efb7c29b210f102c1d285a996f94660
- g_{21} 24ac79d4bf1f93b92ed7ec636d2cdf5ddc0f6a5c7aacff8164380c52af0682395c24d7f51f0604d09997de9f09728bd90f2df028128aca80a983d0454912670f0392deda1cdbf2b3284c34eb5d2f87b7d0f94a63aaefcfb97eba7cbb8b6dd927137375e697d7059ebefb71d8e90c1a3dcc169618c52002cb7823d0cd9fc7842b458882cbab04accd79bb2cbb9782384c930a6b18055b9d3215640579a71d1ce868c43db959a9c0b4c76edcc9026d43b370312ed9e9ad4f47d50430348afc97859e125f5f333f29085773173a6da43dd356c2c60d951415f3eb9ea6d6b1f5095c07c2ade0338fbc038d14e3fcaeca7c699a2559332d6fb474fc806509507e931
- g_{22} 67d44a1199606baa4af7f7bea8656300e48e4d224059638013c3d10c38d8f00d4c4d2ee0339c3d8f6a5ba39d61d78992385eda39fec792f575eed3ceed326752066942d94186b8837191b68ce751957404f97560c8ac537fa2a3d5ab02db1ad6a81e8aba19ebc9031625daa70ed6d816c93e69811176c8b2d4106987fde0ad3cf08647a21d1f1aba970d3562311e07b8441a1819d1fc656e0b96252a2726ceb299597f8805ab395f04ca0bf2b029febf95e1dc25114d18d1f8b74276579a982332d64adb5dce5643a7f776d349a34850e7517b45d0b36edc5a89cc62e489a867c046eea19ec4f7337c9b89116ae7217cb6d736c0b727172b90748f52da95c4572
- g_{23} 3cd021abfc57bf0d66198eb5f3a20af03affba9819a5bdb4e3783d2022cb63111c679cdc3c06480e88d6ad72fda423b9719aee5f74b0874a7ea53f23ee5b9dc07179727269f563a8a48b564196ced7b9412d8e3a40f17ff458a456b71cc7c839e689a67ed6e8e226a5a8b9aa002cdd774d9f6dc03f237780f1f97a7c003397f7a14d9ed8b01fae278ac43fc2eae3f89bb4563d0c21ef6bd67a9e7352ddfc45c488252c8ad1d65dabe33edc03f7694a2fe7d1ba48c6e0a7e96aca194a23f799e5528dcd99e4e07a4796bd6463bcd7fa1c108da1c6791369e1712672a04e7ba115d9735dabaf676760b77ad74fc6c0f36a45e051f503295822c439de260abda51b

g_{24} 4c0e01d5cbae889dbeb06893ea8a38254d4c2c75fb13ab1273c73baf48c1bce844f724e5
498cd6acee990f2c1628169572ce50f1f188138e56dcbead958caa5001f588a35e0f4b37
3aacc169222121ec41e33b99cc9ec57a607bdaf162961a3080fa75a99a3457a41c88502f
541c0d8585f9d73bf4497b7be7e464b732c3a3d5e84446b8c840024b371b4093ab588e95
80125f4dfa6246824caee9ad3985ea621e56af2cfd684cd5e7378b7aedf687e5502269cf
00b8b20f240ed8427daa667999922473a1605284aa178790b9485923041287f016035ff9
ff851483e0db38eb7c25a3bb5a600967f5f4164cdb310ec28602d18a22b0959a944fd78e
66656ff2

g_{25} 5f0c334aaf9722235f9ab3af5323c27636b0a71a8b5f7316183dad892b7b1b22934376c
c4b485a029195511962036ef10159cdebdb77a7607f692bf17c0a67ddeb254265c89de7f
d0e463f33d6a6442fa1235eac19792e7f497750104980abf39e2ab1cb43ec2f5fbbaa47ca
a9ce0f1b3d952477a469aeefb39fc50af807a35b000e8f196dfca6d58446cf7e1c8d8a5a
0635bfa880a6934247e16a0bc6dbfeefd4b994bba8506c0a8602936adf728afd3dd93d01
d3eae2595a8c49c1842786a183adb1ab8aa9a61cc8ec74c9bd6c295150d9d8a121402e92
a4eca3868a56f15a417f3dee07f6dd3508304e7b27c2b1d43eed6d1d71763e413f4609f
1652450

g_{26} 5365ae844436f2a05bedb52cecf66ba0a8e825779522bc58e73970b9b2b981b4461c264d
69562394cd9c8646786ba59d4547e76b80243a9cb31b2782fff5b3d947f1ee1d88709c08
e13fd050fdb4cf29108d6e04157945582614407d60f8b39b87a649aaa2fb0b31d380a530
ea5cfaa6bb126771cb0a68b5085c577f5e66c1fea33fbe9d604415c00761fedd47e5e4d9
462c2d340e7c3058cb569e0ab32ec70e4e4e4093458f395f95e4570cabdf0766e3c474e4
2702c947695b26a691184d0af2d4652439a219840f25d32cf6e5914d7af5fd6f93cc9116
a9d84ee1a2ff6d040d3820928c8e87d3f66b1970a1055b3ab39e025daabe2649b2615e3e
b1c49df1

g_{27} 4d9ff922621537b781bc5345e882a666c89aa3401354ea09ce2a63e70128e1c10fd79d0f
f529c775386e94611b4a1c7e6237c7fb14757a37fcb9a9974a7eda0d975c7216008c59c6
f9c772ef6cbcd445120126c4864eda45c513523a853c5bf2a0908ffea40090c68febed89
4e32e3d9f6c818365f05a7fa3e78619aa9d67d5edc4471e1acff94c67cae60872ca28b71
78d5da3efad704a36e514ed40834980ceb55a2f9d091792f7aa5d901fdb36709668f02a4
e3809111dd9b4668094fbb526bb1691d56c55979559a485c52194dc7ca6d575cf8f3f41e
892bb0e72528bdc34223c6b82a207808c1db325535a85d29f128e293295efc266f158974
d1e2e422

g_{28} 652f95e56d98bb8c8e36edcbb3e94b27e8f5efce3472c9f8b1ac52f880eaed16b11d1ce8
e43ed485edcc6e898e8120fca10aab6bb4c98a62a0004d856536b30b176a2bf318b37ac4
e22a2d3c36137913acd01e951ea890a28a19216cecf335aa7e763092442b2492c864e0b4
57f77ea15a35e50d106a1c226dcf9a939422a63e4254f0df77b4d3685e2075ba03830fdf
83b94df2b754d5bb09a86a3dccc59689fb9fb8aea5e9e6ce7269423bb5c6ef4bf4144b88
65eb222a7056031ce45cda8ad5b5f09c158d8a5d76c6491819b8d6a0f567b633906e8207
bb6e030acd1af6e363f7f86203289a866ecb8933f4d1245360a8cb22268cd0011197bb94
825c3057

g_{29} 4637c6880a3ae0520cdb9447345713fcd19caf397dad11950abb5126a52cf3f77f74176
42649b1599150b4979b65ee5814342c24e9856d54f9ed95bc48ea03090b4c1ed01aa6c88
604ffd269eac96d59ca15a76b29107c4f60f127a7c29442d1295d45caaba459103413444
e830d5c44f657d81f41f58b0514c55f6b922ef979ba900f9d1fe8322696255e860714c0a
1dc0d8245bccb2e7bf68a53545fbb0fff51cd6618f0f44df2510a5640ecfe840be49355d
1caab68c17908acc697a63ec70525792bbe47215531304920126db27beda03db640ec2e8
936fda3c1d293050874152c5c8fd7113dd142cb1c2a9a015c9145d15170a4b37f03812e1
ebee026e

*g*₃₀ e53dd59dafd6d5cf96bfcfd279838701f3ddbb4afa88fd85bbaf8c9f356a900619282854
e9d5aaaa016253672e42a0a7b7ab0ce5bb14c713101bb4233f598e803e032835e0b01f18
4567c55265d0b9a7584dd7a51743c0207640f758d866aa6aa85f0d0053a207942fd3553b
0b94c0ac5adcd51d7420a8063b3195d0cb91b85acedf975413c10bf958f6f7ea9bde5363
dff54f609c084f2c910ffd7d70a385f58dafa3969bb8e456915df7626a787160b04b21ec
4521a6d63a908531e2f578d0736c2ec3161095b90439160992fee43a7844e58e5c0afca7
cc1fd2b55872728a4b4b9d038f9e38cbcce138d117de16672e031eac7a0fef2569e55b7b
f0b328d4

*g*₃₁ 1916c671b85f3a642b3100b3a26a2aac9bb567e669f01a4b3c7930884f04b86090b6541b
6b0fbbc64a264058ce8f65eb7aa138f6e93b2a5870cf322b395c61a2bf773ccdf07af682
9c5a32e0ae2fd0656586c618f15605add76706aa48f93b5cac90917c62f5a87337d9b9d6
185e44ddeec5392b4543517a750ceb84e9e2e7a15d49da9bf074506b2f1a20a49812feb6
e0f9c681a99a0a16cec1c0a038b8c8f894dce32a697595045a92c1f95b5b03b277d8bab5
3c3ffc6270312b47c47aaab777a54680ec13b2177ad5139e914887fa749ab81c3f8b4843
13746c12627365a7037454422bf2139550522f75994c7558964a38e8816382bfc3097ace
95c15744

*g*₃₂ cdb208f5c6910a6a723802dacb2cb7c1919bd19c96b70ff6113986b99472a8245933a0a9
cf62556252963d09bc19f6d00e4447ab228e202bbf163580fbd999f5c73b315e0b5b11b2
694ba55f8abbdd56041edf4008100ccf1c4b139015ff6b88d97c05e49d258451888677ee
7d4e945e0e87ae900da2fd08b56d80b95e008cef08c10a330d7810d536744f7bb57bf0a4
efb4aae8a2de50e1d660113a7137877bb5e2b30fd5ede3bca911266e45984b0ce5e7f9ba
5afcd9c95015347b04d7c03f85dae5d85b4eb439c3afd2336f448c288781902b7562ebee
a6ae018ae04e7ee904626bb6547b7293991c43ad4d3f306b203a40137232fd308a7476d5
2d13cbad

*g*₃₃ 91de45b520104797fc3d5e853262434f3f05da173292041f26ddd46378095e7ff012d7e5
fe27647890273127eecab952f273a0f30eb9a67b1203b295aa6010e5fd0755a18d53e034
761b49bd9ed297469c561c1e2f030ff6b403b5978a498f926ad9687f668c179aa3b66f34
b4cccc93e8328adf50aa79b84a4c0166bd4729035e618c92cb4d58a983df6815cff82a25
2a6afc9b4750abdebe242b9ca000c3ed96c4cf81e17918c2069ecdba0a0ab32a6c8f093b
9517c0358040949a938dc64f49c80e5a3a7c41f249d7cec1aecacbb5921e412f9efce6829
e4af7013befca2e8053a0ef9364efdfa4391c79901bc73dec9c7f85cbdd4aeel1d7fc1362
2b7006ec

*g*₃₄ 7288ffff90cf31e8ee7e7f4d1d424a84b8930c47e712fa507250deb0562474e3b44ac0ab
2b4ed149e6ea90fdd62ead7ad52055cde67318c9c1d78080238c040c6bb02f9a7ea96c73
3884943b24ced763757283edc50401f0b070e238241115a8e463e1332ce050646f96d7d1
6f5ca3c506aa534447f216ffac9f78e23e8cb085416346d0e71db995f5fa565aecc4c99b
46e36cb40195e2f46283ba06966b52e980e4c25add9ee17d4fe0435bdd9f4b85f596fc3d
cfcd59ce7b9bd2df84382183a4e7dc962369e79d8e78cfcfde8f4c7d882e3399262d51e1
b38a3bac6eb21cb1dfd42a997429dfe22a4fc502ec3d98bcb06f311cb5f96297d8d7deee
8cb93edf

*g*₃₅ e36d796e6bb30ec1676b22c6c64d580c8ead1698dfbdd9b30498ced818256d4e2e25753b
189efbe696b4bdfb0043b5041bb36f126e4c0f525e9fc6eae74e402c32ac5188bc239fe8
c8914ea8f4366a2a56999174783fbafbb8123e4fa2bd6c682dbfe0c9192657e3659b5b6b
aee31477bfe8337e99e224554def715ca4964447d3582b3bb02c15f90825cc2dea1b1eec
7196382aafaeb78df75e2c2129029027314b1473c894777a60d091b8af1afda2dcedf637
d75c5b7d6c88fe418d6cb4400a851bd17a1d838a6adcb8ea48e69a210ae7800a6655cd9
fe85f5b4c3af39a8133fa867224f65a57b37b2de445ef0499edb070b14d83723f5222a00
4104317b

- g*₃₆ 22daddb1c6847ee6c29e558a1fb029ca497007903818e3233b532aad2e2dfc2b479dcc8c5722c219af8eb3402e3f4b1b0ae7c3fbb72c4f144604cf2cf3915d4d4f8efb1d392c2d353e06e4d6d5def66b2fbb35888977cdebc7a4038fc9843880a7204451dbf7ee89af9fc9914c68e9a4d8f012ca73e7975465e9ae27e867f65563412f7407a04982977e8d6512d044cf1f4f06e271cb0cae64c108365f956325b2e226cc59c353b5eed9a968b60192effc20292b435242d0a094743af0a6a1abdbf525d1ee8de5293c650f9765c38c66e328e2aa8ceb0d29285084e2addb0f1f5548594fca0759e2c48ff6f6dce578c02ec3a5cde913a301864e69a784a20b7f
- g*₃₇ b6d03b7fc016dcb6483cfe00fff6de486f84de1e8226825416ae5fd895dcc3b34e9080ad692abb921a6b6c0bd9c0c3e8125c8dfcf114c038634392152ef2ff4ccde150e4a083e5560b4fb0211b2c1d85a37abeeff846ac6593f2273e4db0806f278602e650f15e102bcf0d88d8a189298d94cc1343219ee34030b947c37ede2f14597afd084367d600670db5ba8c41023e6e0c242d5b2adf41dfe34cce1088f292a93811d787699e2c50e113ed5e2a99ea1c8c878118540b2527cb1c6aec2e3dc5fa2752d3dc979f040844204ac1a05cd1922701b0dd1ae2964b905824ba2431f45ce2995308acf290b944a65e0ea95b6af94d614a2f38444b49c85f8ff2bcb9a9
- g*₃₈ 2e232340e5b6615e8a25139635ac30bd15281820bb068f8de23431c520e7c141c4f271967ca547230a7144f6a17dc5bb564825786b44025b5fb6af06e655ab0e5e06f7f8eda7d04e31f12b31273dc04158fff6a7f30358208b63b3609dffcf3a2ce15cbd7870c497724b0f1968e8667177a52ac56840e3b2065bbca71fbf336ee7a709d61695ddb6513c22ab7b4401b3cf32e1d4fb44dc647594830e35917fe4f8d59fb95bf4b515b3e06ec7b1198a707ad74733ebd98791488eb890265dbd178bef121a329225c7156ac9be015a398abe6be544ec3b0d9a0b1e7627eec27d4cfec88eebaff402b5227e96a08ca49573bfed27c318238aef19dc4c71c6939ca9
- g*₃₉ a0ce5ed6c778fb18ceb3a57765470076c62b069cfede8dfb70e6156e36f70ecb7a093cd475fe87667f86946862267660dd76ce2fb680a040d229b0a0fa28527d30d3aab04d0f1106b2237729f1f28a87f2f167b6015018c6945089654c93da9d65aab8149e20fd8277debad980428b55540b71c995ea3b87d3a45234756672170aaeb877ebaf3e03b2d428d1cd219984712d18cb76d927e39fd2b788136c08a8ab16f633b99c712fe10da8683e73b4edf83c368a08eba604385b10441192cc076a9740364ed63486f3a46cdb25ef0b5120ebe54e6aa06b4c60f6337d3f566994784882093932c963473d4c1fdef100e0ab9ae632364417f7b2c550df6b48b347
- g*₄₀ 1b3ad950ef15fe8f1915d90872900fa14eda2fd2c431941d70b3b8ceab96999002d74e4aa0991266cc791791604ec09b907d253517e7a4dafb9bb16697c51c11feb440ba411bcfe8d0271830e5118bd85a8421bdd45d8e96cba9454f4f861224add92e1a799d36dd295af57d94c768627f108bf8a3ad95e76e2443c162042ce464d44d7ef915d9ca4cdc7bac0081b991d47b9618c5e45e91412a165534a5583f7d7fd407936b2daf3f6a9f84fa15496bdbb85f655b2afb7215836af1ad9f88c13fc5f0a29d3573446ae1b374e242c4e15098176f3a3fbad5a3b7bed3119691493b48639d87faced853d199383e591f9e32d46f6f5b72a9ceec8335c6003784a7
- g*₄₁ e2d2ad63c6ab014de42ec3a2f7e5db70b7fdebe03d9c258f19a786c89211519c2cfbc9fae0a82fc957bd42924fadaff20e22d2842a330158691cbd2f15328a521262a578ef309e4332ac9504f019d58986f0791fdcd7437c3f7b4686bec7521755dff3e11493547142ca30b85d2589b96aa37ea67ed5152e09d07a2e85b8e0491d04a1769046525bfcbb86f897b9036887effdb6fd86911c160a6d991be4649c9b35f28efcd2d3da929a490d0054897d24228155e0cc190d2e280c0e4e8d1574704cb7ff5c6107a65ae37c8f8036bfb587ca45db30480a2fb89bdb305695b227412e90b04554ffa40bc27b8efc47517db9fea3c45177c5ef721876e9fe40662bb

- g*₄₂ 81fc66ae02d11bf04100161bec9eff07e60809a466cf492d06be233b3045ad5a4b6005ca113e688e20419c52b4f23102552cc669403e4e6f21ae203a82ddddac05c166cd432e2a9ecfa87f68c9040fcd0b67b25a3b1a258decdf3d2ae56e6035d809ccc406e72cc02c910f809d05dc6435bbc00a29d2ce2d0ae31c7f1557b1d9b3c68d17f9a1b0e2ef9bac5989a8e762dc2b96f95941fa2aa4069b99402643ecf8403269dcb121b1e4549d242f86299d068e3cbae6e44a8ee67e113840a9503ef8c15cae828e2b8ce864bb7a5087d8fffc42f524ceaafafaceac343c0642c9242f0b46001db9ff2ed2523c732f041cd303c7d99bd14326ef5102f8ac859a4264b
- g*₄₃ 2afe920b1f3a3563729b149ac7124fe8bdc8587288e11179a263fc3b688077dbf25a96e03deebc66117f88b900ca24dae186aa9fb915f502a1fcb40d25a4e84a3b961c03a311d7f0a1ae58854e5caa7959f05346bbb933510b6cf38110e25c79edc223c9179379da2b97401585e2f51847d094637c0e581c19982d08965c0d52cfb1094e765e0d9ec702eb2e436080359dddba25d3894edad6d914c7232fdad22fcba182622cc1f2a50dc0feeea3475b8aaee86b13a5ad2d8bbcdfcf0fc234d0826d44f12da171a45443e3ab012d8b20af1a119b2f4535893584c6111a9b4318fd5f707e1c79f5ed48d980abfbc3353e42d7954c761df2b6f5b808335e571bf2
- g*₄₄ bbe4e4b8c5d54cb28b1f1b5e4d7e633c2930300c74275c915f6ec7f82d5149923b711928d0eb5962cd7341940adbfe3ff303ac00bb4d3a1e2fe7074fd7af339cda5e99758abad767d9feb1ec5af37d3ce942a7d4e808c19cc0a9a53de1b5b5fefe97fb53d6c158ca3e2534972821a949a69d1bfd198e2ec21dfe4bb672196d44c5a5206af444db247de59d5520372d46c84593a1d4f966c5db93c3d20ef8e6b29d3eb7d45aeecdc91a1de787037196cb27210e20353812d4777a341f411ec9ab66a128b4545f2017e3fc1b86c8ed18b8a9ecf9f6e20533c79fabbb8666f46bb3ddf9247d01b1a7a1c4b6d6dca0ecb9a4f5c0a33733d30d376bbfe8c55e50205e
- g*₄₅ 92337c39b3f221b8a493a620cbcb509d378c88f7b689f81e4ed3cf9ba7e3b4d02da9d3f1245e2afd2bb347a9272ec2af1d5454654bdf6ee5f26258b8bfa4780d8a126b966c68134e74974c3837589fde57726bc5aa7e21f70b0047e0751ee8de613cb22f1b2f8c8d60fb190b0c6d8223d438a7a29d9690fbc1ab576d1fda6fa17de157cd030dc3d19efec4283a246c31b6925828e72c63380a0b8e055cdc5926a3a5db68fa82740dca8181f8b1068abbac122eadc2e21a8efeb323e4577d79eb579451dd1d3d3c9d9907cec5b9ec4e137eae3035f414a52d71ae65f765e19705603ebe0ff216caalad6e72d5c95943db2bbf1306893f412c01f83ee684a2c35
- g*₄₆ cf261067a85092e7726ec2b89b6e3e74d73d4b9df7bb16e1780201f6fce2f7e786ed09696100867419099c2ce2da5644e313b3ab435a198e846da930ac6de5af1100952b3ad6d6d754e857aef43372d5197580eaf2436be2806eb5a48f813f96256faf71251ba7f68bb53123258c0adf49d676e49d29513faa5c3ab87b6d1e9e0dcde6625f842c0eca08e1ed011eafe6010b86bccf868ef02db9d6266e7abff82559aae589195212f7952d2907cd2d2b524b5229469bad962faae44012dd800c1a82754a470544897bd822a37b31ad253edb038c1fa6fddc59fff7619ded23c1d35496d72ab31e5be0ca41d1c29358341118ece8e00c81e8ec497ead0a3083b48
- g*₄₇ e0f9a0ac36e271ddb6f61d1d8fe7eb18dd83decba7ac6b4d11ed36a99b487d243be9057edce74ab16b76bf5b608d5e35109444b94a7b92a669c010d18249b26cc2d27fc7d2da0ff7a2ae7436d5ca2f63b77097555bf200e54cbc977d2d7f36a0b97faf53e4e56e6d24f37bdea537b279b2e25364d27ab75d961c89470f9a0d82f18de10364419886423d35ee13fcd60c601449f58fea951b9ea0c4458765dbb0935398387e5877859494334c18f58f73ebbeb5ff0495ac96f7a0afd6016028a370eb155d31a4109a157ea31ee223520a8b53fd1dd90e454e1171f6b6b145dd44d3c1dff52159d0ffa0fb9f187f5743732e3cb88917725ffa096ad148600419778

g_{48} 3a6d3760ee62e43b2f51740eeea2c537c1e9094b159656bcaa930da5c3180c0618548a33bb00f21be7948645db50c7fb7e8c6d8ec20da55096b7c9762f4991aea4b5a4f171523f272f7cdc7d43a4d735119d4a9a6e2e901735dacb35858b1d9b0953335228e6a3636e01e4f18b178d31a8d6e2334333d79592663c8ad3f7190e9dae22a4192e2eff94f2d803b7335a999ac6cc0f9174dea082d0043b9eaddf5839648bef578e6940ea18e698ab40e4b6f0d716e8688358209f8cd5d1f8ba19b2cfdb5cfa2d9fda5b3dbd2bbd0238ecf9f69126fc4785054e5833b619a67ce7fdeee618343abe7bba60b73ddd70702adc94599ffe8e8ef6f409475eb0510a1b5d

g_{49} 62453773cd4614914205f351443a29fb27d9365fccc35b204ef2d2c1a96cb32cf2c49778e2e86b49483b1f89e784b3cd8baa46b264c902dd30853a3ab99e8006c8c47490b1eba7932992a716e51f1df283d9b2fef3fd993faaac08193505592077225502b119c582a7733dd4d54b7952a77e35854f72cb81d5eebe8aa2a9fa38a9480a5dd27a5b60189eabf7b6fd8ae1f14917718faddeac9b879017d7a8ba411f02e7e7686e39f07b7bcbcb705d943a1af5bb08e057e3516919611334bf1ffec7d7aa9848713986c8e693394fe2ccb1e3b1e3ee2bfaa6554acfe6aeb22b0f3580d25e604090f9b2b9449f93d027b559f8282f83a86e228157f5b0b9242d7513

g_{50} ad2b486bbeb2c05f2b26584fd03b929b300331dfd2b1089a0409615ad7b8578311350f390fba0672e42d83a71aec370bf39998913b05e21d2178c51e85831b0bf5d2693a8ec5142d44c6557b78487865ecf849f4b6e7a702c37c8f1e50f60b740057c97746678f96b4d038cdab3df415211864c9efab10850e2df55fc3422b218692e3b5ecc2ffc333b914485ef577f643a7739b0797c4de194ba6c19e1c1fc64f2d30ab182cb88b910b3c609df1d61dcf734f7d7f0e09abc55bdaa25bd0f06c0750ced3426596a21bcaf441ed1e57b14d657d78408e23e56e607b8bef016e8f7904e30789d37ca2b98bcc126ba35859f84b70518eea5f12e05ff3596c205b9e

g_t e7bd5ba14a14848513f5e56ebdc623f20865479728dd01e18ef920818f83d364e165ecdb12ce11a22ece2c9de7109455418af504ce4592dbc7e53a09ca2e47538dfe3de8a2d1ec7b983680d7355b7474642d2677e9e8c2efd6dd120c9dba69e1dc625a97c04ddc0a1de3d90cddcf8118a7292af2902f51121ddf5cf7ceda8ba682aa2414d9ce9f7c149675c3d1f2df6b1039d1c3890e5cf93f637fc9c8fffb55854378227a47bb77b183e343abb2751d6201243b7f2b4835e97dfe4c9b6edefe7b9de064e063ef9f7151bb35231f3cb70d4fcce6de2de0a354d57750c8b8fed579fbbd22976db4e979b3eba3284e8a0385eec44afb3e8338c0df2df2ddf787f

2.1.4 Device generators

g_d 487813c6d3efc50b646745573142de47649cc77789aa545d2fca97e9e5e94639810fda34e77cfff614b3a86715c7ae093a1070987b183c3c7efa892e3dca1f98fcfaa39e1d649aae00f89473db7c8cf92037ad771fc464cb6b76f18325a1b02ea41d29276a1cf9b9bd7b25bb5f9a219ab022c7ab8d25378bcc7b9ffcd70971c03d320fbff71797338ff24007bd785cfbdaaf4bb219b079b96382dff211e23f554092c3aa8af79e8a60d21355e7d026b3c8207fe4feeaca8a9a8dc5fc8333817c67bf805bbe0c032b10839a9026ba9c9bb120bd4ceebacd3152b66b256e41e4a06224ba3f2d3ab99a26c364fe822c0d2c5e972545c2572561c795fbb68a34018

2.2 L=3072, N=256

2.2.1 Naming

The set of L=3072, N=256 parameters are referred to as OID: "1.3.6.1.4.1.311.75.1.1.2".

2.2.2 Group description

p f302620a44e70f14cd3b936ad402fa78932d1e84aaa0f40e17866254a69b867e8a6f27dc893c864c9da7d35874f0b325ca8c921bebb62a14530340529f3ec38721115a109cfc854d2b38e54ba6ecc7df617b0121ca30fb343e1bbbeba1cd25c68d45bfff102577b408e85942eb6be03523b3740a1d1c9fc7ed5f25e0d488a30d23b742b5e92698ca6ffec92f0c93418623a9a631063a4744651f278ec11e020df9c1a6708c52ebe6a2cca1c69ab7a718de9b0914794f09433c1069d3416c319d0d64bf2210dfdf9c0dad1fa642fcff77f46b677a3d89b84c8feb37feb38aeeddf6d6ddb93bdafe6930853a09c9335724ff020999cd57a3ffeedc0b79ba94aa4c78bf92343cec6cb083f4e744bac259d9879e71217c8327d5f6acd2829e2d886b5ba45d8b82ab09b2fa9eb9a700097ebcdc8910f2417f8db79266ada666cecc04585ca0186d2c7bfeca517b14c9d11bb527a613ae158831283ee1f499504bd5d8cb59313835362559b1af022d9287c8e9536f7834106cb7ccf4162d14a892939ad

q f2057bc96a4f5b6fca7ac1af653fe76d07c19153f6258c8a944c527c5129ebe9

g 67a8f070dc595361b73504470553846f1e9c5eb232f93ad781981757f2d9801398aac5ad71e1abe92ba23d17fce48dd8c94ed4bc615f6d01880fb389c3f9e385675caf2f7a092ccf6fe39262605b11a3635787fe5ba89859e52fd88ae3b9bb5c87e7bec10eb510dc47a05a72865c1b792d29994fb70a8abaa148d23ae5e277bf5bc2649e521fe9c1aa58a6b81183790987d1843d47d3fa8957765480869b3c3d2b894283d59deff6918448b5d05d8f102bf9748b0f56969e87378c698431c14f3c27e3d0a4c3083b2301827dd66631b2198c3d05c9d4478ce34828a2496c687970eb81342aa73894198fd86714112cc591088a5ad2fbbb270c46164037fd2474a0995bdd82b5a21a6f4de93900d3c9f106f41f81d63709bcac3cfb5debcc1dfeeea670ab91f412d98014109d69d317e6004e8e37c699b90bc79dad8a09d374809dafdddd3710796c5ceabdafaf8f243cf0b6840c51791b3d51936bbffc6b84339926f10ba22b23d7175d0ddcabde8f1ca0d4f095cc7540628aaa96273b2ebd7aa

domain_ 31f2d6cfcd652b7db8186e849df14b7560407bca0f0304e09e0d9d2c03d4fa4c
parameter_
seed

2.2.3 Issuer generators

*g*₁ 1a5c96b48b68108c86d77160ecae34b11249b8faad004417ed8b77e5c7d86e23b023a99910c0d553b4931ecec200bfc615f5848e82a5b44f1496d4d94c31b64daa49ff3d21e400564474f21e63ac396f793bead50c3bfdc62ca024c3bc5a5a152616900b119198dd97500f3c323b784e1e82ea4dc679475ae55558edc97a01ab7642e9d847ba94f4b39edbd39bc9e7578bd1cf8a18f02c15112727604ead983356f3b808833746c129152ca51205a8e79d09045a314fa97e61dac14d02b4a461b119506d6b0dfd18013d0740f16f7db1a24e9898392068285d5156fd789cb1ffd2a6de57aa96416021b947e510debcad48ab3873692353c573edf055d6db100658fba259099259338c0e1725ea3c782ce57c0fc5634603d34562584843a7b73e1967809b7eace4a326d911710f8021db182f12c265b6f4b76e981ed331ceafec2c9b91eed8e0b53d100216cd543447c604a416fcd07700948f3a0446d463e6c26f411bf15eaffff41b2b385750c65dcb829bf3107691e1a9e0c2755e78f645088

*g*₂ b8609fd5884cad2f536e5d58a7495607aefb40f202afe91b8c7d0497d55933b584a60ae8166b8747bdd998e318e5aa3a0e3d23ac8f02b5bcaf09eb866472e238734d9c14d5d210d8b7b2b204b114050575ab0389b5f631dd5da1f7ea7c2eb58df297cd10c7573140416eb2dc3582a1c9690c5dd259201d3f9d897b841c546f00f2ad20170fc56a287675caf0db6cfde38818302b979990b253082c45734ff46b09fd7c4b5923f4de5d51c4f75a5559ba5115624055e98e392af615d8f3be9ac9c984b4759903d33c3aa46c15bbc6f5461951b6e49e1af1af6cbb615a0d1339c590ec89ba0752fa8b0b347f52ecc5eb6c7503efbe4d2dce391ed62944e57af6f00ae39a49641468f4d49681fd44c428faae145c0bfbe7530098cbd8d06ef9b7e84a0dd45a51d5d2b447cdf1dc5fd062b7c772b266e3ceb1fd0c6a75085f7a6ea02a663ba5f7bb069488c274013d06f439afac73307b213eace3d87a7c02bc8abc592056421bac2ac9eafb57bb8d130a4d90bace0d84c4ca07b6caf3b4892e271

- g_3 acd28682e90130aecb97981ff5fe559dbd431752f6d625a2b143a203fb1312af516c994d89fd63157dfa56cf65159f029908febea7d729883f73787c11fb49d4448a7ffef8212d098b6289e27bb324a99943ccb46dc2da66bd8c15552c0a57ff0a0c00874646889a75c51c334ad2ce39a55bec1f0cc7718ffc29a95b49c5e2a9c0b911aa16164f0953277314d85414d0a64364c05a5cf564035350f7aeb1085a66d1234a296de5db79960d72f181c3ab166a2b77ffb06d5ecf74b5cd89b66b481caadfe82623c1ed405f61be63ab4ca87887d2bc1a958cd7d0b1695eb2880f724d5b5fdd7c0afa955532b77a4892c4572a4d6bab5ba0417ffd524a59064aa3fe2fc591dcc0c991a033e9b9082b15d438f5e9236a64d5d88638a418ab6ff4afc6aca14048d1684ac10344e6740ff2d81efcaaa09fd30889fb3833737c60d6c5436764219518f9859dcf12f2406ceebc2b733c0cc88cc59b6697207e0a1de3ba89da4456933ff2f8b8d15558518044f92054fddfbdb869f8577dae2b388aa14182
- g_4 f06f709fafad172bad2ae0a2fc384648a7a3158357af4e57494af2fcb41640b88cfb66c190f9c1a7f6ec4ad1924f9dafd504ebb7e6ec083dca88e1b9900b8fca32a802c3e53aa92617ba87994c1dbd26758e38b6264bb8d2f4b6e0456e19c1e2dcf22919602e8b7553d8308e711def40ec25821ecfe7c937332d6212babdfc3808e6d8683ede53d3c052ec0670eef780c0c38be75437e7d23b8d0d9e2873405c67d139d22f963b5861dc212f22050a273a6f9ce9c9d31a5021a5f050b3cf4dbb997971c0ab0ddd9e10fd9d620666400446387b60407e66caf0b6dc26a2386685efee9f97a81f62a5cb0710054f612c5799267c8615da656fc9f1b73dc8df14fb12c0dffbafe2ea23b9f9729fc325de843a96f51d3d2559f746b518bd929530319f388ff90cc8c8577a73bac17bd248431304db25641b50ba7086ad6976716779a29eb44b141c0a7a2e970a9459f19b275d14bccd637f2be0472a0e8d5090eeb63207cc3bb22ba7d3b0038492f13c87077ef9e92f219547bb409f612a63e2
- g_5 1c99659e1b83c3c02387dac30b3725b5af3e46715e5add6a62827b68d9586bb221cddd4d23dc3162f6b6be7c2ac325fb2404455011f05c7254a019d825d9ed9263cbdfcf3cedcda1747570c7f88ebca3a6303d0579080191117cd98c9aa0bc3159ba14242288d3cba1fff92194e9996d5ab79966d3c898833fc6566498597cf96d04c745e1404b2ffa95a2c011b3f4f671af0aab8ade143bd958af43cabfda5452461e51ece3c7bbd6ee9ddd98175c30927b5e510a606f2b77049c4c0e189dbdf1f8ac0d1d31b7156aacdf3d061a4a8cc36e36019adb1a55313860d1a437518c3953f84b62ff3be82af4b9b292526678f336a7d359bf342a652e7318f1b1cfd41dd5dfd8414dbe65ef588bbdelb348f8056caeee6bdf026d1b3d5d16211defb74e9da11b34b88c35d8ce713234054e18b7d7b044ed760340c81aca9ab5601f350d9c32b3af224b465cd79cda05b857cf90e3e600cfbfb7287ec4e1479ea044e685fd0ae1f6483248da180d94ec4c09b2a39896cc42f5d0f69966137732cc36669
- g_6 a84fae8a8b8e5a973968c311e33d2de4f2bb0b86bfbdb955d2d6cbc4c828476fcb6775ca7f0931190233fd8cc45c2bf94dfba567a82ea5798ce3023269b9d0e622583925780f782895288ff52c40a27448e93a89eeb2a53a06cb615b8ad86878f0aef9905ccaf4fclade222f58562dd101d925d8bbc415b815bad909190a65a7353f9eb3a6f03abfeaf62ed4edfed185862d28018d65c3f44ef9b8cf38fe9441b007b8bcca43b8f161d2bb77b39fe51ed93c6bc99f1a94015f282bd7a852a1b89e7d8237fcefc262cad9dd875a7f77d1a0249478bb2f899626fc20ae42cd50f4b01fdb93914ce683c3027190c3e4493a6665d65ebdel1f3574740604e406acdca7528fb90ce0765130d8ed6d5d0e540e873e9b94708a68675c1390a5d624858b8eb2aa8f27d827cdaaa2d6a9f2499af8bb9b3c454269c64c73bc2280d23c9917ca85dd5be1887cf3c595fd260d2176ea6f1f6177df5da527cdfa1ad4a8676aa9493a9063422b4fce7be1e17622d4a9f5feb1baca7266ab23d58cbc2eac7f7cc47071

- g_7 d1485787bb5acfc6d8329f5ae5a2e23c4d8aa32796a0f5cd2a21abb9a479653992c965d87760d10b023aeb0330e6504b30e9db041ba195ae2804ad85270de3532ee7544e22c464c5084fc3092834b2aeaa61339043d15eb21b7d7ebbf04a110cd655f31cfd9d863b0513944a15a3fd5e8b0d9ea7a0ecd0e3b5cf9fc8b234bf3ba3467ac3786fadfbcb49e6b1ba8f608e8156762a2b37c51b0be78ef5d177b3f1309a3d936145aaea99c03429e001d53cf9e4682ff1a53c34a39c1dc9676ff377a4f9ea1005fc0c96c5af2f5cb6df8211cf9b4591710b9bae8bf70d84fb86cbe9b61b363be6b1f2365c0f5ce394e4c36763ce499ed6757a919f0f3cad344ce6e433c9b2146aa07bad76999ec27ca51599033c6aaad8e4880c62b5a61703683cb8896aea4c8fb71f6ab53c3c5c6450eaac45076202e960c28e99b5d8f057d0015412be26589c2a6dd8f0149983d75f25cc44aef34e79f19845075203c326f5c4331255ecad6bbf6d80a273c4d7674c57d4581b3436d42ad7e250a73b4b8b84ed29
- g_8 875982088eed0aaed1d7b0f8cf5162bfda03f58b587f719cbdede669957135ca6b7df9bc5e11db9e40e9e7bc7806f4a4721eeea38a2a15e99d2afa50f73eb815cc516b534f5d1ea874522144c5e16d97dc1f6f42d3d92d345cf3f30be97d1794fca72fd9c514bdcdef90ca85d51df068db82229aec8a803bb11f403a81c2369565fd646b1b095eab9e6fffd530ce7bdf2483754e118976b152aedb5b1a0e2d1fc4efd5efd56c99a3d43a55c0dbf837e3f1ec1b02b33ee59298407b532237574193f2a58707b2a35ca882e02f45ba69d6180405197d9e54d616d61677c8562ce98d28d9cd84ac375b3103a042a73d0b4eea792e616927d550e4c8455e63d3f06a2462eb28c8508e0f20be128f9f717955a72f95d31774627726b8583eb67ac0842d6212eae968bf7c8d5fafc35bed9918a2a7e5560a0850ab4d92a2b8939c059825f7f5691785440c5a006a263dd5c1c406cc84acf2bef264944cd3b943e6789ffdc3c84f1f17d3d4ed9ef2a798674c9cd821322045fabba017a954b86d9ff9be
- g_9 12d10baaa422657e67b2ae7b075afc278823269d0804c16e3802a24abd858847039c232985382f20483e9233f80ac7eb75b49aa32c390d032ea751aca9ed79dd7c20e3593ec729d7c329868d47ecb04c3a6c49e232e0869ac948c7add6969966f5efbf41232ae2b5aa10421de1c688f37941c8200b4b1df5734e52b90690de2a6515636978ff8329aacfa219667935cf62bd658fcd875e47ea6460502a08047f516c1f4ae151b45ae59968f56b18d651419a84cc33c24e50945734f98fbdacc8cb9d08feb08300741570afacf98ef75b4832a96e98646cc9ba45aafb2be7f14f58f1257a12cddfd2ed916c9e789dce0b905c80ce06921180c98c6d4bf979d4044b49839b8ca62ecd04f86d5c7ca65bdd02f04cda94aacd054589c38875805cce37dfb87fb8b54f9f0deb7b920fbd62aafce539e9cc051f747c72a49b26d71863c26d0f3a662f646703bfdded5a7d44ae989d4412764e0880c0244b9f2f2a4b7372fc3901695e6a6870e01d1bd24c930c5d6fdff27294e45b55aba7886374e3c8b
- g_{10} 46fb5e062db7d1c8c192674e7bc051e78c13aa5e1cb53cef8dd5cc6be2d56ca2ad62235bf982afbfff440ba3c4750d488414b992a4f5ace53e41c7644231844fdb5e4b31a2e1d0702c68e774e5ca1711a81d9e5fe69d9d9088c3310c452490ac42f625a9f6183ff2402a3b95228d7aefff122bfad287523bcfab91e649f6f68cba3284c1c77e4c9b46d3190c1ccbabc0c224d67d2d980e4bee7c34f5454eb47319433830eb4e80ac09bd76c9c0516be872900a2e53f90a0e36cd752249556253fd81ff2ca1d4344b2227b96d8911f0862a26ea05c6fcc687791349e16d139add456745a032dc03195fb486d5067269ba6325fedadd6eb43afd9159ee1aaae1380f352a4d4bb4041453719c47fa5f5be50b8b675b206513b98ecd82c73345a985c2aad0857653adda26f89ce78c39adcbdf21f06643de50c1e1192cf004440cb456c8b14005c424d7a612fffd52e6c1465826bb1d6136dbe092dde5df6b4c8b88262e77ca4b24a9a9a41e0fb2e328f2fc366024f8364ae2b4e027ac7ce6f84aef8

- g*₁₁ b7cd497aab8263b2b45cd39c62ffe3e8c24221d8f49a4e6c285226200541f47fd6d0c67f117f93aa00c2b114adc7ab11f7fc6bf78c2e1f479fe55162a856d1669a9809a5911f685ab039d44ef638c2abde4be78f6b37c6af17076dff9e7d9646701b26036e8c40d5c81231384e6c40998aa4300b16e40f2b031bfeff0ccc0f31c2d04bd7c8d6b20e1cf57b83953e270595fe800eaecac416f82fdbbc7afec8f7e3e8d57e4a2bcc62033792428b8d38b31396a8b2003bd37c3a05e734db6f31f6972cb0a6268c09e0fd3624d45e8eb19525df9a0f6c81bcd439498c96110e50dcd428cd76d8544adf865936676bec781cedb8150eb58212dface7668c07890a39bde586d4aa61da710bd38a3ec8c584239667dd7b40caedbf55eec6f2cd1d16cbbd37dfefe5136706e74e986bd3676fd53629f6f1e72af63bd7f7760b7c06da9ec0e32cfa86db3a4380e81a14c37b9548b932fe0d1a51709a45b919a9f508134c0e2714d452aa74f547b1832859f968f62bb2aef3576f9eae9b09c8291e9970f
- g*₁₂ 689e604f2976a9df232171c7ec39a9111cc7b519e1922613bbc199bfa5ead51cdaca2cd304ec6d357320a522542540eef03873d2479d6b9b8d829ca87a635d1701ce876cf177d6ba723c387ff88c26381be7c109bdfbf34334427457116246404a9a81e9baf9ed036a13a1c273255aa0d227311a6c9fe7b67ffe085df7e52393fcf79165ba375ef36a0e51bd4fcfa578944d57a6f69c02170f120ca25dc21bfbf548e2df0d565e1dc00aba419afb17decfff5bb3971bf236e243440f53e28b2f62d2149c4cb1d8691302f3a32e9565f90d0d28de349f6515cec50ed5c41d654547d658fbfa7718a7a5e1c003293fbe78700c4a5b52b8355101795e6ae7b8d1abe102f3b0273a29f050c59018d3b3d53b4b54f23387121a9e2f6128b35900c6f10dfec2f47f262a10c58b1f8dfd9ca7c50cec9cd553609e645021920d6e6afaad416ee3f548e04458ea5283c1cdec4c38d5e4fc9cbeb226d81958cc80893b1b43c5e08d2962b6ae2a0128238079dc825e95a228bae6b2c0a3830b15d35243f26
- g*₁₃ dcc55e566b4c83d599cb08b0132aa80870f5b8865c43268fb91b2e548081fd7769b52201e81c37a77a6ce70a7794704665b56362376b55c21202738441aff77ebde67836c1ab2b68acd3023fbab809f3638e85d0de40780e8ff3305a6df62f50f40481a521074b879fb2f4baf77a0516cedd3dbd217d2e3ff0d2e8b9e5b2dc0343dd9508cd8b12305b08f0d5dac50b71c55f1fd367b527f5ba2ca799a39aa23a77cb5032778cf0acd67842caf158c6c01fab373735d43b6d30eb27a460017a89f2edffe9f47b0ca4997a896f0b40193b71a8b83b1ae1b6021fb68ab604df55a9de050f2620d775e54d65ef1c1b1bc875cc0818c7a122d9a1df0c204e07b94057617b3d1f370ddd505942b939cd3bdc8c8ba22a76c6cf97e5d16519b0a017f55a8e57f125865e991aafb352ce530c01b7010fc0c75a9a82b0dc8a10522052ceb4dc858df366aeed9cff291950f8a14d2806978e287493969d79e9396bd42ac2e18d8dd2afb8d9f717656155960587316bfba7b52bfad2c6c08e78fa1033b31351
- g*₁₄ d8f2af343c94f2c9fea00fbb96d3e76f80fcaa130d8be968983d11f926f40816c77aca62dc78376c2141b1e25a4429257ed8727f50d73ca8c26855e3bbca2ea7435fe68ee82f93cf3d53f4b7e89d808f31f6f0396379493e455969ec4fc0c1864d03e479aae497a42233ecfad6bbefbc9ba54180c6ce79921fe721769b7ecel1a198ad9a8e02fd80f46153daa236d30dbe4c55ae6077df98d88dd42968d3435b7aad694dcb32b2ff747e912ea2c7745cda21a5b63adc71b5ce4ccf56b13f1fe3bf74d5a2d67f865fd0689d77986fb730c9ac517d957fc4097a2e5c0f3e030ec1978d731aca54c765816698073d121f12d8455aa88a77542f6ce03d7712149342040d060edb2bd0a45a8538747950c003f5d05472e8d19a70d9541ed727c01f913fb05e4fe264a51db616028da9123dc4ccdeb4933614359f3b164641b9853427df6a8ed0750b076d50589dcf145ec1c0fe44b4fb14eb555dfe08d6b6e5408838c362d91b4976ec5bfbdac47596669834f45613e989677a45edca8d5bd7a6d47d2c

- g*₁₅ ed73a42bfccd2d5e5545183e60dcd8a5c0f529cc4d969d3b704106d2bb08718834e1063cc25ee11be6f5611188fcd81e33b11ca8b033fed3e70bc8d16fc4f3d7e8e30a318e1baf35b69f40988dc80473aa9cb42c2ad504d909e3641c0d096d05571474d30bf5f20a6842fb4c94fddcea3139a089f716b193838e9f030a178504bd27e239d5c475c80662f52db175eabe03ca343bf440823869b8de65a77bda5bbfb800ff34777e586dd92eafdacf8e932ba239ace02012dcd46252a2ef6596a3bad80725f0edf8acbf827f56b91d5fe80e2a15c649a6a2da8e1d36dad037eac6dc70d55f4c2b137fe115551b879157a00a818a5848d3589b66d0876dbbc55a60aca8d351c1a5ed7621e7ff04a14fee4ed2cbd90bc0a5e51cc007544286f6eaa44ea98f22c0c01662f8200236abd3256b09443905262224ec5670e66a20282198f47c3b53a22fccb0bdb64b58d445f9188e4852966c72f8f139825d935186c539877aa0d375800ad78b8a17943c5ad71d3f53ddfd2c45171ab35255afc5678b
- g*₁₆ 72f32cfa55146cb4abe6a426abf01802d9c0ddf62383d05d95b3b6c9280eb86f5a63f6bf eb1e389bc86702320387179ca90f4dfe93f44516f94ee50c777e8963b07a8606f756a68c deb10a80a07565b8dad08771468aac5fd2ecaae329f6dec6bd47d75f2bd887d51f2c75cb f8f77a372c199b26c13d34b184c96b92a1ccb3a66386d260abe5e578b9fffc2b0e01d03c8 3a00a4b9b246230891d59947f8695cde2c96ac564fd90f169fa5c7c92669807c16046b6f 253892136b0b82ef233d89683561df712081a211d8c72f5a4177d5db3e9aa6d5644f8df6 d23dce941e752ce7c138f3ee88752961a29f75600420a2e9597b59f4802295f6d8a778ef fe2cacf2848574aa172553d43a7dc3cd429dbaefeba838a05dc03a8e2275406e9400db64 71282f427db3eea8965783175fef6d0f97b9c6554d8465a306aaa92fa261d666028388d1 92ee8bb5ab331573edba8caa2b3bc8818991f6dad5b8b71092bad6ce26c537b8e111a745 d5c5194934c96bf309bbfe675a037fb3dd6d1ebf9c2bd88f
- g*₁₇ a12f02eeaaafccdccecd5e4a19ced052d8a8bfbf084e1850a9bbc36365ef2971c44e3e068c 582c5a2327dfe692f033196bf15ede43ac6a5e7af4f1e55da1db4396eb22206ed97c8198 2b27468c6b45e228f86eb3ef766849612315c026a2870c9fcb245ec1daeb4f4cca2e85d2 9d666ee6fde832643947e4b3044028866edfdc29d9be904a85a3d75e37ba22dae5896503 e57227537e9bf1a03acc4cf0c70e1775dfe8fae9e3c12084f2dbb28c2108f6bdab64e730 2ccf34992796d10f256eb049d4963bbc8e8c28a84b53caf3ffe515b79ce13c74f16563e2 730b6e2249a3166377ece495a34dfb74fffd4f6842b42ada7d9f21fe46de3b9535e8a0bfa 38a8b91f78297c06c2384f384f1aeld737de25600b8335873f57d80ff5c5abe8d404a863 6b8f287dc55d1a5e9a19098eec15e23536ad30b970e6c6546cd639bb39a9133d4ef7aca8 34f0dc25511fcf9a288926238f5718bf488bad364211c447a1904b01d5c1a6d343ef7973 a16a9aeadd0e2bdea54014df2954d8e6ef1f9dc580ef6df
- g*₁₈ 47d4b0542310f4cd252e4310ec0a5ba8cc4e6cd37285636763b96d7d42a60349f42b4fb7 a3fdc2f92b4940710f7ff13489375c74962b32c40ae75aa863ea894e8482b09da79da895 b3f26bc761896e34cf7c5ed49b444dbd23bc1a12338fc6dc1fc99b6f245ea273f1516892 0eb34dfab37970a116ac7bdd81f7b80d42e0863b343f04638f812998116382cd4de5a074 bf95918488245595db0d8d739305c9413a38b9f4ce6f8c89878b494a72ff6d9328bc68c0 35c17f5752743bfd34a16a3b599da1806904a684dedfa3772ff1811ca5064b2b5e5f3b9e 20caf5f93a3d8c324803d8feeff50b7d1217527afea7b1f44b50fdec27a7eafe49143fc0 64341193f85bf32819504f29004e2bc5a3404a077640ce5e508c77a44697180b958362d1 8f91cedd1f987831ab367bbc2397536b8523c5ed6fc7895f41aaf61f896775bf4da7c024 fcf0150b2ae6cb5691e3c0995358dcc33c3fb3dca80c2b240157e3da9493786e88c6f63b c4e991e7bcb1b55cfea4ea3295762ae198fea25680020709c

- g*₁₉ d6a16938d2b6af9619f9e99311fd69680516580bee5f0dbae354db684a7c0ba05517f48ae29e9a5e07c950cd066c4fba858b054a67b0d9e8860f99e54788a0e22b8cf7ee8ab429bd685040252f21df4754099e65e1ba5ef72660018e1c850958b55988f5f0ba34a1ac3c75d28f1f8702abf6cf59c1f47a7295ad0403de56036d6cc44af8d8ab82e67abf2d290f40e5fe87ee3d97c1f95cdae3d50f1908bd9432a5507b844adfa1ebf6c0f73ba2954142d281cad49671488312e072605355256c42d7adcd9f9dfb96179383e2866aa97f124a48c36bc2a0b9a214011c4a61143ebedff54bae77e150ff9c3b5e90eb2effae92e894401cd23e35914dfebfbfac816b99eca520e7efb628c03a58c5115fc2d169213a52eb2f9e7ee1023e94e1a396ad693e8cf1dbb7d2f2d6505c89b3156b90e628525d305beca2b5623915ed412085014186f837ffd64b2a4d979eed2d480314c292fd94cd2c45fd06874bd268393e094b1715a91f50d106031dec6a462032b77e2765877d73d6871952591af96
- g*₂₀ 4fca706a07e7f82592cea8bc4c9364797ff2764fcd7f6507e38ac25718acd37cc044cd70948c7129f8dfef63c295559cb286ab7c6043676734f90eac3ff6324f0964d3cb64bb109b909f2b8eaf20da3c012a22e8e4ca9d9889cc5976ba06f8bdd52593e7fa10de434a58827e936cc7690764bca7d5fc25b7239c5e89e5b2205bb5f3143a96b2ff31f8f4d844444b96eaf175458205c2e5ab88fa289ebcf6e769c5417e9571a66129ae7c2647d3d09e446c6092ad50216a96768b59f5e5199fcc83155aad2c9ef4939248044fa03344267c65a8c386857065f7a22893cfe4f132b0b0f346ab83498bce62c9403ff25a4914dad376ba0e9840a02a0122a5b0d0a899462dc7c53bfd5318aa1bd6381d4046e2793f9f1e8f16c60c65b60c8e8f221236e037580b9bc68079eb9499875f4e8728507a6bb375204446fa8f20ee9290ed27cafe4b18874677f9fe5be267b5c1104af0130bbc1e072575d46ad72fdfdfa0b033086099f7ac932fb7f04935002031be7f35fb6b71223e48a963ecfa5feaca
- g*₂₁ 2795122eee1e4d2b0b527dd4cb7481b1122232a1922c9298cb4618fac568d9290fdda030ae2926d0add8b63e11c01eb029d7079a1da709e20959c214446c71fcf1258f50a7ea8e93e5316e5bfe79c35f82ea0ac9853e0eac81c6f7ad2a8830a5253calf53a10da812352efff1625fe41844d49eb257de7124bc7f63c58e69773e81082c620927cab9af197bb214e5e91d11dd3202057b1f6a74dcaef4a775f5015952115501315578819b1703f46fa6d25307891c785a39630bb017199a94adb420a0ef492516133dbdd8e0909e0af2c9b718b72500d9b80d5d7cfc72584eaf8f6130e7972f7b6efd976e40d2f72b9b2b73b1cbe8eb8d94a0775302d8fc6cadf12aaaa27db400632db11cf6aecf943707c5bf59a70dbc66699d66084f63421877ef20fd78a5ad801a075961fb4d163d2e325013ee86f8c6eb788c7cc3e09be1b73aad9eab4f1a2ea386fc39f649b699632dda8684fe45a1f2801d524e8de66bb9bd7930449219b9df47fed3b025d6fd87737dcd40c1ebe9b31032425e5b87db4
- g*₂₂ cc50e92b7b8076433686231ce56e065f74276e4be76d3bb1ddfff80064c50dfeed01c08d94a006a5199ce2e08be25a5d9c0f7fa8e26cf38f9eaa3073b10c049652d8a20b7e360134f2f9293fbbcd42579f7655d5e5df76188b128727f72efc5b11728437ad2d2c288dee9eb573504627b1adaf419444068804cbbd8d24f5952ea77e6bfc843485f539cb88327f3378237dbc1cdb7d2abe88636d1df2b490a1a2a7ee6236e1be6495705148e9dad8b9899b560080fcafcf5fc0abf6da7953ba03938835599fa3b3f4ce0c9bf89801cd75fb196af643a31044e1063b3b389653bf995737f3945cd28a5d2f01d57af1f46973d84468fabadd2aaa8ab4bee4cf77bd54e67435526c8df2c8e2781d926cb5508fb70137bb1299180a5e41fb22ba78556ffcd6fd0ee4714cd4c2af1b5ec56434d02ce7463f34298ae36ee02d358aae34ad6c3d14e4340678c7e9577d30e34afaa7844434c29794e54ec73b4f1b3d84fcdac4291187fcda8330742c9349ae2257c60848ffaf873b4993e3f2f727d599c4

- g*₂₃ cb4edc936ac9fcdd1145f0526d9b67454d68e7df9b7a3d97c523e928bfd0ba3a2a88aa49
1a3586dc92dae759aec944e41454074958aa2ae4ec14f4344919d745dad684d5dad717d1
e0a12f8dce95bea38f610d8e1e7551729965c753f658bf7769ae1c544a9e1241a009677d
b9e67c0db939ddc47b4bb0255e8f6dd915c611bb90a06dd6657e6a31d496dd9bb4060070
936659225dec5d6f00770867cd1f0325b4f8a802b7c1b45223caa61e1aa43a8c633ac7d6
10902c61be694e1ae9b61df6969f03af253e0823bae2e8dbc88a9af2556e7f2ef246640d
09553b06c96c10f45f827ccce4836dc82d63b7dfeff31fdaa3e74fc6bc6f3d320937773e3
21fa219244fe2c023abdc78fb4e688b59450d334e6daa6f1e60eb1c50230728cb41cf3d4
d4e92a5b72a98eb309d4e9fd183d6b7d81e769405d04f7b781ae6f28f42d348973b7ec8f
99e805d6d211ea27d7a1530dc7324643852efabb240b6a1a857f1cc4e39bbde2d6ba4ee1
523203a88ed96fa1e4acd1450d1ec0d4e31078456cb1c327
- g*₂₄ 37b25b18a57a8fd3c96a0673b307bbe5a119e3d5c1f613461881128ad06e3bccfbb99122
06c836bf46123d6b03d2a738172451e2320494f5e7e6403ea50af5a8148c54ce741551f
49cc281305f2060b14dec0fc15f9fe81b72384669a15e1afa7ba405332d7271b376cc95d
fab7417cbef07a77dcf45b0cab3764c2f72e881b8e5e7c8d56924f8e5afce405edf0ddcd
a33e2676f8944890925a14dbc3862b91fb9e29dd850388f34fa4075c49bafce66a4ae938
d038020b4676131582faead3b4bc59077c6d0bdcc13a62bbcfb353305c42dd5b9c860ea1
2ba23a827a8b55be19744f6058c738a79b50d9f3a69cad04290aced6ddebbae8f2b37264d
fd1e06d728175f565d16976bf5447aeb9805fe4dfd79b851857aacf12291613777897927
4c33ecca982b0685403aaf908e754a7dbfadcb424d4e44e018bb4ef77d7d2930feced5ef
803e4345fffc986ad175f52c0fa891d852e4f04bdf982dd9d599bbd0f8f9f5f98c0be2023
d84738dfabea71c980cf69bfc9ed2a79bbd36e2b1eb5ea2
- g*₂₅ ddf5bdf394036f7ea8b6ac9f10d529dcd73c0b57193c5d7ab96ef26ab4e5803ec38dfb7f
140ebabc1e3300c97f7e8bad794b85687aeffaa45539a4c53dd695eed4829b08d0c8f297
fd732a1eca65868575f4ceae871294c029c6b06db0c3eb6086bd1171ad099211c9281898
8d04f4fcb558a67f4bd6d84ef4928f634c294a49f8ed3024d475015d38221abb9ed13906
834d2d14558f535cefaa1b41b099ba5e30f8538249b523199fd6baa4c69429c70844de2a
ef567535562aac76fa3fa957d61197e21d2b8b3e8f97d2292cf9f0ba970d15b9d919528f
185fb38f777b3436ad151671f0c61ad7e0990cb4d96024f5eef57e7818c538b9e824a0b2
bbe53c3b40b0750819a03b4b38a1d2ff0ba23a115535c4d698f22f84aef1f06c39d78100
79cd3e40029d0c8d47d5236ca08deb838bca31b17f27b17690d08e47dca8d099765ba335
222f7abdbf1d1008b308c7cdb645fe01b02e147359c4c2a553a7650d4fb72cd4b46348e0
96ebf65125b8d62f3061f65c3f21b38e6ce8f9ac2672073a
- g*₂₆ 38d91e582440054d9073f293a1851fd6748fb282238a8918c827972aa798fed2b5111e7d
d6953b4740b60f2da02949c3a839a7ce3d86db5a887525bc6d025aa41a017f3ea8f9ce30
1216a27ae6e758e71dd096ac7cc95447502a2f62683f854e88b09d337f32025bf8028fbf
6ef80087401251115867918532b43d367a8df92296bbff0a134f2acaada1004476090a90
97db1cffff14de4e3e090d7e2c0e32750d24e11cf1be391bfe1af189cd8bedd4d2d5abcd4
3e745733e56931b0bbb83f9763f5ec4e8996eaff290a58f930480ea151cbb1f57e3679e5
4c688bba375a00ca579dde865e1ea7f1aaae1edc23338ae9c44a6f399fd36bef39b14f16
609a258876e6b7d235767bb3169bfa4b5702e9d370b666eb2beccdf0acc3865e79cbb9a6
e82d65f354dac5aaacf8198066bb7da2300f2dbd95ad02f9ec5cbce5b07a2d0d4bda1215
c68735be51cb7023c635372da41126d5dd1521ec19d0b3248aef67b21e0c627ee1ab1892
851b57e7eb9fbac8a040cebdl1499be9fed064dc0326acc29

*g*₂₇ 392955eb364946ad9bb0a7abe6765533c19839abc4aa41a7a5965e81fda65103952b036c
68f8a1d16a23bce988639b7cbb11f3c0da402f61369d3ec2ec4410dafd4a83ee02822d52
33583858f83c00ea2e44233d90dd6617216d70520e5378c3fb827444e0ea87ee1ba5f374
8e627d76369847a4776fa88ed50555e4f03c37f41330ca350e7f1aed792f4fce09ba5a59
88932364308c5065cf7bb42404c0eb31bf5d911c6affeff6607986226df037fe5c474dfb
39e7ca0996c33e42b2ad1b9fe5a0bb2544b26d5e2e360d10709c1e4121dfe3a13793cad4
50ad9789c8acf16c47f8e5396c20ce88e471b581d528071220de59de262ff2e31dfa579e
0506eca25d73e85a4db9f858f1e66e8ce14cccc71fd8d2855ac3cf26a4c412c069930299
562d9fefa02a436a39c6ce8a1bd6258e612153d0ff53a4527f1736ac322bde5d3c638a8d
098f3b7c656a8478162ab5f78f276773e5f19862c21880f6e14b89fa1147294933cb52b3
012ea938c8a6ae3c6e1b20741c6a3de3cb9e6fa87e1ebd4

*g*₂₈ 6c19bfff8c68b99ddf1bbf8f7015f02c24a1a74a0548981f3f6b24580590d5173780450f7
3ea7bec8f8d32afd9dc6b25f47bd9b302c7d804dabd59de2e8af0b0d141aab109247c7f6
2e5460ae9a2b4718907f8af057e00be62e6101193b81a0916b8964a6bac27d121797f34b
da5080a7319cba289551d4a1bdd9df05ce16ce5233967ee72ad0d8088737666149752345
cf1e3b0e585147bb2be879683740999a7d91eac57e5d75e575464f9e7a10180e606fb4e8
a832ec3f69dcb4ace70d6add0f1787fe9b6b91a81dfca0ae6e090aab64987d5fdf3cc757
ef353bf6267886bd688768f61432e84bee67db77c42db3158ebb2880cfaf9a08ab55177f
063b6846ffcacad696311e0ddb8f9dd060c0778160a94fe833ef756de72725cab7cb806e
eabc6974118791863a2bd1b8361623111736ec537d724ed598484a9f15b635ff9c0e90dd
81dd03a0ed16df1dab167cbc674f95cd3d1575f1b0cc133498df1d2b73bd9beda114bbcf
08b8115af330e79152ecdc272641c902e631e84f03750064

*g*₂₉ 94120ddab3eb34b0e0b74accccc65107c074b292f55f6f10eaa119550c1cf3fa0ce3b327
98ee8ed2cbf696c6ec5cedd28aece15370aa9c73fb492d37a409c05f4b03fe81ba8104c8
37aefc45d57f9cdd1b8f74167dc7b81517583c147456dbb896c269354c71b65dd7c7bcd1
18691e2084dc8015b4cac191191fa3db28d253457182fd7f423bd7b8edbe8e1d166848a0
b93e7529249d86783b22b2d301b4296139d82ac224a2fb199890002a0b19ef7dde0acb09
e59b213bef649033d364c0585c55574c423600965772c874cf9ee1eaa9ac3d8f4a546db1
f60dc8da7121621b525d0ba8ced796787c542a7379231520f7a4b3a98a355130eecd52a4
021d232e55b6e3295e09460d49fd5b9fd9fe5b484f51008ddeac49ee134384d691538489
85bd4ecdb9069b7817bf74ce4f14685c09dde3db7cee4b2c40cc425c6997aad251328c94
344f00d86bc3c795e8a21ecaab361a21fae7742170e71b4bee43e782bdd352d9ab79d3aa
059f858e5b93020763632b2162450dda7c34931c83bb94e5

*g*₃₀ 16d35faa3550a36b1b12973ef3c5328151e5e6f3d871f36ee03eb9793b2d75c0397f4202
a24fe3c95f10a475efd67cd86fb6165b2061b690ba470c0812502c3a1d43721469276ed4
098b5581a30a318cebe095ca06c64916f026b7fe0cfefb201df95aece443d28297de838ed
63a73455097b57bba18024127f8141f8a96e451f00be5d53226dca469d9093fb6013d6bc
9d163cb7443bfd4c3d673b59678bc49feec6595a007263659ff85b685700e884c66ee60d
914292a81d4f65b80acab2c7b706ff0c2231f4b3c60c76e5445da347033dc1460f089ecf
209c7d06253ce2875f11d50cd1a74fb2851761cb07538dffaed2fb78068f1db5380c9734
fd19379276dae9a474e62a5f3562b8935aafc4f9a4d9ec49ef6ba7b920c32001a7559703
cbb857641cfaca9034d72ab48f72b9e1431bf2b6e7c4e94fd259aa121d52a260e6d52b2e
f229a02a2d4edb8764ed36ee5d23d8c1802015f48f1bc1a06d83b8e6e69c9a9c00f0cc9b
62f54617d3418914548435e41ff0f42edfa55f9b8cbf1078

- g*₃₁ 6c81477141effede5d2e7b4789fee880d30d2e2bd1523320d1f5627d42ef59903711d334
f2e0d991678397f1c56f3e1b8d16783f7f5694c14fb5b555d2eb14f0238f7568206cec89
bdfc75ca09044814c99cba0c28d6763732950d24a310f53c1edf6d847c2a0b1b2c62eaa3
49f61ef7b77efb6fe1ec17e91a467d64afdceccdd5e3486638e9ba73c2e0f167817cf19
cddb0a2acbddfd818b5306801e0f8b24246acbcd3da286aea99b5a61d8a34782f291ecd8
4db56c1413155f0e7d9408998057be9263ec3d554371d80b522268c64d44fb35bcc4184c
32748351805549c8a67f87dfc41b667139fade5ef68e5b2f8f09d3b7d1f83e39fd646087
7f6e6fa46a467e6791ad0587bf949124cd6cc5656948b64238ef4c9f78aa70dc783501c4
b6d7dcba636a15d894378d204c74274bb62d3a1ac710c37990288b72ed52245fafb5c06
aca7766814d8a0e489c5324523ea9a0d82ba453a1d2bb57bb794ff068630950b7259438e
f3ede7abc9f4eaabb30d4c572b7e065e6dca4fdf6201af76
- g*₃₂ 1bd4e12d63589df77583ca6064fc060a9e0d62d513361618845fa81f0b0d28cf3a85bb80
3784819d97514793c595403388a03e9405c8e875c21ff4b858f4044def3f8fc79c321dc5
b5b4ccf49979f3c191806cfaade5e5a23f222e2baad8865b8abfad5d664809f4c8bc2274
6b1b404637c9e2fcae81954c2e69112208a21b5c907514936a0a3284e55b5b60d42a6130
a0ef4778578739fd7628a9bccfca2e9f9e4125e556f184e828b3aa16f976c2a395b9af4d
026f41a48a103415adaaed8ecbeab71f0a14d77038a8c2c5d231035ef012c49df2fdc0d5
d5652c333fc563773d6cb2bfa6ec15a00696742f31f7c04f127870283ceda5be6ddebca1
6b9224d639d9dbeea336ccbf16e3364c3f98acc979989890a0d8903955fce688d01d5242
1d9aabdddc50e05f6871e5e82babdaab017ad00609b2606d6142a0a48b80f1205493087c
748f4f425784b9414533cc6892dfb9f7f284ac198ae1ea50d78994b9309a0729488a197c
01a9731132b001330da024eea34501daa6c66efe8fd0bb0b
- g*₃₃ eae1fb5f962171539f0f160a8e58248d0c0264f0c0a733426cd26babc3f651a78761b40d
ef2c327e6cd6fb78212ffe0ee36040cbd6aed451e230aa89c5cbe882d0d727e501c9e7dd
5feab8bcda7ed09cd943e4816d8696882f93569d9213b48d2b4d37bd12a690c17da57399
660ba238f0b511590f271d949d4c1ca82167b55ea56ef9c90bc73e5a293cffdeee042316
7be12b414665027338acd4db0d0253a15f1f93a235cbd4b9c563c9c2b937cd0a3e29fa12
f86e5b1daa5db87504f4013028556e3e5bebd615488471745a4ec455f1f51838791ada27
5e8308eef907f2c42bccfa2127dfe7ac394ac1d8010f74db1132150ff38996e04fbac8ca
e37a7fbb34b787b31f87a5d212856bd3590563b64635155f101efc8b1a0bd40174b59127
294bf96b3e285746bc03d06ea11cd72c4017ab43b06a392fb2ff0f3dcdade3c448f60822
64ddb6d7f78192aeb35a1e77ac0971e5148efe107494368554e3708a272188d2e49e7b1a
d7537312232a5514fcf82cf9c6676ae3f228620a5f4a13f8
- g*₃₄ ba4a58e21b750bad894c6162a25791669a848c019ad4e30d62d784d360ef54116e90afe1
5241e4f0754230d8dfd9a4f1805462837f2369dd63e7e38dfaed42549b262ebb09886fa5
e998243af2ee9538eb3f4ec7436461116461a3c4a3ae01c09b19a2282fee3d44efe854cd
d18c21cee6adf710d81dbc52691f4e2b07eebceac0857da4ab1e071bc8af661bda236f9e
b502307e265967e9b18e7bd7bc76dd979cf6f10da1fb71659f53311c1aeed6885934f1a9
8454b22efcaf7adeb7d66ad24a64d9e3d0f32bc4ab9e387e9888134f4f8c0627e83fc62a
9a59d8d586e46b2f3658271c5654f3bf89b6c6cd7dbfd18e22c0b73202ea19d022eac171
7298eaa94b846b5c33d0a3d1d768e65645f0f3293fb9c151bbe2e729234888ccc5ac7248
06e1e5c0e0bdde17c8fde8d0651859bd8218e6ec11d1b74b9811c45d066ecc798d38a264
f951f78419dd917c5f47035106c26bce208bb243ec86a004fc783a564a31e6561be1f8f7
f94c352d64882762da51b0a4d8761fecdf07a1c50cd5f67a

- g*₃₅ 22d5f1ba5e01b2b5ebd968719262a4921dc2187729a75fdf3539369e466429297b8a957c
b65a100f16603e253fdbbbbc20578088252f8624a658b9a9b888384ab58d00720d1f457e7
81849a2b5df49e296d3c1f0c44e2588fc7e0c3f308c4b647f9a691138de93fe467eea33b
fd5a78a614fc2ec041a2ad0d08af67ceb91638f995b57fd04172b9825f63666924bef8a5
bcfd7d82e82d1599f0c78b24053d5b73d6804004d04e5b90738bb985766ebfc1fe022f94
c9d618be8cdf935a946d36203ac020a34ed12356d867d9c2f69c605d78968ab8517bd42e
826f573666b0a7233ea9f50bd46ebde1600b9eeb9664c0281c9334d6a0b667629f5ac146
1e02273f4499480a0a50522767350e78ad2b4570f9336b3e442f91501e44256c2c18b5a0
8875e2d91677914254bf77281019b9cec77befee6ab76a12a9e840328d3a7b1f8e49c84a
32368f2efb000ca70c777075b8e6a88f523ec652416a519e19f0a4f7b41746fd69474810
147245259edb4c6348759bbe7bae07223a10f383f82e3839
- g*₃₆ 197a1854aea2f04c1ab2a30bb2388459c1dd665e3645dbe90d7a03168bcea7104250a4f3
3f78bbf50bad0263d0d857d9fa959b40830f8ad703b458853223cf0ccbdade3a42039e4a9
0a43722a7e86e6e970d347e91268a9040e9309b752cccbaf4117c4607023db720a8f45b4
1b99196f6cb1c74770d12741d2d01acalafb36253af79a86f158b4160005871dd1080400
1dff6b15634abb35973f2d4643b41e2486b9435e973d89dc057b5680fd9cb2aa896446db
5bb3f58fbd8d37bbd86f90c870c670fcc8dff719026af818fdf5272864e0553b13cce50
afa599eb817846d86c90701f9dc7202153fdee58c0734fda2c2f3b574d2d6ddcf09a8114
f2db617c9a3049b1408cb66e6206a7553844e66c408338361c9614dc87c016c8c120decf
545cf05d81a673ee9f6f791784c84d9e0d660f38c63763b41ba06bf9447aa9981199242f
660af246d2f46f3aad5a01ae77d632c0aa558e9f05dd5fb8133c89e239dcce43d8c5d878
68b1b8d223b085803e7858cf4f9fdef99d5144072582b6a5
- g*₃₇ 55c3e2f00f1dc67cdb821dcf3d7170c8dc27e28908a18d69aec73f0f85d4fee1da0cc395
af5df98161a438f0a552db1807202e181bc4cfc8901ccfaab47dab11e6505a7f588f120c
8e375a913f5810948842a5b716c3e4d209333b3857b0488c594b0b2e3c93c89fbd9804a5
6ef599e66585ca05a6f9f0db321339d2dfc8f9eb8e84e4222ef8e20a55b8af3b3989fb2f
31c2438a3d8b0852fae4e052c4660238693ba445d87a74b280f57a981ed130b5112dbfe4
748c8044a5fb888a2f45d138dfa7a83ba4c9136b4b95d698e7918bd961394b03cac7a89d
07acf689c166eb4f5572348c5458cfa4c2320f5ae9275752f6c445665a5ca69089c68193
3190e0d5f4568958da741d3b355588c9a88972507facf49ec155809545de9754497ac232
9d8c8f83eb182f873f520e79a853428f9d7744fb9b7fba282bf6c772445542338c12d86b
73d0e8c27749653138b41c5af3afc7419426284af9e1fb0fc59955f6a19b1f47fec3c930
a7931495d09050068c3fc8f6894138847dd2522fbc6b02ef
- g*₃₈ 44b700f4ce429b47f03d5e1f6eb1359ba95c73308801234e252c6080317ae6703ef642dc
b6732f364245d317749e0234fa6bc69d5e7c28c51cd2382e1644b8a930b9ebc154b42906
bcc0451836d152506a3023c076bdf79329d3aacb8f836276f327c6755eb580867c4f735c
e23fab27d09b107627004ea4a3d1af664f19c653ae6844822457454d566514b1414405b5
d07687b1100cb7ddd0d01dec3ea0a01f218d9312bfe6548b3d0f9bc88af044e1c66e6935
28698c90d7b3a720d0012ab973cd1c133dd8ecf3e3b75e5f1fb23c287a5eadcfb7351ddf
6ca813669642d9ae4248f10035b696291892e92861485566fee631918bf65bb251eebcf0
70051dc65fad7d470d95e94d71aa1f6779328494db06d2ca361d737c6b1c8287ef075996
a108c4e278800c6a17d42e9363b8880d4e18bc49270034e828ff4ca9010352808c3b644e
9b5409ca27de74213d42403cc98e20f06fecda48497de9f43690b4a005de3d519efb7609
6bc3b169e61901a7734a1d9247d331c698872dc031c87bd7

- g*₃₉ d10263212e6e9c653849aba782f4b1e2ac320a9357cf7d906f49f27a7c2b10d78fe822a5fa20b6aa7d04c087b0ce0ff9a2da3409724bdb6db0515dd467f69dfc9191a18bdfef29d0ea7907b4e8fed3bbaf1265650669f98e5890868bf7aaed2d780303f2190296b9e0a9b43dda933622cff32412440003bdcc0d8dbc39f4d76ae0528a6964aa145dd4f786f3b78331bf0cea307091f1838a47644d0172a36413cf3d39d3c14690cf6d595c5dc7deb24e4cfe9da6886b5a55b23db02c0005fea4e1a17300ec793d4da3930da0e5d11b268a01106e7ccb342165cd2ccb1fdd6a18e9bdfa9d1061ad5950af096cbdc6615653e799e497ef269f2ccee01767de22bc1ff6690ab6b10ee9498431cc2cfa1a75020d129ff52fb7442cec4309305e5f3b9e3a3ed5ece448bfe2ab2b2d72578d0de94b65daeb9d6b2b88b75571d7228303682ebf18eb8076b07c97dccfb1f91f2046a8f8ac7c0fe1d24efa9c104d43921d4017a74c979546c6521449b3b5fde6cb1fc2ba4b8c3dd2a518ca747d94849b4e
- g*₄₀ 61cfe93a3ee1b91e4fb040afca484753d7e582c7b401bf2a1267612ec21773b759b79741002866e62a080159f752db070a015187115135e8dc4955753190462dec86b1b5d52fdee89bcbbee4199b806b94c7b61330d73f3272aef84905761bc7bbe029d745399946c37267b1607f3a54a6f1e89fe11a4e3cf97632182189e0f9bc2c561bd1f1867573c625c75172a0d98d7939166fd3a696d086970db014731b99658d42923137e68bc10c7850b7267a947239cec4907e49920f9455d88a10001f026815c578ec6b7f2b1e429fed9a88e06545b7b5eb4d793e549069e3aeaa7892f2cd74377eaaa0cfbc54624aa9c9c239d08155edf045a090e99435a122c3d2ad0aeb9fdcb9e7bfe92f378ca4fea249e6ccf1964e71786ffab4c04f400c65b289894a6c294e94af413307908123009544b70c6ed601c676b7c482d3a1b71dc2d5855663ee48cd997bceed937c597d46f794f1b527300db424de3cd9110ff546e02210acc9cca11b06008a17d611bf2ee6299fffc89f10e18cb48a0b00933975e
- g*₄₁ 7bee80bea5719e91cae176e18d8db6484fb8b4d48ff2443e17700f42d82e22ea935cdf8b0fa80730337eb5e2d6602df2e249a87b148999d3521c772212346ec750c612b0215fa6056683610d30cb59be043fe22c993c26fbfa0da987985c582921d7f5308f40125398ab1a03dcb30d5235e6fe0eab18163534edadbf0177122f9ebb3cf349964cb53847527f46b1cee64aadba5ce39f525e329b07a90caec70100fa178ba32495afba1c9d69495b21283aef1c3e1291929c6080d4fde9a1e7cb91c5321b1e3aca2294cd044e6d40c490c4a84e010809be3799d130dc3e501b970d06a7489b96087ec42d6759773bb6537cc25a931747211751734fca1af124984210b3524b94b4cea858df0c9f7c7634ef089ab601d5ce6f0d9d968a8b9929a3c217e8896e4fae0fd1ad2da34d7d7d7ff6311d27ceee6055b952d9e33478fed21fa2588dc0c7c7387b7b91336277f640a2b65dd7dac5dc8411fa1c2e0756d3a76e4fd2a102166d87fdaff34861eb19e365890f4dcd7e57495d7bfbff0736a41c
- g*₄₂ 20d72b58ba0298ff11e367cb56987a5137d8a8f7f48b6446d9d3735422d4a65deb510bb7eca5ee28a095952b08f8clece752a5188099e7f037f150269b2b6b1dddcbf2b90b0d41c974c440b63c6364af99ae807e4fe815c48bb3dc873f804920e2bacd4167e555d57fefb8cceba30af106ba55fd8af1f94c19a56ca2ba53dd51a72fc6cff3fbe3d15232cb6df37fab9c945f5cfb4880c479e2f183473a4e70a70ecc910c678259df977419d4e4a5043bccef1bb2686ff2616eb34b76cd9af50fc57a4a54e5209329ad67c599985739e1d72f6b7eb4eb2178d9ec3b50c66eaae42621b48c2ff06c790ef3d518209df3d828e6553283f6549ff6892df01218ec3014ea234474a177ecdaeb7d8635fd3f8bb43a9d23463e73671ac890aa069300d29e4a71299e9270a9dc27466843907d29ec9393713c8bb0d7e3aaff341e0bf434bb05234754158dd233a6a977e4ab41fcffad43a735f2c2fffb0d68815b607cced34dbf54e28fb7c7c99bfff9eb3d05ad86a3420d59799196125e0beb2a16ba0cdd

- g*₄₃ d99d4e77ae3bf0a9f867c428cc770a2453cd76a700b59c9fbd7f8a5a5f10adb605fe56bd
946f4bb6a013e2c512b5f6a9d41078a58ff5422e2584c079fef324062cd6eeaced1d9e35
0541a4289e3e41764be531639f4a033ad3c221b5b1f98fbc5700b1b7e6d6b5a62c653129
a790e165661f6c1bf6aac3f038a7019905f3b0dc7bf3e028d9e4b78600d47bff986e1f31
e0c527773e4321038810ffed9256fed9392c376ccfc5bdb72e27da62fa573bd61d931925
a50492e08a31ccc08b84a7167d83e1f60d74ba50b51d8955029f4eb133918d7a0a50c4b1
f25deacf74f61d5f26e99560285e32221ca5c7336fe10c73465032d0f032a82f3449a3a6
ef6e2168f639503de61e7b4fd31b41ef2566a30fbfee9106d75d44bfe150ea4b02b8cb8f
7bcc40d8f420fff8b7a20a73688577f9d8059557758be5b39585041125bd617bb7b6e08b
d43bae3438b13f2edf70f0f0c0bb8a5cd40a059ef3fd03f2ebc21522e2e6a160c4ed7e4c
21a9c272132d5557580b0f31fb6e229dfeea249a92ce47e4
- g*₄₄ bd878e6771203f587b9df824b3915ac3bb1575d3950baeff9d2488dda5071a3ad24d0a2c
966b67429917520351adca08fb72cc5ce76581acda48b020724cd3bbbeb847f8634507627
4dacd920a87d6d0392a2bff4387d7271f5450e5614282cdb179bc69a27a14d17777ccb91
734ce419bdb548d4ec6c915cdf937460cf47bc1d77efee2e629b8d2277ba96dad1a03ca5
0d8c3149204e20aa8d6fde872c53364498fee6e67e8a751cda6f5dbb5b6c8300b400e6ac
b328a7a04391b2d6f90fb8d9cb7c719167dc1bfde22a178c15d0bbb5efd6d82c39cad9c4
8726bc25d51c7743addc6dfce39230f7dc18089da6e2487097417a00c6cdfc1037f28066
90b04eaf27ab420df1c0602e1e1f1c9c1f67d6ab8056dec638e8906b89c3a65b2377b43
ed01ab0de57ae4ead3cc157669be3a063f15ff14351185256302f77ce82a8ba96804b31e
922e142715356138c91a7010fe5dccaac3d4e182e5e822d3dd71662d9412fd7486bcde
a0365692633faf5a1d8b30ebf71010fab665455e0057caec
- g*₄₅ ed987e4c1ec7861f2d36911a9b4bdfe9ddddd8fa92a3359c1b435284965dcd0d608696906
4acf9630f0952d77c751b0933ddbd41dc2c5f065d8b56501e312a23f140d48d11350fa21
dd27fcae493983b55f3243a71f9a122166de4ac3db9484dab694a4050c2d86cd488377d1
dc8771cae0cf8401359d58fcfcel134f6873d4628985fac1c6c78c5e31b8fad3e71a6456e
86c8563cd6d4c6ca7de5675972aba257e503548c9e10a8bd6d1f4f50e0db418d489abf9b
42db39dcf4855c432a6e9ef0c074c1f4eb59e36e923b26f33e1b878e926b4bd0bbae2052
933557ecebe089cee242d81a30afcd5006b298a1fd2c96c5bf15e467accee6dd7d240f20
bc98a72945dcf30bc4ec919d76e68021f540d8e7beb8b694f7d255e5706d3d19140c344d
a6b2420ca06717e9f2b8855f5817c699a2a0b8c5f0fdb3adc1436c37016d4cf63f8b7f2
9fa40f41e09dfb6bc82dabf8168002e4e3a79013f6ff48d991a362257dc87d723427ec78
0d83452ec2b8bd571bf6559b3acee10065df1e483310b3d0
- g*₄₆ efa71aab2b771ce67396a791eae478e08e7385f6bf12b4d94f7f3ccce821b70f48324f58
a78c5dc37bdfa5bec8d5e862501f315420bef05769309d2f4f63c5225d7d7c43cf47356f
5d99e824delb0f1c7efda662b6a5699486ed357a7b2f79402ae687841886d820055a10fd
f8900a554b895b918b850d0bafc5a99582295bcd02ee5bff8e3f229a67b6fe9893bcf51e
d2ba964936e01d0cc4e9c4a1059a4718ccffdf7a25a28fa7699fc3e80be3d8aaaa055b8e
7c2291b215156b8ec1604ad0b7ea09d491c9fbf8618fb74bdf0248f4423022cc6cff200d
29e9ea306e569d31e6a840004a42f74d411dada36585ab4a01ed0445b98896b911d580e0
cd459580ad33348a9d35f9d1309c523e0fe3499bb6603ac45727174b2c464d5699c72b43
ca78bfb5abaa7b1acf6532a6bf2fa3f7b0f67854822f1495004fb2d3da110d7bcc96fdd9
f3f848c78207f1486b31b5595b038b729ea33fc9b603eecd157fe940ff445c6b2712a52f
47741db45fed618819513cd0da4d7ccfb93783d8a8b69d7f

*g*₄₇ bffb05ace470b541b3b2336c913b7537ede5b72410845905f3d80c7181c091da7154503b1
888973f41c6938c5be333ee3d0cbb93874fd629924434fe9cc80b2a45e35d762993c1764
946a2e17d7dbeb32387b8dc0aa3d8758d50fbaaab8a7a5cb99c902337da95b2b862e07cd
d382ee5c2fdd3d661124369f65867e25cf55d0bdfbd4f70544c877837b26c4e0ce02f0de
97de2f448f3c63b2572aa7a5e3ed937c64545cf4f081ed95442fa39f8c2cab6013cc5217
3bfd2cccb875a7b4ace592a443711f1e7b63c846f43a97f858b36572c4eae2b6d49b9d9e
0clad9c408f591d0c156d9041e49e4979c224bba67dc90aed3d1bd12cec02f960616c94a
6a9f800034aee724bb749e58190b5969e93aa0828050119691bb5b89993426b37f498b7b
96c09bf9f4d3a6d140ed1e6c725b435698ca5e84930a265f0830d25eec40572dd273fea7
849940fdca9078e54adef84e69dbf830527ee6ee25b691d1d117e6e884a7e4e08717da41
490355c950eae33490af6c0db17284de44d38a2c27e611d5

*g*₄₈ 474de4f170dea8d45a925aee5457e8c631063b409b966d5e7d326cd21033281a8b5824
118b4eed14896d13b3522d1d664b3fdced7fd4f59af1d3fa6dce2d73d75d9870fdd7a91f
c1878225233846f1cb34587d600d60e31cc7688d7d995b6ca0f66c42e22b69859a11f19b
919962319d94efd06692cd5a90b01e264c4f77ec9e8adc52770a8536d2a19b3f6acd6b3b
64dd5b77a823fff778eb405a5b3048acc871271da626f00c6e390fa1fc80f6aa62b595311
68b7719d9a76b7daf15c0a7f8135a7990cc6c8bd8df9739320cfd23df8fe4a7c3992d31b
336d9cf9d7dd0be3ea53795f578b79b330b2a77ead3f0241e94185b4d29cc7ea9efaff34
4afbde6b5e64db22d2e1bf19f9aa136808f4d812932a56a87033ce41662f9602cab5a51f
0525a58ef7ba4eabef5c65c63ffbb037de719a4663420cc2012794f36b1b7e840cff8e65
03e34a6938c28472ba90e3892e69747f22d62cd5559fdbb29d093f2c2bfff9882df2d11dd
3cfc96bbc8792b4f2a3e4f30d724c7823464ccf110b48bbb

*g*₄₉ 8bd43109d89e712ac087ada9847f7b7baa1a9b16362e110605110a4fdebcb1af49dc902
742b6a0910d54b04fea1774d5cb85e1cc6b64b639709bf158c745cefc54f80c96033485f
f9962a2ec269633ae30e9a33b7758aa5760842aa317440c757368d290e9e6dde53780c1f
3796a9387877c576a7a856e4b486115341cbfcf8c702e135909ec679360f3e6706b7ac2e
2fc413f8f334ec5bade3a7af9ef035eab8c8fcc2c2f7cd7810d4f090b434aa3142d85570
51c48f0cd18ed407dfbfcab859dfce5174e56523ae0ebb518ce72985c0b0ce2a76331df7
5abf53978d31a0c5122db2ba344968fcd9da2da8f59e58212faaa4ff9b989aaba4e46487
8c56fb3919da5b5708fce509af219d0634539846a4492e25d19cf6bc8949f4e8c6f33603
93be3d6189a76986cb290df07d24d7eb86547d86c2e97fe27c0a4f7c654443fd7abeba2c
357355e5ea286b9c97c108087d455955873841632bd760aledadc3cdd7027f4b45acd641
e0245e486848f10ff4fdf15943f32f755ef8847df8657a66

*g*₅₀ 9cbc4a0343e8b3e550db6464362e73fcd6824aafb7ac2f3736840298bc3d6a7973752fab
04c0d0d11b666f65e57c31fa45a36919c2ef9a9124e9b2eb888f41ee68da5030510bdeb9
4ed906696309dc415ea48621ef4755313cfffca47935eb6978b5f180f98d530369e63dbde5
7589757364ed39884b7dafc0ebdd523d35a49e5abdd57bf06947518b00311c54488c0e8e
89199d27ac92d5f789f55f2493f403557a79b41dec81fbc53347be893945de84e7972c5d
61896b590924df708eaf407366a50766f05e7916cb249cfba76867344606eab2f8c74991
3739995c1484450e0b5a2ef1e3ac51e0cd6bfa1a5396b2f41f51da8e8157ad53ff4fc17b
6d2869f4cd95778590a98476a49a30e0f05c8373eab47206b7d786990c7c813987845b2b
63b518262839d2354842dcb682af6deedad746da9897c1bb2e70ab6cca81938e1b8ff074
e9ed9d2b18a557779c4bfe8cd6716d64b7a26d5e4a91e6b882ab3d63fcfed599e89106dd
b7cb033b79c6152976fda739923d64a1525c6fe245e9b622

g_t ad7bcf01aea570704230f7dc84b1bfccc8c41f66499d2fb5165b8ba024a839c44d6dcac0
325789131eb75703b144e0a67b8574deaabbefdfef6f48c679fcb0e20eb6b4c9cd8d13390
8d7d29eb69d672d1a4573b7cc978ebaa5ea5112d18b0e258a56433deb7e6ae95370809c1
3161d59a2e986563a0f954d6f7f78378d512164ccda8b5e015782f3d884715cd9803a2ff
97b3b86517d59a419e4fbb5f6ffd78ae79d46b7c4b5fd33bcde17cba7d806185f4f6c1f
8e6f6ebbac9377bb67bddea54590ec83b8d70aac4763bb353dbf4cd0e1aad4b3f0d95121
a6e19a81be2a1f95670ac6f63157d4d462db37f63f9695745eecd24574806b6233169973
8cd85457f8f14641a7aeab8c6c50cb50e8cca36902d25df210756d2dd5460c4f7752c8fd
108a2ca90bfb42734ab5a741ef7d46aad3f47774d4054f87f71e54996b66411597bee33e
f6e6edcfe9921cd1e8b44f0eafe6f9566aad59ee736471ec97546ff4de82895806ad1a57
a223cac4531254490b7a5cc3611712d70dc943b3de031823

2.2.4 Device generators

g_d 8f764d4348d9f31c3bdd6a241f16a3f44b7bbc85ca7b57765a371966b7a36da6d0553238
1d0a2f463966b462e3c580d85ef8dcf13588c1f5426be3b98e1923e1d68f2516ed6a1659
c8d4735fa5bed268059c1339d9bbdd76bce3f06fd695ffbc605181490ad1688f03eab2d2
1070b479006bce47c30afb5e891f1d4171f23b86fc1af0be5a6b87235b300af32082aeab
7bd8ca114a3aa51ee99a358aabed5bcd478de2413aa2dfd670e0c13df44aa7317f420848
ae3ed594fee75f097db1c841f91e09e6c25244b998c181b3af51a0e6102f1f897b42e263
d4d75f0899922b95fda613b58812d6e214285251a1ce624504e0e027d4b19dd948e73071
61aa4dca3079f493cd2dc98af893deddd9cafdd3b43304e4d362596988b7863f202ec873
8432f2d42359c38954f14ef85dd59c3db9d81961d4ad2e7b5eff7c9e619559bf807cb83b
e449fd664352a6c48e9732b4567ac35812bc70c443471ddad109c97c6d9738f6a0085331
2fe0627b0efde26882b291a5179d90a648fe90a02ba4a82b

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	77668d97bfff7d5da695d6d72e4f840205de289ce8ff1e9952435b0b4dd4e222e
	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	18edfa1dfc653a0574ca88fdaaecdf9eb75309aacbe926c2110e92678c84e3d
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 40d26c2adc3f41d09156025a9dc34fd3ca6b96809d3d7cf5f28d00aledbd6995

g_{23} x e513c3e50efa4436199c5a51fd691ea4dcabbc202a8029ba3df0336f12d82663
 y 75f42f58480d2cad569b0f13cbf376c3913271d9f7844242b870519d2be8398e

g_{24} x b42b3b05bcafb72800ee242ab4cb7abd77f1fcea7ce1d327eec25b3de6c43d
 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 4bfff16067e37798ff3e3242b11be39f83dd7451ebe1101eac4887a6f93d50206
 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 592d48158a6358a2900d453d79e88d6bc20b7fa8cb2bfcfcdf082960525ad83
 y 7231c3d1f86fcc1b6c9e8c16ae45a93508c9c49e8a745e64b07636fc6b03103f

g_{38} x 18ffac7507b8f022eba9722aea93c6ca7470825a787c1f982b083dda0490ed32
 y 304b83604a94ff8a2787b047e823e50a64edca0b1dcc9381196597a1c63b362

g_{39}	x	dde5dfc2867a61ba2e046dd52576d3d33a24173e32d716caf0d6bc4bd1194374
	y	79b6e30b1822d61eade59b0ab3edbe8f4291c8e081ddcedeff00bc32ebfc1a93
g_{40}	x	e0f72a8c71395e19063b0e09f947f86c06f4b300c81d3bbbc48dcb219ab960aa
	y	6f231e0a538c8f54c066c93e1af857bc3b1c418802274cbdf5e387d88736f576
g_{41}	x	385388078ea2b4792dac8fbe0b4748b99800ca086662fa8eabd62596dd7e5c53
	y	4d211211d5bf47baed1c4a2688cfa616e7bbb64d412f16b371288bfe957ea61
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	80e8706709bd25a84937417e2d6a6dafa83d3738dfb42f8eeffa0fb5247d69985
	y	6a8f2ea6b2301e3aefbd8246f6eb97ea0ce1155ce0b72c471d01b0d0b88da2ca
g_{49}	x	13bd26060667f8eb7e56e782854af3b3e010cf1825a684bc72b287ea7b2c234c
	y	1871c15aa6f8cc3ada2d4bf6bb2bc6296ca6587c122df3b47a9faa3025863a8c
g_{50}	x	7d5e69bace920e8ed2d0b43ad14849d71e26729cb37f009ae14e6d8a065e9079
	y	13d6c8d6ae0273a1890129779f3e34f0caf6f353bfde9ee337278678c9b6e758
g_t	x	e2ab81def593e999c975a8a48668b9a07e5594cfd68fac29f17a811cb26b3e10
	y	756311f896c503ecdb2f608a1ccbfa378a95eb4578e65f190f1a8b544d20b082

3.1.4 Device generators

g_d	x	4ca625118d0a05d04d275dae1ff096361ebeba345c31270982f796639b1ca574
	y	142d150c855ba9aa7dcc71821a538edb544836df8050912679ccd7233fbba636

3.2 P-384

3.2.1 Naming

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

g_7	x	e42bc176e13bdecf2b316018a22cf95102b71a1fa8ac1cfe14eec54cad256a9ab9b4a7a8ef3cfde3384fe4a1bc11c2f4
	y	4e26002735c92697877057256038e7934c1d428126f41e771b190840dbac0f59bd5e07022522b638a2933e146339dcc6
g_8	x	d71410b3e3a222aafb7f53ed4cd8299e442731203becf643ef81da371d8142191cf25a27019587294d23870c78fca049
	y	5dc9800ad0eda033abe134ddd894f296b5aebd4458ee4254ce70f84dfb0de18fca99bf795ca7e208182ef6c46d7bd494
g_9	x	68872b164a6e9b8f99668b5bfd4ac0770dea64e37732a384bc39c32484b86091cd47ddea5e26b18065e8663e1ecb8b80
	y	66608aa7cf0ab53c375034dde39736dc81d6831bc6ee78c714e010afa5c85425a7ed28ef6f462aeb4d7952eaf488d0c1
g_{10}	x	a04decc7e9f0cf88930ab26c96d6952376b4c3a3db75256efdd466f51f7c01841a5f4e6a9f11877ff286cbc74306bbf1
	y	18c80928ac2082c04f300d31b2e6d00ee687725eb86f0dc7c7a8fb95993ceaca8afce480edc727842efed148882dbaa6
g_{11}	x	e9802ce5361dd79eb14f004d1e2a7dab4ca55862b937593c86035fce0d3a49c1a1347e9d89e9348bf8460fe64668aae7
	y	29992900811b12c42efde123cf65b80bb249e48e3f53e44775cb1b36536e286b23e08d4c59f50ddd89b9db4e012a4f14
g_{12}	x	8537b29a8b60c67394d30378db590fc704ff363a6c7901ee29bb8b183fdc8b0aead5f438e44384d41ed5f26be6a4c7e7
	y	75c3be295e38813b2722bcfcbad491c62bd81a1438864d8f54a48a438a6a556c5cc6bd9549c25ce7e39d9861a30b6e08
g_{13}	x	e46be8fffb1a61277574b4d4e7520bb28df1aa92b75390bf6aa819884a47db67e0a5a3f754cef6dc57d0725c796806d85
	y	1e0cfbc5092582f702002fac85dd2f32ef568e009801c3d79611aa3aa0eebf2d559101144512fb2c1a597f3f0b05f543
g_{14}	x	f6d6df3c867b886a4bd37756056e72009d2e264cb25ddd59c0b83d4d0e40144f649f4357d416a1772f7a1e4e2bddab15
	y	6d9b50e848246f310b92f01835d53dbee8e27f883aa6d2549e527fe7808a9cb61923175a8eecd3328574a3ed7bb59ba
g_{15}	x	388a6cb55c5d08bcead8211cfd20e32c78eb6f06d792101a00c0d757480046f9c4aa5df882176bbc8d831f72814a790c
	y	427b8985182f9036019d28325619b9ca944275082bd2fd198500c17c9bb8ae7d591efd64e18070c4cf3164e0926dfdc
g_{16}	x	f30fbee912971dbaad5ed633b5b2a376ae60e2786af169695af00f6da9bbcf9a43564097c90225c54e2a63b9c0004f
	y	31feb5903cb5679fe9686f17303e8bcf8335fa07f6fde06b7062e2d337f72c7aa1adee5fbf5cb3742844f07e02fd476d
g_{17}	x	bc56187e62b3a3c246df01d8f885c34d54ff81424abd1d227b033f06eccec6278dc0759a16d90f0cc51616c50e9a8845

	<i>y</i>	3a532cd74d1f73dc02befd8b002db362eb133b3d9ccec54529f15d7302da1d8b4c7b36654e4f8d2a3e4da5eb9b29a7e2
<i>g₁₈</i>	<i>x</i>	899772126f9838ec178961507caed8258b6f102f5a7708babf80dd1dccc70021e4f41c2f7438beb67c9a2a9b4d57f84
	<i>y</i>	71b9a6fdb91ebd0a292bdb718377308ededa063d07cb034e1bc86ea2f65fa20f0935c6c8c378caeefe64ddbb3adc79ed
<i>g₁₉</i>	<i>x</i>	cb2ebf807f1e6fe411df6898cdf652cbb9bddf3947355011429d111bb2618dc46defca469a09c19748cf1d09aa8219be
	<i>y</i>	50238a8b2707cdb88c381d57369b4d7838d7895876f9a3d80a9556a5c797a4d0db8399fcd657add1938b65c7afad8a72
<i>g₂₀</i>	<i>x</i>	95fa795aa4f4c0da486420fa941b25d7f70c8073b78bcd8820d8146689d81e1dc2a4098e86afc27b49c86aefed1b0d61
	<i>y</i>	623d37c13dcb6ea9573372888af08beacf94c8dffc2cb615030ae612b0cf1478751dc3b56a66a51db4b98e264eb016dd
<i>g₂₁</i>	<i>x</i>	22f433020dc129c7be74558ef9c291f3938e7817b47d4b41a59221d85b10ffdlb815919fb3717e3e7e15e93fb97f6f7c
	<i>y</i>	14454cae0eecbcc8e521555fd2ec822c290c464671ea7aa99d558909fdcccf68e4d7095c4647a16e47f16c0b68851c1
<i>g₂₂</i>	<i>x</i>	456982b235d9d013c99b64094d4129631fb1c6210628505c744133e6fa175d141fb4c00105f810284c6880b46a4406df
	<i>y</i>	52b8498256516a4fefde13b5a7bbd72d3f19aa00b3626decdd9cd1fff7d175cf744e22416f351f62e5d01be651ca82747
<i>g₂₃</i>	<i>x</i>	451f77cbcf22bee6a407287ef9a36f293fa822f395f64c2edccb9ab5f8ee3fde86efddcf3302e8e9293732a058332816
	<i>y</i>	773401a10fe5069dbcc6870ceb8b15d1cb35227bd8af7d70b63d36e95613deba2d6003835027493c04630edb2700b965
<i>g₂₄</i>	<i>x</i>	a4ad50b7dbcfcdc427e72f850a1bb040281c5f99b914151c47ac48f9fb7b85a05858f303588c57d2ff66b5867145fbdb
	<i>y</i>	a564336b5e37aac39baa0878c6c50d3d36f5409f102f9b8687328094562ca6288b2b69fee43891ad561d32ed4bb20f8
<i>g₂₅</i>	<i>x</i>	f1b4f132b3c29a9e3467a0220817f2587843e77543e812ec524d7d413c6c20c03ec39b55836220717ddd9af42affe667
	<i>y</i>	3447a1342d40a8c094060345102e64b1b3871b80ef28d32770f849b57e7696118f596b8b119babdd2d7ccf27b55acd17
<i>g₂₆</i>	<i>x</i>	970279c58147dd40d2aafebce3e0bc13ee4ddbb746909cce2849bed98d8b7b36ed971a17a8e75cdb5f3ebdc3e71b47b
	<i>y</i>	2cc17acda096b56393de63c66b2342a03e2e504f12398001b8d90fe1581d2696bf8643465854e0d9ade9ee2145f3c02f
<i>g₂₇</i>	<i>x</i>	2b5e17c219e4ea95af39b24a20dc4d5086707ed8066bd298e3047d6459823fff102ef617d4670d59e0efb965e179b01a6
	<i>y</i>	242023567c670bcf21c9c2ef69bb8b87d7a8dcd034b66606900812393ee9989bc37e25ab672a3ea4ef3b028f83495623

g_{28}	x	81fe66dc8e7c583ed15244b5d7ec869725bc35346ff3063e6a22483e92d6708b598f41e4261d4c52c81fd703853c0b5d
	y	23f75a94e5f864850697619cabb8b34eff569f29d88275b7a7ae1d77809e3a5a425c82b5bdb8d7aa75f95c53a37cf960
g_{29}	x	46e4d4bc6281d4943e0b5cead86eb8f5821bffd42888b579db7171c82416bcf863187d868155b4a0aelf3e44cf7107af
	y	1464246c54ca3a8b70da3da93ffd8866336e7abada509d39276d085a9c9dd55c04ffdef0c5ec06983aab0e63fc1186fd
g_{30}	x	e3d327377144a406ff2d22fb26ca634d6a8a0ee4bb39aad0b35e6636accccaf20aca78fc1a02cc604805333034078ef8
	y	47ec98d318f871cb6fe491bfdaf261d862ac92ea5d269b941875e636dc5ce2cc7466908a60af479aa2c70f94ba0ad303
g_{31}	x	bd425497219e2bca3b47629b19f79d4dcb276284b45c3f5ac9b47b76b90ece9235655cf957f77ada902dd175e494da91
	y	2980e0c8d44a32345211554bfb1b7ac1edef0c5cc1a60d42ad4e19e9b9aaae4cf1fbca9eb01e132df66f89857b9303008
g_{32}	x	2a6c576df2af7b1405daade9fb24bbfeb3fa9c5586036088e07d9dbd3155e9a96922aee185f731579c7d8cd1a7a344e4
	y	44916fe5da07e5adfef1837d5d3fc2aeddd5b05b9cd9d40715fea44211486d82ce95a27296b5ab3a901f63d501f2b1f7
g_{33}	x	e7e5b42c722fb47bd92ca581c05aa00f1c18c0ff654939f19cccb6ed3c4df9f7b0a03bb495c44cbbbce93f4895882637
	y	3092e32af39c40c24b5a11100be810329f05016f792faf50876f77f4f561f18766b01da44fb2e54e84946f2a3c9670b0
g_{34}	x	a6959a68a6da7a468d0eef827492d3888af2811d0627c18aa909dd0ae4b020d133e48b911b377e05ccb77feeea326673
	y	70edeb467c18d159474824dfbe59429b4fad9c97cfe3f84986307b4ba50faf2c4b60d73f2b395b595bb6ecdd96a4fe3e9
g_{35}	x	9938127c58ef9efe69cc43ad758b3af23bffd84f7182f090095e118834b67087ee706b46440323889253a223ecfc865
	y	37f1c9424f0860e3ece2f8107800f6d86c909a9f44679c3557eceb4b5814b4b396bc8e9a9a78bbeab7c1313f0a4be318
g_{36}	x	60eae169e138df4979ded509baceed03e6344910d36135ea6653eff55c076cfb54clee9bc0b5e8129c929fda643e82d9
	y	65210212ca8521a0f9022063c3d81634a1b4649b02651987fce2a85e3faea6035bbfa25e4de47695d7ef0be7c65529f4
g_{37}	x	ab09b0485bd7eae24bf82acaf48cb3848a841fe3826ca2bfd91d2afedfbee07a91d1d35b7c422445315d74666a2dc5b
	y	6be91029fed90132982e34f581b85cba8d699062b76578808693f134f203fa866a1fb2fafc8777292bb5c62c130a9410
g_{38}	x	ebca9a02482d7455d0e6af492e611efc908c1fb851b58f331b2ab087a2d9b648f30f3f65533f4c550975beb9168b0849

	<i>y</i>	685df7b2c2757a5b5ba93d91286388f657b89bd12e36c8de9c95818aa4fd357b4c14df72a2bc4136fd9476160aaf651c
<i>g₃₉</i>	<i>x</i>	dab79fea35a2883a43c02852d28dc8b7a02d5f331cf1a5b961aa2b39a036756bfc80f51f945714209b0be881bb82c1b6
	<i>y</i>	4c2d063d405b4569aa6dc92926e3fb363b3fec762d0c6f0db267073cfe3f78baa2b8cb5d7000bc8fdb281ff148e62676
<i>g₄₀</i>	<i>x</i>	2ea5925eede0696e05b575d1ca4466b1a74490fc91d21261257e06c6c5d8d958dc1b34a3c2d14607edbc15199ee36e73
	<i>y</i>	768db9ae8de6a9d51b7325f17471ed6422b8977fbdfefefdeb0d5eb2879cf5b99de7a06beef35d4d4b471e3dae96ae94
<i>g₄₁</i>	<i>x</i>	5fc27113e10eb415118806869490569e9a42d4e3ceb227d8936dcea27cadb16a86fe6c116e60751afc5354f29f9824dd
	<i>y</i>	1c7e890ea76ecafe28b6545a2005b5df5fc23918aa6d4c81f968108ff565fbee01882dee44b23fb42427d8945f49f6f4
<i>g₄₂</i>	<i>x</i>	19f736915014c121612ff0fbaa4479edba30840736d00f18d9c08cfe1770aee912b516f82a71f17625bc10d56ea75586
	<i>y</i>	1a5a311894e90d019fa154c68907068d1a2907e33fd683614fa02ce9e22d4cf40f9cb70ffa74388341e90635a2e260f4
<i>g₄₃</i>	<i>x</i>	29763735c7f56bf6bd7a1b6a1f2f87bc7cd48592270af465970531d6d9fa9a299c4073c2ef5ed3f9605c7dd433b208bc
	<i>y</i>	7484ff6532c7fb294ed4774a629aa2ebafd02b916ecd9184c134c739cd2a592a40984cd21a61c880067eef2c960b23a2
<i>g₄₄</i>	<i>x</i>	82ded039577f4e1db38722200adc9deee477c892948432ea0382f3d314dccbb8944718fbbf92c31a89a8c10daa778ab0
	<i>y</i>	25810280fcf2809fb8e46ea5f75f9c8cd4ae3e560aafb5a0fe8bce7d8ac2811e713fdfca7c2814841e64adc32bfb662d
<i>g₄₅</i>	<i>x</i>	1b41502ecd20817d3c85e7004e669638c725d1158aa803d105abbf85955185598bd316fbbcle9da4b0ab467e34172d41
	<i>y</i>	e3708f721dc69f92af811776fb1e2480251b204f5b1cdf4adaaed66b0698bd9fa66623c5bf056bee34f8cba26944a7c
<i>g₄₆</i>	<i>x</i>	4ae576a41641ac9cee68d76168ca2dd3a5a8a1c2d1b0382df8c4bf77008be3b22d16bfa9da4a5a1cd277a31369ad04fe
	<i>y</i>	53c8ce7a42d2b8d5b94095931a005bd320593955e641b9d41102f81f34465ed967d69992b7810e0b5368e11fa9bf4bc2
<i>g₄₇</i>	<i>x</i>	e2ab8753b11ec352fbdc31819af1937c1d722d100b6d8a0a9dfeaf5bfe261f78801a0b80a2028c767e5790cea94eca1d
	<i>y</i>	4d7c71008a50d8b5f169d23d5821624f6879d3d6924218a94bbf8d69725770773aa87ee4cef01ce6e29435249117f6f
<i>g₄₈</i>	<i>x</i>	37588b4aca0fc5abf529046072e233f77c4b63d97d2a33800c1062c1196c53098e11f643cec1c54abaa6a9b27d1deb7b
	<i>y</i>	c19cecb06a2dc7d0ae76ce2c450180525e3dd02b76d8097ed440bc8d94105e6b6ae57ccf33c902a40c45fbcffd6069f

g_{49}	x	ffedb2a5735c6eab4d3a26ab3f716ad3652f1fa704ea4c5f064e09df59e064fe9aab89b611d0524424b2ec4d35413567
	y	8af913bce60e84ea81c3d7aa637d4077e9a5cc4fa6a801dad9dea69a56cace6fa38b891e3dfa07f2c6bfa45c480f42
g_{50}	x	e51a94f1bb056052f468e2f21bbc5ad2f672ed3f837de089bd59a9c75a7bfb97fb87103ffff415fb194ee8b57f2dcdb25
	y	1b5f770ebc9f6741f97d4e827bfd6acc592ace08107db26f3eb428ee18cd197e72b949e6172545dfdee04645571a3dc7
g_t	x	ae141e91578a2667f7b79061e0a0f5b9e459de3038c697753d2f7ee1c08a662316da0d04c5d2115cfcbcd003e51b8e38
	y	4d4d60f7665183483c8bfb466c36bf1e14837a7753a0dd1dcc036d91af53c10cfe765ac6190847d2f6683b78e1e09f0c

3.2.4 Device generators

g_t	x	ed14ac907cadcededdbb772a2c209604fad1b43bd85acf2df50e848bd9aa5b99b65b6a87d beac90f3301e8c9d45b037f
	y	60448878dc34ae65673d982ef300a565ac0b46510bb962f1a00c459dc969e049add21121 0607db5a06f102505067f598

3.3 P-521

3.3.1 Naming

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

3.3.2 Group description

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

p	1fff fff
a	1fff fffc
b	51953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e1 56193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
$g.x$	c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dba a14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
$g.y$	11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afb1d17273e662 c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
q	1fff a51868783bf2f966b7fcc0148f709a5d03bb5c9b8899c47aebb6fb71e91386409
h	1

3.3.3 Issuer generators

g_1	x	1675b76e4f21cefb11ffe81f3137c19e69992d144033f23f3930d1d5b013ca81698a155f2298500caeee36b13cef52ca1c421286ae59f68684c8578628ba1273b65
	y	c631e60abcdbd970136201e5a8e4359f8cd3169cc396456b9a12d04317b3bee9aa27ac8fd84e67a61934c63d1d95cd3f89003fdb57bfcbb71f811feb596daed7e3a
g_2	x	1e565ee2801f3d822664777b08b43f2e50b60aa669eaf9870b37fe8f73773b8f92ebe0c0519f494bf938d55072dbea59395036e5c0ba68b885ad2abb47c6402b463
	y	7233dbf746dd2c2bf62a860f36450caf295d88d395521d7356c960f65578fcc82c29d6c066f2c4a0f548f86cc1bc7ea12ea7d34ce241d198f954d98c4f667878bd
g_3	x	163e41f82b9d756c774aa84a2089e7dab68a64454912d90e3cf37f9623fbd7c7402417f66ae17519db4c6c698bd853dbfea2fd3ec78efe887d1bd887cddbba0bb06
	y	b0811bd82aca459f969cb5e4642e5b67b52dfc9674e2ba3d24ece862fe79ac513ef65e8c9d3f73bb28c84f20d6b457c1941436e0f280bcd76123f7397af3a0fb8c
g_4	x	1bc68e0cccd3e2f0627589106246317fb73346feb916e2ca613c388254dd6f0f621a9a5f56cac25c353490f432e9dca76ef5a2fffb1851df892082c6d583f4eaa31
	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	431df69b022004caf4c71ece51693202b510f40207e4856e94098215c01f55c19a0728c7481cdffc24b2f80d1d229ecdac1f4d83e8c466cd3586f4e0d13ff25e988
g_{11}	x	1dbac6be0860787def03ffc5472dc23fa06b15af01cbf8bee8f5a0e71ae28b5ecac96fda82e8574741c219fa62d31afd658bb9578d59b279df0949063122665cfb3

	<i>y</i>	36da1a1fbfa65c4ee91d836c2f424ab2845cd6eb7962500665f745c7a83c4da99e07cf2f57d99e5769bfa70bdbde84ede562504b8e84b2c1e159f0dbb9eb58549b
g_{12}	<i>x</i>	eda625de058340213a859df97481c06223337ab42e45599bb5431960d3b9c433d87e6df01bdc895a3c100cf5bd357e42d4cd9eb9eeb47e1929802c20efc65e9e044
	<i>y</i>	c90a0efa16c0bb698e2b67b5bd498a02d8695c73f2626a96dd85371dc8d236af6f234293d09622aa1058859b36961fd59f5e28cb480c202624bef43186fccc396e
g_{13}	<i>x</i>	5f8a499b93c10c49e1e29ac7ba42671fb46ae8d0320bacb5f018f450a5877c0c63656eed3c8043bfe12c9346a6ae1f81ddb90f96a0faef9def3a986becca856fd
	<i>y</i>	63495d5eca21f270e3d599fef3492230eca64c712bb3100b14f4ae2b6218ab68355578ca73a26af4c802021f3a299c84d343aaef237c1ad20503532a468dbef9a5
g_{14}	<i>x</i>	aa86fcd11cb4e5156021f511c2145df198d8fc07e437f7495604efd387100d6ac338934e4307376feb1b9cd231f7e74e1fff768165189442d6a851858db44c3942f
	<i>y</i>	46e345906c1fa961a70cec671fe984ad62926e26af0e49dbaf78081bd4c80af1426cb397e9d414b7c2e83005be4ab1571f2843acd4834d160b38f4704c1c2d1a37
g_{15}	<i>x</i>	60ba95387d52d6f4225ff4c240c4eb061d6da6019467f4a84584fae8e685eaec078f0064c6fc0b5b5e479bda8b19508f64aa6f6bd321ba3bb5599b1fda0bcbf0f42
	<i>y</i>	d0fad9201e634b41f0b9fc7597b77b2fe487e12b83369fe7ff0b65abddac92a02deb1ac54c8d6e0f5e55258430fff618fd1cbf039490a03e26e61104d809de41e45
g_{16}	<i>x</i>	1ecae8827a7b0947daa185e92900e5c5ef25dec1f0821b8a6974bda8192c07b3a3c6769adfdb857c73c9674ead26a3b57a56fa6c15a4732c4bd63061e1cb8d72ea2
	<i>y</i>	75d01f5d3b388a16546bc83efa7f97432fd0071ec7e59293232be9c6aa48d1ae5fa74ba0dd8b99eb8409b54d6d811d164af43085ef860a3a27777c033624a8f669
g_{17}	<i>x</i>	b41a80d0cdae1d86bf0321a9ade6bf3cc1d60bbc32a8cd8ad232c8228e9c15e75cc372d6ca6e5ae70de5fe5202883938b42df2236643569c0ee6a73e0964548c1d
	<i>y</i>	44bb4ea0659a27e612ac00887949400fb8f41c9eb5daff89b5ee4ce979fa1d73b5eada1f6037c8e016e44c1c8a4f9dc2af487cd92a19f450bd71bb4d723e9d04a9
g_{18}	<i>x</i>	d7ea7e804529f3a0889fec632cc6907a24389bc0ba1ee0f648d52e0c0d91744359ca945e0294204a9d8a9056cfc16a01384f43c7b0fe207f37a81ad158455831b
	<i>y</i>	85fa66eede6d452d4c80fb9243bbbcd5500d7c37a87ac687a49ca020bbf00015acd5d427b2e20e733a05849cc13d2c2045c5333d7ec10cc8f2a63f63fe781cbd42
g_{19}	<i>x</i>	6ce87f9f5b5b6fa0fbc51c2e3a2011530bf216cc03cdea0c352733a0dab6efa7ff77efb21698d6a2a30697e35b128c6ee2a02ebc946b7d01d6aef9c4381c12925f
	<i>y</i>	d6031016603250135e19f6bb8086b7519d223b083eb833f4eedb018c5a826ce2092925b68f8b3c825768b587e7400c57be2cbd5af2da4d9adbfdade09641f3eb6c2
g_{20}	<i>x</i>	1074f1716ca1df00f49490c85f9c4be238ae3529ec6b2c49badcf702f90b4bccf915146fbcfa07cf20498677e82f47572bed9e2bb585468a9647df1aa65b10b4bee
	<i>y</i>	e3735d881a471398c8554ecf7d25f5c87190c6de1a04b5c13ed168e2378691266fb98f5bd5f3360cb669cd9a4db32f42f602515a742dfec7ada842d595da6c6e3d
g_{21}	<i>x</i>	4e0aa3b9c2e7147386fa7bed543ebdd415e8c33213c15e28aa8a003e5db378e80cb1daee6002a514a6739c8f618d71104dbcc9d16c7191ee65c967cc3068e71f24
	<i>y</i>	8437e93bf86dbd0eaba383ef307ddb98d27ae63e790338e85b2781680ab0bbfe1712478568e12acedb976a8f38a255c870ac5f97f45141c097746377047927165

g_{22}	x	126b1e605e3bae456c986addb6eba0f750229b3f971235ea827a2e16f45f3a938765af0a0812fa2af0199e2e1801679e43a1ef9421732595dba7e71d9f6d68c30cf
	y	fb8640e49a5fa09c4fcdcf2c37611fc397f5f7b5991709cc6783b92885ee97984744451b533d5710c8b801d5e29ce2e373fc325f329a7502d503f423eb2a3a9d428
g_{23}	x	8094e94e1983a7611a0cd624d94cfa1b3c1e18ebd2767f4f4146c573df368281693ddfa526217a0d935d2256a526c80fe54180d63b44c5a3c44a528bb211d0d40b
	y	2c57eefc512d830eff90f8aa41f867157926ae53727b3651d296a6703878f96738fb308f85cb1530b39ed24ccb60eaaef80aa22f1ca5e9ac794110ac6cd048da9
g_{24}	x	1ddc9a991f6180abefaae9351edce524db8b0d7e427c3eba58817a508396f2dbf6e1a7543627e05c3bbe65dfe40d0b33189401ef19ab1b16ff33bbc443a5fe547f9
	y	fa05ccbe21e0bba18881dc662ab29f3d9c96110b2ab60fa5503221377acfb04851479a9612dab994da5672571dc5c4393f75b2c84aab3fa6a0c4497f0e55b12cb2
g_{25}	x	1eb9035840630ac6fd0a30173a94793f7e81f34455e2e1a600fdec09bb6636163c6c4b24175b56053e67c3e374d35739be31819cde7befc42ebc3aea0abdd03efc7
	y	da5565b4f616dce18be9657f386f0c2792fcf0f602c6acf84fcb976bb276d6d84977875dc12f887654ac7c2873c3aef1c0d45cddce4cd63328598a67b0b222bf
g_{26}	x	12a8c695c849614e9a6a1d4b3988b6a56bbceb780d1cd2b2be337b1720a27936fb05ecfa21aac9e99b7031bda9421b5b3b9555baadac96babce8a7ee4e1e2657527
	y	c2c28763fd1e392d07ae2ed969912db6c78b8bbfa216e5652c6fb47731ec455938da25c17fb582ea502281030849726f478cad1a8b56be921a90b53610b62a09c
g_{27}	x	130b27465ad69c6732cda118050cddda2881a0870f1ee9cebd81a5656755cb6b080a428938baed1f7d6772a8f559234fba20fd300f91d88cff99b794f1fad6479d4
	y	8c6573a89d9b48d9ee8474d747526bcd74b20d545c42ab7550d6f49061fccb09579c39e670bc04be0820bd2fc39a5411486041ba94e4b4056a196b076a222be01b
g_{28}	x	12caeeae62f42d13141fc28bf5232f95dbe9dcd721b2599041507da3a5c1467a19fa469ba09140106622e67771f332e19b3c173afd1e23d845db9600be0755f85ef6
	y	ec2f9195d2bf0f749f1a73dc13b7618924b3d379db2129137188b9e8e55335c096d63a27f5bb02f5b4f5acd7c5c4ba9a7bfbf8beaf1c3747d94ab2fc5f1310fed8
g_{29}	x	c2182ba6e820e8ad89ac8f62552160abcabdd147e63f769adc69a623ebec89102aa83dfa2d6d6af6263b497a7150610eba6ad98297a278eb81d662c2def38de040
	y	9ae7e0671572619b730b33abdc8c9a4608d641e163456310be94cf55ae4c925c6fe63a081fb1419b66c3a8fc199e7ecb114a9bdeb13ee7acf3ac7edd43f7223518
g_{30}	x	517c312655635d41df5efe8f8af30677e0e3cf5add48aab157f45dff6215cdcf5f5c1ad4dc3474bcdd401bfa8b77103b20c9c28925a18ebfeacd8d2b0ald52d48d
	y	5d6830d33c7edf554d9f14c9e6ee502966f833a1c5ef506b6ef44b9171664e99e5cc1c8b09d704ff9e72d0c60e1f7ce6e6f8989a88a03b1c300734f094c2c5624c
g_{31}	x	6f2017da1d5c88274584752c8ab8c7ef8ae7f6a9eceb3a8b3b9af16b5e0347b01fa662b0db27fbab75749ae68357135f3dd2544d2e1a7d9594bfd7d7ddf9d69c25
	y	d62195e14e6b29654147db19d02cd73381020d7a5559880e3e2f41343ef39bd29b613d8b55ae33d559df36a17d1fa4dae0b5a352f459168f94d0a5b4561470272c
g_{32}	x	1f666425fa8bde98bff138161796c12e0e1e485eadacd0ed5adab17ba92b3a29328fe057196d67a036c922f087436e98187a425b9226ae75a0a91b848ada67a9be0

y b78d8152baae1fe290183564ec0cdeddef6249220b986df8bbf3cb9a047f066279d3cd073b5d8f18508a17f7afcccf40758324fe251c54e2bbfdd2be16ddcd35acc
 g₃₃ x 1c78aa5476f6cc9b6d22c3a258bebc1df2ce2e391dc775b814cece94f64fed29c0c9a40ae7b78f2181af163dec8318678493d1b9852606e58f963754652141cd1b
 y 3e4c468142cc1b6fb64117c6697f29c336fdb272a483642339d838220603e11d4c6dc80b7b1e5d1321ab11a02d7d81a25a14eed5808c7a095481c7b9216d076580
 g₃₄ x 14be306c2a30c0b90a741a37de382b565a0787471dbd3726f3adede7ab1fdae81be595ad95e66d7e2dcf5387518badde3128e18f32bc198cb700fa3b8b0fcf3879b
 y c867c121cbb34253c6d4ed65c70be22d1617b6900cabcee928e76b93bd16ba13d493d1c71e627094dd14d6a1b2cbaea64505cc55249c9786971703502723dbeb23
 g₃₅ x 1f97325c455dd3b04d58a79c76d80e419d6e75827847a4b5148cc327c340de6670aefe59988c1b6149ad39d59498afe434fac286f51967de9e126e5a23a31061c82
 y 1aa422ac52f5084393f4640768edf0c2858f79086f924ce3c180b7f11d91c8d4235f9f7457593ec821dda06a10792bd69ec341ba84b12608342cc715d1cd342ffc
 g₃₆ x af4b0e427400a864af899a2a56cf650ef4d4a8665886027bbcce7c1004dd725eb4bb62d1b73c5e285cf2aed3cd490c06fff2a1613eb661f8c0a86738caea2f5d4d9
 y 3494aa6e02e8143a857afc9a6c79e86c31bb5de7a01bfcca4a57572fef373a3436e3229944cca15e526528a22b0fb1a3515695a8e4df14188f81c555e7807a3f78
 g₃₇ x 3593984917824df5c94702cfd7b05b3eb1abf73cbab62a43df9671df6126a165a2727d27997a2b911dc1528fe42263477ce2e8ee8bf1ec22c932459adaa3758e0d
 y 3e000955d568b335fff04c7f011f8b0aeae2ebd066f85bde68882fb840d05b291c94f266e82664f239b968acb220411b546d46cb6ce72d98cd7a6dec54e2469b632
 g₃₈ x 19320c9939df24711f9844f0312aab80e447699e4d072a2d9e80a29dafe86caf058fab3a8a8d4975515864c2b931c7f7db3b25f2f5f9e5f8b5315a681b393b08a7f
 y ab49050ea49925fc1cb86acedf4219659b2490e91b09f425bff051600a9e31464e2ea96974545b7c745838a75a49c88bcacd837ac8957fc14f711dea93070f3d99
 g₃₉ x 12ba5b532acb5ceee9c91a325695786bf7e1842b831f8da30d360d428ae533ef2d1071e8131f7a7a729bc2ed19ae0c129b8ab0377fb55e019e64932eb28f80b9334
 y 803c8ebeaa493d6fcb356fb2562b79d3a376b5bcbf9b22bbe75611075f7b7ab16666abd97be5b7ecb338841fe77ece135f4e2e4b83acafd71e704527a84789468
 g₄₀ x a092eeded185fa7682ef7e4b2a198a4ea043a5eba62b4479a8657d66d9dab7c5de65e47642dcc62e2a561eb494f1e2748cdc792f0114c77f52b7d7c5f5c4b05883
 y d74a594a661d40ea629702dd1247808fb288dd5040e5410d7d6b04591e39696bf29995a3523928413d746acf2cdb55c40aa084cb65a289bdfc8501fdccb40209f9
 g₄₁ x ef451e110daf9d5e391a5359934a9f6969517f438c7bea183d5e96290ddce120873e45486d0c41c887c483b4661dfb48d8d72c0fb89e87e39c8a3716e9cdc76ddd
 y efa5c68d14de0eff1d729005e26e74f49f8bc083124a432ae18dd5131c04776f59a3f93274c5177f3c91a20160657a114f5bc0dbcc5c8069984e341320412adfla
 g₄₂ x 118713fa11a53a24b33f9e156cecf8b415874794508fe5438f8c4dae138666a5b888e8e99438dabc15556465747116ac472ad95d2920fe9b36f30be0963d7e0db12
 y 954bea5f61e4a9d8d093d1b9d6ab52b2fac8b78655802010cf5ed97459864271ef4c34d8044c26c7763de328e509ef0a68c1173130ad6301b20c3bc8f8f26ad296

g_{43}	x	1210b8efd90f3b9ec0d8f3f82f6878abf54a88ff06872064eb7f4e903b530945c5a7f0be3b30d004801700ae3dd25327f4bc28608be512f800a8454df8d15069a18
	y	8e6efc12aad547b3e08d39f7a79e9b034616f098175f716561b7927ab115a54be4fdec3845f7f5358828f175b83ed25ef2492c87296d6d89ecb9881104be9be7d
g_{44}	x	1fbd78c94ec52e5d769392cf084c5e629b29cf6e3bba7f3cd0c612c2f610ce388bb72a9c7d4ddc3f5612086cb42bf340f1e4ac7324c7359ef3351095cb00a7a304e
	y	99dd83d1b4c0b271f51c4851b236ff7b7e866266806847961937ef20aecc988122c076032674be513aa03946163477ddd205945b3917d1a3fcccc2ba9d4205aff7
g_{45}	x	eceadae3607ea6aa2b654ff67f0c1569acc323ba3e6dcc5af8ecea30bba435be1a629a74d9e23736fb93f3beafcfe2d36d59e23317bd0fd1f959bd4586e79f89e
	y	f9735628a382e2ad84fd1badebcbf6c9ee5e39789391de6bfb409b0adacc173105054118b443cb4eda232428f4413183a56486d073b84a56d89cb721ec985ebc751
g_{46}	x	d225f39d10600cc761c17fe15ace8bbadc776aba28bcbae482d15f79fe38dd0bc2c9bde12d6ee250489d0e7a23488711857fb913de74441676fd3c98da4e8fd8f6
	y	97b3f435c00416a59586e7593128c12b734723aa887f98a0b482d18d38707bb933e4b4bccdc71075f5174e8f2133b74b544b29a796b4fd8b783664af1d3659e99
g_{47}	x	dbcc8bb88c00c531890bcc22a2f221b8ca916b9c324c081c7123e5ca66069e0bcac91e09bf95fae7d15f8aacaal726d70ac03057f7d86f0e27376cccc1fcd7b8c7e
	y	2d4001615d625d51263a6f7bf263c0e21c656864bd9b395c1734366ce375518c058a34e74811c14ca07227baa0bd0b59c95356f47f44f390c6a4d16c4a6e0c6fec
g_{48}	x	1045cad535d9236d546d0a1385a3ea41e6586ee0a76c6ff5b81cc887cb58ea259e55214c8289160dc1921c412e4158be0cb54b80641cb657c873a5ca84ef0e5bc5a
	y	56ec9f00a5bd39a7857836235a83f24b21ff89b85484c8a795fe3e3baeed8532ee2b94198c9882035c77b1e75085c5cb936df3063e7173592e2749099a62247d6d
g_{49}	x	8b7af7378ceae85d550bda52ec6744133bc0ed593d612a4718a43b0f85b057f79f434629b170d203a57ac4c006dc4c87b5c92fa7d4af37d5e3651a141531fc151a
	y	9440c6216b46107b253c40bd70fc5fc96fe9b886cf32940958a8024c08595f90a6d783f40a48b1ea9bbc8e0adbb8e4d87300aca7f712a8020b0c43d3b1fd794b1
g_{50}	x	63105a1ff0449d4d5d788395ee7141fd5c44fd0227b3bdc32b9e9d26be5c7b7945faf8ab247eed6e50cb824abe7f5c4b7ed9ed725892d277ada462bb4e72dd5e6d
	y	cb0280e5e9293d2db08d25caad1e7b49aa52fc854fa49402e05e4b6fbcbf0efc1764834c1c4ca13a36ca20e8b8f57bd77aca8f52be06bd9a6929f93ca172d3d86d0
g_t	x	d0bfc69d957f2fc38e5170ac3aae81110dcc7a077c0094ddd29ff12057fcaf56e8d014d016998e44710db3fdf72da65e31cd665abcb35308a6b0ac5f18b3ffb6f7
	y	bfaba1b7ea54552b938ce89d0907797f5f55dd081ca3fb5cf01f2606d464e36e3a37e050cfa0fb9ceee03536707c6d117665b3b1e8344d66939b29792004475053

3.3.4 Device generators

g_t	x	15f3ae2ee57671e1bdc87047f34cbe0aabc693f463b13d42df6fd10f86cc7b4b4b999c9c38bdefa8e13c70174f1be79f8e934a3a01803073b34046b8d8ffc799342
	y	f0984ac43d1a34d52143f09abd1746bcd11e5495a096e307d1ab21648b1118c29c201f29d085d6a8a4da6cf760c818dcdc4ede01b411065cac92eealcc51bdafb2

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*, Microsoft, April 2013. <http://www.microsoft.com/u-prove>.