

DeepL Proに登録して、プレゼン資料を編集しましょう  
詳しくは[www.DeepL.com/pro](https://www.deepl.com/pro?cta=edit-document)をご覧ください。

要旨-スマートフォンは、プライベートメッセージや財務データなどの機密データを管理するために使用されることが多いため、信頼性の高い識別と認証が日常生活において重要である。最近のハードウェアフィンガープリントの研究では、メーカーに関係なく、各スマートフォンはユニークで堅牢、かつ物理的にクローン不可能な様々なハードウェアフィンガープリントを持っていることが示されています。しかし、従来の指紋認証方式は、登録時のオーバーヘッドが大きい、あるいは、指紋偽造による攻撃を受けており、認証システムとして実用的ではありません。本論文では、内蔵カメラの光応答不均一性（PRNU）を利用したリアルタイムスマートフォンオー認証プロトコル「ABC」を提案します。従来のカメラでは、信頼性の高いPRNUの特徴量を構築するために数十枚の画像を必要としましたが、我々は、スマートフォンのイメージセンサーが持つ固有のPRNUにより、1枚の画像だけでスマートフォンを一意に識別できることを初めて観測しました。この発見により、PRNUを用いたスマートフォン認証が実用化されます。ABCは、既存のハードウェア指紋の多くが偽造攻撃に弱いのに対し、可視光通信路を用いたチャレンジレスポンスプロトコルによりスマートフォンのPRNUを検証することで、偽造攻撃に打ち勝ちます。また、時変QRコードはリプレイ攻撃にも対抗することができる。40台のスマートフォンの16,000枚の画像を用いた実験の結果、ABCは0.5%以下のエラーレートで効率的にユーザーデバイスを認証できることがわかった。 I. はじめに「ユーザーが持っている何か」によって個人を識別する認証システムは、なりすましを防ぐためにますます重要な役割を果たすようになってきている。侵害レベル指数[30]によると、2013年以降、平文パスワードや指紋を含む92億件のデータレコードが失われています。このような情報漏えいにより、知識ベース認証は大きく破られ、デバイスを使ったなりすまし攻撃[12]などの脅威がバイオメトリクスベース認証に及んでいます。そのため、デバイスとユーザーの同一性を確認する多要素認証の研究・実装が盛んに行われています。この文献では、スマートフォンを識別するための一般的な方法論の1つとして、内蔵センサーの指紋を区別することが挙げられています。センサーの指紋は、製造上の欠陥によって発生したセンサーの読み取りの系統的な歪みである。このような歪みは、個々のハードウェアに対して一定であり、異なるデバイス間の強い多様性を示す。モーションセンサー、WiFiチップセット、スピーカーのフィンガープリント[20], [37], [6], [8]は、それぞれスマートフォンを識別するのに十分強いことが証明されている。しかし、既存の方法のほとんどは、2つのセキュリティ要件を満たすことができません。しかし、ほとんどの既存方式は、指紋漏えい耐性と指紋偽造耐性という2つのセキュリティ要件を満たしていません[4]。スマートフォンに搭載されたセンサーを盗むことは不可能ですが、そのセンサーが生成する信号は、ほとんどの場合、一般に公開されています。これらの信号を収集した敵対者は、被害者のハードウェア指紋を抽出し、偽造信号を合成する可能性があります[8]、[14]。このような指紋偽造攻撃に対する脆弱性があるため、実際には実現不可能なのです。アニメーションセンサーの光応答不均一性（PRNU）[33]は、デジタルフォレンジックにおいて従来のデジタルカメラを識別する物理層指紋として使用されてきました。本論文では、スマートフォンの画像センサーのPRNUを利用してユーザーの端末を認証し、様々な不正や攻撃に対抗することを検討しています。まず、大きなレジストレーションのオーバーヘッドをなくすこと。従来のデジタルカメラでは、1つの基準指紋を得るために少なくとも50枚の画像が必要でした。このような大きな登録オーバヘッドは、実用的なスマートフォン認証プロトコルの実現には困難な場合があります。2つ目は、なりすまし攻撃への対応です。PRNUベースのフィンガープリントメソッドは、指紋偽造攻撃[27], [36], [24], [38]にも弱いという弱点があります。被害端末になりすますために、敵対者は公開画像から被害端末の指紋を推定し、得られた指紋を自身の端末で撮影した画像に埋め込むことが可能です。既存の偽造検出機構は、信頼性の低さ[27]や膨大な送信・保存オーバーヘッド[36]に悩まされています。我々は、PRNUを使用してスマートフォンを識別・認証する際のこれらの課題に対処するため、スマートフォンカメラのPRNUの特性を理解するための幅広い実験を実施しました。その結果、スマートフォンのイメージセンサーは、従来のデジタルカメラに比べて数十分の一の大きさであることがわかりました。同じレベルの製造誤差であれば、イメージセンサーの寸法が小さくなることで、画素の寸法不均一性が増幅され、より強いPRNUが生成されます。その結果、スマートフォンカメラのPRNUは非常に強く、1枚の画像からスマートフォンカメラを特定できることがわかりました。そこで、スマートフォンで撮影した画像のノイズ残量から推定したPRNUを直接、参照指紋として用いることを提案します。また、スマートフォンのカメラに固有のPRNUを考慮し、様々な攻撃にも対抗できるPRNUベースのスマートフォン認証プロトコールであるABCを提案します。ABCは、登録フェーズと認証フェーズを含んでいます。登録段階では、ユーザは撮影したばかりの画像を検証者／サーバにアップロードします。この画像から、検証者はユーザーのスマートフォンの指紋を推定する。このQRコードには、現在進行中の取引の概要、乱数、タイムスタンプがそれぞれ符号化されています。それぞれのQRコード画像には、撮影には耐えられるが指紋の除去には耐えられないセミフラジャイルプローブ信号も埋め込まれています。ユーザーは、スマートフォンを画面と平行に置き、2つのQRコードを撮影する。そして、QRコードのメッセージを検証し、その画像を検証装置にアップロードします。ユーザが撮影した画像を受け取った検証者は、以下の手順でユーザの端末を認証します。1) 2つの時変QRコードとターゲットのスマートフォンの指紋の存在を検出する。2つのQRコードにより、リプレイ攻撃や中間者攻撃に対抗することができます。2) 受信した2つのQRコード画像の類似度を測定することで、指紋の偽造を検出する。これは、敵対者が偽造した2つの画像には、被害者端末の指紋と敵対者端末の指紋の両方が含まれており、著しく高い類似度値が発生するという観察結果に基づくものです。3）敵対者が偽造画像から自分の端末のPRNUを削除した場合、受信した各画像に埋め込まれたプローブ信号の強度を確認することにより、指紋削除を検出することができます。また、PRNUに基づき、1枚の画像からスマートフォンを識別できることを世界で初めて確認しました。Amazon Mechanical Turkを通じてスマートフォンの画像を収集し、大規模な実験を行った結果、スマートフォンのカメラを識別する際に0.5%以下の誤差を達成することができました。この新発見により、PRNUをスマートフォンの認証に利用することが現実的になりました。本提案では、以下の特徴を持つ。1) 写真1枚を登録する程度のオーバーヘッドで、安全な物理層スマートフォン認証を実現する。2) 4,000枚の偽造画像を用いた実験により、ABCは指紋偽造攻撃を0.47%以下の誤検出率で検出できることを実証しました。3) スマートフォン利用者にとって身近で便利な写真撮影を要件とするため、提案プロトコルのユーザビリティは維持される。セクション II では，現在の PRNU ベースのデジタルカメラ指紋認証方式をレビューする．セクション III では、本論文で取り組むべき問題を定式化する。セクションIVでは、我々のスマートフォン認証プロトコルを紹介する。セクションVでは、提案プロトコルのセキュリティ機能を分析する。セクションVIでは、性能評価を行う。セクションVIIでは、ハードウェアフィンガープリントに関する関連する既存の研究をレビューします。セクション VIII はこの研究の結論です。このセクションでは、まず一般的なPhoto Re-sponse Non-Uniformity (PRNU) based camera fingerprintingtechniqueを紹介し、デジタル画像と対応するカメラの間のリンクを確立する。A. PRNUに基づくカメラ指紋認証PRNU [33], [23] は、イメージセンサーの光に対する感度が一様でないことが原因である。これは、実際の光学的視野に乗法的な要素を導入するものである。実際のセンサー出力をIとし、実際の光学的視野をI(0)とする。デジタルカメラで撮影された画像は、I = I(0) + I(0)K + Θ、(1)ここでKはカメラのPRNU、Θは撮影ノイズや読み出しノイズなど他のノイズ成分を表す。PRNUは3から5の分散を持つ白色ガウスノイズ変数のように振る舞うので、ノイズ除去フィルターを使って抽出できる [33], [10].ここで、Ξ(i)はΘとその他の微小成分を組み合わせたランダムなノイズ成分です。従来のデジタルカメラの場合、その撮像画像のノイズ残差は非常にノイズが多く、指紋として直接利用することはできません。そこで、平均化処理によりランダム成分（Ξ(i)）を低減し、PRNU（K）を向上させる[7]。得られた指紋は、ˆK =∑Ni=1 W(i)I(i)∑Ni=1(I(i))2 = K + ∆、(3) ∆は推定指紋ˆKと実指紋Kの差である、(3) 式で表すことができる。推定指紋の品質はq =corr(K, ˆK) [27]として定義され、これは推定指紋と実際の指紋の間の類似度である。個々のデバイスについて、qは平均化処理で使用される画像数に正の相関がある。最も一般的に使用される類似性メトリックは相関エネルギーに対するピーク（PCE）[26]である。クエリー画像が関心のあるカメラによって撮影されたかどうかを決定するために、既存の指紋検出戦略は、少なくとも50画像から抽出したそのカメラの参照指紋に対して画像のノイズ残留物を相関させている。この戦略に従い、Goljanら[28]は6896台の個々のカメラで撮影された100万以上の画像でカメラのフィンガープリントの正確さとユーザーの能力を証明しました。B. 指紋偽造攻撃と対策被害者の公開画像から推定したPRNU指紋ˆKを用いて、敵は式（4）、J′＝J（1＋αˆK）、（4）ここでJは外国の画像で、αは注入された指紋の強さを制御することにより偽造画像を作成することが可能である。適切なαにより、偽造された画像は様々な指紋検出スキームを容易に通過することができる。最先端の指紋偽造検出メカニズムには脆弱な指紋[36]と三角形テスト[27]がある。脆弱な指紋はPRNUノイズのうち、壊れやすくロッシーJPG圧縮により除去されるコンポーネントを探る。オンライン共有画像の大部分がJPGフォーマットであるという観察に基づいて、このメカニズムは逆者が公開JPG画像から指紋を抽出すると想定し、その指紋は脆弱な指紋を含まないことを前提とする。ユーザが認証のために非圧縮の生画像を提出する必要がある場合、クエリ画像のノイズ残量と対象カメラのフラジャイルフィンガープリントとの相関関係から、指紋偽造攻撃を検出することができます。しかし、この方法では、リファレンスフィンガープリントを推定するために300枚の生画像を必要とし、膨大な伝送コストがかかります。また、この手法の頑健性は、生画像の秘匿性に依存します。三角形テストは、注入されたフィンガープリントˆKが、敵が使用する全てのノイズ残留物W(i)と追加のノイズ成分Ξ(i)を共有するという観察に基づく。これらの共有Ξ(i)はˆKとすべてのW(i)の間のPCE値を急激に増加させます。そのため、偽造画像を検出するために、敵対者がアクセスできる可能性のあるすべての候補画像をテストします。しかし、画像共有の普及により、検証者が敵対者がアクセス可能なすべての候補画像を収集することは不可能である。このセクションでは、まず、システムモデルと脅威モデルを紹介する。次に、認証システムの設計目標について議論する。図1 システムモデル図1 システムモデル 検証者は、スマートフォンの内蔵カメラの指紋を追跡することで、ユーザのスマートフォンを認証する。検証者はまず、スマートフォンのインタフェースに表示された画像を撮影し、アップロードするよう要求します。A. システムモデル スマートフォン認証は、ユーザーの所有物（スマートフォン）を認証するプロセスです。従来、スマートフォンの認証は、プリインストールされたアプリや追加ハードウェア（例：iPhoneのセキュアエルイーメント）により制御される秘密鍵を用いて実現されていた。また、提案するABCは、従来の暗号方式と統合することで、ユーザーエクスペリエンスを損なうことなく、より高い安全性を提供することができます。このシステムは、ユーザー、スマートフォン、検証者の3つのエンティティで構成されています。ユーザーは、取引やログインを行う際に、認証が必要になります。スマートフォンにはカメラが内蔵されており、セキュリティトークンとして機能する。ユーザーは、検証機のインターフェイスと対話し、このセキュリティ・トークンを検証機に提供することで認証されます。検証機は、インターフェースとサーバーから構成される。一般性を損なわないために、ここではPOS端末を用いて、スマートフォンのPRNUによる認証プロセスを説明します。検証者（銀行）は、各ユーザーの口座識別子（例：カード番号）と参照用PRNU指紋を格納するデータベースを保持します。ユーザがPOS端末で決済を行う場合、検証者はユーザにスマートフォンを要求し、端末の画面を撮影させます。ユーザーは、撮影した画像と自分の口座番号を銀行にアップロードします。検証者は、画像からユーザーのスマートフォンの指紋を抽出し、対象口座の参照指紋と関連付けます。相関が閾値より高ければ、取引は実行されます。このように、PRNUベース認証では、スマートフォンという "持っているもの "に依存した認証を行っています。1）検証者のインターフェースからスマートフォンに内蔵されたカメラへの可視光通信（VLC）チャンネル。検証者はVLCチャンネルを利用して、スマートフォンが撮影した画像に情報を埋め込む2）スマートフォンと検証者の間のワイヤレスチャンネル。2）スマートフォンと検証機の間の無線チャネル。スマートフォンは、撮影した画像を検証機に送信するために無線チャネルを使用します。B．脅威モデル我々は、被害者ユーザーについてすべてを知っており、例えば、悪意のあるインターフェースを展開することによって、被害者と検証機の間の通信を盗聴して変更できる強力な敵対者を仮定します。敵対者の目的は、正規のユーザーになりすまし、悪意のあるリクエストを承認することである。また、敵対者は、被害者がスマートフォンで撮影したあらゆる画像にアクセスできると仮定する。このような画像は、例えば、Facebookなどのオンラインソーシャルネットワークで共有される画像など、いずれにせよ非公開にされるべきものである可能性がある。ここで、再びPOS端末の例を用いて、2つのケースで潜在的な攻撃について考察します。1）敵対者は、被害者の銀行口座で決済を行おうとする悪意のあるユーザーである。1）敵対者は、被害者の銀行口座で支払いを行おうとする悪意のあるユーザーであり、被害者の口座識別子と被害者のデバイスで撮影された画像を知っている。敵対者は、以下の攻撃を行うことができる。リプレイ攻撃 - 犠牲者のスマートフォンから検証者に以前の画像トークンをリプレイする。このようなトークンは、以前の認証セッションから被害者スマートフォンの無線チャネルを盗聴することによって取得することができます。指紋偽造攻撃：被害者スマートフォンの指紋と敵対者の画像からなる偽造画像トークンをアップロードします。2) 敵対者は、被害者を誘い出し、悪意のある支払いを承認させようとする悪意のある商人である。被害者の取引を処理するPOS端末を制御する。この敵対者は、さらに中間者攻撃（Manin the middle attack）を行う可能性がある - 敵対者は、被害者のユーザーの進行中の取引を密かに変更する。C. 設計目標私たちは、堅牢で使いやすいスマートフォン認証システムの設計目標として、以下の項目を想定しています。リアルタイム認証：正確なリアルタイム認証が可能なプロトコルであること。指紋照合と攻撃検知の両方が効率的であることが望ましい。関係するオーバーヘッドは、すべての関係するエンティティのための最小値と耐容でなければなりません。提案されたシステムこのセクションでは、私たちのリアルタイムスマートフォン認証システムを紹介します。まず、PRNUをスマートフォンのユニークなアイデンティティとして使用することの実現可能性を調査する。A. Smartphone Camera FingerprintingTable I [1]によると、スマートフォンのカメラとデジタルカメラのイメージセンサーは類似していますが、スマートフォンのイメージセンサーは従来のデジタルカメラのイメージセンサーより数十倍小さくなっています。スマートフォンのイメージセンサーは、従来のデジタルカメラのイメージセンサーと比較して数十分の1の大きさであるため、イメージセンサーが受ける光の量が少なく、撮影した画像のSNR（信号対雑音比）が悪くなることが分かっています。そこで、スマートフォンカメラのPRNUの特性を調べるため、40台のスマートフォンから16,000枚以上の画像を収集し、そのノイズ残量を評価しました。その結果（図2）、同じスマートフォンカメラのノイズ残量には非常に強い相関があることが分かりました。スマートフォンカメラが生成する指紋は、従来のデジタルカメラが生成する指紋よりもはるかに強いことが分かりました。これは、スマートフォンのイメージセンサーの画素サイズが小さいことに起因していると思われます。次に、スマートフォンのカメラで撮影された画像の間に強い相関があることを示します。通常、認証は屋内で行われるため、テスト画像と参照画像がともに屋内画像である場合について検討しました。1）一致画像ペア：同じスマートフォンで撮影された2つの画像を含むペア，2）非一致画像ペア：異なるスマートフォンで撮影された2つの画像を含むペア，の2種類の画像ペアを作成しました．iPhone 6の場合、一致画像ペア1250枚、非一致画像ペア1150枚をテストしました。Galaxy Note5では、一致画像4000枚、非一致画像5300枚のペアをテストしました。図2は、得られたPCE値の分布を示しています。両モデルとも、マッチング画像ペアのPCE値は、非マッチング画像ペアのPCE値よりも有意に高いことがわかります。閾値を用いて一致画像ペアと非一致画像ペアを区別することで、図3に示すようなROC（Receiver Operating Characteristic）が得られました。図3に基づき指紋照合の総合エラー率を最小化するため、照合閾値としてiPhone 6では7.4338を、Galaxy note 5では13.0704を選択しました。iPhone 6の場合、この閾値は0.08%の偽陽性率と0.71%の偽陰性率になります。また、Galaxy Note 5の場合、選択した閾値は0.16%の偽陽性率、0.94%の偽陰性率となった。両モデルとも、PRNUは環境光の強度が低い場合でも高い精度で画像ペアを識別することができた。このことから、1つの画像だけで、スマートフォンを一意に識別するための参照指紋として利用できることが示唆されました。さらに、識別精度を向上させるためには、環境光の強度を上げるか、明るい画像から抽出した参照指紋を使用することができます。VI章で示すように、画像が明るい環境（屋外など）で撮影された場合、指紋検出戦略は100％の精度を達成することができる。高品質の指紋のため、スマートフォンのカメラ指紋は、次の点でデジタルカメラの指紋とは異なる。指紋検出戦略 - すべてのキャプチャ画像上の高品質な指紋で、我々はもはや参照指紋を推定するために、画像の多くを取得する必要はありません。したがって、スマートフォンのカメラでは、1枚の画像のノイズ残りを参照指紋として使用することができます。指紋偽造 - PRNUをスマートフォンカメラの指紋認証に使用すると、指紋偽造攻撃に対して脆弱になります。スマートフォンのカメラで撮影したすべての画像に高品質の指紋があれば、敵はたった1枚の参照画像で指紋偽造攻撃を行うことができます。B. 基本的な認証方式III-Cで述べた3つの設計目標を達成する本格的なABCプロトコルを紹介する前に、カメラ指紋を用いたスマートフォン認証システムのフレームワークと2つの基本方式を紹介します。1) システムのフレームワーク。図4は、2段階の認証プロセスのユースケースを示したものです。登録：検証者は、対象スマートフォンの指紋プロファイルを構築します。このフェーズでは、対象スマートフォンの参照指紋、スマートフォンのメーカーとモデルを収集する。登録プロセスは、検証者のインターフェイス上で行われる。認証：検証者はリアルタイムでスマートフォンを認証する。2) 基本方式I：図5に示すような、リプレイ攻撃や中間者攻撃に対抗できる認証方式です。基本方式I：図5に示すように、リプレイ攻撃や中間者攻撃に対抗できる認証方式であり、現在進行中のトランザクションを抽象化し、新たに構築したシーンを撮影するチャレンジレスポンス方式を搭載している。登録段階では、ユーザの参照画像I(r)に制約を与えない。認証フェーズでは、ユーザから参照画像を受け取ると、検証者はこの画像に含まれる指紋ˆK（c）を抽出し、このスマートフォンのプロファイルP（c）を作成する。ユーザはスマートフォンでQRコードを撮影し、QRコードに埋め込まれたトランザクションを確認する。このとき，ユーザのリクエストに何らかの変更が加えられると，ユーザに気づかれてしまう（中間者攻撃の撃退）．次に、ユーザは撮影した画像I(c)を検証者にアップロードする。最後に、検証者は画像内容照合と指紋照合を行い、認証の判定を行う。画像内容照合では、受信した画像から新たに提示されたQRコードを検出し、認証プロセスの有効性を確保する。指紋照合は、QR画像から抽出したノイズ残量と対象スマートフォンの参照指紋を照合し、受信画像の製作者を検証します。この方式は、利便性が高く、リプレイ攻撃や中間者攻撃には強いものの、指紋偽造攻撃には弱いという欠点があります。本方式は、利便性が高く、リプレイ攻撃や中間者攻撃への耐性に優れていますが、指紋偽造攻撃に対して脆弱です。認証プロセスにおいて、敵対者は提示されたQRコードを外国のスマートフォンで撮影し、その画像に被害者であるスマートフォンの指紋を埋め込むことができます。3) Basic Scheme II: Basic Scheme Iに対する指紋偽造攻撃に対処するため、Basic Scheme IIでは、最新の偽造検出メカニズムである三角形テストを採用しています。完全な履歴画像セットがあれば、三角形テストは、受信した画像に偽造指紋が含まれているかどうかを高い信頼度で判断することができます。三角形テストは、検証者に対して2つの要件を持つ。1) 対象スマートフォンの参照指紋ˆK(c)は、敵対者がアクセスできないプライベート画像から抽出されること、2) 検証者は、対象スマートフォンの履歴画像セットを保持すること。図6は第2のベースライン認証方式である。この方式の登録フェーズでは、ユーザは履歴画像集合｛I1, ..., IN｝と撮影したばかりの画像I(r)をアップロードすることが要求されている。また、本方式では、登録時に履歴画像｛I1...IN｝と撮影画像I(r)の読み込みを要求し、検証者はこれらの画像からノイズ残量を抽出し、スマートフォンのプロファイルP(c)を作成する。検証者は、まずクエリ画像のノイズ残量W(q)を抽出し、各履歴画像のノイズ残量W(i)に対して、W(q)とW(i)の類似度ηを計算する。閾値以上のηがあれば、I(q)はW(i)を使って作られた偽造画像であることが示唆される。この三角形テストは指紋偽造攻撃に対する脆弱性を解消するものであるが、以下のような欠点がある。1) この方式は実時間認証を保証できない。1) この方式はリアルタイム性を保証できない。検証者は履歴画像集合全体をテストする必要があるため、画像集合のサイズが大きくなると、応答時間が大幅に増加する可能性がある。2) ユーザと検証者に大きな負担を強いる。スマートフォンの履歴画像セットを最新の状態に保つために、ユーザは新しい画像を公開するたびに検証者に通知する必要があります。3) 履歴画像セットの完全性を保証することが困難である。履歴画像セットが不完全な場合、検出結果の信頼性が低くなる。C. 本格的な認証プロトコル2つのベースライン方式の欠点を克服するためには、指紋偽造攻撃に対する信頼性の高いリアルタイム検出メカニズムが必要である。ABCは、敵対者のスマートフォンの指紋を追跡することで偽造攻撃を検出します。この指紋は、敵対者が自分のスマートフォンでチャレンジQRコードをキャプチャするチャレンジレスポンスの段階で導入されます。この指紋は、敵対者が自分のスマートフォンでチャレンジQRコードをキャプチャするチャレンジレスポンス段階で導入されます。この攻撃側のスマートフォンの指紋は偽造画像に保存されるため、その存在は指紋偽造攻撃を示唆するものです。ABCは、スマートフォンで撮影したばかりの2枚の画像をアップロードする必要があります。これらの画像が敵によって偽造された場合、そのノイズ残基には被害者端末の指紋と敵対者の指紋の両方が含まれることになります。カメラの指紋はノイズ除去フィルターで除去できるため、敵は被害端末の指紋だけを含む画像を偽造することができます。ABCは、指紋が除去されても撮影に耐えるプローブ信号を各チャレンジに埋め込み、受信した画像にプローブ信号が存在するかどうかを確認することで、指紋除去を検出します。登録段階は基本方式Iと同様であり、ユーザから1枚の参照画像を収集するのみである。認証フェーズは以下の通りである。検証者は，取引概要，タイムスタンプ，およびランダム文字列を符号化した2種類のQRコードを生成する．各QRコードには独立した白色ガウス雑音Γi（分散は5）が埋め込まれている（図8）。攻撃検知フロー：ユーザは進行中の取引の情報を確認しているので、検証者はリプレイ攻撃と指紋偽造攻撃を検知すればよい。QRコードによる挑戦的な場面は、Ii（s）＝QR（stri，Ti）＋Γi，i＝1，2と表すことができる。検証者は、2つのQRコードを順番にインタフェースに表示する。ステップ2.ユーザはI1(s)とI2(s)をキャプチャし、キャプチャした画像を無線チャネルを通じて検証装置にアップロードする。ステップ3.ユーザーがアップロードした画像を受け取った検証者は、図8に示すような動作を行い、ユーザーのスマートフォンを特定します：画像内容の照合。画像内容の照合。受信した画像からチャレンジングなQRコードを検出する。これは、市販のQRコードスキャンツールで簡単に実現できます。受信した各画像のノイズ残量と参照画像のノイズ残量を関連付けることにより、受信画像からターゲットスマートフォンのカムエラフィンガープリントK(c)を検出します。受信画像から敵対者のカメラ指紋K(a)を検出する。アルゴリズム2に示すように、検証者は各受信画像Ii（c）のノイズ残量Wi（c）を抽出し、それらの類似度P CE（W1（c）, W2（c））を計算する。これらの画像が広告主によって偽造された場合、W1(c)とW2(c)にはK(a)とK(c)が含まれ、P CE(W1(c), W2(c)) は通常の類似値P CE(W1(c), ˆK(c)) より著しく高くなる。受信画像中の付加された白色ガウスノイズΓiを検出する。アルゴリズム3に示すように、検証者はまず各受信画像Ii(c)をサブサンプリングし、ˆIi(c)を得る。適切なサブサンプリング手法により、ˆIi(c)には埋め込まれたプローブ信号Γiが含まれるはずである。検証者は、Γi とˆIi(c)のノイズ残差の間の類似値を計算する。V. セキュリティの分析このセクションでは、リプレイ攻撃、中間者攻撃、指紋偽造攻撃に対する耐性を検証することにより、ABCプロトコルのセキュリティを分析します。ABCは、リプレイされた画像を検出するために、ランダムな文字列とタイムスタンプがエンコードされたQRコードを新たに生成し、ユーザーに撮影させることを要求します。ランダムな文字列は、提示されたQRコードが予測困難であることを保証し、タイムスタンプは、各QRコードが各ユーザに対して一度だけ使用されることを保証します。このように、検証者は受信画像中の提示QRコードの存在を確認することで、リプレイアタックを検知することができます。この活性化検知機構の信頼性は、主に提示された課題のエントロピーによって決定される。QRコードの場合、最も低いバージョンのQRコードでさえ、5.7×1045通りの画像を生成することができます[2]。このため、敵対者が将来の認証プロセスで要求されるQRコードを予測することはほとんど不可能です。B. Man in the Middle攻撃敵対者は、ユーザと検証者の間の通信を改ざんすることで、正規のユーザを誘い出し、悪意のある要求を許可させようとすることがある。攻撃プロセスは以下の通りである。1) 正規のユーザーが検証者のインタフェースでリクエストを開始する。2) 敵対者（例えば、悪意のある端末）は、ユーザーのリクエストを傍受し、検証者に悪意のあるリクエストを送信する。3) 検証者のサーバーは、生成したばかりのQRコードをインターフェースに送信し、ユーザーにQRコードのキャプチャを要求する。4) ユーザがスマートフォンで画像を撮影し、アップロードする。4) ユーザはスマートフォンで画像を撮影し、アップロードする。ユーザが提示したスマートフォンは確かに正規のものなので、撮影された画像は認証プロセスを通過する。しかし、このスマートフォンで認証された取引は、ユーザーが要求した取引ではありません。この攻撃に対処するため、ABCはさらに、チャレンジングQRコードに進行中の取引の概要を埋め込むことにしました。認証プロセスにおいて、ユーザーはチャレンジングQRコードをキャプチャし、トランザクションの情報を確認することが要求されます。この設計により、中間者攻撃を行う敵対者は、チャレンジングQRコードを受け取った後（ステップ3）、次の2つの選択肢を持つことになります。1) QRコードを画面上に表示し、ユーザにキャプチャを要求する。この場合、ユーザは要求したQRコードと異なる取引を行うため、認証を終了する。2) ユーザが行った取引の内容を暗号化した偽造QRコードを作成し、表示する。しかし、画面に表示されたQRコードは検証者が生成したものと異なるため、撮影したイメージトークンは画像内容照合に合格しません。C. 指紋偽造攻撃敵対者は、挑戦的なQRコードとターゲットスマートフォンの指紋を含む画像を作成することで、正規のスマートフォンになりすますことができます。この場合、2つの偽造方法が考えられます。1）敵対的なデバイスによってキャプチャされた画像に被害者のカメラ指紋を直接注入する。2）注入プロセスの前に、キャプチャされた画像から敵対者のカメラ指紋を除去する。1）被害端末が撮影した2種類の画像から2つの参照指紋を抽出する。2）同じモデルの別のスマートフォンでチャレンジングなQRコードを撮影する。このようにして作成された画像は、チャレンジングQRコード、被害者のカメラの指紋K（c）、敵対者のカメラの指紋K（a）、およびその他のランダムなノイズ成分で構成されます。この攻撃を検出するため、本プロトコルではK（a）の存在を検出する偽造検出機構を採用しています。K(a)を共有する偽造画像は、正規の画像よりも有意に高い相関値を持つという観測に基づき、本プロトコルでは、ユーザに2つの挑戦的なQRコードを同じデバイスで撮影させ、撮影画像間の相関を用いてこの偽造攻撃を検出します。また、本メカニズムの有効性を証明するために、すべてのテスト画像が屋内環境で撮影された最悪のシナリオを検討する。第VI節で示すように、この環境で撮影された画像は最も弱いフィンガープリントを持つ。我々は、Amazon Mechanical Turkから収集した2つの画像セットと、我々のデバイスをテストした。iPhoneセット：30種類のiPhone6で撮影された6,000枚の画像。解像度は2448×3264。Samsungのセット：10種類のGalaxy Note 5で撮影された10,000枚の画像。両画像セットについて，比較のために2種類の画像ペアを構成する。1）通常画像ペア：同じカメラで撮影された2つの画像，すなわち，同じK（c）で撮影された画像。2) 偽造画像：同じK(c)とK(a)を持つ2つの偽造画像のペア．すべての偽造画像ペアは偽造戦略Iによって作成されています。iPhoneのセットでは、400枚の偽造画像ペアと450枚の通常画像ペアを作成しました。各テスト画像ペアについて、2つの類似性値を計算する。P CE1 = P CE(W1(c), ˆK(c)) は被検査画像のノイズ残量と対象スマートフォンの参照指紋との類似度である。P CE2 = P CE(W1(c), W2(c))は被検査画像のノイズ残量間の類似度である。P CE2は図9に示すようにどちらの画像ペアでもP CE1と正の相関があるため、P CE1とP CE2の差を用いて正常画像と偽造画像を区別することができる。ABCは閾値処理により、P CE2とP CE1の差分が閾値以上であれば偽造画像と判定し、閾値未満であれば偽造画像と判定することで、指紋偽造攻撃の検知を行います。図11は、検出結果の性能をROC曲線で示したものです。真陽性率、偽陽性率ともに閾値の減少に伴い増加する。偽造検出の総誤差率を最小にするために、iPhoneセットの偽造検出閾値として75.7を、Samsungセットの閾値として162.9を選択することにした。iPhone 6の場合，この閾値は偽陽性率0%，偽陰性率1.01%という結果になった．また、Galaxy Note 5では、偽陽性率は0.14%、偽陰性率は0.64%でした。いくつかの偽造画像ペアが偽造検出機構をうまく通過できる理由は、偽造プロセスで導入されたK(a)が弱すぎるためです。ランダムノイズの存在により、光の強さが一定でもK(a)の強さは露光ごとに大きく変化します。このため、認証時にK(a)が弱い画像を撮影してしまうと、偽造検出機構を通過できる偽造画像を作成することができます。しかし、図2に示すように、K(c)の強さによって検出結果が左右されます。PCE1 が大きくなると、PCE2 とPCE1 の差は急激に大きくなります。2) 偽造戦略II：この戦略では、敵は偽造画像から自分の指紋を除去することによって、偽造検出機構を打ち負かそうとします。偽造プロセスは次のように動作する。1) 犠牲者の2つの異なる画像セットから2つの参照指紋を導き出す。2) 課題となるQRコードを撮影し、その画像から敵の指紋を除去する。3）得られた画像に被害者の異なる指紋を埋め込む。この戦略は、偽造戦略Iを打ち負かすための我々のメカニズムを破る可能性があります。ABCは指紋除去を検出することによって、この攻撃を打ち負かすことができます。1) 適応型PRNUノイズ除去技術[31], [22]を用いて撮影した画像にフィルタをかける、2) 提示されたQRコードを含む画像を再構成する。どちらの除去方法もすべてのノイズ成分を除去するため、指紋除去を検出するためにプローブ信号を使用する。プローブ信号は、1) カメラ画面チャンネルの歪みに強く、正規の画像トークンに保存されることを保証する。2) 指紋除去に対して敏感であり、指紋除去プロセスによって信号が変化することを保証する。認証プロセスにおいて、検証者はこのプローブ信号ΓをQRコードに埋め込み、ユーザがこれをキャプチャします。この検出機構の信頼性は、プローブ信号の半脆弱性にある。ABCのプローブ信号は、カメラの指紋と同じタイプ、すなわち分散が3～5の白色ガウスノイズである。この設計では、プローブ信号は適応的なPRNUノイズ除去に対して固有の感度を持つ。敵のフィンガープリントを除去できるフィルタリング手法は、プローブ信号も除去することができる。2番目の除去法では、プローブ信号が未知であるため、敵は自分のカメラの指紋をキャプチャ画像に導入しなければプローブ信号を含む画像を作成することができません。この損失はプローブ信号にも影響しますが、指紋の除去による情報損失はより深刻です。チャネル歪みとフィンガープリント除去を比較するために、3つの異なる設定でプローブ信号をテストしました。1) QRコードにプローブ信号が含まれていない場合。3) 提示されたQRコードに800×800のプローブ信号が含まれ、撮影された画像に対して指紋除去を行う。次に、撮影した画像I(c)に対して領域検出とサブサンプリングを行い、チャレンジングQRコードを抽出し、I′(c)を得る。最後に、I(s) とI′(c) の間のPCE 値を計算する。各設定について、実験を20回繰り返し、PCE値のCDFを図12に示す。その結果、以下のことが確認できた。1) プローブ信号がキャプチャ画像に保存されている。2）プローブ信号を用いることで、指紋の除去を確実に検出することができる。すべての指紋除去方法に対して感度が高く、カメラ画面のチャンネル歪みにも強いため、ABCに適用したプローブ信号は効果的に指紋除去を検出することができる。性能評価このセクションでは、まずasmartphoneカメラのPRNUの特性を調査する。次に、提案するABCプロトコルの効率性を評価する。最後に，ユーザ調査を行い，システムの有用性を示す．評価には、2.6GHzで動作する8コアIntel i7-4720HQプロセッサを搭載したWindowsシステム上でMatlabを使用しています。指紋照合と抽出のアルゴリズムは、digital data embeddinglaboratory [28]によるコードに基づく。iPhone 6の画像は2448×3264、Samsung Galaxy Note5の画像は2048×1152の解像度で、Amazon Mechanical Turkと私たちのデバイスから収集しました。収集した画像のランダム性を確保するため、MechanicalTurkで公開した画像収集タスクは、画像の内容や人々の写真の撮り方について制限を設けていない。測定基準：スマートフォンカメラのフィンガープリントを評価するために、以下の測定基準を使用する。PCE（Peak to Correlation En-ergy）は、クエリ画像のノイズ残量と参照フィンガープリントの相関を測定します。これは、参照指紋の品質と、クエリ画像によって運ばれる指紋の強さを示すために使用することができます。CDFは、特定の値αが与えられたとき、Xがα以下の値をとる確率を示します。B. スマートフォンカメラのPRNUB 実験の詳細な設定を示す前に、まず、調査した質問と我々の重要な観察結果を以下のように要約する：1 PRNUは時間とともに変化するか？我々は3つの異なる年に撮影された画像をテストしました。2 周囲の環境は画像の指紋に影響を与えるか？はい、飛行、温度、相対湿度の影響をテストしています。指紋に影響を与える可能性がある唯一の要因は、環境光の強さです。3 画像の解像度とフィンガープリントの強度にはどのような関係があるのですか？正の相関があります。4 参照画像の数は、抽出された参照指紋の強さにどのような影響を与えるか？各スマートフォンについて、抽出された参照指紋の強さは、参照画像の数にほぼ比例します。スマートフォンの平均寿命は約22ヶ月であるため[3]、2015年、2016年、2017年の3年間に撮影された画像を用いて、スマートフォンのPRNUを評価しました。すべてのテスト画像は、一定の光量で同じ部屋で撮影されました。このテストに適用されたスマートフォンはiPhone 6です。PRNUが時間の経過とともに変化するかどうかを調べるために、まず、2017年に撮影された画像から参照指紋を抽出します。次に、異なる年に収集された3つの画像セットで指紋照合を行います。各画像セットには、テストデバイスによって撮影された200枚の画像が含まれています。図14は、得られたPCE値のCDFを示す。参照指紋は2017年にキャプチャされるため、2017年のCDFは同じ年のノイズ残量（指紋）間の相関を示し、2015年と2016年のCDFは異なる年のノイズ残量間の相関を示しています。この3つのCDFの間には有意な差がないため、テストしたスマートフォンのPRNUは過去3年間で変化していないことになります。2）環境光の影響指紋の抽出品質は、主に画像中のノイズ成分によって決まります。周囲の明るさは、撮影した画像のランダムなノイズ成分に影響を与えるため、周囲の明るさがカメラの指紋に与える影響を調査することは重要です。そこで、6つの環境下で撮影された画像を評価しました。1) 室内低照度：窓のない部屋で、薄暗い照明器具のある環境。2）屋内中央：窓のない部屋で、蛍光灯が数本ある環境。3) Indoor high：窓が数カ所ある室内環境。周囲の光源は太陽。4)屋外の朝。5）屋外の正午。6)屋外の夕方。実験では、各構成で300の画像ペアを作成し、それらの画像ペアで指紋照合を実施した。各画像ペアについて計算されたPCE値は、その画像に含まれる指紋の強さを示しています。図13は、得られたPCE値のCDFを示しています。観察結果は以下の通りである。1) 撮影された画像上の指紋の強度は、環境光の強度の上昇に伴い、著しく増加する。2) 屋内画像と比較して，屋外画像は通常，より強い指紋を持つ。3）周囲温度と相対湿度の影響：周囲環境が撮影画像上の指紋に与える影響を理解するために、周囲温度と相対湿度の影響についてさらに調査しました。環境温度については、17.78°F、45.5°F、85.1°Fでテストしています。相対湿度については、27％、45％、78％（雨の日）の画像をテストしています。前回の実験と同様に、各構成について200枚の画像ペアを作成し、指紋照合を実施しました。図13（c）、図13（d）に示すように、各構成のCDFに有意差はない。したがって、PRNUは周囲の温度や相対湿度に影響されないことがわかる。デジタルカメラで撮影された画像は，ダウンサンプリングやトリミングによりサイズ変更することができます．ダウンサンプリングでは、最近傍補間、バイリニア補間、バイキュービック補間の3つの最も一般的な補間方法をテストしました。画像の切り出しでは、ターゲット画像から矩形領域を切り出す。画像のサイズを変更した後、保存に使用する画像形式を決定する必要がある。ここでは、最も一般的に使用されている2つの画像形式をテストする。1）PNG：可逆圧縮に対応し、正確な画素値を得ることができるが、保存容量が大きくなる。2) JPG, 損失性圧縮をサポートする, 得られる画像はノイズが多いが小さい。スケーリング比は、元画像のサイズに対するリサイズ画像のサイズの比例比として定義される。我々は、40％〜80％の範囲で様々な画像のスケーリング比をテストした。全体として24種類の構成があり、それぞれがSamsung画像セットから生成された100組のマッチング画像と100組の非マッチング画像でテストされています。図15は、得られた類似度のCDFを示したものであり、以下のことがわかる。画像サイズ変更法：画像切り出しは、テストしたすべてのダウンサンプリング法よりもはるかに優れており、すべての構成で最も特徴的な類似値を有する。また、画像の切り出しは最も効率的な方法であることに注意。画像フォーマットPNGはJPGよりも指紋検出において優れている。一致する画像ペアの場合、PNG画像はJPG画像より高いPCE値を生成します。非マッチング画像ペアの場合、JPG画像は、非可逆圧縮プロセス中に導入されるノイズ成分により、PNG画像よりも高いPCE値を生成します。要約すると、最適なリサイズ戦略は、ターゲット解像度に画像を切り出し、得られた画像をPNGフォーマットで保存することです。一致画像と非一致画像の分布を比較すると、拡大率40%（画素量16%）の画像でもそこそこの精度が得られることがわかる。5）参照画像数の影響：拡大縮小率が低い画像に対して、指紋検出の精度を向上させる一つの方法として、ユーザがアップロードする参照画像の枚数を増やすことが挙げられます。この方法は、認証システムの登録オーバーヘッドを増加させるため、参照画像の数がリサイズ画像の類似値にどのように影響するかをさらに調査した。高い登録オーバーヘッドはユーザー体験を著しく低下させるため、1、2、4、6枚の参照画像のみをテストした。画像の拡大縮小率は、40%、60%、80%。24の構成それぞれについて、Samsungの画像セットから生成された100組のマッチング画像と100組の非マッチング画像でテストされた。図16は、得られた類似度値のCDFである。その結果、以下のことがわかった。1) JPGフォーマットでは、参照画像の数を増やすことで指紋検出の精度を向上させることができますが、JPG画像では、合理的な登録オーバーヘッドで公正な精度を達成することは困難です。画像コンテンツ照合：この手順のコストは、主に適用されるQRコードのバージョンによって決まります。[41]の実験結果によると、スマートフォンは非常に高いバージョン（20）のQRコードを0.1秒以内にコード化します。この手順の時間消費を図17（a）に示します。偽造検出：必要なノイズ残基は前の手順で得られているため、この手順ではPCE計算を1回行うだけです。図17(b)にこの処理の消費時間を示す。除去検出：この処理では、ノイズ抽出とPCE計算を2回行う。プロトタイプで使用したプローブ信号（800×800）の場合、プロトコルは指紋除去の検出に最大0.9秒を費やします。2人のワーカーは指紋照合と偽造検出を順次行い、残りの2人は表IIに示すプローブ信号で削除検出を行う。図17(c)に示すように、テストしたほとんどの共通解像度において、ABCは高い効率を達成することができた。高解像度画像における遅延は主に指紋抽出処理によるものである。なお、デジタルデータ埋め込み研究所[28]が公開したコードは、GPUコンピューティングと並列コンピューティングを利用していないため、さらなる最適化により、効率は大幅に改善されると思われます。また、セクションVI-B4およびVI-B5で示したように、スケーリングレートの低い画像は、適度なレジストレーションオーバーヘッドで高い精度を達成することができる。D. ユーザビリティ調査 ユーザのABCプロトコルに対する行動、ニーズ、態度を把握するため、Samsung Galaxy Note 5を被認証者、検証者の2台としてプロトタイプを用いたユーザ調査を実施した。プロトタイプでは，スマートフォンから検証機への無線通信にNFCチャネルを使用した．21歳から54歳までの40名（男性20名、女性20名）を対象に、本システムを検証しました。テストでは、まず1分間のシステム紹介を行った。テストでは、まず1分間のシステム紹介を行い、その後、参加者は何も指示されることなく、私たちのプロトタイプを使ってスマートフォン認証を行うことができました。スマートフォンで撮影することに慣れているため、すべての参加者が初回で簡単にタスクを完了することができました。図17(d)は、難易度の高いQRコードの撮影に要した時間のCDFを示したものである。95%の参加者が、撮影の段階は効率的で快適だと考えている。特に、女性参加者5名からは、パスワードを覚えるのが大変なので、パスワードを入力するよりも撮影した方が良いという意見があった。NFCの通信速度については、男性参加者の8割が「通信速度が遅い」と回答したのに対し、女性参加者の9割が「通信速度は許容範囲であり、撮影の仕方も効率的で快適である」と回答しました。特に、女性参加者5名からは、「パスワードを覚えるのが大変なので、パスワードを入力するよりも撮影した方が良い」という指摘がありました。NFC送信フェーズでは、男性参加者の80％がNFCチャネルの通信速度がやや遅いと評価した一方、女性参加者の90％が通信速度は許容範囲であり、データ転送の方法も面白いと考えています。関連研究ハードウェア・フィンガープリンティングは、近年活発に研究されています。製造上の不完全性により、物理的なセンサーはその出力に系統的な歪みを引き起こす。Deyら[21]は、加速度センサーの不完全性を利用しています。彼らは、振動モーターでセンサーを刺激し、指紋を作成するために機械学習を使用します。Bojinov et al.[5]は加速度センサーの校正誤差を分析し，多数のデバイスでその有効性を検証している．この方法では，ユーザが加速度センサーのキャリブレーションを行う必要があります．Dasら[19]は、より正確な指紋を生成するために、加速度センサとジャイロセンサの両方の特徴を組み合わせることをさらに研究しています。しかし、彼らの方法は、ユーザーがいくつかの角度で正確にスマートフォンを回転させる必要があります。さらに、モーションセンサーの指紋は操作可能であり、簡単に除去することができます[19]、[18]。音響指紋もスマートフォンを一意に識別するために使用することができます。Das ら [17], [16] は、オーディオクリップの再生と録音のプロセ スから聴覚的なフィンガープリントを抽出しています。Zhou et al.Zhou ら [42]は、特別に設計された音声入力に対するスピーカーの 周波数応答を調査している。しかし、これらの方法はマイクへのアクセスを必要とし、プライバシーの問題を引き起こします[18]。無線信号の生成過程におけるいくつかの個別ステップは、トランスミッタのハードウェアの不完全性 [15]に起因し、RFフィンガープリントのソースとなる可能性があります。ハードウェアフィンガープリントはスマートフォンのトラッキングに有効であることが証明されていますが、これらの方法がなりすまし攻撃に耐えられるかどうかは明らかではありません。センサーによって生成された信号は操作可能であるため、ほとんどの fingerprintingmethods は、広告主が故意にセンサーデータを改ざんする偽造攻撃に対して脆弱である [8], [14]VIII.結論と今後の課題 本論文では、画像センサーのPRNUをスマートフォン固有の指紋として利用し、物理層デバイス認証を実現するアイデアを探りました。その結果、スマートフォンのカメラは非常に強いPRNUを持つことが分かりました。この事実に基づいて、我々は、内蔵カメラのPRNUによってスマートフォンを識別する、攻撃に強く、リアルタイムで使いやすいスマートフォン認証プロトコルABCを設計しています。スマートフォンのPRNUを登録するために必要な画像は1枚だけです。我々はABCのプロトタイプを実装し、Amazon MechanicalTurkと我々のデバイスから収集した16,000枚の画像を用いてテストを行った。その結果、ABCは0.5%以下のエラーレートでユーザのデバイスを効率的に認証でき、0.47%以下のエラーレートで指紋偽造攻撃を検出できることが分かりました。今後、デュアルカメラ（レア）システムを採用するスマートフォンメーカーが増える中、余分なカメラを活用し、ABCの安全性を向上させる方法を検討する予定です。デュアルカメラ方式では、検証者は2つのカメラの指紋で各スマートフォンを識別することができ、指紋偽造の難易度をさらに高めることができます。また、デュアルカメラシステムのタイプ別の特徴についても検討していきます。また、アイフォン7プラスは広角カメラと望遠カメラを搭載し、より遠くからの高品質なズームを実現。ファーウェイP9はRGBとモノクロの2つのイメージセンサーを組み合わせ、撮影した画像のディテールを向上させています。関連する仕事ハードウェアの指紋は、近年活発に研究されています。製造上の不完全性により、物理センサーはその出力に系統的な歪みを発生させる。Deyら[21]は、加速度センサーの不完全性を利用しています。彼らは、振動モーターでセンサーを刺激し、指紋を作成するために機械学習を使用します。Bojinov et al.[5]は加速度センサーの校正誤差を分析し，多数のデバイスでその有効性を検証している．この方法では，ユーザが加速度センサーのキャリブレーションを行う必要があります．Dasら[19]は、より正確な指紋を生成するために、加速度センサとジャイロセンサの両方の特徴を組み合わせることをさらに研究しています。しかし、彼らの方法は、ユーザーがいくつかの角度で正確にスマートフォンを回転させる必要があります。さらに、モーションセンサーの指紋は操作可能であり、簡単に除去することができます[19]、[18]。音響指紋もスマートフォンを一意に識別するために使用することができます。Das ら [17], [16] は、オーディオクリップの再生と録音のプロセ スから聴覚的なフィンガープリントを抽出しています。Zhou et al.Zhou ら [42]は、特別に設計された音声入力に対するスピーカーの 周波数応答を調査している。しかし、これらの方法はマイクへのアクセスを必要とし、プライバシーの問題を引き起こします[18]。無線信号の生成過程におけるいくつかの個別ステップは、トランスミッタのハードウェアの不完全性 [15]に起因し、RFフィンガープリントのソースとなる可能性があります。ハードウェアフィンガープリントはスマートフォンのトラッキングに有効であることが証明されていますが、これらの方法がなりすまし攻撃に耐えられるかどうかは明らかではありません。センサーによって生成された信号は操作可能であるため、ほとんどの fingerprintingmethods は、広告主が故意にセンサーデータを改ざんする偽造攻撃に対して脆弱である [8], [14]VIII.結論と今後の課題 本論文では、画像センサーのPRNUをスマートフォン固有の指紋として利用し、物理層デバイス認証を実現するアイデアを探りました。その結果、スマートフォンのカメラは非常に強いPRNUを持つことが分かりました。この事実に基づいて、我々は、内蔵カメラのPRNUによってスマートフォンを識別する、攻撃に強く、リアルタイムで使いやすいスマートフォン認証プロトコルABCを設計しています。スマートフォンのPRNUを登録するために必要な画像は1枚だけです。我々はABCのプロトタイプを実装し、Amazon MechanicalTurkと我々のデバイスから収集した16,000枚の画像を用いてテストを行った。その結果、ABCは0.5%以下のエラーレートでユーザのデバイスを効率的に認証でき、0.47%以下のエラーレートで指紋偽造攻撃を検出できることが分かりました。今後、デュアルカメラ（レア）システムを採用するスマートフォンメーカーが増える中、余分なカメラを活用し、ABCの安全性を向上させる方法を検討する予定です。デュアルカメラ方式では、検証者は2つのカメラの指紋で各スマートフォンを識別することができ、指紋偽造の難易度をさらに高めることができます。また、デュアルカメラシステムのタイプ別の特徴についても検討していきます。アイフォン7プラスは広角カメラと望遠カメラを搭載し、より遠くからの高画質ズームを実現、ファーウェイP9はRGBとモノクロの2つのイメージセンサーを組み合わせ、撮影画像の精細感を高めている。