Les courbes elliptiques jouent maintenant un rôle primordial dans le domaine de la cryptographie à clé publique. En effet, compte tenu des tailles des clés actuelles pour les systèmes à clé secrète (128 bits, 192 bits et 256 bits) les systèmes basés sur RSA ou sur du logarithme discret dans Z/pZ ne peuvent plus suivre. Il faut de l'ordre de 4096 bits RSA pour avoir une sécurité équivalente à 128 bits de clé pour un système à clé secrète, de l'ordre de 15000 bits RSA pour une clé secrète de 192 bits. Ces tailles de clé sont trop grandes et on doit utiliser des courbes elliptiques pour lesquelles les tailles équivalentes sont de l'ordre de 256 bits, 384 bits et 512 bits. Il convient en fait de disposer de courbes elliptiques construites sur un corps premier Z/pZ avec p premier ayant de l'ordre de 256 bits, 384 bits, 512 bits et dont le nombre de points est aussi un nombre premier. Or le NIST ne fournit qu'une telle courbe de chaque taille. Nous avons donc construit une base de courbes elliptiques bonnes pour la cryptographie. Cette base, appelée ARCANA-ECDB peut être téléchargée et utilisée librement ici . Une note technique se trouve ici . Outre des courbes sous la forme courte de Weierstrass on trouve aussi une base de courbes d'Edwards et une base de courbes de Montgomery.