

IBE/PKG

Identity Based Encryption / Private Key Generator

- Identity-Based Encryption / Private Key Generator

Identity-Based Encryption / Private Key Generator

Der Private Key Generator (PKG) berechnet als Teil eines "Identity Based Encryption Systems" die privaten Schlüssel der Empfänger. Ein Empfänger muss ein eindeutiges Identitätsmerkmal (bspw. eine KVNR, TID, E-Mail-Adresse besitzen).

Mit dem PKG kann man ebenfalls einen Hashwert inkl. Zeitinformationen von beliebigen Nutzerdaten bestätigen lassen (quasi als Fernsignatur-Light).

Beispiel-Implementierung: https://bitbucket.org/andreas_hallof/pkg/

Vorträge:

Toller Vortrag von John Tate allgemein über die Arithmetik von elliptischen Kurven:

<https://www.youtube.com/watch?v=RtiVaALdqX0>

Super Vortragsreihe: [https://www.youtube.com/playlist?list=PL8Vt-](https://www.youtube.com/playlist?list=PL8Vt-7cSFnw2V2Wpf4MpwtSjvLvZo1ADB)

[7cSFnw2V2Wpf4MpwtSjvLvZo1ADB](https://www.youtube.com/playlist?list=PL8Vt-7cSFnw2V2Wpf4MpwtSjvLvZo1ADB), The 3rd BIU Winter School: Bilinear Pairings in Cryptography