TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 13462-2:2022

ISO/IEC 19592-2:2017

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN – CÁC KỸ THUẬT AN TOÀN – CHIA SẺ BÍ MẬT – PHẦN 2: CÁC CƠ CHẾ CƠ BẢN

Information technology — Security techniques — Secret sharing — Part 2: Fundamental mechanisms

HÀ NỘI – 2022

Mục Lục

Thư mục tài liệu tham khảo

[1]. TCVN 12852-1:2020 (ISO/IEC 15946-1:2016), Công nghệ thông tin — Các kỹ thuật an toàn — Kỹ thuật mật mã dựa trên đường cong elliptic — Phần 1: Tổng quan

[2]. TCVN 12853:2020 (ISO/IEC 18031:2011), Công nghệ thông tin — Các kỹ thuật an toàn — Bộ tạo bit ngẫu nhiên

[3]. Blakley G., & Meadows C. Security of ramp schemes. Proc. of CRYPTO '84, 1984, pp. 242–268

[4]. Cr amer R., Damgard I., Ishai Y. Share conversion, pseudorandom secret-sharing and applications to secure computation. Proc. of TCC, 2005, pp. 342–362

[5]. Ito M., Saito A., Nishizeki T. Secret sharing scheme realizing general access structure. *Electron. Commun. Jpn. Part III Fundam. Electron. Sci. 1989*

[6]. Kikuchi R., Chida K., Ik ar ashi D., Wak aha O., Hamada K., Tak ahashi K. Secret sharing with share-conversion: achieving small share-size and extendibility to multiparty computation. *IEICE Transactions*. 2015, 98-A (1) pp. 213–222

[7]. Krawczyk H. Secret sharing made short. *Proc. of CRYPTO*. 1993, pp. 136–146

[8]. Shamir A. How to share a secret. *Commun. ACM*. 1979, 22 (11) pp. 612–613

Lời nói đầu

TCVN 13462-2: 2022 hoàn toàn tương đương với ISO/IEC 19592-2:2017.

TCVN 13462-2: 2022 do Cục Quản lý mật mã dân sự và Kiểm định sản phẩm mật mã biên soạn, Ban Cơ yếu Chính phủ đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

Bộ tiêu chuẩn TCVN 13462 *Công nghệ thông tin – Các kỹ thuật an toàn – Chia sẻ bí mật* gồm các phần:

- TCVN 13462-1: 2022 (ISO/IEC 19592-1-1:2016) Phần 1: Tổng quan.

- TCVN 13462-2: 2022 (ISO/IEC 19592-2:2017) Phần 2: Các cơ chế cơ bản.

0x56e4df33d4b1036c,0xf51ca162795d1156,0x3a35b068fb3e120d,0x75c644944cdd2cad

Phần tách của bên 2 của t: $\langle t \rangle_2 =$ 0x

e102426f5a9b5a49	9fbf2904bde581f0	5a1ca0ec1aa56910	45de94124265332e
28b2f43aa9a55f20	e9e71c9f9603c80a	ea8f55eee3310db9	ee1ce5ed81a293d2
757160e701615d89	b66540cfe0f65eb2	bdb22522e79cb878	dd941ff9eed50e44
72371091d88e68cc	2a5792b59d7b388c	1c78d8f754fdfb38	950ec1d5cd2c0abb
506a4db2009c9b9d	beeb011413de005c	46023a4aba3e326e	f85a706d34fe19e8
3c82ff75c31de041	55fcf01aadba7940	127a35c8e347b5f5	555acceded9b832c
9d94f31551ac7772	5f9797137414f34c	0384ad2536994d7d	a353b731e176472c
7bbcf952e13e5a6b	890b492a60bbaf89	646f87ad2b232803	d928ffb2196ed428
31845f26683da2d5	9770c53439ade0ee	28de28b243f540b4	d10227aff80690f8
c78c3161db747c80	49323ba38d665599	eba4d2d9d7603a9a	b92a02f72b579077
430b331e434e9e79	d27a5246c5946550	68b05d74b069b1d4	b92b3561b3298c91
cc755d1f5d18ddc3	a663564d0ddacaaa	6a334cb6c163968a	5dfa5f6fe982214c
212dab63cd3de243	e334fc6b0b063be7	8b345949a0ef64f0	5cba1029283417e0
cba6598b810c42e6	f4110eaee335fead	099b38be85c36b15	eb1cf479bf7a81a0
62f03d69326d09a2	ffd52bdcf8896f95	ad0e958a478e57cb	459e6cdbd63817c0
70b2a6da8a617aa5	294fd9927ec68b5f	85d936b9db527ae8	f5a518fc2148f18e

Phần thông điệp chia sẻ của bên 3 của s_1: $[s_1]_3 =$

0x4fc6a6b6a3aba51b,0x2b860d2544a3086c,0x8229500623da6c7f,0x2f308e612492ad7a

Phần thông điệp chia sẻ của bên 3 của s_2: $[s_2]_3 =$

0x6f130eed1ca1c3ae,0xd6896e9c44e78fa9,0xef8660a3f670f87a,0x9ba706b578acc957

Phần tách của bên 3 của t: $\langle t \rangle_3 =$ 0x

eeac77ab2fd95472	741e08c1ac103eff	5eb2ca4c502a4b52	fc062dc269357f67
fbbac8e72cdad2df	49811c989f1ef03f	d7d5dce1f5c94538	8e875de76c4d4a35
e0d5d264a576142a	957b2939c86d849d	695cbe1548f944de	75568bc96f8b5d4b
cf6b53cc720cb2ab	743df918493e949b	bc623a8032df1f28	4b991b4b4f6e24f1
4cd309706af1c251	d7e68fb0ec123147	606aa63f6671078c	7845f771b1c7b407
e006d77cade61ee7	f63d1e0d045eb6ba	08c1f1bac5747aae	e255d0353c56eb68
f84da1c521d01e1e	a8dc9910cb7e57a1	982b72caa4c9dfd2	817d1612e4bd80d0
e80fcff0a57c6e51	e3021afd6a110643	45b240a2167c51e3	83a6e2a6427f7e0b
d6078c0af89051b3	4d03740b83f7ba5c	9e6ed28ee323e67e	f0394d651c3bcd1c
abd8809304879343	f2d699a0b299bf85	2809b0af41520aa4	16a5754e6b5ee8f8
2cdd8228b66f02ca	be6c39361642257e	42ea1b046bbcd517	0906ea52c20a447f
5260dab085b233db	053275df0648004b	9b9dcafca2bc1682	951cd720f9dc4575
2525497661552909	83b27bca84ea172f	fbc5c0096c730b43	7dbac332534d33c0
75de230c5e688210	3eac4b065e217f74	6e5dd8d817f3df55	50c18b13d75ad098
3a58291a4ac6cd54	bd435b153fd0b7b2	3019b2156df390d7	f4e19332563785cb
947012a33582a493	b50036f61ea8001a	9d294dba6f9cbff9	a5016d64d5f43d4c

```
bd5c435daa82da67   5e6a6badd445ac17   a01ae2776622e410   de97da9e82422e4a
1cb944c26a6d59cc   690d8ea4ffcc311b   26689c75dc4f35e2   801f871c8539adef
dc8428096efbfea6   a3c1ee17a9e4cffa   1abbc4722633cf5b   b70f1cd8d1cd6844
65d952d0707c696c   f74b0e03bf6aa4ed   9bafdfef925092af   222ea12305cbc7fc
93b336a24442343a   6a0953d70aaaa9ca   21ddc70f3d5f79e0   5a8e1d145b11aa23
e783d32c90adf366   da73b13fba5a5ab2   b6b0fa3ca0d6a6ca   213b6acae43d5de4
6c54b1f2dff3efc3   bbe4a2033fffea1c   c3ad62769632303e   af8f77b94009788f
6fd6b136f5219cb3   6c166b70d3d6402e   2a5a4670dbd564c3   b02ddf337123c8ee
9e1587afd8aaee18   a35123920b92cae1   f1ae864a63df8008   c8e6884f105e6439
0408e215ac68cb4a   608687a18fec2cc8   70f19940cc9c6fb3   2100d31b7b792420
be787a87df64c0f6   cabd45a8bd1481d9   67c6e0669230b440   bbdd7f6a68205138
58a8147378abc4f6   429670c9c759d827   9d17279f2a7dc71c   b17fffe9800f920b
e4c2b479bfe3de36   9c4fef64606e8b45   18f07b03b4cec511   50a47598f4bcccc2
```

Hệ số ngẫu nhiên của s_1:

```
0x7e01f1635b80cbe9,0x62a94e04c2e20edc,0x7bd35def99d695f9,0x3426b244381eed81
```

Hệ số ngẫu nhiên của s_2:

```
0x39f7d1dec810c0c2,0x2395cffe3dba9eff,0xd5b3d0cb0d4eea77,0xee6142213471e5fa
```

Phần thông điệp chia sẻ của bên 1 của s_1: $[s_1]_1$=

```
0xb3c5447014aa32c9,0xeed4912cc16715d4,0x758febd91077478d,0x477deae954af7678
```

Phần thông điệp chia sẻ của bên 1 của s_2: $[s_2]_1$=

```
0x1cfcad508c80422a,0x91a2f1603f92b257,0x44e1c135eced2c8f,0x476582f7104f02b8
```

Phần tách của bên 1 của t: $\langle t \rangle_1 =$ `0x`

```
f1f01c23c55d4804   a35c4b4b8ffb40fa   57ee1f0cc5340fd6   8fb75e623f95e7ee
5daab15c2625c93a   094d1c968d24804e   ad60ceffd839d43a   4fb02df2b792f9fb
cb9cb763ed588777   d347fad5995a30c3   c081887a1632bd89   24d3a3a86d37fb4e
b5d3d5772709067e   c8e92e43e1b5ccb5   fc57fe6efe9ad713   f6b6ae764bea787e
75a180f4be2b71c9   05fd92f9138a5371   2cbb9ed4deef6c48   787af948bbb4efc2
590e876e7011e3b0   b1bec22257972955   3db6795e8913e418   8c4be9849fcc3bfb
33ff0465c128ccc6   464a8517b5ab1e60   af74cd158068fa97   c5205454ef2a0f28
cf69a2b42df8063e   3710bd537f4455d7   0609cebc6cc2a223   36bad88ef45c2a4d
19002a53d9cbb764   f9e41674f7430f23   f30f26f7a28eabf1   b24f98f0d44176d4
7371e376bb604cc5   851fdda6cd666ba6   af5374426d366ac3   49bb9a3ceb4c19fd
f370e0455c2c3bac   6640efd7b1eea522   165e97e5dc161c91   695d5434204dd5b8
6e4bd5ef34e7eff0   439032fb116d9592   78c0c66865031689   04d1c7bed9608d1c
2d348d5d3984bf9d   42bf74899b324ebf   1a26f288f54bd425   3fbb6504a5bf7b80
092ed603e0a103e7   abd6c05724087cdd   a1d018153392b7d5   277b75c7071a72f3
8b0801fcbb9144b8   386fba86b16307fc   0a37fd2b39081ef4   961e6ce15628a1c6
5df57a504a4518e4   8d9fe83ede75168b   acc9bbbd060135db   044986553c8da4c8
```

Phần thông điệp chia sẻ của bên 2 của s_1: $[s_1]_2 =$

```
0x31c757d5f82b6ef2,0x492f4321864106b0,0xf9fa0de9ba0cf986,0x1b163c251c8c40fb
```

Phần thông điệp chia sẻ của bên 2 của s_2: $[s_2]_2 =$

Công nghệ thông tin – Các kỹ thuật an toàn – Chia sẻ bí mật – Phần 2: Các cơ chế cơ bản

Information technology — Security techniques — Secret sharing — Part 2: Fundamental mechanisms

Tiêu chuẩn này đặc tả các lược đồ chia sẻ bí mật.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau đây rất cần thiết cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng phiên bản được nêu. Đối với các tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả các sửa đổi, bổ sung (nếu có).

TCVN 13462-1:2022 (ISO/IEC 19592-1:2016), *Công nghệ thông tin - Các kỹ thuật an toàn - Chia sẻ bí mật - Phần 1: Tổng quan*

3 Thuật ngữ và định nghĩa

Trong tiêu chuẩn này áp dụng các thuật ngữ và định nghĩa trong TCVN 13462-1 và các thuật ngữ và định nghĩa dưới đây:

3.1

Nhóm abel (abelian group)

Nhóm (3.8) $(G, +)$ sao cho $a + b = b + a$ đối với mỗi a và b trong G.

[NGUỒN: TCVN 12852-1:2020 (ISO/IEC 15946-1:2016), 3.1, đã được thay đổi]

3.2

Độ phức tạp (complexity)

Số lượng các phép tính đơn vị cần thiết để thực hiện một thủ tục.

3.3

Giao thức chuyển đổi (conversion protocol)

Giao thức chuyển đổi các phần thông điệp chia sẻ của lược đồ chia sẻ bí mật thành các phần thông điệp chia sẻ của một lược đồ chia sẻ bí mật khác.

3.4

Bộ sinh bit ngẫu nhiên tất định (deterministic random bit generator)

DRBG

Bộ sinh bit ngẫu nhiên tạo ra một chuỗi bit ngẫu nhiên bằng cách áp dụng thuật toán tất định cho giá trị ban đầu ngẫu nhiên phù hợp được gọi là mầm và có thể thêm một số đầu vào phụ mà tính bảo mật của bộ sinh bit ngẫu nhiên không phụ thuộc vào.

CHÚ THÍCH 1 Đầu vào của DRBG là một chuỗi ngẫu nhiên được giữ bí mật có độ bất định cao và đầu ra là một chuỗi bit dài hơn, chuỗi bít này không thể tính toán được bởi kẻ tấn công nếu không biết được chuỗi bit đầu vào.

[NGUỒN: TCVN 12853:2020 (ISO/IEC 18031:2011), 3.10, đã thay đổi]

3.5

Trường (field)

Tập hợp các phần tử K và một cặp phép toán $(+,*)$ được xác định trên K sao cho: (i) $a * (b + c) = a * b + a * c$ với mọi a, b và c trong K, (ii) K cùng với phép toán + tạo thành một *nhóm abel* (3.1) (có phần tử đơn vị 0) và (iii) K khác 0 cùng với phép toán * tạo thành một nhóm abel.

3.6

Nhóm cyclic hữu hạn (finite cyclic group)

Nhóm abel (3.1) G sao cho tồn tại g trong G, trong đó với mỗi a trong G được xác định bằng g hoặc bội của g.

3.7

Trường hữu hạn (finite field)

Trường (3.5) chứa số lượng phần tử hữu hạn.

[NGUỒN: TCVN 12852-1:2020 (ISO/IEC 15946-1:2016), 3.5, đã thay đổi]

3.8

Nhóm (group)

Tập hợp các phần tử G và một phép toán + được xác định trên tập hợp các phần tử sao cho (i) $a + (b + c) = (a + b) + c$ với mọi a, b và c trong G, (ii) tồn tại một phần tử đơn vị e trong G sao cho $a + e = e + a = a$ với mọi a trong G và (iii) với mọi a trong G tồn tại phần tử nghịch đảo a^{-1} trong G sao cho $a + a^{-1} = a^{-1} + a = e$.

[NGUỒN: TCVN 12852-1:2020 (ISO/IEC 15946-1:2016), 3.6, đã thay đổi]

3.9

Thuật toán phân mảnh thông tin (information dispersal algorithm)

IDA

Thuật toán bao gồm hai thuật toán con riêng biệt: thuật toán phân mảnh có nhiệm vụ phân chia thông điệp thành n thành phần và thuật toán khôi phục có nhiệm vụ khôi phục thông điệp từ bất kỳ k của n thành phần nào, trong đó k và n là số nguyên và $n \geq k$.

CHÚ THÍCH 1: Không giống như trong một lược đồ chia sẻ bí mật, không có gì đảm bảo về bảo mật. Có nghĩa là thuật toán có thể tái tạo thông tin bí mật hoặc các phần của thông tin bí mật từ ít hơn k thành phần.


```
5699461e53388573  30c47eb03b0e90e7  e404cc834830ba31  2da271e611a921ca
006d46655c52ca12  fb6d414a0ceb8ffc  d9fc1c27b2bdbade  367532f4e40d48e8
5ac52978c1d4c000  86c6cc84925c069b  b5064a39f449ec6c  d7d1f440a938ba6f
eb97de718c67fdd7  1d2b5dd44e3fa45a  68ddb249d8de9a1a  14bc32899a504fe1
8476f6373db40eab  76dfdc48d9397e1a  5afe8a5949057586  b8812e8bd6bc33b3
4311bf6263556bc9  96da0be69b6cb635  fcc0e65e20d953ab  7452585378ed269e
dd8f4128eee08013  3b39e3bd19f22e0c  956f401e4f00b30f  c37a3cd9f12a6c26
68d6d314d6565012  d60bc626cb0f8c30  51e6375003747f86  9fbd9c5def83b88c
cd3b420d4186b2c5  68cce1e8a9e6ceab  a0e3ab8f3bace6da  d692e9cdde6b9867
b52acfb952704a3b  978112c2f8e1ccfe  0cf05a016e258645  f4a9296ddff62f13
7fab6690c778c5b6  524140113c10e822  b0076ec3ca1018df  6438398336c673ff
0125e968fffafeb4  6b7bc5c029313343  4f38b40bdcbd541a  0060333d73d785ff
0d47e353ccdd721f  ada697375b18d141  418842edb794dc0e  11a2ae94b9550ea1
85fa37eb52ed53bd  003e2bf6261adea8  1a6cf2c99409665b  b7758159e6d79661
b5df286af12459a4  51af54dc6323010b  5fff21f77e7ba9d5  6c5ee06b48211634
343708ccfb3bd7c4  190b269af67ec105  fee0dc005e51dd17  1d73b3786a01a4d7
c66d5da4b66585ba  893416ee4bca5bf0  0abc73225ca42893  b75c6e2576c1431b
fdddba304a1ca48c  e5b2a8bf9584d01f  359c035e14657e21  75f076cdf7fe18cc
ddaac20a16d9f735  f187062d42a91a20  297446c1f82c5eb6  010830c9fc38fd8a
856509b4204f7899  195eefa7b8441466  6c94a605ebede1dd  ec02afa14f4666eb
8a975e52e5974f5f  e6f0c0c73ee4f295  9fab5332e4ca7973  c5ba0a9d3e8f1aa0
e1bca72e8f24801c  502c76b6f597c224  718c6684e797fd36  eba690a49605d950
b5da2b6007486117  4863ed30c65a716a  8381fc0496e9de92  ebdac934d8afcdc7
a93ad96ae4b78d65  e472f11dec4a554d  033c0bc2cfecb5a0  15e9f4809d843c30
97469e7c018a9628  6d84d99413df93e4  41f48da750bb39d6  71399cb01102fd9a
c2c7e718a12e4af1  0ce81afcaa36fe07  d60910ee82bfc216  8e75ad655452ebdb
7b31d256405fdedb  c669c7c272b82b92  2b22f03f00db9c5b  3c52cfcff3708032
a7a7bd66e462c2ab  ad0efae4a4415d78  c7d67bf8cd1d5e60  ded73f4ca26da5f6
71903c60fb06112c  8c6e0ed4f66573cf  a92be21cc4b56a9c  32fcd6b416252110
ebad4cb577d398b2  0d4f95a5fd3ba752  e10bfa8342e0cc49  4686a5d5528c1231
74286d70660a77b4  dcedb52cfb1c557f  b00e3a5b2d34854d  2c313e013def2d44
3f9c551adbc1f3db  c7a03b2a7a768ca3  f1b84945f1e07a5b  7787f5e0b67654ca
```

Thông điệp đã được che giấu bằng phương pháp mặt nạ `t=0x`.

```
fe5e29e7b01f463f  48fd6a8e9e0efff5  534075ac8fbb2d94  366fe7b214c5aba7
8ea28d81a35a44c5  a92b1c918439b87b  903a47f0cec19cbb  2f2b95f85a7d201c
5e3805e0494fced4  f0599323b1c1eaec  146f134db957412f  8c113798ec69a841
088f962a8d8bdc19  968345ee35f060a2  5c4d1c1998b83303  282174e8c9a85634
6918c436d4462805  6cf01c5dec46626a  0ad302a102a059aa  f8657e543e8d422d
858aaf671eea1d16  127f2c35fe73e6af  270dbd2caf202b43  3b44f55c4e0153bf
562656b5b154a5aa  b1018b140ac1ba8d  34db12fa12386838  e70ef577eae1c8d4
5cda941669ba3204  5d19ee8475eefc1d  27d409b3519ddbc3  6c34c59aaf4d806e
fe83f97f49664402  2397a74b4d195591  45bfdccb02580d3b  9374f23a307c2b30
1f2552846493a306  3efb7fa5f29981ba  6cfe1634fb045afd  e634ed85ab456172
9ca65173a90da71f  0a5684a76238e50c  3c04d19507c37852  d9708b07516e1d56
f05e5240ec4d01e8  e0c111691aff5f73  896e402206dc9681  cc374ff1c93ee925
293c6f4895ec74d7  2239f32814de6277  6ad76bc839d7bb96  1ebbb61fdec65fa0
b756ac843fc5c311  616b85ff991cfd04  c616f873a1a20395  9ca60aad6f3a23cb
d3a0158fc33a804e  7af9ca4f763adfdb  9720dab41375d9e8  27619308d62733cd
b937ce29f5a6c6d2  11d0075abe1b9dce  b439c0beb2cff0ca  54edf3cdc831680a
0fae35c475420e3b  eba121c511f5bf0f  04ae6aa04a8f2242  b9d8b9d02b504c49
d3083cdd857f8dff  a0660007091d3835  3d5a890f16f84881  609bb80aedefd9e7
95a4b283a41749a3  231e69f6289bda2f  d4ee9b37af65fca6  a8c29430815e530f
```

```
030a80f8c062a4c5  d3f4fb3f8645089b  1c89562ee4cef02c  b00079552629ede4
250224e5dc4de95e  f98bb2daab97500e  e20bb4d65f3941ec  b293480d9d350f7d
af30c399abde695d  dd52b0a600d88bfe  0aa4b6756e5bcaca  f00d2cd9661475a7
48d5a75a22a94647  2065f73b588aa371  9f5d41516323ce90  9750a96070bd7e5c
46a3dd00cab74127  b1e22f14163a7bf9  fbe067f968e04ba5  eb29bfdecb741617
6d56ff045efa1156  2f68c8d2465a3713  7000b473acbc1f61  e4db420e15a912a8
2064f89c7cf14230  21f587a83076f308  0a79bde57e7dbcbe  8fb926af388ec37b
9fc1a8039ca9059f  20dfc7a39da417a4  ddffd1e271acc3cc  5844b6c6638b5f6b
987554732ba5914e  e096a9a2c7bafcb3  4e9198451ab18c68  ee2bf4f6cd52d4de
01c2723c15a68eb4  02b78266293d2acd  cbc3a334b664bb31  b9502be957f629e8
48c0d8e24d300520  f3da2bb77d6d6aa7  27ce5057ee960704  16855d8544ed0920
5ab6542930f298d5  20773ba8108b0bb9  6d9b1b28f924a512  679a93cd99ac0b53
8fb6631a7a746141  24528b1e6c83d4bf  8092c624ad060011  a4d4f78a44d63688
9961746e4e6df725  ca9841089c434425  77b7e5bb16ee0247  801e64f5aaa8d223
cdb2d2e4115bbe63  809b7192365cb959  631214424e4b17b4  e0f29c62bd434270
26cd29e42dd8769f  a316cec16b203b42  e114f3bfcfdb4a54  e253afb48175ab54
620e8761e062ec08  c958d82a797a8376  a5dff683356e6d58  a54938f47ed468db
851869ecec264efa  ee1947b9bfdc8fa3  a30b655021d85129  bea621c63954a6a2
e3c39f88918bd91f  795480da4977a786  565732f7740cc599  02074bf85e23c90c
93f4a5e8a988c577  ecf96b0b4f44dff8  6743ab73ae8a6244  99589a3eee412f28
3de3f591acbf711a  2430a162e26da407  120e20461bc02b18  ee68628098f3d0c6
96f56026c29a1933  582077a07f366a57  c0fa4df7e2e155e4  f764637d648dd69d
7bce96b154716ff2  14e50c325a75b20e  b3e3ccea27fc2bb4  62398716fe216db2
914400c983b0ded6  25b64dcbc5a59b0e  892c23ccd1f6abc9  e4aa0695e5d0f19a
db08a251b26202c7  1c3a87aa8ac0aedf  5c89989ad328f895  fbcf197bd67ac7f7
055eb9eb5d98c2bb  1cc157feb68c7392  be699d9937c895a1  8a3735dd371ef4dd
bf2a8c61963b25e1  01b243b3822b0c35  aab5594ef84b9f11  27b2fffda1162f55
927fd5c81f8d4b3a  a59236778c96f010  9db512b38d87b9e1  bdfc58029176a646
de553174742bbdef  472566745acc388e  7217945d2b6c62a6  b831eaae4e1962b9
fe18d9338bf23fcd  6c3f3f0c636a4102  2d00f5e4f3951f80  569635be19e92480
874d96023de4d4cb  35b62ae41f00ead1  86d4f2c5240c25d8  36832ee99ea5d8c6
70930e6247674a64  f0223b4f395d606f  4285dd47666bd8c3  8cee6f79618fff81
```

Đầu ra của DRBG trong G: NIST_CTR_DRBG(s_2) =0x

4 Ký hiệu và chữ viết tắt

$a \in A$	a là phần tử của A
$A \subset B$	A là tập con của B
$\|A\|$	Số phần tử của A
$A \times B$	Tích trực tiếp của A và B
A^m	Tập hợp các bộ m phần tử của A
${}_iC_j = \binom{i}{j} = \frac{i!}{j!\,(i-j)!}$	Hệ số nhị thức, cụ thể là i chọn j với i, j là số nguyên không âm thỏa mãn $j \leq i$
$[a]_i$	Phần thông điệp chia sẻ thứ i của thông điệp bí mật a
n	Số lượng phần thông điệp chia sẻ
k	Ngưỡng của phần thông điệp chia sẻ
G	Nhóm cyclic hữu hạn
K	Trường hữu hạn
$K[x]$	Tập hợp tất cả các đa thức tính theo x với hệ số tính bằng K
$Split$	Thuật toán phân chia thông điệp của một lược đồ IDA
Rec	Thuật toán tái tạo thông điệp của một lược đồ IDA
$Share$	Thuật toán chia sẻ thông điệp của một lược đồ chia sẻ bí mật
$Reconst$	Thuật toán tái tạo thông điệp của một lược đồ chia sẻ bí mật
$HomShare$	Thuật toán chia sẻ thông điệp của một lược đồ chia sẻ bí mật đồng cấu
$HomReconst$	Thuật toán tái tạo thông điệp của một lược đồ chia sẻ bí mật đồng cấu

5 Lược đồ chia sẻ bí mật

5.1 Tổng quan

Trong tiêu chuẩn này, mỗi phần 5.2, 5.3, 5.4, 5.5 và 5.6 bao gồm đặc tả kỹ thuật của một hoặc nhiều lược đồ chia sẻ bí mật. Đối với mỗi lược đồ chia sẻ bí mật, các mục sau đây được liệt kê:

a) Tham số
   1) Không gian thông điệp, tức là tập hợp các thông điệp khả dĩ mà có thể làm đầu vào của thuật toán chia sẻ thông điệp.

2) Không gian phần thông điệp chia sẻ, tức là tập hợp các phần thông điệp chia sẻ khả dĩ mà có thể được xuất ra bởi thuật toán chia sẻ thông điệp.
3) Số lượng phần thông điệp chia sẻ, tức là phạm vi các giá trị có thể có của n được lược đồ hỗ trợ.
4) Một trong những thuộc tính sau đây thể hiện phần thông điệp chia sẻ nào được yêu cầu để tái tạo:
   i. Ngưỡng, tức là một số dương k sao cho bất kỳ k phần thông điệp chia sẻ nào cũng đủ để thực hiện thành công thuật toán tái tạo thông điệp.
   ii. Cấu trúc truy cập, tức là tập hợp tối thiểu các tập hợp con khả dĩ của các phần thông điệp chia sẻ cần thiết để làm đầu vào cho thuật toán tái tạo thông điệp sao cho thuật toán có thể xuất ra thông điệp một cách thành công.
   iii. Cấu trúc đối nghịch, tức là tập hợp các tập hợp con của các phần thông điệp chia sẻ mà không thể tái tạo lại thông điệp.
5) Các tham số khác (nếu có).

b) Mô tả thuật toán chia sẻ thông điệp, tức là phương pháp phân chia thành các phần thông điệp chia sẻ.
c) Mô tả thuật toán tái tạo thông điệp, tức là phương pháp tái tạo thông điệp từ một tập hợp các phần thông điệp chia sẻ
d) Thuộc tính của lược đồ chia sẻ bí mật.

CHÚ THÍCH 1: Không có lược đồ chia sẻ bí mật nào được đặc tả trong tiêu chuẩn này có thuộc tính xác thực.

CHÚ THÍCH 2: Trong các cơ chế được đặc tả trong tiêu chuẩn này, các phần tử được chọn ngẫu nhiên từ một số tập hợp (hữu hạn). Tất cả các lựa chọn này được thực hiện đồng nhất (hoặc gần như đồng nhất) một cách ngẫu nhiên từ tập hợp các giá trị khả dĩ.

CHÚ THÍCH 3: Nếu không gian thông điệp là một nhóm hoặc trường, thì các phép toán số học được thực hiện trong nhóm hoặc trường này.

5.2 Lược đồ chia sẻ bí mật Shamir

5.2.1 Tổng quan

Các tham số, thuật toán chia sẻ thông điệp, thuật toán tái tạo thông điệp và các thuộc tính của lược đồ chia sẻ bí mật Shamir [8] được mô tả trong 5.2.

5.2.2 Tham số

Không gian thông điệp: K

Không gian phần thông điệp chia sẻ: giống như không gian thông điệp.

Số lượng các phần thông điệp chia sẻ: n, sao cho $n \geq 2, n < |K|$.

Ngưỡng: k, sao cho $n \geq k \geq 2$.

Các phần tử trường cố định: $x_i \in K$ với $1 \leq i \leq n$.

CHÚ THÍCH: Giả định rằng người nhận biết được các phần tử trường cố định. Các phần tử này có thể được gửi đến người nhận với phần thông điệp chia sẻ tương ứng hoặc được công bố dưới dạng tham số hệ thống.

Lược đồ Rabin (lược đồ Ramp với $L = k$) là lược đồ IDA được sử dụng để chia sẻ thông điệp đã được che giấu bằng phương pháp mặt nạ.

Thông điệp trong G: a= 0x

abcdef0123456789 abcdef0123456789 abcdef0123456789 abcdef0123456789

B.3 Lược đồ chia sẻ bí mật bổ sung cho một cấu trúc đối nghịch tổng quát.

Tham số:

Nhóm cyclic hữu hạn G là nhóm cộng tính của một trường hữu hạn cấp nguyên tố $p = 2^{61} - 1$.

$A = \{\{134\}, \{023\}, \{24\}\}$

Thông điệp: a= "abcdef"= 0x 00006162 63646566

Phần thông điệp chia sẻ:

$[a]_0 = \{r_{\{134\}} =$ 0x 044d9c51 20caed38$, r_{\{24\}} =$ 0x 0098c62d 99061f19$\}$

$[a]_1 = \{r_{\{023\}} =$ 0x 1b19fee3 a9935914$, r_{\{24\}} =$ 0x 0098c62d 99061f19$\}$

$[a]_2 = \{r_{\{134\}} =$ 0x 044d9c51 20caed38$\}$

$[a]_3 = \{r_{\{24\}} =$ 0x 0098c62d 99061f19$\}$

$[a]_4 = \{r_{\{023\}} =$ 0x 1b19fee3 a9935914$\}$

B.4 Lược đồ chia sẻ bí mật bổ sung

Tham số:

Nhóm cyclic hữu hạn G là nhóm cộng tính của một trường hữu hạn cấp nguyên tố $p = 2^{61} - 1$.

$(k, n) = (2,3)$

$A = \{Z | Z \subset \{1, \dots, n\}, |Z| = k - 1\} = \{\{1\}, \{2\}, \{3\}\}$

Thông điệp: a= "abcdef"= 0x 00006162 63646566

Phân thông điệp chia sẻ:

$[a]_1 = \{r_{\{2\}} =$ 0x 1a0779c3 11ad29a1$, r_{\{3\}} =$ 0x 16891be2 631205c6$\}$

$[a]_2 = \{r_{\{3\}} =$ 0x 16891be2 631205c6$, r_{\{1\}} =$ 0x 0f6fcbbc eea535fd$\}$

$[a]_3 = \{r_{\{1\}} =$ 0x 0f6fcbbc eea535fd$, r_{\{2\}} =$ 0x 1a0779c3 11ad29a1$\}$

B.5 Lược đồ chia sẻ bí mật bổ sung tính toán

Tham số:

K là trường hữu hạn của cấp $p = 2^{64}$ được mở rộng bằng cách sử dụng đa thức bất khả quy $x^{64} + x^4 + x^3 + x + 1$.

$G = K^{128}$(1k Byte), $X = K^4$ (32 Byte)

$(k, n) = (2,3), m = 2$.

DRBG được định nghĩa trong NIST 800-90A (http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf) cùng với mã hóa AES và không có hàm dẫn xuất và NIST_CTR _DRBG ký hiệu là DRBG.

Lược đồ chia sẻ bí mật Shamir với $(x_1, x_2, x_3) = (1, x, x + 1)$ được sử dụng để chia sẻ mầm.

5.2.3 Thuật toán chia sẻ thông điệp

Đầu vào: thông điệp $a \in K$

Đầu ra: Véc tơ chia sẻ $([a]_1, \dots, [a]_n) \in K^n$

a) Chọn một cách ngẫu nhiên $(r_1, \dots, r_{k-1}) \in K$
b) Tính toán $[a]_i = a + \sum_{j=1}^{k-1} r_j x_i^j \in K$ với $1 \leq i \leq n$
c) Xuất ra $([a]_1, \dots, [a]_n) \in K^n$

5.2.4 Thuật toán tái tạo thông điệp

Đầu vào: véc tơ chia sẻ $([a]_{i_1}, \dots, [a]_{i_k}) \in K^k$

Đầu ra: thông điệp $a \in K$

a) Tính toán $a = \sum_{j=1}^{k} [a]_{i_j} \prod_{u=1, u \neq j}^{k} (0 - x_{i_u})/(x_{i_j} - x_{i_u}) \in K$
b) Tính toán $a \in K$

CHÚ THÍCH: Thuật toán tái tạo còn được biết tới là đa thức nội suy Lagrange. Nếu $f(x) = a + \sum_{j=1}^{k-1} r_j x^j$ thì thông điệp bí mật là $f(0)$ và mỗi phần thông điệp chia sẻ $[a]_i$ là $f(x_i)$. Vì $f(x)$ là một đa thức bậc k, $f(0)$ có thể được tính từ tọa độ k sử dụng phép nội suy Lagrange.

5.2.5 Thuộc tính

Tính bí mật: Lược đồ chia sẻ bí mật Shamir hoàn toàn bảo mật lý thuyết thông tin khi người nhận chỉ có quyền truy cập đến ít hơn k phần thông điệp chia sẻ.

Tỷ lệ thông tin: lược đồ chia sẻ bí mật Shamir có tỷ lệ thông tin là 1, vì kích thước của thông điệp và phần thông điệp chia sẻ giống như kích thước của một phần tử của trường hữu hạn K. Do đó, lược đồ này là lý tưởng.

Phép toán đồng cấu: Lược đồ chia sẻ bí mật Shamir là đồng cấu $(+, +)$, trong đó phép cộng trên véc tơ chia sẻ được thực hiện bằng cách tính $[a + a']_i = [a]_i + [a']_i$.

Độ phức tạp: Thuật toán chia sẻ thông điệp cần $(k - 1)\, n$ phép nhân và $(k - 1)\, n$ phép cộng. Thuật toán tái tạo thông điệp cần k phép chia, $2k^2 - 3k$ phép nhân và $k^2 - 1$ phép cộng. Nếu bất cứ điều gì không liên quan đến a hoặc r_j với $1 \leq j \leq k - 1$ đã được chuẩn bị sơ bộ, cả hai thuật toán đều cần k phép nhân và $k - 1$ phép cộng.

5.3 Lược đồ chia sẻ bí mật Ramp Shamir

5.3.1 Tổng quan

Các tham số, thuật toán chia sẻ thông điệp, thuật toán tái tạo thông điệp và các thuộc tính của phiên bản ramp của lược đồ chia sẻ bí mật Shamir [3] được mô tả trong 5.3. Cơ chế này là sự tổng quát hóa của một lược đồ được đặc tả trong 5.2. Lược đồ chia sẻ bí mật Ramp Shamir giảm kích thước của mỗi phần thông điệp chia sẻ liên quan đến thông điệp được tái tạo bởi một thừa số của L. Mặc dù k phần thông điệp chia sẻ vẫn cần để có thể tái tạo thông điệp, nhưng bất kỳ số lượng phần thông điệp chia sẻ nào lớn hơn $(k - L)$ đều tiết lộ một phần thông tin về thông điệp. Các tham số k và L có thể được chọn linh hoạt trong giới hạn $k \geq L \geq 1$.

CHÚ THÍCH 1: Lược đồ chia sẻ bí mật Shamir với tham số $L = 1$ tương đương với lược đồ chia sẻ bí mật Shamir được đặc tả trong 5.2.

CHÚ THÍCH 2: Trong các lược đồ chia sẻ bí mật an toàn theo lý thuyết thông tin, mỗi phần thông điệp chia sẻ của một thông điệp bí mật có kích thước ít nhất bằng kích thước của thông điệp. Có hai phương pháp để giảm thiểu điều này. Một là dựa vào các giả định độ khó tính toán thay vì an toàn theo lý thuyết thông tin. Hai là sử dụng các lược đồ chia sẻ bí mật ramp. Trong lược đồ ramp, kích thước của phần thông điệp chia sẻ có thể ngắn hơn kích thước của thông điệp bí mật, trong khi có những nhóm các phần thông điệp chia sẻ vốn dĩ không cho truy cập nhưng có thể làm rò rỉ thông tin về thông điệp bí mật.

5.3.2 Tham số

Không gian thông điệp: K^L.

Không gian phần thông điệp chia sẻ K.

Số lượng phần thông điệp chia sẻ: n, thỏa mãn $n \geq 2, n < |K|$.

Ngưỡng: k, thỏa mãn $n \geq k \geq 2$.

Số lượng thông điệp được nhúng: L, thỏa mãn $k \geq L \geq 1$.

Phần tử trường cố định: $x_i \in K$ với $1 \leq i \leq n$.

CHÚ THÍCH: Các phần tử trường cố định có thể được gửi đến người nhận với các phần thông điệp chia sẻ tương ứng hoặc được công khai dưới dạng tham số hệ thống.

5.3.3 Thuật toán chia sẻ thông điệp

Đầu vào: Thông điệp $(a_1, \ldots., a_L) \in K^L$.

Đầu ra: Véc tơ chia sẻ $([(a_1, \ldots., a_L)]_1, \ldots., [(a_1, \ldots., a_L)]_n) \in K^n$.

a) Chọn ngẫu nhiên $r_L, \ldots., r_{k-1} \in K$.
b) Tính toán $[(a_1, \ldots., a_L)]_i = \sum_{j=0}^{L-1} a_{j+1} x_i^j + \sum_{j=L}^{k-1} r_j x_i^j \in K$ với $1 \leq i \leq n$.
c) Xuất ra $([(a_1, \ldots., a_L)]_1, \ldots., [(a_1, \ldots., a_L)]_n) \in K^n$.

5.3.4 Thuật toán tái tạo thông điệp

Đầu vào: Véc tơ chia sẻ $\left([(a_1, \ldots., a_L)]_{i_1}, \ldots., [(a_1, \ldots., a_L)]_{i_k}\right) \in K^k$.

Đầu ra: Thông điệp $(a_1, \ldots., a_L) \in K^L$.

a) Xác định đa thức: $f(x) = \sum_{j=1}^{k} [(a_1, \ldots., a_L)]_{i_j} \prod_{u=1, u \neq j}^{k} (x - x_{i_u})/(x_{i_j} - x_{i_u}) \in K[x]$.
b) Tính toán $f(x) = \sum_{i=0}^{k-1} b_{i+1} x^i \in K[x]$ và đặt $a_i = b_i$ sao cho $1 \leq i \leq L$
c) Xuất ra $(a_1, \ldots., a_L) \in K^L$.

5.3.5 Thuộc tính

Tính bí mật: Phiên bản ramp của lược đồ chia sẻ bí mật Shamir là bí mật theo lý thuyết thông tin khi người nhận có quyền truy cập vào ít hơn $k - L + 1$ phần thông điệp chia sẻ. Khi người nhận có quyền truy cập đến nhiều hơn $k - L$ phần thông điệp chia sẻ nhưng ít hơn k, một phần thông tin sẽ bị tiết lộ. Việc suy giảm tính bảo mật này được định lượng như sau: nếu một thực thể biết $k - L + i$ phần thông

Phụ lục B
(Tham khảo)
Ví dụ số

B.1 Lược đồ chia sẻ bí mật Shamir

Tham số:

Trường giới hạn K là một trường hữu hạn của cấp nguyên tố $p = 2^{61} - 1$.

$(k, n) = (2,3)$

$(x_1, x_2, x_3) = (2,3,4)$

Thông điệp: a= “abcdef” =`0x 00006162 63646566`

Phần thông điệp chia sẻ:

$[a]_1$= `0x 099634bb be0a753d`

$[a]_2$=`0x 1e611e68 6b5d7d28`

$[a]_3$= `0x 132c0815 18b08514`

Hệ số ngẫu nhiên: r= `0x 14cae9ac ad5307eb`

B.2 Lược đồ chia sẻ bí mật Ramp Shamir

Tham số:

Trường giới hạn K là một trường hữu hạn của cấp nguyên tố $p = 2^{61} - 1$.

$(k, L, n) = (3,2,5)$

$(x_1, x_2, x_3, x_4, x_5) = (2,3,4,5,6)$

Thông điệp: a= “abcdef” =`0x 00006162 63646566`

a_1= “abc”= `0x 00616263`

a_2= “def”= `0x 00646566`

Phần thông điệp chia sẻ:

$[a]_1$= `0x 02d2614f 437c38a3`

$[a]_2$= `0x 06595af2 56c72c5a`

$[a]_3$= `0x 0b49853d 0b3b25cb`

$[a]_4$= `0x 11a2e02f 60d824f6`

$[a]_5$= `0x 19656bc9 579e29db`

Hệ số ngẫu nhiên: r_2 = `0x 00b49853 d09482dd`

```
id-ss-fm-ss-4-1 OID ::= { id-ss-fm-ss-4 share(1) }
id-ss-fm-ss-4-2 OID ::= { id-ss-fm-ss-4 reconst(2) }
-- Secret Sharing Mechanism 5 --
id-ss-fm-ss-5-1 OID ::= { id-ss-fm-ss-5 share(1) }
id-ss-fm-ss-5-2 OID ::= { id-ss-fm-ss-5 reconst(2) }
id-ss-fm-ss-5-3 OID ::= { id-ss-fm-ss-5 convert(3) }
END -- secret-sharing-fundamental-mechanisms --
```


điệp chia sẻ với i $(1 \leq i \leq L-1)$ thì thực thể đó biết được phần thông điệp bí mật có kích thước nằm trong một tập hợp kích thước $|\mathrm{K}|^{\mathrm{L-i}}$.

Tỷ lệ thông tin: Phiên bản ramp của lược đồ chia sẻ bí mật Shamir có tỷ lệ thông tin là kích thước thông điệp L bằng L lần kích thước của phần tử trường và kích thước của phần thông điệp chia sẻ bằng với kích thước một phân tử của trường.

Phép toán đồng cấu: Phiên bản ramp của lược đồ chia sẻ bí mật Shamir là $(+,+)$- đồng cấu, trong đó phép cộng trên véc tơ chia sẻ được thực hiện bằng cách tính $[(a_1 + a'_1, \ldots., a_L + a'_L)]_i = [(a_1, \ldots., a_L)]_i + [(a'_1, \ldots., a'_L)]_i$.

Độ phức tạp: Thuật toán chia sẻ thông điệp cần $(k-1)n$ phép nhân và $(k-1)n$ phép cộng. Thuật toán tái tạo thông điệp cần $k(k-1)(k+1)/3$ phép chia, $k(k-1)/2$ phép nhân và $k(k-1)(2k+5)/6$ phép cộng sử dụng phương pháp khử Gauss. Nếu bất cứ điều gì không liên quan đến a hoặc r_j trong $L \leq j \leq k-1$ đã được chuẩn bị sơ bộ, thì thuật toán chia sẻ thông điệp cần k phép nhân và $k-1$ phép cộng.

5.4 Lược đồ chia sẻ bí mật bổ sung cho một cấu trúc đối nghịch tổng quát

5.4.1 Tổng quan

Các tham số, thuật toán chia sẻ thông điệp, thuật toán tái tạo thông điệp và các thuộc tính của sơ đồ chia sẻ bí mật bổ sung cho cấu trúc đối nghịch tổng quát [5] được mô tả trong 5.4. Đặt A là cấu trúc đối nghịch chứa m tập hợp con của các số $\{1, 2, \ldots, n\}$ có kích thước khác nhau đại diện cho các nhóm đối nghịch. Các thuật toán được sắp xếp sao cho không có tập hợp đối nghịch nào trong A có thể kết hợp để khôi phục a. Các phần tử của A được gắn nhãn $Z_j, j = 1, 2, \ldots, m$. Trong thuật toán chia sẻ thông điệp, các giá trị r_{Z_1}, ..., $r_{Z_{m-1}}$ được tạo ngẫu nhiên một cách đồng nhất trong trường và $r_{Z_m} = a - (r_{Z_1} + \ldots + r_{Z_{m-1}})$. Sau đó phần thông điệp chia sẻ $[a]_i$ bao gồm tất cả các giá trị r có chỉ số không chứa giá trị i, trong đó $i = 1, 2, \ldots, n$.

CHÚ THÍCH 1: Cấu trúc đối nghịch biểu thị tập hợp tất cả các liên minh tối đa của những người tham gia mà không thể tái tạo thông điệp bí mật.

CHÚ THÍCH 2 : Một khái niệm bổ sung cho khái niệm cấu trúc đối nghịch của lược đồ chia sẻ bí mật là cấu trúc truy cập của lược đồ. Cấu trúc truy cập chứa tất cả các liên minh tối thiểu của những người tham gia của lược đồ, những người có thể cùng nhau tái tạo thông điệp bí mật.

5.4.2 Tham số

Không gian thông điệp:G

Không gian phần thông điệp chia sẻ: giống như không gian thông điệp.

Số lượng phần thông điệp chia sẻ: n, sao cho $n \geq 2$.

Cấu trúc đối nghịch: $A \subset \{S | S \subset \{1, \ldots, n\}\}$

Tập hợp con cố định: $Z_0 \in A$

CHÚ THÍCH: Chỉ số $Z \in A$ của r_Z có thể được gửi tới người nhận với phần thông điệp chia sẻ tương ứng hoặc được công khai dưới dạng tham số hệ thống.

5.4.3 Thuật toán chia sẻ thông điệp

Đầu vào: thông điệp $a \in G$.

Đầu ra: véc tơ chia sẻ $([a]_1, \ldots, [a]_n)$.

a) Chọn một cách ngẫu nhiên $r_Z \in G$ đối với tất cả $Z \in A - \{Z_0\}$ và tính toán $r_{Z_0} = a - \sum_{Z \in A - \{Z_0\}} r_Z \in G$.
b) Tính $[a]_i = \{r_z | i \notin Z \in A\}$ đối với $1 \leq i \leq n$.
c) Xuất ra $([a]_1, \ldots, [a]_n)$.

5.4.4 Thuật toán tái tạo thông điệp

Đầu vào: véc tơ chia sẻ $\{[a]_i | i \in K\}$, trong đó K thỏa mãn yêu cầu rằng với mọi $Z \in A$, tồn tại $i_Z \in K$ K sao cho $i_Z \notin Z$.

Đầu ra: thông điệp $a \in G$.

a) Trích xuất $r_Z \in G$ từ phần thông điệp chia sẻ $[a]_{i_Z}$ đối với tất cả $Z \in A$.
b) Tính toán $a = \sum_{Z \in A} r_Z \in G$.
c) Xuất ra $a \in G$.

5.4.5 Thuộc tính

Tính bí mật: Lược đồ chia sẻ bí mật bổ sung cho cấu trúc đối nghịch tổng quát hoàn toàn bí mật theo lý thuyết thông tin khi người nhận chỉ có quyền truy cập vào phần thông điệp chia sẻ $\{[a]_i | \, i \in Z\}$ đối với một số $Z \in A$.

Tỷ lệ thông tin: Tỷ lệ thông tin cho sơ đồ chia sẻ bí mật bổ sung cho cấu trúc đối nghịch tổng quát là $1/max_{\,1 \leq i \leq n} |\{r_Z \, | i \notin Z \in A\}|$, kích thước của thông điệp bằng với kích thước của phần tử trong G và kích thước của một phần thông điệp chia sẻ bằng $max_{\,1 \leq i \leq n} |\{r_Z \mid i \notin Z \in A\}|$ lần kích thước phần tử. Nếu $|A| = 1$, sơ đồ là lý tưởng.

Phép toán đồng cấu: Lược đồ chia sẻ bí mật bổ sung cho cấu trúc đối nghịch tổng quát là $(+,+)$- đồng cấu, trong đó phép cộng trên véc tơ chia sẻ được thực hiện bằng cách tính. $[a]_i + [a']_i = \{r_z + r'_z \mid i \notin Z \in A\}$.

Độ phức tạp: thuật toán chia sẻ thông điệp cần $|A| - 1$ phép cộng. thuật toán tái tạo thông điệp cần $|A| - 1$ phép cộng.

5.5 Lược đồ chia sẻ bí mật bổ sung được nhân rộng

5.5.1 Tổng quan

Các tham số, thuật toán chia sẻ thông điệp, thuật toán tái tạo thông điệp và các thuộc tính của lược đồ chia sẻ bí mật bổ sung được nhân rộng [4] được mô tả trong 5.5. Trong lược đồ này, mỗi phần thông điệp chia sẻ lớn hơn nhiều so với thông điệp được chia sẻ. Tuy nhiên, việc tái tạo là không thể tính toán được, tùy thuộc vào nhóm và số lượng phần thông điệp chia sẻ được sử dụng làm tham số. Lược đồ này là trường hợp đặc biệt của lược đồ chia sẻ bí mật được mô tả trong 5.4 với các cấu trúc đối nghịch cụ thể $A = \{Z | Z \subset \{1, \ldots, n\}, |Z| = k - 1\}$.

Phụ lục A
(Tham khảo)
Định danh đối tượng

Phụ lục này liệt kê các định danh đối tượng được gán cho các lược đồ chia sẻ bí mật được đặc tả trong tiêu chuẩn này.

```
secret-sharing-fundamental-mechanisms {
iso(1) standard(0) secret-sharing(19592) fundamental-mechanisms(2)
asn1-module(0) object-identifiers(0) }
DEFINITIONS EXPLICIT TAGS ::= BEGIN
-- EXPORTS All; --
-- IMPORTS None; --
OID ::= OBJECT IDENTIFIER -- Alias
-- Synonyms --
id-ss-fm OID ::= {
iso(1) standard(0) secret-sharing(19592) fundamental-mechanisms(2) }
-- Assignments --
id-ss-fm-ss-1 OID ::= { id-ss-fm shamir-ss(1) }
id-ss-fm-ss-2 OID ::= { id-ss-fm ramp-ss(2) }
id-ss-fm-ss-3 OID ::= { id-ss-fm additive-general-ss(3) }
id-ss-fm-ss-4 OID ::= { id-ss-fm additive-threshold-ss(4) }
id-ss-fm-ss-5 OID ::= { id-ss-fm computational-additive-ss(5) }
-- Secret Sharing Mechanism 1 --
id-ss-fm-ss-1-1 OID ::= { id-ss-fm-ss-1 share(1) }
id-ss-fm-ss-1-2 OID ::= { id-ss-fm-ss-1 reconst(2) }
-- Secret Sharing Mechanism 2 --
id-ss-fm-ss-2-1 OID ::= { id-ss-fm-ss-2 share(1) }
id-ss-fm-ss-2-2 OID ::= { id-ss-fm-ss-2 reconst(2) }
-- Secret Sharing Mechanism 3 --
id-ss-fm-ss-3-1 OID ::= { id-ss-fm-ss-3 share(1) }
id-ss-fm-ss-3-2 OID ::= { id-ss-fm-ss-3 reconst(2) }
-- Secret Sharing Mechanism 4 --
```

CHÚ THÍCH: Khái niệm của (+, +)-đồng cấu được giới thiệu trong ISO/IEC 19592-1:2016, 5.2.2.

Các bên tham gia giao thức chuyển đổi: Bên P_i thứ i có phần chia sẻ thứ i là $[a]_i^{(Comp)}$.

5.6.6.3 Giao thức chuyển đổi

Đầu vào: Các phần thông điệp chia sẻ của lược đồ chia sẻ bí mật bổ sung tính toán $[a]_{i_u}^{(Comp)}$ của P_{i_u} với $1 \le u \le m$.

Đầu ra: Các phần thông điệp chia sẻ của lược đồ chia sẻ bí mật đồng cấu $[a]_i^{(Hom)}$ của P_i với $1 \le i \le n$.

a) Mỗi P_{i_u} với $1 \le u \le m$ tách $[a]_{i_u}^{(Comp)}$ thành $([s_1]_{i_u}, \dots, [s_m]_{i_u}, {t'}_{i_u})$.
b) Mỗi P_{i_u} với $1 \le u \le m$ gửi $[s_j]_{i_u}$ đến P_{i_j} với $1 \le j \le m$
c) Mỗi P_{i_u} với $1 \le u \le m$ tính $s_u = Reconst([s_u]_{i_1}, \dots, [s_u]_{i_k})$ và $r_u = DRBG(s_u)$
d) Mỗi P_{i_u} với $1 \le u \le k$ gửi ${t'}_{i_u}$ tới P_{i_1}
e) P_{i_1} tính $t = Rec({t'}_{i_1}, \dots, {t'}_{i_k})$
f) P_{i_1} tính $\left([t]_1^{(Hom)}, \dots, [t]_n^{(Hom)}\right) = HomShare(t)$ và gửi $[t]_i^{(Hom)}$ tới P_i với $1 \le i \le n$.
g) Mỗi P_{i_u} với $1 \le u \le m$ tính $\left([r_u]_1^{(Hom)}, \dots, [r_u]_n^{(Hom)}\right) = HomeShare(r_u)$ và gửi $[r_u]_j^{(Hom)}$ tới P_j với $1 \le j \le n$.
h) Mỗi P_i với $1 \le i \le m$ xuất ra $[a]_i^{(Hom)} = [t]_i^{(Hom)} + \sum_{j=1}^{m} [r_j]_i^{(Hom)}$.

5.6.6.4 Thuộc tính sau khi thực thi giao thức chuyển đổi

Tính bí mật: Việc chuyển đổi đồng cấu của lược đồ chia sẻ bí mật tính toán là bí mật về mặt tính toán khi người nhận có quyền truy cập ít hơn k phần thông điệp chia sẻ và các giao dịch của giao thức chuyển đổi.

Phép toán đồng cấu: Chuyển đổi đồng cấu của lược đồ chia sẻ bí mật tính toán là $(+, +)$ - đồng cấu, trong đó phép cộng trên các véc tơ chia sẻ được thực hiện bởi phép tính: $[a + a']_i^{(Hom)} = [a]_i^{(Hom)} + [a']_i^{(Hom)}$.

Mỗi bên có số ngẫu nhiên tương ứng với các nhóm đối nghịch mà không bao gồm chính bên này. Do đó, các bên mà tạo thành tập hợp con của một tập hợp kích thước $k-1$ không thể tái tạo thông điệp bí mật vì chúng không có số ngẫu nhiên tương ứng với tập hợp đó. Mặt khác, các bên không phải là tập hợp con của bất kỳ tập hợp có kích thước $k-1$ nào có thể tái tạo thông điệp bí mật vì với bất kỳ tập hợp kích thước $k-1$ nào cũng tồn tại một bên không có trong tập hợp đó và bên đó có số ngẫu nhiên tương ứng với tập hợp kích thước $k-1$.

5.5.2 Tham số

Không gian thông điệp: G

Không gian phần thông điệp chia sẻ: giống với không gian thông điệp.

Số lượng phần thông điệp chia sẻ: n, sao cho $n \ge 2$.

Ngưỡng: k, sao cho $n \ge k \ge 2$

Cấu trúc đối nghịch: $A = \{Z | Z \subset \{1, \dots, n\}, |Z| = k-1\}$.

Tập hợp con cố định: $Z_0 \in A$

CHÚ THÍCH: Chỉ số $Z \in A$ của r_Z có thể được gửi tới người nhận với phần thông điệp chia sẻ tương ứng hoặc được công khai dưới dạng tham số hệ thống.

5.5.3 Thuật toán chia sẻ thông điệp

Giống với thuật toán chia sẻ thông điệp trong phần 5.4.3.

5.5.4 Thuật toán tái tạo thông điệp

Giống với thuật toán tái tạo thông điệp trong phần 5.4.4.

5.5.5 Thuộc tính

Tính bí mật: Lược đồ chia sẻ bí mật bổ sung được nhân rộng hoàn toàn bí mật theo lý thuyết thông tin khi người nhận chỉ có quyền truy cập vào ít hơn k phần thông điệp chia sẻ.

Tỷ lệ thông tin: Tỷ lệ thông tin cho lược đồ chia sẻ bí mật bổ sung được nhân rộng là $1/\ {}_{n-1}C_{k-1}$, kích thước của thông điệp bằng với kích thước của phần tử trong G và kích thước của một phần thông điệp chia sẻ bằng ${}_{n-1}C_{k-1}$ lần kích thước phần tử.

Phép toán đồng cấu: Lược đồ chia sẻ bí mật bổ sung được nhân rộng là $(+, +)$- đồng cấu, trong đó phép cộng trên véc tơ chia sẻ được thực hiện bằng cách tính. $[a]_i + [a']_i = \{r_Z + r'_Z \mid i \notin Z \in A\}$.

Độ phức tạp: Thuật toán chia sẻ thông điệp cần ${}_nC_{k-1} - 1$ phép cộng. thuật toán tái tạo thông điệp cần ${}_nC_{k-1} - 1$phép cộng.

5.6 Lược đồ chia sẻ bí mật bổ sung tính toán

5.6.1 Tổng quan

Điều 5.6 mô tả các tham số, thuật toán chia sẻ thông điệp, thuật toán tái tạo thông điệp, giao thức chuyển đổi và các thuộc tính của lược đồ chia sẻ bí mật bổ sung tính toán [6] [7]. Lược đồ chia sẻ bí mật bổ sung tính toán đạt được tỷ lệ thông tin lớn thông qua việc cung cấp bảo mật tính toán và loại bỏ các phép toán

đồng cấu. Các phép toán đồng cấu có thể được thực hiện trên các véc tơ chia sẻ nếu chúng được chuyển đổi thành lược đồ chia sẻ bí mật đồng cấu trước. Lược đồ này cung cấp một giao thức chuyển đổi như vậy.

5.6.2 Tham số

Số lượng thông điệp chia sẻ: n sao cho $n \geq 2$.

Ngưỡng: k, sao cho $n \geq k \geq 2$.

Lược đồ chia sẻ bí mật: một thuật toán chia sẻ thông điệp $Share: X \to S^n$, thuật toán tái tạo thông điệp $Reconst: S^k \to X$ có không gian X của thông điệp, không gian S của phần thông điệp chia sẻ, số lượng phần thông điệp chia sẻ n và ngưỡng k.

Không gian thông điệp: G

Không gian mầm: nhóm X

Số lượng mầm: $m \geq 1$

Bộ sinh bit ngẫu nhiên tất định: $DRBG: X \to G$ có đầu vào là một mầm và đầu ra là một phần tử giả ngẫu nhiên trong G.

CHÚ THÍCH 1 Cả đầu vào và đầu ra của DRBG thông thường đều là các chuỗi bit, nhưng DRBG với đầu ra phần tử nhóm có thể được xây dựng theo hướng dẫn trong ISO/IEC 18031: 2011, B.1.

Thuật toán phân mảnh thông tin: IDA bao gồm $Split: G \to N^n$ và $Rec: N^k \to G$ có không gian G của thông điệp, không gian N của đầu ra, số lượng đầu ra n và ngưỡng k.

CHÚ THÍCH 2 Lược đồ này sử dụng IDA để đạt được kích thước đầu ra tối ưu, nghĩa là kích thước đầu ra là $1/k$ của kích thước thông điệp [6] [7].

Không gian phần thông điệp chia sẻ: $S^m \times N$.

5.6.3 Thuật toán chia sẻ thông điệp

Đầu vào: thông điệp $a \in G$.

Đầu ra: véc tơ chia sẻ $[a]_1, \dots, [a]_n$

a) Chọn một cách ngẫu nhiên $s_1, \dots, s_m \in X$.
b) Tính toán $r_i = DRBG(s_i)$ với $1 \leq i \leq m$.
c) Tính toán $t = a - \sum_{i=1}^{m} r_i \in G$.
d) Tính toán véc tơ chia sẻ $([s_i]_1, \dots, [s_i]_n) = Share(s_i)$ với $1 \leq i \leq m$.
e) Tính toán véc tơ $(t'_1, \dots, t'_n) = Split(t)$.
f) Đặt $[a]_i = ([s_1]_i, \dots, [s_m]_i, t'_i)$ với $1 \leq i \leq n$.
g) Xuất ra $[a]_1, \dots, [a]_n$.

5.6.4 Thuật toán tái tạo thông điệp

Đầu vào: Véc tơ chia sẻ $([a]_{i_1}, \dots, [a]_{i_k})$

Đầu ra: Thông điệp $a \in G$

a) Tính toán $s_j = Reconst([s_j]_{i_1}, \dots, [s_j]_{i_k})$ với $i \leq j \leq m$.
b) Tính toán $r_j = DRBG(s_j)$ với $1 \leq j \leq m$.
c) Tính toán $t = Rec(t'_{i_1}, \dots, t'_{i_k})$.
d) Tính toán $a = t + \sum_{i=1}^{m} r_i \in G$.
e) Xuất ra $a \in G$.

5.6.5 Thuộc tính

Tính bí mật: Lược đồ chia sẻ bí mật bổ sung tính toán là bí mật về mặt tính toán khi bên nhận có ít hơn k phần thông điệp chia sẻ có sẵn.

Tỷ lệ thông tin: Tỷ lệ thông tin đối với lược đồ chia sẻ bí mật bổ sung tính toán là gần như bằng k, nghĩa là tối ưu. Cụ thể hơn, kích thước của thông điệp là kích thước của một phần tử của G và kích thước của một phần thông điệp chia sẻ là $m|S| + |N|$. Nếu cả lược đồ chia sẻ bí mật và IDA đều đạt được kích thước đầu ra tối ưu và $|S|$ nhỏ hơn nhiều so với $|G|$ thì kích thước của một phần thông điệp chia sẻ gần bằng $1/k$ kích thước của một phần tử G.

Các phép toán đồng cấu: Lược đồ chia sẻ bí mật bổ sung tính toán không có các phép toán đồng cấu.

Độ phức tạp: Thuật toán chia sẻ thông điệp yêu cầu có m phép cộng, m phép toán $DRBG$, m phép toán chia sẻ và 1 phép toán phân mảnh. Thuật toán tái tạo thông điệp yêu cầu có m phép cộng, m phép toán $DRBG$, m phép toán tái tạo và 1 phép toán Rec.

5.6.6 Giao thức chuyển đổi

5.6.6.1 Tổng quan

Mặc dù lược đồ chia sẻ bí mật bổ sung tính toán không phải là đồng cấu, nhưng các phần thông điệp chia sẻ của lược đồ chia sẻ bí mật có thể được chuyển đổi thành các phần thông điệp chia sẻ của lược đồ chia sẻ bí mật đồng cấu. Giao thức chuyển đổi [6] được mô tả dưới đây.

5.6.6.2 Tham số

Lược đồ chia sẻ bí mật đồng cấu: Lược đồ chia sẻ bí mật đồng cấu bao gồm $HomShare: G \to S'^n$, $HomReconst: S'^k \to G$, trong đó không gian phần thông điệp chia sẻ là S', số lượng phần thông điệp chia sẻ là n, ngưỡng là k và phép toán đồng cấu.

Số lượng mầm của lược đồ chia sẻ bí mật bổ sung $m \geq k$

Phần thông điệp chia sẻ của lược đồ chia sẻ bí mật bổ sung tính toán: Phần thông điệp chia sẻ thứ i $[a]_i^{(Comp)}$ của lược đồ chia sẻ bí mật bổ sung tính toán.

Phần thông điệp chia sẻ của lược đồ chia sẻ bí mật đồng cấu: Phần thông điệp chía sẻ thứ i $[a]_i^{(Hom)}$ của lược đồ chia sẻ bí mật đồng cấu.

Phép toán đồng cấu của lược đồ chia sẻ bí mật đồng cấu: Lược đồ chia sẻ bí mật đồng cấu là $(+,+)$-đồng cấu, trong đó phép cộng trên các véc tơ chia sẻ được thực hiện bởi phép tính: $[a + a']_i^{(Hom)} = [a]_i^{(Hom)} + [a']_i^{(Hom)}$.