【19】中華民國　　【12】專利公報　（U）

【11】證書號數：M585458
【45】公告日： 中華民國 108 (2019) 年 10 月 21 日
【51】Int. Cl.：　*H04L9/26　(2006.01)*　*H04L9/28　(2006.01)*
新型　　全 4 頁

【54】名　　稱：　架構於混沌理論之網路資料加密系統
【21】申請案號：　108206353　　【22】申請日： 中華民國 108 (2019) 年 05 月 21 日
【72】新型創作人：顏錦柱 (TW) YAN, JUN-JUH；詹哲瑜 (TW) ZHAN, ZHE-YU；宋家偉 (TW) SONG, JIA-WEI；周昱宏 (TW) CHOU, YU-HONG
【71】申 請 人：　樹德科技大學　　SHU-TE UNIVERSITY
高雄市燕巢區橫山路 59 號
【74】代 理 人：　葉大慧
(NOTE)備註：　相同的創作已於同日申請發明專利(Another patent application for invention in respect of the same creation has been filed on the same date)

【57】申請專利範圍

1. 一種架構於混沌理論之網路資料加密系統，包括：　一聊天室伺服機，該聊天室伺服機設有一聊天室前端模組及一聊天室資料庫，該聊天室前端模組可於該聊天室資料庫中存取聊天紀錄；及　一安全伺服機本體，該安全伺服機本體與該聊天室伺服機相接，其設有一混沌加密模組，並具有複數個聊天室，使用者利用各該聊天室進行聊天並請求加密時，聊天紀錄將經過一混沌 AES 安全通道至該混沌加密模組，使該混沌加密模組透過 AES 對稱加密演算法，將當下的動態混沌值當作金鑰進行資料加密，並將同步所需要的資料送出，以便後續解密用，再將具混沌加密聊天紀錄存入該聊天室伺服機之聊天室資料庫中；而在有人請求解密時，可自該聊天室伺服機之聊天室資料庫中讀取該具混沌加密聊天紀錄，透過該安全伺服機本體之混沌加密模組啟動另一混沌系統作為同步動態金鑰之步驟，還原加密時的動態金鑰，並完成最後解密。
2. 如申請專利範圍第 1 項所述之架構於混沌理論之網路資料加密系統，其中該混沌加密模組之 AES 對稱加密演算法可為數位化超混沌 Henon map，利用數位化超混沌 Henon map 來設計動態金鑰產生器，並結合 SHA-256 利用其雪崩效應將原本 3 個狀態的 Henon map 透過 SHA-256 函式擴充成個狀態，提供 AES 加密所需求的金鑰長度。

圖式簡單說明

第 1 圖為本創作之架構於混沌理論之網路資料加密系統之系統方塊圖。

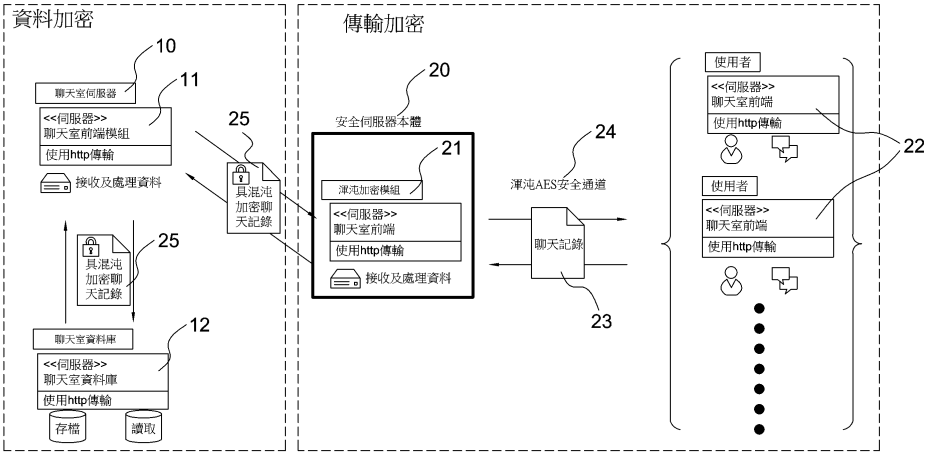
第 2 圖為為本創作之架構於混沌理論之網路資料加密系統之動態金鑰產生器之方塊示意圖。

第 3 圖為本創作之架構於混沌理論之網路資料加密系統之傳輸加密端架構圖。

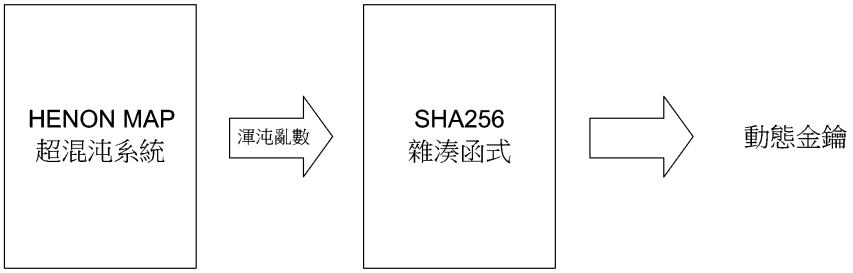
第 4 圖為本創作之架構於混沌理論之網路資料加密系統之資料加解密端流程圖。

第 5 圖為本創作之架構於混沌理論之網路資料加密系統之加密與動態金鑰未加入同步控制器之示意圖。

第 6 圖為本創作之架構於混沌理論之網路資料加密系統之加密與動態金鑰加入同步控制器之示意圖。

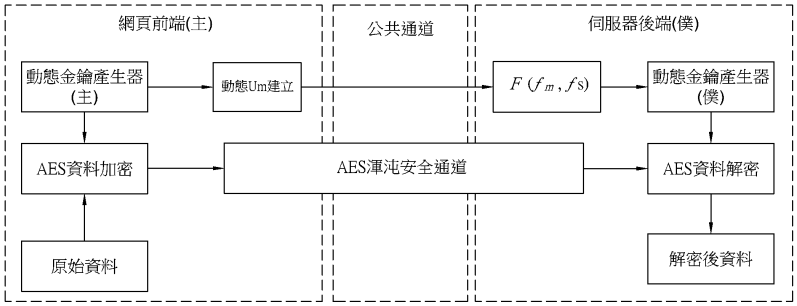

資料加密
傳輸加密
聊天室伺服器
10
11
<<伺服器>>
聊天室前端模組
使用http傳輸
接收及處理資料
25
具混沌
加密聊
天記錄
25
具混沌
加密聊
天記錄
聊天室資料庫
12
<<伺服器>>
聊天室資料庫
使用http傳輸
存檔
讀取
20
安全伺服器本體
21
渾沌加密模組
<<伺服器>>
聊天室前端
使用http傳輸
接收及處理資料
24
渾沌AES安全通道
聊天記錄
23
使用者
<<伺服器>>
聊天室前端
使用http傳輸
22
使用者
<<伺服器>>
聊天室前端
使用http傳輸

第1圖

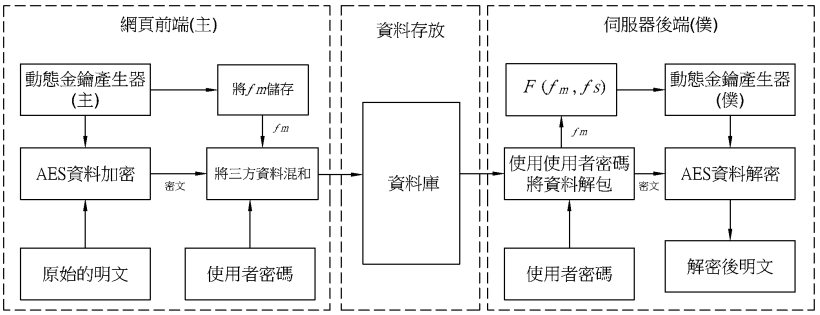

HENON MAP
超混沌系統
渾沌亂數
SHA256
雜湊函式
動態金鑰

第2圖

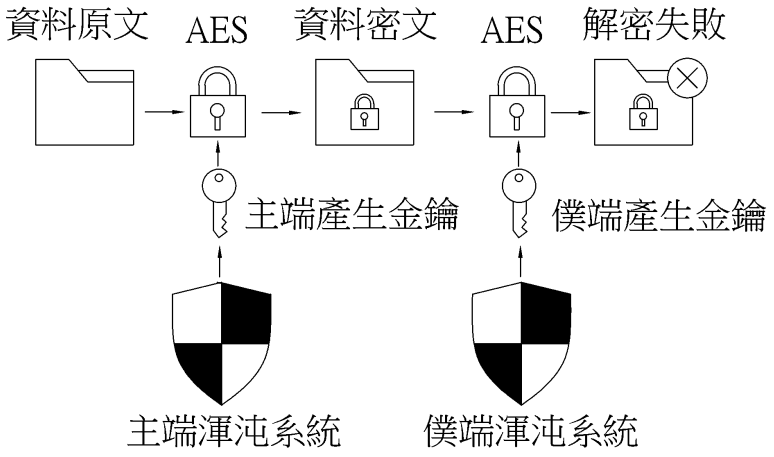
(3)


網頁前端(主)
公共通道
伺服器後端(僕)
動態金鑰產生器(主)
動態Um建立
F (fm , fs)
動態金鑰產生器(僕)
AES資料加密
AES渾沌安全通道
AES資料解密
原始資料
解密後資料

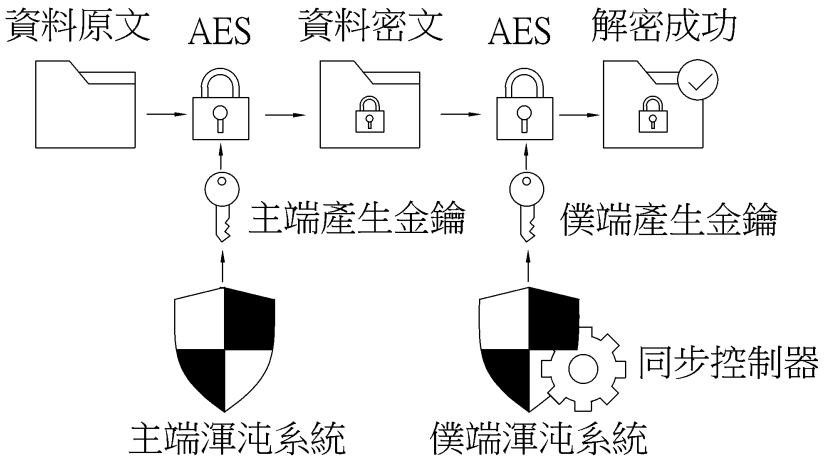
第3圖


網頁前端(主)
資料存放
伺服器後端(僕)
動態金鑰產生器(主)
將fm儲存
F (fm , fs)
動態金鑰產生器(僕)
fm
fm
AES資料加密
密文
將三方資料混和
資料庫
使用使用者密碼將資料解包
密文
AES資料解密
原始的明文
使用者密碼
使用者密碼
解密後明文

第4圖


資料原文
AES
資料密文
AES
解密失敗
主端產生金鑰
僕端產生金鑰
主端渾沌系統
僕端渾沌系統

第5圖


資料原文
AES
資料密文
AES
解密成功
主端產生金鑰
僕端產生金鑰
同步控制器
主端渾沌系統
僕端渾沌系統

第6圖