الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T X.1811

(2021/04)

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن شبكات الاتصالات المتنقلة الدولية–2020

مبادئ توجيهية تتعلق بالأمن من أجل تطبيق خوارزميات آمنة من حيث الحوسبة الكمومية في أنظمة الاتصالات المتنقلة الدولية–2020

التوصية ITU-T X.1811

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199–X.1
التوصيل البيني للأنظمة المفتوحة	X.299–X.200
التشغيل البيني للشبكات	X.399–X.300
أنظمة معالجة الرسائل	X.499–X.400
الدليل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699–X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799–X.700
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899–X.850
المعالجة الموزعة المفتوحة	X.999–X.900
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029–X.1000
أمن الشبكة	X.1049–X.1030
إدارة الأمن	X.1069–X.1050
الخصائص البيومترية	X.1099–X.1080
تطبيقات وخدمات آمنة (1)	
أمن البث المتعدد	X.1109–X.1100
أمن الشبكة المحلية	X.1119–X.1110
أمن الخدمات المتنقلة	X.1139–X.1120
أمن الويب	X.1149–X.1140
بروتوكولات الأمن (1)	X.1159–X.1150
الأمن بين جهتين نظيرتين	X.1169–X.1160
أمن معرفات الهوية عبر الشبكات	X.1179–X.1170
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1199–X.1180
أمن الفضاء السيبراني	
الأمن السيبراني	X.1229–X.1200
مكافحة الرسائل الاقتحامية	X.1249–X.1230
إدارة الهوية	X.1279–X.1250
تطبيقات وخدمات آمنة (2)	
اتصالات الطوارئ	X.1309–X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1319–X.1310
أمن شبكة الكهرباء الذكية	X.1339–X.1330
البريد المعتمد	X.1349–X.1340
أمن إنترنت الأشياء (IoT)	X.1369–X.1360
أمن أنظمة النقل الذكية (ITS)	X.1389–X.1370
أمن سجل الحسابات الموزع	X.1429–X.1400
أمن سجل الحسابات الموزع	X.1449–X.1430
البروتوكول الأمني (2)	X.1459–X.1450
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1519–X.1500
تبادل مواطن الضعف/الحالة	X.1539–X.1520
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل السياسات	X.1559–X.1550
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569–X.1560
تعرف الهوية والاكتشاف	X.1579–X.1570
التبادل المضمون	X.1589–X.1580
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1601–X.1600
تصميم أمن الحوسبة السحابية	X.1639–X.1602
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1659–X.1640
تنفيذ أمن الحوسبة السحابية	X.1679–X.1660
أمن أشكال أخرى للحوسبة السحابية	X.1699–X.1680
الاتصالات الكمومية	
المصطلحات	X.1701–X.1700
مولّد الأعداد العشوائية الكمومية	X.1709–X.1702
إطار أمن شبكات توزيع المفاتيح الكمومية	X.1711–X.1710
تصميم أمن شبكات توزيع المفاتيح الكمومية	X.1719–X.1712
تقنيات أمن شبكات توزيع المفاتيح الكمومية	X.1729–X.1720
أمن البيانات	
أمن البيانات الضخمة	X.1759–X.1750
أمن شبكات الاتصالات المتنقلة الدولية–2020	**X.1819–X.1800**

لمزيد من التفاصيل يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصية ITU-T X.1811

مبادئ توجيهية تتعلق بالأمن من أجل تطبيق خوارزميات آمنة من حيث الحوسبة الكمومية في أنظمة الاتصالات المتنقلة الدولية–2020

ملخص

تحدد التوصية ITU-T X.1811 التهديدات التي تثيرها الحوسبة الكمومية وتواجهها أنظمة الاتصالات المتنقلة الدولية–2020 (IMT-2020)، من خلال تقييم مستوى الأمن لخوارزميات التجفير المستعملة حالياً. وتستعرض هذه التوصية بإيجاز الخوارزميات الآمنة من حيث الحوسبة الكمومية، بما في ذلك الأنماط التناظرية وغير التناظرية، وتقدم مبادئ توجيهية من أجل تطبيق خوارزميات آمنة من حيث الحوسبة الكمومية في أنظمة الاتصالات المتنقلة الدولية–2020.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1811	2021-04-30	17	11.1002/1000/14454

مصطلحات أساسية

نظام الجيل الخامس، خوارزمية غير تناظرية، نظام الاتصالات المتنقلة الدولية–2020، الحاسوب الكمومي، خوارزمية آمنة من حيث الحوسبة الكمومية، خوارزمية تناظرية.

* للنفاذ إلى توصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات وكالة الأمم المتحدة المتخصصة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يلزم" وصيغ ملزمة أخرى مثل فعل "يجب" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، كان الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

الصفحة

مقدمة

يَعد نظام الاتصالات المتنقلة الدولية–2020 (IMT-2020) بدعم مجموعة واسعة من الخدمات مع متطلبات أداء متنوعة من أجل إنشاء مجتمع موصول بالكامل. ولتحقيق هذا الهدف الصعب، تم تطوير عدد من التكنولوجيات المبتكرة في نظام الاتصالات المتنقلة الدولية–2020، مثل تقسيم وظائف الشبكة والشبكة المعرفة بالبرمجيات والتمثيل الافتراضي لوظائف الشبكة والفصل بين الوحدات المركزية/الوحدات الموزعة (CU/DU). وتعتبر الإجراءات الأمنية أساسية لضمان التشغيل الاعتيادي لنظام الاتصالات المتنقلة الدولية–2020. فإلى جانب استخدام خوارزميات التشفير التناظرية، تم نشر الخوارزميات غير التناظرية في نظام الاتصالات المتنقلة الدولية–2020.

يثير الحاسوب الكمومي واسع النطاق مخاوف أمنية إزاء خوارزميات التشفير التناظرية وغير التناظرية الحالية على نطاق واسع. ولم تعد الخوارزميات غير التناظرية توفر الأمن في عصر الحوسبة الكمومية. علاوة على ذلك، يجب أن تضاعف خوارزميات التشفير التناظرية أطوال مفاتيحها لمقاومة هجمات الحوسبة الكمومية. ولهذا الغرض، يعد نشر خوارزميات التشفير الآمنة من حيث الحوسبة الكمومية أمراً مرغوباً للغاية في نظام الاتصالات المتنقلة الدولية–2020.

وفي هذه التوصية، يتم تناول نظام الاتصالات المتنقلة الدولية–2020 ومعماريته الأمنية باختصار. ويتم تقييم التهديدات التي تتعرض لها أنظمة الاتصالات المتنقلة الدولية–2020 بسبب أجهزة الحاسوب الكمومية. وتم استعراض الخوارزميات الآمنة من حيث الحوسبة الكمومية بإيجاز، لكن لا يتم توصيف تفاصيلها في هذه التوصية. وسيتم تضمين مبادئ توجيهية أمنية في توصية عالية المستوى لتكييف الخوارزميات الآمنة من حيث الحوسبة الكمومية مع أنظمة الاتصالات المتنقلة الدولية–2020. وتهدف هذه التوصية إلى توفير المبادئ التوجيهية لتطبيق الخوارزميات التناظرية وغير التناظرية الآمنة من حيث الحوسبة الكمومية على نظام الاتصالات المتنقلة الدولية–2020، فضلاً عن تنسيق مستويات الأمن بين الخوارزميات التناظرية وغير التناظرية الآمنة من حيث الحوسبة الكمومية.

مبادئ توجيهية تتعلق بالأمن من أجل تطبيق خوارزميات آمنة من حيث الحوسبة الكمومية في أنظمة الاتصالات المتنقلة الدولية–2020

1 مجال التطبيق

تتناول هذه التوصية:

- مقدمة للمعمارية الأمنية لأنظمة الاتصالات المتنقلة الدولية–2020 (IMT-2020)؛
- تقييماً أمنياً لأنظمة الاتصالات المتنقلة الدولية–2020 عندما تتوفر أجهزة حاسوب كمومية على المستوى التجاري؛
- مواصفة لاستعمال الخوارزميات الآمنة من حيث الحوسبة الكمومية في أنظمة الاتصالات المتنقلة الدولية–2020.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة، يرجى من جميع المستعملين لهذه التوصية السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة ما في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

[ITU-T X.800] التوصية ITU-T X.800 (1991)، *معمارية الأمن في التوصيل البيني للأنظمة المفتوحة من أجل تطبيقات اللجنة الاستشارية الدولية للبرق والهاتف.*

[ITU-T X.1038] التوصية ITU-T X.1038 (2016)، *المتطلبات الأمنية والمعمارية المرجعية للشبكات المعرّفة بالبرمجيّات.*

3 التعاريف

1.3 المصطلحات المعرَّفة في مراجع أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في مراجع أخرى:

1.1.3 الاستيقان (authentication) [b-ITU-T Y.2014]: خاصية تُحدَّد بفضلها الهوية الصحيحة لكيان ما أو طرف ما، بدرجة التأكد المطلوبة. ومن الممكن أن يكون الطرف موضوع الاستيقان أحد المستعملين أو المشتركين كما يمكن أن يكون بيئة محلية أو شبكة قائمة بالخدمة.

2.1.3 بروتوكول الاستيقان (authentication protocol) [b-ITU-T X.1254]: تسلسل محدد من الرسائل بين كيان وجهة التحقق يمكّن جهة التحقق من أجراء استيقان الكيان.

3.1.3 التخويل (authorization) [b-ISO 7498-2]: منح الحقوق بما يشمل إتاحة النفاذ استناداً إلى حقوق النفاذ.

4.1.3 التيسر (availability) [ITU-T X.800]: خاصية إمكانية النفاذ وإمكانية الاستعمال بناءً على طلب من كيان مخول.

5.1.3 أوراق الاعتماد/إثباتات (credential) [b-ITU-T X.1252]: مجموعة بيانات تقدّم كدليل على هوية و/أو استحقاقات مدّعاة.

6.1.3 السرية (confidentiality) [ITU-T X.800]: خاصية عدم إتاحة المعلومات أو الكشف عنها لأشخاص غير مخولين أو لكيانات، أو عمليات غير مُخَوَّلَة.

7.1.3 سلامة البيانات (data integrity) [ITU-T X.800]: خاصية بقاء البيانات على حالتها دون أن يطرأ عليها تغيير أو تلف بطريقة غير مرخص بها.

8.1.3 الخصوصية (privacy) [ITU-T X.800]: حق الأفراد في التحكم أو التأثير فيما يتناول المعلومات التي تتعلق بهم من حيث جمعها وتخزينها ومن يقوم بذلك ولمن يجوز إفشاء هذه المعلومات.

9.1.3 تراتبية المفاتيح (key hierarchy) [b-ITU-T X.1196]: هيكل شجري يمثل علاقة المفاتيح المختلفة. وفي أي تراتبية للمفاتيح، تمثل العقدة مفتاحاً يستخدم لاشتقاق المفاتيح التي تمثلها العقد التنازلية. ويمكن أن يكون للمفتاح سابقة واحدة فقط، ولكن قد يحتوي على عدة عقد تنازلية.

10.1.3 التمثيل الافتراضي لوظائف الشبكة (network function virtualization؛ NFV) [b-ISO/IEC TR 22417]: التكنولوجيا التي تتيح إنشاء أقسام الشبكة المعزولة منطقياً عبر الشبكات المادية المشتركة بحيث يمكن للمجموعات غير المتجانسة من الشبكات الافتراضية المتعددة أن تتعايش في نفس الوقت عبر الشبكات المشتركة.

2.3 المصطلحات المعرَّفة في هذه التوصية

لا يوجد.

4 المختصرات

تستخدم هذه التوصية المختصرات التالية:

4G الجيل الرابع *(fourth Generation)*

AES معيار تحفير متقدم *(Advanced Encryption Standard)*

AES-CBC معيار تحفير متقدم – تسلسل كتل التجفير
(Advanced Encryption Standard-Cipher Blocker Chaining)

AES-GCM معيار تحفير متقدم– أسلوب غالوا للعداد *(Advanced Encryption Standard-Galois Counter Mode)*

AES-GMAC معيار تحفير متقدم– شفرة غالوا لاستيقان الرسائل
(Advanced Encryption Standard-Galois Message Authentication Code)

AF وظيفة تطبيق *(Application Function)*

AKA اتفاق الاستيقان والمفتاح *(Authentication and Key Agreement)*

AMF وظيفة النفاذ وإدارة التنقلية *(Access and Mobility management Function)*

API السطح البيني لبرمجة التطبيقات *(Application Programming Interface)*

ARPF وظيفة مستودع إثباتات الاستيقان ومعالجتها
(Authentication credential Repository and Processing Function)

AS طبقة النفاذ *(Access Stratum)*

AUSF وظيفة مخدم الاستيقان *(Authentication Server Function)*

AV متجه الاستيقان *(Authentication Vector)*

CEK مفتاح تجفير المحتوى *(Content Encryption Key)*

CM إدارة التشكيلة *(Configuration Management)*

CP مستوى التحكم *(Control Plane)*

CU/DU وحدة مركزية/وحدة موزعة *(Central Unit/Distributed Unit)*

DH وضع ديفي–هيلمان *(Diffie-Hellman)*

DHE وضع ديفي–هيلمان السريع الزوال *(Diffie-Hellman Ephemeral)*

DNSSec تمديدات أمن نظام أسماء الميادين *(Domain Name System Security extensions)*

DSA خوارزمية التوقيع الرقمي *(Digital Signature Algorithm)*

DTLS أمن طبقة نقل وحدات البيانات *(Datagram Transport Layer Security)*

EAP بروتوكول الاستيقان القابل للتوسع *(Extensible Authentication Protocol)*

ECC تجفير المنحني الإهليلجي *(Elliptic-Curve Cryptography)*

ECDH وضع ديفي–هيلمان للمنحني الإهليلجي *(Elliptic Curve Diffie-Hellman)*

ECDHE وضع ديفي–هيلمان السريع الزوال للمنحني الإهليلجي *(Elliptic Curve Diffie-Hellman Ephemeral)*

ECDLP مشكلة اللوغاريتم المنفصل بالمنحنى الإهليلجي *(Elliptic Curve Discrete-Log Problem)*

ECDSA خوارزمية توقيع رقمي بالمنحنى الإهليلجي *(Elliptic Curve Digital Signature Algorithm)*

ECIES مخطط تجفير مدمج بمنحنى إهليلجي *(Elliptic Curve Integrated Encryption Scheme)*

ECP مستوى الثلمة الموسع *(Extended Cutting Plane)*

eMBB النطاق العريض المتنقل المعزز *(enhanced Mobile Broadband)*

ESP الحمولة النافعة الأمنية المغلِّفة *(Encapsulating Security Payload)*

FM *إدارة الأعطال (Fault Management)*

GKDF وظيفة اشتقاق المفاتيح التنوعية *(Generic Key Derivation Function)*

gNB العقدة B للتكنولوجيا الراديوية الجديدة (NR) *(NR Node B)*

GUTI معرّف هوية مؤقت فريد عالمياً *(Globally Unique Temporary Identifier)*

HMAC شفرة استيقان الرسائل القائمة على دالة الاختزال *(Hash-based Message Authentication Code)*

HKDF وظيفة اشتقاق المفاتيح بالاستخلاص والتوسيع القائمة على الشفرة HMAC *(HMAC-based Extract-and-Expand Key Derivation Function)*

ICV قيمة التحقق من السلامة *(Integrity Check Value)*

IPsec أمن بروتوكول الإنترنت *(Internet Protocol Security)*

IKE بروتوكول تبادل مفاتيح الإنترنت *(Internet Key Exchange)*

IKEv2 الإصدار 2 من بروتوكول تبادل مفاتيح الإنترنت *(Internet Key Exchange version 2)*

IMT-2020 الاتصالات المتنقلة الدولية–2020 *(International Mobile Telecommunications-2020)*

IP بروتوكول الإنترنت *(Internet Protocol)*

IPX نقطة تبادل إنترنت *(IP exchange)*

JOSE توقيع وتجفير الأشياء بلغة Javascript *(Javascript Object Signing And Encryption)*

JSON	ترميز الأشياء بلغة Javascript *(JavaScript Object Notation)*
JWE	تجفير مواقع الويب باستخدام الترميز JSON *(JSON Web Encryption)*
JWS	*توقيع مواقع الويب باستخدام الترميز JSON (JSON Web Signature)*
KDF	وظيفة اشتقاق المفاتيح *(Key Derivation Function)*
KEM	آلية تغليف المفاتيح *(Key Encapsulation Mechanism)*
LTE	*التطور طويل الأجل (Long-Term Evolution)*
LWE	التعلم من خلال الأخطاء *(Learning With Errors)*
MAC	شفرة استيقان الرسائل *(Message Authentication Code)*
mIoT	إنترنت أشياء كثيفة *(massive Internet of Things)*
mMTC	الاتصالات الكثيفة من آلة لأخرى *(massive Machine-Type Communication)*
MNO	مشغل شبكة متنقلة *(Mobile Network Operator)*
MODP	دالة أسية معيارية *(Modular exponential)*
MPLS	*تبديل الوسم متعدد البروتوكولات (Multiprotocol Label Switching)*
N3IWF	وظيفة تشغيل بيني خلاف وظائف مشروع الشراكة 3GPP *(Non-3GPP Interworking Function)*
NAS	طبقة عدم النفاذ *(Non-Access Stratum)*
NDS	أمن ميدان الشبكة *(Network Domain Security)*
NEF	وظيفة عرض شبكية *(Network Exposure Function)*
NF	وظيفة شبكية *(Network Function)*
NFV	التمثيل الافتراضي لوظائف الشبكة *(Network Function Virtualization)*
NFVI	البنية التحتية للتمثيل الافتراضي لوظائف الشبكة *(Network Function Virtualization Infrastructure)*
NG-RAN	شبكة نفاذ راديوي من الجيل التالي *(Next Generation-Radio Access Network)*
NP	زمن متعدد الحدود غير محدد *(Non-deterministic Polynomial time)*
NRF	وظيفة مستودع لوظائف الشبكة *(NF Repository Function)*
NSSF	وظيفة اختيار قسم الشبكة *(Network Slice Selection Function)*
NTRU	حلقة متعددة الحدود مشذبة من الدرجة *N (Nth degree Truncated Polynomial Ring)*
PCF	وظيفة التحكم في السياسات *(Policy Control Function)*
PDCP	بروتوكول تقارب بيانات الرزم *(Packet Data Convergence Protocol)*
PKI	*البنية التحتية للمفاتيح العمومية (Public-Key Infrastructure)*
PKE	تجفير المفاتيح العمومية *(Public-Key Encryption)*
PM	إدارة الأداء *(Performance Management)*

PRF وظيفه شبه عشوائية *(Pseudo-Random Function)*

PSK مفتاح مشترك مسبقاً *(Pre-Shared Key)*

RLC التحكم في الوصلة الراديوية *(Radio Link Control)*

R-LWE حلقة تعلم من خلال الأخطاء *(Ring Learning With Errors)*

RRC التحكم في المورد الراديوي *(Radio Resource Control)*

RSA ريفيست وشامير وأدلمان *(Rivest, Shamir and Adelman)*

PLMN شبكة متنقلة برية عمومية *(Public Land Mobile Network)*

PQC تجفير ما بعد الحوسبة الكمومية *(Post-Quantum Cryptography)*

SBA معمارية قائمة على الخدمة *(Service-Based Architecture)*

SDAP بروتوكول تكييف بيانات الخدمة *(Service Data Adaptation Protocol)*

SDN شبكة معرفة بالبرمجيات *(Software-Defined Network)*

SEAF وظيفة مركز أمني *(Security Anchor Function)*

SEPP وكيل حماية حافة الأمن *(Security Edge Protection Proxy)*

SHA خوارزمية اختزال مأمونة *(Secure Hash Algorithm)*

SIDF وظيفة إلغاء إخفاء معرف هوية الاشتراك *(Subscription Identifier De-concealing Function)*

SIDH وضع ديفي–هيلمان متساوي المنشأ فائق التفرد *(Supersingular-Isogeny Diffie–Hellman)*

SIKE تغليف المفاتيح متساوي المنشأ فائق التفرد *(Supersingular Isogeny Key Encapsulation)*

SMF وظيفة إدارة الدورة *(Session Management Function)*

SSH درع مأمون *(Secure Shell)*

SUCI معرف هوية مخفي للاشتراك *(Subscription Concealed Identifier)*

SUPI معرف هوية ثابت للاشتراك *(Subscription Permanent Identifier)*

SVP مشكلة المتجه الأقصر *(Shortest Vector Problem)*

TLS أمن طبقة النقل *(Transport Layer Security)*

TM *إدارة مسار التتبع (Trace Management)*

UDM إدارة البيانات الموحدة *(Unified Data Management)*

UDR مستودع بيانات المستعمل *(User Data Repository)*

UE معدة المستعمل *(User Equipment)*

UOV مخطط Oil and Vinegar غير المتوازن *(Unbalanced Oil and Vinegar)*

UP مستوى المستعمل *(User Plane)*

UPF وظيفة مستوى المستعمل *(User Plane Function)*

URLLC اتصالات فائقة الموثوقية ومنخفضة الكمون *(Ultra-Reliable and Low-Latency Communication)*

USIM *الوحدة النمطية لتعرّف هوية المشترك العالمية (Universal Subscriber Identity Module)*

VNF وظيفة شبكة افتراضية *(Virtual Network Function)*

WLAN شبكة محلية لاسلكية *(Wireless Local Area Network)*

XMSS مخطط ميركل الموسع للتوقيع *(extended Merkle Signature Scheme)*

5 الاصطلاحات

يتعين فهم المصطلحات الأساسية التالية في هذه التوصية على النحو التالي:

"**يجب**" تدل على متطلَّب إلزامي يجب التقيّد به بصرامة، ولا يُسمح بأي انحراف عنه في حال ادعاء الامتثال لهذه التوصية.

"**يوصى**" كلمة تدل على متطلب يوصى به لكنه غير إلزامي في المطلق. وبالتالي لا يتعين تقدم هذا المتطلب لزعم الامتثال.

"**يحظر**" تدل على متطلب إلزامي يجب التقيد به بصرامة ولا يسمح بأي انحراف عنه في حال زعم الامتثال لهذه التوصية.

"**من الجائز**" تدل على متطلب اختياري مسموح به دون أن ينطوي على أي توصية به. ولا يرمي هذا المصطلح إلى إلزام تطبيق البائع بتقديم هذا الخيار الذي يمكن أن يقدمه مشغل الشبكة/مورد الخدمة اختيارياً. وبالأحرى، فإن البائع يمكنه إدراج هذه الخاصية اختيارياً ويدعى إلى الامتثال لهذه المواصفة في نفس الوقت.

6 نظرة عامة

تم تطوير تكنولوجيا الاتصالات المتنقلة الدولية–2020 لتلبية احتياجات الأعمال لعام 2020 وما بعده. وتعد المعمارية الأمنية أساسية لتمكين التشغيل العادي لأي شبكة من شبكات الاتصالات المتنقلة الدولية–2020. وفي الجيل الرابع/التطور طويل الأجل (4G/LTE)، تُستخدم الخوارزميات المتناظرة فقط لحماية التشوير وبيانات المستعمل. وبالإضافة إلى ذلك، تقدم أنظمة الاتصالات المتنقلة الدولية–2020 خوارزميات غير متناظرة لحماية ليس فقط معرفات هوية المشتركين، ولكن أيضاً لحماية الاتصالات بين مشغلي الشبكات المتنقلة (MNO).

وفي الآونة الأخيرة (في سبتمبر 2020)، أعلنت شركة IBM عن حاسوب كمومي بسعة 50 بتة كمومية (qubit) [b-QC1]. أدى هذا الاختراق إلى تبديد التوقع الأصلي بأن أجهزة الحاسوب الكمومية واسعة النطاق ستطرح في السوق خلال 20 عاماً. ويقدر التقرير الجديد [b-QC2] الآن أن 10 سنوات هي مدة واقعية لتوافرها.

ويعتمد أمن خوارزميات تجفير المفاتيح العمومية على صعوبة المشكلات الحسابية، مثل تحليل العوامل الصحيحة أو مشكلة اللوغاريتم المنفصل عبر مجموعات مختلفة. تم إثبات أن أجهزة الحاسوب الكمومية يمكنها حل كل من هذه المشكلات بكفاءة [b-Shor 1997]، مما يجعل جميع أنظمة تجفير المفاتيح العمومية القائمة على مثل هذه الافتراضات عاجزة. وبالتالي، فإن الحاسوب الكمومي القوي بما فيه الكفاية سيعرض للخطر العديد من أشكال أنظمة التجفير الحديثة، مثل تبادل المفاتيح والتجفير والاستيقان الرقمي.

وستؤثر أجهزة الحاسوب الكمومية على القوة الأمنية للخوارزميات المتناظرة وغير المتناظرة بدرجة مختلفة. حيث ستنخفض قوة التجفير المتناظر إلى النصف، على سبيل المثال، معيار التجفير المتقدم (AES) بمفاتيح 128 بتة والذي يعطي قوة مقدارها 128 بتة ستنخفض إلى 64 بتة، في حين أن العديد من الخوارزميات غير المتناظرة شائعة الاستخدام، مثل ريفيست وشامير وأديلمان (RSA)، وخوارزمية التوقيع الرقمي (DSA) وتجفير المنحنى الإهليلجي (ECC)، لن توفر أي أمن.

ويهدف نظام الاتصالات المتنقلة الدولية–2020 إلى تقديم مجموعة واسعة من الخدمات بمتطلبات أداء مختلفة. ويمكن تصنيف الخدمات المقدمة في شبكات الاتصالات المتنقلة الدولية–2020 ضمن خدمات النطاق العريض المتنقل المعزز (eMBB) وإنترنت الأشياء الكثيفة (mIoT) والاتصالات فائقة الموثوقية ومنخفضة الكمون (URLLC).

ويطرح نظام الاتصالات المتنقلة الدولية–2020 عدداً من التكنولوجيات المبتكرة، مثل تقسيم وظائف الشبكة والتمثيل الافتراضي لوظائف الشبكة (NFV) والشبكة المعرفة بالبرمجيات (SDN) والمعمارية القائمة على الخدمة (SBA). وتجعل هذه التكنولوجيات نظام الاتصالات المتنقلة الدولية–2020 منصة مرنة تتيح حالات عمل جديدة وتدمج الصناعات الرأسية. ومن ناحية أخرى، تجعل هذه التكنولوجيات المعمارية الأمنية لنظام الاتصالات المتنقلة الدولية–2020 أكثر تعقيداً من الأجيال السابقة لشبكات الاتصالات المتنقلة.

وهناك رغبة عارمة في دراسة كيفية حماية الاتصالات في أنظمة الاتصالات المتنقلة الدولية–2020 باستخدام خوارزميات آمنة من حيث الحوسبة الكمومية. وذلك لأنه من المحتمل أن تصبح أجهزة الحاسوب الكمومية التجارية متاحة خلال دورة حياة أنظمة الاتصالات المتنقلة الدولية–2020. حالياً، يبلغ طول مفتاح الخوارزميات المتناظرة المحددة لأنظمة الاتصالات المتنقلة الدولية–2020 128 بتة. وقد بدأ مشروع شراكة الجيل الثالث (3GPP) للتو بند دراسة للبحث في كيفية تطبيق خوارزميات متناظرة بطول مفتاح 256 بتة على أنظمة الاتصالات المتنقلة الدولية–2020 [b-3GPP TR 33.841]. ومع ذلك، لم تكن هناك منظمة لدراسة كيفية تطبيق خوارزميات غير متناظرة آمنة من حيث الحوسبة الكمومية على أنظمة الاتصالات المتنقلة الدولية–2020 حتى الآن. ويجب إجراء بعض التكييف عند استخدام خوارزميات التجفير الآمنة من حيث الحوسبة الكمومية في أنظمة الاتصالات المتنقلة الدولية–2020، نظراً لأن لها أطوال مفتاح أكبر من تلك المستخدمة في التجفير الكلاسيكي. وعلاوة على ذلك، هناك حاجة لدراسة كيفية تعايش المفاتيح ذات الأحجام المختلفة في أنظمة الاتصالات المتنقلة الدولية–2020، نظراً لأنه من المستحيل استبدال جميع الخوارزميات الكلاسيكية بخوارزميات آمنة من حيث الحوسبة الكمومية بين عشية وضحاها. ويجب التفكير في الانتقال إلى التجفير الآمن من حيث الحوسبة الكمومية في أنظمة الاتصالات المتنقلة الدولية–2020 مبكراً، بحيث لا تصبح أي معلومات يتم اختراقها لاحقاً بواسطة تحليل التجفير الكمومي حساسة.

وفي هذه التوصية، يتم تقييم التهديدات التي تتعرض لها أنظمة الاتصالات المتنقلة الدولية–2020 بسبب أجهزة الحاسوب الكمومية. ويتم استعراض الخوارزميات الآمنة من حيث الحوسبة الكمومية بإيجاز، بيد أنه لا توصف تفاصيلها في هذه التوصية. وتوصي المبادئ التوجيهية المتعلقة بالأمن، على مستوى عالٍ، بتكييف خوارزميات آمنة من حيث الحوسبة الكمومية مع أنظمة الاتصالات المتنقلة الدولية–2020. وتقدم هذه التوصية المبادئ التوجيهية الشاملة لتطبيق الخوارزميات المتناظرة وغير المتناظرة الآمنة من حيث الحوسبة الكمومية على أنظمة الاتصالات المتنقلة الدولية–2020، فضلاً عن مواءمة مستويات الأمن بين الخوارزميات المتناظرة وغير المتناظرة الآمنة من حيث الحوسبة الكمومية.

7 مقدمة للمكونات الأمنية لأنظمة الاتصالات المتنقلة الدولية–2020

تقدم هذه الفقرة معلومات أساسية عن المكونات الأمنية لأنظمة الاتصالات المتنقلة الدولية–2020، والتي تم توصيفها في قطاع تقييس الاتصالات بالاتحاد الدولي للاتصالات (ITU-T) ومشروع شراكة الجيل الثالث (3GPP) والمعهد الأوروبي لمعايير الاتصالات (ETSI) وفريق مهام هندسة الإنترنت (IETF) وغيرها.

وينبغي أن يكون نظام الاتصالات قادراً على توفير بعض خدمات الأمن التالية لضمان أمن النظام أو نقل البيانات [ITU-T X.800]: التحكم في النفاذ (التخويل)؛ الاستيقان؛ الخصوصية؛ السرية؛ سلامة البيانات؛ عدم الرفض؛ والتيسر.

ويمكن تنفيذ خدمات الأمن باستخدام آليات تجفيرية وغير تجفيرية. وتركز هذه التوصية على الأولى، لأنها تدرس تطبيق خوارزميات التجفير الكمومية على أنظمة الاتصالات المتنقلة الدولية–2020.

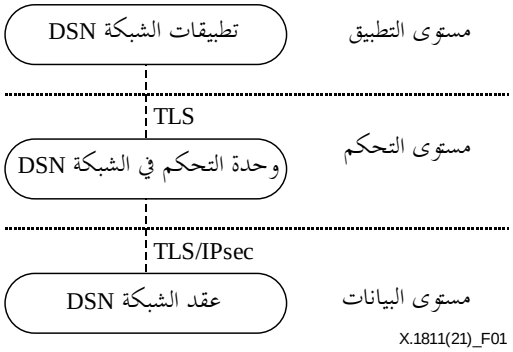
ووفقاً لمعمارية الأنظمة IMT-2020 الواردة في التذييل I، يمكن وصف المعمارية الأمنية للأنظمة IMT-2020 في ثلاث طبقات: طبقة البنية التحتية وطبقة الشبكة ومستوى الإدارة.

1.7 أمن طبقة البنية التحتية

طبقة البنية التحتية هي القاعدة المشتركة لدعم الطبقة العليا في نظام الاتصالات المتنقلة الدولية–2020، والتي تشمل الشبكة المعرفة بالبرمجيات وطبقة البنية التحتية للتمثيل الافتراضي لوظائف الشبكة (NFVI).

1.1.7 أمن الشبكة المعرفة بالبرمجيات

تستخدم تكنولوجيا الشبكات المعرفة بالبرمجيات لتوصيل البيانات في الأنظمة IMT-2020 بسبب إدارتها الدينامية والمرنة لتدفقات الحركة. ويرد توصيف معمارية أمن الشبكة المعرفة بالبرمجيات في التوصية [ITU-T X.1038]، وتوضح بالتبسيط في الشكل 1.



الشكل 1 – معمارية أمن الشبكة المعرفة بالبرمجيات

وتحدد التوصية [ITU-T X.1038] التوصيات التالية بشأن خوارزميات وبروتوكولات التجفير.

يوصى بنشر بروتوكول أمن طبقة النقل (TLS) [b-IETF RFC 5246] في السطح البيني بين تطبيق الشبكة SDN ووحدة التحكم في الشبكة SDN. واستناداً إلى البروتوكول TLS، يقوم تطبيق الشبكة SDN ووحدة التحكم في الشبكة SDN باستيقان أحدهما الآخر والاتفاق على مفتاح الدورة؛ وإلى جانب ذلك، يتم ضمان سرية البيانات وسلامة البيانات عبر السطح البيني للتحكم في التطبيق.

ويوصى بنشر البروتوكول TLS [b-IETF RFC 5246] أو بروتوكولات أمن بروتوكول الإنترنت (IPSec) ([b-IETF RFC 4301] و[b-IETF RFC 4303] و[b-IETF RFC 4835]) ووضعها في السطح البيني بين وحدة التحكم في الشبكة SDN وعقدة الشبكة SDN. واستناداً إلى البروتوكول TLS أو البروتوكول IPSec، تقوم عقدة الشبكة SDN ووحدة التحكم في الشبكة SDN باستيقان بعضهما البعض والاتفاق على مفتاح الدورة؛ وإلى جانب ذلك، يتم ضمان سرية البيانات وسلامة البيانات عبر السطح البيني للتحكم في التطبيق.

ويمكن أن تستند آليات الاستيقان إلى مفتاح مشترك مسبقاً (PSK) [b-IETF RFC 4279] [b-IETF RFC 4306] أو شهادة [b-IETF RFC 4306] و[b-IETF RFC 5246]. ويمكن تطبيق إما المخطط RSA [b-ONF TR-511] أو خوارزميات التوقيع الرقمي في الاستيقان القائم على الشهادة. ويمكن تنفيذ بروتوكول تبادل المفاتيح ديفي–هيلمان (DH) أو ديفي–هيلمان السريع الزوال (ECDH) في سياق TLS أو IPsec للاتفاق على المفتاح المشترك بين الكيانين.

ويمكن أن تكون خوارزميات التجفير المستخدمة لتجفير البيانات AES [b-NIST FIPS 197] أو Blowfish [b-Schneier] أو 3DES [b-NIST SP 800-67]. ويمكن أن تكون خوارزميات التجفير المستخدمة لآليات سلامة البيانات عبارة عن شفرة استيقان الرسائل (MAC) [b-IETF RFC 2104]، أو شفرة استيقان الرسائل القائمة على دالة الاختزال (HMAC) [b-IETF RFC 2104] أو التوقيع الرقمي [b-NIST FIPS 186-4].

2.1.7 أمن طبقة البنية التحتية للتمثيل الافتراضي لوظائف الشبكة (NFVI)

تدعم طبقة البنية التحتية للتمثيل الافتراضي لوظائف الشبكة تشغيل وظائف الشبكة الافتراضية (VNF)، والتي يتم تصوير هيكلها في الشكل 2.

الشكل 2 – هيكل البنية التحتية للتمثيل الافتراضي لوظائف الشبكة
(مكيفة من الشكل 1 بالمعيار [b-ETSI GS NFV 002])

وفقاً للمعيار [b-ETSI GS NFV-SEC 012]، يجب أن تدعم البنية التحتية للتمثيل الافتراضي لوظائف الشبكة وظائف الأمن التالية لضمان أمن وظائف الشبكة الافتراضية التي تعمل فوقها: تسجيل مأمون للحركة؛ والنفاذ إلى مستوى نظام التشغيل والتحكم في الحصر؛ والضوابط وأجهزة الإنذار المادية؛ وضوابط الاستيقان؛ وضوابط النفاذ؛ وأمن الاتصالات؛ الشهادة؛ أقسام تنفيذ بوساطة العتاد؛ وجذر الثقة القائم على العتاد؛ والتخزين ذاتي التجفير؛ والنفاذ المباشر إلى الذاكرة؛ ووحدات أمن العتاد النمطية؛ وحماية سلامة البرمجيات والتحقق منها. ولهذا الغرض، يجب أن تنفذ البنية التحتية NFVI خوارزميات التجفير التالية [b-ETSI GS NFV-SEC 012]:

1) خوارزميات دالة الاختزال: SHA-256، SHA-384، AES128-GMAC، HMAC-SHA128، HMAC-SHA256، HMAC-SHA384؛

2) خوارزميات التجفير: AES-CBC-128، AES-GCM-128 (قيمة التحقق من السلامة (ICV) 16 أثمونًا)، AES-CBC-256، AES-GCM-256 (قيمة التحقق من السلامة (ICV) 16 أثمونًا)؛

3) التوقيع: RSA 2048، RSA 3072، RSA 4096، ECDSA-256 (secp256r1)، ECDSA-384 (secp384r1)؛

4) البنية التحتية للمفاتيح العمومية (PKI): RSA 2048، RSA 3072، RSA 4096، id-ecPublicKey (secp256r1)؛

5) تبادل المفاتيح: مجموعة DH 14 (دالة أسية معيارية (MODP)، 2 048 بتة)، مجموعة DH 19 (مجموعة مستوى الثلمة الموسع (ECP)، 256 بتة)، مجموعة DH 20 (مجموعة ECP عشوائية، 384 بتة)، وضع ديفي–هيلمان السريع الزوال للمنحني الإهليلجي (ECDHE)، secp256r1 (P-256)، مجموعات وضع ديفي–هيلمان السريع الزوال (DHE) التي لا تقل عن 2048 بتة؛

6) الوظيفة شبه العشوائية (PRF): PRF-HMAC-SHA2-256، PRF-HMAC-SHA2-384.

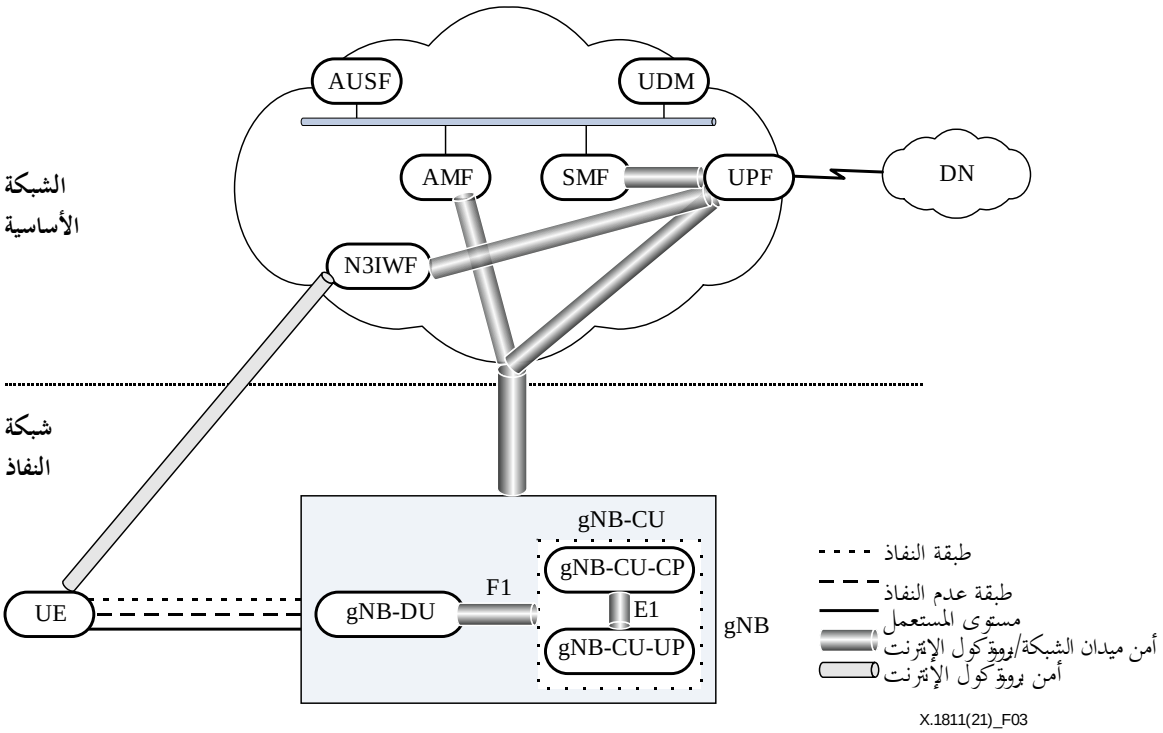
2.7 أمن طبقة الشبكة

1.2.7 أمن شبكة النفاذ

يهدف أمن شبكة النفاذ [b-3GPP TS 33.501] إلى التأكد من أن معدة المستعمل (UE) المستيقن منها قادرة على النفاذ إلى شبكة الاتصالات المتنقلة الدولية–2020، ويمكن حماية الاتصالات بين معدة المستعمل وشبكة الاتصالات المتنقلة الدولية–2020 بطريقة قابلة للاختيار وفقاً لسياسة أمن المشغل MNO.

ويوضح الشكل 3 المعمارية المنية لشبكة نفاذ الاتصالات المتنقلة الدولية–2020، والتي يمكن تحديدها على النحو التالي. تحاول المعدة UE التمكن من النفاذ إلى شبكة بهوية مخصصة مؤقتاً أو هوية دائمة مخفية قبل استخدام بروتوكول اتفاق الاستيقان والمفتاح (AKA). وتقوم معدة المستعمل والشبكة بالاستيقان المتبادل والاتفاق على مفتاح للدورة عن طريق تشغيل البروتوكول AKA. وتستخرج معدة المستعمل والشبكة مجموعة من المفاتيح بناءً على مفتاح الدورة. واستناداً إلى هذه المفاتيح، فإن سلامة وحماية الرد على رسائل تشوير طبقة عدم النفاذ (NAS) المتبادلة بين معدة المستعمل ووظيفة إدارة النفاذ والتنقلية (AMF) تكون إلزامية، في حين أن حماية سريتها تكون اختيارية؛ وتعد سلامة وحماية الرد على رسائل تشوير طبقة النفاذ (AS) المتبادلة بين UEالمعدة والعقدة NR Node B (gNB) إلزامية، بينما حماية السرية اختيارية. وتعتبر حماية سرية وسلامة بيانات المستعمل في مستوى المستعمل (UP) بين المعدة UE والعقدة gNB اختيارية. وتتم حماية الاتصالات بين المعدة UE ووظيفة التشغيل البيني خلاف وظائف مشروع الشراكة 3GPP (N3IWF) باستخدام مسير IPsec في حالة النفاذ خلاف وظائف مشروع الشراكة 3GPP. ونظراً لأنه يمكن نشر الوحدتين gNB-DU وgNB-CU في مواقع مختلفة، فإن السطح البيني F1 بينهما تتم حمايته بتطبيق أمن ميدان الشبكة/بروتوكول الإنترنت (NDS/IP). وبالمثل، يتم تأمين سطح بيني E1 بين gNB-CU-CP وgNB-CU-UP على أساس أمن NDS/IP. وتتم حماية شبكة التوصيل المباشر التي توصل العقدة gNB بشبكة أساسية باستخدام NDS/IP، ما لم تكن هناك حماية مادية في شبكة التوصيل المباشر. وحيث إنه يمكن نشر وظيفة مستوى المستعمل (UPF) على حافة الشبكة، يتم أيضاً تأمين الاتصالات بين الوظيفة UPF ووظيفة إدارة الدورة (SMF) باستخدام NDS/IP. وفيما يتعلق بالمعمارية الأمنية لشبكة النفاذ، يتم التطرق بشكل موجز إلى الخدمات أو الوظائف الأمنية التالية:

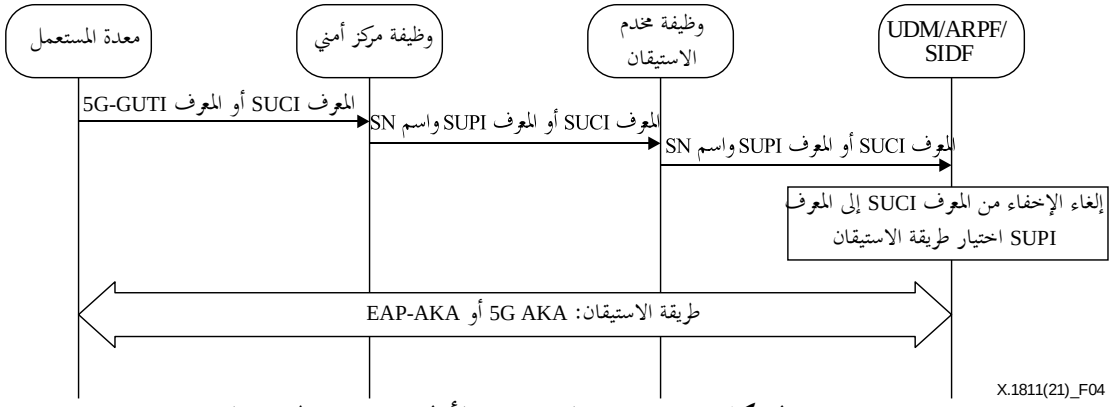
- خصوصية المشترك؛
- الاستيقان؛
- تراتب المفاتيح؛
- أمن تشوير طبقة عدم النفاذ، وأمن تشوير طبقة النفاذ، وأمن بيانات المستعمل؛
- أمن ميدان الشبكة/بروتوكول الإنترنت (NDS/IP)؛
- أمن النفاذ خلاف وظائف مشروع الشراكة 3GPP.



الشكل 3 – المعمارية الأمنية لشبكة النفاذ

1.1.2.7 خصوصية المشترك

يخصص للمعدة UE معرف هوية ثابت للاشتراك (SUPI) فريد عالمياً في نظام الاتصالات المتنقلة الدولية–2020، والذي يتم توفيره في الوحدة النمطية لتعرّف هوية المشترك العالمية (USIM) وإدارة البيانات الموحدة/مستودع بيانات المستعمل (UDM/UDR). ولا يتم نقل المعرف SUPI أبداً في وضع واضح عبر السطح البيني الراديوي عند نشر وحدة نمطية USIM في شبكة الاتصالات المتنقلة الدولية–2020. ومن أجل النفاذ الأولي، تنشئ الوحدة UE معرف هوية مخفي للاشتراك (SUCI)، وترسله إلى إدارة البيانات الموحدة/وظيفة مستودع إثباتات الاستيقان ومعالجتها (ARPF/UDM)، كما هو موضح في الشكل 4. وعند استلام معرف SUCI، تقوم وظيفة إلغاء إخفاء معرف هوية الاشتراك (SIDF) الموجودة في ARPF/UDM بإلغاء إخفاء المعرف SUPI من المعرف SUCI. وبناءً على المعرف SUPI، تختار UDM/ARPF طريقة الاستيقان وفقاً لبيانات الاشتراك.



الشكل 4 – إجراء الاستيقان الأولي واختيار طريقة الاستيقان
(مأخوذ بتصرف من الشكل 1-2.1.6 من المعيار [b-3GPP TS 33.501])

ويتكون المعرف SUCI من جزء واضح وجزء مجفر. الأول يحتوي على الرمز الدليلي القُطري للاتصالات المتنقلة والرمز الدليلي للشبكة المتنقلة كمعلومات تتعلق بالشبكة المنزلية لتوجيه المعرف SUCI إلى الوظيفة UDM/ARPF المستهدفة. ويحتوي الأخير على معلومات الاشتراك الحساسة، أي رقم تعرف هوية الاشتراك المتنقل، والذي يتم تجفيره باستخدام مخطط تجفير مدمج بمنحنى إهليلجي (ECIES). ويتم توفير المفتاح العمومي للشبكة المنزلية بشكل آمن في الوحدة USIM والوظيفة SIDF، على التوالي.

ويتمثل مبدأ المخطط ECIES في أن المعدة UE والشبكة يطبقان مفتاحهما الخاص والمفتاح العمومي للشريك للاتفاق على المفاتيح المشتركة باستخدام آلية ECDH. واستناداً إلى المفاتيح المشتركة، يتم تحقيق سرية البيانات وحماية سلامتها باستخدام خوارزميات التجفير المتناظرة وخوارزميات MAC، على التوالي. ووفقاً للمواصفات المحددة في المعيار [b-3GPP TS 33.501]، تُستخدم آليات ECDH (X25519، الصيغة الأولية لمخطط ديفي هيلمان للعامل المشترك للمنحنى الإهليلجي) لإنشاء المفاتيح المشتركة، ويتم استخدام AES-128 في وأسلوب العداد وHMAC-SHA-256 لسرية البيانات وسلامة البيانات، على التوالي.

وبعد الشروع في إجراء الاستيقان، يتم تخصيص معرف هوية مؤقت فريد عالمياً لنظام الاتصالات المتنقلة الدولية–2020 (5G-GUTI) للمعدة UE بشكل آمن لإخفاء المعرف SUPI في إجراء الاستيقان التالي.

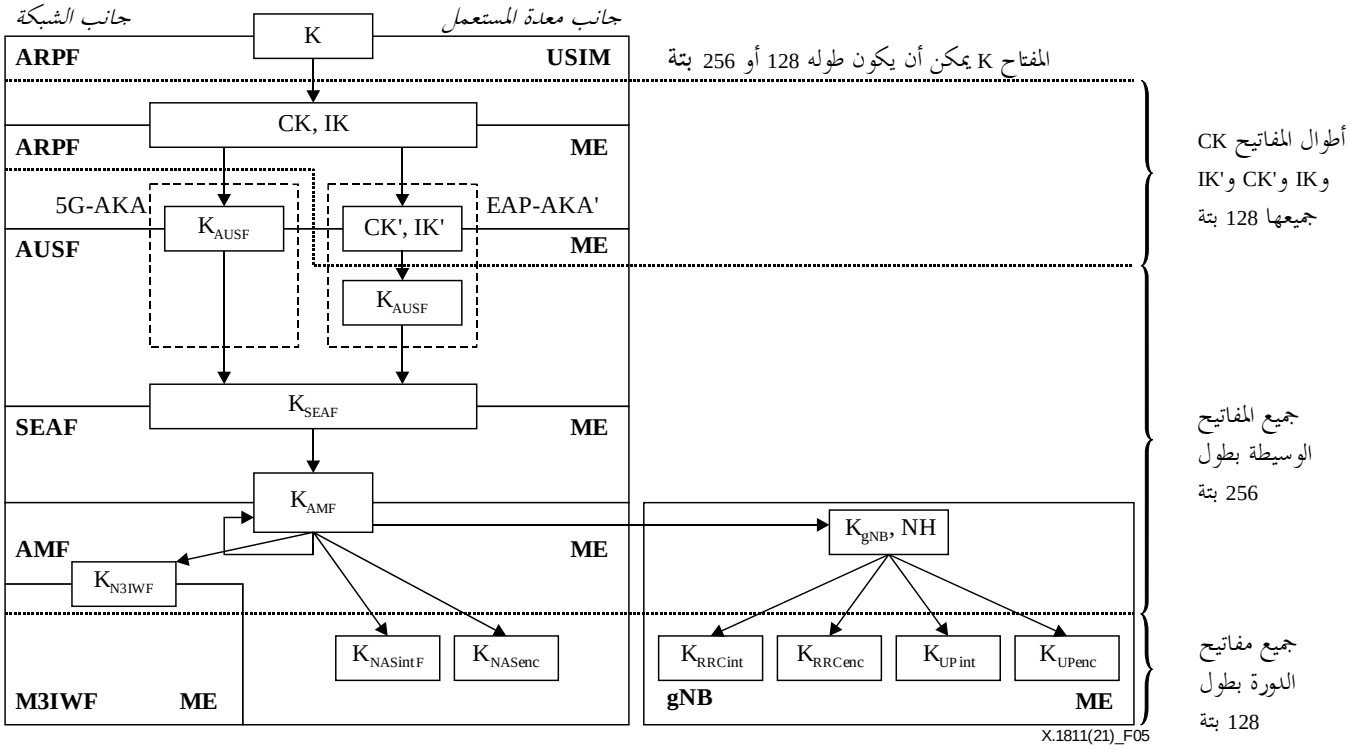
2.1.2.7 الاستيقان

يطبق نظام الاتصالات المتنقلة الدولية–2020 نوعين من البروتوكولات AKA للاستيقان المتبادل بين المعدة UE والشبكة بالإضافة إلى إنشاء مفتاح الدورة KSEAF، وهما 5G-AKA وبروتوكول الاستيقان القابل للتوسع – اتفاق الاستيقان والمفتاح ('EAP-AKA). ويمكن استخدام الأخير للنفاذ بوظائف مشروع الشراكة 3GPP وبخلاف هذه الوظائف. بالمقارنة مع بوتوكولات الجيل الرابع، توفر بروتوكولات استيقان الاتصالات المتنقلة الدولية–2020 تحكماً منزلياً أكبر لتخفيف رسوم الاحتيال المحتملة من شبكة التجوال. وفي حالة 'EAP-AKA، يتم تنفيذ التحقق من هوية معدة المستعمل على جانب الشبكة في وظيفة مخدم الاستيقان (AUSF) للشبكة المنزلية. وفي حالة 5G-AKA، فعلى الرغم من إجراء التحقق من هوية المعدة UE على جانب الشبكة عند وظيفة المركز الأمني (SEAF) لشبكة التجوال، فإن الوظيفة AUSF للشبكة المنزلية سوف تتحقق الاستيقان أثناء كل إجراء للاستيقان.

ويتم استخدام مجموعة من خوارزميات إنشاء المفاتيح (*f1* و*f1* و*f2* و*f3* و*f4* و*f5* و*f5) في إجراء الاستيقان لإنشاء متجه الاستيقان (AV) والرد على الاستيقان. وهناك نوعان من مجموعات الخوارزميات المتاحة لهذا الغرض. واحد يسمى مجموعة الخوارزمية MILENAGE [b-ETSI 135205]، حيث يوصى باستخدام AES-128 كقاعدة. والآخر يسمى مجموعة خوارزمية TUAK [b-ETSI 135231]، حيث يتم استخدام الوظيفة Keccak sponge [b- Bertoni] كقاعدة، حيث يمكن أن يكون حجم مفتاح الدخل الخاص بها إما 128 أو 256 بتة. ويلاحظ أنه من الناحية العملية، يتم نشر مجموعة خوارزمية MILENAGE على نطاق أوسع مقارنة بالمجموعة TUAK.

3.1.2.7 تراتب المفاتيح

استناداً إلى المفتاح الجذري K تجري المعدة UE والشبكة الاستيقان المتبادل وإنشاء مفتاح الدورة K_{SEAF}، وهو مركز المفاتيح (K_{N3IWF} وK_{NASint} وK_{NASenc} وK_{RRCint} وK_{RRCenc} وK_{UPint} وK_{UPenc}) المستخدمة لتأمين الاتصالات بين المعدة UE والشبكة، كما هو موضح في الشكل 5.



الشكل 5 – تراتب المفاتيح (مأخوذ بتصرف من الشكل 6.2.1-1 من المعيار [b-3GPP TS 33.501])

يمكن أن يكون طول المفتاح الجذري K إما 128 بتة أو 256 بتة. ومن الجدير بالذكر أن المفتاح الجذري K في الوحدة USIM التقليدية يبلغ طوله 128 بتة فقط، مما يعني أنه يتم توفير مفاتيح جذرية بطول 128 بتة فقط في إدارة البيانات الموحدة للوحدة USIM المقابلة.

المفاتيح CK وIK وCK' وIK' هي المفاتيح المتعلقة بإجراء الاستيقان والتي يبلغ طولها 128 بتة. ويعتمد إنشاء المفتاحين CK وIK على مجموعة الخوارزمية MILENAGE أو مجموعة الخوارزمية TUAK، بينما تُستخدم وظيفة اشتقاق المفاتيح التنوعية (GKDF) المعرفة في المعيار [b-3GPP TS 33.220] لإنتاج المفتاحين CK' وIK'.

يبلغ طول جميع المفاتيح الوسيطة 256 بتة، ويعتمد إنشاؤها على الوظيفة GKDF باستثناء المفتاح K_{AUSF} في البروتوكول EAP-AKA'. وتستخدم وظيفة اشتقاق المفاتيح بالاستخلاص والتوسيع القائمة على الشفرة HMAC (HKDF) الموصفة في المعيار [b-IETF RFC 5869] لإنشاء المفتاح K_{AUSF} في البروتوكول EAP-AKA'.

ويبلغ طول المفاتيح (K_{N3IWF} وK_{NASint} وK_{NASenc} وK_{RRCint} وK_{RRCenc} وK_{UPint} وK_{UPenc}) المستخدمة لتأمين الاتصالات بين المعدة UE والشبكة 128 بتة، حيث يتم اقتطاعها من خرج الوظيفة GKDF البالغ طوله 256 بتة.

4.1.2.7 أمن تشوير طبقة عدم النفاذ، وتشوير طبقة النفاذ، وبيانات المستعمل

لضمان سرية تشوير طبقة عدم النفاذ، وتشوير طبقة النفاذ، وبيانات المستعمل يجب أن يدعم نظام الاتصالات المتنقلة الدولية–2020 الخوارزمية SNOW القائمة على الجيل الثالث بطول 128 بتة (128-NEA1) وخوارزمية قائمة على المعيار AES بطول 128 بتة (128-NEA2). وبالإضافة إلى ذلك، يمكن دعم خوارزمية قائمة على ZUC بطول 128 بتة في نظام الاتصالات المتنقلة الدولية–2020.

ولضمان سلامة تشوير طبقة عدم النفاذ، وتشوير طبقة النفاذ، وبيانات المستعمل، يجب أن يدعم نظام الاتصالات المتنقلة الدولية–2020 الخوارزمية SNOW القائمة على الجيل الثالث بطول 128 بتة (128-NEA1) وخوارزمية قائمة على المعيار AES بطول 128 بتة (128-NEA2). وبالإضافة إلى ذلك، يمكن دعم خوارزمية قائمة على ZUC بطول 128 بتة في نظام الاتصالات المتنقلة الدولية–2020.

5.1.2.7 أمن ميدان الشبكة/بروتوكول الإنترنت

السطوح البينية بين شبكة النفاذ والشبكة الأساسية (أي السطح البيني N2 بين gNB وAMF، والسطح البيني N2 بين N3IWF وAMF، والسطح البيني N3 بين gNB وUPF، والسطح البيني N3 بين N3IWF وUPF)، والسطوح البينية بين gNB-DU وgNB-CU (السطح البيني F1)، والسطوح البينية بين gNB-CU-CP وgNB-CU-UP (السطح البيني E1) محمية عن طريق تطبيق أمن ميدان الشبكة/بروتوكول الإنترنت [b-3GPP TS 33.210]، و[b-3GPP TS 33.310]، الذي يحدد المواصفة الأمنية المستخدمة في أنظمة مشروع الشراكة 3GPP من أجل أمن بروتوكول الإنترنت، والإصدار 2 من بروتوكول تبادل مفاتيح الإنترنت (IKEv2)، وأمن طبقة نقل وحدات البيانات (DTLS) [b-IETF RFC 6083].

ولحماية سلامة وسرية البيانات المنقولة عبر السطح البيني N2 والسطح البيني E1 والسطح البيني F1، بالإضافة إلى منع هجمات إعادة التشغيل، يوصى بالتنفيذ باستخدام الاستيقان القائم على شهادة أمن بروتوكول الإنترنت والحمولة النافعة الأمنية المغلِّفة (ESP) والإصدار 2 من بروتوكول تبادل مفاتيح الإنترنت. وبالإضافة إلى ذلك، يجب دعم أمن طبقة نقل وحدات البيانات.

ولتوفير السلامة والسرية وحماية الرد للحركة عبر السطح البيني N3، يوصى بالتنفيذ باستخدام الاستيقان القائم على شهادة أمن بروتوكول الإنترنت والحمولة النافعة الأمنية المغلِّفة (ESP) والإصدار 2 من بروتوكول تبادل مفاتيح الإنترنت.

وكخوارزميات تجفير ESP، يجب دعم معيار التجفير المتقدم–تسلسل كتل التجفير (AES-CBC) معيار التجفير المتقدم–أسلوب غالوا للعداد (AES-GCM) مع قيمة ICV تساوي 16 أثمونًا، بالإضافة إلى AES-256. كخوارزميات استيقان ESP، يجب دعم HMAC-SHA1-96 ومعيار التجفير المتقدم– شفرة غالوا لاستيقان الرسائل (AES-GMAC) مع AES-128.

وفيما يتعلق بالإصدار 2 من بروتوكول تبادل مفاتيح الإنترنت، ينبغي دعم الخوارزميات التالية:

- السرية: ENCR_AES_CBC بمفتاح طوله 128 بتة، وAES-GCM بقيمة ICV تساوي 16 أثمونًا مع مفتاح طوله 128 بتة؛
- الوظيفة شبه العشوائية: PRF_HMAC_SHA1, PRF_HMAC_SHA2_256؛
- السلامة: AUTH_HMAC_SHA256_128؛
- المجموعة DH 14 (دالة MODP، 2 048 بتة)، والمجموعة DH 19 (مجموعة ECP عشوائية، 256 بتة)؛

وفيما يتعلق بالإصدار 2 من بروتوكول تبادل مفاتيح الإنترنت، لتحقيق مستوى مرتفع من الأمن، ينبغي دعم الخوارزميات التالية:

- السرية: AES-GCM بقيمة ICV تساوي 16 أثمونًا مع مفتاح طوله 256 بتة؛
- الوظيفة شبه العشوائية: PRF_HMAC_SHA2_384؛
- المجموعة DH 20 (مجموعة ECP عشوائية، 384 بتة).

ويتقاسم الأمن DTLS 1.2 نفس متواليات التجفير للأمن TLS 1.2. وحيث إن الأمن DTLS 1.2 على النحو الموصف في [b-IETF RFC 6347] يستند إلى TSL 1.2، يجب اتباع متواليات التجفير المسموح بها والإلزامية الواردة في TLS 1.2 [b-IETF RFC 6347]. وإلى جانب ذلك، من الإلزامي دعم متواليات التجفير التالية ويوصى باستخدامها:

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256، على النحو المعرف في [b-IETF RFC 5289]؛
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256، على النحو المعرف في [b-IETF RFC 5288].

ولمستوى عال من الأمن، يوصى بدعم متواليات التجفير التالية:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384، على النحو المعرف في [b-IETF RFC 5289]؛
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384، على النحو المعرف في [b-IETF RFC 5288].

وفيما يتعلق بالمجموعات DH، فإنه بالنسبة للوضع ECDHE، يجب دعم المنحنى (P-256) secp256r1 كما هو معرف في [b-IETF RFC 4492]؛ وينبغي دعم (P-384) secp256r1 كما هو معرف في [b-IETF RFC 4492]. وبالنسبة للوضع DHE، ينبغي دعم مجموعات DH بحجم 4 096 بتة على الأقل؛ ويجب عدم دعم المجموعات DH الصغر من 2 048 بتة.

ويسمح باستخدام الاستيقان القائم على المفتاح PSK في التعارف بين الإصدار IKEv2 والأمن TLS في سياق أمن ميدان الشبكة/ بروتوكول الإنترنت.

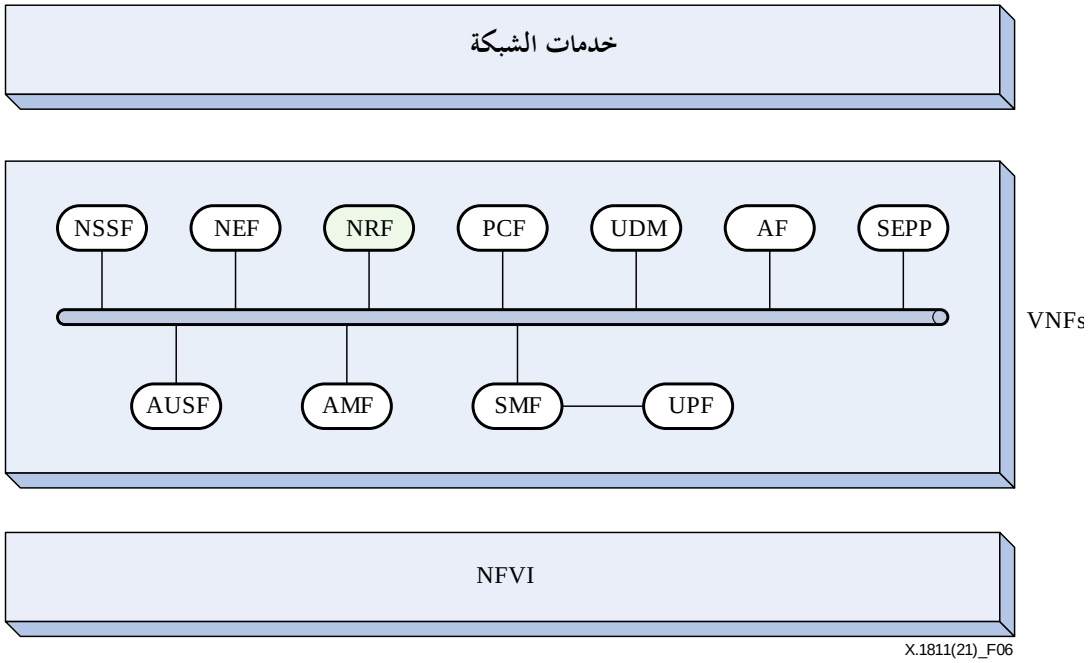
6.1.2.7 أمن النفاذ خلاف مشروع الشراكة 3GPP

يتحقق أمن النفاذ خلاف مشروع الشراكة 3GPP بإنشاء مسير IPsec بين معدة المستعمل ووظيفة تشغيل بيني خلاف وظائف مشروع الشراكة 3GPP (N3IWF). ويستخدم الإصدار IKEv2 [b-IETF RFC 7296] لإجراء الاستيقان المتبادل بين معدة المستعمل والوظيفة N3IWF استناداً إلى المفتاح K_{N3IWF} من أجل إنشاء رابطة أمنية واحدة أو أكثر من IPsec ESP [b-IETF RFC 4303] للمسيرات IPsec.

ويضمن أمن الاتصالات بين الوظيفتين N3IWF وAMF (السطح البيني N2)، وكذلك بين الوظيفتين N3IWF وUPF (السطح البيني N3) باستخدام أمن ميدان الشبكة/بروتوكول الإنترنت.

2.2.7 أمن الشبكة الأساسية

من المتوقع أن يتم إنشاء شبكة الاتصالات المتنقلة الدولية–2020 الأساسية على أساس إطار التمثيل الافتراضي لوظائف الشبكة [b-ETSI GS NFV 002]، حيث يتم فصل اقتران وظائف الشبكة (NF) عن العتاد المخصص للنشر السريع للخدمة وتحسين الكفاءة التشغيلية .كما هو مبين في الشكل 6، يمكن تقسيم إطار التمثيل الافتراضي لوظائف الشبكة إلى ثلاث طبقات تسمى: NFVI؛ وVNF؛ وخدمات الشبك وتعمل الوظائف VNF فوق الطبقة NFVI المشتركة لتوفير خدمات الشبكة المطلوبة. أمن الشبكة الأساسية هو في الأساس للطبقة VNF.



الشكل 6 – إطار شبكة أساسية للاتصالات المتنقلة الدولية–2020 قائمة على التمثيل الافتراضي لوظائف الشبكة (مأخوذ بتصرف من الشكل 1 بالمعيار [b-ETSI GS NFV 002])

تنظم وظائف الشبكة الافتراضية في معمارية قائمة على الخدمة، حيث تقوم وظيفة مستودع وظائف الشبكة (NRF) بدور رئيسي في النظام. وتحدد الوظيفة NRF ما إذا كانت الوظيفة NF مخولة بالقيام باكتشاف وتسجيل وإصدار تأشيرة النفاذ للوظيفة NF. ويمكن النظر في أمن الطبقات VNF داخل شبكة الاتصالات المتنقلة البرية العمومية (PLMN) وفيما بين الشبكات PLMN، على التوالي.

1.2.2.7 داخل شبكة الاتصالات المتنقلة البرية العمومية

1) الاستيقان

يجب أن يجري الاستيقان المتبادل بين الوظيفتين NRF وNF أثناء عملية الاكتشاف والتسجيل وطلب تأشيرة النفاذ. ويمكن تحقيق ذلك باستخدام إما NDS/IP أو الأمن المادي. ويمكن إجراء الاستيقان بين الوظائف NF بنفس الطريقة.

2) التخويل

– **التخويل السكوني**

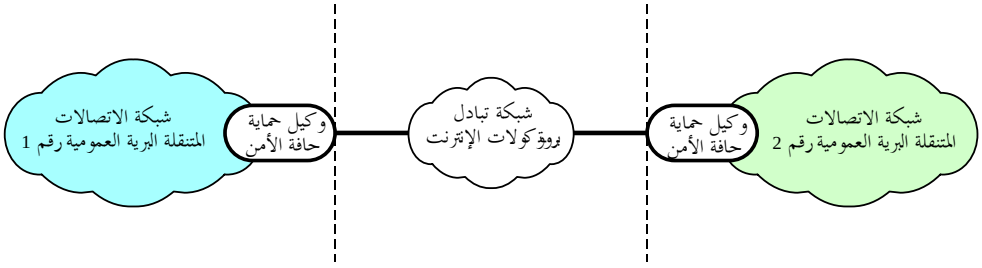
بعد استيقان الوظيفة NF لمستهلك الخدمة والوظيفة NF لمنتج الخدمة لبعضهما البعض، يجب على الوظيفة NF لمنتج الخدمة التحقق من تخويل الوظيفة NF الخاصة بمستهلك الخدمة بناءً على السياسة المحلية قبل منح النفاذ إلى السطح البيني لبرمجة التطبيق (API) الخاص بالخدمة.

– **التخويل القائم على الاستيقان OAuth 2.0**

يمكن تنفيذ التحكم في النفاذ إلى خدمات الشبكة التي توفرها الوظائف NF باستخدام إطار الاستيقان OAuth 2.0 الموصف في [b-IETF RFC 6749]. ويجب أن تكون تأشيرات النفاذ عبارة عن تأشيرات ويب بترميز الأشياء بلغة Javascript (JSON) كما هو موصوف في [b-IETF RFC 7519]، مؤمنة بالتوقيعات الرقمية أو توقيعات MAC الرقمية بناءً على توقيع الويب بالترميز JSON (JWS) كما هو موضح في [b-IETF RFC 7515]. وتعمل الوظيفة NRF كمخدم استيقان للإطار OAuth 2.0. ويقابل مستهلك خدمة الوظيفة NF ومنتج خدمة الوظيفة NF عميل الإطار OAuth 2.0 ومخدم مورد الإطار OAuth 2.0، على التوالي. وتتم حماية الاتصالات بين الوظائف NF والوظيفة NRF باستخدام أمن TLS، نظراً لنقل الإثباتات فيما بينها.

2.2.2.7 بين شبكتين PLMN

يُفعل الأمن بين شبكتين PLMN بواسطة وكيلي حماية حافة الأمن (SEPP) في الشبكتين عبر سطح بيني N32، كما هو مبين في الشكل 7.



X.1811(21)_F07

الشكل 7 – الأمن بين الشبكات PLMN

يتكون السطح البيني N32 من توصيلة N32-c وتوصيلة N32-f. فالأولى مسؤولة عن إدارة السطح البيني N32، بما في ذلك الاتفاق AKA المتبادل بين الوكيلين SEPP باستخدام أمن TLS. بينما تضمن التوصيلة الثانية إرسال الرسائل المحمية بتوقيع وتجفير الأشياء بلغة Javascript (JOSE) بين الوكيلين SEPP.

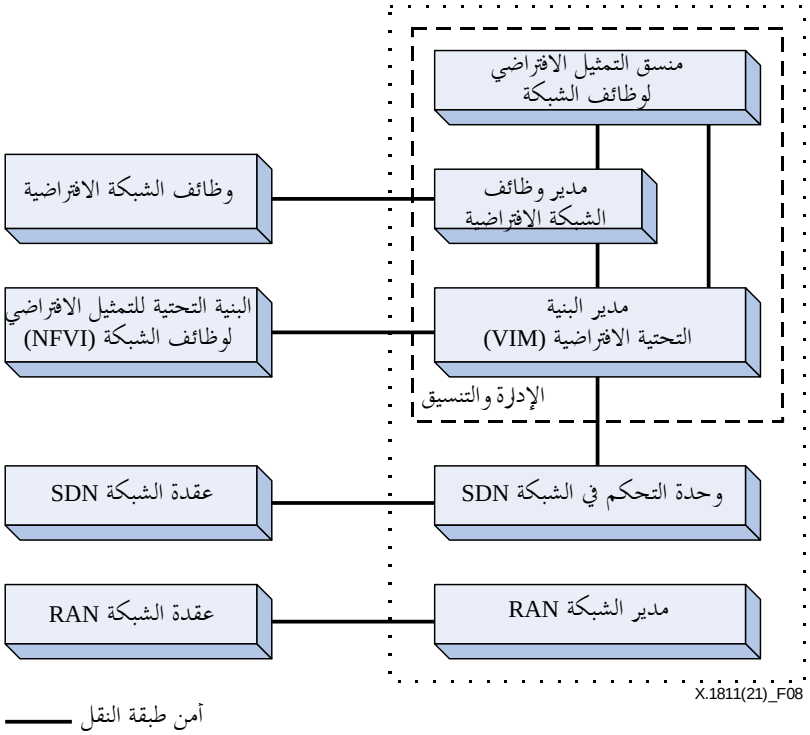
ويستخدم الوكيلان SEPP تجفير الويب JSON (JWE، الموصف في [b-IETF RFC 7516]) لحماية الرسائل على السطح البيني N32، حيث تُطبق المفاتيح المتفق عليها بين الوكيلين SEPP في التوصيلة N32-c. ويطبق موردو نقاط تبادل الإنترنت (IPX) التوقيع JWS، الموصف في [b-IETF RFC 7515]، لتوقيع التعديلات اللازمة لخدمات الوساطة الخاصة بهم.

ويجب أن تستخدم جميع الكيانات والوظائف التي تدعم التجفير JWE الخوارزميات التالية [b-3GPP-TS 33.210]: يجب دعم تجفير "enc" المعلمة A128GCM (AES-GCM) بمفتاح 128 بتة). يجب دعم تجفير "enc" المعلمة A256GCM (AES-GCM) باستخدام مفتاح 256 بتة). يجب دعم "alg" للمعلمة "dir" (الاستخدام المباشر لمفتاح متناظر مشترك كمفتاح لتجفير المحتوى (CEK)).

ويجب أن تستخدم جميع الكيانات والوظائف التي تدعم التوقيع JWS الخوارزميات التالية [b-3GPP-TS 33.210]: يجب دعم "alg" للمعلمة ES256 (خوارزمية توقيع رقمي بالمنحنى الإهليلجي (ECDSA) باستخدام P-256 وخوارزمية دالة اختزال مأمونة–256 (SHA-256)).

3.7 أمن مستوى الإدارة

يتكون مستوى الإدارة من مجموعة مدراء (منسق التمثيل الافتراضي لوظائف الشبكة، ومدير وظائف الشبكة الافتراضية، ومدير البنية التحتية الافتراضية، ووحدة التحكم في الشبكة SDN، ومدير الشبكة RAN). تتولى مجموعة المدراء هذه إدارة التشكيلة والأداء والأعطال الخاصة بالأغراض المقابلة عبر السطوح البينية. ويجب منع أي تعديل أو حذف أو إدخال أو إعادة تشغيل أثناء نقل البيانات بين المدير والغرض المدار [b-ETSI GS NFV-SEC 014]. لذا، يُطبق أمن TLS على هذه السطوح البينية آلياً في الصناعة، كما هو موضح في الشكل 8.



الشكل 8 – أمن مستوى الإدارة

4.7 ملخص لخوارزميات التجفير المستخدمة في نظام الاتصالات المتنقلة الدولية–2020

استناداً إلى مقدمة معمارية الأمن لنظام الاتصالات المتنقلة الدولية–2020 في الفقرات من 1.7 إلى 3.7، يمكن تلخيص خوارزميات التجفير المستخدمة في نظام الاتصالات المتنقلة الدولية–2020 في الجدول 1.

الجدول 1 – خوارزميات التجفير المستخدمة في نظام الاتصالات المتنقلة الدولية–2020

النوع	الاسم	الوظيفة	سيناريو التطبيق
خوارزميات التجفير المتناظرة	128-NEA1	تجفير	حماية السرية بين المعدة UE والوظيفة AMF، وكذلك بين المعدة UE والعقدة gNB
	128-NEA2		
	128-NEA3		
	128-NIA1	شفرة MAC	حماية السلامة بين المعدة UE والوظيفة AMF، وكذلك بين المعدة UE والعقدة gNB
	128-NIA2		
	128-NIA3		
	AES-128	تجفير	IPsec وTLS وDTLS وJWE وECIES وNFVI
	AES-256	تجفير	IPsec وTLS وDTLS وJWE وNFVI
	Blowfish	تجفير	SDN
	3DES	تجفير	SDN
	SHA-256	اختزال	IPsec وTLS وDTLS وJWS وNFVI
	SHA-384	اختزال	IPsec وTLS وDTLS وJWS وNFVI
	HMAC-SHA-256	اشتقاق المفاتيح/الشفرة MAC/ وظيفة شبه عشوائية	تراتب المفاتيح IPsec وTLS وDTLS وJWS وNFVI
	HMAC-SHA-384	اشتقاق المفاتيح/الشفرة MAC/ وظيفة شبه عشوائية	IPsec وTLS وDTLS وJWS وNFVI
خوارزميات التجفير غير المتناظرة	RSA	توقيع	IPsec وTLS وDTLS وJWS وNFVI
	ECDSA	توقيع	IPsec وTLS وDTLS وJWS وNFVI
	DH	اتفاق مفاتيح	IPsec وTLS وDTLS وNFVI
	ECDH	اتفاق مفاتيح	IPsec وTLS وDTLS وNFVI

الملاحظة 1 – لم تدرج الخوارزمية SHA-1 لضعف قوتها الأمنية.

الملاحظة 2 – لم يوسم حجم المفتاح لخوارزميات التجفير غير المتناظرة المستخدمة حالياً لأنه يمكن كسرها بغض النظر عن حجم المفتاح في حالة تيسر حاسوب كمومي كبير.

الملاحظة 3 – لا يقل إصدار المن TLS عن 1.2 لأسباب أمنية.

8 التقييم الأمني لأنظمة الاتصالات المتنقلة الدولية–2020 في إطار الحوسبة الكمومية

الحاسوب الكمومي هو جهاز يستغل ظواهر الميكانيكا الكمومية (التراكب والتشابك) لإجراء العمليات الحسابية ومعالجة البيانات. ويقوم الأساس الأمني لخوارزميات التشفير الشائعة حالياً على بعض المشكلات الرياضية المستعصية. ونظراً لخاصية التوازي المتأصلة للحاسوب الكمومي، يمكن لبعض الخوارزميات الكمومية أن تحل المشكلات الرياضية الصعبة بكفاءة أكبر من الخوارزميات التقليدية. ويشكل هذا الأمر تهديدات أمنية خطيرة وواقعية للتجفير المعاصر. ويسرد التذييل III تأثير الحوسبة الكمومية على خوارزميات التجفير الشائعة. وفي الفقرة 1.8، يتم تقديم التهديدات التي تتعرض لها خوارزميات التجفير التقليدية بسبب توافر أجهزة الحاسوب الكمومية. وبعد ذلك، يتم تحليل التأثيرات على أنظمة الاتصالات المتنقلة الدولية–2020 الناجمة عن أجهزة الحاسوب الكمومية.

1.8 التهديدات التي تتعرض لها خوارزميات التجفير التقليدية

1.1.8 خوارزميات التجفير غير المتناظرة

يمكن لخوارزمية Shor حل مشكلة تحليل عدد صحيح كبير ومشكلة السجل المنفصل في وقت متعدد الحدود [b-Shor 1999]. ويقوض ذلك أمن الخوارزميات غير المتناظرة الشائعة الحالية. ويعني ذلك أن تجفير المفتاح العمومي المستند إلى الخوارزمية RSA، والذي يعتمد أمنه على مشكلة تحليل عدد صحيح كبير، وبروتوكول تبادل المفاتيح DH، الذي يعتمد أمنه على مشكلة السجل المنفصل، لن يوفر أي أمن. ومثل الخوارزمية DH، يعتمد أمن الخوارزمية DSA على اللوغاريتم المنفصل. لذلك، تخضع الخوارزمية DSA لهجمات كمومية. وقد تم نشر التجفير ECC، الذي يعتمد أمنه على مشكلة اللوغاريتم المنفصل بالمنحنى الإهليلجي (ECDLP)، على نطاق واسع بسبب حجم مفاتيحها الأصغر كثيراً مقارنةً بنظام المفتاح العمومي القائم على الخوارزمية RSA. ومع ذلك، يمكن كسر الخوارزمية باستخدام متغير من خوارزمية Shor [b-Roetteler]. ويعني ذلك ضمناً أن التجفير ECC، بما في ذلك الخوارزميتين ECDSA وECDH، غير آمنتين في حال توافر أجهزة حاسوب كمومية كبيرة. ويسرد الجدول 2 الموارد الكمومية المطلوبة لكسر خوارزميات التجفير غير المتناظرة المستخدمة حالياً على نطاق واسع.

الجدول 2 – الموارد الكمومية المطلوبة لكسر خوارزميات التجفير غير المتناظرة

الخوارزمية	حجم المفتاح العمومي	مستوى الأمن مقارنة بالخوارزميات المتناظرة (بالبتات)	عدد البتات الكمومية المنطقية	عدد البتات الكمومية المادية (انظر الملاحظة 1)	بوابة Toffoli المنطقية (انظر الملاحظة 1)	الوقت اللازم لكسر الخوارزمية (انظر الملاحظة 2)
RSA [b-Häner]	1 024	80	2 050	$7{,}38 \times 10^6$	$5{,}81 \times 10^{11}$	9,68 ساعات
	2 048	112	4 098	$1{,}48 \times 10^7$	$5{,}2 \times 10^{12}$	3 أيام و14 ساعة
	4 096	128	8 194	$2{,}95 \times 10^7$	$5{,}59 \times 10^{13}$	31 يوم و21 ساعة
قائمة على التجفير ECC [Roetteler]	256	128	2 330	$8{,}39 \times 10^6$	$1{,}26 \times 10^{11}$	2,1 ساعة
	384	192	3 484	$1{,}25 \times 10^7$	$4{,}52 \times 10^{11}$	7,5 ساعات
	521	256	4 719	$1{,}69 \times 10^7$	$1{,}14 \times 10^{12}$	19 ساعة

الملاحظة 1 – تتطلب أجهزة الحاسوب الكمومية بتات كمومية مادية إضافية لتصحيح الأخطاء. ويتراوح العدد المقدر من البتات الكمومية المادية لكل بتة كمومية منطقية من 10 إلى 000 10. وهنا نفترض بتة كمومية منطقية واحدة لكل 600 3 بتة منطقية مادية، انظر [b-Fowler].

الملاحظة 2 – نفترض أن مدة تشغيل بوابة Toffoli المنطقية 60 ns، انظر [b-Banchi].

2.1.8 خوارزميات التجفير المتناظرة

توفر خوارزمية Grover تسريعاً تربيعياً للبحث في مجموعة بيانات غير منظمة في بنية محددة عبر الخوارزميات الكلاسيكية [b-Grover]. ويمكن استغلال ذلك للبحث عن المفتاح في حيز المفتاح لخوارزمية متناظرة للمفتاح. وبالنسبة لخوارزمية مفتاح متناظرة بطول n من البتات للمفتاح، يمكن العثور على المفتاح مع العمليات الكمومية $O(2^{n/2})$ على الآلة الكمومية بدلاً من $O(2^n)$ من العمليات الكلاسيكية على الحاسوب التقليدي. إن المورد الكمومي المطلوب للبحث في مفتاح الخوارزمية المتماثلة كبير جداً لدرجة أن تنفيذ خوارزمية جروفر لكسر خوارزمية المفتاح المتناظرة على حاسوب كمومي مادي فعلي أمر مشكوك فيه. فعلى سبيل المثال، يحتاج البحث الشامل عن معيار AES باستخدام خوارزمية Grover إلى الأرقام التالية من بوابات Toffoli وClifford: 2^{86} من أجل AES-128؛ و2^{118} من أجل AES-192؛ و2^{151} من أجل AES-256، على الرغم من أن عدد البتات الكمومية المنطقية المطلوبة يتراوح من 000 3 إلى 000 7 [b-Grassl].

وتقوم خوارزمية Grover بتخفيض حجم المفتاح الفعال إلى النصف، أي أنها تقلل إلى النصف قوة الأمن لخوارزمية المفتاح المتناظرة. وبالتالي لتحقيق المساعدة الكمومية، يجب مضاعفة حجم المفتاح في خوارزمية المفتاح المتناظرة.

3.1.8 خوارزميات الاختزال

لا تسرع خوارزمية Grover ومتغيرها من اكتشاف تصادمات الاختزال مقارنة بالخوارزميات الكلاسيكية [b-Bernstein 2009]. وأفضل طريقة هي استخدام نسخة متوازية من طريقة النموذج ρ لبولارد على مجموعة حواسيب كلاسيكية [b-ETSI GR QSC 006]. وهذا يعني أنه إذا كانت خوارزميات الاختزال المستخدمة حالياً آمنة، فستكون آمنة ضد هجمات الحوسبة الكمومية في العصر الكمومي. وقد ثبت أيضاً أن SHA-256 الذي تبين أنه آمن باستخدام الحوسبة الكلاسيكية قادر على مقاومة هجوم ما قبل الصورة الكمومي [b-Amy].

4.1.8 وظائف اشتقاق المفاتيح

الغرض من وظائف اشتقاق المفاتيح (KDF) هو إنشاء المفاتيح المستخدمة لحماية السرية والسلامة، وهو ما يتحقق من خلال تضمين المفتاح المشترك في دوال الاختزال. وهناك نوعان من الوظائف KDF المستخدمة في نظام الاتصالات المتنقلة الدولية–2020. الأولى هي الوظيفة GKDF الموصفة في [b-3GPP TS 33.220]، والثانية هي الوظيفة HKDF الموصفة في [b-IETF RFC 5869].

وأساس الوظيفتين GKDF وHKDF هو دالة الاختزال ذات المفاتيح HMAC-SHA-256. ويعتمد أمن الشفرة HMAC على قوة التجفير لدالة الاختزال المستخدمة [b-IETF RFC 2104]. ونتيجة لذلك، لا تتأثر الوظائف KDF المستخدمة في نظام الاتصالات المتنقلة الدولية–2020 بشكل كبير بأوجه التقدم في مجال الحوسبة الكمومية.

ويلاحظ أن إنتروبيا خرج الوظائف KDF تعتمد على إنتروبيا مفتاح الدخل المستخدم في الوظائف KDF. وبالنسبة لخرج إنتروبيا بمقدار 256 بتة، يلزم وجود مفتاح دخل إنتروبيا بمقدار 256 بتة عند تطبيق الوظائف KDF.

2.8 التنبؤ بالجدول الزمني للحاسوب الكمومي واسع النطاق

من الصعب التنبؤ بالجدول الزمني الدقيق لتوافر أجهزة الحاسوب الكمومية على نطاق واسع، لأنه لا يوجد توافق في الآراء بشأن هذه المسألة. ويقدر المعيار [b-NISTIR 8105] أن الحاسوب الكمومي الذي تبلغ تكلفته مليار دولار أمريكي قد يكسر خوارزمية RSA بطول 048 2 بتة في عام 2030. وقد توصل المعهد الأوروبي لمعايير الاتصالات (ETSI) إلى نتيجة مماثلة مفادها أن أجهزة الكمبيوتر كبيرة الحجم قد يتم بناؤها في عام 2031 [b-ETSI GR QSC 004]. ونتيجة لذلك، قد يتم اختراق أمن أنظمة الاتصالات المتنقلة الدولية–2020 لأن أنظمة الاتصالات المتنقلة الدولية–2020 ستعمل على مدار فترة تمتد من 10 إلى 20 عاماً. وعلى الجانب الآخر، ينص المعيار [b-NASEM] على أنه من غير المحتمل جداً أن يتم بناء حاسوب كمومي يكسر خوارزمية RSA بطول 048 2 بتة في العقد القادم. وهذا لا يعني ضمناً أنه لا ينبغي دراسة وتقييس خوارزميات التجفير الآمنة من حيث الحوسبة الكمومية الآن، لأن الإطار الزمني للانتقال إلى خوارزمية أمن جديدة طويل بما فيه الكفاية وغير مؤكد [b-NASEM].

3.8 التأثيرات على أنظمة الاتصالات المتنقلة الدولية–2020

كما هو موضح في الفقرة 7، تم نشر المعايير الأمنية IPsec وTLS وDTLS في العديد من الأماكن في شبكات الاتصالات المتنقلة الدولية–2020. ومن الضروري أولاً إعطاء نظرة عامة لتقييم التهديدات التي تنشأ عليها من الحواسيب الكمومية. وبعد ذلك، سيتم تقييم التأثيرات على أمن أنظمة الاتصالات المتنقلة الدولية–2020 وفقاً للهيكل المقدم في البند 7.

1.3.8 التأثيرات على المعايير الأمنية IPsec وTLS وDTLS

على الرغم من أن المعايير الأمنية IPsec وTLS وDTLS تعمل على طبقات مختلفة لحماية إرسال الرسائل (IPsec يقع في طبقة الشبكة، وTLS وDTLS يقعان بين طبقتي الشبكة والتطبيق)، فإن تصميمها يسير على مبدأ مماثل. وهي تتألف من جزأين: الأول هو الاستيقان وإنشاء المفتاح لإنشاء مفاتيح الدورة؛ والآخر هو حماية سرية وسلامة الرسائل باستخدام خوارزميات متناظرة مع مفاتيح الدورة.

وتوجد طريقتان لإجراء الاستيقان وإنشاء المفاتيح، بناءً على: (1) مفتاح متماثل مشترك مسبقاً؛ و(2) مفتاح عمومي (عادة ما يتم استخدام شهادة).

ولحماية السرية والسلامة، يمكن أن تدعم متواليات التجفير الحالية في المعايير IPsec وTLS وDTLS كلاً من الخوارزميات المتناظرة بطول 128 و256 بتة على السواء.

ونتيجة لذلك، يمكن تقييم ما إذا كان بإمكان المعايير IPsec وTLS وDTLS مقاومة هجمات الحوسبة الكمومية من خلال النظر في الحالات من 1 إلى 4.

الحالة 1: استيقان قائم على المفتاح العمومي مع خوارزميات متناظرة بطول 128 و256 بتة

في هذه الحالة، يمكن للمهاجمين استرداد مفاتيح الدورة حيث يمكن كسر الخوارزميات غير المتناظرة المحددة حالياً في معايير فريق مهام هندسة الإنترنت (IETF) بواسطة أجهزة الحاسوب الكمومية بسبب خوارزمية Shor. لذلك، فإنه بغض النظر عن طول حجم الخوارزميات المتناظرة، لا يمكن ضمان أمن الرسائل المرسلة.

الحالة 2: استيقان قائم على مفتاح PSK بطول 128 بتة مع خوارزميات متناظرة بطول 128 بتة

في هذه الحالة، ونتيجة لخوارزمية Grover، يكون حجم مفتاح الأمن الفعلي 64 بتة في حال تيسر الحاسوب الكمومي واسع النطاق. وبالتالي، فإن هذه البروتوكولات الثلاثة ليست آمنة ضد الهجوم الكمومي.

الحالة 3: استيقان قائم على مفتاح PSK بطول 256 بتة مع خوارزميات متناظرة بطول 128 بتة

في هذه الحالة، على الرغم من استخدام مفتاح PSK بطول 256 بتة للاستيقان وإنشاء المفاتيح، يتم تطبيق خوارزميات متناظرة بطول 128 بتة فقط لحماية الرسائل. وبالتالي، فإن قوة أمن هذه البروتوكولات الثلاثة هي 64 بتة.

الحالة 4: استيقان قائم على مفتاح PSK بطول 256 بتة مع خوارزميات متناظرة بطول 256 بتة

في هذه الحالة، تكون قوة الأمن الفعلية لهذه البروتوكولات الثلاثة هي 128 بتة. لذلك يمكن إحباط الهجمات الكمومية باستخدام مواصفة التجفير هذه.

والحالة 4 فقط هي الآمنة ضد الهجوم الكمومي بالنسبة لمواصفات التجفير الحالية. بيد أن الاستيقان المستند إلى المفتاح PSK يناسب فقط مجموعة اتصالات صغيرة حيث يجب تشكيل المفتاح PSK يدوياً في الأجهزة المقابلة. ويوصى بتطبيق الاستيقان القائم على المفتاح العمومي عندما تصبح مجموعة الاتصالات كبيرة. ولهذا الغرض، يوصى بإدخال خوارزميات التجفير غير المتناظرة الآمنة من حيث الحوسبة الكمومية في البروتوكولات المذكورة أعلاه (أي IPsec وTLS وDTLS) لأغراض الاستيقان.

2.3.8 التأثيرات على طبقة البنية التحتية

كما هو موضح في الفقرة 1.7، يتم استخدام البروتوكول TLS لحماية السطح البيني بين التطبيقات ووحدة التحكم في الشبكة SDN، وكذلك السطح البيني بين وحدة التحكم في الشبكة SDN وعقد الشبكة SDN. ويمكن تطبيق البروتوكول IPsec على السطح البيني بين وحدة التحكم في الشبكة SDN وعقد الشبكة SDN. واستناداً إلى التحليلات الواردة في الفقرة 1.3.8، يخضع هذان السحان البينيان لهجمات كمومية، أي يمكن للمهاجمين التنصت على الرسائل المرسلة عبر هذين السطحين البينين وتعديلها وحقنها، ما لم يتم نشر الخوارزميات المبينة في الحالة 4 في البروتوكولين TLS وIPsec.

وطبقة البنية التحتية NFVI معرضة للهجوم الكمومي لأنها تعتمد على خوارزميات التجفير غير المتناظرة الكلاسيكية لتنفيذ بعض وظائف الأمن. وقد يؤدي ذلك إلى عواقب وخيمة، مثل النفاذ غير القانوني إلى المنصة، وزرع البرمجيات الضارة.

3.3.8 التأثيرات على شبكة النفاذ

1.3.3.8 خصوصية المشترك

يتم إخفاء معرف الهوية SUPI عن طريق تحويله إلى معرف SUCI باستخدام المخطط ECIES كما هو مقدم في الفقرة 2.7. ويستخدم البروتوكول ECDH للموافقة على المفتاح المشترك بين المعدة UE والشبكة في المخطط ECIES. ويمكن للهجمات

استعادة المفتاح المشترك بسبب الخوارزمية Shor في حالة تيسر أجهزة حاسوب كمومية كبيرة الحجم. وبالتالي، يتم الكشف عن المعرف SUPI للمهاجمين عن طريق فك تجفير المعرف SUCI بالمفتاح المشترك.

2.3.3.8 الاستيقان

يقوم كل من بروتوكول الاتفاق 5G-AKA والبروتوكول 'EAP-AKA لنظام الاتصالات المتنقلة الدولية–2020 بإجراء استيقان متبادل بين المعدة UE والشبكة بناءً على المفتاح طويل المدى K، والذي قد يكون حجمه 128 أو 256 بتة. وبالنسبة إلى المفتاح K الذي يبلغ حجمه 256 بتة، حتى الآن، لم تكن هناك هجمات على دوال الاختزال (أي مجموعة الخوارزمية TUAK) التي تعد الأساس الذي يمكن من خلاله اشتقاق المعلمات المختلفة المستخدمة في بروتوكول الاستيقان باستخدام حاسوب كلاسيكي. وبالتالي، فإن كلا من بروتوكولي الاستيقان آمنان ضد الهجمات الكمومية، حيث لا توجد خوارزمية أكثر كفاءة لكسر دوال الاختزال باستخدام الحواسيب الكمومية من استخدام الحواسيب الكلاسيكية في سياق مفتاح K يبلغ حجمه 256 بتة. أما بالنسبة للمفتاح K الذي يبلغ حجمه 128 بتة، والذي تبلغ قوة أمنه الفعلية 64 بتة في العصر الكمي، يمكن للمهاجمين استعادة المفتاح K من الرسائل الملتقطة المتعلقة ببروتوكولي الاستيقان، على سبيل المثال AV، عن طريق إجراء عدد 2^{64} عملية كمومية باستخدام الخوارزمية Grover.

3.3.3.8 تراتب المفاتيح

يستخدم تراتب المفاتيح من أجل اشتقاق المفاتيح ذات الحجم 128 بتة من المفتاح K طويل الأمد (الجذر) كما هو مبين في الشكل 5، من أجل حماية الاتصالات بين المعدة UE والشبكة. وحالياً، يتم استخدام المفتاح K بالحجم 128 بتة على نطاق واسع، بينما نادراً ما يتم تطبيق المفتاح K بالحجم 256 بتة. أما بالنسبة للمفتاح K الذي يبلغ حجمه 128 بتة، والذي تبلغ قوة أمنه الفعلية 64 بتة في العصر الكمي، فإن قوة الأمن للمفاتيح المشتقة تبلغ 64 بتة. ونتيجة لذلك، يمكن للهجمات استعادة المفاتيح من هذه الرسائل الملتقطة المجفرة بمفاتيح حجمها 128 بتة.

4.3.3.8 تشوير الطبقة NAS وتشوير الطبقة AS وبيانات المستعمل

تتم حماية سرية تشوير الطبقة NAS وتشوير الطبقة AS وبيانات المستعمل باستخدام الخوارزميات المتناظرة ذات المفاتيح التي تبلغ أطوالها 128 بتة. ومن هنا، يمكن للمهاجمين فك تجفير هذه الرسائل باستخدام حواسيب كمومية.

تتم حماية سلامة تشوير الطبقة NAS وتشوير الطبقة AS وبيانات المستعمل باستخدام الخوارزميات MAC ذات المفاتيح التي تبلغ أطوالها 128 بتة. ويشذب خرج الخوارزميات MAC إلى وسم طوله 32 بتة ويستخدم كوسم للخوارزمية MAC. ومن الواضح أن بإمكان المهاجم تزوير أي رسالة بعد عدد من المحاولات يبلغ 231 محاولة إذا كان طول وسم الخوارزمية 32 بتة. وتحديد ما إذا كانت هناك مخاطر على أمن النظام IMT-2020 في حالة تشذيب وسم بطول 32 بتة للخوارزمية MAC من الوسم الأصلي البالغ طوله 64 بتة أو الوسم الأصلي البالغ طوله 128 بتة، يحتاج إلى مزيد من الدراسة.

5.3.3.8 أمن ميدان الشبكة (NDS)/بروتوكول الإنترنت (IP)

يتم نشر البروتوكولات TLS وDTLS وIPsec لحماية السطح البيني N2 والسطح البيني N3 والسطح البيني E1 والسطح البيني F1 على النحو الوارد في الفقرة 1.2.7. وينطوي هذا على نفس التأثيرات كما هو الحال مع طبقة النقل، أي أنه يمكن للمهاجمين التنصت وتغيير وحقن الرسائل المرسلة عبر هذه السطوح البينية، إذا لم يتم استخدام متواليات التجفير المدرجة في الحالة 4 من الفقرة 1.3.8.

6.3.3.8 أمن النفاذ خلاف نفاذ مشروع الشراكة 3GPP

يؤمن النفاذ خلاف نفاذ مشروع الشراكة 3GPP باستخدام البروتوكول IPsec. وللأسباب المطروحة في الفقرة 1.3.8، لا يمكن ضمان أمن النفاذ خلاف نفاذ مشروع الشراكة 3GPP، ما لم تستخدم متواليات التجفير المدرجة في الحالة 4 من الفقرة 1.3.8.

4.3.8 التأثيرات على الشبكة الأساسية

1.4.3.8 داخل شبكة PLMN

1) الاستيقان

لن يتأثر الاستيقان بين الوظائف NF إذا كان تشغيلها يعتمد على الأمن المادي. وقد يخضع الاستيقان لنفس التهديدات المحددة في الفقرة 3.3.8 إذا تم تحقيقه باستخدام أمن ميدان الشبكة (NDS)/بروتوكول الإنترنت (IP).

2) التخويل

لن يتأثر التخويل السكوني، نظراً لعدم تطبيق أي خوارزميات للتجفير.

بالنسبة للتخويل القائم على الاستيقان OAuth 2.0، هناك سيناريوهان لضمان سلامة تأشيرة النفاذ. يمكن للمهاجم تزوير تأشيرة نفاذ إذا كانت سلامتها محمية باستخدام توقيع. وفي المقابل، لا يمكن تزوير تأشيرة النفاذ إذا تم تطبيق شفرة MAC بمفتاح طوله 256 بتة لحماية سلامتها. وقد يتم الكشف عن الإثباتات المستخدمة في التخويل حيث يتم إرسالها عبر البروتوكول TLS بين الوظائف NFs، ما لم تنطبق الحالة 4 من الفقرة 1.3.8.

2.4.3.8 بين شبكتين PLMN

يمكن للمهاجمين التنصت وتعديل وحقن الرسائل المرسلة عبر السطح البيني N32 بين شبكتين PLMN. والسبب هو أن التوصيلة N32-c تعتمد على الاستيقان المستند إلى الشهادة في البروتوكول TLS لإنشاء مفاتيح الدورة، ويمكن للمهاجمين الحصول على هذه المفاتيح باستخدام الحواسيب الكمومية.

5.3.8 التأثيرات على مستوى الإدارة

من الممكن إجراء أي تعديل أو حذف أو إدراج أو إعادة تشغيل أثناء نقل البيانات بين المدير والأهداف المدارة، حيث يتم استخدام البروتوكول TLS مع الاستيقان القائم على الشهادة في مستوى الإدارة. ويمثل ذلك تهديداً خطيراً لأنظمة الاتصالات المتنقلة الدولية–2020، حيث يمكن للمهاجمين النفاذ إلى نظام إدارة شبكة الاتصالات المتنقلة الدولية–2020.

9 خوارزميات التجفير الآمنة من حيث الحوسبة الكمومية

تقدم الحوسبة الكمومية نموذجاً جديداً تماماً للحوسبة. ومن شأن ذلك أن يؤثر على أمن كل من خوارزميات المفاتيح المتناظرة (مثل شفرات الكتل) وخوارزميات المفاتيح العمومية (مثل RSA)، على الرغم من أن خطورة التأثير ستكون مختلفة لكل منهما.

ويوضح المعيار [b-Moses] أن الحوسبة الكمومية تقلل بشكل فعال عدد بتات قوة المفتاح لأي خوارزمية مفتاح متناظرة إلى النصف وأن أجهزة الحاسوب الكمومية يمكنها تشغيل الخوارزميات (على سبيل المثال، خوارزمية المعيار [b-Grover]) والعثور على مفتاح شفرة متناظرة مع مفتاح بحجم N بتة في عمليات عددها $2^{N/2}$. وبالتالي، إذا أصبحت الحوسبة الكمومية حقيقة واقعة، يمكن حماية خوارزميات المفاتيح المتناظرة من ذلك ببساطة عن طريق مضاعفة حجم المفتاح. وبالطبع، سيكون لهذا تأثير على أداء خوارزمية المفتاح المتناظرة.

وبالنسبة لخوارزميات المفاتيح غير المتناظرة، مثل RSA وDSA وECC وDH، يُعتقد أن تأثير الحوسبة الكمومية خطير للغاية. فيمكن لأجهزة الحاسوب الكمومية تشغيل الخوارزميات (على سبيل المثال، تلك الخاصة بالمعيار [b-Shor 1997]) التي تحطم جميع أنظمة المفاتيح العمومية الشائعة في فترات زمنية قصيرة للغاية. فعلى سبيل المثال، يمكن لخوارزمية كمومية تسمى خوارزمية Shor استعادة مفتاح RSA في زمن كثير الحدود [b-Moses].

ويجب اختيار خوارزميات التجفير الآمنة من حيث الحوسبة الكمومية حسب معايير التقييم (انظر التذييل IV، على سبيل المثال معايير التقييم الصادرة عن المعهد الوطني للمعايير والتكنولوجيا (NIST)).

1.9 خوارزميات المفاتيح المتناظرة الآمنة من حيث الحوسبة الكمومية

من المعتقد على نطاق واسع أن أنظمة التجفير المتناظرة الأساسية، مثل شفرات الكتل أو دالات الاختزال، آمنة من حيث الحوسبة الكمومية [b-CSA] كما هو موضح في التذييل III. ويقدم المعيار [b-ITU-T X.1197] قائمة بأمثلة للخوارزميات الآمنة من حيث الحوسبة الكمومية وأطوال المفاتيح. وسيتطلب ظهور أجهزة الحاسوب الكمومية ذات الصلة بالتجفير بشكل ملحوظ زيادة في حجم المفتاح المتناظر، مما يضاعف المفاتيح ذات الحجم البالغ 128 بتة الحالية المستخدمة في الاتصالات المتنقلة الدولية–2020. ويوضح المعيار [b-CSA] أن حجم المفتاح الحالي الموصى به والذي يبلغ 256 بتة يعتبر آمناً، حتى مقابل الخوارزمية Grover.

2.9 خوارزميات المفاتيح غير المتناظرة الآمنة من حيث الحوسبة الكمومية

على الرغم من أن أجهزة الحاسوب الكمومية يمكنها تشغيل الخوارزميات التي تكسر أنظمة المفاتيح العمومية الحالية (على سبيل المثال، RSA وECC) في فترات زمنية بالغة القصر كما هو موضح في التذييل III، فإن هناك العديد من الأصناف المهمة من أنظمة التجفير بخلاف RSA وECC الآمنة ضد أي هجوم بواسطة جهاز حاسوب كمومي، ويرد توصيفها في الفقرات من 1.2.9 إلى 5.2.9. وترد قائمة بالمعايير الحالية للخوارزميات غير المتناظرة الآمنة من حيث الحوسبة الكمومية في المعيار [b-ITU-T X.1197].

ملاحظة – توزيع المفتاح الكمومي (QKD) هو طريقة لتنفيذ اتفاق المفاتيح والتي ثبت أنها قوية ضد الحوسبة الكمومية.

1.2.9 الخوارزميات المستندة إلى الشبكة

تعتمد الخوارزميات المستندة إلى الشبكة على بعض المشكلات الصعبة المعروفة على الشبكة لبناء سابقات تجفير آمنة من حيث الحوسبة الكمومية. واحدة من هذه المشكلات هي مشكلة المتجه الأقصر (SVP)، أي العثور على أقصر متجه غير صفري في شبكة معينة، والتي ثبت أنها مشكلة غير حتمية متعددة الحدود صعبة (NP-hard) في ظل التخفيضات العشوائية [b-Ajtai].

ويوضح المعيار [b-CSA] أن الخوارزميات المستندة إلى الشبكة يمكن أن توفر توقيعاً رقمياً مع تجفير مفتاح عمومي أو خاص واتفاق مفاتيح. ويتم سرد بعض الخوارزميات القائمة على الشبكة في الفقرة 1.II.

2.2.9 الخوارزميات المستندة إلى الاختزال

تعتمد الخوارزميات المستندة إلى الاختزال على أمن دالة الاختزال التجفيرية الأساسية.

ويبين المعيار [b-CSA] أن الخوارزميات المستندة إلى الاختزال تستخدم في التوقيعات الرقمية التي تُنشأ باستخدام دوال الاختزال. وتسرد في الفقرة 2.II بعض الخوارزميات المستندة إلى الاختزال.

3.2.9 الخوارزميات المستندة إلى الشفرة

تعتمد الخوارزميات المستندة إلى الشفرة على بعض شفرات تصحيح الأخطاء، حيث يصعب فك تشفير مخططات التشفير بكفاءة، حتى بالنسبة للحاسوب الكمومي. فعلى سبيل المثال، يعتمد نظام التجفير McEliece [b-McEliece] على مشكلة NP-hard لفك تشفير أي شفرة خطية عامة.

ويوضح المعيار [b-CSA] أن الخوارزميات المستندة إلى الشفرة يمكن أن توفر توقيعاً رقمياً مع تجفير مفتاح عمومي أو خاص واتفاق مفاتيح. ويتم سرد بعض الخوارزميات القائمة على الشفرة في الفقرة 3.II.

4.2.9 الخوارزميات متعددة المتغيرات

تعتمد الخوارزميات متعددة المتغيرات على صعوبة حل أنظمة المعادلات متعددة المتغيرات غير الخطية عبر الحقول المحدودة. وتعرف هذه المشكلة باسم NP-hard [b-Garey].

ويوضح المعيار [b-CSA] أن الخوارزميات متعددة المتغيرات يمكن أن توفر توقيعاً رقمياً مع تجفير مفتاح عمومي أو خاص. ويتم سرد بعض مخططات التوقيع العملية المستندة إلى الخوارزميات متعددة المتغيرات في الفقرة 4.II.

5.2.9 الخوارزميات فائقة التفرد القائمة على تساوي المنشأ

تُبنى الخوارزميات فائقة التفرد القائمة على تساوي المنشأ على أساس صعوبة استرجاع منشأ متساو مجهول بين زوج من المنحنيات الإهليلجية فائقة التفرد المعروف أنها متساوية المنشأ.

وهي توفر أمناً مثالياً في الاتجاه المباشر، وتعمل كبديل مباشر مقاوم للحوسبة الكمومية لطريقتي DH وECDH. ومن الأمثلة النموذجية خوارزمية وضع ديفي–هيلمان متساوي المنشأ فائق التفرد (SIDH) [b-Jao].

10 مبادئ توجيهية لاستخدام خوارزميات التجفير الآمنة من حيث الحوسبة الكمومية في أنظمة الاتصالات المتنقلة الدولية–2020

يولى اعتبار عام أولاً للتعامل مع الزيادة الكبيرة في حجم الرسالة عندما يتم إدخال خوارزميات غير متناظرة آمنة من حيث الحوسبة الكمومية في أنظمة الاتصالات المتنقلة الدولية–2020. ثم يتم أخذ استخدام خوارزميات التجفير الآمنة من حيث الحوسبة الكمومية في البروتوكولات IPsec وTLS وDTLS في الاعتبار، حيث تم نشرها في أكثر من موضع في أنظمة الاتصالات المتنقلة الدولية–2020. ثم يتم تحديد مبادئ توجيهية لتطبيق خوارزميات التجفير الآمنة من حيث الحوسبة الكمومية على شبكة نفاذ من الاتصالات المتنقلة الدولية–2020 وشبكة أساسية من الاتصالات المتنقلة الدولية–2020، على التوالي.

1.10 حجم الرسالة

ستتم زيادة حجم الرسائل التي تحتوي على مفتاح عمومي أو نص مشفر أو توقيع بشكل كبير، نظراً لأن الخوارزميات غير المتناظرة الآمنة من حيث الحوسبة الكمومية عادةً ما يكون لها حجم أكبر بكثير، فيما يتعلق بالمفتاح العمومي أو النص المشفر أو التوقيع، من الخوارزميات غير المتناظرة الكلاسيكية. فعلى سبيل المثال، يختلف حجم المفتاح العمومي للخوارزميات غير المتناظرة الآمنة من حيث الحوسبة الكمومية من 726 بايتة إلى حوالي 1 Mbyte كما هو موضح في الفقرة 5.II، بينما يختلف حجم المفتاح العمومي للخوارزميات غير المتناظرة الكلاسيكية عادةً من 32 بايتة فقط إلى 256 بايتة. ويخطط المعهد الوطني للمعايير والتكنولوجيا (NIST) لتقييس أكثر من خوارزمية غير متناظرة آمنة من حيث الحوسبة الكمومية. وبالتالي، من البديهي أن يتم اختيار الخوارزميات غير المتناظرة الآمنة من حيث الحوسبة الكمومية ذات الحجم الأصغر للمفتاح العمومي أو النص المشفر أو التوقيع للاستخدام في أنظمة الاتصالات المتنقلة الدولية–2020. علاوة على ذلك، تحتاج معايير أنظمة الاتصالات المتنقلة الدولية–2020 إلى تحديد حجم الرسالة المناسب لاستيعاب المفتاح العمومي أو النص المشفر أو التوقيع عند نشر خوارزميات غير متناظرة آمنة من حيث الحوسبة الكمومية.

2.10 البروتوكولات IPsec وTLS وDTLS

إذا تم تطبيق PSK على الاستيقان واتفاق المفتاح، فمن المستحسن أن يكون حجم المفتاح PSK مساوياً 256 بتة، ويوصى باستخدام خوارزميات متناظرة آمنة من حيث الحوسبة الكمومية يبلغ طول مفتاحها 256 بتة لسرية وسلامة الرسائل المرسلة عبر الشبكة. وإذا تم استخدام مخططات الاستيقان المستند إلى الشهادات، يوصى بدمج الخوارزميات غير المتناظرة الآمنة من حيث الحوسبة الكمومية في بروتوكولات الاستيقان من أجل تنفيذ استيقان آمن من حيث الحوسبة الكمومية واتفاق مفتاح دورة آمن من حيث الحوسبة الكمومية، من أجل حماية سرية وسلامة الرسائل، ويوصى بنشر خوارزميات متناظرة آمنة من حيث الحوسبة الكمومية يبلغ طول مفتاحها 256 بتة. وبهذه الطريقة، فإن الشبكة SDN وأمن ميدان الشبكة/وبروتوكول الإنترنت ومستوى الإدارة لا تكون عرضة للهجمات الكمومية.

لم يبدأ فريق مهام هندسة الإنترنت العمل على كيفية إضافة خوارزميات آمنة من حيث الحوسبة الكمومية إلى متواليات التجفير في البروتوكولات IPsec وTLS وDTLS، حيث لم ينته المعهد الوطني للمعايير والتكنولوجيا من تحديد المرشحين للخوارزميات غير المتناظرة الآمنة من حيث الحوسبة الكمومية. ومن المتوقع أن تكون مشاريع معايير المعهد الوطني للمعايير والتكنولوجيا متاحة في الفترة من 2022 إلى 2024 [b-Moody]. وبمجرد أن يحدد فريق مهام هندسة الإنترنت متواليات التجفير المقاومة للحوسبة الكمومية من أجل البروتوكولات IPsec وTLS وDTLS، مع الأخذ في الاعتبار عرض النطاق اللاسلكي الشحيح وإمكانيات الحوسبة المحدودة في الأجهزة، يوصى بنشر متوالية تجفير ذات حجم مفتاح أصغر وعملية تجفير عالية السرعة في أنظمة الاتصالات المتنقلة الدولية–2020.

3.10 طبقة البنية التحتية

يوصى بشبكة SDN لتطبيق الاقتراحات المحددة في الفقرة 2.10 على استخدامات البروتوكولين IPsec وTLS.

يوصى بالاستعاضة عن خوارزميات التجفير الكلاسيكية المنتشرة في طبقة البنية التحتية NFVI بخوارزميات تفير آمنة من حيث الحوسبة الكمومية، بما في ذلك الخوارزميات من الأنواع المتناظرة وغير المتناظرة.

4.10 شبكة نفاذ الاتصالات المتنقلة الدولية–2020

1.4.10 خصوصية المشترك

يوصى بالمخطط ECIES لتطبيق الخوارزميات المتناظرة الآمنة من حيث الحوسبة الكمومية مثل DH لتوليد مفتاح مشترك، مثل تغليف المفاتيح متساوي المنشأ فائق التفرد (SIKE) وNewHope، وهما مرشحان من الدورة الثانية في إجراء تقييس تجفير ما بعد الكمومية للمعهد NIST (انظر التذييل II). ويوصى بإخفاء المعرف SUCI باستخدام خوارزمية متناظرة آمنة من حيث الحوسبة الكمومية بمفتاح مشترك طوله 256 بتة.

2.4.10 الاستيقان

نظراً إلى أن مجموعة الخوارزمية MILENAGE تدعم فقط دخل مفتاح حجمه 128 بتة، في حين أن مجموعة الخوارزمية TUAK يمكن أن تدعم واحدة من تلك التي حجمها 256 بتة، يوصى باستخدام مجموعة خوارزمية TUAK في إجراء الاستيقان لإنشاء رد بالمتجه AV والاستيقان بدلاً من مجموعة الخوارزمية MILENAGE.

3.4.10 تراتب المفاتيح

لإنشاء مفتاح الدورة K_{SEAF} مع إنتروبيا 256 بتة، يجب أن يقوم تراتب المفاتيح بإجراء التعديلات التالية: (1) يوصى بأن يكون حجم مفتاح الجذر K مقداره 256 بتة؛ (2) يوصى بعدم اقتطاع خرج الوظيفة GKDF ذي الطول 256 بتة بعد الآن.

ومن الناحية العملية، يبلغ طول مفتاح الجذر K عادةً 128 بتة، وذلك بسبب استخدام بطاقات USIM التقليدية في أنظمة الاتصالات المتنقلة الدولية–2020 التي تحتوي على هذه التشكيلة؛ وستظل بطاقات USIM الجديدة المستخدمة لأنظمة الاتصالات المتنقلة الدولية–2020 المبكرة من قبل العديد من المشغلين تخزن فقط مفتاح جذر طوله 128 بتة. والنتيجة هي أن طول إنتروبيا مفتاح الدورة K_{SEAF} المشتقة من المفتاح K هو 128 بتة فقط، وهي ليست آمنة من حيث الحوسبة الكمومية.

ولتعزيز الأمن لمفتاح الدورة الحالية K_{SEAF} عندما تكون البطاقة USIM مزودة بمفتاح جذر طوله 128 بتة، فإن إنشاء مفتاح الدورة الحالية K_{SEAF} لا يعتمد فقط على مفتاح الدورة الأولى 'K_{SEAF}' الذي يحدده المفتاح طويل المدى K، ولكن أيضاً مفتاح واحد على الأقل من المفاتيح الإضافية. ويمكن أن تكون المفاتيح الإضافية هي مفتاح الدورة الأولي $K_{SEAF\_INITIAL}$ الذي تم إنشاؤه في المرة الأولى التي يتم فيها توصيل المعدة UE بالشبكة و/أو مفتاح الدورة K_{SEAF_PRV} المستخدم في الدورة السابقة. وكل من مفتاح الدورة الأولى والمفاتيح الإضافية مفاتيح متناظرة، مما يعني أن المعدة UE والشبكة يشتركان فيها. وبهذه الطريقة، ستكون إنتروبيا مفتاح الدورة الحالية K_{SAEF} بطول 256 بتة على الأقل، حيث إن إنتروبيا مفتاح الدورة الأول 'K_{SEAF}' ستكون بطول 128 بتة وأن إنتروبيا المفاتيح الإضافية (مفتاح $K_{SEAF\_INITIAL}$ و/أو مفتاح K_{SEAF_PRV}) ستكون بطول 128 بتة على الأقل.

وكممارسة جيدة، يمكن استخدام بطاقات SIM الجديدة اختيارياً لتحقيق إنتروبيا بطول 256 بتة لمفتاح الدورة K_{SEAF}. ويمكن أن تكون هذه البطاقة إما SIM أو USIM أو eSIM أو غيرها من عوامل وأنواع البطاقات SIM غير القياسية مع التعديلات المقابلة من أجل:

أ) تخزين مفتاح جذر بطول 256 بتة، ليؤدي نفس الغرض الذي يؤديه مفتاح الجذر K في البطاقات SIM أو USIM القديمة؛

ب) دعم تسريع العتاد من أجل الوظيفة KDF الضرورية والعروة الأساسية للتجفير المتناظر (مثل المعيار AES) في بطاقات SIM الجديدة. وهذا الأمر مهم بشكل خاص لإنترنت الأشياء وفي البلدان التي تشكل فيها الهواتف المميزة

جزءاً مهماً من العدد الإجمالي للأجهزة الخلوية المستخدمة، ومع ذلك يمكن جعلها متوافقة مع نظام IMT-2020 آمن من حيث الحوسبة الكمومية – إن لم تكن سريعة – من خلال إعادة استخدام الترددات وترجمة البروتوكول.

4.4.10 أمن تشوير الطبقة NAS وتشوير الطبقة AS وبيانات المستعمل

كما هو مبين في الفقرة 7، فإن خوارزميات المفاتيح المتناظرة ذات الطول 128 بتة مثل AES-128 وSNOW 3G وZUC-128 هي الأساس لحماية سرية وسلامة تشوير الطبقة NAS وتشوير الطبقة AS وبيانات المستعمل في شبكة نفاذ IMT-2020.

ولمقاومة الهجمات الكمومية، يوصى بنشر خوارزميات المفاتيح المتناظرة ذات الطول 256 بتة في أنظمة الاتصالات المتنقلة الدولية–2020. ويوفر حجم الشفرة MAC الأطول ضماناً أكبر ضد الهجمات التي تخمن الشفرة MAC الصحيحة للرسالة. ويوصي المعيار [b-NIST SP 800-38B] باستخدام شفرة MAC بطول 64 بتة على الأقل للدفاع ضد هجمات التخمين. ويبلغ طول الشفرة MAC في شبكة نفاذ الاتصالات المتنقلة الدولية–2020 32 بتة فقط. وهناك تأثير كبير على شبكة الاتصالات المتنقلة الدولية–2020 وبروتوكولها إذا تمت زيادة حجم الشفرة MAC من 32 إلى 64 بتة. وما إذا كانت شبكة نفاذ الاتصالات المتنقلة الدولية–2020 لا تزال قادرة على الدفاع ضد هجمات التخمين عند تطبيق خوارزميات متناظرة آمنة من حيث الحوسبة الكمومية بطول 256 بتة لتوليد شفرة MAC بطول 32 بتة يحتاج إلى مزيد من الدراسة.

5.4.10 أمن النفاذ خلاف نفاذ مشروع الشراكة 3GPP

لاستراتيجية مقاومة الهجوم الكمومي للنفاذ خلاف نفاذ مشروع الشراكة 3GPP، راجع الفقرة 2.10، حيث يعتمد أمن النفاذ خلاف نفاذ مشروع الشراكة 3GPP على البروتوكول IPsec.

5.10 الشبكة الأساسية للاتصالات المتنقلة الدولية–2020

1.5.10 داخل الشبكة PLAN

1) الاستيقان

لمقاومة الهجوم الكمومي، يوصى بالاستيقان القائم على NDS/IP لتطبيق نفس الإستراتيجية المقدمة في الفقرة 2.10.

2) التخويل

يوصى بنشر دالات الاختزال ذات المفاتيح الآمنة من حيث الحوسبة الكمومية، مثل HMAC-SHA-256، بالإضافة إلى خوارزميات التوقيع الآمنة من حيث الحوسبة الكمومية، في الاستيقان OAuth 2.0 لضمان سلامة تأشيرة النفاذ. ولاستراتيجية الانتقال إلى متواليات التجفير الآمنة من حيث الحوسبة الكمومية في البروتوكول TLS، انظر الفقرة 2.10.

ويوصى بنشر خوارزميات التوقيع الآمنة من حيث الحوسبة الكمومية من أجل التوقيع JWS.

2.5.10 بين شبكتين PLMN

يوصى بتطبيق الطريقة المقدمة في الفقرة 2.10 على التوصيلة N32-c لمنع المهاجم الكمومي من اشتقاق مفاتيح الدورة. ويوصى بنشر المعيار AES-GCM مع مفتاح بطول 256 بتة في سطح بيني N32 لضمان سرية وسلامة الاتصالات بين الشبكتين PLMN.

ويوصى بنشر خوارزميات التوقيع الآمنة من حيث الحوسبة الكمومية بدلاً من الخوارزمية ECDSA من أجل التوقيع JWS.

التذييل I

نظرة عامة على نظام الاتصالات المتنقلة الدولية–2020

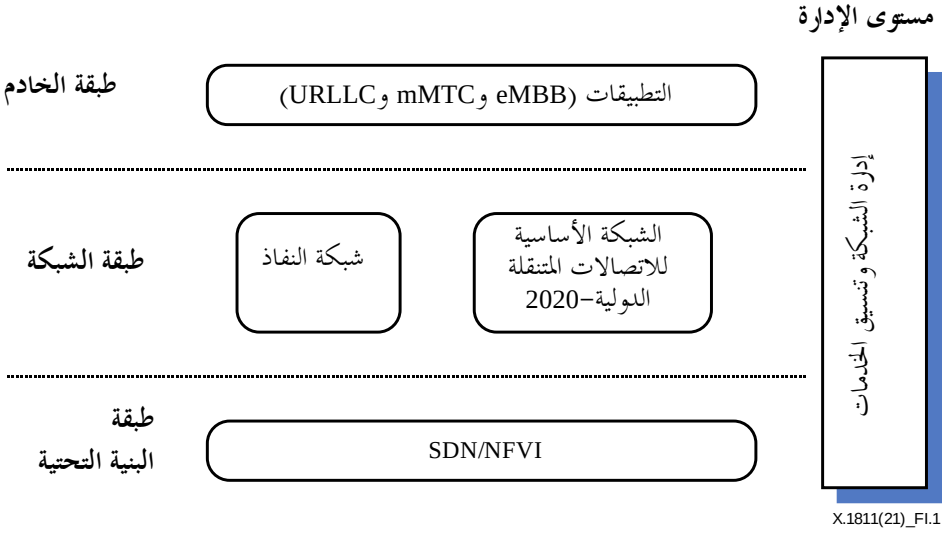
(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية.)

يقدم هذا التذييل وصفاً عاماً لنظام الاتصالات المتنقلة الدولية–2020.

1.I المعمارية العامة

يهدف نظام الاتصالات المتنقلة الدولية–2020 إلى تقديم مجموعة واسعة من الخدمات بمتطلبات أداء مختلفة. ويمكن تصنيف الخدمات المقدمة في شبكات الاتصالات المتنقلة الدولية–2020 إلى ثلاث فئات وفقاً لمواصفات مشروع الشراكة 3GPP: (1) يدعم النطاق العريض المتنقل المعزز معدلات بيانات أعلى وتنقلية أكبر للمستعمل مقارنة بالتكنولوجيا طويلة الأجل/الجيل الرابع؛ (2) توفر إنترنت الأشياء الكثيفة اتصالات كثيفة من آلة لآلة؛ (3) تدعم الاتصالات URLLC خدمات المهام الحرجة التي تتطلب موثوقية أعلى وكمون أقل. ومن المزمع أن يكون نظام الاتصالات المتنقلة الدولية–2020 منصة مرنة تتيح حالات أعمال جديدة وتدمج الصناعات الرأسية، مثل السيارات والتصنيع والطاقة والصحة الإلكترونية والترفيه. وعلاوة على ذلك، سيكون نشر وصيانة نظام الاتصالات المتنقلة الدولية–2020 أسهل مقارنة بالأجيال السابقة من الشبكات المتنقلة. ولمواجهة هذه المتطلبات الصعبة، أدخل نظام الاتصالات المتنقلة الدولية–2020 عدداً من التكنولوجيات المبتكرة، مثل تقسيم الشبكة، والتمثيل الافتراضي لوظائف الشبكة (NFV)، والشبكات SDN، والمعمارية SBA، والفصل بين الوحدة المركزية/الوحدة الموزعة (CU/DU).

يمكن تقسيم المعمارية العامة لنظام الاتصالات المتنقلة الدولية–2020، الموضحة في الشكل 1.I، إلى: طبقة البنية التحتية؛ وطبقة الشبكة؛ وطبقة الخدمة ومستوى الإدارة، حسب الوظيفة.



الشكل 1.I – المعمارية العامة لنظام الاتصالات المتنقلة الدولية–2020

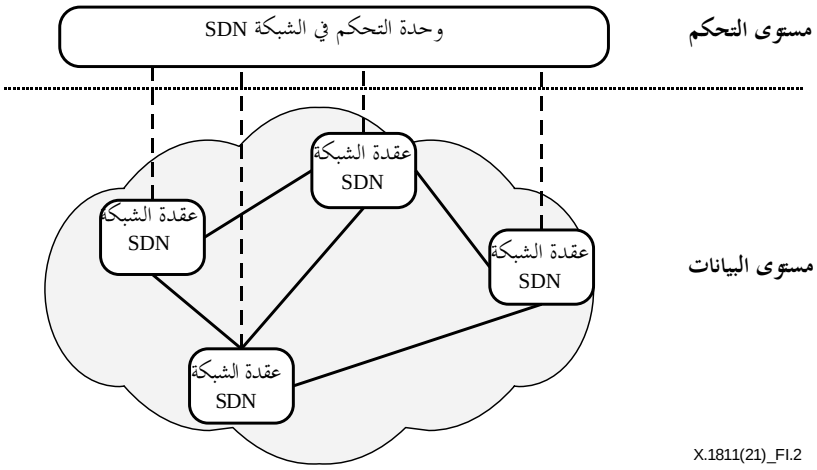
- طبقة البنية التحتية، تضم الشبكة SDN والبنية التحتية NFVI. وتستخدم الشبكة SDN لنقل الحزم إلى المقصد. وإلى جانب تكنولوجيات النقل التقليدية (على سبيل المثال، تبديل الوسم متعدد البروتوكولات (MPLS))، أدخل نظام الاتصالات المتنقلة الدولية–2020 تكنولوجيا الشبكات SDN لزيادة سرعة النقل والتكيف السهل مع متطلبات الخدمة. . والبنية التحتية NFVI هي الأساس المشترك لتشغيل الوظائف VNF.
- طبقة الشبكة، تضم شبكة النفاذ والشبكة الأساسية. وتمكن الأولى المعدة UE من النفاذ إلى شبكة من شبكات الاتصالات المتنقلة الدولية–2020 في أي مكان. والثانية مصممة مع وضع المعمارية SBA في الاعتبار من أجل

إمكانية التوسع والتبسيط. وهي تتكون من عدد من الوظائف NF لدعم توصيلية البيانات ونشر الخدمات، مثل AUSF وAMF وSMF.

- طبقة الخدمة، تتألف من التطبيقات التي تُشغل على قمة النظام IMT-2020، والتي قد تكون تطبيقات eMBB، وتطبيقات الاتصالات الكثيفة من آلة لآلة (mMTC)، وتطبيقات URLLC.
- مستوى الإدارة، هو المسؤول عن إدارة الشبكة وتنسيق الخدمات.

2.I الشبكة المعرفة بالبرمجيات (SDN)

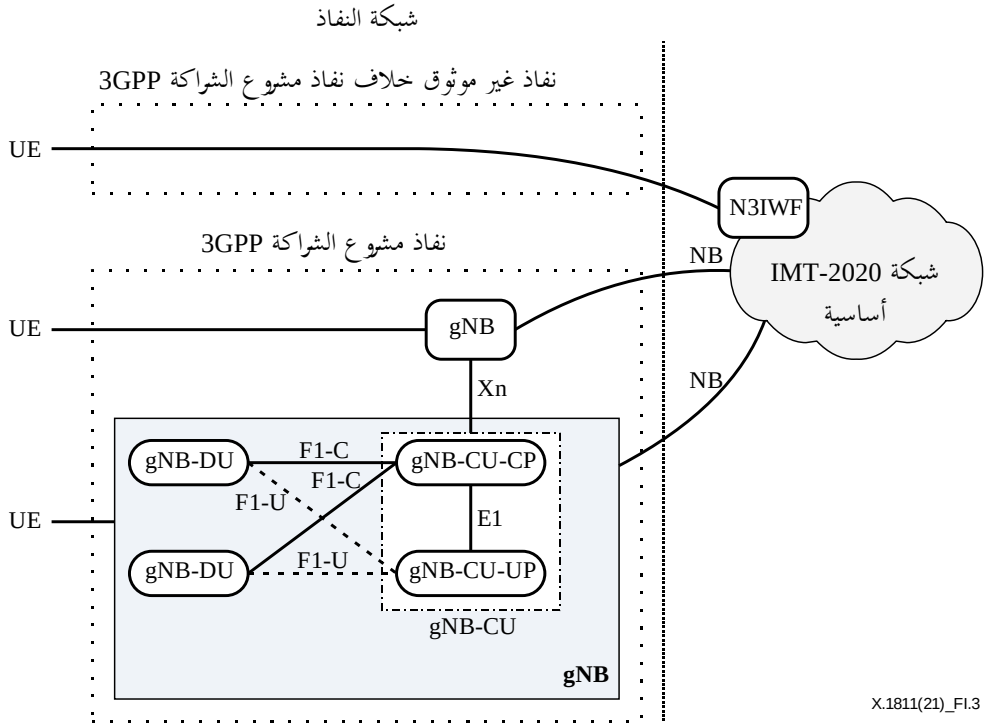
يتمثل المبدأ الأساسي للشبكة SDN في فصل مستوى البيانات عن مستوى التحكم (CP)، بحيث يمكنها دعم البرمجة الدينامية لعقد الشبكة في عملية إعادة تسيير البيانات. وتتخذ وحدة التحكم في الشبكة SDN قرارات الربط الشبكي وترسل قواعد إعادة التسيير الناتجة إلى عقد الشبكة. وتعمل آلية إعادة التسيير هذه على تبسيط تنفيذ عقد الشبكة وتؤدي إلى تحسين أداء مستوى البيانات. وتوضح معمارية الشبكة SDN في الشكل 2.I.



الشكل 2.I – معمارية الشبكة SDN

3.I شبكة النفاذ

يمكن للمعدة UE الحصول على النفاذ إلى شبكة IMT-2020 أساسية إما بأسلوب نفاذ غير موثوق خلاف نفاذ مشروع الشراكة 3GPP أو بأسلوب نفاذ مشروع الشراكة 3GPP، كما هو موضح في الشكل 3.I. وتوفر شبكة النفاذ الخدمات المتعلقة بإرسال البيانات عبر السطح البيني الراديوي.



الشكل I.3 – شبكة النفاذ

– النفاذ غير الموثوق خلاف نفاذ مشروع الشراكة 3GPP

يعني النفاذ غير الموثوق خلاف نفاذ مشروع الشراكة 3GPP أن تكنولوجيا النفاذ غير موصفة من قبل مشروع الشراكة 3GPP وغير موثوق بها بالنسبة للشبكة IMT-2020 الأساسية، مثل نفاذ الشبكة المحلية اللاسلكية (WLAN). وفي هذا السياق، توصل المعدة UE بالشبكة IMT-2020 الأساسية عبر الوظيفة N3IWF.

– نفاذ مشروع الشراكة 3GPP

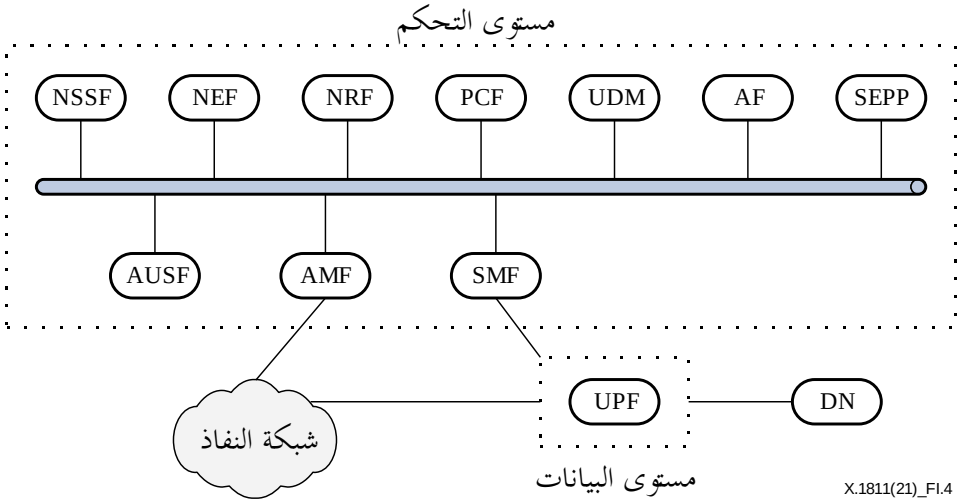
نفاذ مشروع الشراكة 3GPP تكنولوجيا موصفة من قبل مشروع الشراكة 3GPP، أي تكنولوجيا النفاذ الراديوي من الجيل التالي (NG-RAN) في سياق تكنولوجيا الاتصالات المتنقلة الدولية–2020. ويمكن للمعدة UE النفاذ إلى الشبكة IMT-2020 الأساسية باستخدام سطح بيني NG عبر عقدة gNB مسطحة دون الفصل بين الوحدتين CU/DU. والسطح البيني NG هي سطح بيني منطقي يدعم تبادل معلومات المستوى CP ومعلومات المستوى UP بين العقدة gNB والشبكة IMT-2020 الأساسية. ولتحقيق مزيد من المرونة في نشر الشبكة وخفض التكاليف، يمكن تقسيم العقدة gNB إلى العقدتين gNB-DU وgNB-CU. والعقدة gNB-CU هي عقدة منطقية تنفذ بروتوكولات الطبقة الأعلى، بما في ذلك بروتوكول تكييف بيانات الخدمة (SDAP)، والتحكم في الموارد الراديوية (RRC)، وبروتوكول تقارب بيانات الرزم (PDCP). والعقدة gNB-DU هي عقدة منطقية تؤدي وظائف الطبقة الأدنى، بما في ذلك التحكم في الوصلة الراديوية (RLC) والتحكم في النفاذ إلى الوسائط (MAC) ووظائف الطبقة المادية.

وانطلاقاً من مفهوم الشبكة SDN، يمكن تقسيم العقدة gNB-CU إلى العقدتين gNB-CU-CP وgNB-CU-UP. وسيؤدي هذا إلى تحلل وظيفي للنفاذ اللاسلكي بين المستعمل والكيانات CP. ويوفر هذا الفصل بين المستويين CP وUP المرونة في تشغيل وإدارة الشبكات المعقدة، ودعم طوبولوجيا الشبكات المختلفة والموارد ومتطلبات الخدمة الجديدة.

ويتم توصيل وحدات العقدتين gNB-CU وgNB-DU عبر سطح بيني منطقي F1، والذي يمكن تمييزه عن السطح البيني F1-C لتوصيل العقدة gNB-CU-CP والسطح البيني F1-U لتوصيل العقدة gNB-CU-UP. وتتواصل العقدة gNB-CU-CP مع العقدة gNB-CU-UP من خلال سطح بيني E1.

4.I الشبكة الأساسية

تُعرَّف الشبكة IMT-2020 الأساسية بأنها معمارية SBA، كما هو موضح في الشكل 4.I. وتم تحديد عدد من الوظائف NF في المعمارية SBA لخدمة أغراض مختلفة. وتعرض كل وظيفة NF مجموعة من الخدمات تسمى خدمة الوظيفة NF تستهلكها الوظائف NF الأخرى المعتمدة. وتقوم الوظائف NF بالاستعلام من الوظيفة NRF لاكتشاف كل منها الأخرى والاتصال فيما بينها.



الشكل 4.I – الشبكة IMT-2020 الأساسية

ويمكن تقسيم الشبكة IMT-2020 الأساسية إلى مستوى التحكم (CP) ومستوى المستعمل (UP).

- **مستوى التحكم**

يوفر هذا المستوى خدمات التحكم في الشبكة، بما في ذلك النفاذ والتنقلية والسياسات والعرض والاعتراض القانوني والتحكم المرتبط بالترسيم. وتم تعريف الوظائف NF التالية في المستوى CP.

- **وظيفة اختيار قسم الشبكة (NSSF)**، تستخدم لاختيار حالات أقسام الشبكة التي تخدم المعدة UE.
- **وظيفة عرض شبكية (NEF)**، تدعم الكشف عن القدرات والأحداث. وتعرض الوظائف NF القدرات والأحداث على الوظائف NF الأخرى عبر الوظيفة NEF. وقد يتم الكشف بشكل آمن عن القدرات والأحداث الخاصة بالوظيفة NF، على سبيل المثال لطرف ثالث، ولوظائف التطبيقات ولحوسبة الحافة.
- **وظيفة مستودع الوظيفة NF (NRF)**، توفر وظائف التسجيل والاكتشاف، بحيث يتسنى للوظائف NF اكتشاف كل منها الأخرى والاتصال فيما بينها عبر السطوح البينية لبرمجة التطبيقات.
- **وظيفة التحكم في السياسات (PCF)**، تدعم توفير إطار سياساتي موحد للتحكم في سلوك الشبكة.
- **إدارة البيانات الموحدة (UDM)**، تخزن بيانات وخصائص المشتركين. وتستخدم الإدارة UDM أيضاً لتوليد المتجهات AV للاتفاق AKA الخاص بمشروع الشراكة 3GPP.
- **وظيفة التطبيق (AF)**، تتفاعل مع الشبكة الأساسية 3GPP من أجل توفير الخدمات. وتوفر الوظيفة AF أيضاً معلومات عن تدفق الرزم إلى الوظيفة PCF.
- **وكيل حماية حافة الأمن (SEPP)**، وكيل غير شفاف يستخدم لحماية الرسائل المتبادلة على السطوح البينية بين الشبكات PLMN والمستوى CP وإخفاء طبولوجيا الشبكة PLMN الداخلية.
- **وظيفة مخدم الاستيقان (AUSF)**، تعالج طلبات الاستيقان لكل من نفاذ مشروع الشراكة 3GPP والنفاذ خلاف نفاذ مشروع الشراكة 3GPP.
- **وظيفة إدارة النفاذ وإدارة التنقلية (AMF)**، توفر الاستيقان والتخويل وإدارة التنقلية للمعدات UE.

- **وظيفة إدارة الدورة (SMF)**، تستخدم لإدارة الدورة، مثل إنشاء الدورة، وتعديلها، وإطلاقها. وتقوم الوظيفة SMF أيضاً بتوزيع عناوين بروتوكول الإنترنت للمعدات UE.

– مستوى المستعمل

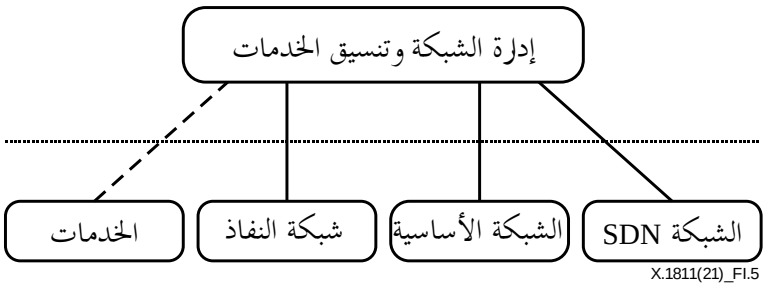
وظيفة مستوى المستعمل (UPF) هي الوظيفة الوحيدة المعرفة لمستوى المستعمل. وتدعم هذه الوظيفة العمليات والوظائف المختلفة المتعلقة برزم مستوى المستعمل، مثل تسيير الرزم وإعادة تسييرها، وإدارة الحركة، والتفتيش على الرزم ومزاوجتها.

وتختلف الشبكة IMT-2020 الأساسية كثيراً عن الشبكة الأساسية للشبكات المتنقلة من الأجيال السابقة في السمات التالية.

- **المعمارية SBA**، التي تعمل خدماتها بتقسيم أدق من الشبكات التقليدية وتقترن بأريحية مع بعضها البعض. ويسمح ذلك بوقت قصير لتسويق الخدمات الجديدة ومرونة أكبر بالنسبة لتحديثات النظام.
- **الفصل بين مستوى التحكم ومستوى المستعمل**، يسمح بنشر الوظيفة UPF في مكان أقرب إلى المعدة UE، بحيث يمكن تلبية متطلبات الكمون الصارمة هذه من الخدمات URLLC. ويمكن الفصل بين مستوى التحكم ومستوى المستعمل أيضاً من قياس موارد كل مستوي بشكل مستقل.
- **الفصل بين الوظيفتين AMF وSMF**، يمكن من إدارة النفاذ والتنقلية بصورة مركزية. وعلى النقيض، يمكن وضع الوظيفة SMF في المكان التي تحتاجها الخدمة فيه.
- **التمثيل الافتراضي لوظائف الشبكة (NFV)**، يفترض في الشبكة IMT-2020 الأساسية أن الوظائف NF تنفذ بصورة افتراضية من أجل إدارة أفضل للموارد وتحقيق وفر في التكلفة. والتمثيل الافتراضي لوظائف الشبكة الذي يفصل بين العتاد والبرمجيات يجعل الشبكة أكثر مرونة وأكثر بساطة من خلال تدنية الاعتماد على قيود العتاد.
- **قسم الشبكة**، الغرض منه دعم أنواع خدمات متعددة على بنية تحتية شبكية مادية مشتركة. ويمكنه توفير شبكات مكيفة من طرف إلى طرف لتلبية المتطلبات المختلفة. وقد يضم كل قسم من أقسام الشبكة وظائف NF مختلفة تبعاً لمتطلبات الخدمة.

5.I مستوى الإدارة

مستوى الإدارة مسؤول عن إدارة الشبكة وتنسيق الخدمة. ومن أجل إدارة ومراقبة الشبكات، يوصل مستوى الإدارة بشبكة النفاذ والشبكة الأساسية والشبكة SDN عبر قناة اتصالات فردية مخصصة، كما هو موضح في الشكل 5.I. وتحتوي إدارة الشبكة على الوظائف التالية على أقل تقدير: إدارة الأعطال (FM)، وإدارة الأداء (PM)، وإدارة التشكيلة (CM) وإدارة التتبع (TM). وبالإضافة إلى وظائف إدارة الشبكة هذه، تحتاج إدارة قسم الشبكة أيضاً إلى الوظائف التالية: إدارة دورة حياة القسم، وإدارة قدرات القسم، واكتشاف موارد الشبكة. ويطبق تنسيق الخدمات آليات تحكم ومراقبة في الموارد تتسم بالمرونة لتوفير وإدارة وإعادة استمثال خدمات الشبكة.



الشكل 5.I – المعمارية العامة للإدارة

التذييل II

خوارزميات تجفير المفاتيح غير المتناظرة الآمنة من حيث الحوسبة الكمومية

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية.)

يسرد هذا التذييل خوارزميات تجفير المفاتيح غير المتناظرة الآمنة من حيث الحوسبة الكمومية المعروفة جيداً.

1.II الخوارزميات القائمة على الشبكة

فيما يلي بعض الخوارزميات القائمة على الشبكة:

- الحلقة متعددة الحدود المشذبة من الدرجة N (NTRU) [b-Hoffstien]؛
- التعلم من خلال الأخطاء (LWE) [b-Regev]؛
- حلقة تعلم من خلال الأخطاء (R-LWE) [b-Lyubashevsky]؛
- مخطط NewHope [b-Alkim].

2.II الخوارزميات القائمة على الاختزال

فيما يلي بعض الخوارزميات القائمة على الاختزال:

- مخطط ميركل الموسع للتوقيع (XMSS) [b-Buchmann]؛
- SPHINCS [b-Bernstein 2015]؛
- توقيعات Leighton-Micali المستندة إلى الاختزال (LMS) [b-IRTF RFC 8554].

3.II الخوارزميات القائمة على الشفرة

فيما يلي بعض الخوارزميات القائمة على الشفرة:

- McEliece التقليدية [b-McEliece]؛
- مخطط Niederreiter [b-Dinh].

4.II الخوارزميات متعددة المتغيرات

فيما يلي بعض مخططات التوقيع العملية المستندة إلى خوارزميات متعددة المتغيرات:

- Rainbow [b-Ding]؛
- مخطط oil and vinegar غير المتوازن (UOV) [b-Kipnis].

5.II تقييس المعهد الوطني للمعايير والتكنولوجيا (NIST) لتجفير ما بعد عصر الحوسبة الكمومية

في 20 ديسمبر 2016، أعلن المعهد الوطني للمعايير والتكنولوجيا (NIST) عن طلب الترشيحات لخوارزميات التجفير لما بعد عصر الحوسبة الكمومية للمفاتيح العمومية. وفي الجولة الأولى، قبل المعهد الوطني للمعايير والتكنولوجيا 69 ترشيحاً، تتكون من 20 مخططاً للتوقيع الرقمي و49 تجفيراً للمفاتيح العمومية (PKE) أو آليات تغليف للمفاتيح (KEM). وفي 30 يناير 2019، اختار المعهد الوطني للمعايير والتكنولوجيا 26 خوارزمية مدرجة في الجدول 1.II كخوارزميات مرشحة للجولة الثانية، والتي تشمل تسعة مخططات للتوقيع الرقمي، و17 مخططاً للتجفير PKE وإنشاء المفاتيح [b-NISTIR 8240].

الجدول 1.II – خوارزميات الجولة الثانية للمعهد الوطني للمعايير والتكنولوجيا

التصنيف	أساس المشكلة	الخوارزمية
تجفير/KEM	قائم على الشبكة	Crystals-Kyber
		FrodoKEM
		LAC
		NewHope
		NTRU
		NTRU Prime
		Round 5
		Saber
		Three Bears
	قائم على الشفرة	Classic McEliece
		NTS-KEM
		BIKE
		HQC
		Rollo
		LEDAcrypt
		RQC
	على أساس تساوي المنشأ	SIKE
توقيع	قائم على الشبكة	Crystals-Dilithium
		Falcon
		qTesla
	قائم على تعدد المتغيرات	GeMSS
		LUOV
		MQDSS
		Rainbow
	قائم على الاختزال	Sphincs+
		Picnic

يعتزم المعهد NIST تقييس خوارزميات المفاتيح العمومية لما بعد عصر الحوسبة الكمومية لاستخدامها في مجموعة متنوعة من البروتوكولات، مثل TLS والدرع المأمون (SSH) وتبادل مفاتيح الإنترنت (IKE) وIPsec وتمديدات أمن نظام أسماء الميادين (DNSSEC) [b-NISTIR 8240].

ويقوم المعهد NIST بتقييم خوارزميات الجولة الثانية من منظوري الأمن والأداء. واكتشف تجفير NTRU في عام 1996، وقد تم استيعاب أمنه جيداً ودراسته بشكل معقول لعقود. وعلاوة على ذلك، تم تقييس تجفير NTRU في المعيار [b-IEEE Std 1363.1]. وتعتمد خوارزمية Classic McEliece على المعيار [b-McEliece]، والتي لم يتم كسرها، وتعتبر آمنة في عالم الحوسبة الكمومية. وفي المقابل، لم يتم إصدار العديد من المخططات الأخرى منذ مدة تزيد عن 10 سنوات. وبالتالي، لا تزال هذه المخططات بحاجة إلى تحليل عميق للتجفير من قبل مجتمع التجفير من أجل زيادة الثقة في أمنها. ويعتمد التغليف SIKE، الذي نشأ من المعيار [b-Jao]، بشكل خاص، على مشكلة إيجاد التماثل في المنشأ بين المنحنيات الإهليلجية فائقة التفرد، والتي لم تتم دراستها بنفس قدر بعض المشكلات الأمنية المرتبطة بالمرشحين الآخرين [b-NISTIR 8240].

تعني السرية التامة في الاتجاه المباشر أنه لن يتم الكشف عن مفاتيح الجلسة السابقة، حتى إذا تم كشف المفتاح طويل المدى. وهذه خاصية أمن مفيدة تحبذها بروتوكولات الأمن المستخدمة على نطاق واسع، مثل IPsec وTLS. ومن بين جميع المرشحين، يمكن للخوارزميتين SIKE وNewHope فقط دعم السرية المثلى في الاتجاه المباشر.

ويقاس أداء الخوارزميات من حيث حجم المفاتيح العمومية والنص المجفر والتوقيعات، بالإضافة إلى كفاءة حساب التجفير وفك التجفير. وعادة ما يكون لخوارزميات PQC حجم أكبر بكثير من المفاتيح العمومية والنص المجفر والتوقيعات مقارنة بخوارزميات المفاتيح العمومية الكلاسيكية. ويتراوح حجم المفتاح العمومي للخوارزميات المرشحة بين 726 بايتة وأكثر من 1 Mbyte حسب المعيار [b-NIST PQC]. وللخوارزمية SIKE أصغر حجم للمفتاح العمومي، في حين أن حجم المفتاح العمومي في الخوارزميتين McEliece وNTS-KEM الكلاسيكيتين أكبر بكثير منه في المخططات الأخرى. ومع ذلك، يمكن للخوارزميتين McEliece وNTS-KEM الكلاسيكيتين إنشاء نص تجفير أصغر من المخططات الأخرى بسرعة تجفير تنافسية. ويبدو أن أداء الخوارزمية SIKE يحتل ترتيباً أبطأ من حيث الكم من العديد من الخوارزميات المرشحة الأخرى على الرغم من وجود أصغر حجم للمفتاح العمومي. ولذلك فإن المفاضلة بين كفاءة عرض النطاق وكفاءة الحوسبة ضرورية عند اختيار الخوارزميات PQC.

ويخطط المعهد NIST في 2020 إما لاختيار الخوارزميات المتأهلة للتصفيات النهائية للجولة النهائية أو اختيار عدد صغير من الخوارزميات المرشحة للتقييس [b-NISTIR 8240]. وهذا يعني أنه لن يتم تقييس خوارزمية واحدة فقط، ولكن سيتم تقييس مجموعة من الخوارزميات PQC. وفي بيئة الاتصالات المتنقلة، يعد الأداء بالغ الأهمية بسبب الموارد اللاسلكية الثمينة في السطح البيني الراديوي وقدرات الحوسبة المحدودة في الأجهزة. ويجب إدخال الخوارزميات المقيسة النهائية، والتي تتسم بأحجام أصغر من المفاتيح العمومية والنص المجفر، مع سرعة تشفير تنافسية في الأنظمة IMT-2020.

التذييل III

تأثير الحوسبة الكمومية على خوارزميات التجفير الشائعة

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية.)

يسرد هذا التذييل تأثير الحوسبة الكمومية على خوارزميات التجفير الشائعة.

يعرض الجدول 1.III ملخصاً لتأثير أجهزة الحاسوب الكمومية كبيرة الحجم على خوارزميات التجفير الشائعة، مثل RSA ومعيار التشفير المتقدم (AES).

وليس من المعروف إلى أي مدى يمكن دفع هذه المزايا الكمومية، ولا مدى اتساع الفجوة بين الجدوى في النماذج الكلاسيكية والكمومية [b-NISTIR 8105].

الجدول 1.III – تأثير الحواسيب الكمومية على خوارزميات التجفير شائعة الاستخدام [b-NISTIR Quantum report]

خوارزمية التجفير	النوع	الاستخدام	التأثير
AES	متناظرة	تجفير	يلزم أحجام مفاتيح كبيرة
SHA-2، SHA-3	اختزال	دالة اختزال	يلزم خرج أكبر
RSA	مفتاح عمومي	التوقيع، نقل المفتاح	لم تعد مأمونة
ECDSA وECDH	مفتاح عمومي	التوقيع، تبادل المفتاح	لم تعد مأمونة
DSA	مفتاح عمومي	التوقيع، تبادل المفتاح	لم تعد مأمونة

التذييل IV

معايير تقييم من أجل التجفير الآمن من حيث الحوسبة الكمومية

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية.)

يقدم هذا التذييل معايير التقييم الصادرة عن المعهد NIST لاختيار التجفير الآمن من حيث الحوسبة الكمومية.

ستقيم خوارزميات التجفير المقدمة استناداً إلى ثلاثة جوانب: الأمن والتكلفة والخوارزمية وخصائص التنفيذ [b-NIST-Sub].

1.IV الأمن

يعتبر الأمان الذي يوفره مخطط التجفير هو العامل الأكثر أهمية في التقييم. سيتم الحكم على المخططات بناءً على العوامل التالية:

تطبيقات تجفير المفاتيح العمومية: سيتم تقييس خوارزميات ما بعد عصر الحوسبة الكمومية وفقاً لمعاييرها الحالية بشأن التوقيعات الرقمية (FIPS 186) وإنشاء المفاتيح (SP 800-56A وSP 800-56B). وتُستخدم هذه المعايير في مجموعة متنوعة من بروتوكولات الإنترنت، مثل TLS وSSH وIKE وIPsec وDNSSEC. وستقيم المخططات بحسب الأمن الذي توفره في هذه التطبيقات أثناء عملية التقييم. وستقيم التطبيقات المطالب بها بشأن أهميتها العملية إذا كان هذا التقييم ضرورياً لتحديد الخوارزميات التي يجب تقييسها.

تعريف الأمن للتجفير/إنشاء المفاتيح: يجب أن تكون خوارزميات ما بعد عصر الحوسبة الكمومية للتجفير أو إنشاء المفاتيح "مأمونة دلالياً" فيما يتعلق بهجمات التجفير المختارة بشكل تكيفي. ويُشار إلى هذه الخاصية عموماً بأمن *IND-CCA2* في الأدبيات الأكاديمية.

ويجب أن يؤخذ تعريف الأمن أعلاه على أنه بيان لما يعتبره المعهد NIST هجوماً ذا صلة. وسيتم تقييم الآلية KEM ومخططات التجفير المقدمة بناءً على مدى جودة توفيرها لهذه الخاصية، وذلك عند استخدامها على النحو المحدد من قبل الجهة المقدمة. ولا تحتاج الجهات المقدمة للمخططات إلى تقديم إثبات على الأمن، على الرغم من أنه سيتم النظر في هذه الإثباتات، إن وجدت.

ولأغراض تقدير نقاط القوة الأمنية، قد يُفترض أن المهاجم لديه نفاذ إلى فك تجفير ما لا يزيد عن 2^{64} من النصوص المجفرة المختارة؛ ومع ذلك، يمكن أيضاً النظر في الهجمات التي تتضمن عدداً أكبر من النصوص المجفرة.

تعريف الأمن للتجفير المؤقت فقط/إنشاء المفاتيح: بالرغم من أن أمن النص المجفر المختار ضروري للعديد من التطبيقات الحالية (على سبيل المثال، بروتوكولات تبادل المفاتيح المؤقتة اسمياً التي تسمح بالتخزين المؤقت للمفتاح)، فإنه يمكن تنفيذ بروتوكول تبادل المفاتيح المؤقت في طريقة تتطلب فقط الأمن المنفعل من التجفير أو سابقة الآلية KEM.

وبالنسبة لهذه التطبيقات، يجب أن تكون خوارزميات ما بعد عصر الحوسبة الكمومية للتجفير/إنشاء المفاتيح المؤقت فقط مأمونة دلالياً فيما يتعلق بهجمات النص غير المجفر المختار. وتوسم هذه الخاصية بشكل عام بأمن *IND-CPA* في الأدبيات الأكاديمية.

وستقيم الآلية KEM ومخططات التجفير المقدمة بناءً على مدى جودة توفيرها لهذه الخاصية، عند استخدامها على النحو المحدد من قبل الجهة المقدمة. ولا تحتاج الجهات المقدمة إلى تقديم إثبات على الأمن، على الرغم من أنه سيتم النظر في هذه الإثباتات، إن وجدت. ويجب شرح أي مواطن ضعف أمنية ناتجة عن إعادة استخدام أي مفتاح بشكل كامل.

تعريف الأمن للتوقيعات الرقمية: تتيح خوارزميات ما بعد عصر الحوسبة الكمومية للتوقيع الرقمي التوقيعات الرقمية غير القابلة للتزوير الوجودي فيما يتعلق بهجمات الرسائل المختارة التكيفية. ويُشار إلى هذه الخاصية عموماً بأمن *EUF-CMA* في المؤلفات الأكاديمية.

وستُقيم الخوارزميات المقدمة للتوقيعات الرقمية بناءً على مدى جودة توفيرها لهذه الخاصية عند استخدامها كما هو محدد من قبل الجهة المقدمة.

ولأغراض تقدير نقاط القوة الأمنية، قد يُفترض أن المهاجم لديه نفاذ إلى فك تجفير ما لا يزيد عن 264 من الرسائل المختارة.

خصائص الأمن الإضافية: بينما تغطي تعاريف الأمن المدرجة آنفاً العديد من سيناريوهات الهجوم التي سيتم استخدامها في تقييم الخوارزميات المقدمة، هناك العديد من الخصائص الأخرى التي قد تكون مرغوبة:

إحدى هذه الخصائص هي السرية التامة. فبينما يمكن الحصول على هذه الخاصية من خلال استخدام وظائف التجفير والتوقيع القياسية، قد تكون تكلفة القيام بذلك باهظة في بعض الحالات. وعلى وجه الخصوص، تعتبر مخططات تجفير المفاتيح العمومية ذات خوارزمية إنشاء مفاتيح بطيئة، مثل RSA، غير مناسبة عادةً للسرية التامة في الاتجاه المباشر. وهذه حالة يوجد فيها ارتباط كبير بين التكلفة والأمن العملي لأي خوارزمية.

وهناك حالة أخرى يتفاعل فيها الأمن والأداء وهي مقاومة هجمات القنوات الجانبية. تعد المخططات التي يمكن جعلها مقاومة لهجمات القنوات الجانبية بأدنى تكلفة، مرغوبة أكثر من تلك التي يتم إعاقة أداؤها بشدة بسبب أي محاولة لمقاومة هجمات القنوات الجانبية. ونلاحظ أيضاً أن عمليات التنفيذ المستمثلة التي تعالج هجمات القنوات الجانبية (مثل عمليات التنفيذ في وقت ثابت) تكون أكثر فائدة من تلك التي لا تفعل ذلك.

والخاصية الثالثة المرغوبة هي مقاومة الهجمات متعددة المفاتيح. فمن الناحية المثالية، لا ينبغي للمهاجم أن يكتسب ميزة من خلال مهاجمة مفاتيح متعددة في وقت واحد، سواء كان هدف المهاجم هو الإخلال بزوج مفاتيح واحد، أو بعدد عدد كبير من المفاتيح.

والخاصية المرغوبة النهائية، على الرغم من سوء تعريفها، هي مقاومة سوء الاستخدام. فمن الناحية المثالية، يجب ألا تفشل المخططات بشكل كارثي بسبب أخطاء التشفير المعزولة، وأعطال مولد الأرقام العشوائية، وإعادة الاستخدام غير المتكرر، وإعادة استخدام أزواج المفاتيح (للتجفير المؤقت فقط/إنشاء المفاتيح)، وما إلى ذلك.

عوامل اعتبارية أخرى: نظراً إلى أن تجفير المفاتيح العمومية يميل إلى احتواء بنية رياضية دقيقة، فمن المهم جداً أن يتم فهم البنية الرياضية جيداً من أجل الحصول على الثقة في أمن نظام التجفير. ولتقييم هذا الأمر، سيتم النظر في مجموعة متنوعة من العوامل. فمع تساوي جميع الأشياء الأخرى، تتسم المخططات البسيطة بالفهم بشكل أفضل من المخططات المعقدة. وبالمثل، فإن المخططات التي يمكن أن ترتبط مبادئ تصميمها بهيئة راسخة للأبحاث ذات الصلة تميل إلى أن تكون مفهومة بشكل أفضل من المخططات الجديدة تماماً، أو المخططات التي تم تصميمها من خلال التصحيح المتكرر لأخطاء المخططات القديمة التي ثبت أنها عرضة لتحليل التجفير.

سيُنظر في وضوح توثيق المخطط وجودة التحليل المقدم من قبل الجهة المقدمة. وسيساعد التحليل الواضح والشامل على تطوير جودة ونضج التحليل من قبل المجتمع الأوسع. وسيتم النظر في أي حجج أو إثباتات أمنية تقدمها الجهة المقدمة. وفي حين تستند الإثباتات الأمنية بشكل عام إلى افتراضات غير مثبتة، فإنها غالباً ما تستبعد الأصناف الشائعة من الهجمات أو تربط أمن أي مخطط جديد بمشكلة حاسوبية أقدم وأفضل من حيث دراستها.

2.IV التكلفة

يمكن قياس تكلفة أي نظام تجفير للمفاتيح العمومية على عدة أبعاد مختلفة.

حجم المفتاح العمومي والنص المجفر والتوقيع: ستقيم المخططات بناءً على أحجام المفاتيح العمومية والنصوص المجفرة والتوقيعات التي تنتجها. وقد تكون كل هذه عوامل اعتبار مهمة للتطبيقات المقيدة بعرض النطاق أو في بروتوكولات الإنترنت التي لها حجم محدود للرزم. وقد تختلف أهمية حجم المفتاح العمومي حسب التطبيق؛ فإذا كان بإمكان التطبيقات تخزين المفاتيح العمومية مؤقتاً، أو تجنب إرسالها بشكل متكرر، فقد يكون حجم المفتاح العمومي أقل أهمية. وفي المقابل، من المرجح أن تستفيد التطبيقات التي تسعى إلى الحصول على سرية تامة في الاتجاه المباشر عن طريق إرسال مفتاح عمومي جديد في بداية كل جلسة بشكل كبير من الخوارزميات التي تستخدم مفاتيح عمومية صغيرة نسبياً.

الكفاءة الحاسوبية لعمليات المفاتيح العمومية والخاصة: ستقيم أيضاً المخططات بناءً على الكفاءة الحاسوبية لعمليات المفاتيح العمومية (التجفير والتغليف والتحقق من التوقيع) والمفاتيح الخاصة (فك التشفير وإزالة التغليف والتوقيع). وستقيم التكلفة الحاسوبية

لهذه العمليات في كل من العتاد والبرمجيات. ومن المحتمل أن تكون التكلفة الحاسوبية لعمليات المفاتيح العمومية والخاصة مهمة لجميع العمليات تقريباً، ولكن قد تكون بعض التطبيقات أكثر حساسية لأحدهما أو الآخر. فعلى سبيل المثال، يمكن إجراء عمليات التوقيع أو فك التجفير بواسطة جهاز مقيد حاسوبياً مثل البطاقة الذكية؛ أو بدلاً من ذلك، قد يحتاج المخدم الذي يتعامل مع حجم كبير من الحركة إلى إنفاق جزء كبير من موارده الحاسوبية للتحقق من توقيعات العملاء.

الكفاءة الحاسوبية لتوليد المفاتيح: ستقيم المخططات أيضاً بناءً على الكفاءة الحاسوبية لعمليات توليدها للمفاتيح، حيثما أمكن ذلك. والسيناريو الأكثر شيوعاً والذي يكون وقت توليد المفتاح فيه مهماً هو عندما يتم استخدام خوارزمية تجفير المفاتيح العمومية أو الآلية KEM لتوفير سرية تامة في الاتجاه المباشر. ومع ذلك، من الممكن أن تكون أوقات توليد المفاتيح مهمة أيضاً لأنظمة التوقيع الرقمي في بعض التطبيقات.

حالات فشل فك التجفير: بعض خوارزميات تجفير المفاتيح العمومية والآليات KEM، حتى عند تنفيذها بشكل صحيح، تنتج أحياناً نصوصاً مجفرة لا يمكن فك تجفيرها/إزالة تغليفها. وبالنسبة لمعظم التطبيقات، من المهم أن تكون حالات فشل فك التجفير هذه نادرة أو غير موجودة. وبالنسبة للخوارزميات التي بها حالات فشل في فك التجفير/إزالة التغليف، يجب على الجهات المقدمة تقديم معدل الفشل، بالإضافة إلى تحليل التأثيرات على الأمن الذي يمكن أن تسببه حالات الفشل هذه. وفي حين يمكن للتطبيقات دائماً الحصول على معدل فشل منخفض مقبول لفك التجفير عن طريق تجفير نفس النص غير المجفر عدة مرات، مع إمكانية إعادة تشغيل البروتوكولات التفاعلية عند فشل إنشاء المفتاح فحسب، فإن هذه الأنواع من الحلول لها تكاليف الأداء الخاصة بها.

3.IV الخوارزمية وخصائص التنفيذ

المرونة: بافتراض وجود مستوى جيد عام من الأمن والأداء، فإن المخططات التي تتمتع بقدر أكبر من المرونة ستلبي احتياجات عدد أكبر من المستعملين من المخططات الأقل مرونة، وبالتالي فهي مفضلة.

وقد تشمل بعض أمثلة "المرونة" (على سبيل الذكر وليس الحصر) ما يلي:

1) يمكن تعديل المخطط لتوفير وظائف إضافية تحقق ما هو أبعد من المتطلبات الدنيا لتجفير المفاتيح العمومية، أو آلية تغليف المفاتيح (KEM)، أو التوقيع الرقمي (مثل تبادل المفاتيح غير المتناظرة أو المستيقن منها ضمناً، وما شابه).
2) من السهل تخصيص معلمات المخطط لتلبية مجموعة من أهداف الأمن وأهداف الأداء.
3) يمكن تنفيذ الخوارزميات بأمن وكفاءة على مجموعة متنوعة من المنصات، بما في ذلك البيئات المقيدة، مثل البطاقات الذكية.
4) يمكن موازاة عمليات تنفيذ الخوارزميات لتحقيق أداء أعلى.
5) يمكن دمج المخطط في البروتوكولات والتطبيقات الحالية، مما يتطلب أقل عدد ممكن من التغييرات.

البساطة: سيتم الحكم على المخطط وفقاً لبساطته النسبية في التصميم.

الاعتماد: سيتم النظر في العوامل التي قد تعيق أو تعزز اعتماد أي خوارزمية أو تنفيذها في عملية التقييم، بما في ذلك، على سبيل المثال لا الحصر، الملكية الفكرية التي تغطي خوارزمية ما أو تنفيذها ومدى تيسرها وشروط التراخيص للأطراف المعنية. وسينظر في الضمانات الواردة في البيانات المتوفرة من الجهة (الجهات) المقدمة وأي مالك (مالكين) لبراءات اختراع، مع تفضيل قوي للخوارزميات المقدمة التي توجد بها التزامات بالترخيص، دون تعويض، بموجب شروط وأحكام معقولة وخالية بشكل واضح من أي تمييز غير عادل.

بيبليوغرافيا

[b-ITU-T X.1196] Recommendation ITU-T X.1196 (2012), *Framework for the downloadable service and content protection system in the mobile Internet Protocol television environment.*

[ITU-T X.1197] Recommendation ITU-T X.1197 (2019), *Guidelines on the selection of cryptographic algorithms for IPTV services, Amendment 1*.

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.

[b-ITU-T X.1254] Recommendation ITU-T X.1254 (2012), *Entity authentication assurance framework*.

[b-ITU-T Y.2014] Recommendation ITU-T Y.2014 (2008), *Network attachment control functions in next generation networks.*

[b-ETSI 135 205] ETSI 135 205 V4.0.0 (2001), *Universal mobile telecommunications system (UMTS); LTE;3G security*; Specification of the MILENAGE algorithm set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General.

[b-ETSI 135 231] ETSI 135 231 V12.1.0 (2014), *Universal mobile telecommunications system (UMTS)*; LTE; Specification of the TUAK algorithm set: A second example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: Algorithm specification.

[b-ETSI GR QSC 004] ETSI GR QSC 004 V1.1.1 (2017), *Quantum-safe cryptography; Quantum-safe threat assessment*.

[b-ETSI GR QSC 006] ETSI GR QSC 006 V1.1.1 (2017), *Quantum-safe cryptography (QSC); Limits to quantum computing applied to symmetric key sizes*.

[b-ETSI GS NFV 002] ETSI GS NFV 002 V1.1.1 (2013). *Network functions virtualisation (NFV); Architectural framework*.

[b-ETSI GS NFV-SEC 012] ETSI GS NFV-SEC 012 V3.1.1 (2017), *Network functions virtualisation (NFV) release 3;Security; System architecture specification for execution of sensitive NFV components*.

[b-ETSI GS NFV-SEC 014] ETSI GS NFV-SEC 014 V3.1.1 (2018), *Network functions virtualisation (NFV) release 3; NFV security; Security specification for MANO components and reference points*.

[b-3GPP TS 33.210] 3GPP TS 33.210 V16.2.0 (2019), *3G security; Network domain security (NDS); IP network layer security*.

[b-3GPP TS 33.220] 3GPP TS 33.220, V16.0.0 (2019), *Generic authentication architecture (GAA); generic bootstrapping architecture (GBA)*.

[b-3GPP TS 33.310] 3GPP TS 33.310 V16.2.0 (2019), *Network domain security (NDS); Authentication framework (AF)*.

[b-3GPP TS 33.501] 3GPP TS 33.501, version 16.1.0 (2019), *System architecture for the 5G system*.

[b-3GPP TR 33.841] 3GPP TR 33.841 (2018), *Study on the support of 256-bit algorithms for 5G*.

[b-Häner] Häner, T., Roetteler, M., Svore, K.M. (2017). Factoring using 2*n* + 2 qubits with Toffoli based modular multiplication. *Quantum Information and Computation*, **18**(7-8), pp. 673-684.

[b-Hoffstein] Hoffstein, J., Pipher, J., Silverman, J.H. (1998). NTRU: A ring-based public key cryptosystem. In: Buhler, J.P. (editor), *Algorithmic number theory – ANTS 1998*, pp. 267-288. *Lecture Notes in Computer Science*, volume. 1423. Berlin: Springer.DOI: 10.1007/BFb0054868.

[b-IEEE Std 1363.1] IEEE Std 1363.1-2008, *IEEE Standard Specification for public key cryptographic techniques based on hard problems over lattices*.

[b-IETF RFC 2104] IETF RFC 2104 (1997), *HMAC: Keyed-hashing for message authentication*.

[b-IETF RFC 4279] IETF RFC 4279 (2005), *Pre-shared key ciphersuites for transport layer security (TLS)*.

[b-IETF RFC 4301] IETF RFC 4301 (2005), *Security architecture for the Internet protocol*.

[b-IETF RFC 4303] IETF RFC 4303 (2005), *IP encapsulating security payload (ESP)*.

[b-IETF RFC 4306] IETF RFC 4306 (2005), *Internet key exchange (IKEv2) protocol*.

[b-IETF RFC 4492] IETF RFC 4492 (2006), *Elliptic curve cryptography (ECC) cipher suites for transport layer security (TLS)*.

[b-IETF RFC 4835] IETF RFC 4835 (2007), *Cryptographic algorithm implementation requirements for encapsulating security payload (ESP) and authentication header (AH)*.

[b-IETF RFC 5246] IETF RFC 5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2*.

[b-IETF RFC 5288] IETF RFC 5288 (2008), *AES Galois counter mode (GCM) cipher suites for TLS*.

[b-IETF RFC 5289] IETF RFC 5289 (2008), *TLS elliptic curve cipher suites with SHA-256/384 and AES Galois counter mode (GCM)*.

[b-IETF RFC 5869] IETF RFC 5869 (2010), *HMAC-based extract-and-expand key derivation function (HKDF)*.

[b-IETF RFC 6083] IETF RFC 6083 (2011), *Datagram transport layer security (DTLS) for stream control transmission protocol (SCTP)*.

[b-IETF RFC 6347] IETF RFC 6347 (2012), *Datagram transport layer security version 1.2*.

[b-IETF RFC 6749] IETF RFC 6749 (2012), *The OAuth 2.0 authorization framework*.

[b-IETF RFC 7296] IETF RFC 7296 (2014), *Internet key exchange protocol version 2 (IKEv2)*.

[b-IETF RFC 7515] IETF RFC 7515 (2015), *JSON web signature (JWS)*.

[b-IETF RFC 7516] IETF RFC 7516 (2015), *JSON web encryption (JWE)*.

[b-IETF RFC 7519] IETF RFC 7519 (2015), *JSON web token (JWT)*.

[b-IRTF RFC 8554] IRTF RFC 8554 (2019), *Leighton-Micali hash-based signatures*.

[b-ISO 7498-2] ISO 7498-2:1989, *Information Processing Systems* – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture

[b-ISO/IEC TR 22417] ISO/IEC TR 22417:2017, *Information technology* – Internet of things (IoT) use cases.

[b-Ajtai] Ajtai, M. (1998). The shortest vector problem in L_2 is NP-hard for randomized reductions (extended abstract). In: Vitter, J. (editor). *STOC '98: Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, pp 10–19. New York, NY: Association for Computing Machinery. DOI: 10.1145/276698.276705.

[b-Alkim] Alkim, E., Ducas, L., Pöppelmann, T., Schwabe, P. (2017). Post-quantum key exchange – A new hope, *Cryptology ePrint Archive*, Report 2015/1092. Available [viewed 2020-02-03] at: https://eprint.iacr.org/2015/1092 .

[b-Amy] Amy, M., Di Matteo, O., Gheorghiu, V., Mosca, M., Parent, A., Schanck, J. (2017). Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3. In: Avanzi, R., Heys H. (editors). *Selected areas in cryptography, SAC 2016*, St. Johns, Canada, 2016, pp. 317-337. *Lecture Notes in Computer Science*, volume 10532. Cham: Springer. DOI: 10.1007/978-3-319-69453-5_18.

[b-Banchi] Banchi, L., Pancotti, N., Bose, S. (2016). Quantum gate learning in qubit networks: Toffoli gate without time-dependent control. *npj Quantum Information* **2**, 16019. DOI: 10.1038/npjqi.2016.19. Available [viewed 2020-02-02] at: https://www.nature.com/articles/npjqi201619#ref-link-section-82

[b-Bertoni] Betrtoni, G., Daemen, J., Peeters, M., Van Assche, G. *Keccak sponge function family main document*. Available at: https://keccak.team/obsolete/Keccak-main-1.1.pdf

[b-Bernstein 2009] Bernstein, D.J. (2009). Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete? In: Workshop Record of SHARCS '09: Special-purpose Hardware for Attacking Cryptographic Systems. Available [viewed 2020-02-03] at: https://cr.yp.to/hash/collisioncost-20090517.pdf

[b-Bernstein 2015] Bernstein, D.J., Hopwood, D., Hülsing, A., Lange, T., Niederhagen, R., Papachristodoulou, L., Schneider, M., Schwabe, P., Wilcox-O'Hearn, Z. (2015). SPHINCS: Practical stateless hash-based signatures. In: Oswald, E., Fischlin, M. (editors). *Advances in Cryptology – EUROCRYPT 2015*, pp. 368-397. *Lecture Notes in Computer Science*, volume 9056. Berlin: Springer. DOI: 10.1007/978-3-662-46800-5_15

[b-Buchmann] Buchmann, J., Dahmen, E., Hülsing, A. (2011). XMSS: A practical forward secure signature scheme based on minimal security assumptions. In: Yang, B.-Y. (editor). *Post-quantum cryptography*, pp. 117-129. *Lecture Notes in Computer Science*, volume 7071. Berlin: Springer. DOI: 10.1007/978-3-642-25405-5_8

[b-CSA] Cloud Security Alliance (2017), *Applied quantum-safe security: Quantum-resistant algorithms and quantum key distribution.* Available [viewed 2020-02-03] from: https://cloudsecurityalliance.org/download/applied-quantum-safe-security

[b-Dinh] Dinh, H., Moore, C., Russell, A. (2011). McEliece and Niederreiter cryptosystems that resist quantum Fourier sampling attacks. In: Rogaway, P. (editor). *Advances in cryptology – CRYPTO 2011*, pp. 761-779. *Lecture Notes in Computer Science*, volume 6841. Berlin: Springer. DOI: 10.1007/978-3-642-22792-9_43.

[b-Ding] Ding, J. Schmidt, D. (2005). Rainbow, a new multivariable polynomial signature scheme. In: Ioannidis, J., Keromytis, A., Yung, M. (editors). *Applied Cryptography and Network Security, ACNS 2005*, pp. 164-175. *Lecture Notes in Computer Science*, volume 3531. Berlin: Springer. DOI: 10.1007/11496137_12.

[b-Fowler] Fowler, A.G., Mariantoni, M., Martinis, J.M., Cleland, A.N. (2012). Surface codes: Towards practical large-scale quantum computation. *Physical Review A*, **86**, 032324. DOI: 10.1103/PhysRevA.86.032324. Available [viewed 2020-02-02] at: https://web.physics.ucsb.edu/~martinisgroup/papers/Fowler2012.pdf

[b-Garey] Garey, M.R. Johnson, D.S. (1979). *Computers and intractability: A guide to the theory of NP-completeness*. New York, NY: W.H. Freeman. 338 pp.

[b-Grassl] Grassl, M., Langenberg, B., Roetteler, M., Steinwandt, R. (2016). Applying Grover's algorithm to AES: Quantum resource estimates. In: Takagi T. (editor). *Post-quantum cryptography – PQCrypto 2016*, pp. 29-43. *Lecture Notes in Computer Science*, volume 9606. Cham: Springer. Available [viewed 2020-02-03] at: https://www.microsoft.com/en-us/research/wp-content/uploads/2016/04/1512.04965-1.pdf

[b-Grover] Grover, L.K. (1996). A fast quantum mechanical algorithm for database search. In: *STOC '96: Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, pp 212-219. New York, NY: Association for Computing Machinery. DOI: 10.1145/237814.237866.

[b-Jao] Jao, D., De Feo, L. (2011), Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In: Yang, B-Y. (editor). *Post-quantum cryptography*, pp 19-34. *Lecture Notes in Computer Science*, volume 7071. Berlin: Springer. DOI: 10.1007/978-3-642-25405-5_2.

[b-Kipnis] Kipnis, A., Patarin, J., Goubin, L. (1999), Unbalanced oil and vinegar signature schemes. In: Stern, J. (editor). *Advances in Cryptology – EUROCRYPT '99*. pp. 206-222. *Lecture Notes in Computer Science*, volume 1592. Berlin: Springer. DOI: 10.1007/3-540-48910-X_15.

[b-Lyubashevsky] Lyubashevsky, V., Peikert, C., Regev, O. (2013), On ideal lattices and learning with errors over rings. *Journal of the ACM*, **60**(6), Article No. 43. DOI: 10.1145/2535925.

[b-McEliece] McEliece, R.J. (1978), A *public-key cryptosystem based on algebraic coding theory*. In: *DSN Progress Report*, No. 44, pp. 114–116. Bibcode:1978DSNPR. Available [viewed 2020-02-03] at: https://ipnpr.jpl.nasa.gov/progress_report2/42-44/44N.PDF

[b-Moody] Moody, D. (2019), *NIST status update on elliptic curves and post-quantum crypto*. Gaithersberg, MA: National Institute of Standards and Technology. 20 pp. Available [viewed 2020-02-03] at: https://csrc.nist.gov/CSRC/media/Presentations/NIST-Status-Update-on-Elliptic-Curves-and-Post-Qua/images-media/moody-dustin-threshold-crypto-workshop-March-2019.pdf

[b-Moses] Moses, T. (2009), *Quantum computing and cryptography – Their impact on cryptographic practice*. Minneapolis, MN: Entrust Inc. 12 pp. Available [viewed 2020-02-03] at: https://www.entrust.com/wp-content/uploads/2013/05/WP_QuantumCrypto_Jan09.pdf

[b-NASEM] National Academies of Sciences, Engineering, and Medicine (2018). *Quantum computing: Progress and prospects*. Washington, DC: National Academies Press. 272 pp. DOI: 10.17226/25196.

[b-NIST FIPS 186-4] National Institute of Standards and Technology Federal Information Processing Standard 186-4 (2013), *Digital signature standard (DSS)*. DOI: 10.6028/NIST.FIPS.186-4. Available [viewed 2020-02-03] at: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

[b-NIST FIPS 197] National Institute of Standards and Technology Federal Information Processing Standard 197 (2001), *Specification for the advanced encryption standard (AES)*. Available [viewed 2020-02-14] at: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

[b-NISTIR 8105] National Institute of Standards and Technology Internal Report 8105 (2016), *Report on* post-*quantum cryptography*. Gaithersberg, MA: National Institute of Standards and Technology. 15 pp. DOI: 10.6028/NIST.IR.8105. Available [viewed 2020-02-03] at: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

[b-NISTIR 8240] National Institute of Standards and Technology Internal Report 8240 (2019), *Status* report on the first round of *the NIST post-quantum cryptography standardization process*. Gaithersberg, MA: National Institute of Standards and Technology. 27 pp. DOI: 10.6028/NIST.IR.8240. Available [viewed 2020-02-03] at: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8240.pdf

[b-NIST PQC] National Institute of Standards and Technology Post-Quantum Cryptography: Round 2 – algorithm comparison. Available [viewed 2020-02-14] at:http://hdc.amongbytes.com/post/20190130-pqc-round2/

[b-NIST SP 800-38B] National Institute of Standards and Technology Special Publication 800-38B, *Recommendation for block cipher modes of operation: The CMAC mode for authentication*. Gaithersberg, MA: National Institute of Standards and Technology. 21 pp. DOI: 10.6028/NIST.SP.800-38B. Available [viewed 2020-02-03] at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38b.pdf

[b-NIST SP 800-67] National Institute of Standards and Technology Special Publication 800-67 Rev. 2 (2017), *Recommendation for the triple data encryption algorithm (TDEA) block cipher.* DOI: 10.6028/NIST.SP.800-67r2.

[b-NIST-Sub] National Institute of Standards and Technology. *Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process*. Available [viewed 2020-03-20] at : https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf

[b-ONF TR-511] Open Network Foundation Technical Recommendation 511 (2015), *Principles and practices for securing software-defined networks*. Available [viewed 2020-02-02] at: https://www.opennetworking.org/wp-content/uploads/2014/10/Principles_and_Practices_for_Securing_Software-Defined_Networks_applied_to_OFv1.3.4_V1.0.pdf

[b-QC1] IBM's processor pushes quantum computing closer to 'supremacy' available at: https://www.engadget.com/2017/11/10/ibm-50-qubit-quantum-computer/

[b-QC2] Practical Quantum Computers, available at: https://www.technologyreview.com/s/603495/10-breakthrough-technologies-2017-practical-quantum-computers/

[b-Regev] Regev, O. (2005). On lattices, learning with errors, random linear codes, and cryptography. In: *STOC'05 Proceedings of the 37th Annual ACM Symposium on Theory of Computing*. pp. 84-93. New York, NY: Association for Computing Machinery. DOI: 10.1145/1060590.1060603

[b-Roetteler] Roetteler, M., Naehrig, M., Krysta M. Svore, K.M., Lauter, K. (2017). Quantum resource estimates for computing elliptic curve discrete logarithms. In: Takagi T., Peyrin T. (editors). *Advances in Cryptology – ASIACRYPT 2017*, pp. 241-270. *Lecture Notes in Computer Science*, volume 10625. Cham: Springer. DOI: 10.1007/978-3-319-70697-9_9. Available [viewed 2020-02-02] at: https://www.microsoft.com/en-us/research/wp-content/uploads/2017/09/1706.06752.pdf

[b-Schneier] Schneier, B. (1994). The Blowfish encryption algorithm. *Dr. Dobb's Journal*, 19(4), pp. 38-40. Available [viewed 2020-02-03] from: https://www.drdobbs.com/security/the-blowfish-encryption-algorithm/184409216

[b-Shor 1997] Shor, P.W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5), pp. 1484–1509. DOI: 10.1137/S0097539795293172

[b-Shor 1999] Shor, P.W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev*. 41(2), pp. 303-332. DOI: 10.1137/S0036144598347011.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2021