Contents

Chapter 1

Functions

1.1 factor.ecm – ECM factorization

This module has curve type constants:

S : aka SUYAMA. Suyama's parameter selection strategy.

B : aka BERNSTEIN. Bernstein's parameter selection strategy.

A1 : aka ASUNCION1. Asuncion's parameter selection strategy variant 1.

A2 : aka ASUNCION2. ditto 2.

A3 : aka ASUNCION3. ditto 3.

A4 : aka ASUNCION4. ditto 4.

A5 : aka ASUNCION5. ditto 5.

See J.S.Asuncion's master thesis [1] for details of each family.

1.1.1 ecm – elliptic curve method

> ecm(n: *integer*, curve_type: **curvetype**=**A1**, incs: *integer*=**3**, trials: *integer*=**20**, verbose: *bool*=**False**)
> $\rightarrow$ *integer*

n

n 1

curve_type **curvetype**

`incs` specifies a number of changes of bounds. The function repeats factorization trials several times changing curves with a fixed bounds.

Optional argument `trials` can control how quickly move on to the next higher

bounds.

    `verbose` toggles verbosity.

Bibliography

[1] Janice S. Asuncion. Integer factorization using different parameterizations of Montgomery's curves. Master's thesis, Tokyo Metropolitan University, 2006.