L'Internet devient de plus en plus omniprésent dans notre vie quotidienne et intervient dans divers domaines, où l'échange et le traitement de l'information doivent être sécurisés. La cryptographie est la solution qui est la plus utilisée pour sécuriser l'information, en assurant les contraintes de sécurité, à savoir la confidentialité, l'intégrité, l'authentification et la non-répudiation. Deux types de cryptographie sont classiquement distingués. La cryptographie asymétrique offre une distribution de clés sécurisée ainsi que la signature numérique, mais elle nécessite plus de calculs que la cryptographie symétrique. Pour cette raison, l'utilisation de la cryptographie basée sur les courbes elliptique prend de plus en plus de l'ampleur. C'est une cryptographie asymétrique connue pour sa robustesse qui est basée sur la difficulté de résoudre le problème de logarithme discret, d'une part, et pour son utilisation de clés de taille nettement plus réduite que celles de RSA, en offrant le même niveau de sécurité, d'autre part.

Dans cette thèse, nous essayons de répondre aux contraintes de sécurité et de performance qu'impose le fonctionnement efficace des protocoles cryptographiques basés sur les courbes elliptiques, notamment à l'échange de clé Diffie-Hellman (DH), au crypto-système d'ElGamal et à l'algorithme de signature numérique. Nous proposons deux solutions pour répondre aux contraintes d'authentification. Dans la première, nous présentons une nouvelle approche d'échange de clé secrète DH. La deuxième concerne l'intégration de l'algorithme de signature numérique sur courbes elliptiques au protocole d'accord de clé DH. Nous analysons l'algorithme de signature numérique basé sur les courbes elliptiques ainsi que ses variantes, et nous proposons des améliorations y afférentes