Les systèmes de communication et d'information deviennent de plus en plus ubiquitaires en faisant partie intégrante de notre vie quotidienne et en intervenant dans divers domaines. Dans ce contexte de démocratisation, la vulnérabilité quant aux données traitées et échangées par ces systèmes, est par conséquent grandissante. Le fonctionnement efficace des systèmes de communication et d'information impose alors d'une part, des contraintes de sécurité en rapport avec la confidentialité, l'intégrité, l'authentification et la non-répudiation et d'autre part des contraintes de performance relatives à la puissance de calcul, le coût, la limite de ressources et la consommation d'énergie. Dans cette thèse, les travaux qui suivent tentent de répondre aux contraintes de sécurité et de performance imposées par les systèmes de communication et d'information, en proposant des solutions cryptographiques optimales basées sur les courbes elliptiques. Nous proposons à cet effet, deux nouvelles solutions. La première répond aux contraintes d'authentification, de haute flexibilité, de faible empreinte Silicium et de faible consommation de mémoire, imposées par les systèmes d'identification par radio fréquence. Alors que la seconde répond aux contraintes de confidentialité et de haute performance temporelle, nécessaires lors des échanges qui ont lieu sur Internet, notamment ceux que l'on effectue lors de transactions de commerce électronique