Codes Non-Malléables et Coset Coding *

Alain Patey
(Morpho, Télécom ParisTech, Identity and Security Alliance †) ‡

En 2010, Dziembowski, Pietrzak et Wichs [DPW10] ont introduit la notion de *Codes Non-Malléables*, en adaptant la définition cryptographique de non-malléabilité à la théorie des codes. On dit ainsi qu'un code est non-malléable vis-à-vis d'une famille de fonctions si le résultat du décodage d'un mot de code altéré par une des fonctions de cette famille est ou bien le mot initialement encodé ou bien un mot qui ne lui est pas du tout lié.

La motivation pour une telle notion est la protection contre les injections de faute. On peut en effet supposer que des données sont stockées encodées dans une mémoire qu'un attaquant ne peut pas lire mais dans laquelle il peut injecter des fautes. L'idée est alors que soit les erreurs induites seront corrigées, soit les données qui résulteront du décodage seront totalement décorrélées des données initiales et l'attaquant ne pourra donc pas profiter de ses attaques.

Le modèle des codes non-malléables peut être rapproché de deux modèles déjà connus : la deuxième version du Wire-Tap Channel [OW84] et le *Secure Network Coding* [CY02]. Dans ces deux modèles, on peut utiliser un type de codage particulier, le *linear coset coding*, pour remplir des propriétés de sécurité.

En partant de résultats connus dans ces deux modèles, nous proposons de faire un parallèle avec le modèle des codes non-malléables afin de démontrer la non-malléabilité du linear coset coding vis-à-vis de familles de fonctions d'intérêt, dans un premier temps les *bit-wise independent functions*, à partir du Wire-Tap Channel et, dans un deuxième temps, les fonctions linéaires, à partir du Secure Network Coding.

Ces résultats ont respectivement été publiés dans [CCFP11] et [CCP12].

Références

[CCFP11] H. Chabanne, G. Cohen, J. Flori, and A. Patey. Non-malleable codes from the wire-tap channel. In *Information Theory Workshop (ITW), 2011 IEEE*, pages 55 –59, oct. 2011.

[CCP12] H. Chabanne, G. Cohen, and A. Patey. Secure network coding and non-malleable codes : Protection against linear tampering. In *ISIT*, 2012.

[CY02] N. Cai and R.W. Yeung. Secure network coding. In *Information Theory, 2002. Proceedings. 2002 IEEE International Symposium on*, page 323, 2002.

[DPW10] S. Dziembowski, K. Pietrzak, and D. Wichs. Non-malleable codes. In A. Yao, editor, *ICS*, pages 434–452. Tsinghua University Press, 2010.

[OW84] L.. Ozarow and A. Wyner. Wire-tap channel II. In *EUROCRYPT*, pages 33–50, 1984.

*Ce travail a été partiellement financé par le projet ANR SPACES.

†The Morpho and Télécom ParisTech Research Center

‡Travaux effectués avec Hervé Chabanne (Morpho, Télécom ParisTech), Gérard Cohen et Jean-Pierre Flori (Télécom ParisTech).