Mathematical Mesh 3.0 Part VIII: Cryptographic Algorithms

Mesh Cryptographic Algorithms

<series>draft-hallambaker-mesh-cryptography

<status>informational

<stream>independent

<ipr>trust200902

<author>Phillip Hallam-Baker

<surname>Hallam-Baker

<initials>P. M.

<firstname>Phillip

<email>phill@hallambaker.com

<also>http://mathmesh.com/Documents/draft-hallambaker-mesh-cryptography.html

The Mathematical Mesh ‘The Mesh’ is an infrastructure that facilitates the exchange of configuration and credential data between multiple user devices and provides end-to-end security. This document describes the

# Introduction

This document describes the cryptographic algorithm suites used in the Mesh and the implementation of Multi-Party Encryption and Multi-Party Key Generation used in the Mesh.

# Multi-Party Cryptography

The multi-party key generation and multi-party decryption mechanisms used in the Mesh protocols are made possible by the fact that Diffie Hellman key agreement and elliptic curve variants thereof support properties we call the Key Combination Law and the Result Combination Law.

Let {*X*, *x*}, {*Y*, *y*}, {*E*, *e*} be {public, private} key pairs.

The Key Combination law states that we can define an operator ⊗ such that there is a keypair {*Z*, *z*} such that:

*Z* = *X* ⊗ *Y* and *z* = (*x* + *y*) mod *o* (where *o* is the order of the group)

The Result Combination Law states that we can define an operator ⊙ such that:

(*x* ⊙ *E*) ⊕ (*y* ⊙ *E*) = (*z* ⊙ *E*) = (*e* ⊙ *Z*).

## Application to Diffie Hellman (not normative)

For the Diffie Hellman system in a modular field p, o = p-1 and *a* ⊗ *b* = *a* ⊙ *b* = *a*.*b* mod *p*.

*Proof:*

By definition, X = ex mod p, Y = ey mod p, and Z = ez mod p.

Therefore,

Z = ez mod p = ex+y mod p = (exey) mod p = ex mod p.ey mod p = X.Y

A similar proof may be constructed for the operator ⊙.