k-times Anonymity for Proxy and Sanitizable Signature

Charles Olivier-Anclin*[1,2]

[1]Laboratoire d'Informatique, de Modélisation et d'Optimisation des Systèmes – Ecole Nationale Supérieure des Mines de St Etienne, Centre National de la Recherche Scientifique, Université Clermont Auvergne, Institut national polytechnique Clermont Auvergne, Ecole Nationale Supérieure des Mines de St Etienne : UMR6158, Centre National de la Recherche Scientifique : UMR6158, Université Clermont Auvergne : UMR6158, Institut national polytechnique Clermont Auvergne : UMR6158 – France

[2]be ys Pay – be ys Pay – France

Résumé

Fully traceable k-times anonymity is a security property concerning anonymous signatures: if a user produces more than k anonymous signatures, its identity is disclosed and all its previous signatures can be identified.
In this paper, we show how this property can be achieved for delegation-supported signature schemes, especially proxy signatures, where the signer allows a delegate to sign on its behalf, and sanitizable signatures, where a signer allows a delegate to modify certain parts of the signed messages. In both cases, we formalize the primitive, give a suitable security model, provide a scheme and then prove its security under the DDH assumption. The size of the keys/signatures is logarithmic in k in our two schemes, making them suitable for practical applications, even for large k.

Mots-Clés: Signature, Anonymat, Proxy, Traceable

*Intervenant