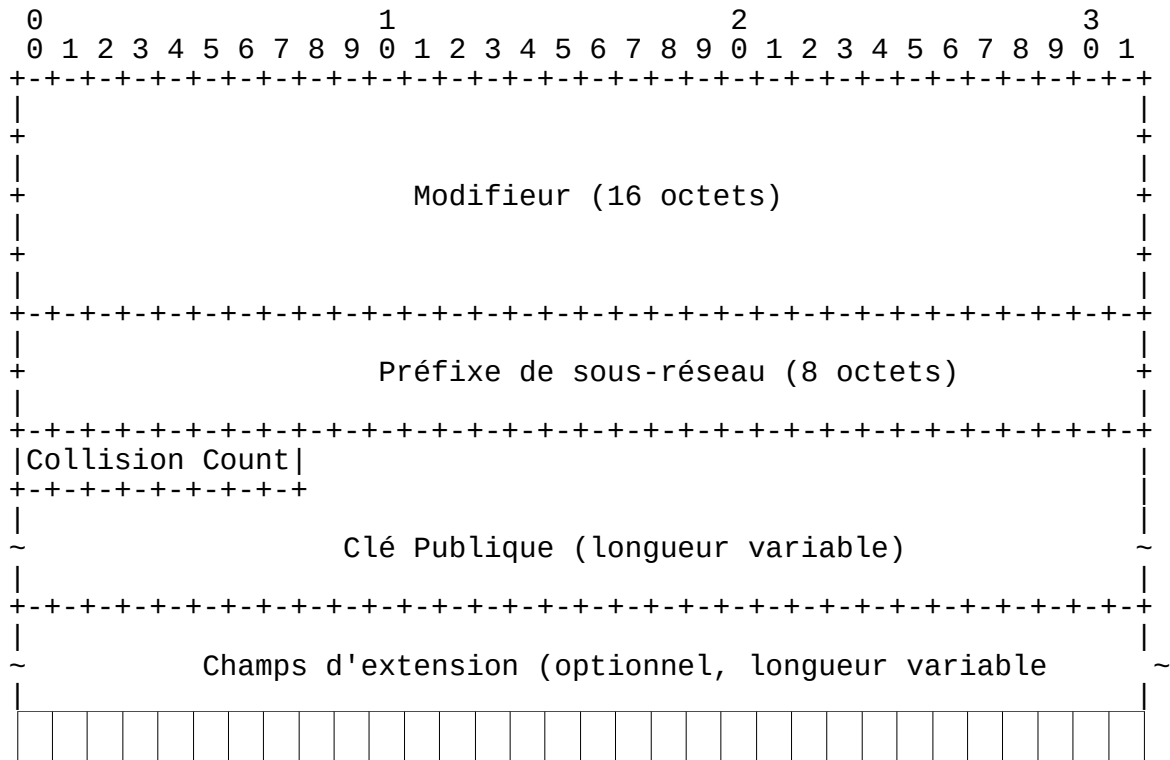


Paramètres liés à une adresse CGA (source : livre de Gisèle Cizeault)

Chaque adresse CGA est associée à des paramètres CGA, dont voici le format:



Modifieur : il s'agit d'un entier sur 128 bits, non signé, qui peut contenir n'importe quelle valeur. Le modifieur est utilisé lors de la génération et permet d'introduire de l'aléa dans la valeur de l'adresse.

Préfixe de sous réseau : préfixe de sous réseau de l'adresse CGA (64 bits)

Compteur de collision : entier non signé sur 8 bits dont les valeurs **DOIVENT** être 0, 1 ou 2.

Clé publique : c'est un champ de longueur variable qui contient la clé publique du propriétaire de l'adresse. Le format **DOIT** être la forme DER du champ ASN.1 SubjectPublicKeyInfo tel que présent dans les certificats X509 ([RFC 3280](#)). SEND devrait utiliser une paire de clé RSA, avec une longueur minimale de 384 bits.

Champs d'extension : ces champs ne sont pas encore utilisés dans la spécification, mais pourront l'être dans le futur.