# Concilier sécurité et droit à la vie privée : le projet DECoD

Jérôme Lacan*†[1], Benoît Parrein*[2], Nicolas Normand*‡[2], and Vincent Roca*§[3]

[1]Institut Supérieur de l'Aéronautique et de l'Espace (ISAE) – Ministère de la Défense – ISAE - 10 av. Edouard Belin - BP 54032 - 31055 TOULOUSE Cedex 4, France

[2]Institut de Recherche en Communications et en Cybernétique de Nantes (IRCCyN) – CNRS : UMR6597, Université de Nantes, Ecole Centrale de Nantes, Ecole des Mines de Nantes, Ecole Polytechnique de l'Université de Nantes – 1, rue de la Noë BP92101 44321 Nantes Cedex 03, France

[3]PRIVATICS (Inria Grenoble Rhône-Alpes / CITI Insa de Lyon) – INRIA – Inovallée Montbonnot 655 avenue de l'Europe 38 334 Saint Ismier Cedex, France

**Résumé**

En 1981, Mac Eliece et Sarwate [1] généralisent le schéma de partage du secret de Shamir [2] par l'usage des codes de Reed-Solomon. Cette proposition est cryptographiquement sûre au sens de la théorie de l'information même si l'attaquant dispose de moyens de calcul infinis. Curieusement, encore aujourd'hui, les travaux de Mac Eliece et Sarwate demeurent une étude théorique. L'objet du projet DECoD est de proposer des réalisations pratiques de ce schéma par l'usage de codes linéaires variés (RS, LDPC ou Mojette) en fonction des contextes de communication de type multi-chemins ou de stockage des données en mode Cloud. Nous tenterons de démontrer comment la notion de partage de secret, de surcroît théoriquement sûre, permet de concilier les problématiques de sécurité intérieure et de droit à la vie privée. Ce projet fait suite au projet FEC4Cloud présenté l'an dernier à Troyes (RESSI 2015).

McEliece, R. J., & Sarwate, D. V. (1981). On sharing secrets and Reed-Solomon codes. Communications of the ACM, 24(9), 583-584.

Shamir, A. (1979). How to share a secret. Communications of the ACM, 22(11), 612-613.

**Mots-Clés:** codes correcteurs linéaires, partage du secret, schéma de Mac Eliece

*Intervenant

†Auteur correspondant: jerome.lacan@isae.fr

‡Auteur correspondant: nicolas.normand@polytech.univ-nantes.fr

§Auteur correspondant: vincent.roca@inria.fr