# An Efficient Generic Insider Secure Signcryption with Non–Interactive Non–Repudiation

Augustin P. Sarr*[1] and Ngarenon Togde

[1]Département de Mathématiques Appliquées / Université Gast Berger de Saint-Louis – Sénégal

**Résumé**

We present a novel generic construction of an insider secure signcryption scheme with non-interactive non-repudiation. Our generic construction uses as building blocks a signature scheme, a key encapsulation mechanism (KEM), a keyed hash function, a symmetric encryption scheme, and a pseudo–random function. We show that our construction is insider secure in the dynamic multi–user model, without resorting the random oracle or the key registration model; it provides non–interactive non repudiation.

*Intervenant