I796885

(19)中華民國智慧財產局

(12)發明說明書公告本 **(11)證書號數：TW I796885 B**

(45)公告日： 中華民國 112 (2023) 年 03 月 21 日

(21)申請案號：110147844 (22)申請日： 中華民國 110 (2021) 年 12 月 21 日

(51)Int. Cl.： ***H04L9/28 (2006.01)*** ***H04L9/06 (2006.01)***

(71)申請人：龍華科技大學 (中華民國) LUNGHWA UNIVERSITY OF SCIENCE AND TECHNOLOGY (TW)

桃園市龜山區萬壽路一段 300 號

(72)發明人：王柏東 WANG, PO-TONG (TW)

(74)代理人：李彥慶；林宗武

(56)參考文獻：

TW	I736271B	TW	202121191A
CN	110622477A	CN	110636028A
US	2019/0349762A1		

審查人員：黃偉倫

申請專利範圍項數：10 項 圖式數：4 共 12 頁

(54)名稱

工業物聯網及其安全通訊方法

(57)摘要

一種工業物聯網的安全通訊方法，其中工業物聯網包括主控端裝置以及從屬端裝置，通訊方法包括：主控端裝置發送加密密鑰至從屬端裝置；從屬端裝置解密加密密鑰以獲取一次性密鑰以及人工生命演化規則；從屬端裝置通過一次性密鑰以及人工生命演化規則加密明文以產生密文；從屬端裝置傳送密文至主控端裝置；以及主控端裝置通過一次性密鑰以及人工生命演化規則解密密文以獲得明文。藉此，以提升工業物聯網資訊安全與商業實用價值。

A safe communication method for the Industrial Internet of Things, where the Industrial Internet of Things includes a master device and a slave device. The safe communication method includes: the master device sending an encryption key to the slave device; the slave device decrypting the encryption key to obtain a one-time security key and artificial life evolution rules; the slave device encrypting a plaintext through the one-time security key and the artificial life evolution rules to generate a ciphertext; the slave device transmits the ciphertext to the master device; and the master device decrypting the ciphertext through the one-time security key and the artificial life evolution rules to obtain the plaintext. In this way, the industrial Internet of Things information security and commercial practical value are enhanced.

指定代表圖：

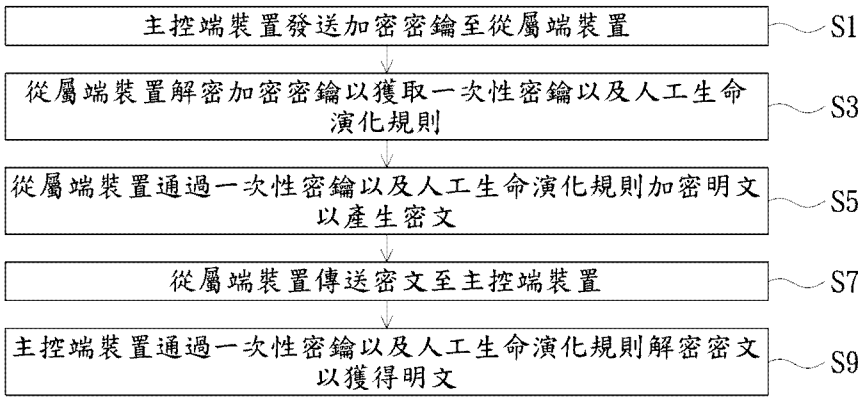

圖2

符號簡單說明：

S1,S3,S5,S7,S9:步驟

專利案號：110147844

公告本

I796885

【發明摘要】

【中文發明名稱】 工業物聯網及其安全通訊方法

【英文發明名稱】 INDUSTRIAL INTERNET OF THINGS AND SAFE COMMUNICATION METHOD THEREOF

【中文】

一種工業物聯網的安全通訊方法，其中工業物聯網包括主控端裝置以及從屬端裝置，通訊方法包括：主控端裝置發送加密密鑰至從屬端裝置；從屬端裝置解密加密密鑰以獲取一次性密鑰以及人工生命演化規則；從屬端裝置通過一次性密鑰以及人工生命演化規則加密明文以產生密文；從屬端裝置傳送密文至主控端裝置；以及主控端裝置通過一次性密鑰以及人工生命演化規則解密密文以獲得明文。藉此，以提升工業物聯網資訊安全與商業實用價值。

【英文】

A safe communication method for the Industrial Internet of Things, where the Industrial Internet of Things includes a master device and a slave device. The safe communication method includes: the master device sending an encryption key to the slave device; the slave device decrypting the encryption key to obtain a one-time security key and artificial life evolution rules; the slave device encrypting a plaintext through the one-time security key and the artificial life evolution rules to generate a ciphertext; the slave device transmits the ciphertext to the master device; and the master device decrypting the ciphertext through the one-time security key and the

artificial life evolution rules to obtain the plaintext. In this way, the industrial Internet of Things information security and commercial practical value are enhanced.

【指定代表圖】　　圖2

【代表圖之符號簡單說明】

S1, S3, S5, S7, S9　　步驟

111 年 10 月 18 日修正替換頁

【發明說明書】

【中文發明名稱】　工業物聯網及其安全通訊方法

【英文發明名稱】　INDUSTRIAL INTERNET OF THINGS AND SAFE COMMUNICATION METHOD THEREOF

【技術領域】

【0001】本發明是有關一種物聯網，尤其是一種工業物聯網及其安全通訊方法。

【先前技術】

【0002】傳統的密碼方式重複使用會發生被盜用，常常更換密碼又容易搞混或忘記，已不能滿足安全機制的需要。針對日趨普遍的工業物聯網面向的密碼與通訊應用，如何提供一種工業物聯網的安全通訊方法為本領域所要解決的技術問題。

【發明內容】

【0003】本發明提供一種工業物聯網及其安全通訊方法，可藉由工業物聯網裝置的唯一性代碼(UID)作為主控端/從屬端架構下的網路協議，並以從屬端的唯一性代碼作為網路身分認證的憑證，實現一種基於一次性密碼本(OTP)的高安全性的工業物聯網的安全通訊方法。

【0004】本發明所提供的工業物聯網的安全通訊方法包括：主控端裝置發送加密密鑰至從屬端裝置；從屬端裝置解密加密密鑰以獲取一次性密鑰以及人工生命演化規則；從屬端裝置通過一次性密鑰以及人工生命演化規則

加密明文以產生密文；從屬端裝置傳送密文至主控端裝置；以及主控端裝置通過一次性密鑰以及人工生命演化規則解密密文以獲得明文。

【0005】本發明所提供的工業物聯網包括從屬端裝置以及連接從屬端裝置的主控端裝置。其中主控端裝置與從屬端裝置之間執行安全通訊方法包括：主控端裝置發送加密密鑰至從屬端裝置；從屬端裝置解密加密密鑰以獲取一次性密鑰以及人工生命演化規則；從屬端裝置通過一次性密鑰以及人工生命演化規則加密明文以產生密文；從屬端裝置傳送密文至主控端裝置；以及主控端裝置通過一次性密鑰以及人工生命演化規則解密密文以獲得明文。

【0006】在本發明的一實施例中，上述從屬端裝置的唯一性代碼儲存於主控端裝置及從屬端裝置的非揮發性記憶體中。

【0007】在本發明的一實施例中，上述唯一性代碼用以隨機產生一次性密鑰。

【0008】在本發明的一實施例中，上述一次性密鑰基於人工生命演化規則產生一次性密碼本。

【0009】在本發明的一實施例中，上述一次性密碼本中加密明文的密碼位元數相同明文的位元數。

【0010】本發明因利用從屬端裝置的唯一性代碼產生一次性密碼本以作為工業物聯網安全的保密通訊及資訊交換，因此可以提升工業物聯網資訊安全與商業實用價值。

【0011】為讓本發明之上述和其他目的、特徵和優點能更明顯易懂，下文特舉實施例，並配合所附圖式，作詳細說明如下。

【圖式簡單說明】

【0012】

圖1為本發明一實施例所提供的工業物聯網的示意圖；

圖2為本發明一實施例所提供的工業物聯網的安全通訊方法的流程示意圖；

圖3為本發明一實施例所提供的工業物聯網裝置的示意圖；以及

圖4為本發明一實施例所提供的產生一次性密碼本的架構示意圖。

【實施方式】

【0013】請參閱圖1，為本發明一實施例所提供的工業物聯網的示意圖。本發明實施例所提供的工業物聯網1包括主控端裝置2以及至少一從屬端裝置3，其中至少一從屬端裝置3連接主控端裝置2。可以注意的是，主控端裝置2及至少一從屬端裝置3為工業用裝置如機器、設備、計算機、感測器等，而主控端裝置2及至少一從屬端裝置3之間可以無線/有線連接的方式傳輸資訊。另外，本發明將簡化以一主控端裝置2及一從屬端裝置3進行描述，以使本發明所屬技術領域中具有通常知識者更可以理解本發明之精神。

【0014】首先，從屬端裝置3的唯一性代碼儲存於主控端裝置2及從屬端裝置3的非揮發性記憶體中，較佳地儲存在主控端裝置2及從屬端裝置3的微控制單元(MCU)的閃存(Flash)或電子抹除式可複寫唯讀記憶體(EEPROM)中，用以進行從屬端裝置3的口令(token)認證。在主控端裝置2與從屬端裝置3確認彼此身分之後，將執行本發明實施例所提供的工業物聯網的安全通訊方法。

【0015】請參閱圖2，為本發明一實施例所提供的工業物聯網的安全通訊方法的流程示意圖。本發明實施例所提供的工業物聯網的安全通訊方法是執行於主控端裝置2及從屬端裝置3之間，用以對裝置之間通訊的資訊進行加密，以提升工業物聯網資訊安全與商業實用價值。

【0016】本發明實施例所提供的工業物聯網的安全通訊方法包括以下操作。步驟S1：主控端裝置2發送加密密鑰至從屬端裝置3。步驟S3：從屬端裝置3解密加密密鑰以獲取一次性密鑰以及人工生命演化規則。步驟S5：從屬端裝置3通過一次性密鑰以及人工生命演化規則加密明文以產生密文。步驟S7：從屬端裝置3傳送密文至主控端裝置2。步驟S9：主控端裝置2通過一次性密鑰以及人工生命演化規則解密密文以獲得明文。

【0017】其中，主控端裝置2及從屬端裝置3儲存的從屬端裝置3的唯一性代碼可隨機產生一次性密鑰，而一次性密鑰基於人工生命演化規則產生一次性密碼本(OTP)。其中，人工生命演化規則係一種渾沌動態系統，用以接收125/256/512位元的一次性密鑰來產生一次性密碼本。也就是說，只要一次性密鑰不同，一次性密碼本也就不同。

【0018】請參閱圖3所示，為本發明一實施例所提供的工業物聯網裝置的示意圖。主控端裝置2及從屬端裝置3分別包含明文/密文輸入模組4、連接明文/密文輸入模組4的人工生命演化模組5，以及連接人工生命演化模組5的加密/解密模組6。從屬端裝置3通過明文/密文輸入模組4接收明文，並以一次性密鑰通過人工生命演化模組5以人工生命演化規則產生一次性密碼本，接著通過加密/解密模組6以一次性密碼本加密明文以產生密文，並發送密文至主控端裝置2，其中一次性密鑰基於人工生命演化規則產生一次性密碼本以加密明文，且一次性密碼本中加密明文的密碼位元數相同明文的位元數。而主控端裝置2接收到密文之後，通過明文/密文輸入模組4接收密文，並以一次性密鑰通過人工生命演化模組5以人工生命演化規則產生一次性密碼本，接著通過加密/解密模組6以一次性密碼本解碼密文以取得明文。如此，通過裝置之間通訊資訊的加密，以提升工業物聯網資訊安全與商業實用價值。

【0019】請參閱圖4所示，為本發明一實施例所提供的產生一次性密碼本的架構示意圖。當主控端裝置2與從屬端裝置3確認彼此身分後，從屬端裝置3將會接收到主控端裝置2的加密密鑰，從屬端裝置3解密加密密鑰後獲取一次性密鑰與人工生命演化規則，從此從屬端裝置3可以得知主控端裝置2的一次性密鑰與人工生命演化規則，從屬端裝置3將可與主控端裝置2同步產生相同的一次性密碼本，以此通過相同的一次性密碼本對主控端裝置2與從屬端裝置3之間通訊的資訊加解密，以達到提升工業物聯網資訊安全與商業實用價值的目的。

【0020】可以注意的是，本發明所使用的工業物聯網裝置的唯一性代碼是安全並秘密的儲存在非揮發性記憶體中，可隨機產生一次性密鑰來做為工業務聯網的應用，除了可以達到真正隨機之外更可以防範隱私暴露的問題。並且本發明所實現的一次性密碼本是非全部或部分重複，而可以應用於各種身分認證領域中。同時本發明所使用的安全通訊方法可以應用於IEC 61158所規範的工業通訊協議中的現場總線，其所涵蓋的標準包括多種通信行規族群(Communication Profile Families, CPF)，如CPF01到CPF15包括：Foundation Fieldbus、CIP(Common Industrial Protocol)、PROFIBUS and PROFINET、P-NET、WorldFIP、INTERBUS、CC-Link、HART、Vent/IP、TCnet、EtherCAT、Ethernet POWER LINK、MODBUS-RTU、SERCOS、CANopen、以及CAN BUS等。

【0021】綜上所述，本發明所提供的工業物聯網及其安全通訊方法，因利用從屬端裝置的唯一性代碼為媒介來產生一次性密碼本以作為工業物聯網安全的保密通訊及資訊交換的手段，使工業物聯網裝置的唯一性代碼作為主控端/從屬端架構下的網路協議，並以從屬端裝置的唯一性代碼作為網路

身分認證的憑證，實現基於一次性密碼本的高安全性的工業物聯網的安全通訊方法，因此可以提升工業物聯網資訊安全與商業實用價值。

【0022】雖然本發明已以實施例揭露如上，然其並非用以限定本發明，本發明所屬技術領域中具有通常知識者，在不脫離本發明之精神和範圍內，當可作些許之更動與潤飾，因此本發明之保護範圍當視後附之申請專利範圍所界定者為準。

【符號說明】

【0023】

1　工業物聯網

2　主控端裝置

3　從屬端裝置

4　明文/密文輸入模組

5　人工生命演化模組

6　加密/解密模組

S1, S3, S5, S7, S9　步驟

【發明申請專利範圍】

【請求項1】 一種工業物聯網的安全通訊方法，適用於一工業物聯網，其中該工業物聯網包括一主控端裝置以及一從屬端裝置，該安全通訊方法包括：

該主控端裝置發送一加密密鑰至該從屬端裝置；

該從屬端裝置解密該加密密鑰以獲取一一次性密鑰以及一人工生命演化規則；

該從屬端裝置通過該一次性密鑰以及該人工生命演化規則加密一明文以產生一密文；

該從屬端裝置傳送該密文至該主控端裝置；以及

該主控端裝置通過該一次性密鑰以及該人工生命演化規則解密該密文以獲得該明文。

【請求項2】 如請求項1所述之安全通訊方法，其中該從屬端裝置的一唯一性代碼儲存於該主控端裝置及該從屬端裝置的非揮發性記憶體中。

【請求項3】 如請求項2所述之安全通訊方法，其中該唯一性代碼用以隨機產生該一次性密鑰。

【請求項4】 如請求項3所述之安全通訊方法，其中該一次性密鑰基於該人工生命演化規則產生一一次性密碼本以加密該明文。

【請求項5】 如請求項4所述之安全通訊方法，其中該一次性密碼本中加密該明文的密碼位元數相同該明文的位元數。

【請求項6】 一種工業物聯網，包括：

一從屬端裝置；以及

一主控端裝置，連接該從屬端裝置；

其中，該主控端裝置與該從屬端裝置之間執行一安全通訊方法，該安全通訊方法包括：

該主控端裝置發送一加密密鑰至該從屬端裝置；

該從屬端裝置解密該加密密鑰以獲取一一次性密鑰以及一人工生命演化規則；

該從屬端裝置通過該一次性密鑰以及該人工生命演化規則加密一明文以產生一密文；

該從屬端裝置傳送該密文至該主控端裝置；以及

該主控端裝置通過該一次性密鑰以及該人工生命演化規則解密該密文以獲得該明文。

【請求項7】 如請求項6所述之工業物聯網，其中該從屬端裝置的一唯一性代碼儲存於該主控端裝置及該從屬端裝置的非揮發性記憶體中。

【請求項8】 如請求項7所述之工業物聯網，其中該唯一性代碼用以隨機產生該一次性密鑰。

【請求項9】 如請求項8所述之工業物聯網，其中該一次性密鑰基於該人工生命演化規則產生一一次性密碼本。

【請求項10】 如請求項9所述之工業物聯網，其中該一次性密碼本中加密該明文的密碼位元數相同該明文的位元數。

【發明圖式】

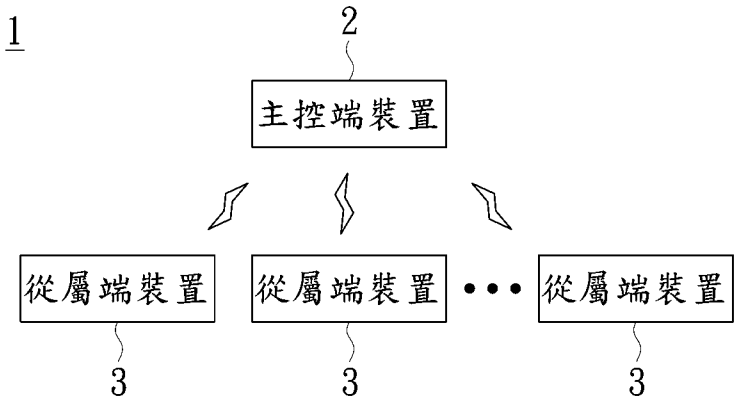
1
2
主控端裝置
從屬端裝置
從屬端裝置
從屬端裝置
3
3
3

圖1

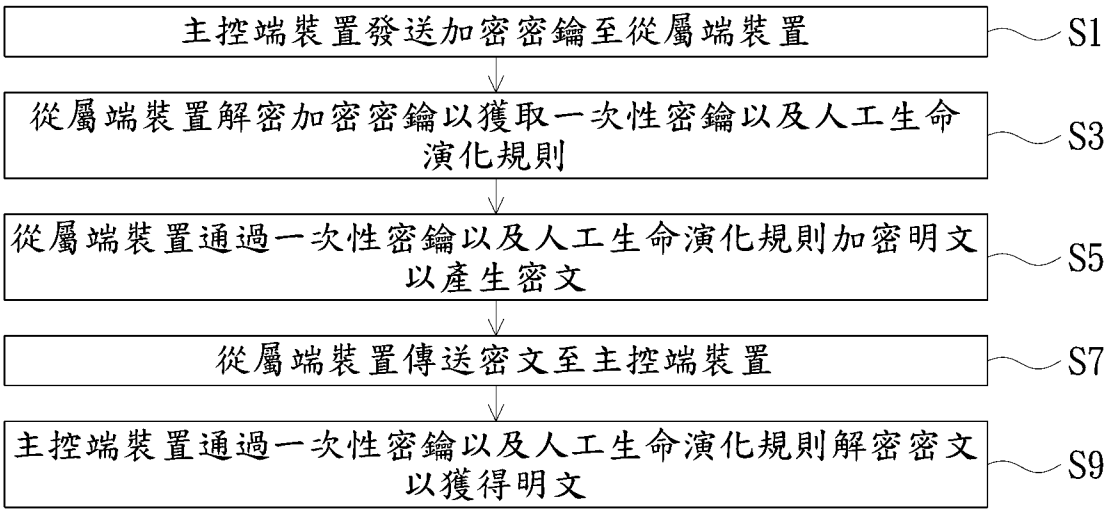
主控端裝置發送加密密鑰至從屬端裝置
S1
從屬端裝置解密加密密鑰以獲取一次性密鑰以及人工生命演化規則
S3
從屬端裝置通過一次性密鑰以及人工生命演化規則加密明文以產生密文
S5
從屬端裝置傳送密文至主控端裝置
S7
主控端裝置通過一次性密鑰以及人工生命演化規則解密密文以獲得明文
S9

圖2

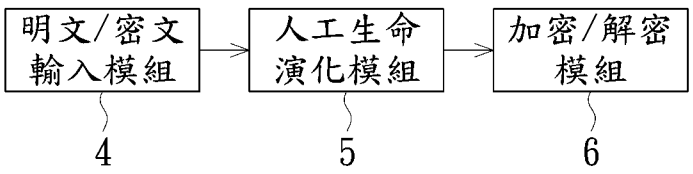
明文/密文輸入模組
人工生命演化模組
加密/解密模組
4
5
6

圖3

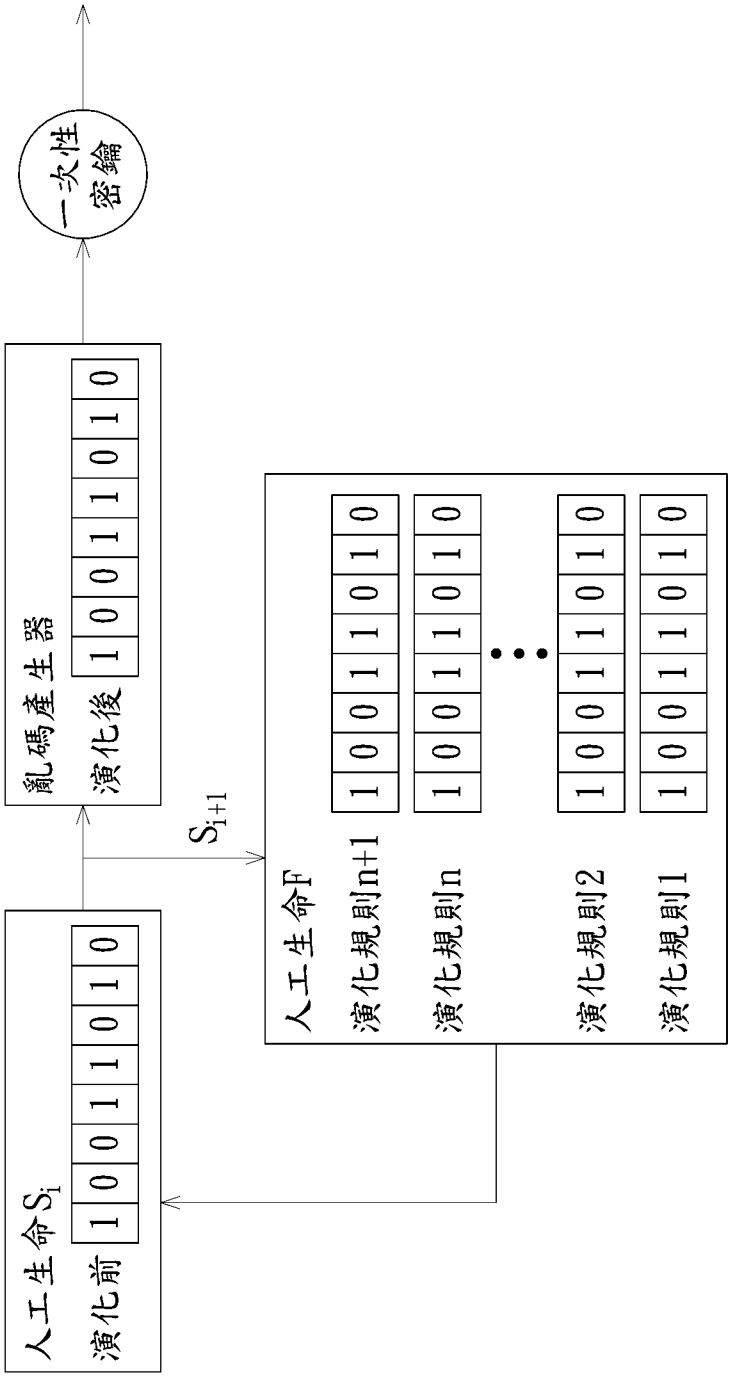
一次性密鑰
亂碼產生器
演化後
1 0 0 1 1 0 1 0
人工生命F
演化規則n+1
1 0 0 1 1 0 1 0
演化規則n
1 0 0 1 1 0 1 0
演化規則2
1 0 0 1 1 0 1 0
演化規則1
1 0 0 1 1 0 1 0
S_{i+1}
人工生命S_i
演化前
1 0 0 1 1 0 1 0

圖4