Accréditations Anonymes et Déléguables

Yaël Pajot*[1]

[1]Laboratoire de Mathématiques de Versailles – Université de Versailles Saint-Quentin-en-Yvelines, Université Paris-Saclay, Centre National de la Recherche Scientifique – France

Résumé

Un schéma d'Accréditations Anonymes et Déléguables (DAC, Delegatable Anonymous Credentials) est un schéma où une autorité peut attribuer des accréditations (valeurs permettant de s'authentifier) à des utilisateurs, qui peuvent ensuite les déléguer à d'autres utilisateurs.
Une application pratique peut être la suivante : un magasin de luxe peut attribuer un certificat d'authenticité d'un produit à un client, et lorsque le client souhaitera revendre son article, il pourra alors déléguer le certificat d'authenticité à son nouveau propriétaire.
Un utilisateur est caractérisé par sa clé publique.
Pour attribuer une accréditation, l'autorité signe la clef publique de l'utilisateur à l'aide sa clé privée. Le crédit est alors la concaténation de la signature et de la clef publique de l'utilisateur qui a recu le crédit.
Pour déléguer un crédit, un utilisateur signe avec sa clé privée la clef publique du receveur, et rajoute la signature et la clef publique du receveur au crédit.
Pour vérifier qu'un crédit est valide, on regarde itérativement si la signature de la clé publique actuelle est bien vérifiée par la clé publique précédente.
Pour prouver la possession d'un crédit, un utilisateur effectue une preuve à divulgation nulle de conaissance sur sa clef privée.
Ainsi, dans un DAC, tout le monde peut vérifier l'authenticité d'un crédit, et seul son propriétaire peut en prouver sa possession.
Malheureusement, pour garantir l'authentification, on n'arrive pas à se reposer sur des hypothèses cryptographiques standard.
Ainsi, afin de construire un schéma de DAC, on se place dans le Modèle du Groupe Générique (GGM, Generic Group Model).
Le paradigme du GGM considère uniquement les attaques où l'on ne peut faire que des opérations entre les éléments observés : on suppose que les groupes sont génériques: ils ne possèdent à priori pas de structure particulière.
Nous prouvons la sécurité de notre schéma dans ce modèle.
Collaboration avec Balthazar Bauer.

*Intervenant