La NSA dans un article intitulé " NSA Suite B cryptography " définit ses recommandations concernant les primitives cryptographiques de base. Ceci inclut le chiffrement (qui rappelons le, pour un flux de données ne peut se faire qu'avec du chiffrement à clé secrète), la signature numérique, l'échange de clés, les fonctions de hachage. La caractéristique la plus visible est l'abandon de la cryptographie RSA au profit de la cryptographie elliptique sur un corps fini premier. Ainsi seules les courbes elliptiques sur Z/pZ sont conseillées, celles sur les corps finis ayant 2^n éléments ne sont pas citées (bien entendu le cas q=p^n avec p premier quelconque et n>1 n'était déjà plus envisagé depuis un certain temps).

Si on se reporte au niveau de sécurité conseillé pour le chiffrement à clé secrète on voit que:

1) AES avec 128 bits de clé est conseillé pour des applications de niveau de securité élevé

2) AES avec 192 bits de clé est conseillé pour une securité "top level secret". Mais s'il est bien spécifié que 192 bits sont suffisant pour cette sécurité très élevée, pour des raisons de compatibilité c'est en définitive AES 256 bits de clés qui sera utilisé.

De ce fait les autres circuits (courbes elliptiques, hachage) doivent suivre cette sécurité, c'est-à dire une courbe elliptique de 256 bits et SHA256 pour aller avec AES128, une courbe de 384 bits et SHA384 pour aller avec AES192 (remplacé en fait par AES256). A vrai dire, si on voulait bénéficier de la sécurité complète de AES256 il faudrait prendre une courbe elliptique de 512 bits et SHA512, mais ceci n'est pas le conseil de la NSA.

L'article " Les standards en cryptographie sont ils souhatables " de Arjen Lenstra à ce sujet est très intéressant et relativise un peu le rôle de la cryptographie dans le processus global de sécurité des systèmes.

Il me semble que la disparition de RSA était inéluctable. En effet déjà pour suivre la sécurité de AES128, ce qui est considéré comme un minimum, le module RSA devrait avoir peut être 4096 bits alors qu'une courbe elliptique aura un nombre de points qui s'écrit avec 256 bits. Et si on passe à l'echelon suivant, pour suivre la sécurité d'AES256 il faudrait plus de 15000 bits pour un module RSA, ce qui sort du raisonnable, alors qu'avec une courbe elliptique on travaillera

avec des nombres de 512 bits. Même si l'opération est un peu plus compliquée, compte tenu des tailles bien plus courtes des données traitées, le bilan devient largement en faveur des courbes elliptiques.