一般社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report

モバイルネットワークサービスの利用者認証に関するセキュリティ
― 5G の現状および Beyond5G/ 6 G に向けた研究動向 ―

才所 敏明[*1] 辻井 重男[*2] 櫻井 幸一[*3]

*1 (株)IT 企画 〒158-0083 東京都世田谷区奥沢 6-18-10
*2 中央大学研究開発機構 〒112-8551 東京都文京区春日 1-13-27
*3 九州大学大学院システム情報科学研究院 〒819-0395 福岡市西区元岡 744 番地,
(株) 国際電気通信基盤技術研究所 〒619-0288 京都府相楽郡精華町光台二丁目 2 番地 2

E-mail: *1 toshiaki.saisho@advanced-it.co.jp, *2 tsujii@tamacc.chuo-u.ac.jp, *3 sakurai@INF.kyushu-u.ac.jp

あらまし モバイルネットワークサービス事業者が実施する利用者認証にかかわるセキュリティについて，5G の現状，Beyond5G/6G に向けた検討課題，研究動向等を報告する．モバイルネットワークサービスの事業者の視点，利用者の視点，社会の視点から，利用者の確実な本人確認（身元確認＋当人確認），利用者の匿名性の確保，不正・不法な利用者の特定・追跡性を，利用者認証のセキュリティ要件とし，このようなセキュリティ要件の観点から，身元確認や当人確認に関連するプロセスや利用者の情報のセキュリティについて，5G の現状，Beyond5G / 6G に向けて検討すべき課題，研究動向などを報告する．

キーワード 5G，Beyond5G，6G，モバイルネットワーク，利用者認証，身元確認，当人確認，本人確認，匿名性，特定・追跡性，研究動向

Security related to user authentication in mobile network services
― Current status of 5G and research trends toward Beyond 5G / 6G ―

Toshiaki Saisho[*1] Shigeo Tsujii[*2] Kouichi Sakurai[*3]

*1 Advanced IT Corporation 6-18-10 Okusawa, Setagaya-ku, Tokyo, 158-0083 Japan
*2 Research and Development Initiative, Chuo University 1-13-27 Kasuga, Bunkyo-ku, Tokyo, 112-8551 Japan
*3 Graduate School and Faculty of Information Science and Electrical Engineering, Kyushu University 744 Motooka, Nishi-ku Fukuoka 819-0395 Japan
Advanced Telecommunications Research Institute International 2-2-2 Hikaridai, Seika-cho, Souraku-gun, Kyoto, 619-0288 Japan

E-mail: *1 toshiaki.saisho@advanced-it.co.jp, *2 tsujii@tamacc.chuo-u.ac.jp, *3 sakurai@INF.kyushu-u.ac.jp

Abstract We will report on the current status of 5G, issues to be examined for Beyond 5G / 6G, research trends, etc. regarding security related to user authentication implemented by mobile network service providers. From the perspective of mobile network service providers, users, and society, we have defined 3 major security requirements for user authentication such as secure user authentication (identity proofing + identity verification), user anonymity and the identifiability and traceability of fraudulent and illegal users. From the viewpoint of such security requirements, regarding the security about the process and the user information related to identity proofing and identity verification, we report the current status of 5G, issues to be examined for Beyond 5G / 6G, and research trends, etc.

Keywords 5G, Beyond5G, 6G, mobile network, authentication, identity proofing, identity verification, anonymity, identifiability, traceability, research trend

1. はじめに

1974 年の TCP/IP 発表に始まるインターネットの歴史は高々半世紀ではあるが，今やインターネット無しでは産業界の経済活動や国民の生活活動も成り立たない，まさにインターネット（依存）社会である．社会の安心・安全は，インターネット上の活動の安心・安全に強く依存する時代となった．

インターネットの最大の課題は，利用者の確実な認証（本人確認）機能の欠如である．もともと研究者間のコミュニケーションツールとしての利用を想定されていたためであるが，世界各国の不特定多数の人々が利用する現在，インターネット上のさまざまの事故・

事件の氾濫を招き，大きな社会問題となっている．

一方，1985 年のショルダーホン発売に始まるモバイル端末の利用の進展も目覚ましく，2010 年にはモバイル端末からのインターネット利用がパソコンを上回り，モバイルインターネット時代に突入した．モバイルネットワークも 1985 年当時の 1 G から，2010 年当時の 3 G，そしてこれからの 5G へと発展してきた．

モバイルネットワークの場合，インターネットと異なり，事業者による有料サービスとして発展してきたため，一定レベルの利用者認証機能は実装されている．しかし，利用者認証にかかわるセキュリティ要件である，利用者の確実な本人確認，利用者の匿名性確保，不正・不法な利用者の特定・追跡の仕組みの面ではまだまだ課題も多い．

本稿では，モバイルネットワークサービス事業者が実施する利用者認証にかかわるセキュリティについて，5G の現状，Beyond5G/6G に向けた検討課題，研究動向等を報告する．

2. 利用者認証（本人確認）とその信頼性

インターネット上のサイバー空間における本人確認は，一般に身元確認と当人確認から構成される．

身元確認とは，サイバー空間で定義される仮想エンティティに対応するフィジカル空間の実エンティティ（登録利用者）の実在性，特定・追跡性を確認することである．当人確認とは，サービス要求者が身元確認された仮想エンティティが同一であることを確認することである．身元確認および当人確認により，登録利用者とサービス要求者が同一であることが確認され，本人確認が完了する（図 1）．

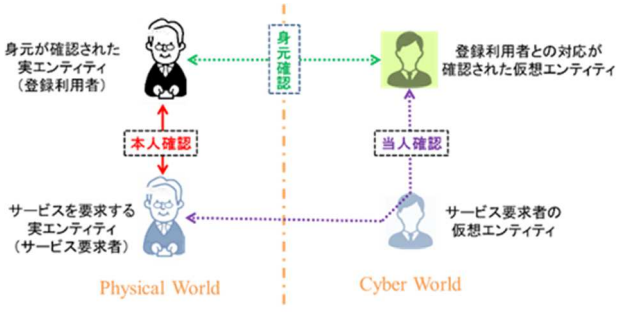

図 1　本人確認＝身元確認＋当人確認

このような本人確認を構成する身元確認および当人確認の信頼性については，米国 NIST が「Digital Identity Guidelines」[1]にまとめており，日本をはじめ多くの国が NIST のドキュメントをベースにインターネット上での本人確認方法に関するガイドラインを策定している．身元確認の信頼性レベルは，IAL（Identity Assurance Level）として，身元確認方法に応じて IAL1 から IAL3 の 3 段階に整理されている．当人確認の信頼性レベルは， AAL（Authentication Assurance Level）として，当人確認方法に応じて AAL1 から AAL3 の 3 段階に整理されている．

3. モバイルネットワークサービスにおける利用者認証にかかわるセキュリティ

モバイルネットワークにおける利用者認証は，利用者が契約するモバイルネットワークサービス事業者（HN サービス事業者）が実施する身元確認および契約利用者かどうかの確認をする当人確認（Primary Authentication）と，利用者が契約するアプリケーションサービス事業者が実施する身元確認および契約者かどうかの確認をする当人確認(Secondary Authentication)に分類される（図２）．

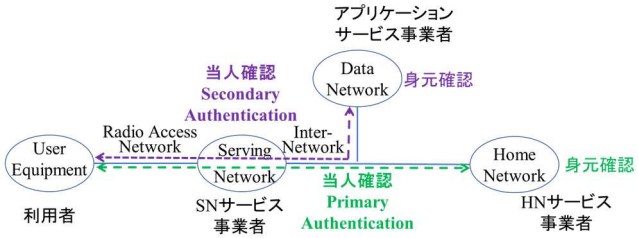

図２　モバイルネットワークの基本構成

本稿では，モバイルネットワークサービス事業者（HN サービス事業者）が実施する身元確認および当人確認（Primary Authentication）を対象としている．

HN サービス事業者は利用者との契約時に，利用者の実名や住所等の身元を確認し，身元情報および当人確認に使用する情報（当人確認情報）を登録する．

利用者は契約後のサービス要求時に，モバイルデバイス（UE：User Equipment）からアクセス可能なモバイルネットワーク（SN：Serving Network）経由，利用者が契約しているモバイルネットワーク（HN：Home Network）との当人確認（Primary Authentication）により契約利用者であることの確認を受け，モバイルネットワークサービスの利用が可能となる．

以上のような，モバイルネットワークサービスにおける利用者認証（本人確認）かかわるセキュリティの主要な要件は次の 3 項目である．

①確実な本人確認

＊HN サービス事業者が実施する利用者の身元確認を信頼できるかどうか

＊モバイルネットワーク上で実施される利用者の UE と HN 間の当人確認を信頼できるかどうか

②利用者の匿名性の確保

＊HN サービス事業者が管理する利用者情報（身元情報）の保護は確実かどうか

＊UE と HN 間の当人確認プロセスで送受される情報から利用者の匿名性が脅かされないかどうか

③合法的な利用者の特定・追跡性の確保

＊法執行機関は適切な手続きの元，当人確認プロセ

スで送受される情報から利用者を特定できる ID 等を入手できるかどうか

＊法執行機関は適切な手続きの元，利用者の追跡に必要な身元情報等を入手できるかどうか

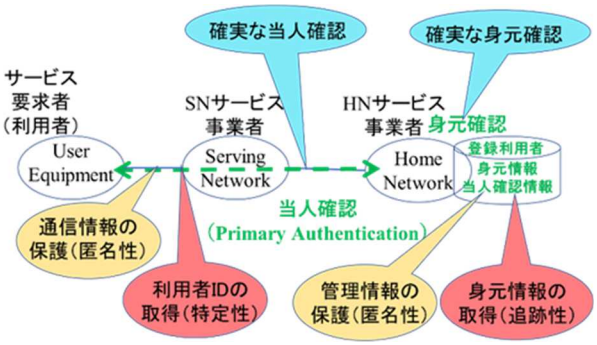

図３　利用者認証にかかわるセキュリティ課題

4. 5G における利用者認証にかかわるセキュリティ課題の現状

4.1　確実な本人確認

①身元確認

HN サービス事業者が契約時に実施する利用者の身元確認では，一般に各国の公的機関や民間組織で発行される身元に関する証明書等が利用され，身元確認方法は各国ごとに異なる．実施される身元確認の信頼性のレベルも身元確認方法ごとに異なっているものと考えられるが，現状，5G では身元確認方法やその信頼性のレベルに対する要件等は規定されていない．

なお，HN サービス事業者は契約時に，身元確認後，身元情報を HN 内に格納すると共に，当人確認用の情報として利用者固有の ID（SUPI：Subscription Permanent Identifier）および利用者固有の長期秘密鍵（K）を割り当て，HN および利用者の UE 内に格納する．

②当人確認

利用者がモバイルネットワークへアクセスする時には，UE と HN 間で共有する利用者固有 ID（SUPI）や長期秘密鍵（K）を使用し，契約利用者であることが確認（当人確認）される．具体的な当人確認のためのプロトコルとして，5G では 5G-AKA，EAP-AKA’および IoT 向けの EAP-TLS が定義されているが，本稿では 5G で新たに定義されたプロトコル 5G-AKA を対象とし以下に概要を示している（図４）．

5G-AKA では，利用者の UE は保有している利用者固有 ID（SUPI）を SN 経由で HN へ送信する．HN では，事業者が管理する利用者情報 DB を検索し利用者固有 ID（SUPI）に対応する契約者を特定する．次に，その利用者固有 ID（SUPI）に対応する長期秘密鍵（K）を利用者情報 DB から抽出し，この長期秘密鍵（K）を UE が保有するかどうかを確認し，契約利用者が保有する UE からのアクセス要求であることを確認する．

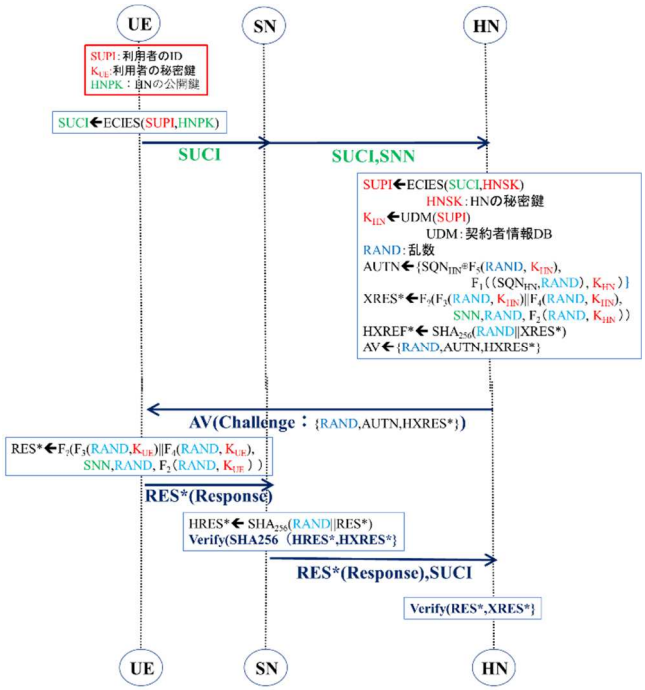

図４　5G-AKA の仕組み概要

4.2　利用者の匿名性の確保

①HN サービス事業者が管理する利用者情報の保護

利用者情報は，利用者の実名や住所，その他の個人情報やプライバシー情報の塊であり，匿名性維持の観点からは確実な保護が必要な情報である．

各国の HN サービス事業者が管理する利用者情報の保護については，HN サービス事業者が活動を展開する国の法制度やガイドライン等に基づき実施されている．その保護の確実性については各国で異なっていると考えられるが，現状，5G では保護の仕組みや保護のレベルに対する要件等は定義されていない．

②モバイルネットワーク上で送受される利用者に関する情報の保護

5G-AKA では，前節の②で記載したように，まず UE が保有する利用者固有 ID（SUPI）を HN へ送信するが，暗号方式 ECIES（Elliptic Curve Integrated Encryption Scheme）を利用し，都度生成される共通鍵により暗号化された利用者 ID（SUCI）へ変換し送信することにより，利用者固有 ID（SUPI）の送信情報からの漏洩を防いでいる．

HN では，受信した SUCI の復号により SUPI を得，その SUPI を使用し利用者に割り当てられた長期秘密鍵（K）を入手する．その長期秘密鍵（K）を UE が保有するかどうかは，長期秘密鍵（K）をハッシュ関数 HMAC-SHA-256 等により変換したワンタイム情報を使用したチャレンジ・レスポンス方式のプロトコルにより確認され，モバイルネットワーク経由の確認プロセスでの長期秘密鍵（K）の漏洩を防いでいる．

上記の通り，当人確認に必要な利用者固有の情報で

ある利用者固有 ID（SUPI）および長期秘密鍵（K）は共に暗号化，ワンタイム化しモバイルネットワーク上を流れるため，利用者の匿名性は一定レベル確保されていると考えられる．

4.3 合法的な手続きに基づく利用者の特定・追跡性の確保

①利用者の特定性

5G-AKA においてはモバイルネットワーク上を流れる利用者固有 ID（SUPI）は都度生成される共通鍵により暗号化された利用者 ID（SUCI）へ変換されており，モバイルネットワーク上を流れる情報から利用者固有 ID（SUPI）を特定するのは困難である．

しかし，SUCI の一部に含まれている HN サービス事業者を示す HNID（Home Network Identifier）は暗号化されておらず，利用者が契約している HN サービス事業者の特定は可能である．HN サービス事業者は SUCI を復号し SUPI を入手できるため，利用者が契約している HN サービス事業者の協力により，利用者固有 ID（SUPI）の特定は可能である．

②利用者の追跡性

利用者の追跡のためには，利用者の実名や住所等の利用者情報が必要であるが，当人確認のプロセスでは利用者情報はモバイルネットワーク上では送受されない．

利用者情報は，利用者固有 ID（SUPI）と対応付けられ，HN サービス事業者が管理している．①で述べたように，モバイルネットワーク上で入手した暗号化された利用者 ID（SUCI）から HN サービス事業者の協力により利用者固有 ID（SUPI）を入手でき，更に HN サービス事業者の協力によりその利用者固有 ID（SUPI）と対応付けられ管理されている利用者の追跡に必要な実名，住所等の身元情報を入手することが可能である．

5. Beyond5G/6G に向けた利用者認証にかかわるセキュリティ課題と研究動向

5.1 確実な本人確認

①身元確認

各国の HN サービス事業者による利用者の身元確認の信頼性レベルについては 5G でも規定されておらず，身元確認が不十分な事業者を利用した不正・不法な目的でのモバイルネットワーク利用により，社会の安心・安全が脅かされかねない．

2 章で述べたように，身元確認の信頼性については NIST の SP 800-63A「Enrollment and Identity Proofing Requirements」にて，身元確認方法の特徴に基づき信頼性レベル（Identity Assurance Level）が定義されている．グローバルなモバイルネットワークにおいても，HN サービス事業者が確保すべき身元確認の信頼性レベルおよびその評価・認定方法についての議論が始まり，ガイドライン等が策定されることが望ましい．

②当人確認

5G の当人確認プロトコル 5G-AKA では，IMSI catcher 等の４G で指摘されていた主な脆弱性については対応されている．

しかし，5G-AKA についても多くの研究が活発に展開され，様々の課題が提起されている．利用者のプライバシー情報（SUPI）等の漏洩，セッションの linkability（複数セッションが同一利用者であることの特定），ロケーション情報の漏洩，リプレイアタックによるなりすまし等につながりかねない脆弱性の指摘および様々の改善提案が行われている（[3]～[8]）．このような 5G の当人確認プロトコル（5G-AKA）の課題分析および改善提案の発展形として，Beyond5G/6G における当人確認プロトコルが形成されることも考えられる．

量子コンピュータへの対応も，Beyond5G/6G における当人確認の課題である．5G の当人確認への量子コンピュータの影響についても多くの調査・研究レポートが発表されている（[9]～[13]）．５G-AKA では，公開鍵暗号方式 ECIES を利用し利用者固有 ID（SUPI）を保護しているが，Shor アルゴリズムによりその安全性が脅かされ，また 128 ビットの鍵長の暗号鍵を使用した暗号化・ワンタイム化により長期秘密鍵（K）等を保護しているが，Grover アルゴリズムによりその安全性が脅かされることが指摘されている．今後の NIST における標準化・評価活動を睨みながら，Beyond5G/6G に向けた量子コンピュータ対応の当人確認方式案も多く提案されるものと想定される．

新たな技術の活用の観点から，Beyond5G/6G の利用者認証にかかわるセキュリティ課題へのより確実な対応・高度化を目指す研究も展開されている．

一つは Blockchain 技術である．5G の当人確認プロセス，モバイルねえとワークを構成する多くの機器を経由し実施される UE と HN 間の当人確認プロセスに Blockchain を利用し，UE と HN 間の通信を少なくし，応答性能向上，ネット負荷軽減と共に，モバイルネットワーク上を流れる情報からの利用者に関する情報の漏洩リスクを軽減する方式が提案されている（[14]～[16]）．

バイオメトリクス認証技術もその一つである．従来からの静的生体特徴を利用したバイオメトリクス認証も当人確認の高度化に有効であるが，動的生体特徴を利用したバイオメトリクス認証，連続的利用者認証を可能とする当人確認に関する研究が展開されている（[17]～[20]）．

なお，Beyond5G/6G 時代の UE がどのような形態で

どのような機能が搭載されるかによっては，当人確認方式/プロセスは大幅に変わる可能性もあり，新たに提起されるセキュリティ課題，新たに活用が可能となる技術も想定され，今後の研究開発，実用化の動向を注視する必要があろう．

5.2 利用者の匿名性の確保

①HN サービス事業者が管理する利用者情報の保護

各国の HN サービス事業者による利用者の身元情報の保護については 5G では規定されていない．身元情報の漏洩は，なりすまし等の不正なモバイルネットワークの利用を可能とし，身元情報の保護が不十分な HN サービス事業者の存在は，社会の安心・安全が脅かされかねない．

管理する情報の保護については，情報の機密性・完全性・可用性の維持を要求する情報セキュリティマネジメントシステムに関する国際規格 ISO27001 および適切な個人情報の取り扱いを要求する国際規格 ISO29100，それらの国際規格に基づく認証制度やグローバルな相互認証制度が存在する．グローバルなモバイルネットワークにおいても，HN サービス事業者が確保すべき身元情報の保護レベルおよびその評価・認定方法についての議論が始まり，ガイドライン等が策定されることが望ましい．

②モバイルネットワーク上で送受される情報からの利用者情報の保護

当人確認プロセスにおける匿名性の維持は，確実な当人確認の研究の一環として展開されており，**5.1** の②で述べた研究動向，論文リストを参照願いたい．

5.3 合法的な手続きに基づく利用者の特定・追跡性の確保

①モバイルネットワーク上で送受される情報からの利用者の特定性

Beyond5G/6G における当人確認は 5G の脆弱性を克服し，利用者の匿名性も強化される見通しで，利用者の匿名性確保の観点からは好ましいが，利用者の特定・追跡は 5G に比べ更に困難になることが考えられる．しかし，Beyond5G/6G においても HN サービス事業者が契約利用者かどうかを確認できる情報が UE から送信される必要があり，5G と同様の通信情報の収集と HN サービス事業者の協力により，利用者固有 ID の特定は可能できると考えられる．5G において合法的傍受の仕様（[6]～[8]）が定められているが，Beyond 5G/6G においても新たな当人確認方式，Blockchain 等の異なるルートを経由した当人確認方式に対しても同様の仕組みが必要と考えられる．

②利用者の追跡性

Beyond5G/6G においても，利用者の追跡に必要な身元情報がモバイルネットワーク上を流れることは考えられず，利用者の身元情報入手には当該利用者が契約する HN サービス事業者の協力が不可欠である．他国の HN サービス事業者の協力を得るには，HN サービス事業者を管轄する国の捜査当局の協力が必要であろう．

社会の安心・安全のためには，法執行機関による利用者の特定・追跡の仕組みが必要であるが，その実現にあたっては，技術仕様のみならず各国の捜査機関間の連携の仕組みも必要であろう．Beyond5G/6G の検討・議論においては，法執行機関による社会の安心・安全維持のための仕組みに関する議論も必要と考える．

6. おわりに

Beyond5G/6G モバイルネットワークサービスにおけるネットワークアクセス時の利用者認証にかかわる三つのセキュリティ要件，確実な本人確認，利用者の匿名性，利用者の特定・追跡性について，利用者の契約時の HN サービス事業者による身元確認および利用者のサービス要求時のモバイルデバイス（UE）と契約モバイルネットワーク（HN）間で実施される当人確認（Primary Authentication）のセキュリティの５G の現状および Beyond5G/6G の課題や研究動向を整理・考察した．

Beyond5G/6G に向け更に発展が期待され，産業界の経済活動や国民の生活活動を支えることになると考えられるモバイルネットワークサービスにおける利用者認証にかかわるセキュリティ課題は，技術的側面および社会的側面の両面から検討が必要であろう．

技術的側面としては，Beyond5G/6G に期待される超安全・信頼性を実現すべく，利用者認証にかかわるセキュリティの高度化を目指した研究開発・標準化活動が必要であろう．なお，Beyond5G/6G のアーキテクチャおよびその上でのサービスのイメージが具体化するにつれ，新たなセキュリティ課題の発生が想定され，一方，研究開発の進展によりセキュリティ分野で活用可能な新たな技術の出現も想定される．今後の Beyond5G/6G の具体化に関する議論を注視しつつ，利用者認証にかかわるセキュリティ課題および研究課題の見直しも適宜必要となろう．

社会的側面としては，個人の権利を尊重した匿名性と社会の安心・安全の維持のための不正・不法な利用者の特定・追跡性の両立に関する国民の合意形成が必要であろう．また国際連携も重要で，各国の主権の尊重とグローバルなインターネット社会の安心・安全を確保するための国際連携，に関する国際的合意形成も必要であろう．

謝辞 本研究の一部は，一般財団法人テレコム先端技術研究支援センターの研究助成を受けている．

文　献

[1] 「Digital Identity Guidelines」, NIST Special Publication 800-63-3, June 2017.
https://pages.nist.gov/800-63-3/

[2] 3GPP Specifications.
https://www.3gpp.org/specifications

[3] “Novel 5G Authentication Protocol to Improve the Resistance Against Active Attacks and Malicious Serving Networks”(2019)
https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8706883

[4] “A Survey of Subscription Privacy on the 5G Radio Interface - The Past, Present and Future” (2020)
https://eprint.iacr.org/2020/101.pdf

[5] “Private Identification of Subscribers in Mobile Networks : Status and Challenges” (2019)
https://ieeexplore.ieee.org/document/8847241

[6] “The SUCI-AKA Authentication Protocol for 5G Systems” (2020)
https://ojs.bibsys.no/index.php/NIK/article/view/885

[7] “Component-Based Formal Analysis of 5G-AKA:Channel Assumptions and Session Confusion”（2018）
https://people.cispa.io/cas.cremers/downloads/papers/CrDe2018-5G.pdf

[8] “Formal Verification and Analysis of Primary Authentication based on 5G-AKA Protocol”（2020）
https://ieeexplore.ieee.org/abstract/document/9143899

[9] “Study on the support of 256-bit algorithms for 5G(Release 16)”(3GPP,2019)
https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3422

[10] ”TUTORIAL: Post-Quantum Cryptography and 5G Security”(NIST,2019)
https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=927805

[11] ”An overview of cryptographic primitives for possible use in 5G and beyond”(2020)
https://link.springer.com/content/pdf/10.1007/s11432-019-2907-4.pdf

[12] ”The Quantum Computing Threat to Cybersecurity and 5G Security”(2019)
https://www.linkedin.com/pulse/quantum-computing-threat-5g-security-marin-ivezic/

[13] “Identity Confidentiality in 5G Mobile Telephony Systems” (2018)
https://pure.royalholloway.ac.uk/portal/files/31392585/Accepted_Manuscript.pdf

[14] ”Blockchain-based Authentication for 5G Networks” (2020)
https://ieeexplore.ieee.org/document/9089507

[15] ”A Security Authentication Scheme of 5G Ultra-Dense Network Based on Block Chain”(2018)
https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8470085

[16] ”A blockchain-enabled 5G authentication scheme against DoS Attacks”(2020)
https://iopscience.iop.org/article/10.1088/1742-6596/1812/1/012030/pdf

[17] ” Mobile Based Continuous Authentication Using Deep Features” (2018)
https://www.sigmobile.org/mobisys/2018/workshops/deepmobile18/papers/Mobile_Based_Continuous_Authentication.pdf

[18] ” Authentication of Smartphone Users Using Behavioral Biometrics”(2019)
https://arxiv.org/pdf/1911.04104.pdf

[19] ” Using behavioral biometric sensors of mobile phones for user authentication”(2019)
https://www.sciencedirect.com/science/article/pii/S1877050919313845

[20] ”Mobile terminal identity authentication system based on behavioral characteristics”(2020)
https://journals.sagepub.com/doi/full/10.1177/1550147719899371