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　６ 年　 ５ 月 １０ 日現在

機関番号：１２６０５
研究種目：基盤研究(B)（一般）
研究期間：2020～2023
課題番号：２０Ｈ０２１４４

研究課題名（和文）生体認証技術を見据えたセキュアな分散検定理論の構築

研究課題名（英文）Secure Distributed Hypothesis Testing for Biometrics

研究代表者
渡辺　峻（Watanabe, Shun）

東京農工大学・工学（系）研究科（研究院）・准教授

研究者番号：７０５４６９１０

交付決定額（研究期間全体）：（直接経費）　　12,700,000円

研究成果の概要（和文）：本研究では、セキュアな分散検定理論の構築を目指し様々な研究を行った。主な成果を要約すると、（１）分散仮説検定において、これまでに知られていた検定方法が準最適であることを世界で初めて明らかにした；（２）同定符号化符号において、従来未解決であった強逆性の仮定なして容量を求めることに成功した；（３）可逆なマルコフ連鎖が指数型族をなすこと、ならびにそこに付随する様々な性質を明らかにした；（４）暗号システムの安全性を議論される際に使われるビットセキュリティの操作的な定義を情報理論的な道具により提案した；（５）情報理論的暗号を体系的にまとめた著書を執筆した。

研究成果の学術的意義や社会的意義
IoT技術の発展に伴い，システムへの不正アクセスを防ぐための認証技術はますます重要になってきている．そのようなシステムの安全性を保証するためにも、なぜ安全性が保証されるのか、どうすれば効率を高めることができるのか、といったことの原理をしっかりと理解しなければならない。本研究で得られた成果はIoT技術の理論基盤を築く際の指針となり得るものであると考える。

研究成果の概要（英文）：We have conducted various research related to the theory of security and distributed hypothesis testing. We can summarize the research outcomes as follows: (1) In the problem of distributed hypothesis testing, we have proved that the previously known best testing scheme is suboptimal; (2) In the problem of identification over noisy channel, we have proved the capacity without the assumption of strong converse property, which has been an open problem for a while; (3) We have proved that the family of reversible Markov kernel constitute an exponential family, and also demonstrated certain properties induced from that fact; (4) In the analysis of crypto systems, we often evaluate the security level of certain systems using the concept of bit-security. By using tools from information theory, we have introduced a novel definition of bit-security that has an operational meaning; (5) We have written a textbook that systematically summarizes the information-theoretic cryptography.

研究分野：情報理論、暗号理論

キーワード：情報理論　暗号理論　計算量理論

様　式　Ｃ－１９、Ｆ－１９－１（共通）

１．研究開始当初の背景

IoT技術の発展に伴い，システムへの不正アクセスを防ぐための認証技術はますます重要になってきている．特にデバイスの数が増加するにつれ認証のためのパスワードを管理することが煩雑になるため，指紋認証や虹彩認証などの生体認証の利用は増加していくと考えられる．生体認証における認証精度は通常，正規のユーザを誤って拒否してしまう本人拒否率と，不正ユーザを誤って受け入れてしまう他人受入率のトレードオフによって評価される．また，認証精度に加えて重要になってくるのが，生体情報の漏洩を防ぐことである．生体認証をリモートで行う際に，生体情報をそのまま回線で送信してしまうと，通信途中で生体情報が盗聴されてしまう危険性がある．また，アクセスしようとしているシステム自体が偽装されたものであった場合にも，生体情報が漏洩してしまう危険性がある．従って，生体情報の漏洩を抑えた認証方式の提案が望まれる．

２．研究の目的

IoT技術の発展に伴い，システムへの不正アクセスを防ぐための認証技術はますます重要になってきており，指紋認証や虹彩認証などの生体認証の利用は増加していくと考えられる．しかしながら，生体認証をリモートで行う際に，生体情報をそのまま回線で送信してしまうと，通信途中で生体情報が盗聴されてしまう危険性がある．生体情報は一度漏洩してしまうとパスワードのように変更ができないため，極めて深刻な問題となる．従って，情報の漏洩を抑えた認証方式の提案が望まれる．本研究では，生体認証をネットワーク情報理論における分散検定として捉え，不正検出のための分散検定理論を構築する．

３．研究の方法

（１）本研究ではまず，分散仮説検定の数理構造を明らかにするために，従来知られていた分散検定法の中で最も優れているとされていた Shimokawa-Han-Amari 検定法の調査を行った．
（２）本研究ではさらに，雑音のある環境下における認証の数理構造を明らかにするために，同定符号の研究を行った．同定符号は 1989 年に Ahlswede-Dueck により導入され，強逆性の条件下での容量が Han-Verdu によって明らかにされていた．しかしながら強逆性の条件なしでは，同定容量が長い間未解決であった．
（３）統計学等において，分布のパラメータ族が指数型族をなす場合，下界を達成する推定法がある等，様々なご利益が得られることが多い．相関のあるデータの最も基本モデルであるマルコフ過程においても，指数型族を考えることはできる．一方，マルコフ過程の解析において，時系列データを逆むきに観測した際の確率法則が元の確率法則と同じであることを主張する可逆性は，様々な解析上の利点があることが知られている．そこで，本研究では可逆マルコフ過程の情報幾何学的な構造の解析を行った．
（４）様々な暗号技術において，攻撃に対してどのくらい耐性があるのかを測る尺度として，ビットセキュリティの概念がある．ビットセキュリティは実用的には頻繁に使われているものの，理論的な裏付けがなされていない状況であった．2018 年に Miciancio-Walter はビットセキュリティの定義を与えたものの，彼らの定義は天下り的であるという欠点があった．
（５）現代暗号は攻撃者の計算資源に仮定をおかずに安全性を議論する情報理論的暗号と，現実的な時間内には破られないということを要求する計算量理論的暗号に大別される．情報理論的暗号はシャノンの論文に端を発し，様々な研究が行われてきたが，特に 1990 年代頃から量子暗号との関わりなどもあり，大きく発展していた．

４．研究成果

（１）本研究の成果として，Shimokawa-Han-Amari 検定法は準最適であり，この検定を修正することでより検定力と通信レートのトレードオフが優れた検定法を提案することに成功した．Shimokawa-Han-Amari 検定法は長い間最も優れた検定法と考えられていたため，本成果のインパクトは大きい．本成果は 2022 年の IEEE 情報理論の国際会議 International Symposium on Information Theory にて発表を行った．
（２）本研究の成果として，近年発展した仮説検定を用いた逆定理の証明法により，強逆性の条件なしで同定容量を導出することに成功した．本成果は IEEE 情報理論部門のトップジャーナルである Transactions on Information Theory に掲載されている．
（３）本研究の成果として，可逆マルコフ過程は指数型族をなすことが明らかになった．可逆マルコフ過程が混合型族

をなすことは可逆性の条件式から容易に導くことができるが，指数型族をなすことは非自明であり，インパクトのある成果となった．また，可逆マルコフ過程が指数型族であることにより，射影の簡潔な式など，付随する成果も得られた．本成果は情報幾何学の論文し Information Geometry に掲載されている．

（４）本研究の成果として，情報理論のツールを利用することで，操作的な意味付けが明確なビットセキュリティの定義を与えることに成功した．さらに続く研究において，我々が導入した定義と，Miciancio-Walter の定義は見かけ上は異なっているものの，本質的には等価であることを証明した．これらの成果は暗号理論のトップ国際会議である ASIACRYPT 2021 と ASIACRYPT 2023 にて発表した．

（５）本研究の成果として，情報理論的暗号のこれまでの発展を体系的にまとめた教科書を執筆した．これまでは，研究成果は原著論文において記号や流儀もバラバラに説明されていたため，新規参入者の障壁となっていた．本研究ではそれらの成果を統一的な視点でまとめたため，この分野のさらなる発展に役立つものと考える．本成果は Cambridge University Press から 500 ページほどの教科書として出版した．

５．主な発表論文等

〔雑誌論文〕　計6件（うち査読付論文　6件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 Watanabe Shun	４．巻 68
２．論文標題 Minimax Converse for Identification via Channels	５．発行年 2022年
３．雑誌名 IEEE Transactions on Information Theory	６．最初と最後の頁 25～34
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIT.2021.3120033	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Watanabe Shun	４．巻 66
２．論文標題 A Classification of Functions in Multiterminal Distributed Computing	５．発行年 2020年
３．雑誌名 IEEE Transactions on Information Theory	６．最初と最後の頁 6169～6183
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIT.2020.3002756	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 －

１．著者名 Watanabe Shun、Yasunaga Kenji	４．巻 13092
２．論文標題 Bit Security as?Computational Cost for?Winning Games with?High Probability	５．発行年 2021年
３．雑誌名 ASIACRYPT 2021 (Lecture Notes in Computer Science)	６．最初と最後の頁 161～188
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-92078-4_6	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 －

１．著者名 Wolfer Geoffrey、Watanabe Shun	４．巻 11
２．論文標題 Information geometry of Markov Kernels: a survey	５．発行年 2023年
３．雑誌名 Frontiers in Physics	６．最初と最後の頁 1195562
掲載論文のDOI（デジタルオブジェクト識別子） 10.3389/fphy.2023.1195562	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 －

1．著者名 Wolfer Geoffrey、Watanabe Shun	4．巻 4
2．論文標題 Information Geometry of Reversible Markov Chains	5．発行年 2021年
3．雑誌名 Information Geometry	6．最初と最後の頁 393～433
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s41884-021-00061-7	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 －

1．著者名 Watanabe Shun、Yasunaga Kenji	4．巻 14443
2．論文標題 Unified View for?Notions of?Bit Security	5．発行年 2023年
3．雑誌名 ASIACRYPT 2023 (Lecture Notes in Computer Science)	6．最初と最後の頁 361～389
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-981-99-8736-8_12	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4件（うち招待講演　0件／うち国際学会　3件）

1．発表者名 Shun Watanabe
2．発表標題 On Sub-optimality of Random Binning for Distributed Hypothesis Testing
3．学会等名 2022 IEEE International Symposium on Information Theory（国際学会）
4．発表年 2022年

1．発表者名 Takuto Kakishima and Shun Watanabe
2．発表標題 A Numerical Study of Multi-letter Ahlswede-Han Scheme for Modulo-Sum Problem
3．学会等名 International Symposium on Information Theory and It Applications（国際学会）
4．発表年 2022年

１．発表者名 Shun Watanabe
２．発表標題 Minimax Converse for Identification via Channels
３．学会等名 電子情報通信学会　情報理論研究会
４．発表年 2020年

１．発表者名 Daisuke Takeuchi and Shun Watanabe
２．発表標題 Tight Exponential Strong Converse for Source Coding with Encoded Side Information
３．学会等名 2023 IEEE International Symposium on Information Theory（国際学会）
４．発表年 2023年

〔図書〕　計1件

１．著者名 Himanshu Tyagi and Shun Watanabe	４．発行年 2023年
２．出版社 Cambridge University Press	５．総ページ数 517
３．書名 Information-theoretic Cryptography	

〔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

インド	Indian Institute of Science, Bangalore			