様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　４ 年　 ６ 月　 ３ 日現在

機関番号：１５４０１
研究種目：基盤研究(C)（一般）
研究期間：2019～2021
課題番号：１９Ｋ１１９６４

研究課題名（和文）プライバシーを保護した群集センシング実現のための匿名認証

研究課題名（英文）Anonymous Authentications for Privacy-Enhancing Crowd Sensing

研究代表者
中西　透（Nakanishi, Toru）

広島大学・先進理工系科学研究科（工）・教授

研究者番号：５０３０４３３２

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：多数のユーザのモバイル端末を利用した群衆センシングが盛んに研究されているが，ユーザがIDと共に位置情報を送信するため，プライバシー問題を引き起こす.そこでIDを必要としない匿名認証が提案されている.また，匿名のままユーザおよびデータの信頼度を測る手法も提案されている.しかし，従来方式ではその匿名性に問題がある.本研究では，匿名性を改良した方式を構築し，その安全性を検討する.さらに，各アルゴリズムをプロトタイプ実装するとともに，群衆センシングを想定した環境で実験し，有用性を示す.

研究成果の学術的意義や社会的意義
本研究により，従来の匿名認証方式におけるユーザ失効方法や匿名評判システムでは十分に達成されていなかったユーザのプライバシー（匿名性）と実用的な効率を達成している．さらに，方式提案だけではなく，理論的な定式化と証明による安全性保証に加えて，実際の群衆センシング環境における実用性評価も行っており，理論的な安全性と実用的な効率を両立した群衆センシングにおけるプライバシー保護を達成していると考える.

研究成果の概要（英文）：Crowd sensing using lots of users' mobile devices has been studied extensively because of its ease of implementation and use. However, it may cause a privacy problem, since users send their location information along with their IDs. Thus, anonymous authentication without user ID has been proposed. In addition, since the trustworthiness of anonymized users cannot be determined, a method to measure the trustworthiness of anonymous users and data has been proposed. However, conventional methods have problems in anonymity. In this research, we construct methods with improved anonymity, and examine the security. In addition, we implement prototypes of each algorithm and conduct experiments in an environment that assumes crowd sensing to demonstrate their usefulness.

研究分野：情報セキュリティ

キーワード：プライバシー　匿名認証　群衆センシング

様　式　C－１９、F－１９－１、Z－１９（共通）

１．研究開始当初の背景

近年，スマートフォンやウェアラブルデバイスなど，多種多様なセンサーを装備したユーザ所有のモバイル端末が普及している．さらに今後は，自動車も，各種センサー・カメラを装備するとともに常時ネットワーク接続され，スマート化が進むと考えられる．このような状況において，センサー装備のモバイル端末を利用した群衆センシングが盛んに研究されている．群衆センシングでは，モバイル端末を携帯した多数のユーザが参加する．各モバイル端末は，移動しながら付近の環境データ，騒音レベル，混雑状況などをセンシングし，位置情報とともに逐次サーバへ送信する．サーバでは，大量のユーザのセンシングデータを集約・解析することにより，都市レベルでの環境モニタリングや混雑予測などが可能となる．群衆センシングでは，ユーザが携帯するモバイル端末を利用するため，導入・利用が容易である．

群衆センシングでは，外部の攻撃者による不正なセンシングデータ送信を防止するために，送信時にユーザ認証が必要となる．一方で，位置情報を送信するため，プライバシー問題を引き起こす．すなわち，サーバ側では，ユーザ ID を紐付けることにより，そのユーザがどの時間においてどこを移動しているかといった個人情報の収集を許してしまう．こうして，群衆センシングの実用化には，プライバシーを保護したユーザ認証が必要不可欠である．その解決策として，匿名でのユーザ認証を可能とする匿名認証が盛んに研究されている．匿名認証では，ユーザ ID を明かすことなく正当なユーザかどうかのみ認証するために，ユーザ ID の紐付けができず，上記のプライバシー問題を解決できる．

２．研究の目的

本研究では，プライバシーを保護した群衆センシング実現のための匿名認証における以下の二つを研究目的とする．

(1) ユーザがサービスから脱退する場合や秘密鍵を漏洩した場合に，その秘密鍵に基づくユーザ権限を失効させるユーザ失効処理が必要となる．群衆センシングに適した失効可能方式が提案されており，失効確認処理において失効数 R に依存した暗号計算を必要せず，失効リスト中の失効トークンとの単純なデータ照合処理を繰り返すのみでよく，効率的な失効を実現している．しかし，従来方式は，匿名性が弱いという安全性の問題がある．そこで本研究では，従来方式同様に，失効数 R に依存した暗号計算を行なわずデータ照合のみで高速に失効確認できるとともに，さらにプライバシーを強化した匿名認証方式を提案する．

(2) 群衆センシングでは，各ユーザがデータをセンシングしてサーバへ送信するため，ユーザ端末において不正にセンシングデータが改ざんされる恐れがある．また，センサー自体の不良により正しくないデータが送信される可能性もある．その一方で，プライバシー保護のために認証を匿名化してしまうと，各送信ユーザの信頼性も追跡できなくなってしまう．この信頼性とプライバシーの問題を解決する手法として，匿名評判(reputation)システムが研究されており．群衆センシングでの方式が提案されている．この方式では，サーバが，各ユーザのこれまでの送信データの評価点から算出される評判を値として自身のデータベースで各ユーザとともに管理している．各ユーザがセンシングデータを送信すると，そのユーザの評判に加えて，今回の送信データの時刻・場所や他ユーザのデータとの相関に基づいて信頼度を評価点として算出する．センシングデータの解析時には，この評価点を加味して解析することにより解析結果の正確さが向上すると考えられる．しかし従来方式では，サーバ側で評判を管理するために，匿名性を弱める攻撃を行なうことができる．そこで本研究では，サーバ側で管理する代りに，証明書付きでユーザ側で管理することにより，より強固な匿名性をもつ匿名評判システムを提案する．

３．研究の方法

(1) 匿名認証でのユーザ失効における従来方式では，署名生成時に，期間中の何番目の署名かを表わすkを公開する必要がある．また，同一の署名者は，期間中に同じkを一度しか使用できない．このとき．kの漏洩は匿名性を弱めており，例えば，以下の攻撃が考えられる．ある期間kにおいて，センシングデータの送信での位置情報と他の情報などを利用して，あるデータ送信S_jのユーザの ID が数人，簡単化のため二人のユーザ(ユーザ ID をP_1およびP_2とする)のいずれかに特定できたと仮定する．さらに，位置情報を関連づけるなどして，P_2のデータ送信履歴の一部が追跡でき，既にkの認証を行なっているとする．すると，各ユーザは同一のkでの認証を一度しかできないため，サーバは，S_jがP_1によるものと特定できてしまう．もし認証でkが漏洩しないなら，このような特定はできない．

そこで本研究では，kを秘匿して失効確認できる方式を提案する．そのために，検証可能な疑似ランダム関数hを用いる．この出力は疑似ランダムである一方で，関数のため同じ入力に対しては同じ出力を取る．失効確認タグとして$h(x+T+k)$を署名に付加する(xはユーザ秘密鍵，Tは現在の期間であり，秘匿されるx,kの正当性は証明書で保証)．そして，期間Tでこのユーザを失効するとき，サーバが，すべてのkに対して，$h(x+T+k)$を計算して失効トークンとして公開

する．これにより，署名に付加されたタグと失効トークンが同じかチェックすることにより，失効されているかを高速なデータ照合のみでチェックできる．

(2) 匿名評判システムの従来方式では，ユーザの評判の概算値$\widetilde{R}_i$を保証する匿名証明書をサーバがユーザに発行しておく．データS_jを送信時には，乱数によりブラインド化した証明書を送信する．データS_jのフィードバック値f_jを算出後，アンブラインドした証明書とf_jをユーザが再送して，データベースでのそのユーザの評判R_jを更新する．このように証明書ベースのブラインド化により，ユーザ ID と送信データが直接リンクされることを防いでいる．しかし，データS_jとそのフィードバック値f_jはリンクできる．評判の更新時には ID とf_jが送付されるため，f_jを経由して ID とデータがリンクできることになる．

本研究では，ユーザ側で評判R_jを管理することを考える．ユーザはサーバから現在のR_jを暗号化した$E(R_j)$に対する証明書(ディジタル署名)が発行される．データ送信時には，証明書をそのまま送付するのではなく，$E(R_j)$を再暗号化して送信するとともに，評判の概算値$\widetilde{R}_i$と証明書を保持していることをゼロ知識証明する．これにより，余分な情報をもらすことなく，R_jがユーザ側で改ざんされていないことを保証できる．また，フィードバック値f_jを算出後，暗号化関数Eの準同型性を利用して，暗号化したまま加算を行なうことにより$E(R_j + f_j)$を生成し，その証明書(更新後の評判$R_j + f_j$に対する証明書)をユーザに発行する．この手法では，評判の更新においてユーザ ID が必要ないため，強固なプライバシーが実現できる

４．研究成果

(1) 群衆センシング向け匿名認証のユーザ失効については，3.(1)に示した着想に基づいて，方式の構築を行った．ペアリングベースの匿名認証方式をベースとして，秘密鍵xおよび期間T，期間T中の署名回数kに対して擬似ランダム関数の出力$h(x + T + k)$を失効トークンとすることにより，kを秘匿した強い匿名性を維持しつつ効率的なマッチングによる失効確認を構築した．本方式の安全性を示すために，不正認証に対する安全性および（強い意味での）匿名性を定義し，標準的な数学的仮定の下で，定式的に安全性証明を行った．また，従来方式に対して，処理時間（署名生成，署名検証，失効確認，失効リスト作成処理）およびデータサイズ（公開鍵・秘密鍵サイズ，署名長，失効リストサイズ）について比較を行った．その結果，マッチングを行わない従来方式に対しては失効確認における暗号処理が失効数 R に依存しないことを確認した．一方，マッチングベースの従来方式に対しては，同等の失効確認処理時間および失効リストサイズであることも確認した．しかし，失効確認処理時間および失効リストサイズはともに，期間中の署名回数Kに対して$O(KR)$となり，その実用性が問題となる．そこで，群衆センシングのユースケースにおいて実用性の確認を行った．1 日毎の失効リスト更新で 1 分ごとのデータ送信を想定したK = 720とした場合，R = 100,000でも通常の PC において並列計算なしで 200 秒程度での失効リスト生成処理を行うことができ，失効リストサイズも 4GB 程度となるため，現在の環境においても十分実用的であることが分かった．これらの成果は，国内シンポジウムおよび研究会で発表するとともに，国際会議 CANDAR2021 で採択され，Best paper award に選ばれた．また，PC において実装を行い，十分実用的な時間で処理できることも確認した．さらなる拡張として，ブルームフィルターを用いることにより，偽陽性を許しつつ失効リストのサイズを軽減した方式も提案している．

(2) 群衆センシング向け匿名評判システムについても，3.(2)に示した着想に基づいて，方式の構築を行った．ペアリングベースでの評判値に対する更新可能な証明書を用いた P2P 向けの匿名評判システムをベースとして，群衆センシングのサーバー・クライアントモデルで必要な機能に単純化した方式を構築した．本方式の安全性を構築するために，評判値の偽造に対する安全性および匿名性を定式化し，その安全性の概要を示した．本内容は国際会議 CANDAR のワークショップで発表している．さらに安全性証明および処理時間および通信コストを評価した上で論文誌に投稿中である．一方，実際の群衆センシング環境での実用性を示すために，クライアントとして Raspberry pi を想定した環境において，評価実験を行っている．その際，通信時間を軽減するため，センサーデータ送信開始以前に処理できる部分（ゼロ知識証明でのランダム化など）はできる限りオフライン処理することにより，オンライン処理の高速化を図った．また，(1)の匿名認証でのユーザ失効処理を組み込んだシステムへの拡張も行った．その結果として，十分実用的な処理時間(0.01 秒以内)で動作することが確認できた．

(3) 匿名認証の実用化においては，ユーザの属性情報を匿名で確認できる匿名属性認証や第三者機関を利用せずに不正者の排除が可能な方式も必要となる．本研究では，属性の論理式を AND,OR に加えて NOT も含む形で証明可能な方式を実現し，国際会議 IWSEC2019 で発表し，その拡張した論文は電子情報通信学会英文論文誌でも採択されている．第三者機関なしに不正者を排除可能な方式については，サーバの各ユーザの振る舞いに対しての評価値を匿名のまま積算し，その論理式に基づいて特定の条件の不正者を排除可能な匿名認証方式を提案している．この方式では，アキュームレータと呼ばれる圧縮技術を利用することにより，評価対象のカテゴリ数に依存しない認証時間を実現している．

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　1件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 OKISHIMA Ryo、NAKANISHI Toru	４．巻 E103.A
２．論文標題 An Anonymous Credential System with Constant-Size Attribute Proofs for CNF Formulas with Negations	５．発行年 2020年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 1381～1392
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2020TAP0003	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計10件（うち招待講演　0件／うち国際学会　3件）

１．発表者名 Yuto Nakazawa, Toru Nakanishi
２．発表標題 A Strongly Unlinkable Group Signature Scheme with Matching-Based Verifier-Local Revocation for Privacy-Enhancing Crowdsensing
３．学会等名 CANDAR2021（国際学会）
４．発表年 2021年

１．発表者名 木村魁，中西透
２．発表標題 失効可能グループ署名におけるブルームフィルタを用いた失効リストの削減
３．学会等名 コンピュータセキュリティシンポジウム2021(CSS2021)
４．発表年 2021年

１．発表者名 小林春輝，中西透，北須賀輝明
２．発表標題 クラウドセンシング向けの失効可能な匿名評価システム
３．学会等名 電子情報通信学会ISEC研究会
４．発表年 2021年

１．発表者名
中澤勇人，中西透

２．発表標題
クラウドセンシング向け失効可能グループ署名の高速化

３．学会等名
電子情報通信学会ISEC研究会

４．発表年
2020年

１．発表者名
小林春輝，中西透

２．発表標題
クラウドセンシング向けの効率的な匿名評価システムの実装

３．学会等名
2020年度(第71回)電気・情報関連学会中国支部連合大会

４．発表年
2020年

１．発表者名
中澤勇人，中西透

２．発表標題
クラウドセンシング向け失効可能グループ署名における匿名性の強化

３．学会等名
電子情報通信学会ISEC研究会

４．発表年
2019年

１．発表者名
Ryo Okishima, Toru Nakanishi

２．発表標題
An Anonymous Credential System with Constant-Size Attribute Proofs for CNF Formulas with Negations

３．学会等名
IWSEC2019（国際学会）

４．発表年
2019年

１．発表者名
新居稜介，中西透

２．発表標題
アキュームレータを用いたポリシーベースのブラックリスト型匿名認証システム

３．学会等名
CSS2019

４．発表年
2019年

１．発表者名
並木聖，中西透

２．発表標題
失効可能グループ署名を用いたクラウドセンシングにおける認証処理の実装

３．学会等名
電子情報通信学会ISEC研究会

４．発表年
2019年

１．発表者名
Shahidatul Sadiah, Toru Nakanishi

２．発表標題
An Efficient Anonymous Reputation System for Crowd Sensing

３．学会等名
WICS2019（国際学会）

４．発表年
2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関