المملكة العربية السعودية
Kingdom of Saudi Arabia

الهيئة السعودية للملكية الفكرية
Saudi Authority for Intellectual Property

براءة اختراع

إن الرئيس التنفيذي للهيئة السعودية للملكية الفكرية و بموجب أحكام نظام براءات الإختراع و التصميمات التخطيطية للدارات المتكاملة و الأصناف النباتية و النماذج الصناعية الصادر بالمرسوم الملكي الكريم رقم م/27 وتاريخ 1425/05/29هـ و المعدل بقرار مجلس الوزراء رقم 536 و تاريخ 1439/10/19هـ ، و لائحته التنفيذية.
يقرر منح :

جامعة طيبة
Taibah University

براءة اختراع رقم : SA 19859

بتاريخ : 1446/09/29 هـ
الموافق : 2025/03/29 م

عن الإختراع المسمى :

تامين البيانات وادارة مفاتيح التشفير الخاصة بأجهزة انترنت الاشياء في السحابة الالكترونية العامة

Secure data and encryption keys Management of Internet of things devices in the public cloud

وفق ما هو موضح في وصف الاختراع المرفق، ولمالك البراءة الحق في الانتفاع بكامل الحقوق النظامية في المملكة العربية السعودية خلال فترة سريان الحماية.

الرئيس التنفيذي

د. عبدالعزيز بن محمد السويلم

الهيئة السعودية للملكية الفكرية
Saudi Authority for Intellectual Property

[19] **الهيئة السعودية للملكية الفكرية**
[11] **رقم البراءة:** SA 19859 B1

[12] براءة اختراع

[45] **تاريخ المنح:** 1446/09/29 هـ
الموافق: 2025/03/29 م

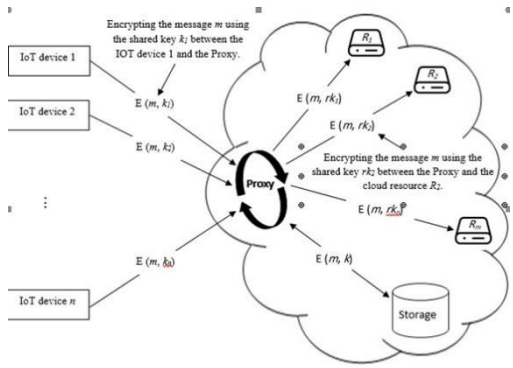
[21] **رقم الطلب:** 121430423
[22] **تاريخ الايداع:** 1443/05/08 هـ
الموافق: 2021/12/12 م
[72] **اسم المخترع:** علاء الدين عمرو ،محمد عبدالقادر العسلي
[73] **مالك البراءة:** جامعة طيبة
عنوانه: 344 المدينة المنورة، المملكة العربية السعودية
جنسيته: سعودية
[51] **التصنيف الدولي(IPC[8]):**
G06F21/30; G06F21/50; G06F21/57
[56] **المراجع:**
US 2015/ 0365412 A1
الفاحص: لينه عبدالكريم العبدالكريم

[54] **اسم الاختراع:** تامين البيانات وادارة مفاتيح التشفير الخاصة بأجهزة انترنت الاشياء في السحابة الالكترونية العامة

Secure data and encryption keys Management of Internet of things devices in the public cloud

[57] **الملخص:** يتعلق الاختراع بتامين البيانات وادارة مفاتيح التشفير الخاصة بأجهزة انترنت الاشياء في السحابة الالكترونية العامة و يتم زرع (حرق) خوارزمية التشفير في اجهزة انترنت الاشياء 1 [IoT devices] في مرحلة التصنيع و تتم عملية انشاء و تبادل المفاتيح مع مزود الخدمة السحابية و الاجهزة المراد التواصل معها في السحابة الالكترونية. يتم تبادل مفاتيح التشفير مع محول المفاتيح 3 [Proxy] الذي يقع في داخل السحابة الالكترونية بشكل آمن بحيث انه لا يمكن معرفة هذه المفاتيح الا من قبل [IoT devices 1] و 3 [Proxy] فقط. بعد ذلك لو تم تعيين أي من الأجهزة المتوفرة في السحابة الالكترونية المورد السحابي] 1[لكي يقوم بعملية معالجة البيانات المشفرة فانه يتم مشاركة مفتاح جديد بينه وبين محول المفاتيح ومن دون تدخل اجهزة انترنت الاشياء. وكذلك يتم تشفير البيانات التي ينبغي ان تخزن بالسحابة الالكترونية باستخدام مفتاح تشفير لا يمكن معرفتها الا من قبل محول المفاتيح فقط. ينبغي ملاحظة ان محول المفاتيح ليس برنامج (Software) يعمل على جهاز حاسب عادي كما هو الحال في الانظمة السحابية الحالية وانما جهاز مادي (Hardware) يتم برمجته بشكل آمن خارج السحابة الالكترونية ولا يوجد أي تحكم به من قبل مزود خدمة السحابة الالكترونية. الاختراع لا يمكن المهاجم او حتى مزود الخدمة من معرفة مفاتيح فك التشفير ولا تتطلب قدرات تشفير عالية مما يحقق الهدف دون اضافة تعقيدات كبيرة. ايضا، تستخدم الطريقة المقترحة خوارزمية التشفير المتقدم Advanced Encryption Standard (AES) المعمول بها حاليا في الجهات الصناعية المتخصصة في انترنت الاشياء ولا تتطلب اي خوارزمية جديدة مما يجعل الطريقة أكثر فعالية وأكثر قابلية للتطبيق. الشكل (1)

عدد عناصر الحماية (1)، عدد الأشكال (3)



الشكل ١: الطريقة المبتكرة لحماية سرية البيانات في السحابة الالكترونية

تامين البيانات وادارة مفاتيح التشفير الخاصة بأجهزة انترنت الاشياء في السحابة الالكترونية العامة

Secure data and encryption keys Management of Internet of things devices in the public cloud

الوصف الكامل

خلفية الاختراع

يحل الاختراع مشكلتين رئيستين تتعلق بتأمين بيانات أجهزة انترنت الاشياء في السحابة الالكترونية الاولى: و هي إمكانية الاختراق من قبل مزود الخدمة السحابية و الثانية: بطئ التشفير البرمجي العادي وامكانية استبداله بتشفير العتاد (Hardware encryption) المقترح في هذا الاختراع.

يقدم الاختراع طريقة لتأمين البيانات وإدارة مفاتيح التشفير بأجهزة انترنت الأشياء في السحابة الالكترونية العامة حيث يتم زرع (حرق) خوارزمية التشفير في مرحلة التصنيع و تتم عملية انشاء و تبادل المفاتيح مع مزود الخدمة السحابية و الاجهزة المراد التواصل معها في السحابة الالكترونية.

و أقرب حالات التقية للاختراع الحالي كالاتي:

الوثيقة الامريكية 8,826,013 B1 حيث تكشف عن نظام حماية بيانات العملاء في الأجهزة الافتراضية السحابية باستخدام خادم إدارة مركزي حيث ترسل وحدة التحقق طلبًا رئيسيًا إلى خادم إدارة المفاتيح ، والذي يوفر خدمة رئيسية لأنظمة كمبيوتر سحابية مختلفة و يقوم خادم إدارة المفاتيح بالتحقق من صحة الطلب ، وإذا كان الطلب صالحًا ، فإنه يوفر المفتاح للجهاز الظاهري ولكن الطريقة المقترحة لا تخدم أجهزة انترنت الأشياء في السحابة العامة.

الوثيقة الامريكية US 2017/0223019 A1 حيث تكشف طريقة مصادقة تفويضية بين التطبيقات المختلفة تتضمن نظام لتفويض مصادقة تطبيق غير موثوق به يتم تنفيذه على جهاز عميل. للمصادقة المفوضة ، يعتمد التطبيق غير الموثوق به على تطبيق موثوق به يتم تنفيذه في نفس البيئة لأغراض المصادقة. تتجنب عملية المصادقة المفوضة مطالبة مستخدم التطبيق غير

الموثوق به تقديم أوراق اعتماد المصادقة. يتيح النظام الذي تم الكشف عنه لتفويض المصادقة أي تطبيق موثوق به يتم تنفيذه في نفس بيئة الحوسبة لمصادقة التطبيق غير الموثوق به. ولكن النظام المقترح لا يناسب البيئة السحابية ولكن يناسب بيئة التطبيقات فقط.

الوثيقة اليابانية JP6518844B1 حيث تكشف عن طبقة أمان البرمجيات الوسيطة لخدمات الحوسبة السحابية وتتضمن إدارة أمن الشبكة أو سياسات أمن الشبكة ، على سبيل المثال الخدمات المُدارة ، وتحديد مكان وضع جدران الحماية ، والبيانات المراد تشفيرها ، وطريقة المصادقة التي يجب استخدامها ، وما إلى ذلك ولكن الطريقة لم تتطرق للحماية بشكل كلي في السحابة ولكن وصفت ما يمكن تقديمه لادارة عناصر الحماية في السحابة العامة.

<u>الوصف العام للاختراع</u>

التقنية المقترحة هي التشفير المادي (Hardware encryption) بحيث يتم زرع (حرق) خوارزمية التشفير في اجهزة انترنت الاشياء IoT devices [1] في مرحلة التصنيع و تتم عملية انشاء و تبادل المفاتيح مع مزود الخدمة السحابية و الاجهزة المراد التواصل معها في السحابة. كما هو موضح في الشكل-1، يتم تبادل مفاتيح التشفير مع Proxy [3] الذي يقع في داخل السحابة الالكترونية بشكل آمن بحيث انه لا يمكن معرفة هذه المفاتيح الا من قبل IoT devices [1] و Proxy [3] فقط. بعد ذلك لو تم تعيين أي من المورد السحابي [2] المتوفرة في السحابة الالكترونية لكي يقوم بعملية معالجة البيانات المشفرة فانه يتم مشاركة مفتاح جديد بينه وبين Proxy [3] ومن دون تدخل IoT devices [1] . وكذلك يتم إعادة تشفير البيانات التي ينبغي ان تخزن في السحابة الالكترونية باستخدام مفتاح تشفير لا يعرف الا من قبل Proxy [3] فقط. ينبغي ملاحظة ان Proxy [3] ليس برنامج (Software) يعمل على جهاز حاسب عادي وانما Hardware يتم برمجتها بشكل آمن خارج السحابة العامة ولا يوجد أي تحكم بها من قبل مزود خدمة السحابة الالكترونية.

الطريقة المقترحة لا تمكن المهاجم او حتى مزود الخدمة من معرفة مفاتيح فك التشفير ولا تتطلب قدرات تشفير عالية مما يحقق الهدف دون اضافة تعقيدات كبيرة على النظام. ايضا، تستخدم الطريقة المقترحة خوارزمية التشفير AES المعمول بها حاليا في الجهات الصناعية المتخصصة في انترنت الاشياء ولا تتطلب اي خوارزمية جديدة مما يجعل الطريقة أكثر فعالية وأكثر قابلية للتطبيق.

لمعرفة طريقة عمل تحويل البيانات عن طريق Proxy [3] . يلاحظ ان IoT devices [1] و المورد السحابي [2] تعطي مفاتيح التشفير ومعلومات أخرى ل Proxy [3] لكي يتم عملية تحويل البيانات المشفرة لكي يتم فك تشفيرها بشكل آمن من قبل المورد السحابي [2]. ان طريقة تحويل البيانات الموضحة في الشكل سريعة جدا عندما يتم تنفيذها في Hardware ولا تستغرق وقت كبير وبالتالي أداء هذه الطريقة مثالي وآمن. لكي يتم تبادل المعلومات بين هذه الجهات، يتم استخدام مفتاح تشفير Public key خاص ب Proxy [3] ويتم فك التشفير باستخدام Private key خاص ب Proxy [3] بشكل آمن باستخدام خوارزمية RSA. كما يمكن الاستغناء عن خوارزمية AES كما هو موضح بالشكل-3.

<u>شرح مختصر للرسومات</u>

الشكل 1: الطريقة المبتكرة لحماية سرية البيانات في السحابة الالكترونية

الشكل 2: طريقة عمل ال Proxy

الشكل 3: طريقة عمل ال Proxy بدون استخدام خوارزمية AES

<u>الوصف التفصيلي:</u>

طريقة تامين البيانات و ادارة مفاتيح التشفير الخاصة باجهزة انترنت الاشياء في السحابة الالكترونية تتم من خلال الخطوات التالية:

1 . الشكل-2 يوضح التقنية المقترحة في التشفير المادي (Hardware encryption) بحيث يتم زرع (حرق) خوارزمية التشفير في اجهزة انترنت الاشياء IoT devices [1] في مرحلة التصنيع وتتكون خوارزمية التشفير من خوارزمية Hash وخوارزمية AES المعروفتين في المجال الصناعي حاليا. حيث يتم تزويد Hash بمفتاح k1 مضاف اليه رقم يستخدم لمرة واحدة n1 وكذلك يتم تزويد AES بعداد CTR. يتم عمل XOR بين المخرج من AES وبين البيانات المراد ارسالها P . يتم إضافة n1 الى الرسالة المشفرة لمنع عديد من الهجمات مثل replay attack. في حالة ان IoT devices [1] مصادرها ضعيفة جدا يمكن الاستغناء عن AES كما هو موضح بالشكل-3. تقوم IoT devices [1] بإرسال البيانات المشفرة الى Proxy [3] في السحابة العامة.

2 . يتم زرع (حرق) خوارزمية إعادة التشفير في Proxy [3] من قبل طرف ثالث ليس له علاقة بمزود الخدمة السحابية ويتم مشاركة مفتاح k1 باستخدام مفتاح تشفير Public key خاص ب Proxy [3] ويتم فك التشفير باستخدام Private key خاص ب Proxy [3] بشكل آمن باستخدام خوارزمية RSA المعروفة. الشكل-2 يوضح طريقة عمل ال Proxy [3] حيث يتم استقبال البيانات المشفرة من IoT devices [1] ويتم اخذ n1 واضافته الى k1 المشارك سابقا ويتم عمل Hash لهما لكي يتم انتاج نفس المفتاح المكون في IoT devices [1]. بعد ذلك يتم ادخال القيمة المخرجة من Hash الى AES ويتم استخدام نفس عداد CTR لتكوين المفتاح النهائي الذي استخدم لتشفير البيانات في IoT devices [1]. قد تكون البيانات المشفرة اتية من اكثر من جهاز IoT devices [1] وهذا يصعب من عملية فك تشفيرها في المورد السحابي الذي سيقوم بمعالجة البيانات ولذلك يتم إعادة تشفير البيانات بشكل متماثل عن طريق ال Proxy [3]. تقوم Proxy [3] بعمل XOR للمخرج من AES مع البيانات المشفرة الواردة من IoT devices [1] ومع المخرج من AES باستخدام عداد CTR2 ومفتاح rk1 الذي تم مشاركته بين المورد السحابي [2] و Proxy [3] لإعادة تشفير البيانات دون الحاجة لفك التشفير وإعادة التشفير بشكل متماثل. يمكن الاستغناء عن AES كما هو موضح بالشكل-3. تقوم Proxy [3] بارسال البيانات المعاد تشفيرها الى بالمورد السحابي [2] في السحابة العامة.

3 . يستقبل المورد السحابي [2] البيانات المعاد تشفيرها ويقوم بفك التشفير بنفس الطريقة التي تم تشفيرها في اجهزة انترنت الاشياء IoT devices [1] كم في الشكل-2 والشكل-3 ولكن

باستخدام مفتاح rk1 مما يحافظ على امان مفاتيح IoT devices [1] حيث ان هذه المفاتيح غير معروفة الا لل Proxy [3] فقط في السحابة العامة مما يجعل عملية زرع (حرق) خوارزمية التشفير في IoT devices [1] تتم مرة واحدة فقط اثناء التصنيع.

.4 يتم تشفير البيانات التي ينبغي ان تخزن في خوادم التخزين [4] بالسحابة العامة باستخدام مفتاح تشفير لا يعرف الا من قبل Proxy [3] فقط.

الطريقة المقترحة لا تمكن المهاجم او حتى مزود الخدمة من معرفة مفاتيح فك التشفير ولا تتطلب قدرات حسابية عالية مما يحقق الهدف دون اضافة تعقيدات كبيرة على النظام. ايضا، تستخدم الطريقة المقترحة خوارزمية التشفير AES و Hashالمعمول بهما حاليا في الجهات الصناعية المتخصصة في انترنت الاشياء ولا تتطلب اي خوارزمية جديدة مما يجعل الطريقة أكثر فعالية وأكثر قابلية للتطبيق.

الشكل-1 يوضح التصور العام وعلاقة الجهات المختلفة بالجهات الأخرى في هذه الطريقة المخترعة. طريقة عمل تحويل البيانات عن طريقProxy [3] تتم بشكل امن وفعال حيث ان IoT devices [1] و المورد السحابي [1] تعطي مفاتيح التشفير ومعلومات أخرى لProxy [3] لكي يتم عملية تحويل البيانات المشفرة ولكي يتم فك تشفيرها بشكل آمن من قبل المورد السحابي [1] .ان طريقة تحويل البيانات عن طريق Proxy [3] الموضحة في الشكل سريعة جدا حيث يتم تنفيذها في Hardware ولا تستغرق أي وقت وهي تعتبر مكون كاي مكون في الشبكة الخاصة بالسحابة العامة وبالتالي أداء هذه الطريقة مثالي وآمن. ان ال Proxy [3] قابل للتوسع ويمكن إضافة وحرق نسخ منه حسب الحاجة مما يجعله مثالي في بيئة السحابة العامة. كما هو موضح في الشكل-1، يتم تبادل مفاتيح التشفير مع Proxy [3] الذي يقع في داخل السحابة العامة بشكل آمن بحيث انه لا يمكن معرفة هذه المفاتيح الا من قبل IoT devices [1] و Proxy [3] فقط. بعد ذلك لو تم تعيين أي من المورد السحابي [1] المتوفرة في السحابة العامة لكي يقوم بعملية معالجة البيانات المشفرة فانه يتم مشاركة مفتاح جديد بينه وبين Proxy [3] ومن دون تدخل IoT devices [1] .

عناصر الحماية

1. طريقة لإدارة مفاتيح التشفير لأجهزة إنترنت الأشياء(1) في السحابة الالكترونية العامة بواسطة حرق أو برمجة صلبة (hardware encryption) لخوارزمية التشفير المتماثل أثناء تصنيع أجهزة انترنت الاشياء(1) لضمان تأمين مفاتيح التشفير وبإضافة بروكسي متماثل (3) يقوم بتوزيع مفاتيح التشفير بأمان بين أجهزة إنترنت الأشياء المتعددة (1) و الموارد السحابية (2)، حيث يتم توليد هذه المفاتيح بشكل آمن بواسطة البروكسي المتماثل داخل السحابة الإلكترونية العامة

حيث تشتمل الطريقة على الخطوات التالية:

- يتم حرق خوارزمية التشفير المتماثل في تصاميم أجهزة انترنت الاشياء(1) اثناء مرحلة تصنيعها;

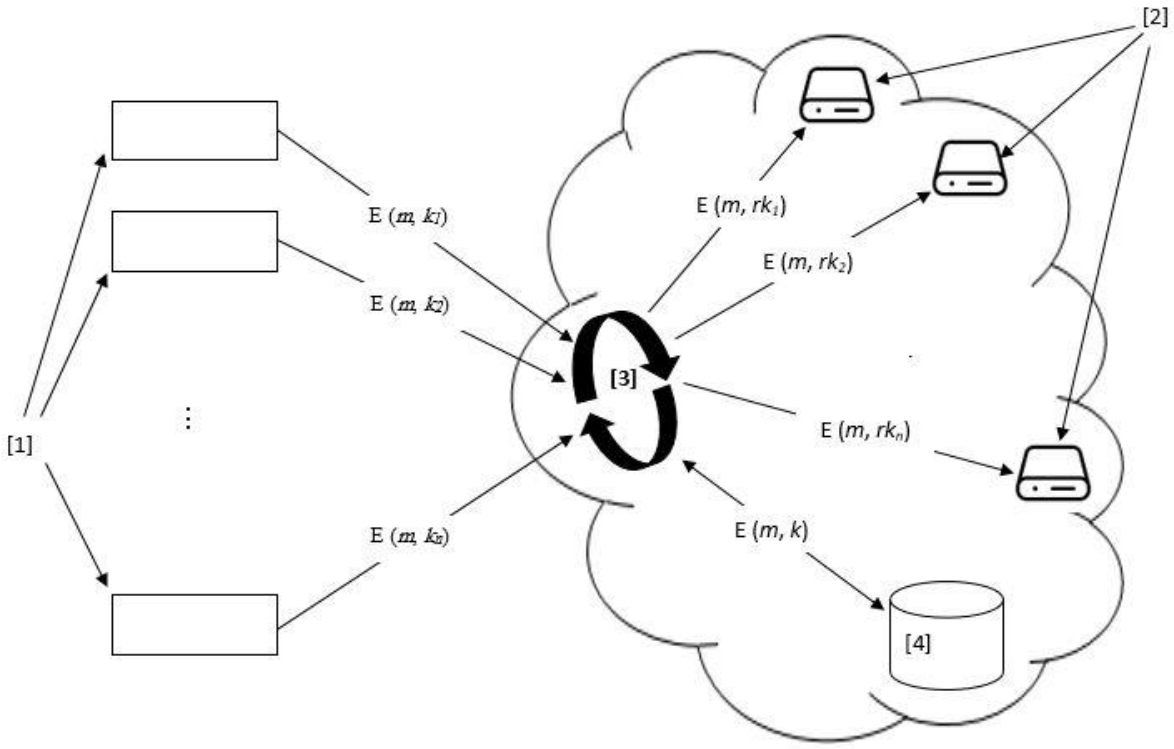
-ثم يقوم البروكسي المتماثل بتوزيع مفاتيح التشفير بأمان بين أجهزة إنترنت الأشياء(1) المتعددة و المورد السحابي (2) بعد اتصال أجهزة انترنت الاشياء(1) بالسحابة، حيث يتم توليد هذه المفاتيح بشكل آمن بواسطة البروكسي;

-ثم يقوم البروكسي المتماثل باستقبال البيانات المشفرة من أجهزة إنترنت الأشياء (1) المتعددة ونقلها بأمان دون فك التشفير، مع استخدام مفتاح تشفير واحد للبيانات المُرسلة إلى المورد السحابي(2);

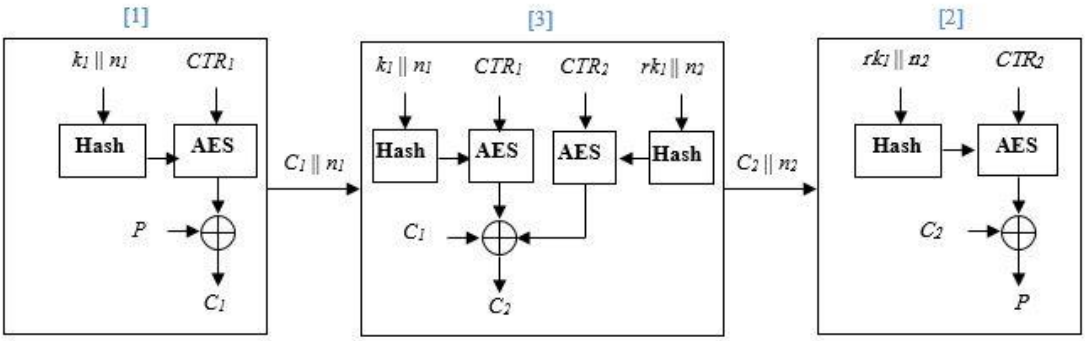
-ثم يتم إعداد تزامن بين البروكسي المتماثل(3) وأجهزة إنترنت الأشياء (1) حسب خوارزمية التشفير المتماثل ;

- ثم يتم توليد مفاتيح التشفير و إعداد تزامن بين البروكسي المتماثل(3) و المورد السحابي(2) حسب خوارزمية التشفير المتماثل;

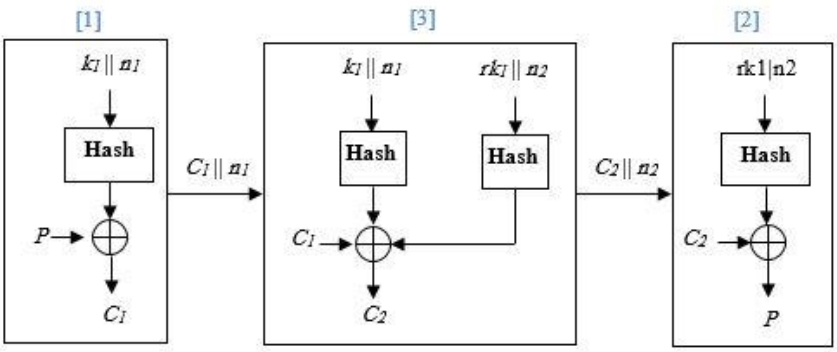
-حينها يتم فك تشفير البيانات في المورد السحابي (2) فقط أثناء معالجة البيانات.



الشكل -1


[1]
[3]
[2]
$k_1 \| n_1$
CTR_1
Hash
AES
P
C_1
$C_1 \| n_1$
$k_1 \| n_1$
CTR_1
CTR_2
$rk_1 \| n_2$
Hash
AES
AES
Hash
C_1
C_2
$C_2 \| n_2$
$rk_1 \| n_2$
CTR_2
Hash
AES
C_2
P

الشكل- 2


[1]
[3]
[2]
$k_1 \| n_1$
Hash
P
C_1
$C_1 \| n_1$
$k_1 \| n_1$
$rk_1 \| n_2$
Hash
Hash
C_1
C_2
$C_2 \| n_2$
rk1|n2
Hash
C_2
P

الشكل - 3

مدة سريان هذه البراءة عشرون سنة

من تاريخ إيداع الطلب

وذلك بشرط تسديد المقابل المالي السنوي للبراءة وعدم بطلانها أو سقوطها لمخالفتها لأي من أحكام نظام براءات الاختراع والتصميمات التخطيطية للدارات المتكاملة والأصناف النباتية والنماذج الصناعية أو لائحته التنفيذية.

صادرة عن

الهيئة السعودية للملكية الفكرية

ص ب ٦٥٣١ ، الرياض ١٣٣٢١ ، المملكة العربية السعودية

SAIP@SAIP.GOV.SA