CYBERSEC 2025 臺灣資安大會 | 4/15-4/17 臺北南港展覽二館

PQC Forum

後量子密碼論壇

量子電腦對行動通訊身份安全的威脅與量子安全網路的重要性

The Threats of Quantum Computers to the Security of Subscription Concealed Identifier (SUCI) and the Importance of Quantum Safe Network

TEAM CYBERSECURITY

蔡宜學 博士 Dr. Yi-Hsueh Tsai

Cyber Security Technology Institute
Institute for Information Industry

Senior Technical Manager

National Taipei University of Technology

Assistance Professor (Part-Time)

yihsuehtsai@g.ntu.edu.tw; yihsueh.tsai@mail.ntut.edu.tw

財團法人資訊工業策進會
INSTITUTE FOR INFORMATION INDUSTRY

Outline

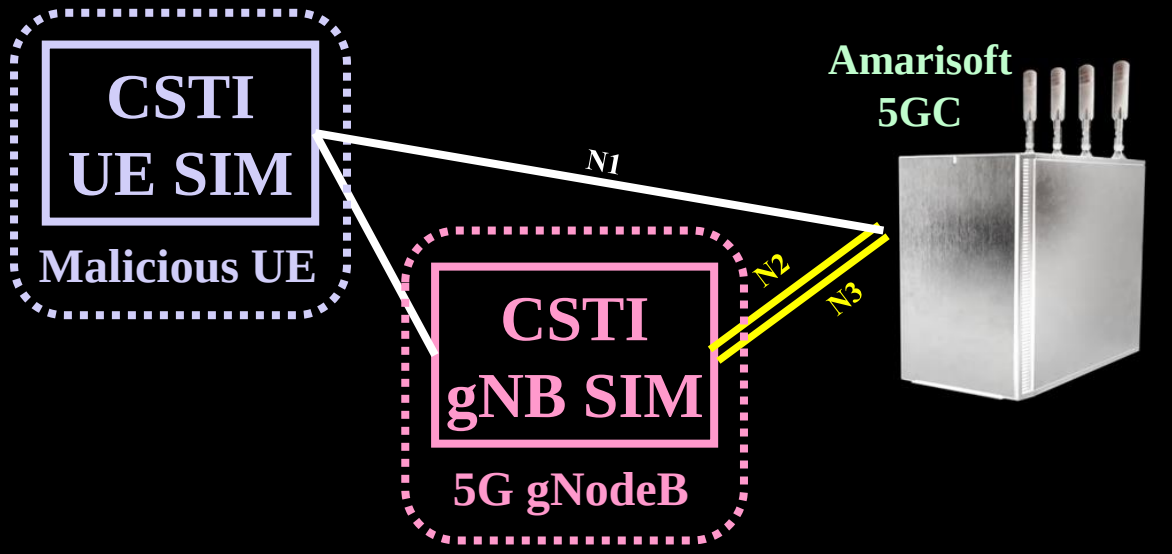
- **How to acquire the list of SUPI stored in the database of 5GC UDM?**
  - Experiment & Demo
  - Summit findings to GSMA CVD program and SA3 Working Group
- **Enabling Quantum Safe Network in the 3GPP SA1 Working Group**
- **Strengthening SUPI Security in 5G Core Networks for Non-Public Applications**
- **Harnessing the Potential of IBM Quantum Computers with Qiskit**
- **How to Leverage Generative AI for Effective Programing on QSN**
- **Conclusion**

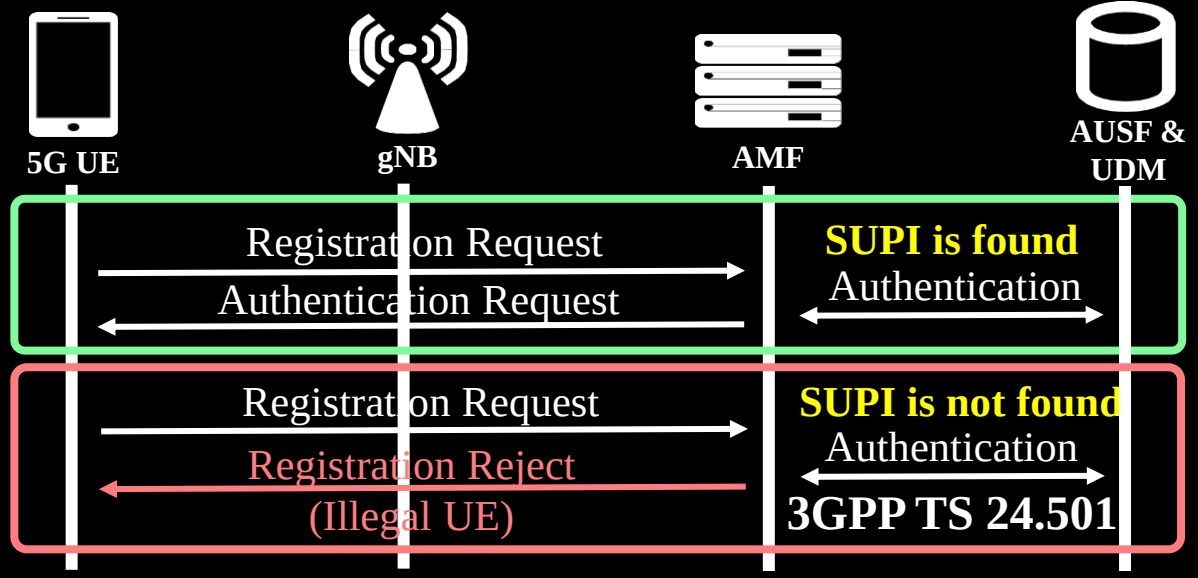
Acquire the list of SUPI stored in the database of 5GC UDM

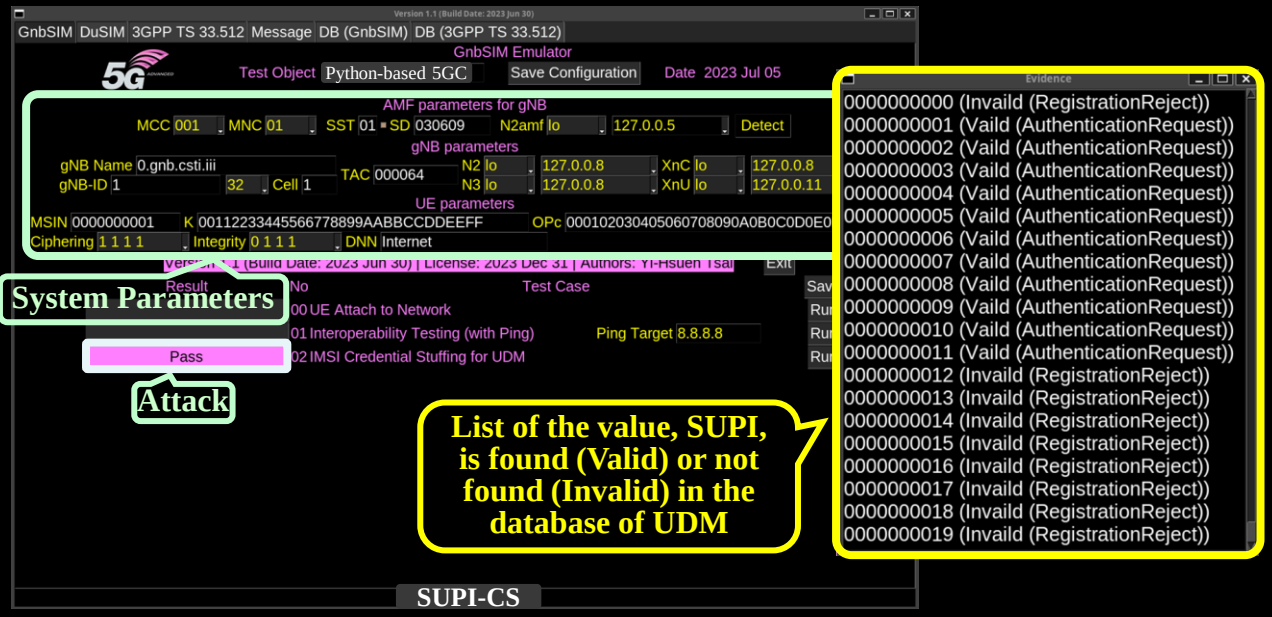
UE and gNB Emulator

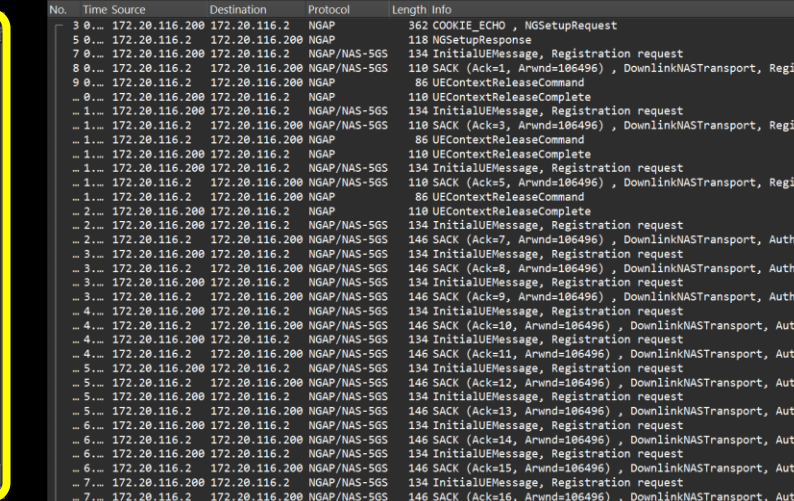
5GC

How to acquire the list of SUPI

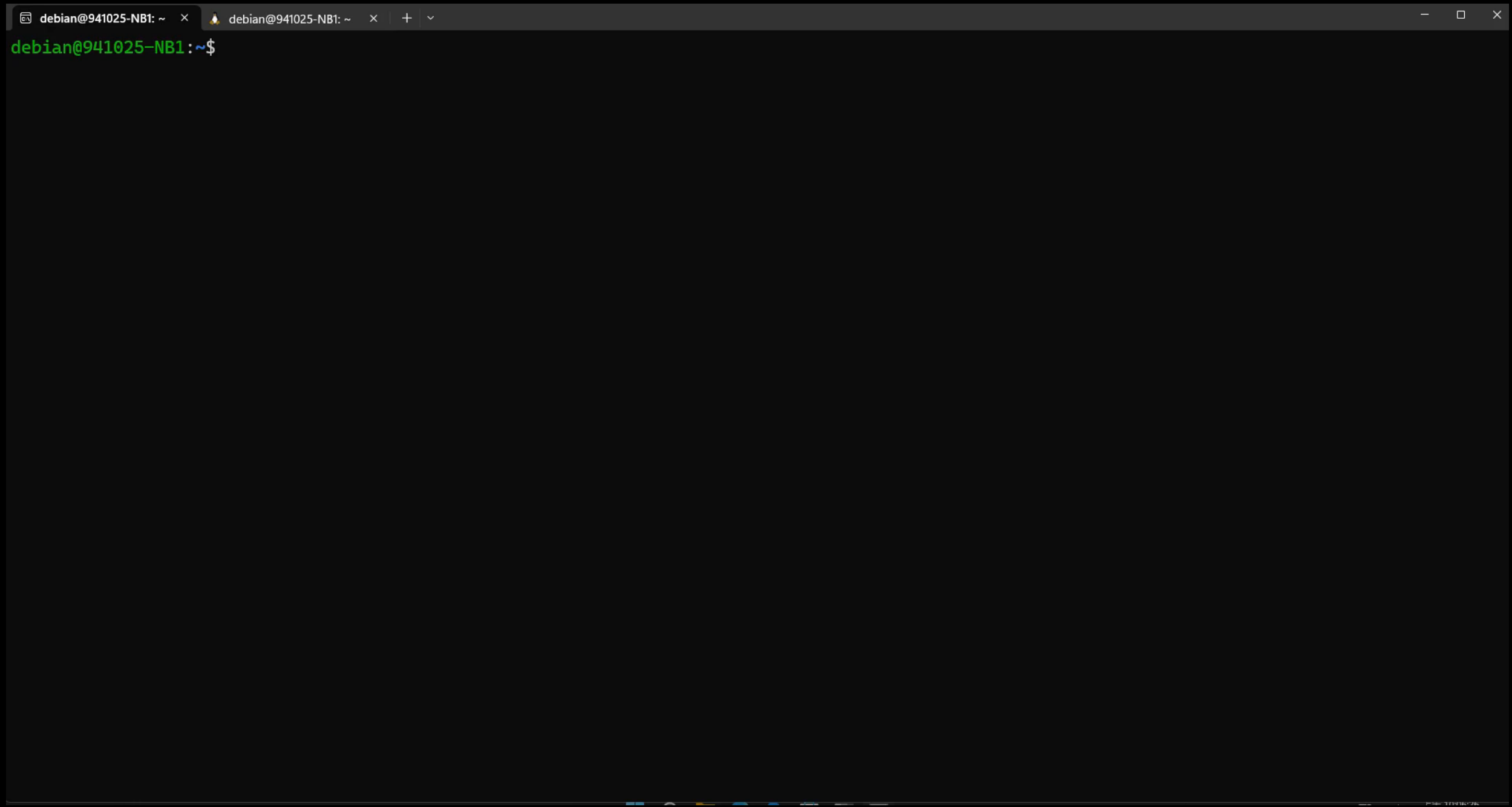








List of the value, SUPI, is found (Valid) or not found (Invalid) in the database of UDM



Submit the findings to the GSMA CVD program

GSMA Coordinated Vulnerability Disclosure

Document Template – WORD Format

Reporter Details	
Name (either full or nickname): ***(Mandatory Field)***	Yi-Hsueh Tsai
Organisation	Institute for Information Industry
Email ***(Mandatory Field)***	lucas@iii.org.tw
Telephone	+886266078962, +18586337590
Can we provide your name to the vendor if required	No ☐ Yes ☒
Do you want to be publicly acknowledged	No ☐ Yes ☒
Vulnerability Details ***(All below are mandatory fields)***	
Title of Vulnerability	
Acquiring the list of SUPI stored in the database of 5GC UDM	
Description of Vulnerability	

According Annex A.1 of 3GPP TS 24.501, the 5GMM cause, Cause #3 – Illegal UE, is sent to the UE when the network refuses service to the UE either because an identity of the UE is not acceptable to the network or because the UE does not pass the authentication check.

Therefore, the UE will receive Registration Reject with Cause, Illegal UE, after sending Registration Request with SUPI, which the value is not found in the database of UDM.

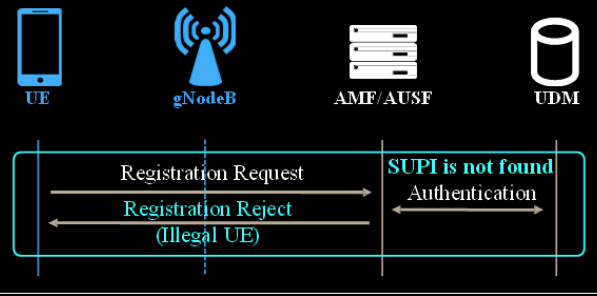


Figure 1: SUPI is not found in UDM

According 4.4.4.2 of 3GPP TS 24.501, except the messages listed below, no NAS signalling messages shall be processed by the receiving 5GMM entity in the UE or forwarded to the 5GSM entity, unless the network has established secure exchange of 5GS NAS messages for the NAS signalling connection: … b) AUTHENTICATION REQUEST; …

Therefore, the UE will receive Authentication Request after sending Registration Request with SUPI, which the value is found in the database of UDM.

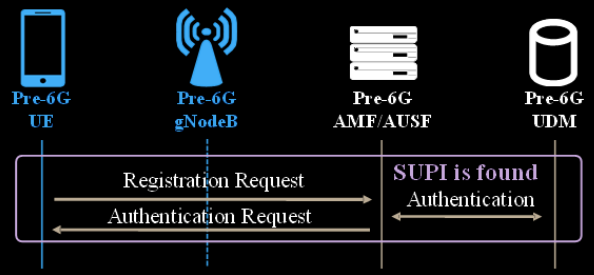


Figure 2: SUPI is found in UDM

The attacker could acquire the list of SUPI stored in the database of 5GC UDM by recently sending Registration Request with increased value of SUPI. For non-public network (NPN), there are a few SUPI stored in the database of 5GC UDM, therefore the attacker could perform future attack to UE in the list of SUPI.

The following test is performed over N1 interface via N2 Interface of gNB/UE emulator. The same result will be obtained over N1 interface via NR-Uu air interface of UE emulator.

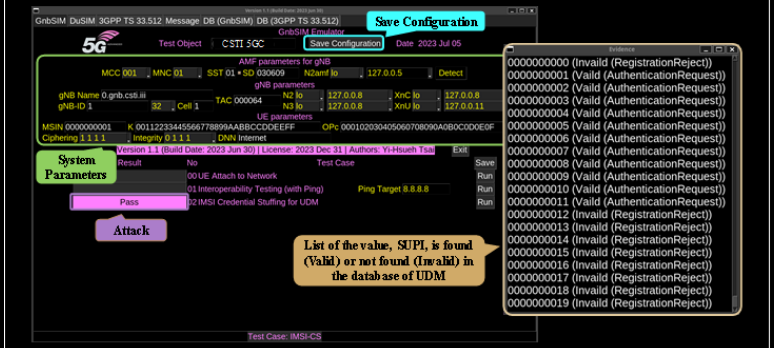
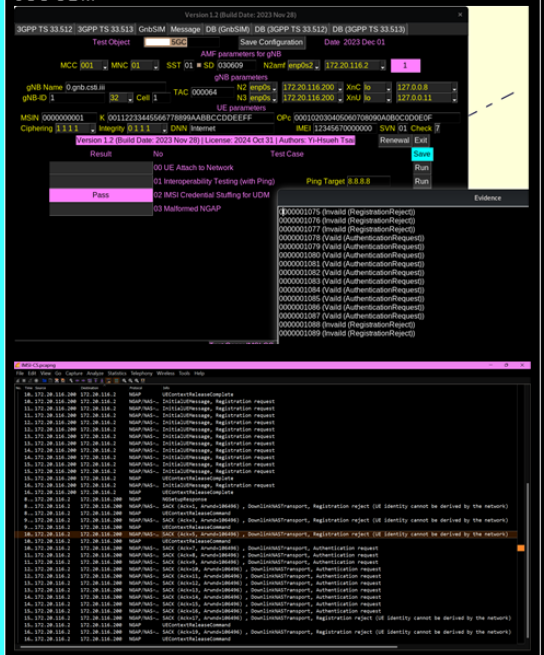


Figure 3: Demonstration of Acquiring the list of SUPI stored in the database of 5GC UDM

Suggested Mitigation:

The 5GC should send Authentication Request instead of Registration Reject with Cause, Illegal UE to UE, after receiving Registration Request with SUPI, which the value is not found in the database of UDM. And then sending Authentication Failure to UE, after receiving Authentication Response from UE.

Product or Service Name	5GC
Date Vulnerability Found	5 Jun 2023
Is the Vulnerability still live	No ☐ Yes ☒
Do you believe the vulnerability is being currently exploited	No ☐ Yes ☒
Probability of reproduction of vulnerability	1 – Always ☒ 2 – Often ☐ 3 – Rarely ☐
Possible threat caused by the vulnerability	Acquiring the list of SUPI stored in the database of 5GC UDM for non-public network (NPN)
Can you provide any PoC Code, Screenshots or Http requests etc.	Filed Test of Acquiring the list of SUPI stored in the database of 5GC UDM
Do you intend to let us review the vulnerability before going public	No ☒ Yes ☒



Source: http://www.3gpp.org/specifications/coordinated-vulnerability-disclosure-cvd

Response from GSMA CVD program

RE: CVD: Acquiring the list of SUPI stored in the database of 5GC UDM for non-public network (NPN)

Hi Lucas, [redacted]

Thank[redacted] the CVD panel feel they now have enough information to assess the case fully and would like to thank you for bringing this [redacted]

[redacted]roblem as well as the proposed mitigation. Their conclusion is that the case is identical to the one studied in 3GPP [redacted] [redacted]ution would bring its own problems [redacted]riticality than the actual problem it tries to solve. This is in line with the [redacted]n by 3GPP as well. The panel se[redacted] [redacted]rting the procedure to change the [redacted]r enumeration has been present in all mobile technologies, starting w[redacted] [redacted]erefore it shall be considered a[redacted] [redacted]nt mobile network.

[redacted]y be needed is an update to a GSMA document as we feel the issue you [redacted] not be documented very well. It [redacted] [redacted]anning and deployment of a mobile [redacted]are of this risk.

Fi[redacted] we continue to [redacted]r 2 other CVD cases on N4 interfaces and False base stations and expect to be back in contact soon on those.

Kind Regards,
Roger Brown

GSMA

[redacted]
Security Services Manager
[redacted]

gsma.com

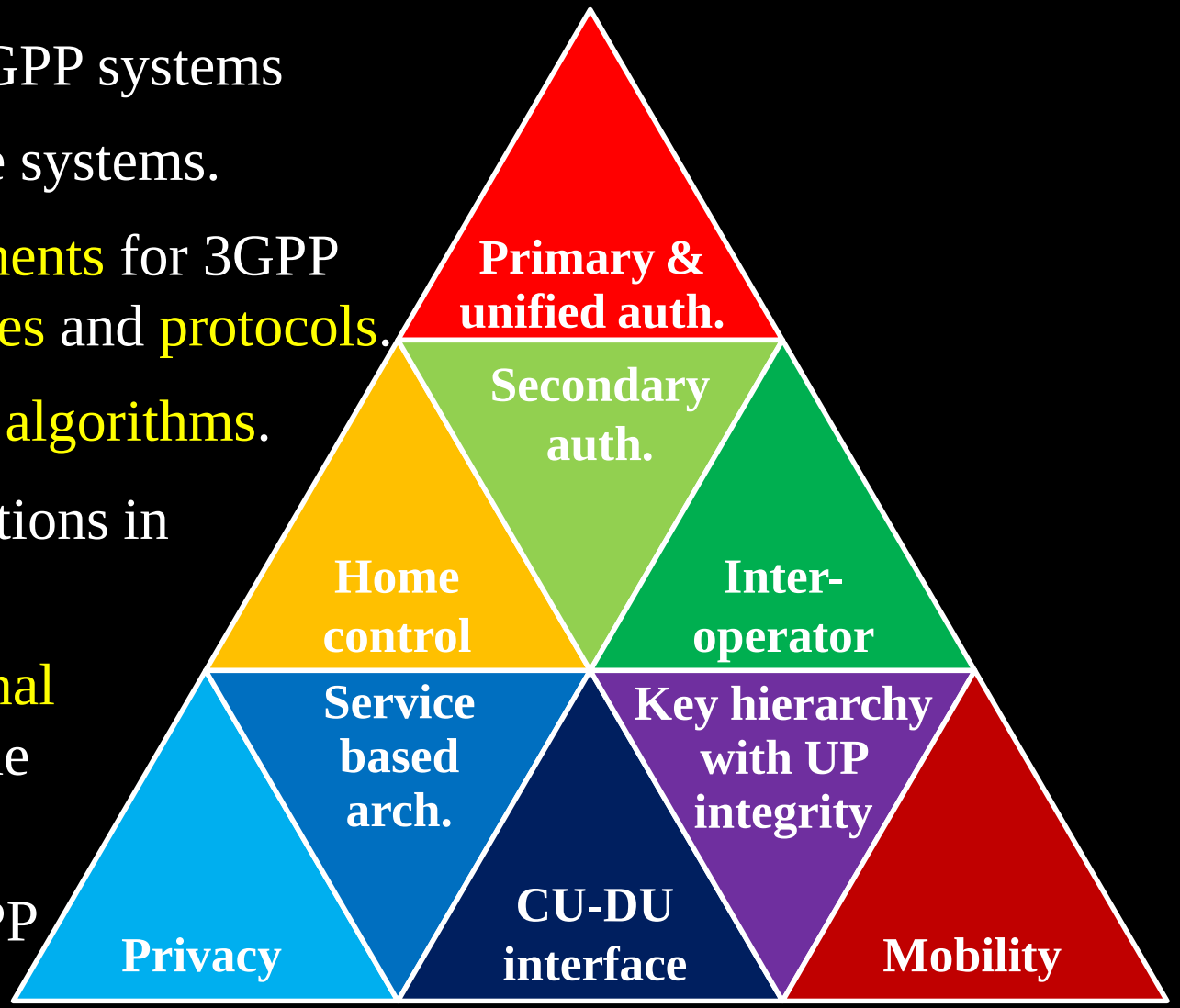
Coordinated Vulnerability Disclosure (CVD) submission

Coordinated Vulnerability Disclosure (CVD) submission form

Your real name or nickname (*)	Anne Onimus	This field is mandatory, but you can use an alias if you wish to remain anonymous.
Your organization		e.g. employer
Your email address (*)		Need not be a corporate address, you can use, for example, gmail. You can supply a dummy email address, but in that case we will not be able to contact you concerning your submission.
Can we provide your name and email address to the Group which will be tasked with investigating your submission?	☐ **No, I do not wish you to provide my coordinates to the Group.**	The investigating Group may wish to contact you for clarification or supplementary information, so it is highly recommended that you allow them to do so.
Do you want to be publicly acknowledged as the author of this submission?	☐ **No, I do not wish to be acknowledged as the author of this submission.**	If you wish to be acknowledged, make sure you have supplied a valid email address above.
Subject of the vulnerability (*)		Brief but meaningful
Vulnerability details (*)		Give as full a description as possible.
3GPP Technical Specifications implicated		List here any Specifications which might need to be updated to correct the vulnerability, if you can identify them.
Approximate date the vulnerability was identified, format YYYY-MM-DD. (*)	When was the vulnerability identified?	
Repeatability	○ **always** ○ **often** ○ **sometimes** ○ **rarely**	Is the vulnerability easy to reproduce?
Possible threat caused by the vulnerability		Be as explicit as possible
Supporting file	Browse...	You may upload a file containing supporting material (diagrams, timings, supplementary text, ...). Acceptable file types are: .txt, .doc, .docx, .jpg .
Do you intend to go public with this information before we have reviewed it?	☐ **Yes, I have already made / intend to make details of this vulnerability public without leaving sufficient time for 3GPP to resolve the problem.**	We really hope you will say "no" !
List any other organizations to which you have reported or intend to report this vulnerability		We will coordinate with those organizations if aappropriate.
I am not a robot (*)	xgvk	Type the characters you can see in the design
	Refresh	
	By submitting this form, you are agreeing to the use of the data you have provided for the appropriate processing of your declaration. All data will be treated in accordance with the 3GPP privacy policy.	
Submit your CVD declaration.	SUBMIT	

3GPP TSG SA WG3 Security and Privacy

1. Responsibility for security and privacy in 3GPP systems
2. Perform analysis of potential threats to these systems.
3. Determine the security and privacy requirements for 3GPP systems, and specify the security architectures and protocols.
4. Ensure the availability of any cryptographic algorithms.
5. Accommodate any regional regulatory variations in security objectives and priorities.
6. Accommodate as far as is practicable, regional regulatory requirements that are related to the processing of personal data and privacy.
7. Requirements for lawful interception in 3GPP systems.



3GPP SA3#116 Meeting

Proposal for Discussion on Prevent acquiring the list of SUPI at the SA3 #116

3K 3GPP [redacted]

To: **+1 other** Sat 5/11/2024 7:57 PM

Cc: [redacted] **+4 others**

Dear [redacted],

Thank you for your guidance on the SUPI attack issue. Following your suggestion, I have prepared a contribution for the **SA3 #116** meeting, focusing on enhancing security against SUPI guessing attacks, especially under null-scheme conditions in NPN environments.

The proposal is titled "Prevent acquiring the list of SUPI stored in the database [redacted]DM" and has been submitted for discussion at the upcomi[redacted]ing. It suggests modifications to 3GPP TS 24.501 to mitig[redacted]ks by potentially issuing a Registration Reject under spe[redacted]tions.

I would appreciate your [redacted]sights and any further recommendations on this matter. The document can be accessed here for a more detailed view:
https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_116_Jeju/Docs/S3-241712.zip.

Best regards, [redacted]

Dear [redacted]

Thanks for sharing the discussion paper.
Observation 1 is related to the interation wit[redacted]PLMNNPN_Sec[redacted]ed to have UE impacts, I am not sure if PLMNNPN_[redacted]ght place to d[redacted]

BR,
[redacted]

Dear [redacted]
Thank you for your feedback on our discussion paper. I would like to clarify an important as[redacted] of our proposal. The focus of the security enhancements discussed, particularly regarding the integrity of the SUPI list in the 5GC UDM database, is strictly on strengthening the network's defenses against potential security threats.

Our proposal does not advocate for changes to UE behavior or interactions. Instead, it aims to enhance the security measures at the network level, such as implementing robust encryption and improving access controls. These measures are designed to protect the network and its users without altering how UEs operate or interact within the network.

We believe this clarification helps align our discussion with the intended scope of enhancing network security without impacting UE functionalities. We believe that discussing the practical implementation of these security measures would be highly beneficial and would appreciate if we could explore this further in a CT 1 session to align our approach effectively.

Best regards,
[redacted]

3GPP TSG-SA3 Meeting #116
Jeju, South Korea, 20th - 24th May 2024

S3-241712

Source: ISSDU, III, NYCU
Title: Prevent acquiring the list of SUPI stored in the database of 5GC UDM
Document for: Discussion
Agenda Item: 5.3

1 Decision/action requested

Endorse the proposal and recommend CT1 to modify 3GPP TS 24.501 based on the observation in this contribution.

2 References

[1] 3GPP TS 33.501, Security architecture and procedures for 5G system; (Release 18)

[2] 3GPP TS 24.501, Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3 (Release 18)

3 Rationale

In accordance with 3GPP TS 33.501, null-scheme should be implemented such that it returns the same output as the input, which applies to both encryption and decryption. This ensures that when using the null-scheme, the SUCI (Subscription Concealed Identifier) does not conceal the SUPI (Subscription Permanent Identifier) and therefore the newly generated SUCIs do not need to be fresh, maintaining the network's integrity and preventing unauthorized access.

The concerns highlighted in Annex A.1 of TS 24.501, particularly regarding Cause #3 – Illegal UE, when the network refuses service to the UE either because an identity of the UE such as SUPI is not acceptable to the network or because the UE does not pass the authentication checks. However, these issues are not thoroughly addressed the security of the context in UDM database, especially for NPN, where the risk of multi-UE, under null-scheme conditions considering Registration Reject, could be more pronounced.

Refer to Section 4.4.4.2 of TS 24.501, NAS signaling messages received by the 5GMM entity within the UE, or relayed to the 5GSM entity, should not be processed, except when a secure exchange of 5GS NAS messages has been established for the NAS signaling connection, specifically including the Authentication Request message.

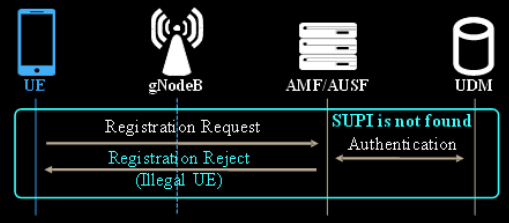


Figure 1: SUPI is not found in UDM

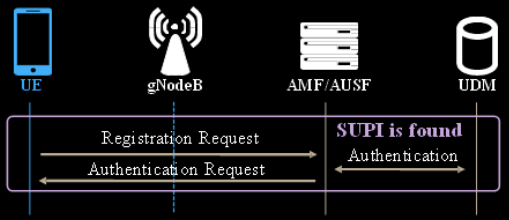
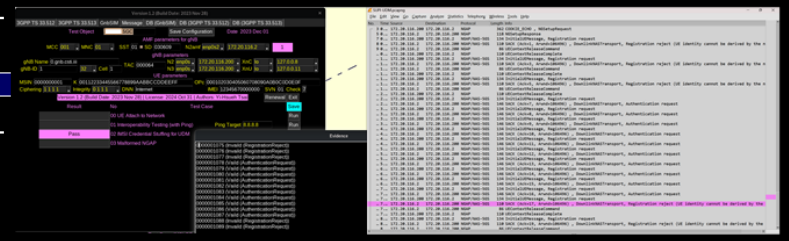


Figure 2: SUPI is found in UDM

These figures illustrate the difference between cases where the UDM has the SUPI of the UE and where it does not. The SUPI is a globally unique identifier for the subscriber that can be either concealed or not concealed by the UE. When the UDM possesses the SUPI, it can authenticate the UE and authorize network access. When the UDM does not have the SUPI, it needs to request it from another UDM.

In the simulation, a Registration Request containing SUPI is sent through the N1 interface via the N2 interface from a gNB/UE emulator. Identical results are achieved when sending a Registration Request with SUPI through the N1 interface via the NR-Uu air interface from a UE emulator.



(a) Demonstration of filed Test (b) Evidence of pcap log

Figure 3: Acquiring the list of SUPI stored in the database of 5GC UDM

Test results from gNB/UE emulators using N1 and N2 interfaces show that the integrity of the SUPI list in the 5GC UDM database is susceptible to malicious attacks in NPN configurations. Specific adjustments to the Registration Request message and enhanced security measures are crucial to reduce cybersecurity risks.

TS 24.501 should clarify that robust encryption and improved access control significantly reduce the risk of SUPI threats, as demonstrated by tests on the NR-Uu air interface with UE emulators. Ensuring the security of the SUPI list is essential as it protects customer information, prevents unauthorized network access, and preserves the uniqueness of each customer. Under conditions applying the null-scheme, considering a Registration Reject scenario, enhancing the protection of the SUPI when concealed is necessary to secure the data from unauthorized access.

Observation1: The risk of attacks on the SUPI list in 5GC UDM databases shows the need for stronger security, like better encryption and access control. These steps are important to keep subscriber information safe and ensure data safety in the network, especially with the null-scheme.

In NPN scenarios, the application of the null-scheme exposes a significant security vulnerability by not encrypting the SUPI. To mitigate this risk, it is recommended that when a registration request is received using the null-scheme, the network should promptly issue a Registration Reject response. Therefore, under conditions applying the null-scheme and considering a scenario of NPN, the UE will only receive an Authentication Request if the SUCI is found in the UDM database.

NPN network to reject a registration request if it uses the null-scheme might not be the best way. This could wrongly block real users from accessing the network, which would make their experience worse and slow down the network. It is crucial to develop more nuanced mechanisms that distinguish between genuine security threats and normal user requests to minimize unnecessary disruptions and maintain robust network performance.

Observation2: We should get support from SA3 and keep the discussion going in CT1 to make sure we find a balance between keeping the network safe and keeping it user-friendly.

Proposal: 3GPP TS 24.501 should specify that in order to prevent acquiring the list of SUPI stored in the database of 5GC UDM, the NPN network should send Registration Reject with Cause #3 (Illegal UE) after receiving the Registration Request using the null-scheme.

4 Conclusion and Proposal

Observation 1: The risk of attacks on the SUPI list in 5GC UDM databases shows the need for stronger security, like better encryption and access control. These steps are important to keep subscriber information safe and ensure data safety in the network, especially with the null-scheme.

Observation2: We should get support from SA3 and keep the discussion going in CT1 to make sure we find a good balance between keeping the network safe and keeping it user-friendly.

Proposal: 3GPP TS 24.501 should specify that in order to prevent acquiring the list of SUPI stored in the database of 5GC UDM, the NPN network should send Registration Reject with Cause #3 (Illegal UE) after receiving the Registration Request using the null-scheme.

S3-241712	Prevent acquiring the list of SUPI stored in the database of 5GC UDM	ISSDU, III, NYCU	discussion	Endorsement	Yes	Ye[redacted]noted	No	
S3-242510	Draft TR 33.757	China Telecom	draft TR	Approval	No	Yes	[redacted] approval	No	

SA3 Relevant TRs for QSC (3GPP SA1#106 Meeting)

3GPP TR 33.841 V16.1.0 (2019-03)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and Systems Aspects;
Security aspects;
Study on the support of 256-bit algorithms for 5G
(Release 16)

Support of 256-bit algorithms

Comparison of conventional and quantum security levels of some popular ciphers

Algorithm	Key Length	Effective Key Strength / Security Level	
		Conventional Computing	Quantum Computing
RSA-1024	1024 bits	80 bits	0 bits
RSA-2048	2048 bits	112 bits	0 bits
ECC-256	256 bits	128 bits	0 bits
ECC-384	384 bits	256 bits	0 bits
AES-128	128 bits	128 bits	64 bits
AES-256	256 bits	256 bits	128 bits

3GPP TR 33.700-41 V0.1.0 (2024-03)

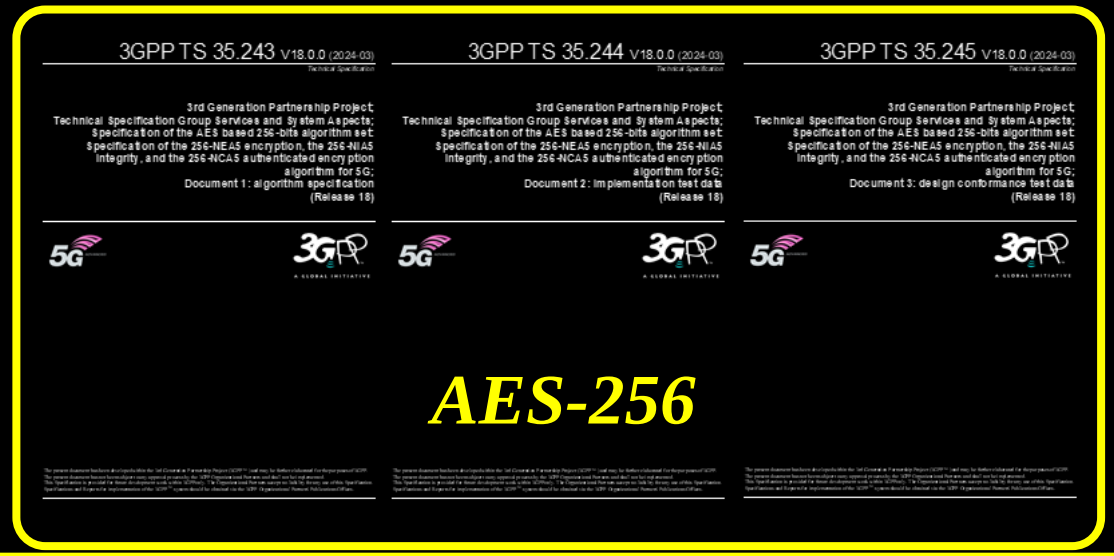
Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Study on enabling a cryptographic algorithm transition to 256-bits
(Release 19)

Enabling a cryptographic algorithm transition to 256-bits

SA3 Relevant TSs for QSC (3GPP SA1#106 Meeting)

SNOW 5G



AES-256

ZUC-256

MILENAGE-256

Why we need migration to QSC? (3GPP SA1#106 Meeting)

- As specified in clause 6.12.2 of 3GPP TS 33.501, the SUCI is generated using a protection scheme such as **Elliptic Curve Integrated Encryption Scheme (ECIES)** with the Home Network public key.
- The main vulnerability of the ECIES protocol with respect to the quantum threat is actually the **Diffie-Hellman key exchange** step, regardless of the used profile.

Post Quantum Cryptography – Guidelines for Telecom Use Cases

Version 1.0

22 February 2024

Source: GSA PQ.03 Post Quantum Cryptography Guidelines for Telecom Use v1.0

3GPP SA1#106 Meeting (email discussion)

This is Steve [redacted] "GE [redacted] rk Technologies" in 3G[redacted]
I was interes[redacted] 3GPP agenda item as it rela[redacted]
We would be [redacted] discussing this topic with [redacted]
TCON.
Let me know if you would be i[redacted]ested in following up via Teams perhaps?

Dear [redacted],

Thank you for re[redacted]pressing interest in our 3GPP agenda item rela[redacted]
We are very inte[redacted]g this topic with you and would like to arrange a te[redacted]a Teams. Given the potential time difference, could you please prov[redacted]some available times for you? We will do our best to accommodate[redacted]ur schedule.
Looking forward to your response.

Best regards,
[redacted]

[redacted],

Sorry for my confusion, I also sent a Teams invitation for ET Fri 5/24 8AM, which corresponds to TST Fri 5/24 8PM. I canceled it and will use yours.

Some questions to discuss:

- Who is endorsing this Study Item besides the following (they all seem to be from Taiwan)?
  - Information Security Service Digital United Inc.
  - Institute for Information Industry
  - National Yang Ming Chiao Tung University
- Can you include concerns about the [redacted]plexity of classical Post-Quantum Cryptography being [redacted]propriate for industrial (control system) use? A[redacted]ve less overhead and provides warning [redacted]
- I think QKD will be tough to get ap[redacted] be willing to help support it.
  - I think you need to get the big co[redacted]rd with the proposal? But either way, the discussion will be [redacted]esting.

We can talk more at our meeting.

Thanks,
[redacted]

Hi [redacted],

Thank you for your interest and support regarding the company's view for 6G. Here are my short responses to your questions:

1. **Supporters List**: We are actively seeking additional support from both international and local companies. We hope you can provide more suggestions and resources in this regard.
2. **Concerns about Classical Post-Quantum Cryptog[redacted]**: include these concerns in the propos[redacted]e advantages of Quantum Key Distrib[redacted]e scenarios, particularly its lower s[redacted]d ability to provide warnings of attacks.

We are planning to revise the S1-24[redacted]9 according to your suggestions and submit the new versi[redacted] SA1. Your insights are invaluable, and we would like to invite yo[redacted]co-source this contribution with us. Would you be available and willing to collaborate more closely on this?

Looking forward to discussing this further in our meeting.

Best regards,

You may also want to consider hybrid QKD/QSC – that is, a combination of post-quantum cryptography (classical) and QKD (quantum).
This could be a 3rd topic area if you [redacted]

...just a thought.

Hi [redacted],

Thank you for suggesti[redacted] QKD/QSC a[redacted]
combination of post-q[redacted]QKD
(quantum). I've added t[redacted]arked i[redacted]
red.

If you think the hybrid approa[redacted]an
propose it at the next SA1 meeting[redacted]ppy to s[redacted]it.

I'll send the revised document to Alain for a new tdoc number.
Thanks again for your suggestion.

Best regards,
[redacted]
Technical Manager, Ph.D
Network Technologies & Operations | EVP office

[DRAFT]Revision of S1-241059 - Enable Quantum-Safe Cryptography for 6G

Hi all,

I have revised S1-241059 to incorporate new ideas from GE Network Technologies. As a result, it has been assigned a new tdoc number: S1-241240.

The changes to the content (indicated by red text) are as follows:

- Addition of the idea from GE Netw[redacted]gies.
- Added a new sectio[redacted]page 7: "[redacted]Quantum Key Distributi[redacted]
- Proposal: Cor[redacted]post[redacted]yptography (classical) a[redacted]m).

I will upload the rev[redacted]t in the inbox at the start of the meeting.

Best regards,

RE: [S1-241240]Revision Submission and Agenda Update

3K [redacted]
To: **+1 other**
Cc: 蔡宜學 Yi-Hsueh Tsai; **+2 others**
Thu 5/30/2024 11:02 AM

Hi [redacted],

Thank you for your email.

Regarding S1-241240 being "Noted," I wanted to update you on the developments from yesterday's report. Several companies were initially set to speak, but the chairperson stopped them, indicating that the discussion should be moved to SA3. However, we believe that SA1 is an appropriate forum to present usage requirements.

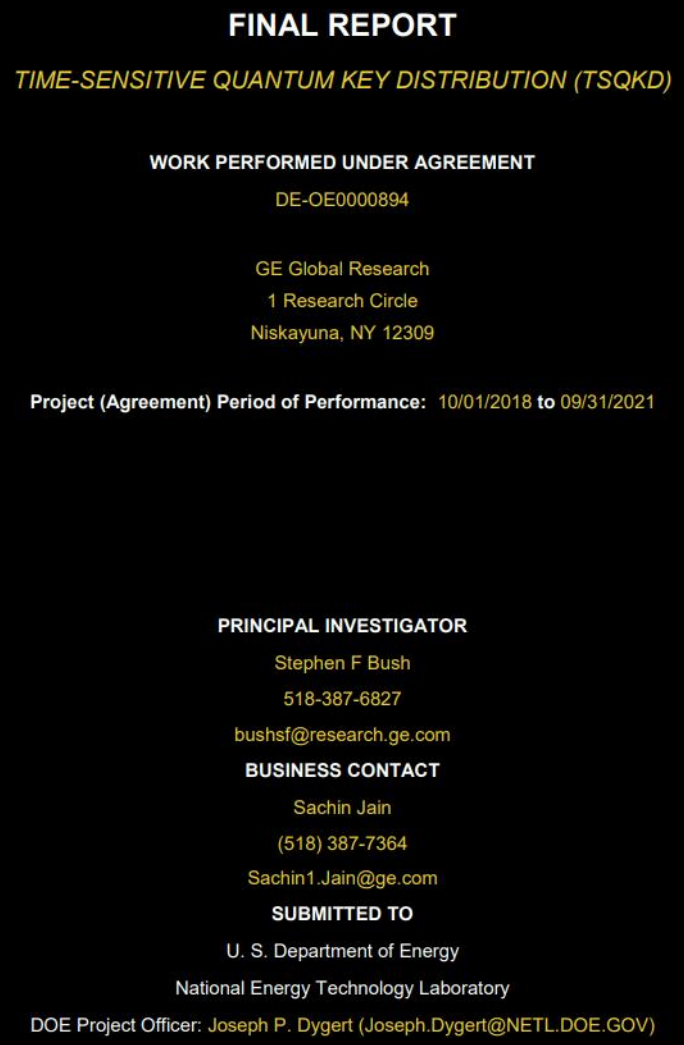
In the August SA1 meeting, a study ite[redacted]established. I am considering whether GE Network Technologies cou[redacted]ffort with support from other major companies. We propose to start d[redacted]se cases from November onwards.

[redacted]se let me know your thoughts on this approach and if there are any specific [redacted]you would recommend.

Best regards,
[redacted]

Why we need migration to QSC? (3GPP SA1#107 Meeting)

- Therefore, we are concerned that the increasing complexity of implementing **PQC**, as this may be too slow and unacceptable for time sensitive **industrial control** system application.
- Introducing **Quantum Key Distribution (QKD)** technology could reduce overhead, shortens latency, and provides warnings of eavesdropper attacks.



FINAL REPORT

TIME-SENSITIVE QUANTUM KEY DISTRIBUTION (TSQKD)

WORK PERFORMED UNDER AGREEMENT

DE-OE0000894

GE Global Research
1 Research Circle
Niskayuna, NY 12309

Project (Agreement) Period of Performance: 10/01/2018 to 09/31/2021

PRINCIPAL INVESTIGATOR

Stephen F Bush
518-387-6827
bushsf@research.ge.com

BUSINESS CONTACT

Sachin Jain
(518) 387-7364
Sachin1.Jain@ge.com

SUBMITTED TO

U. S. Department of Energy
National Energy Technology Laboratory
DOE Project Officer: Joseph P. Dygert (Joseph.Dygert@NETL.DOE.GOV)

Source: Bush, Stephen F., "Time-Sensitive Quantum Key Distribution (TSQKD)"

3GPP SA1#107 & SA1#108 Meetings

- **Collaborating with 3GPP delegates from AT&T, GE, and FET**
- **S1-242083: Quantum-Safe Network for 6G mobile networks**
  - **Post-Quantum Cryptography** (PQC) to protect 6G system communication
  - **Quantum Key Distribution** (QKD) to provide secure key management for ultra-low-latency small-data-rate communication for critical applications
- **The 6G system shall provide security protection for communication against the potential attacks posed by quantum computing.**

8 Rel-20 6G contributions				
8.1 SID contributions (official template)				
WID	S1-242292	Neutral Editor, SA1 chair	6G SID initial draft	Revised to S1-242450
WID	S1-242450	Neutral Editor, SA1 chair	6G SID initial draft	Revised to S1-242452
WID	S1-242452	Neutral Editor, SA1 chair	6G SID initial draft	Revised to S1-242499
WID	S1-242499	Neutral Editor, SA1 chair	6G SID initial draft	Revised to S1-242525
WID	S1-242525	Neutral Editor, SA1 chair	6G SID initial draft	Revised to S1-242545
WID	S1-242545	Neutral Editor, SA1 chair	6G SID initial draft	Agreed
Cont	S1-242300	Neutral Editor, SA1 chair	Extracts of 6G SID objectives from SID-related contributions	Noted
WID	S1-242083	III, AT&T, GE Network Technologies, ISSDU	Proposal for 6G SID: Quantum-Safe Network (QSN)	Merged into S1-242292
Cont	S1-242126	III, GE Network Technologies, ISSDU	Motivation for 6G SID: Quantum Safe Network (QSN)	Noted

3GPP TSG- SA1 Meeting # 107 S1-242083
Maastricht, The Netherlands, 19-23 August 2024

Source:	III, AT&T, GE Network Technologies, ISSDU	
Title:	Proposal for 6G SID: Quantum-Safe Network (QSN)	
Document for:	Approval	
Agenda Item:	8.1	
Contact:	Yi-Hsueh Tsai	lucas@iii.org.tw
	Stephen F Bush	stephen.bush@ge.com
	Feng-Ming Yang	kelvinfomi@issdu.com.tw

3GPP™ Work Item Description

Information on Work Items can be found at http://www.3gpp.org/Work-Items
See also the 3GPP Working Procedures, article 39 and the TSG Working Methods in 3GPP TR 21.900

Title: Proposal for 6G SID: Quantum-Safe Network (QSN)

Acronym: FS_6G

Unique identifier:

[Leave blank]

Potential target Release: Rel-20

1 Impacts

Affects:	UICC apps	ME	AN	CN	Others (specify)
Yes		X	X	X	
No					
Don't know	X				

2 Classification of the Work Item and linked work items

2.1 Primary classification

This work item is a …

X	Study
	Normative – Stage 1
	Normative – Stage 2
	Normative – Stage 3
	Normative – Other*

* Other = e.g. testing

2.2 Parent Work Item

For a brand-new topic, use "N/A" in the table below. Otherwise indicate the parent Work Item.

Strengthening SUPI Security in 5G Core Networks for Non-Public Applications

IEEE Communications Standards Magazine

Strengthening SUPI Security in 5G Core Networks for Non-Public Applications

Yi-Hsueh Tsai
National Taipei University of Technology
yihsuehtsai@g.ntu.edu.tw

Shiang-Jiun Chen*
National Taipei University of Technology
annette@ntut.edu.tw

corresponding author: * annette@ntut.edu.tw

***Abstract** - This study addresses key security challenges in managing the Subscription Permanent Identifier (SUPI) within 5G Non-Public Networks (NPNs). Existing 3GPP standards, optimized for public networks, leave private networks vulnerable to risks such as unauthorized SUPI access and systematic guessing attacks. To address these issues, we propose several enhancements, including adaptive access controls, measures to prevent the vulnerabilities associated with the null-scheme, and the adoption of post-quantum cryptography to safeguard sensitive subscriber data. Our methodology combines simulation-based vulnerability assessments with targeted countermeasures to reduce SUPI-related security risks. The results highlight a significant reduction in potential attack vectors, providing practical recommendations for improving privacy and data security within 5G NPNs. By aligning with ongoing 3GPP standardization efforts, our work offers a forward-looking framework to mitigate emerging threats, particularly as quantum computing becomes a critical concern.*

Index Terms – SUCI, NPN, Security, Privacy, and PQC

Introduction

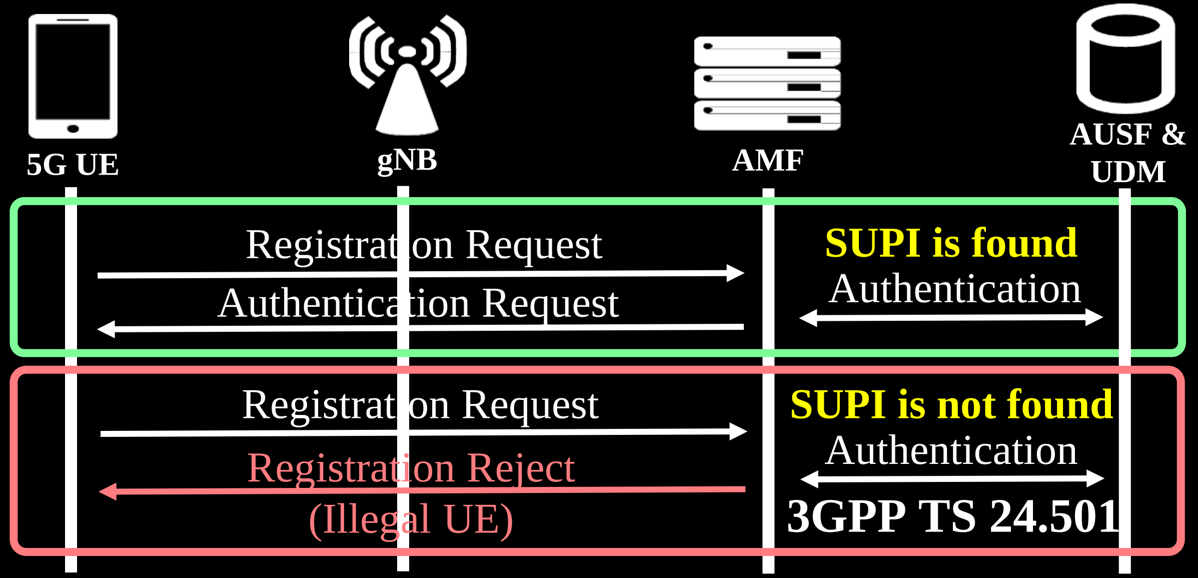
5G technology marks a significant leap forward in wireless communication, providing unprecedented data rates, reduced latency, and the capacity to support extensive device connectivity [1, 2]. This advancement paves the way for transformative applications across diverse domains, including augmented reality, autonomous vehicles, smart cities, and the Internet of Things (IoT) [3]. Among the notable developments within the 5G ecosystem is the emergence of Non-Public Networks (NPNs), which are tailored to meet the unique needs of industries, enterprises, and private organizations [4]. NPNs offer enhanced control, security, and customization options often unavailable in public 5G environments, making them ideal for industrial automation, innovative infrastructure, healthcare, and logistics applications. These characteristics ensure improved reliability, minimized latency, and enhanced data confidentiality—essential for mission-critical operations [5].

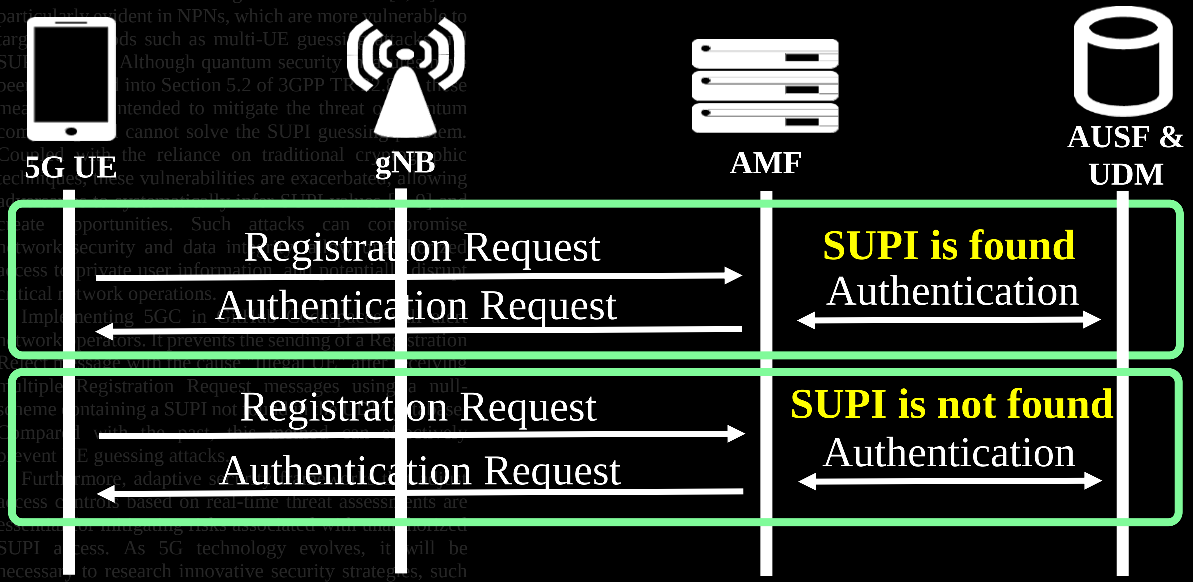
However, a central challenge in NPNs is the safeguarding of sensitive subscriber information, particularly the Subscription Permanent Identifier (SUPI), within the 5G Core (5GC) Unified Data Management (UDM) database. The SUPI serves as a unique identifier for each subscriber in the 5G network, making it an attractive target for cyberattacks. Unauthorized access to SUPI data can lead to severe privacy breaches, enabling attackers to track users, intercept communications, or manipulate network access controls.

The limitations of existing 3GPP standards [6, 7] are particularly evident in NPNs, which are more vulnerable to targ[illegible]ds such as multi-UE guess[illegible] SU[illegible] Although quantum security [illegible] bee[illegible] into Section 5.2 of 3GPP TR [illegible] these mea[illegible]ntended to mitigate the threat o[illegible]ntum com[illegible] cannot solve the SUPI guessin[illegible]em. Coupled with the reliance on traditional cry[illegible]phic techniques, these vulnerabilities are exacerbated, allowing adv[illegible] create [illegible]pportunities. Such attacks can compromise network security and data int[illegible] access to private user information [illegible] disrupt critical network operations.

Imple[illegible]nting 5GC in [illegible] network operators. It prevents the sending of a Registration Reject message with the cause "Illegal UE" after receiving multiple Registration Request messages using a null-scheme containing a SUPI not [illegible] Compared with the past, this [illegible] prevent [illegible]E guessing attacks.

Furthermore, adaptive se[illegible] access controls based on real-time threat assessments are essential for mitigating risks associated with unauthorized SUPI access. As 5G technology evolves, it will be necessary to research innovative security strategies, such as post-quantum cryptography protocols [9], to protect SUPI data against emerging threats. The continuous development of global policies and standards will also play a critical role in ensuring that NPNs maintain a strong

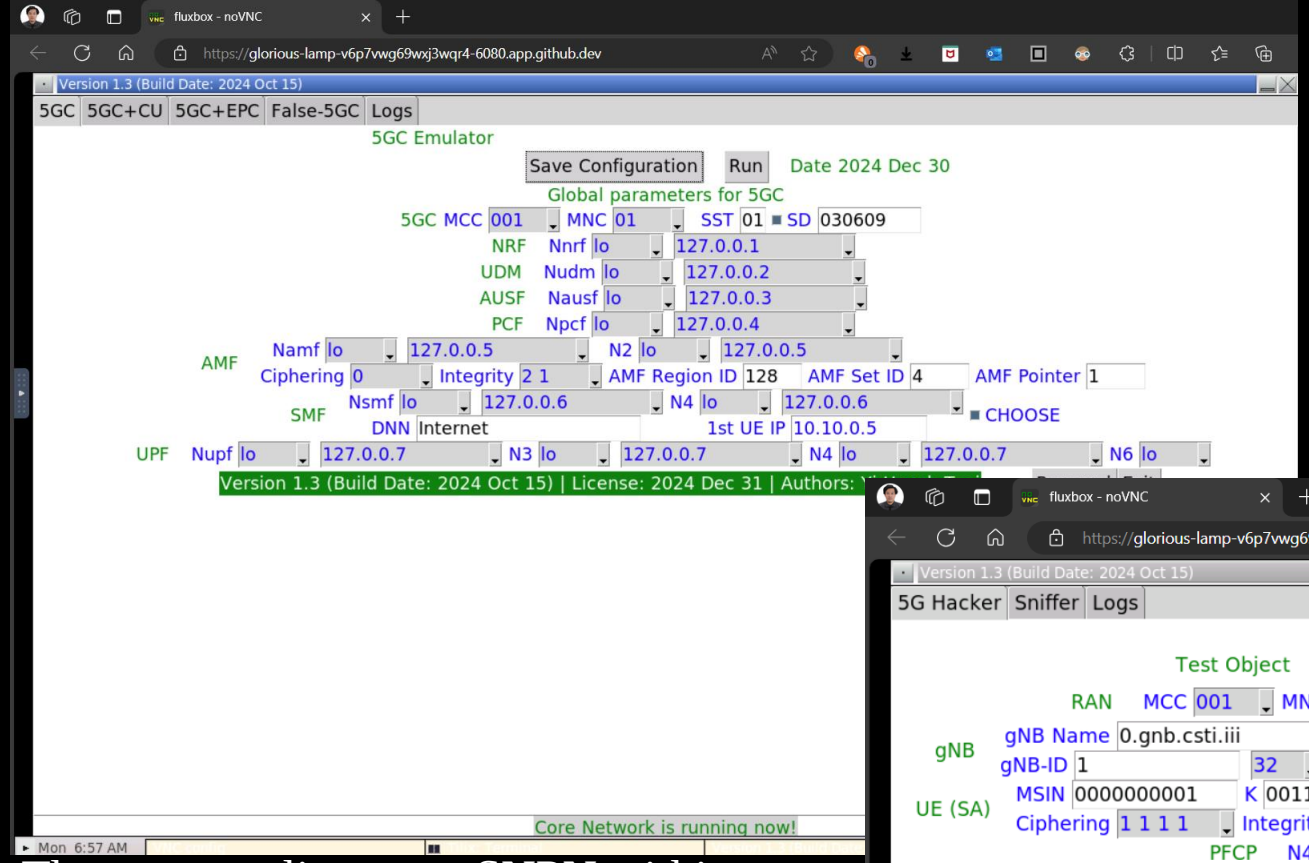


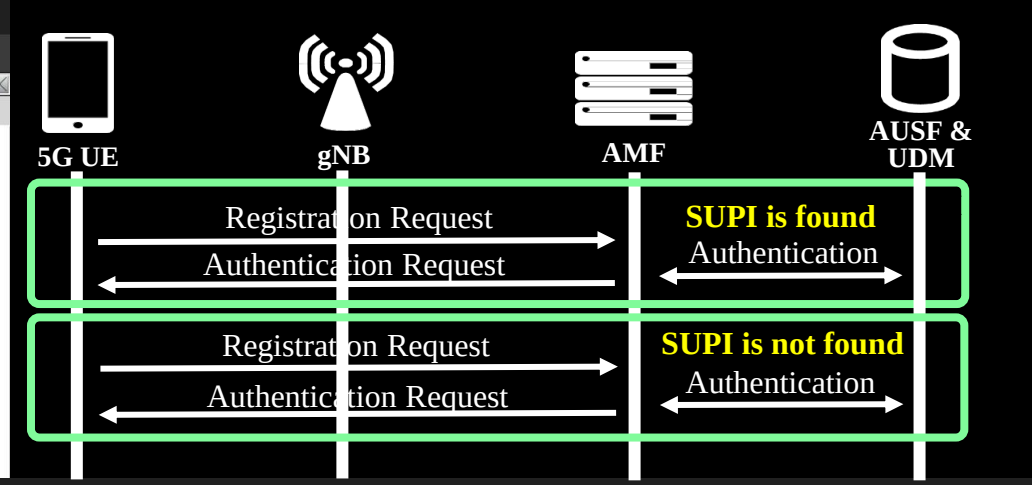


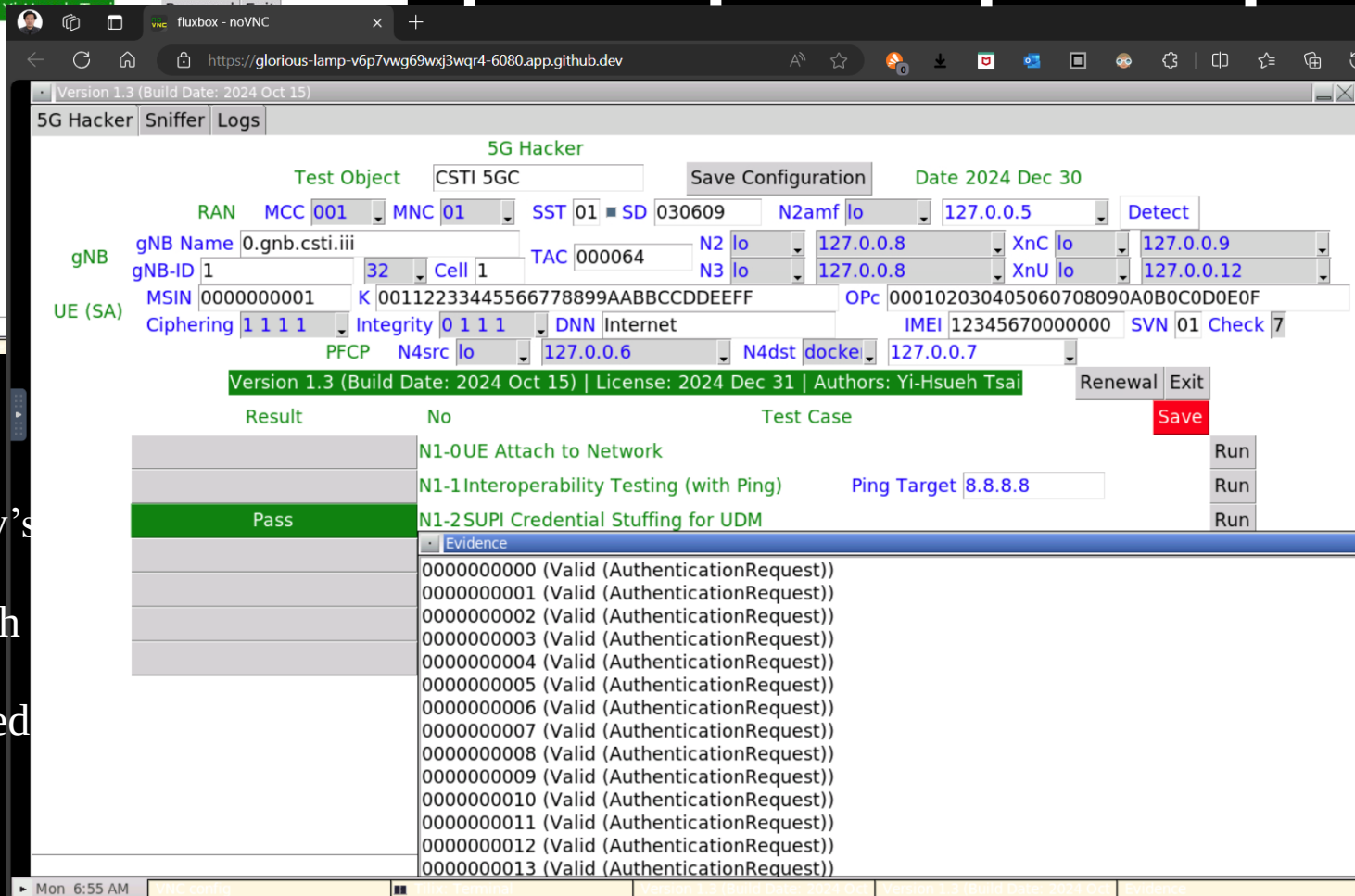
- Accept with Minor Revisions (06-Feb-2025)

■普通級

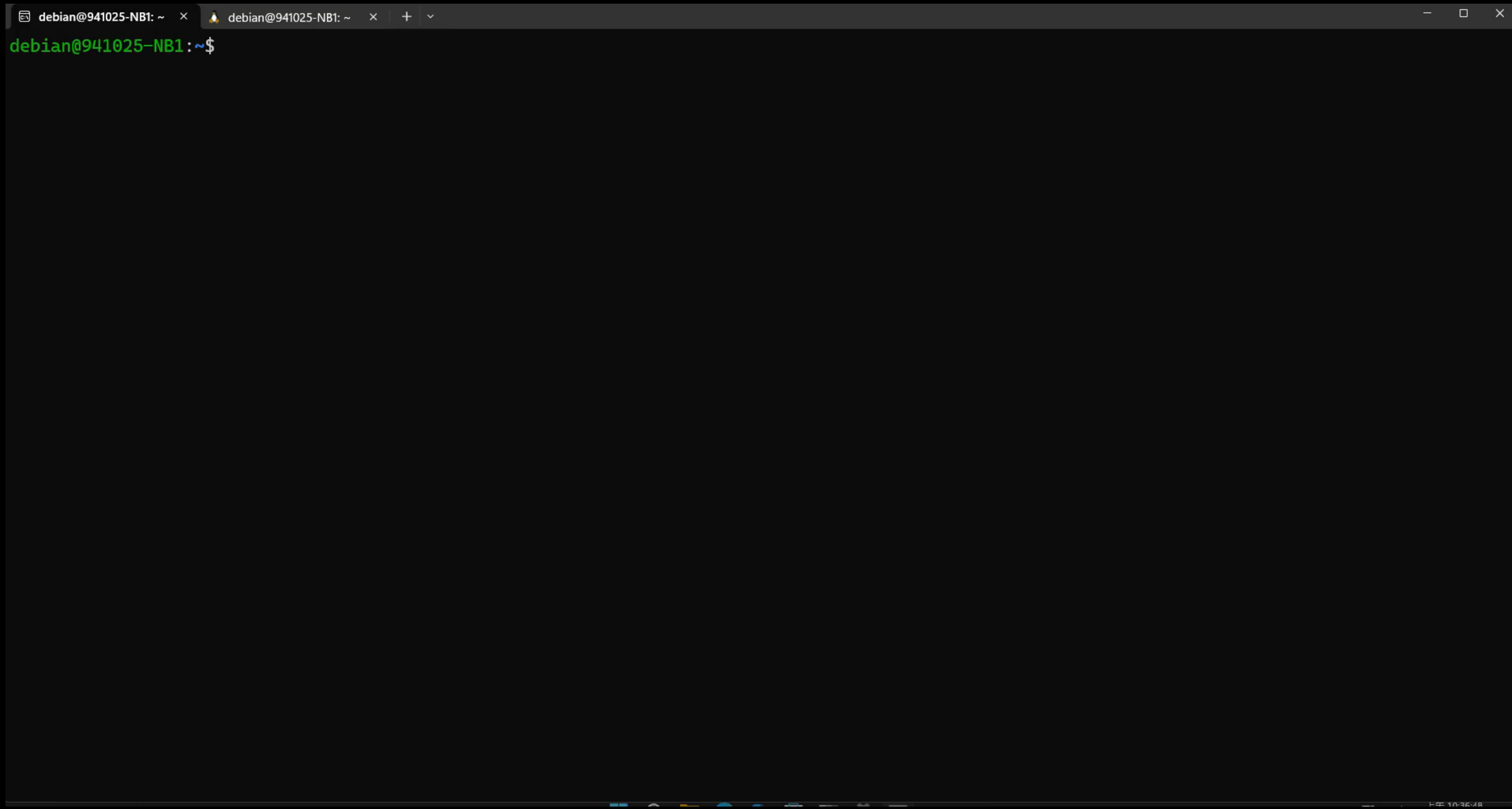
Secure Handling of Registration Request



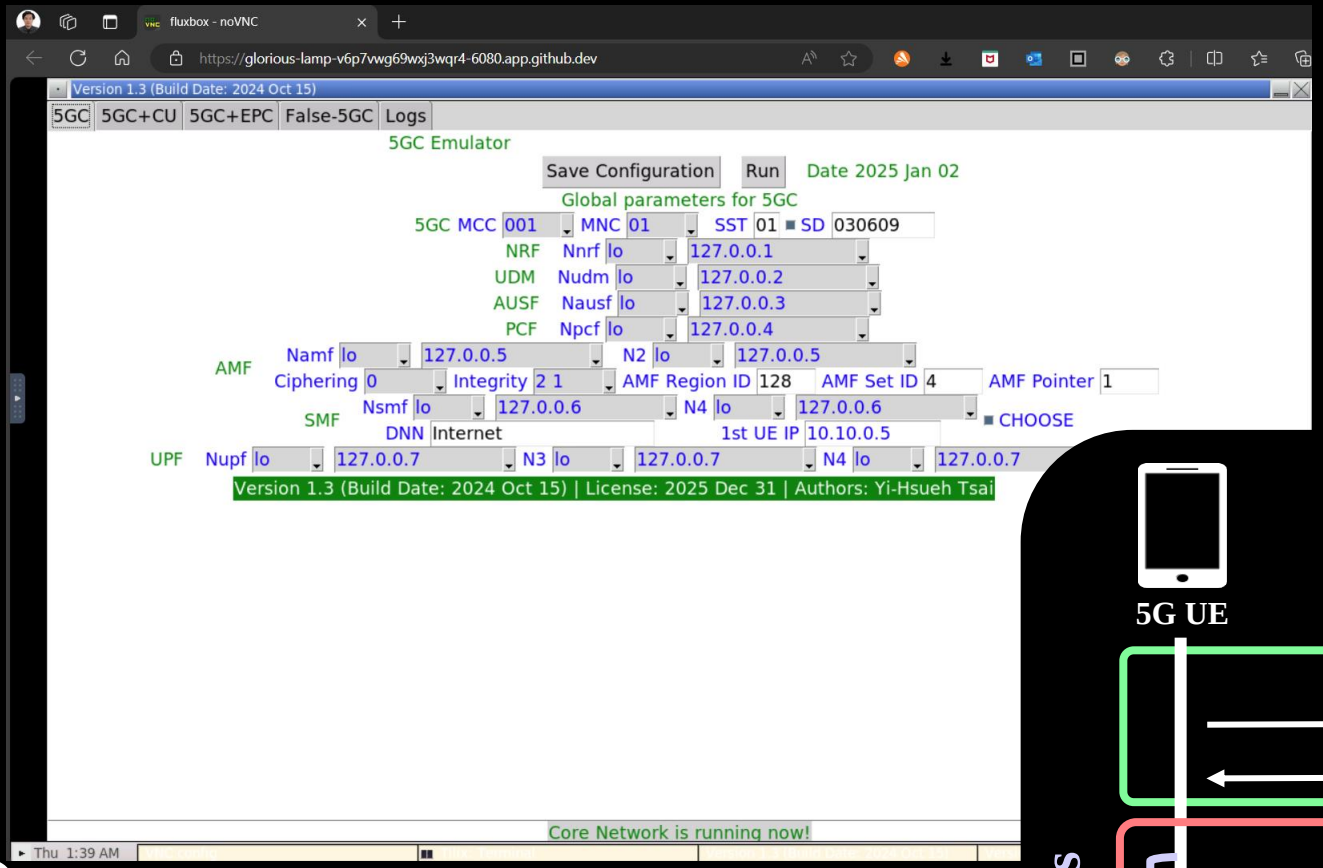




The setup replicates an SNPN within an emulated private network using GitHub Codespaces. It uses Python-based gNB and 5GC emulators, developed with P1 Security's pycrate library, to simulate the operator's infrastructure. If a Registration Request with a SUPI not found in the UDM database is received, an Authentication Request is issued instead of a Registration Reject with the cause "Illegal UE."

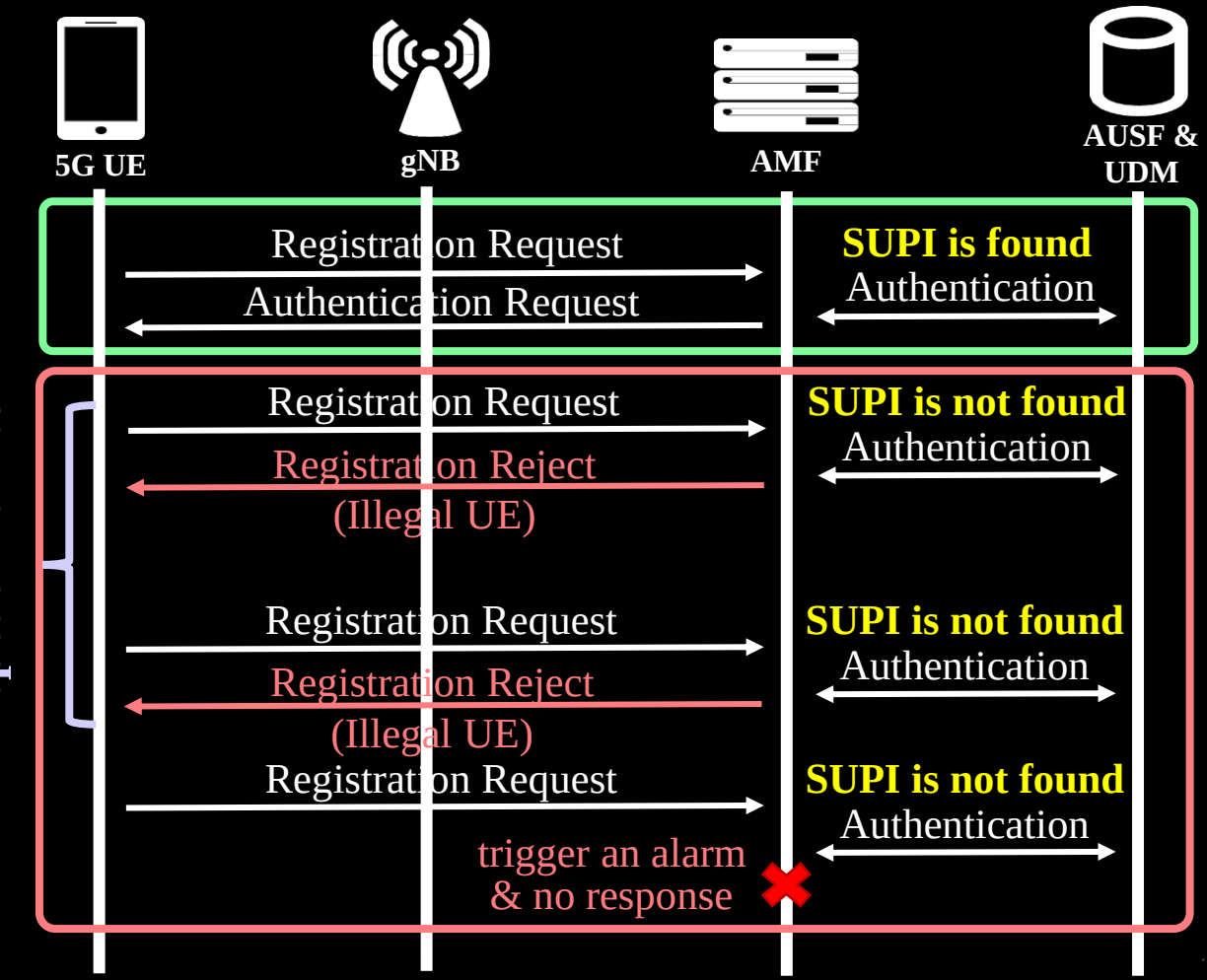


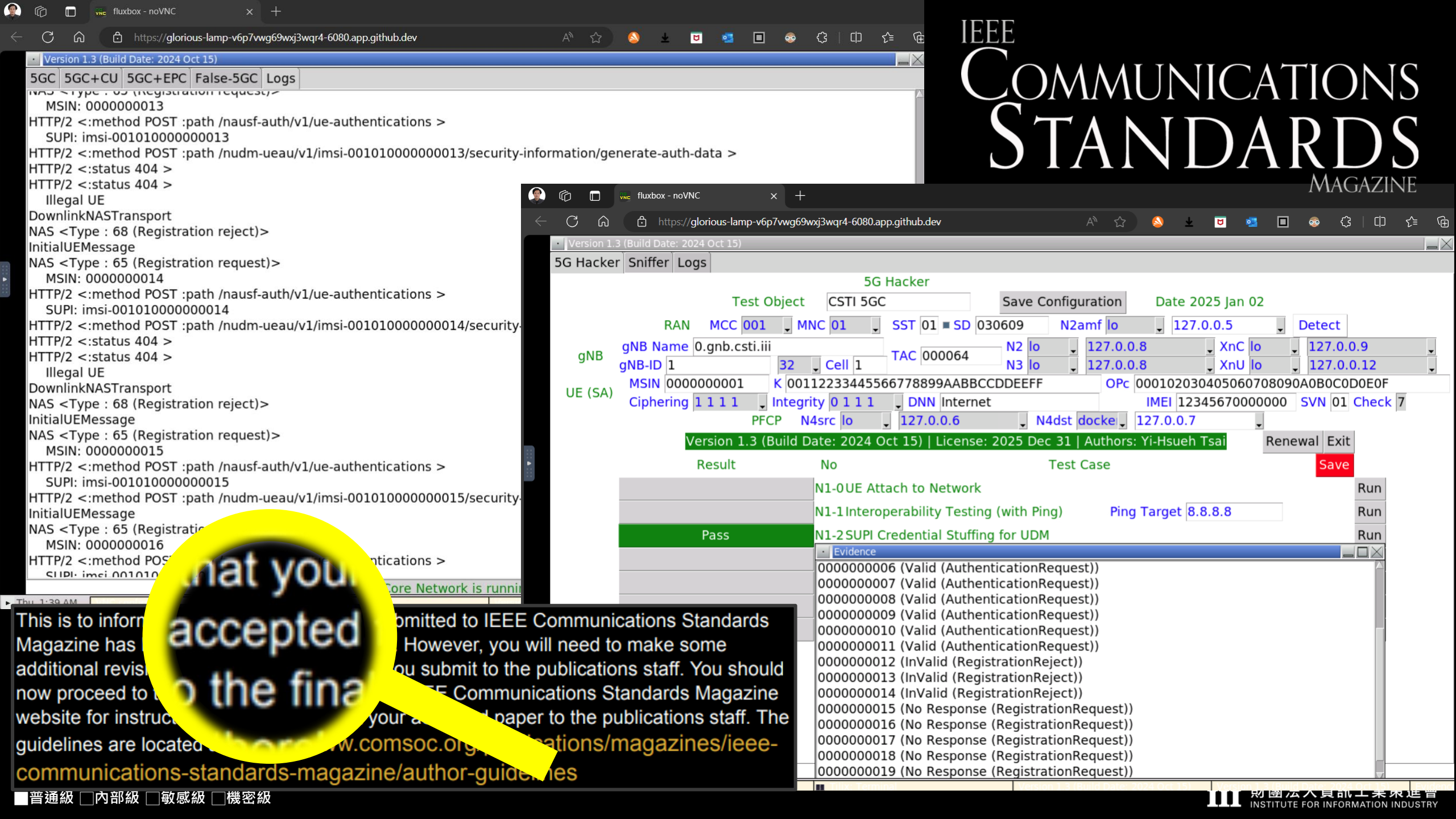
Demonstration of SUPI Security Mechanisms



Our implementation replicates an emulated private network environment using a Python-based 5GC emulator to simulate the operator's infrastructure. These emulators are developed using P1 Security's pycrate Python library.

We recommend that the 5GC trigger an alarm to the network operator and refrain from sending a Registration Reject with the cause "Illegal UE" after receiving multiple Registration Request messages.




fluxbox - noVNC
https://glorious-lamp-v6p7vwg69wxj3wqr4-6080.app.github.dev
Version 1.3 (Build Date: 2024 Oct 15)
5GC
5GC+CU
5GC+EPC
False-5GC
Logs
MSIN: 0000000013
HTTP/2 <:method POST :path /nausf-auth/v1/ue-authentications >
SUPI: imsi-001010000000013
HTTP/2 <:method POST :path /nudm-ueau/v1/imsi-001010000000013/security-information/generate-auth-data >
HTTP/2 <:status 404 >
HTTP/2 <:status 404 >
Illegal UE
DownlinkNASTransport
NAS <Type : 68 (Registration reject)>
InitialUEMessage
NAS <Type : 65 (Registration request)>
MSIN: 0000000014
HTTP/2 <:method POST :path /nausf-auth/v1/ue-authentications >
SUPI: imsi-001010000000014
HTTP/2 <:method POST :path /nudm-ueau/v1/imsi-001010000000014/security-
HTTP/2 <:status 404 >
HTTP/2 <:status 404 >
Illegal UE
DownlinkNASTransport
NAS <Type : 68 (Registration reject)>
InitialUEMessage
NAS <Type : 65 (Registration request)>
MSIN: 0000000015
HTTP/2 <:method POST :path /nausf-auth/v1/ue-authentications >
SUPI: imsi-001010000000015
HTTP/2 <:method POST :path /nudm-ueau/v1/imsi-001010000000015/security-
InitialUEMessage
NAS <Type : 65 (Registrati
MSIN: 0000000016
HTTP/2 <:method POS
ore Network is runni
fluxbox - noVNC
https://glorious-lamp-v6p7vwg69wxj3wqr4-6080.app.github.dev
Version 1.3 (Build Date: 2024 Oct 15)
5G Hacker
Sniffer
Logs
5G Hacker
Test Object
CSTI 5GC
Save Configuration
Date 2025 Jan 02
RAN
MCC 001
MNC 01
SST 01
SD 030609
N2amf lo
127.0.0.5
Detect
gNB
gNB Name 0.gnb.csti.iii
TAC 000064
N2 lo
127.0.0.8
XnC lo
127.0.0.9
gNB-ID 1
32
Cell 1
N3 lo
127.0.0.8
XnU lo
127.0.0.12
UE (SA)
MSIN 0000000001
K 00112233445566778899AABBCCDDEEFF
OPc 000102030405060708090A0B0C0D0E0F
Ciphering 1 1 1 1
Integrity 0 1 1 1
DNN Internet
IMEI 12345670000000
SVN 01
Check 7
PFCP
N4src lo
127.0.0.6
N4dst docke
127.0.0.7
Version 1.3 (Build Date: 2024 Oct 15) | License: 2025 Dec 31 | Authors: Yi-Hsueh Tsai
Renewal
Exit
Result
No
Test Case
Save
Pass
N1-0 UE Attach to Network
Run
N1-1 Interoperability Testing (with Ping)
Ping Target 8.8.8.8
Run
N1-2 SUPI Credential Stuffing for UDM
Run
Evidence
0000000006 (Valid (AuthenticationRequest))
0000000007 (Valid (AuthenticationRequest))
0000000008 (Valid (AuthenticationRequest))
0000000009 (Valid (AuthenticationRequest))
0000000010 (Valid (AuthenticationRequest))
0000000011 (Valid (AuthenticationRequest))
0000000012 (InValid (RegistrationReject))
0000000013 (InValid (RegistrationReject))
0000000014 (InValid (RegistrationReject))
0000000015 (No Response (RegistrationRequest))
0000000016 (No Response (RegistrationRequest))
0000000017 (No Response (RegistrationRequest))
0000000018 (No Response (RegistrationRequest))
0000000019 (No Response (RegistrationRequest))
IEEE
COMMUNICATIONS
STANDARDS
MAGAZINE
nat you
accepted
the fina
This is to inform
bmitted to IEEE Communications Standards Magazine has
However, you will need to make some additional revis
u submit to the publications staff. You should now proceed to t
E Communications Standards Magazine website for instruc
your a
paper to the publications staff. The guidelines are located
w.comsoc.org
ations/magazines/ieee-communications-standards-magazine/author-guide
es
普通級 內部級 敏感級 機密級
INSTITUTE FOR INFORMATION INDUSTRY

debian@941025-NB1: ~

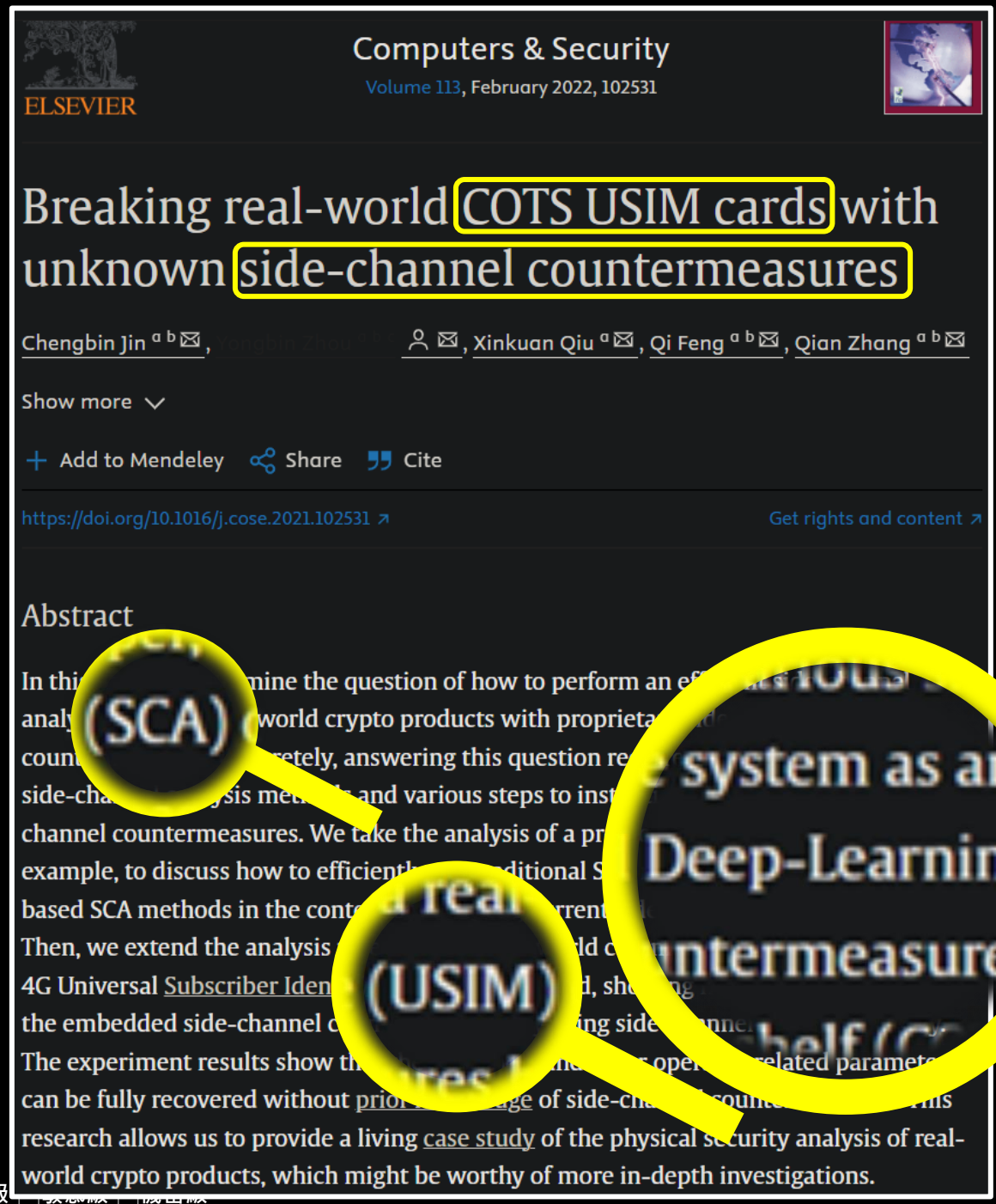
debian@941025-NB1: ~

```
debian@941025-NB1:~$
```

Reviewer's Comment

1. Comment 3: In 2-3 sentences, talk about security aspects of your work including connections with **post quantum crypto KEMs** and **signatures**. **NTT** is an important topic to consider.
2. Comment 4: How about future work, it gives motivation so add that in 2-3 bullets. Related to PQC, there is a **2023 competition by NIST for signatures**. For example, **Raccoon** is promising. Connect your work to that.
3. Comment 7: Add a paragraph, how about **fault detection** and **cryptography**, how about the notion of **SCAs** and combined attacks and countermeasures, relate that to your work in one paragraph.
   - Last but not least, I would like you to comment about accurate power derivation using **VCD** or **SAIF** as well as **energy consumption**.
   - Overall, your work will be enhanced addressing the above for another round of review. You can also talk about HW SW co-design using **Xilinx AMD Versal 2**.

Response to Comment



Computers & Security

Volume 113, February 2022, 102531

ELSEVIER

Breaking real-world COTS USIM cards with unknown side-channel countermeasures

Chengbin Jin [a b], Yongbin Zhou [ ], Xinkuan Qiu [a], Qi Feng [a b], Qian Zhang [a b]

Show more

+ Add to Mendeley Share Cite

https://doi.org/10.1016/j.cose.2021.102531 Get rights and content

Abstract

In thi…mine the question of how to perform an ef…ious… analy…world crypto products with proprieta… coun…retely, answering this question re… side-cha…ysis meth…and various steps to inst… channel countermeasures. We take the analysis of a pr… example, to discuss how to efficient…ditional S… based SCA methods in the conte…rrent… Then, we extend the analysis …ld c… 4G Universal Subscriber Iden…d, sho…g the embedded side-channel c…ing side…nne… The experiment results show th…r oper…related parameter… can be fully recovered without prior …ge of side-cha…counte…This research allows us to provide a living case study of the physical security analysis of real-world crypto products, which might be worthy of more in-depth investigations.

(SCA)

(USIM)

system as an

Deep-Learning

ntermeasures

Discussions on Side-Channel Vulnerabilities and Shortcomings

This study enhances SUPI security in 5G NPNs, but certain limitations must be addressed, particularly regarding real-world implementation and scalability. The simulated environment used to evaluate quantum-safe mechanisms simplifies network interactions, failing to capture scalability challenges, dynamic key exchanges, and operational diversity. While this research focuses on SUPI guessing attacks, it does not fully explore hybrid cryptographic schemes, SUCI decryption resilience, or real-time key exchanges. Future work should incorporate field trials to validate quantum-safe frameworks and investigate hybrid encryption models that combine post-quantum and traditional cryptographies for better security and adaptability.

Fault attacks (FAs) remain a significant concern, exploiting electromagnetic interference, voltage fluctuations, and clock manipulation, leading to side-channel vulnerabilities. Despite the growing adoption of PQC, GSMA guidelines [9] do not explicitly address SUCI decryption security in SIM cards, creating risks of side-channel leakages. Future implementations should …grate hardware-based countermeasures, including cryptographic co-processors, real-time anomaly monitoring, and fault detection mechanisms, ensuring protection in resource-constrained environments like SIM cards.

Harnessing the Potential of IBM Quantum Computers with Qiskit

Colaboratory

Access quantum computing

Open Plan

Free

Access to utility scale quantum computers for up to 10 minutes of runtime per month.

Best for

Learning quantum computing and exploring IBM quantum technology.

Pay-as-you-go

Starting at

$96 USD / minute

Pay for what you use. Billed per second of usage via IBM Cloud.

Best for

Performing quantum utility research projects and testing business models with flexible access.

Premium Plan

Subscription required

Equivalent to

$48 USD / minute*

Reserve the capacity you need for the year with Quantum Allocation Units (QAUs). Use up to 1600 minutes per QAU every 28 day rolling time-window.

Best for

Executing a strategic quantum roadmap and developing quantum algorithms and applications at scale.

Dedicated Service

Subscription required

Price requires quote

Access to an entirely dedicated quantum system that is serviced and maintained by IBM Quantum.

Best for

Exploring classical quantum algorithms and applications with high control over your resources and data.

Log in to IBM

IBMid

yihsueh.tsai@mail.ntut.edu.tw

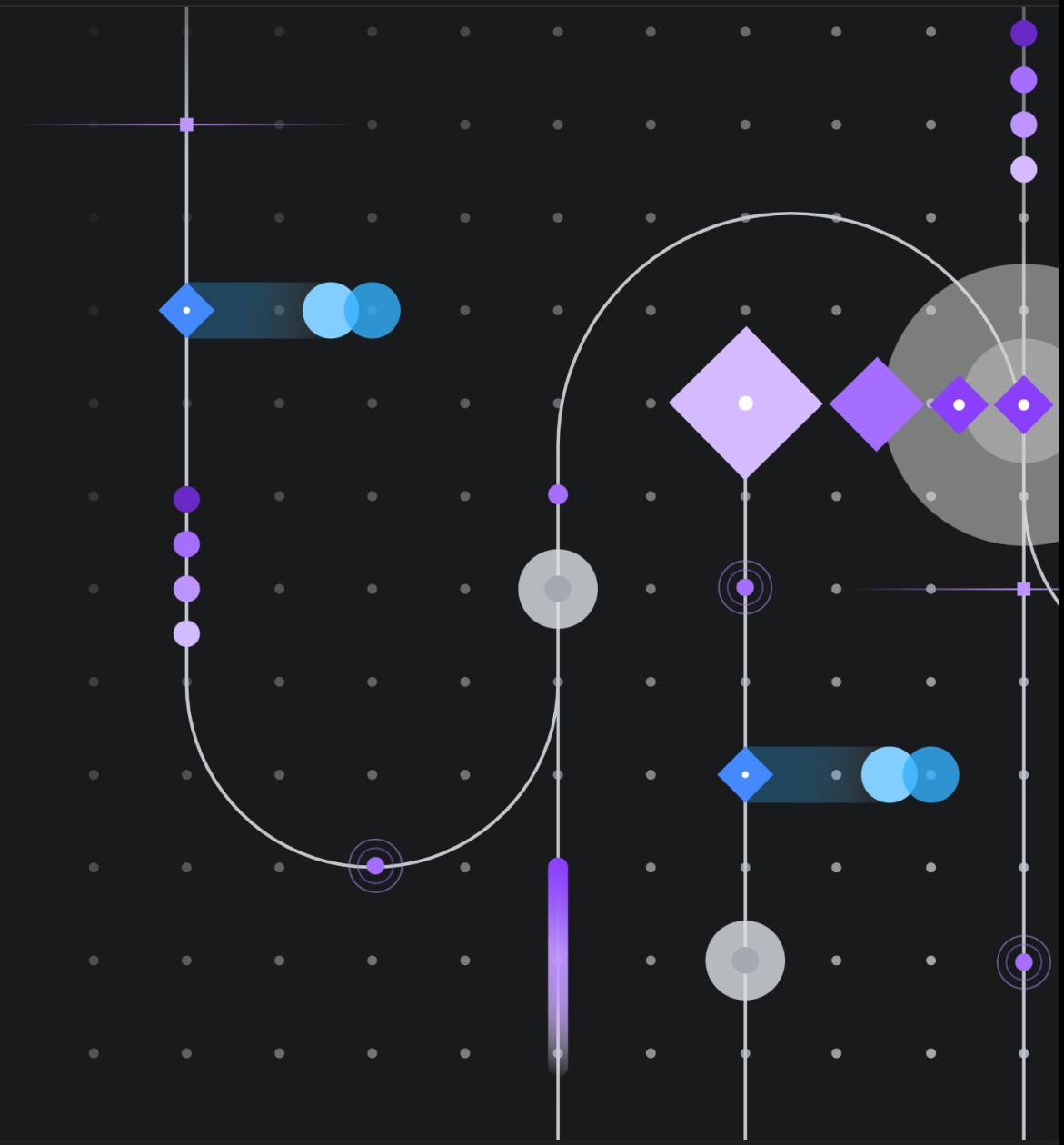
Continue →

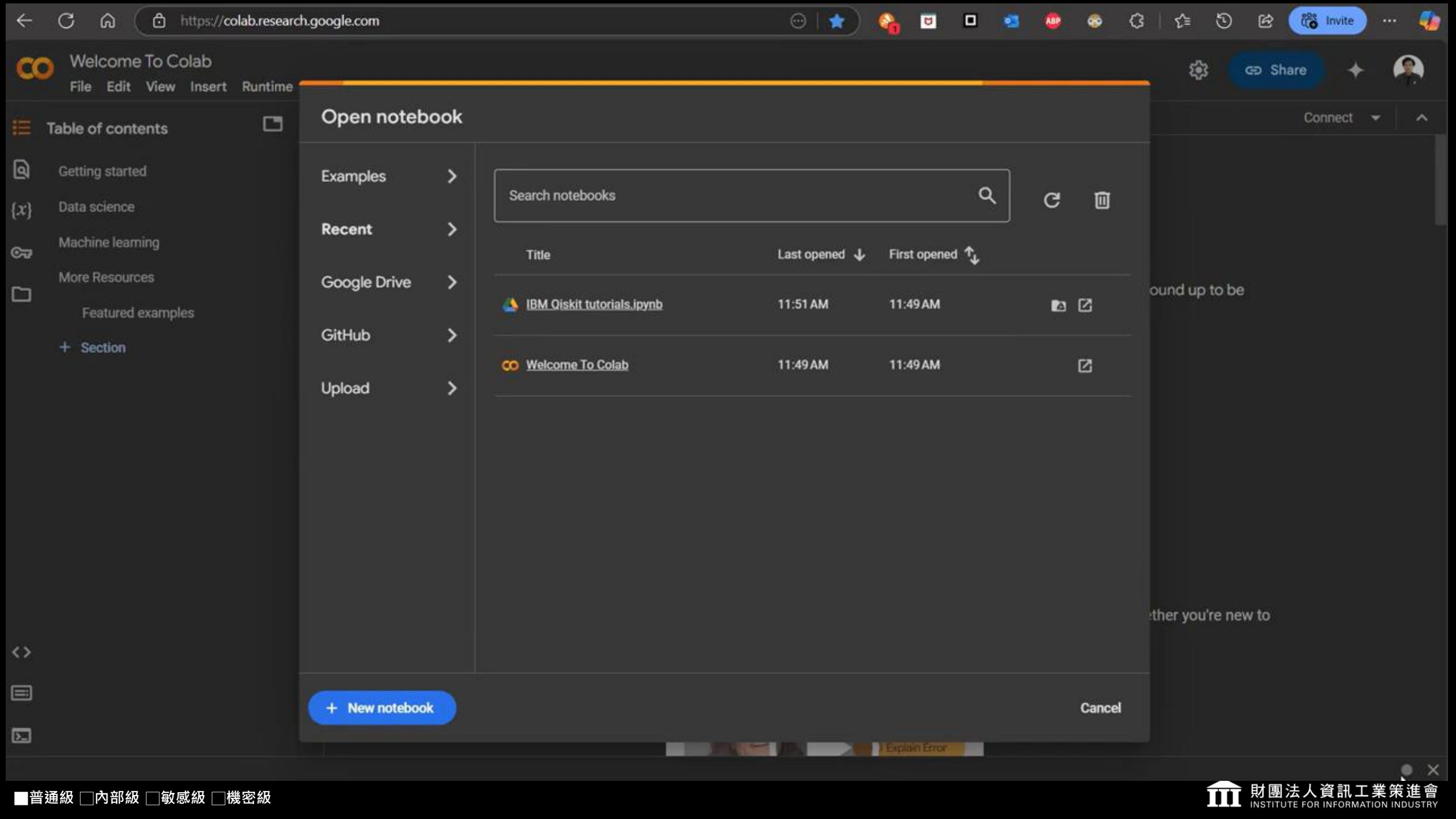
Remember me ⓘ

Don’t have an account?

Create an IBMid →

Forgot IBMid? Contact the IBMid help desk





IBM Quantum Platform

API Token

••••••••••••••••••••••••••••

Open Plan
View details | Upgrade
Up to 10 minutes/month

Monthly usage

Used	Remaining
0ms	10m

What's new →

- Service alert
  Upcoming maintenance
  4 days ago • Read more
- Blog
  Exploring the potential for quantum advantage in mathematical optimization
  18 days ago • Read more
- Blog
  Two new IBM Quantum blogs
  29 days ago • Read more
- Product update
  What's new in the docs?
  2 months ago • Read more
- Product update
  Sunset of backend.run
  2 months ago • Read more
- Blog
  IBM Quantum delivers on performance challenge
  3 months ago • Read more

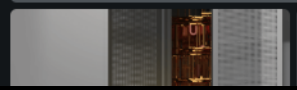
Recent workloads View all

1 Pending
7 Finished workloads

ID	Status	Completed	Mode	Compute resource	Usage
cyykyma78z600083arkg	Pending Est. wait: 2 minutes	--	Job	ibm_kyiv Queue position: 16	Est. 9.6s
cxnqwvk0v15000803ye0	Completed	25 Dec 2024	Session	ibm_brisbane	0s
cx7x32wztp30008ftak0	Completed	04 Dec 2024	Job	ibm_brisbane	7s
cx7w218ztp30008ft6yg	Completed	04 Dec 2024	Job	ibm_brisbane	10s
cx7vqxfpjw30008gvktg	Canceled	04 Dec 2024	Job	ibm_brisbane	0s

Instance QPUs →

3



All QPUs →

Documentation Open app ↗

Search docs

Hello World
Create a simple quantum program and run it on a quantum processing unit (QPU)

Learning Open app ↗

Featured course
Quantum Computing in Practice

Catalog
Explore all courses and tutorials

All workloads /

cyykyma78z600083arkg

Edit Tags

Details

Mode:	Job
QPU name:	ibm_kyiv
Instance:	ibm-q/open/main
Program:	estimator
# of PUBs:	1

Status details

Status

Pending

Usage stats

Actual usage	Estimated QR usage
N/A	9.6s

Status timeline

- Created: Feb 25, 2025 11:56 AM
- Pending
  Estimated wait time: 1 minute, Project pos: 8, QPU pos: 15
- In progress
  Estimated usage: 9.6s
- Completed

Job results

Use Qiskit IBM Runtime to retrieve your job results. Learn more ↗

```python
from qiskit_ibm_runtime import QiskitRuntimeService

service = QiskitRuntimeService(
    channel='ibm_quantum',
    instance='ibm-q/open/main',
    token='***'
)
job = service.job('cyykyma78z600083arkg')
job_result = job.result()

for idx, pub_result in enumerate(job_result):
    print(f"Expectation values for pub {idx}: {pub_result.data.evs}")
```

IBM Quantum Platform

API Token

••••••••••••••••••••••••••••

Open Plan
View details | Upgrade
Up to 10 minutes/month

Monthly usage
Used 6s
Remaining 9m 54s

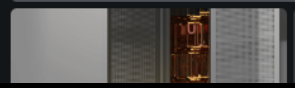
Recent workloads View all

0 Pending
8 Finished workloads

ID	Status	Completed	Mode	Compute resource	Usage
cyykyma78z600083arkg	Completed	25 Feb 2025	Job	ibm_kyiv	6s
cxnqwvk0v15000803ye0	Completed	25 Dec 2024	Session	ibm_brisbane	0s
cx7x32wztp30008ftak0	Completed	04 Dec 2024	Job	ibm_brisbane	7s
cx7w218ztp30008ft6yg	Completed	04 Dec 2024	Job	ibm_brisbane	10s
cx7vqxfpjw30008gvktg	Canceled	04 Dec 2024	Job	ibm_brisbane	0s

Instance QPUs →

3



All QPUs →

Documentation Open app ↗

Search docs

Hello World
Create a simple quantum program and run it on a quantum processing unit (QPU)

Learning Open app ↗

Featured course
Quantum Computing in Practice

Catalog
Explore all courses and tutorials

What's new →

- Service alert
  Upcoming maintenance
  4 days ago • Read more
- Blog
  Exploring the potential for quantum advantage in mathematical optimization
  18 days ago • Read more
- Blog
  Two new IBM Quantum blogs
  29 days ago • Read more
- Product update
  What's new in the docs?
  2 months ago • Read more
- Product update
  Sunset of backend.run
  2 months ago • Read more
- Blog
  IBM Quantum delivers on performance challenge
  3 months ago • Read more

https://colab.research.google.com/drive/1BJzRihHDdcEudPbj_Np9qdaH1kjXyVxS#scrollTo=r9xPTKv...

IBM Qiskit tutorials.ipynb

File Edit View Insert Runtime Tools Help

Share

+ Code + Text

RAM Disk

[5]
```
# This is the result of the entire submission.  You submitted one Pub,
# so this contains one inner result (and some metadata of its own).
job_result = job.result()

# This is the result from our single pub, which had six observables,
# so contains information on all six.
pub_result = job.result()[0]
```

```
# Use the following code instead if you want to run on a simulator:

from qiskit_ibm_runtime.fake_provider import FakeAlmadenV2
backend = FakeAlmadenV2()
estimator = Estimator(backend)

# Convert to an ISA circuit and layout-mapped observables.

pm = generate_preset_pass_manager(backend=backend, optimization_level=1)
isa_circuit = pm.run(qc)
mapped_observables = [
    observable.apply_layout(isa_circuit.layout) for observable in observables
]

job = estimator.run([(isa_circuit, mapped_observables)])
result = job.result()

# This is the result of the entire submission.  You submitted one Pub,
# so this contains one inner result (and some metadata of its own).

job_result = job.result()

# This is the result from our single pub, which had five observables,
```

Connected to Python 3 Google Compute Engine backend

IBM Quantum Platform

API Token

Open Plan
View details | Upgrade
Up to 10 minutes/month

Monthly usage

Used	Remaining
12s	9m 48s

What's new

- Service alert — Upcoming maintenance — 4 days ago • Read more
- Blog — Exploring the potential for quantum advantage in mathematical optimization — 18 days ago • Read more
- Blog — Two new IBM Quantum blogs — 29 days ago • Read more
- Product update — What's new in the docs? — 2 months ago • Read more
- Product update — Sunset of backend.run — 2 months ago • Read more
- Blog — IBM Quantum delivers on performance challenge — 3 months ago • Read more

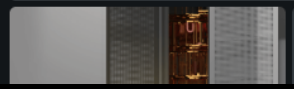
Recent workloads View all

0 Pending
9 Finished workloads

ID	Status	Completed	Mode	Compute resource	Usage
cyynkenq5bwg00849ng0	Completed	25 Feb 2025	Job	ibm_kyiv	6s
cyykyma78z600083arkg	Completed	25 Feb 2025	Job	ibm_kyiv	6s
cxnqwvk0v15000803ye0	Completed	25 Dec 2024	Session	ibm_brisbane	0s
cx7x32wztp30008ftak0	Completed	04 Dec 2024	Job	ibm_brisbane	7s
cx7w218ztp30008ft6yg	Completed	04 Dec 2024	Job	ibm_brisbane	10s

Instance QPUs

3



All QPUs

Documentation Open app

Search docs

Hello World
Create a simple quantum program and run it on a quantum processing unit (QPU)

Learning Open app

Featured course
Quantum Computing in Practice

Catalog
Explore all courses and tutorials

How to Leverage Generative AI for Effective Programing on QSN

Decomposing Prime Numbers with Shor's Algorithm: A GitHub Copilot Code Generation

GPT-4o

Question

Decomposing Prime Numbers using Shor

Sure! Below is an example Python script that demonstrates decomposing prime numbers using Shor's algorithm. Shor's algorithm is a quantum algorithm for integer factorization that runs in polynomial time. It can efficiently find the prime factors of a composite number.

The following code uses the `qiskit` library to implement Shor's algorithm:

Answer

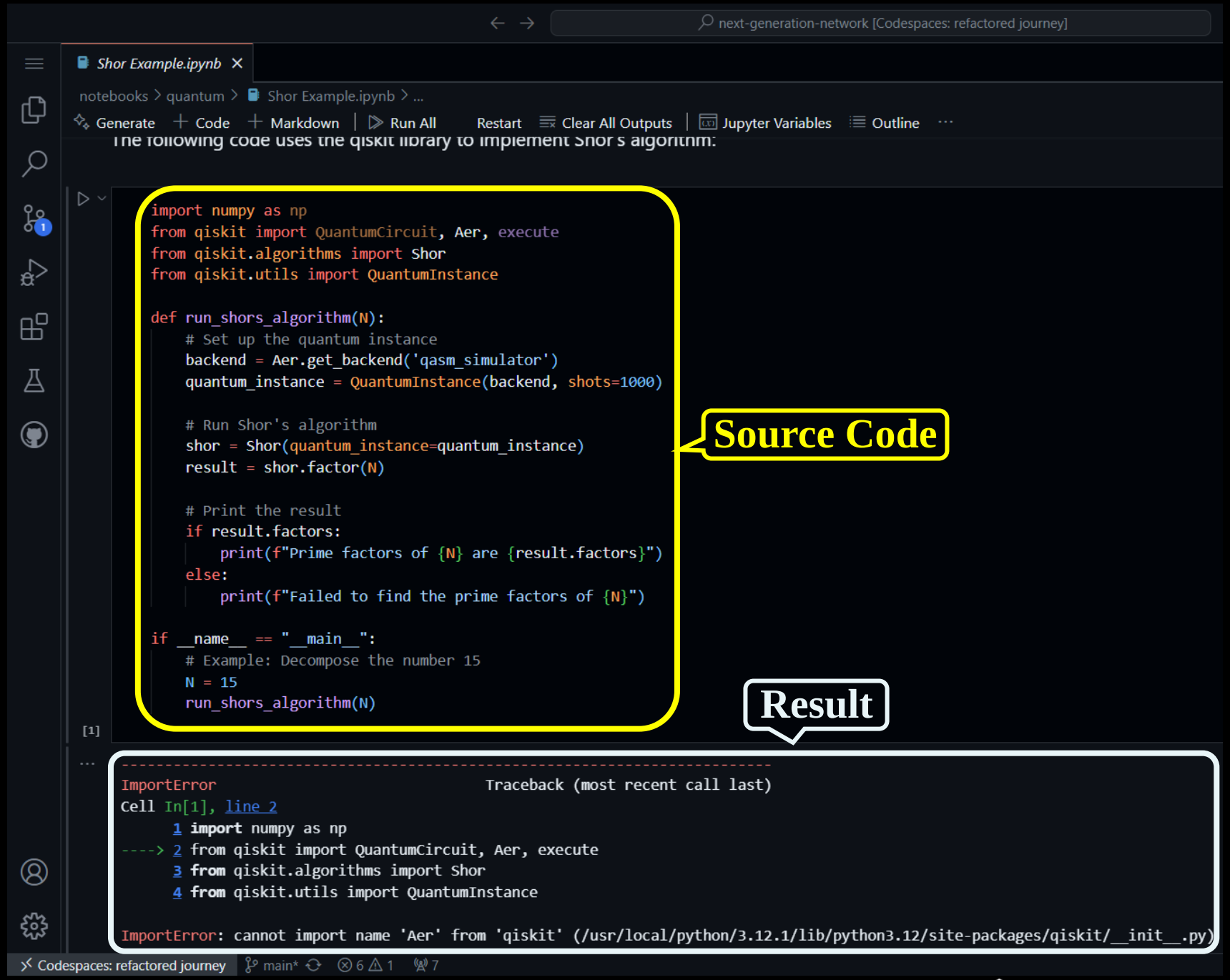
shor_algorithm.py v1

```
import numpy as np
from qiskit import QuantumCircuit, Aer, execute
from qiskit.algorithms import Shor
from qiskit.utils import QuantumInstance
```

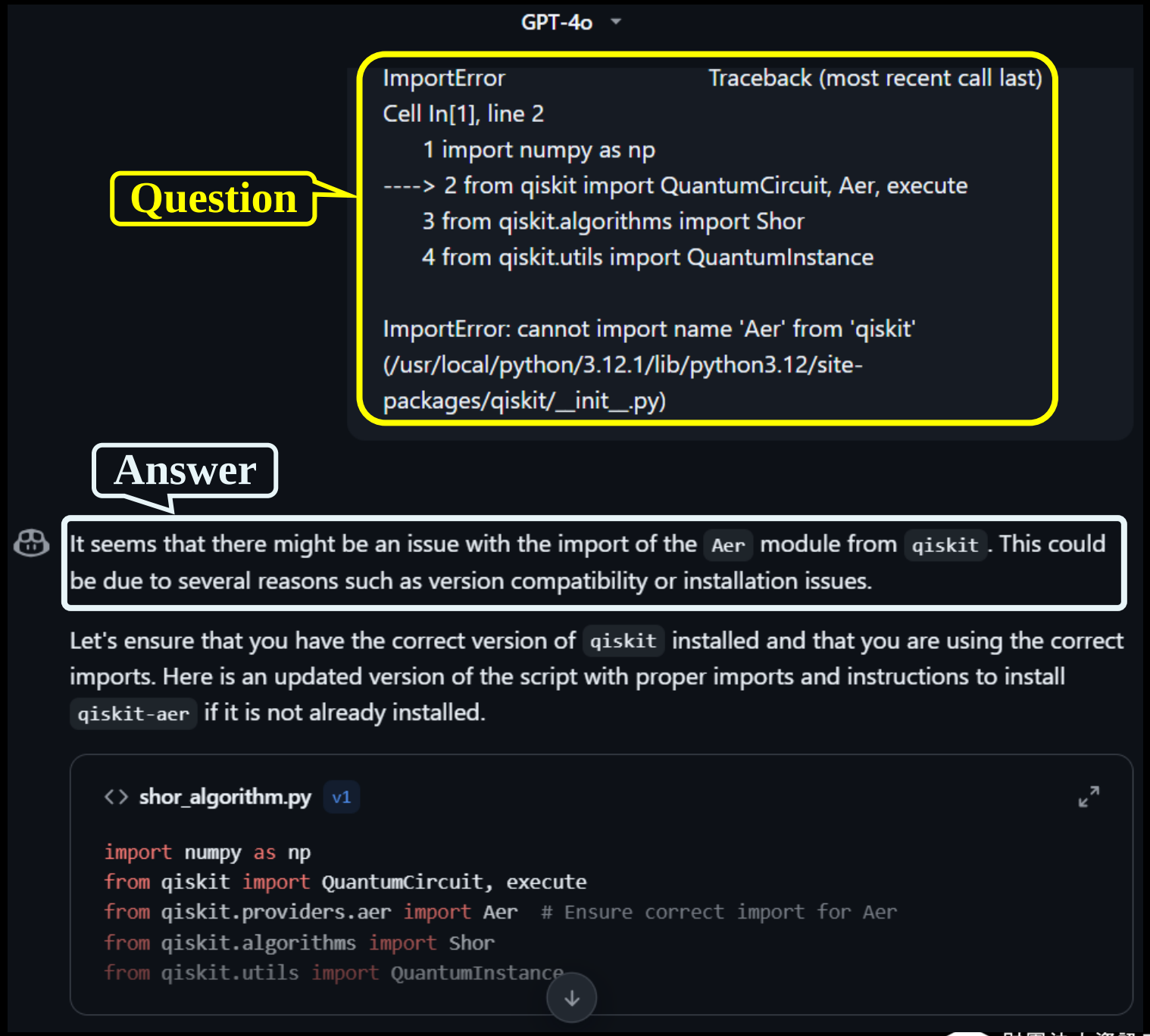
Explanation:

1. **Import necessary libraries**: Import `numpy`, `qiskit`, and other necessary modules.
2. **Define `run_shors_algorithm` function**: This function sets up the quantum instance, runs Shor's algorithm, and prints the result.
3. **Set up the quantum instance**: Use the `Aer` simulator backend from Qiskit.
4. **Run Shor's algorithm**: Create an instance of `Shor` and run it with the provided number `N`.
5. **Print the result**: If prime factors are found, print them; otherwise, indicate failure.
6. **Main block**: Define the number `N` to de pose and call the `run_shors_algorithm` function.

Executing Code Generated by GitHub Copilot: Encountering Error Messages



Re-generating Code with GitHub Copilot to Eliminate Error Messages



Executing Re-generated Code by GitHub Copilot: Facing Error Messages Again

Shor Example.ipynb

notebooks > quantum > Shor Example.ipynb > ...

Generate | Code | Markdown | Run All | Restart | Clear All Outputs | Jupyter Variables | Outline

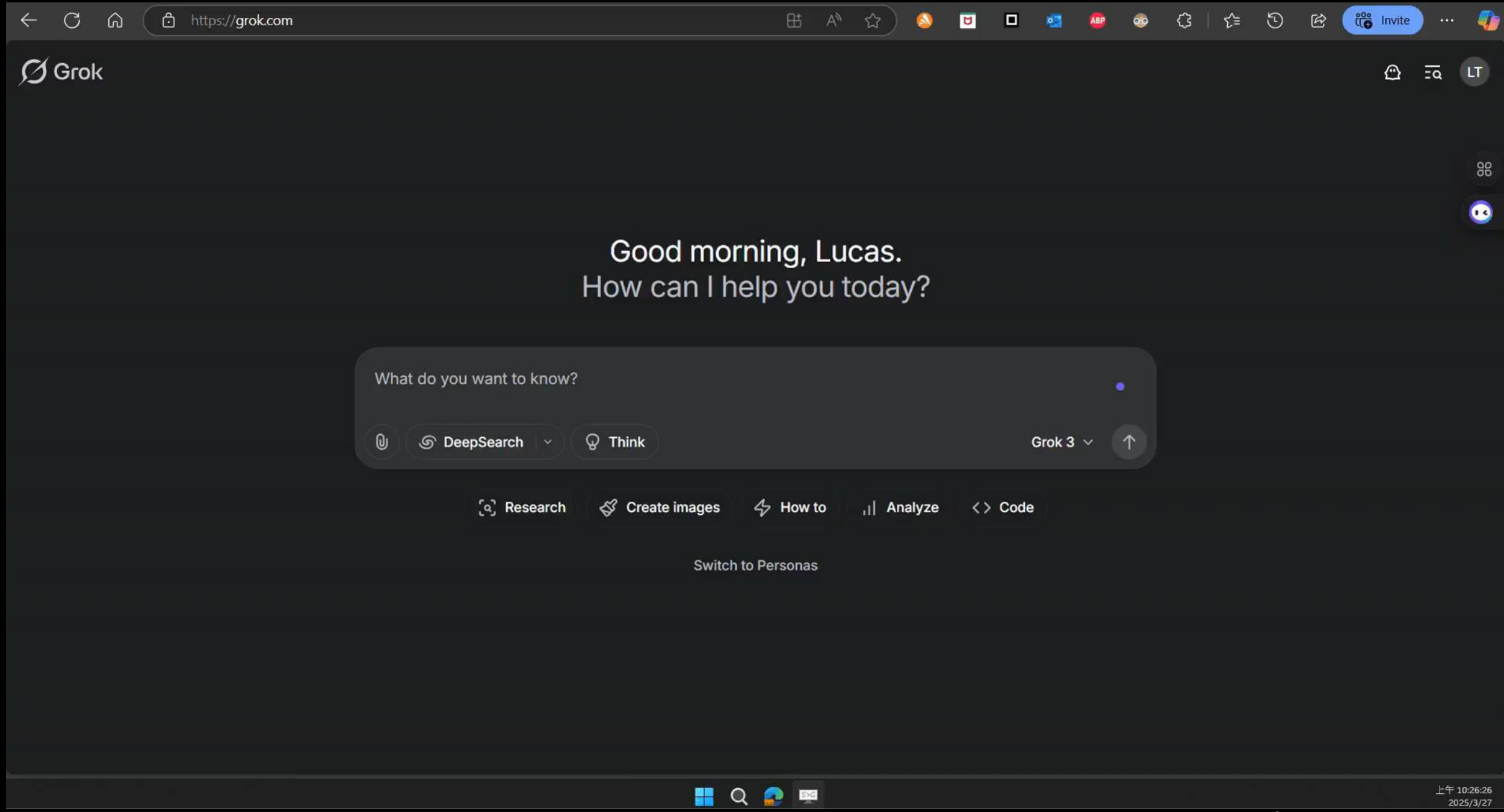
```python
import numpy as np
from qiskit import QuantumCircuit, execute
from qiskit.providers.aer import Aer  # Ensure correct import for Aer
from qiskit.algorithms import Shor
from qiskit.utils import QuantumInstance

def run_shors_algorithm(N):
    # Set up the quantum instance
    backend = Aer.get_backend('qasm_simulator')
    quantum_instance = QuantumInstance(backend, shots=1000)

    # Run Shor's algorithm
    shor = Shor(quantum_instance=quantum_instance)
    result = shor.factor(N)

    # Print the result
    if result.factors:
        print(f"Prime factors of {N} are {result.factors}")
    else:
        print(f"Failed to find the prime factors of {N}")

if __name__ == "__main__":
    # Example: Decompose the number 15
    N = 15
    run_shors_algorithm(N)
```

Source Code

[4]

Result

```
ImportError                               Traceback (most recent call last)
Cell In[4], line 2
      1 import numpy as np
----> 2 from qiskit import QuantumCircuit, execute
      3 from qiskit.providers.aer import Aer  # Ensure correct import for Aer
      4 from qiskit.algorithms import Shor

ImportError: cannot import name 'execute' from 'qiskit' (/usr/local/python/3.12.1/lib/python3.12/site-packages/qiskit/__init__.py)
```



EXPLORER

NEXT-GENERATION-NETWORK [CODESPACES: REFA...

- .venv
- computer-and-human-life
- data
- gui
- interfaces
- logs
- nfs
- ngs
- nodes
- notebooks
  - computer-and-human-life
  - copilot
  - ngn
  - quantum
    - Grok - Shor's algorithm.ipynb
    - Hello world.ipynb
    - Shor Example.ipynb
    - shor15.ipynb
    - shor39.ipynb
    - shor55.ipynb
    - shor77.ipynb
  - image-classifier.ipynb
  - matplotlib.ipynb
  - population.ipynb
- protocals
- trp

OUTLINE

TIMELINE

Grok - Shor's algorithm.ipynb

notebooks > quantum > Grok - Shor's algorithm.ipynb > ...

Generate | Code | Markdown | Run All | Clear All Outputs | Outline | Select Kernel

factor integers into their prime factors, and prime numbers by definition have no non-trivial factors. Here's a Python implementation that simulates Shor's algorithm. Note that a true quantum implementation would require a quantum computer (e.g., using Qiskit), but this classical simulation illustrates the logic. I'll use a simplified version with modular arithmetic and the quantum period-finding concept approximated classically.

```
import random
import math

def gcd(a, b):
    """Compute the Greatest Common Divisor of a and b."""
    while b:
        a, b = b, a % b
    return a

def modular_exp(base, exponent, modulus):
    """Efficient modular exponentiation."""
    result = 1
    base = base % modulus
    while exponent > 0:
        if exponent & 1:
            result = (result * base) % modulus
        base = (base * base) % modulus
        exponent >>= 1
    return result

def is_prime(n):
    """Check if a number is prime."""
    if n < 2:
        return False
    for i in range(2, int(math.sqrt(n)) + 1):
        if n % i == 0:
```

Codespaces: refactored journey | main | 0 0 | 6 | Spaces: 4 | Cell 2 of 3 | Layout: US

上午 10:52:52
2025/3/27

Grok

factors.

5. **Retry Logic**: If period finding fails or yields invalid results, the algorithm retries with a new `a`.

Limitations:

- This is a classical simulation, so it's inefficient for large numbers (Shor's algorithm shines on quantum hardware).
- For large `N`, the period-finding step would be infeasible classically but is polynomial-time on a quantum computer.
- Works best with small composite numbers like 15 (3 × 5) or 21 (3 × 7).

Example Output for N = 15:

text Collapse Wrap Copy

```
Attempting to factor 15
Randomly chosen a = 7
Found period r = 4
Factors found: 3 and 5
Final factors: 3 and 5
```

Let me know if you'd like a quantum-specific version (e.g., with Qiskit) or further refinements!

Generate a Python algorithm for decomposing prime numbers using Shor's algorithm and IBM's Qiskit quantum computing framework.

DeepSearch Think Grok 3

上午 11:16:22
2025/3/27

https://refactored-journey-wqxqwq469j3r57.github.dev

next-generation-network [Codespaces: refactored journey]

EXPLORER

NEXT-GENERATION-NETWORK [CODESPACES: REFA...

- data
- gui
- interfaces
- logs
- nfs
- ngs
- nodes
- notebooks
  - computer-and-human-life
  - copilot
  - ngn
  - quantum
    - Grok - Shor's algorithm.ipynb M
    - Hello world.ipynb
    - Shor Example.ipynb
    - shor15.ipynb
    - shor39.ipynb
    - shor55.ipynb
    - shor77.ipynb
  - image-classifier.ipynb
  - matplotlib.ipynb
  - population.ipynb
- protocals
- trp
- ue
- utils
- .gitignore

OUTLINE

TIMELINE

Grok - Shor's algorithm.ipynb M

notebooks > quantum > Grok - Shor's algorithm.ipynb > ...

Generate | Code | Markdown | Run All | Restart | Clear All Outputs | Go To | Jupyter Variables | Outline | Python 3.12.1

Since you've requested a Python algorithm using IBM's Qiskit framework to factor numbers (I'll assume you meant factoring composite numbers int primes, as Shor's algorithm doesn't decompose primes), I'll provide a quantum implementation. This code uses Qiskit to simulate Shor's algorithm on a quantum simulator, as true quantum hardware access would require an IBM Quantum account and sufficient qubits, which are limited for large numbers. Below is a practical implementation for small numbers like 15 (3 × 5).

```
from qiskit import QuantumCircuit, Aer, execute
from qiskit.circuit.library import QFT
import math
import random

def gcd(a, b):
    """Compute the Greatest Common Divisor of a and b."""
    while b:
        a, b = b, a % b
    return a

def modular_exp_circuit(a, N, n_count):
    """Create a quantum circuit for modular exponentiation a^x mod N."""
    n = math.ceil(math.log2(N))  # Number of bits to represent N
    circuit = QuantumCircuit(n + n_count, n_count)

    # For simplicity, simulate a^x mod N classically and apply controlled-U gates
    for x in range(n_count):
        # Compute a^(2^x) mod N
        power = pow(a, 2**x, N)
        # Apply controlled multiplication by 'power' mod N
        for qubit in range(n):
            if (power >> qubit) & 1:
                circuit.cx(x, qubit + n_count)
```

[ ]

Codespaces: refactored journey | main* | 0 1 | 8 | Spaces: 4 | Cell 5 of 6 | Layout: US

上午 11:24:17
2025/3/27

Grok

```
Factors found: 3 and 5
Final factors: 3 and 5
```

Collapse | Wrap | Copy

Notes:

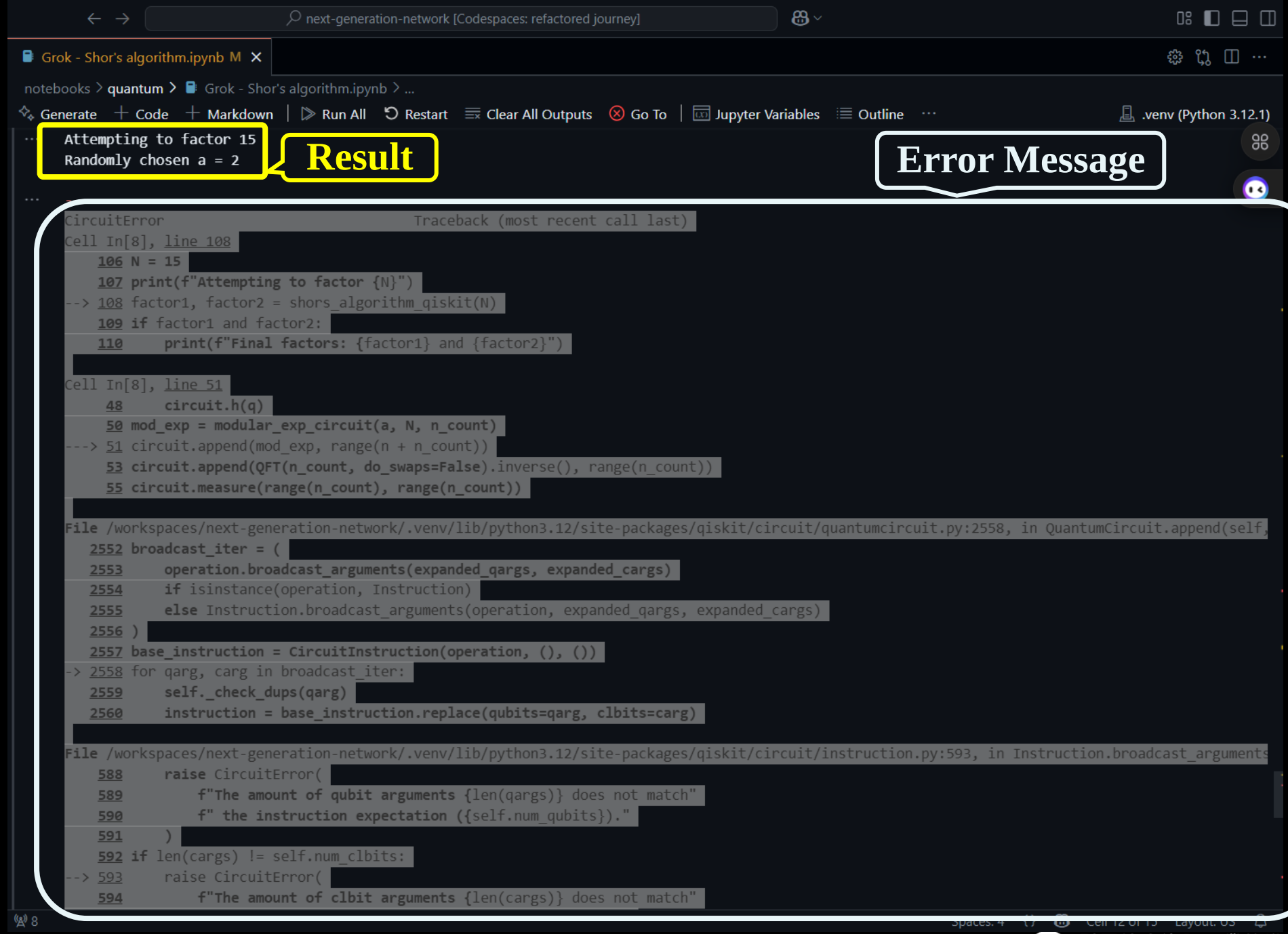
- **Scalability**: This works for small numbers (e.g., 15, 21) due to simulator limitations. Factoring large numbers requires a real quantum computer with many qubits and low noise.
- **Simplifications**: The modular exponentiation is simplified; a full quantum implementation would use a gate sequence for `a^x mod N`.
- **Retries**: If the period is invalid (odd or doesn't yield factors), it retries with a new `a`.

Let me know if you'd like to refine this further or adapt it for a specific quantum backend!

```
---------------------------------------------------------------------------
ImportError                               Traceback (most recent call last)
Cell In[1], line 1
----> 1 from qiskit import QuantumCircuit, Aer, execute
      2 from qiskit.circuit.library import QFT
      3 import math

File /usr/local/python/3.12.1/lib/python3.12/site-packages/qiskit/__init__.py:38
     36     _suppress_error = os.environ.get("QISKIT_SUPPRESS_1_0_IMPORT_ERROR", False) ==
"1"
     37     if int(_major) > 0 and not _suppress_error:
---> 38         raise ImportError(
```

DeepSearch | Think | Grok 3

Executing Re-generated Code by Grok: Facing Error Messages Again



Re-generating Code with Grok to Eliminate Error Messages

The `CircuitError` you're encountering arises because the `modular_exp_circuit` function creates a `QuantumCircuit` with classical bits (clbits) that are not properly handled when appended to the main circuit in `shors_algorithm_qiskit`. Specifically:

- `modular_exp_circuit` defines a circuit with `n + n_count` qubits and `n_count` clbits, but when it's appended to the main circuit (which also has `n_count` clbits), Qiskit expects the number of classical bits in the instruction to match the number provided in the `cargs` argument of `circuit.append`. By default, no `cargs` are provided, leading to a mismatch (0 clbits provided vs. `n_count` expected).

To fix this, we need to:

1. Ensure the `modular_exp_circuit` doesn't include unnecessary clbits, since we're not measuring within that subcircuit.
2. Properly specify both qubit and clbit arguments when appending the circuit if clbits are involved, or adjust the circuit construction to avoid this mismatch.

Here's the corrected version of the code:

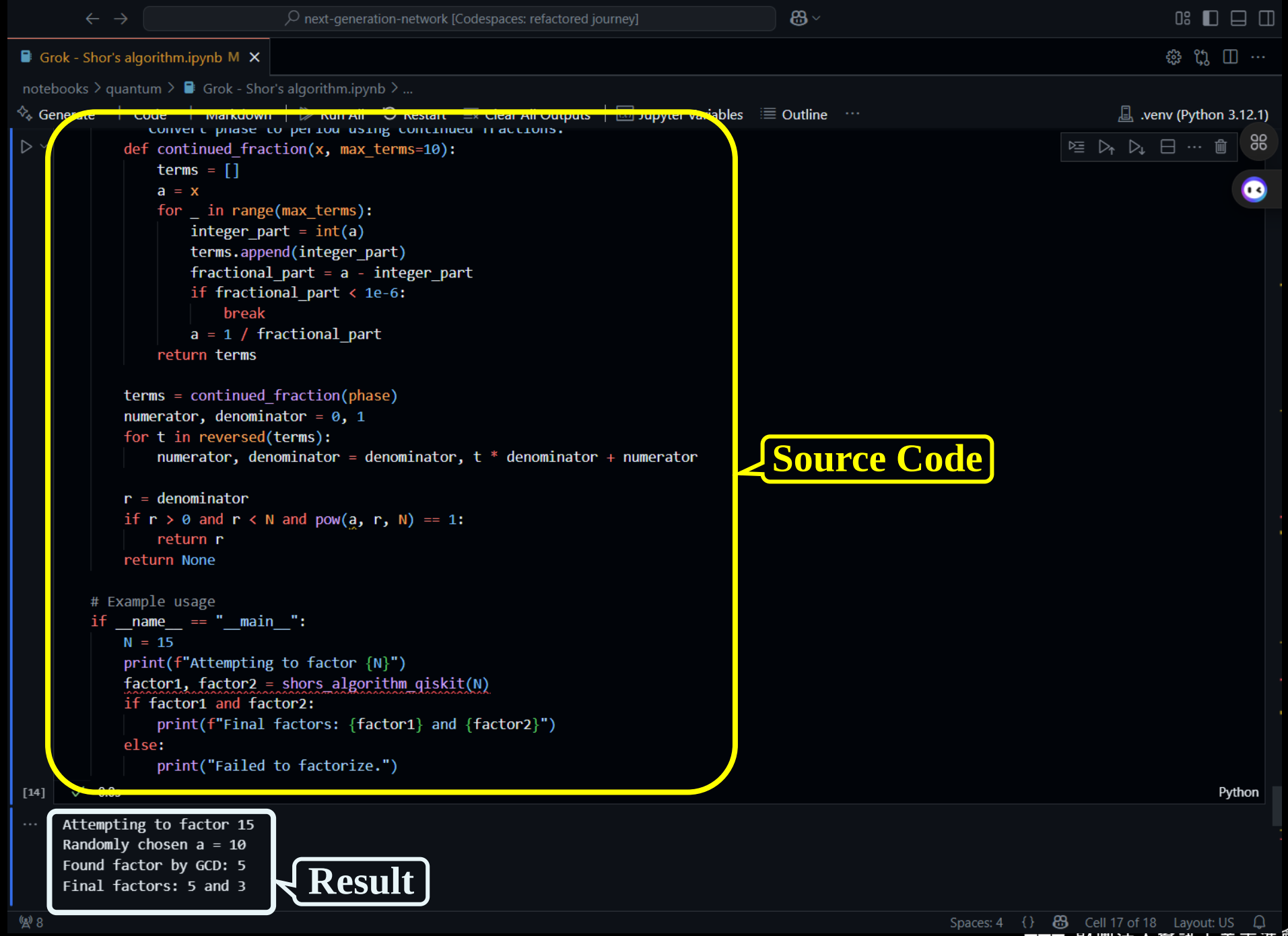
python Collapse Wrap Copy

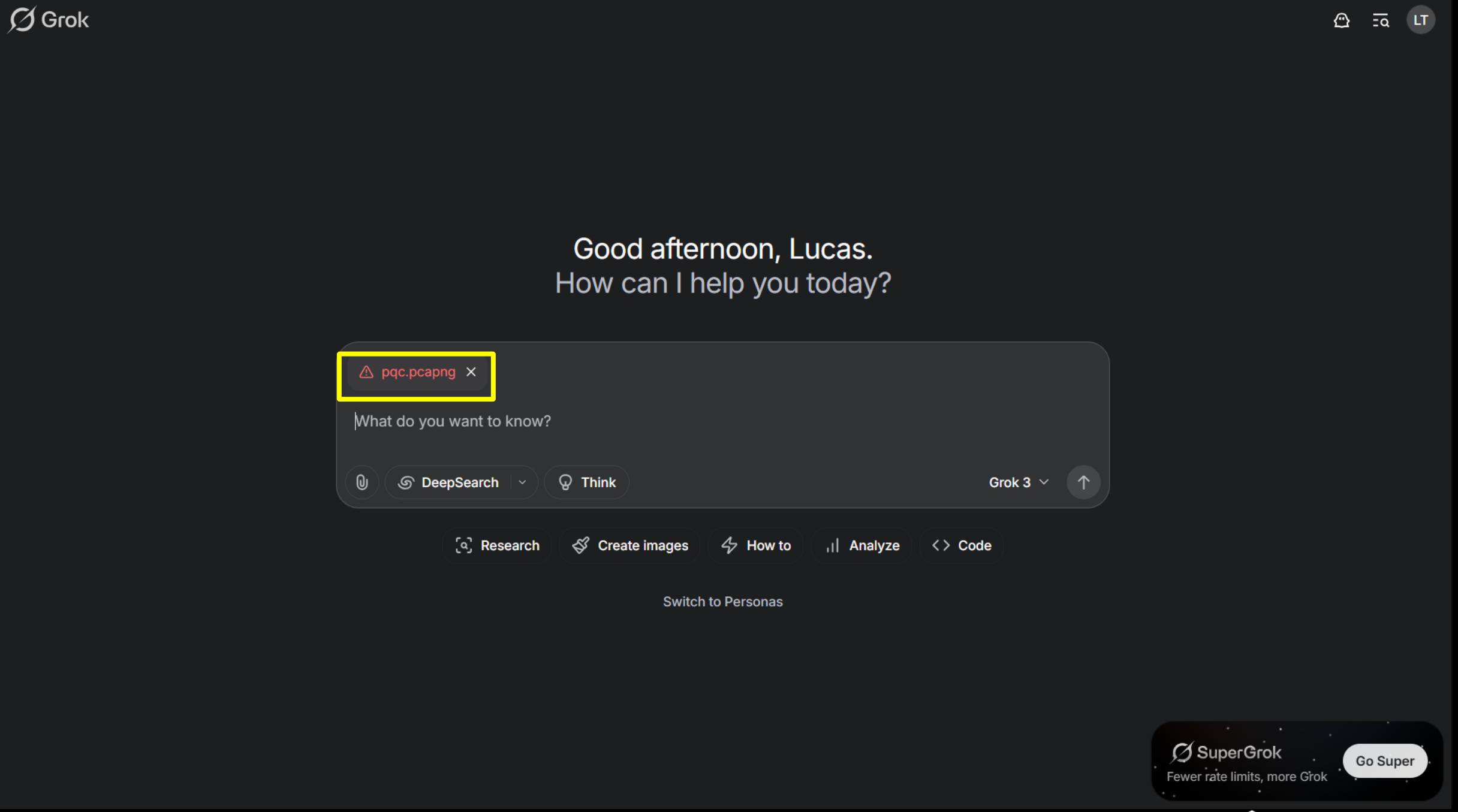
```python
from qiskit import QuantumCircuit
from qiskit.circuit.library import QFT
from qiskit_aer import AerSimulator
import math
import random

def gcd(a, b):
    """Compute the Greatest Common Divisor of a and b."""
    while b:
        a, b = b, a % b
```

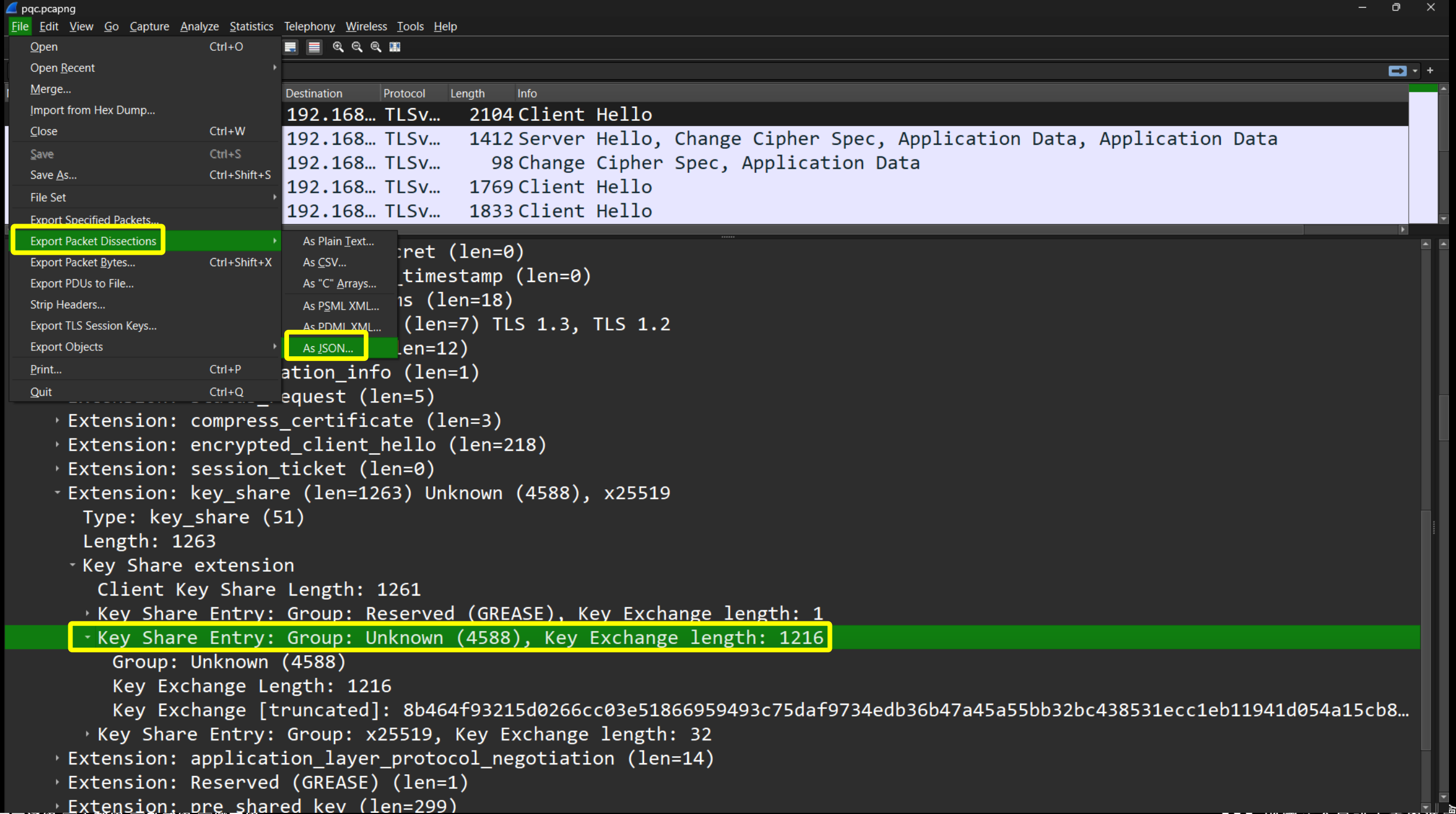
How can Grok help?

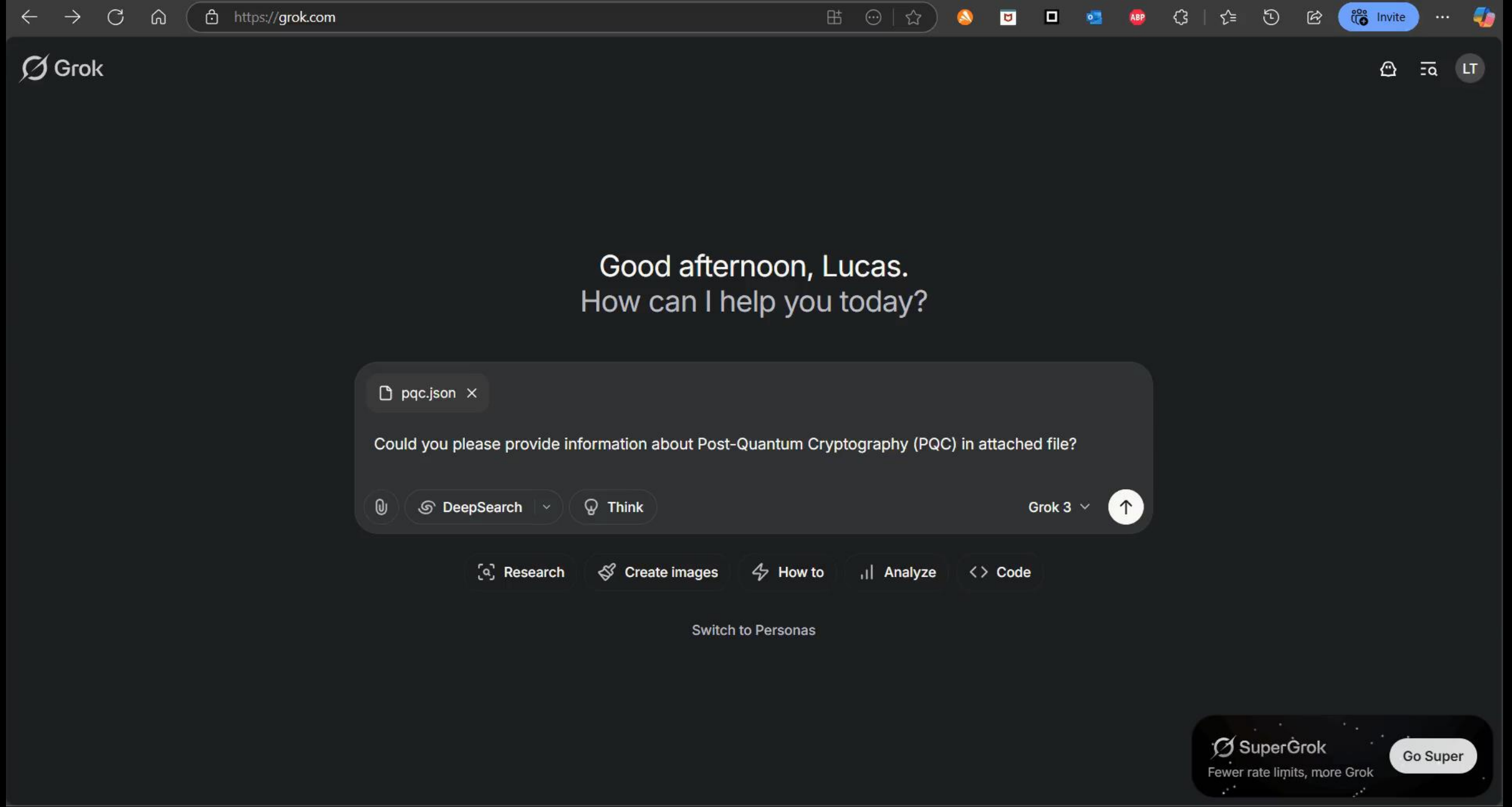
DeepSearch Think Grok 3

Executing Re-generated Code by Grok Successfully









Conclusion

- The rise of quantum computing poses real threats to 5G identity protection, especially SUCI encryption based on ECIES. As shown in our emulation experiments, vulnerabilities exist that could be exploited once quantum capabilities mature.
- To build resilience, migration to Quantum Safe Networks (QSN) is necessary—incorporating Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD). We actively engage with 3GPP and GSMA to align with future 6G standards.

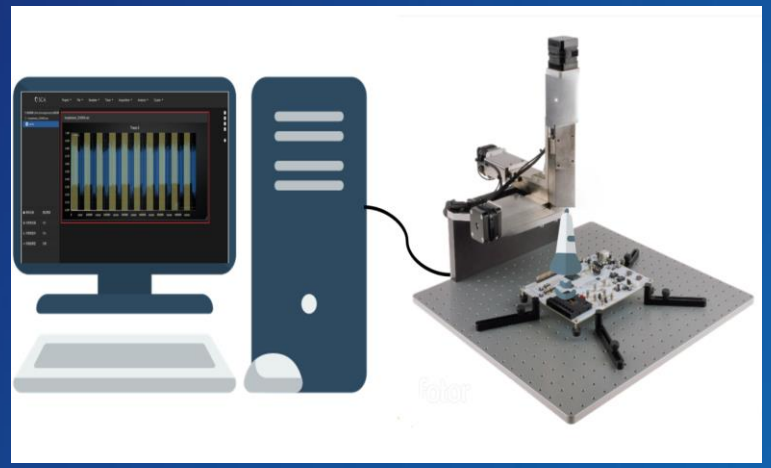
Conclusion

- Our study also explores the potential of IBM Qiskit, which allows simulation of quantum algorithms like Shor's, helping assess actual risks.
- In parallel, we demonstrate how Generative AI, such as GitHub Copilot, can aid rapid quantum code prototyping and learning—though iterative validation remains crucial.
- Together, quantum technologies and AI tools offer new ways to enhance network security, accelerate R&D, and shape a trustworthy communication future.

PQC 晶片安全國際合規

後量子加密晶片旁通道檢測系統

支援國際PQC標準，協助廠商進行合規預檢測、降低驗證成本。



PQC 產品安全提升

後量子加密產品脆弱性評估工具

識別後量子加密場域與產品潛在風險與弱點，降低未來營運風險與合規成本。

場域密碼系統現況評估

後量子安全評估工具 (PQ-SAT)

提供後量子加密遷移計畫之關鍵參考依據，提升組織的運營效率和安全性。

PQ-SAT ：Post-Quantum Security Assessment Tool
後量子安全評測工具