Conclusion

"Il ne faut cesser de s'enfoncer dans sa nuit : c'est alors que brusquement la lumière se fait."

F. Ponge

Des nouveaux schémas d'identification, dépendant de la difficulté de résolution du problème SD ont été proposés. L'un d'entre eux est, à ce jour, le plus performant des schémas SD. Plusieurs alternatives ont été suggérées afin d'améliorer ses paramètres. Pour cela, nous avons travaillé sur des sous-instances du problème général considéré.

Si de nouvelles cryptanalyses ne sont pas élaborées, pour ces instances particulières, alors ces schémas constituent une bonne alternative aux schémas classiques, dépendant d'un problème issue de la théorie des nombres.

Chacun d'entre eux possède ses avantages et ses inconvénients selon que l'on privilégie deux paramètres parmi les trois suivants : taille de la ROM, complexité de calcul, débit de transaction.

Tous les schémas basés sur le problème SD utilisent une fonction de hachage et un générateur de permutation aléatoire. Une amélioration consisterait à élaborer un nouveau schéma, n'utilisant pas ces deux objets. Ceci permettrait, entre autre, de mettre au point des systèmes interactifs de preuve, à divulgation nulle, ne dépendant pas du modèle de l'oracle aléatoire.

En ce qui concerne les codes de Goppa, de nombreuses questions sont encore sans réponse. Notamment, est-il possible de complètement caractériser les codes à poids pair ? Peut-on prouver que les bornes que nous avons proposées sont toujours atteintes lorsque $g(z) = \mathrm{Tr}_{\mathbb{F}_{p^{2s}}:\mathbb{F}_{p^s}}(z)$. Pour certains polynômes $a(z)$ et $b(z)$, est-il possible d'améliorer les bornes proposées ? En ce qui concerne la distance minimale, les bornes obtenues ne sont pas assez fines. Peut-on les améliorer ? Les résultats obtenus sur l'intersection de $\Gamma_{2,2}(1,z)$ et $\Gamma_{2,2}(1,z)^{\perp}$ doivent se généraliser à tout corps de caractéristique p quelconque. L'utilisation de certaines propriétés des codes de Reed et Muller doit permettre une nouvelle étude de ces deux codes.