

Olivier Blazy ★ **Designated Verifier Signature**

Résumé :

Les signatures permettent d'authentifier un message (mail) pour que le destinataire soit convaincu de sa provenance. Cependant dans certains cas, on veut pouvoir faire en sorte que le destinataire ne puisse pas convaincre quelqu'un d'autre que le message vient bien de nous.

Le sujet consiste à regarder les diverses solutions théoriques proposées, et essayer de les catégoriser pour dégager les grands mécanismes cryptographiques utilisés pour y arriver.