Data Storage By Secure Crumbling With Signing Trusted Third Parties

Cyril Dever
Edgewhere

September 18, 2020

Abstract

We define a secure data storage solution based on the presence of one (or more) trusted third parties necessary to perform encryption and decryption operations on a message split in crumbs. This secure storage method is particularly safe since the encryption elements are distributed among the different participants and can't be discovered by a single procedure which would allow breaking a unique encryption code. We show that this distribution of crumbs and their separate encryption considerably increases the security of the storage since, in the absence of a participant, the message can't be recovered. Furthermore, the algorithm doesn't allow anyone other than the rightful owner of the original message to know in clear all or part of the data at any time whatsoever.

I. Introduction

There are already multiple available ways to store data after encrypting it. However, the current techniques of data encryption for the storage and recovery of stored data and their decryption are operations all the more complex as the security must be high.

This complexity comes with the added burden of the risk that the encryption key is always susceptible to being broken and/or hacked.

The goal of our new algorithm, called the `crumbl` technology, is to develop simple yet particularly effective means for securing data storage.

Our procedure describes a method of secure storage of a source data, owned by one (or more) holder(s), using already proven techniques of asymmetric encryption with the participation of so-called trusted third parties, each having a pair of private and public keys.

II. The Algorithm

Lorem ipsum...

Contents

References

[1] Horst Feistel. *Cryptography and Computer Privacy*, Scientific American, 1973.

[2] Michael Luby, Charles Rackoff. *How to Construct Pseudorandom Permutations from Pseudorandom Functions*, SIAM Journal on Computing, 1988.