Annales UMCS Informatica AI XI, 2 (2011) 49–60
DOI: 10.2478/v10065-011-0011-x

Annales UMCS
Informatica
Lublin-Polonia
Sectio AI

http://www.annales.umcs.lublin.pl/

Methods of encrypting monotonic access structures

Jakub Derbisz*

Faculty of Mathematics, Computer Science and Mechanics, University of Warsaw, ul. Banacha 2, 02-097 Warsaw, Poland

Abstract

We will present some ideas about sharing a secret in a monotonic access structure. We show the relations which occur between the method of encrypting a monotonic access structure with the use of basis sets or maximal unprivileged sets, and that based on a logical formula (used by Benaloh and Leichter in [**1**]). We will also give some facts connected with the problem of security, including the aspects of a hierarchy security in the structure. The method of encrypting a monotonic access structure using a family of basis sets or a family of maximal sets that cannot reconstruct the secret will be described in a general way. Some aspects of using the latter based on a logical formula will be also given. Any (general) access structure can be encrypted by each of them but the way of sharing a secret is quite different and usually a specified method has to be chosen to achieve a desirable level of security and time complexity.

1. Introduction

The question of how to distribute a secret among a group of participants such that only certain subgroups, called privileged, could reconstruct it was answered in 1979 by Blakley [**2**] and Shamir [**3**]. The Shamir scheme with the threshold k frequently used allows to distribute a secret number s to n participants, such that any k or more entities can reconstruct it, but not fewer. This threshold scheme is denoted by (k,n). Typically it is realized by a polynomial f of the

*E-mail address: Jakub.Derbisz@mimuw.edu.pl

degree $k-1$, in which the free term represents the secret value s, and the shares of n participants are nodes of the form $(x, f(x))$. With k of these nodes we can reconstruct the polynomial (corresponding system of equations would have a unique solution), so in particular we can read a free term. As we can see, in the threshold systems we do not choose which groups of participants are privileged and we have only some freedom in choosing k, that is the minimal size of a group that can reconstruct the secret. Ito, Seito, Nishizeki in their work [**4**] from 1987 described a general method of distributing a secret such that only previously chosen, privileged subsets can reconstruct it. Then in [**1**] Benaloh and Leichter proposed a simpler and more efficient way of sharing a secret for a monotonic access structure. They have also given an example of a family of base sets which was of type $\{\{A, B\}, \{C, D\}\}$ that generates a monotonic access structure that cannot be realized by a generalized threshold scheme (in which each participant could receive several shares). This shows in particular, that if we want to have a freedom in choosing privileged sets for a monotonic access structure, we have to introduce some new ideas. One of the ideas, proposed in [**1**] which fulfills our requirements is based on a logical formula, the other one on a method using a family of maximal unprivileged sets, see also [**5**]. We will show some properties of the method in [**1**] and its relations to that based on the families of sets. We would also discuss efficiency and security issues.

2. Preliminaries

At the beginning we introduce some definitions and terminology.
Let $X = \{P_1, ..., P_n\}$ be a set of all entities and $P(X)$ a set of all subsets of X. A family Γ of subsets, that can reconstruct the secret is an *access structure*, and the elements of that family are called *privileged sets*. We say that an access structure is *monotonic* if every superset of a privileged set is also in the access structure. A *minimal element* of an access structure Γ is a set in Γ such that its every proper subset is not in Γ. We call a family of minimal sets a *basis of an access structure*, which we will denote by $\mathbf{B}$. On the other hand, every subset of $P(X)$, which is not in Γ can be extended to the maximal set not in Γ. That kind of subset is called *maximal* and adequate family a *family of maximal unprivileged sets*, denoted by $\mathbf{N}$.

Theorem 1. *One can determine a unique access structure by providing a family of basis sets* $\boldsymbol{B}$ *or by saying what family of maximal unprivileged sets* $\boldsymbol{N}$ *is.*

Proof. It is clear that a family of basis sets uniquely determines an access structure. We will show that having a family of maximal unprivileged sets $\mathbf{N}$

we can uniquely reconstruct the basis. Assume otherwise, let $\mathbf{B}_1$ and $\mathbf{B}_2$ be two different bases determined by $\mathbf{N}$. Without loss of generality we may assume that there exists $B \in \mathbf{B}_2$ such that $B \notin \mathbf{B}_1$. We have two possible cases:

1) B is a superset of certain $B' \in \mathbf{B}_1$, i.e. $B' \subseteq B$ (but we do not have equality), then B' is not in the access structure Γ_2 so we may extend B' to the maximal unprivileged set, but sets from $\mathbf{N}$ obviously do not include basis sets so that cannot be true.
2) B is not a superset of any $B' \in \mathbf{B}_1$, i.e. B is not in the access structure Γ_1. Similarly to that before, extension of B leads to the contradiction.

□

Instead of determining an access structure by giving a base one can also, as in [**1**], use a method with a logical formula consisting of a conjunction and disjunction but without negation (these are called *monotonic logical formulas*). Taking such a formula F on the variables indexed by a set P, the *access structure defined by* F is the family of these subsets A of a set P for which F is true precisely when the variables indexed by A have a logical value 1.

For example for a formula $(a_1 \vee a_2) \wedge a_3$ we have $P = \{1, 2, 3\}$ and the family of base sets of access structure defined by this formula is $\{\{1, 3\}, \{2, 3\}\}$.

3. Characterization of schemes

We will briefly show the way of distributing a secret proposed by Benaloh and Leichter [**1**] and the other method based on a family of basis sets or a family of maximal unprivileged sets, see also [**5**], then we will draw some attention to practical aspects of those methods.

A general method of sharing a secret described in [**1**] uses a monotonic logical formula. If s is a secret value that is going to be shared, we distribute it by going to more and more detailed parts of the formula (as we will see it in the example below) until we get to each participant. In particular, where we have disjunction, all of its components receive the same part of actually distributed part of a secret. Where we have conjunction, we divide randomly actually distributed part of a secret to a sum of s_i that sums up to this part and each of the components of the conjunction receives s_i. In this method of distributing a secret we may allow a threshold distribution, which means that when there is disjunction we use a threshold scheme with threshold 1 (which is equivalent to the method described earlier) and when there is conjunction of k components we use a threshold scheme with the threshold k. When using a threshold distribution for reconstruction, we have to remember identities of parts.

As for example, we will distribute in a ring modulo m a secret value $s \in \{0, 1, ..., m-1\}$ to entities $\{1, 2, 3\}$ with a structure defined by the formula $(a_1 \wedge a_3) \vee (a_2 \wedge a_3)$. First we look at the disjunction so s is distributed to $a_1 \wedge a_3$ and to $a_2 \wedge a_3$. Now looking at $a_1 \wedge a_3$ we randomly divide s into two parts s_1, s_2 such that $s_1 + s_2 = s$ and give s_1 to entity 1 and s_2 to entity 3. Similarly, getting s_3 and s_4 such that $s_3 + s_4 = s$ we distribute them to entities 2 and 3 respectively. It is also worth considering the formula $((a_1 \vee a_2) \wedge a_3) \vee (a_1 \wedge (a_2 \vee a_3) \wedge a_4)$ defining an access structure, where firstly s is distributed to both components of disjunction, then in the left component it is divided into appropriate s_1 and s_2 where s_1 is given to entities 1 and 2, s_2 to entity 3 (here instead of dividing s into two parts we could use the Shamir scheme with threshold 2). In the right component of the formula s is divided randomly into s_3, s_4 and s_5 which are distributed: s_3 to entity 1, s_4 to entities 2 and 3 and s_5 to entity 4 (here we could also use the Shamir scheme with threshold 3). We also notice that for a formula $(a_1 \vee a_2) \wedge (a_3 \vee a_4) \wedge \ \ldots \ \wedge (a_{2n-1} \vee a_{2n})$ each entity would get only one number.

Let us now describe the generalized method of creating a monotonic access structure from a family of basis sets or a family of maximal unprivileged sets, see also [**5**]. Let us consider a set of all entities $X = \{P_1, \ldots, P_n\}$ and an access structure Γ. Let us assume we have a family of k maximal unprivileged sets $\mathbf{N} = \{N_1, \ldots, N_k\}$. We can think of it as it is given and it determines the family of basis sets $\mathbf{B}$ or firstly we had a basis and it determined $\mathbf{N}$. We will distribute with the use of special function f subsets S_i of $S = \{a_1, \ldots, a_k\}$ to the participants. It means that entity P_i will receive the value $f(S_i)$. Function f is a function for which the following condition holds:

$$f\ (f(A) \cup f(B)) = f(A \cup B),$$

where A, B are certain sets. Notice that the examples of functions for which this condition holds are identity on the subsets of S or f being the least common multiple, when S is a set of pairwise coprime numbers least common multiple is understood here as a function that takes on the input a set and returns a singleton consisting of an element being the least common multiple. This kind of function 'forgets' the repeated terms of inputs and we can use it in sharing a secret by giving to participants for shares the values of f in certain sets. Value of f in the sum of all sets used for the construction of shares would be a secret that is going to be distributed among participants. Our function f is publicly known and safety issues are connected with choosing the function. Reconstructing the secret will be performed by taking values as in the left hand side of the equation that f satisfies. Notice that connecting $f(A \cup B)$ with a share $f(C)$ of a certain participant we compute $f\ (f(A \cup B) \cup f(C)) = f(A \cup B \cup C)$ as we wanted

for the process of reconstruction. Going back to distributing the shares to the participants, for each $N_i \in \mathbf{N}$, we connect a_i with every entity of X except those which are in N_i. So we have connected a subset $S_i \subseteq S$ with every participant P_i . After computing the value $f(S_i)$ that value is given to the participant P_i as his share. Notice that participants from a selected basis set can reconstruct the secret, because taking $B \in \mathbf{B}$ and selecting any value a_i, there would be participant B who received a_i (if not then $B \subseteq N$ for certain $N \in \mathbf{N}$ and it cannot happen). Because neither participants from the set $N_i \in \mathbf{N}$ has received a_i we may use it to set up safety conditions for our sharing scheme (depending on the chosen f). For example for f being the least common multiple we may require elements of S to be appropriately large pairwise coprime numbers, larger than a certain threshold (safety) value, [**5**].

4. Dependencies

The methods of determining an access structure from a family of base sets and determining it with a monotonic logical formula are related and any access structure can be defined using each of them.

Theorem 2. *Let F be any monotonic logical formula that defines an access structure Γ. Converting F to the disjunctive normal form (i.e. equivalent formula which is a disjunction of conjunction of the literals) and making reductions of a type $(a \vee b) \wedge a \Leftrightarrow a$ such that there are no clauses contained (as sets of literals) in other clauses, sets made of indices of clauses define a basis of Γ.*

As a remark, the formula $(a_1 \vee a_2) \wedge a_3$ is equivalent to $(a_1 \wedge a_3) \vee (a_2 \wedge a_3)$ and so we can read the basis.

Proof. Let **B'** be a family of sets that were formed from the reduced disjunctive normal form, as described in the theorem. We will show that **B'** = **B**, where **B** is the family of basis sets of Γ.

For any $B \in \mathbf{B}$ setting variables indexed by the elements of B to 1 gives a value of F equal to 1 no matter what the values of other variables are. In particular, setting all other variables to 0 we conclude that there exists $B' \in$ **B'** such that $B' \subseteq B$ and because the sets from **B'** are also in the access structure Γ we have $B' = B$, which shows that **B** $\subseteq$ **B'**

Now, let us take any $B' \in$ **B'**. As we know, it is in the access structure and we will show that it does not contain properly any basis set (which is enough). If it contained properly certain $B \in \mathbf{B}$ then, from what we have just shown, B' would have a proper subset from **B'**. That cannot be true since

B' was constructed from the reduced form. This shows that $B' \in \mathbf{B}$ and so **B'** $\subseteq \mathbf{B}$. □

There is a dual theorem for maximal, unprivileged sets.

Theorem 3. *Let F be any monotonic logical formula that defines an access structure Γ. Writing F in a conjunctive normal form (i.e. logical formula which is a conjunction of disjunction of the literals) which is reduced such that there are no clauses contained (as sets of literals) in other clauses (using $(a \wedge b) \vee a \Leftrightarrow a$), sets forming a family of maximal, unprivileged sets **N** are constructed by operation of choosing one clause of the formula and writing all indices except those that are indexing the chosen clause.*

Proof. Let **N'** be a family of sets constructed as stated in the theorem. Any set $N' \in$ **N'** is not in the access structure because setting variables indexed by elements which are not in N' to 0, i.e. all variables in a certain clause, we have the value of that clause equal to 0 so F is false. Let us call the clause selected for the construction of N' by C. We will show that N' is maximal. In each clause different from C we can find a variable indexed by an element of N', if not then there would exist a clause different from C which is contained (as a set) in the selected clause C and this cannot occur as the formula F is reduced. For that reason when we add any other element to N' it would be from a selected clause and setting appropriate variables to 1 the formula F would be true.

Let us take any maximal unprivileged set $N \in \mathbf{N}$. It is not in the access structure so the formula F is false when setting all variables indexed by N to 1 and others to 0. That means a certain clause has to have value 0 so there are not any variables indexed by N in that clause. Because of N being maximal all indices indexes apart from those indexing the mentioned clause are in N so N is in **N'**. □

We also observe that having a basis **B** it is easy to construct a logical formula that defines the same access structure, similarly to a family of maximal, unprivileged subsets. These results indicate, for example, that after encoding the access structure using one of the described methods it may be possible to encode it using the other one.

Sometimes it is much easier to construct a monotonic access structure using a logical formula. For example if we have a group of n pairs of entities of the form $(2i-1, 2i)$ for $i = 1, 2, \ldots, n$ and want to construct such a structure that for reconstruction of the distributed value s we need at least one entity from

each pair, then we can describe it shortly by a formula:

$$(a_1 \vee a_2) \wedge (a_3 \vee a_4) \wedge \quad \ldots \quad \wedge (a_{2n-1} \vee a_{2n})$$

The family of basis sets would consist of 2^n elements, in each there would be exactly one element of each pair. On the other hand, the family of maximal unprivileged sets would have n elements. Depending on a method of distributing a secret for a monotonic access structure the number of basis sets, maximal unprivileged sets or the number of parts from which the logical formula consists is important for the time complexity of the scheme.

Some aspects of hierarchical structure of the access structure including those connected with hiding places that entities take in the hierarchy may sometimes also be important. Looking from this perspective at the sharing schemes that were described, more suitable is the scheme which uses a family of maximal unprivileged sets and a function f being the least common multiple. For our set S of distributed values connected with entities we take a set of certain prime numbers or pairwise coprime numbers. An aspect of security in this case is based on the problem that it is hard to compute how many distinct prime divisors or distinct coprime parts (that come from the process of distributing the shares) does a composite number (here, the share) have. That is because each entity P_i, intuitively speaking, is the more important (higher in the hierarchy) the larger is its set S_i of distributed numbers connected to it (recall that the share of P_i is the least common multiple of elements of S_i, not the set S_i itself). When distributing the prime numbers we have the problem of telling how many distinct prime divisors a composite number have, which is considered to be comparatively difficult for the problem of factorization of a composite number which, as we know, is considered to be hard. Distributing coprime parts instead of prime numbers is in that case even better. For security reasons one has to guarantee the proper size of shares and that shares are not divisible by one another. It can be achieved by modifying the family of basis sets as presented below.

We will consider the case when there is no entity that is able to reconstruct the secret by himself (which is a natural assumption while sharing a secret).

Theorem 4. *Having a family of basis sets* $\boldsymbol{B}$ *such that no entity can reconstruct the secret by himself, it can be guaranteed that subsets* S_i *connected with the entities in a process of distributing the shares are not contained in one another.*

Proof. Let Γ be the access structure determined by the family of basis sets $\mathbf{B}$. Looking at the elements of sets from the family $\mathbf{B}$, if two entities P_j

and P_k are both the elements of a certain basis set, then their corresponding subsets S_j and S_k would not be contained in one another (in the family of maximal, unprivileged sets **N** there would be a set that contains entity P_j and does not contain the entity P_k, and the other set for which the opposite is true). On the other hand, if for entities P_j and P_k there is no basis set that these entities are the elements of, we add a new auxiliary entity P_l to the set of entities and create a new basis set from the entities P_j, P_k, P_l. The family of sets with the additional set is again a basis (the sets that previously were in **B** still do not contain proper subsets of the access structure because the only new sets in Γ are those that contain the new basis set). Due to this, all previous connections between entities have been preserved, and the additional entity is only auxiliary. We perform the described procedure for all such pairs of entities and create a new basis **B'**. After obtaining from **B'** the family of maximal unprivileged sets **N'** and distributing the shares as it was described, the condition from the theorem is fulfilled. □

4.1. Example

Let us consider a set of entities $\{P_1, P_2, P_3, P_4\}$ and the family of basis sets $\mathbf{B} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_2, P_3\}, \{P_1, P_4\}\}$. One may easily see that the family of maximal unprivileged sets $\mathbf{N} = \{\{P_1\}, \{P_2, P_4\}, \{P_3, P_4\}\}$.
The most privileged entity (highest in the hierarchy) is P_1 because he can reconstruct the secret cooperating with any other entity. The least privileged entity is P_4 because he can reconstruct the secret only with P_1. One may also see that after performing the steps described in the proof of the theorem above because the pairs of entities P_2 and P_4, similarly P_3 and P_4 are not the elements of any basis sets, we obtain
$\mathbf{B'} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_2, P_3\}, \{P_2, P_4, P_5\}, \{P_3, P_4, P_5\}\}$ and
$\mathbf{N'} = \{\{P_1, P_5\}, \{P_2, P_4\}, \{P_2, P_5\}, \{P_3, P_4\}, \{P_3, P_5\}, \{P_4, P_5\}\}$ where P_5 is the auxiliary entity.

While using logical formulas, the elements distributed (as shares) to a certain entity have a strictly specified meaning and so, in the process of reconstructing the secret value s we need to use the information about the access structure (for example which of the distributed elements one should use in the specified groups of entities to finally reconstruct s). This information may be used by a third party to gain knowledge about the access structure.

5. The ways of secret sharing in the monotonic access structures and possibilities of corruption

We will give and describe the ways the entity that constructs the monotonic access structure can share the information about it with the participants.

– The information about the possible groups of entities that can reconstruct the secret is publicly available for every entity in the structure.

– Every entity has the information only about the groups of participants with whom he can reconstruct the secret.

– The information about the possible privileged groups is given to a certain (trusted) external entity and the participants obtain incomplete information about privileged groups that they construct.

– The information about the privileged groups is given to a certain trusted external entity and every participant receives incomplete information about the privileged groups he is an element of.

First, the simplest method, in which information about the basis sets is publicly known is at the same time the least secure. Adversary, after corrupting any entity, gains the whole information about the hierarchical structure in the access structure. This information helps him choose the strategically best for him 'path of corruption', which after being performed, allows him to reconstruct the secret.

In the second method, entity has only partial information about the hierarchy in the structure and so strategies of an adversary after corrupting an entity are limited.

The third method uses an entity, who knows the whole family of basis sets. Entities even during the meetings would not be able to tell which privileged groups they are constructing (unless it is a meeting of such a group) because they do not know if the value they are reconstructing is the actual secret. The outer subject on the other hand, in some situations can disclose to entities information about the privileged groups. That is also helpful with protection against the corruption of entities, i.e. corrupted entities do not have the whole information about what other entities should be corrupted to reconstruct the secret.

In the fourth method each entity has even less knowledge about the family of basis sets. Planning the strategy of corrupting the entities of the structure is therefore even more difficult.

The third and fourth methods made use of an additional, external entity, after corruption of whom, we have the same situation as in the first method. His introduction, however, leads to new possibilities in using such a system, which may be interesting from the practical point of view. At some point though, the additional entity may adjudge that it is necessary to reveal to the certain group of entities the information that they can reconstruct the secret.

6. Security issues in sharing a secret

So far we have shown some safety aspects connected with monotonic access structures. We will now present the others, that are known in the literature, however, it is important here to realize the fact of what should be taken into consideration while constructing an access structure. In particular, we will see what assumptions could be made about possible attacks on the structure.

Generally, examining a sharing system one introduces some models that allow him to prove within them certain issues connected with security of a system [**6**], [**7**]. Here, we will present some of those models and possible attacks and types of an adversary related to them. One usually considers two basic models of exchanging information. First, called cryptographic [**7**], assumes that everyone has access to the information that is being exchanged between the participants of the scheme. Security of the scheme in such a model has to be guaranteed by a computationally hard problem, which adversary would not be able to solve in a reasonable time. Then there is the information-theoretic model [**8**], [**9**], which assumes that entities communicate with the use of pairwise secure channels. In this case safety is guaranteed even if an adversary has unlimited computing power. Let us now look at the sharing scheme from the aspect of possible corruption that could be performed by the adversary. The important concept here is the idea of adversary structure, which is a family of sets of entities, that may be corrupted by an adversary (for example it may consist of all subsets of cardinality less than a threshold value t). Passive corruption means that the adversary only acquires information about shares of corrupted participants, who (if they want) can perform reconstruction of the secret correctly. The corruption is called active, when the adversary takes full control of corrupted participants and the rest (not corrupted participants) cannot say which of the others were corrupted. We may also distinguish types of adversaries as being static or adaptive. Static adversary corrupts a set of participants only once and during the time the set does not change. Adaptive adversary can corrupt new participants at any time during the protocol, based on the information he gathers during the time, as long as the total set of corrupted participants is in the adversary structure.

The most appropriate model of computation is selected and depends on the type of practical purpose of sharing scheme as well as the issues connected with its implementation, safety and computational efficiency, and after setting a type of adversary, the features of the system are examined.

7. Conclusions

We have presented some ideas which could be also taken into consideration when constructing another than the presented methods of sharing a secret in the access structure. As we have shown, at the more general level, a method of constructing the access structure from a family of basis sets or a family of maximal unprivileged sets, and a method using a logical formula are similar. They both allow to construct any general access structures and after coding the structure using one of them there is a possibility to code it using the other one (at least theoretical, because sometimes coding using the other structure would be computationally too complex). Going into details about the schemes, we saw that in certain situations often connected with security or time complexity it is better to use the specified one. This depends on what we are expecting from our sharing system. Some other aspects of constructing a sharing scheme may sometimes be important as well. One can see that in the Shamir scheme it is easy to dynamically add a new entity because we give him an argument (his identity) and the value in this argument of the polynomial that we use in the scheme. Looking at the method with a logical formula or with families of sets we should verify and make new connections of the new entity and the existing ones (that is because it is a general access structure). Therefore, analyzing a sharing system that one wants to create, one has to prepare earlier estimates of a number of entities, dynamics in the system i.e. the number of possible addition and removal of entities and methods of implementation related to them operations. One should also set the matters connected with security which are going to be the most important for the scheme. We have presented how different levels of security are acquired depending on how the entity that is constructing the access structure reveals the information about it to the participants. As we point out, gathering information about hierarchical structure may help the adversary in setting the most suitable path of corruption for him, after performing of which he reconstructs the secret. Hiding information about a hierarchical structure can be performed by choosing an appropriate method of sharing a secret (for example a method with the families of basis sets) and a proper way of distributing the information about the structure by the constructor of the access structure. Realizing and setting models of information exchange (cryptographic/information-theoretical) and possible types of corruption (active/passive) and types of an adversary (adaptive/static), as well as setting the adversary structure for our system are crucial (although usually clear from the purpose we want to use our structure for).

References

[1] Benaloh J., Leichter J., Generalized secret sharing and monotone functions, "Advances in Cryptology - CRYPTO '88".
[2] Blakley, G. R., Safeguarding cryptographic keys, Proceedings of the National Computer Conference 48 (1979): 313.
[3] Shamir A., How to Share a Secret, Communications of the ACM 22(11): 612.
[4] Ito M., Saito A. and Nishizeki T., Secret Sharing Scheme Realizing General Access Structure, Proc. Glob. Com. (1987).
[5] Derbisz J., Pomykała J., Uogólnione rozdzielanie sekretu w systemach rozproszonych, submitted.
[6] Cramer R., Damgård I. and Maurer U., General Secure Multi-Party Computation from any Linear Secret-Sharing Scheme, B. Preneel (Ed.), Advances in Cryptology, EuroCrypt 2000, Lecture Notes in Computer Science 1807 (2000): 316.
[7] Goldreich O., Micali S. and Wigderson A., How to play any mental game or a completeness theorem for protocols with honest majority, Proc. ACM STOC '87, 218.
[8] Ben-Or M., Goldwasser S. and Wigderson A., Completeness theorems for non-cryptographic fault-tolerant distributed computation, Proc. ACM STOC '88, 1.
[9] Chaum D., Crépeau C. and Damgård I., Multi-party unconditionally secure protocols, Proc. ACM STOC '88, 11.