Asymmetric Key Derivation Functions

Simon Fernandez

But principal

À partir d'une pair asymmétrique de clefs, en déduire une nouvelle paire qui soit valide et qui permette de conserver des propriétés de répudiation et de non-transitivité de la paternité.

Mathématiquement, on se place dans un système cryptographique dans lequel les clefs publiques sont dans G et les clefs privées dans S. Usuellement, $S = \mathbb{Z}/q\mathbb{Z}$ et G est un groupe cyclique d'ordre p premier.

Il faut donc :

- $f : S \to S$
- $F : G \to G$

Telles que (k, K) est une paire de clefs asymmetrique valide $\Rightarrow (f(k), F(K))$ est une paire de clefs valide