de k bits, on a

$$\begin{aligned}\mathtt{Signature}(m) &= (y_{1m_1}, y_{2m_2}, \ldots, y_{km_k}) \\ &= (s_1, \ldots, s_k).\end{aligned}$$

1) Calculer pour $n = 256$ et $k = 256$ les tailles des clés publiques et privées. Comparer aux tailles de clés pour R.S.A. ou D.S.A.
2) Justifier que pour une seule signature, la sécurité du schéma repose sur la sécurité de la fonction de hachage f.
3) Peut-on prendre k petit pour le protocole, par exemple $k = 1$ ou 2 ?
4) Montrer qu'en prenant une attaque à messages choisis en deux signatures pour deux messages choisis, on peut récupérer toute la clé publique. Justifier la notion d'usage unique pour ce protocole.

8.8. *

On considère le protocole de Schnorr. Soient p et q deux entiers (grands) tels que q divise $p-1$, et soit g un entier d'ordre q modulo p. Le secret détenu par Alice est un entier $a \in [0, q-1]$ et la donnée de $A = g^{-a} \pmod p$ est rendue publique. Le protocole est alors le suivant :
- Alice fournit un engagement aléatoire k dans l'intervalle $[0, q-1]$ et calcule $K = g^k \pmod p$. Elle transmet K à Bob.
- Bob choisit un défi r au hasard dans $[0, q-1]$ et le transmet à Alice.
- Alice calcule la réponse $y = (k + ar) \pmod q$ et la transmet à Bob. Bob vérifie que $g^y A^r = K \pmod p$.

1) Faire un schéma de ce protocole. Vérifier que le protocole fonctionne.
2) Montrer que le protocole est cohérent et signifiant pour une probabilité $1/q$.
3) Quel est l'intérêt de ce protocole par rapport au protocole de Fiat-Shamir (en termes de nombre de passes).

8.9. ***

Il est possible de faire un algorithme de signature avec un protocole de type zero-knowledge avec une probabilité de triche donnée.
1) Montrer qu'en fixant par avance les engagements dans un protocole à divulgation nulle de connaissance et en les reliant par une fonction de hachage aux défis, on peut obtenir une signature pour une sécurité quelconque.
2) Dans le cas de Fiat-Shamir, avec $n = 1024$, quelle est la taille de la signature ?

8.10. ***

Pour des raisons de sécurité, il peut être intéressant que seule une coalition d'un nombre k de personnes parmi n soit capable de retrouver un secret. Par exemple, au moment de la création de la clé privée, on suppose qu'une autorité, avant de détruire la clé (et après l'avoir transmise à son propriétaire), donne certains éléments liés à la clé à 3 individus, de telle sorte qu'en cas de perte de clé privée, au minimum 2 individus parmi les 3 doivent collaborer pour retrouver cette clé privée, et cela afin de limiter les fuites possibles sur la clé tout en gardant un moyen de la retrouver.
Proposer une méthode pour partager un secret utilisant des polynômes de degré k et la notion d'interpolation de Lagrange pour distribuer des données à n personnes, de telle sorte qu'au moins k personnes parmi ces n doivent collaborer pour retrouver le secret et qu'une coalition de $k-1$ ne puisse rien retrouver.

8.11. *

1) On suppose qu'Alice partage une clé de chiffrement par blocs K_{AB} avec Bob et une clé K_{AC} avec Charlie. Donner une méthode pour qu'Alice chiffre un long message M de m blocs qui ne soit déchiffrable que par une coopération entre Bob et Charlie. On peut supposer que Bob et Charlie partagent un canal secret pour leur communication. Le chiffré devra être de taille fixe, à peine plus grand que m blocs et Alice ne devra chiffrer les m blocs du message qu'une seule fois.
2) On suppose maintenant qu'Alice partage une clé de chiffrement par blocs avec Bob (K_{AB}), Charlie (K_{AC}) et David (K_{AD}). Donner une méthode de chiffrement de telle sorte qu'Alice envoie un message de m blocs chiffrés par une seule clé, mais que pour déchiffrer le message, il y a besoin qu'au moins deux personnes parmi Bob, Charlie et David coopèrent pour déchiffer le message. Indice : il faut ajouter simplement trois blocs chiffrés bien choisis aux m blocs chiffrés.
3) Donner une idée de la méthode pour généraliser cette idée au cas de n personnes dont tout sous-groupe de k personnes puissent déchiffrer le message (on pourra utiliser l'exercice précédent).

8.12. **

Pour le chiffrement de McEliece, la taille de la clé publique est nk ; il pourrait être plus intéressant de mettre cette matrice sous forme systématique pour diminuer sa taille. Le problème est que l'on risque alors, en chiffrant (en multipliant par une telle matrice), de donner des informations sur le message.
Proposer une variation sur le système de chiffrement en utilisant une fonction de hachage sur l'erreur ajoutée, qui permet d'utiliser pour le chiffrement une matrice sous forme systématique.