Value of s: 71f2791d84af21f123a826d7bbb33d8018fbae7607375461b1341a13e8238ff4

Value of M (enc): 

Processing token: business\_staff

Processing token: strategy\_team

Processing token: executive\_level=7#32

Processing token: office=2362#32

Processing token: hire\_date=1742309083#32

Processing token: 5of5

Value of q->coef[0]: 71f2791d84af21f123a826d7bbb33d8018fbae7607375461b1341a13e8238ff4

Value of q->coef[0]: 49017ad890b27f379c17f458506ad30885a6d51c5bfce13f325077721605717a

h\_attr for business\_staff: 025a52741cea7e054bf634c13675f8edb406d5c7ea6abc5705afed2d2d307ee658

h2\_attr for business\_staff: 027328d596c1f0c793b8aa136dd2fb2ba24e63d6ed36c752c8f0770aea2c4d106860e2544668e41ea2125051fed7a7a1f3b6994fa67f4b9bcbb8bd2d8e8647add9

p->c for business\_staff: 034ef07482898f48d632f2ff5a3d33b0a6b91dfe6fe7c115d6fc4ef8aeebd679ff

p->cp for business\_staff: 03207a799890fc41e0c1004b3f01f6823d338a18e16418b33fa4c1d9c88fa7975d2841ecd9e1d328ff95d0f5876ebe0d1d32eee8903a8a0a5c7ce6dce32a9feff6

Value of q->coef[0]: 3fce64304ef848b20077f567e9007fc2f7a0e7dbe70b74a17335374136841fd3

h\_attr for strategy\_team: 0229a208223c542443712220ab392b063338f28af88105d170d206205650c7eff6

h2\_attr for strategy\_team: 036a2927874d5be9575a3e8651e73a661d8bf92793ec98626027ad2978127bde1ea53eb08bf36bff5f5c5ceaaf8fdf290095700fe3463331c9f4ea40f62f439b25

p->c for strategy\_team: 02551989279aaef74b4219c4f8204381dffaa60bad9619097bcea7d78b451ddb8e

p->cp for strategy\_team: 02ac778f43a7b3e7365694a149cad11fb5d7b6d14c0de9528120470cbb693caf6d62c3135663d57d991af1e91c7e74885b736654f4757694f89361390b06ff2f4a

Value of q->coef[0]: 590d9c1a7e58303e418b8c075f17e0b813713b6318f81fde2e1a14672d413e49

h\_attr for executive\_level=7#32: 0245b66ab555a51f1c860c55bd67540d8ebe65093c436b09f11b9ff6f2679fa53e

h2\_attr for executive\_level=7#32: 02543f6566e1190d85e6dff85558b95b21ddebc7f16fe573734db110e9feb68c076c51733cd7318c1499e8a0f66622524e6b666c22c32426d8b2271d5bce0bda8f

p->c for executive\_level=7#32: 03831aee51e20ca540112a1e3adee17cd94ad4d61b5cb4dff10cf23d760202ff05

p->cp for executive\_level=7#32: 0372e7fd382dd151deece6b5ab1f0563334bb2f5163aa5e767ca94518b07b1fa5f0cf32c757508938d0fbc02fc39165f23e244a5c8bdfa6f01c0822d5c95f03d9e

Value of q->coef[0]:

3040a33091afc1c0cf0e4f8dc15acc2f82532aad089fb4190e06f3425d916fb7

h\_attr for office=2362#32: 020e324ed382680e4e8ee4a940b0e20c79444b785440edaecfc7aab0b9fdbb8426

h2\_attr for office=2362#32: 0231f82cb3dbf83658c92c744e1e8fc4f80d9cfa15a67f73f7a7cdf254f51ce8c89d973c8a5f05fc50f819de067586e35845914c5df1150ad16c43359659458fdb

p->c for office=2362#32: 027935586cf3bb4a8018c2894fc9bb1c94853507e8d32acd9f0ace945f388d0c05

p->cp for office=2362#32: 03359ae3d908c8690c1fda457d3bf5eca7e573d4b72e8754171ba877427a5131193dbdd42796a1b0cafdced5ae73cd06bf57b0f252090212e87e7247fdcf5cd806

Value of q->coef[0]: 663613afafe46182dbb40ca95f73faafa236558ae096abb3344ce4c8a15435bb

h\_attr for hire\_date=1742309083#32: 03a54311c401bf704843a8dff8081128b6138491ba4ea6f76f9d41d3658dcd6238

h2\_attr for hire\_date=1742309083#32: 02107817b71e375a9afccff43f8536776c53ab710e1bb3782197009a47e6ceedf5974d7b84480b1b43f9ddc1d0ea2083ea6f8a239e118dac254148e0bafd42a98a

p->c for hire\_date=1742309083#32: 032531737e5d7e7fc93696d656dc6b7d302266c42a238cf7518f9469aa9be75b60

p->cp for hire\_date=1742309083#32: 0367a762f692e2b9c63e6733dd177709f8733c9ebe863b045bace561296914b58706c20d155175a2e8a94cf7b9c3b8566e28d06bdbcdf8828e608d235cf5eb0479

AES key (enc, pack=1): 7e136f2ccf0a5a3f5fd3dc224ac29b4c

serialize\_g1: len = 33 serialize\_g1: len = 33

serialize\_g1: len = 33 serialize\_g1: len = 33 serialize\_g1: len = 33 serialize\_g1: len = 33

DEBUG (enc): ciphertext\_len = 8499, CP-ABE ciphertext length = 1179

DEBUG (enc): expected total file size = 9714

AES key (enc, final): 7e136f2ccf0a5a3f5fd3dc224ac29b4c

┌──(thanh㉿kali)-[~/Documents/demo\_cpabe\_relic] └─$ cpabe-dec pub\_key kevin\_priv\_key security\_report.pdf.cpabe

unserialize\_g1: offset = 4, len = 33, total buffer len = 439

unserialize\_g1: offset = 370, len = 33, total buffer len = 439

g size: 33 gp size: 65

unserialize\_g1: offset = 164, len = 33, total buffer len = 1237

unserialize\_g1: offset = 270, len = 33, total buffer len = 1237

unserialize\_g1: offset = 393, len = 33, total buffer len = 1237

unserialize\_g1: offset = 499, len = 33, total buffer len = 1237

unserialize\_g1: offset = 629, len = 33, total buffer len = 1237

unserialize\_g1: offset = 735, len = 33, total buffer len = 1237

unserialize\_g1: offset = 859, len = 33, total buffer len = 1237

unserialize\_g1: offset = 965, len = 33, total buffer len = 1237

unserialize\_g1: offset = 1098, len = 33, total buffer len = 1237

unserialize\_g1: offset = 1204, len = 33, total buffer len = 1237

Before IV: offset=0, need=12, file\_len=9730

Before tag: offset=12, need=16, file\_len=9730

Before sym\_len: offset=28, need=4, file\_len=9730

Before abe\_len: offset=32, need=4, file\_len=9730

DEBUG (dec): cph\_buf->len = 1179, expected = 1179

AES key (dec read from file): 7e136f2ccf0a5a3f5fd3dc224ac29b4c

unserialize\_g1: offset = 264, len = 33, total buffer len = 1179

unserialize\_g1: offset = 335, len = 33, total buffer len = 1179

unserialize\_g1: offset = 506, len = 33, total buffer len = 1179

unserialize\_g1: offset = 684, len = 33, total buffer len = 1179

unserialize\_g1: offset = 856, len = 33, total buffer len = 1179

unserialize\_g1: offset = 1037, len = 33, total buffer len = 1179

[check\_sat] leaf: policy\_attr='business\_staff', key\_attr='business\_staff'

[check\_sat] match => satisfiable=1, attri=0

[check\_sat] leaf: policy\_attr='strategy\_team', key\_attr='business\_staff'

[check\_sat] leaf: policy\_attr='strategy\_team', key\_attr='strategy\_team'

[check\_sat] match => satisfiable=1, attri=1

[check\_sat] leaf: policy\_attr='executive\_level=7#32', key\_attr='business\_staff'

[check\_sat] leaf: policy\_attr='executive\_level=7#32', key\_attr='strategy\_team'

[check\_sat] leaf: policy\_attr='executive\_level=7#32', key\_attr='executive\_level=7#32' [check\_sat] match => satisfiable=1, attri=2

[check\_sat] leaf: policy\_attr='office=2362#32', key\_attr='business\_staff'

[check\_sat] leaf: policy\_attr='office=2362#32', key\_attr='strategy\_team'

[check\_sat] leaf: policy\_attr='office=2362#32', key\_attr='executive\_level=7#32'

[check\_sat] leaf: policy\_attr='office=2362#32', key\_attr='office=2362#32'

[check\_sat] match => satisfiable=1, attri=3

[check\_sat] leaf: policy\_attr='hire\_date=1742309083#32', key\_attr='business\_staff'

[check\_sat] leaf: policy\_attr='hire\_date=1742309083#32', key\_attr='strategy\_team'

[check\_sat] leaf: policy\_attr='hire\_date=1742309083#32', key\_attr='executive\_level=7#32' [check\_sat] leaf: policy\_attr='hire\_date=1742309083#32', key\_attr='office=2362#32'

[check\_sat] leaf: policy\_attr='hire\_date=1742309083#32', key\_attr='hire\_date=1742309083#32' [check\_sat] match => satisfiable=1, attri=4

[check\_sat] node(k=5): sat\_count=5, needed=5

[check\_sat] => satisfiable=1

[pick\_sat\_min\_leaves] leaf 'business\_staff' => satisfiable=1 => min\_leaves=1 [pick\_sat\_min\_leaves] leaf 'strategy\_team' => satisfiable=1 => min\_leaves=1 [pick\_sat\_min\_leaves] leaf 'executive\_level=7#32' => satisfiable=1 => min\_leaves=1 [pick\_sat\_min\_leaves] leaf 'office=2362#32' => satisfiable=1 => min\_leaves=1 [pick\_sat\_min\_leaves] leaf 'hire\_date=1742309083#32' => satisfiable=1 => min\_leaves=1 [pick\_sat\_min\_leaves] => p->min\_leaves=5

[dec\_node\_naive] internal => p->k=5, satl->len=5

p->c: 034ef07482898f48d632f2ff5a3d33b0a6b91dfe6fe7c115d6fc4ef8aeebd679ff

c->d: 021c507a3015a1fbcc06716552c67dc9dc08c007ed1b8a724f257e6a477527e9c9135532454c0eca703eddb087f8dfee26e3f70df5daf31699c9729096754f49a8

c->dp:

0330121202d65fc2b713b753a13dc8d53f85a2620f0ebb4043050a68782a9cc441 p->cp: 03207a799890fc41e0c1004b3f01f6823d338a18e16418b33fa4c1d9c88fa7975d2841ecd9e1d328ff95d0f5876ebe0d1d32eee8903a8a0a5c7ce6dce32a9feff6

[dec\_node\_naive] leaf => p->attr='business\_staff', attri=0 Intermediate temp: 

p->c: 02551989279aaef74b4219c4f8204381dffaa60bad9619097bcea7d78b451ddb8e

c->d: 0232c1b043f3c0325a72fa2cad97d5cfdf8a1f916eed3eca58be47e18690fd8d9596591b4b7761882bf5abe7aa59bae34e5934db158eb2843da124980092090afa

c->dp: 02793bfb5a107a84fa5040e46843dfabd47bb5760f84bc81e0eaa0eb83a4fcd6cd

p->cp: 02ac778f43a7b3e7365694a149cad11fb5d7b6d14c0de9528120470cbb693caf6d62c3135663d57d991af1e91c7e74885b736654f4757694f89361390b06ff2f4a

[dec\_node\_naive] leaf => p->attr='strategy\_team', attri=1 Intermediate temp: 

p->c: 03831aee51e20ca540112a1e3adee17cd94ad4d61b5cb4dff10cf23d760202ff05

c->d: 0399a2750bd330f1b3a9746918725c4f3fac163064a5dba028b23f461ddb3f70b92bd26a89c881ea2e31bddaef85583e846d72730eea269c09e15ebfa8d09fbf50

c->dp: 031ffa8cd57d24e8db3839ee22c0311231cc9f127dca1ab6c622f551b6fe2f35df

p->cp: 0372e7fd382dd151deece6b5ab1f0563334bb2f5163aa5e767ca94518b07b1fa5f0cf32c757508938d0fbc02fc39165f23e244a5c8bdfa6f01c0822d5c95f03d9e

[dec\_node\_naive] leaf => p->attr='executive\_level=7#32', attri=2 Intermediate temp: 

p->c: 027935586cf3bb4a8018c2894fc9bb1c94853507e8d32acd9f0ace945f388d0c05

c->d: 0263114aec7d78824045c3c419b1f1796d7e243b7c0dcb5680b7dea41b0ed58906a21277278fac4c6f0423410ded12b64b18ab6acb051ed3f2686d96d978299744

c->dp: 023027340048275b11af4f9b652f73019e2de270d92d831b56af00bf9fd5910469

p->cp: 03359ae3d908c8690c1fda457d3bf5eca7e573d4b72e8754171ba877427a5131193dbdd42796a1b0cafdced5ae73cd06bf57b0f252090212e87e7247fdcf5cd806

[dec\_node\_naive] leaf => p->attr='office=2362#32', attri=3 Intermediate temp: 

p->c: 032531737e5d7e7fc93696d656dc6b7d302266c42a238cf7518f9469aa9be75b60 c->d: 033527fdb88d8f5c20afbe2f748da794a83a032077f3100b490811b5a955c107dd5d20068d9d5cd34b0320b08816fa43a5bfeb8db82498ebec560d05562bdfde5f

c->dp: 028368de27737707ff4c677646426147e31feb83ae0f4a10fb95e9e58d84f3d622

p->cp: 0367a762f692e2b9c63e6733dd177709f8733c9ebe863b045bace561296914b58706c20d155175a2e8a94cf7b9c3b8566e28d06bdbcdf8828e608d235cf5eb0479

[dec\_node\_naive] leaf => p->attr='hire\_date=1742309083#32', attri=4 Intermediate temp: 

Value of F: 

Value of m (dec): 

AES key (dec computed): 5bea5850cb0820f0015ea4df119e80ae

IV: f0ed54d785f5a8ad723e45fa

Tag: 3445472b660414677b9766d2d7c58180

AES-GCM authentication failed! Possible incorrect key.