様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２８ 年　 ９ 月 １４ 日現在

機関番号：３２６８９
研究種目：基盤研究(C)（一般）
研究期間：2013～2015
課題番号：２５４２０３９０

研究課題名（和文）確率的要素を含む情報セキュリティシステムの利便性と安全性からの最適化と統合評価

研究課題名（英文）A Unified Analysis and Optimization of Information Security System with Probabilistic Components from Viewpoints of Convenience and Safety

研究代表者

松嶋　敏泰（MATSUSHIMA, Toshiyasu）

早稲田大学・理工学術院・教授

研究者番号：３０２１９４３０

交付決定額（研究期間全体）：（直接経費）　　3,900,000円

研究成果の概要（和文）：確率的要素を含む情報セキュリティ問題に対し確率モデルにより定式化を行い，安全性や利便性等の評価基準を明確にし，最適な攻撃法や認証法等を理論的に明らかにした．個々の符号やシステムに対して安全性を評価するのではなく，統一的数理モデルの枠組のもとで安全性の理論的な限界を不変的に評価した．さらに，安全性と利便性のトレードオフ関係についても，理論的限界や最適性を明らかにし，情報セキュリティシステムの新たな評価指標を示した．また，学習理論や最適化理論等の周辺研究分野における等価な確率モデルを用いた問題の成果を応用することで，最適法を近似する高性能アルゴリズムを構成し，安全性や利便性を具体的に評価した．

研究成果の概要（英文）：Information security problem with probabilistic components has been formulated by probabilistic models. Theoretical criteria for evaluation such as convenience and safety have been defined clearly and optimal attack or an authentication method has been derived theoretically. Theoretical safety bounds have been evaluated with respect to mathematical models with unified framework for each cipher or security system. A theoretical safety bound or optimality has been clarified with respect to a tradeoff between convenience and safety. New theoretical criteria have been derived for information security systems. Approximation algorithms with high performance for optimal attack or an authentication method have been constructed applying results of studies on problems in related fields such as learning or optimization theory that is formulated by probabilistic models equivalent to our study. Convenience or safety of information security systems has been simulated by applying these algorithms.

研究分野：情報理論，統計学，学習理論とその応用

キーワード：情報セキュリティ　暗号・認証等　確率モデル　理論的安全性評価

１．研究開始当初の背景

情報セキュリティの研究において，確率モデルを用いた考察が不可欠となる問題が増加していた．例えば，Physically Unclonable Function(PUF)等の物理的特徴を利用した認証システムや，フィンガープリンティング符号におけるランダム性を利用した攻撃などである．しかし，従来研究には以下のような解決すべき点が存在した．

(1) 新たな情報セキュリティシステムを提案し，それに対する個別の攻撃法の提案とそれに基づく安全性評価を行うという研究が，従来盛んに行われていた．しかしこのようなアプローチでは，より強力な攻撃法が新たに提案される可能性が残り，安全性の保証が非常に不安定であった．特に，確率変動をシステムや攻撃法に含む PUF やフィンガープリンティング符号等においては，実験による安全性の評価のみしか行われていないものも多かった．

(2) 一般に，利便性と安全性はトレードオフの関係にある．例えば，認証システムにおいて，本人の認証確率を高めることと，攻撃成功確率を低くすることはトレードオフの関係になっている．従来，利便性と安全性のトレードオフを定性的に論じた研究は見受けられたが，理論的に明確に論じた研究はほとんど見られなかった．

２．研究の目的

上記研究背景で述べた問題点を踏まえ，本研究では以下の２点を研究目的とした．

(1) 符号やシステムに対して個々の攻撃法を提案することで安全性を評価するのではなく，統一的数理モデルの枠組のもと，攻撃成功確率や認証確率等の明確な評価基準から，最強力な攻撃法や安全性を不変的に評価する．

(2) 情報セキュリティシステムの利便性と安全性のトレードオフ関係を上記の最適な方法やその限界から理論的に考察し，新たな評価指標を示す．また，学習理論や最適化理論等の周辺研究分野における等価な確率モデルを用いた問題の成果を応用することで，最適法を近似する高性能アルゴリズムを構成し，安全性や利便性を具体的に評価する．

３．研究の方法

(1) 確率モデルの視点からの情報セキュリティ問題の整理

情報セキュリティ問題に含まれる確率的変動要素を適切に数理モデルに取り込み，問題の本質を捉えた確率モデルを構築した．具体的には，PUF やフィンガープリンティング符号を主な対象に数理モデルの構築を行った．さらに，構築された確率モデルと情報理論，統計科学，学習理論等の周辺分野において用いられる確率モデルとを比較することによって，情報セキュリティ問題の性質や本質的な難しさがどこにあるのかを明らかにした．

(2) 統一された数理モデル上での評価基準の明確化

(1)で得られた統一的な数理モデルに類似する周辺分野の数理モデルから得られた知見を応用することで，これまで定性的にしか論じられることのなかった安全性と利便性のトレードオフ関係を理論的に明確に記述し，ある安全性を保証したもとで原理的に実現可能な利便性の限界やそれを達成する手法を明らかにした．

４．研究成果

確率的変動を含む情報セキュリティ問題を確率モデルとして定式化し，明確な評価基準のもと，その理論的限界について考察した．

PUF を利用した認証デバイスでは，デバイスの物理的特徴を条件付き確率のパラメータとおくことで，パラメトライズされた分布による確率モデルとして表現した．このモデルは，周辺分野において頻繁に用いられるモデルと類似していることがわかったため，周辺分野において得られていた知見を応用することで，安全性と利便性のトレードオフ関係を明らかにし，ある安全性を保証したもとでの利便性の限界を評価し，それを達成する手法を提案した．

フィンガープリンティング符号の攻撃においては，複数のユーザの符号語から改ざんされた符号語が生成される過程を，多変数が入力されたもとで一変数が出力される条件付き確率モデルとして定式化した．このモデルは情報理論における多端子通信路のモデルに類似しているため，それらの成果を利用した解析を行った．

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　6　件）

① Shota Saito, Nozomi Miya, Toshiyasu Matsushima, Evaluation of the Bayes Code from Viewpoints of the Distribution of Its Codeword Lengths, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol.E98-A, no.12, 2015, pp.2407-2414, DOI:10.1587/transfun.E98.A.2407

② 吉田　隆弘，地主　創，相異なるハフマン符号が構成される２値無記憶拡大情報源の分類に関する一検討，電子情報通信学会論文誌，vol.J98-A，no.3，2015，pp.284-295，http://search.ieice.org/bin/summary.php?id=j98-a_3_284

③ 須子　統太，堀井　俊佑，小林　学，後藤　正幸，松嶋　敏泰，平澤　茂一，プライバシー保護機能を持つ線形回帰モデルにおける最小二乗推定量の分散計算法について,日本経営工学会論文誌, vol.65, no.2, 2014, pp.78-88, DOI:10.11221/jima.65.78

④ Nozomi MIYA, Tota SUKO, Goki YASUDA, Toshiyasu MATSUSHIMA, Asymptotics of Bayesian Inference for a Class of Probabilistic Models under Misspecification, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences,vol.E97-A, no.12, 2014, pp.2352-2360, DOI:10.1587/transfun.E97.A.2352

⑤ 前田　康成，後藤　文太朗，升井　洋志，桝井　文人，鈴木　正清，松嶋　敏泰，マルコフ決定過程で表現されたロールプレイングゲームにおける攻略法の能動学習，バイオメディカル・ファジィ・システム学会誌，査読有，vol.15, no.1, 2013, pp.69-81, http://ci.nii.ac.jp/naid/110009634833

⑥ 前田　康成，後藤　文太朗，升井　洋志，桝井　文人，鈴木　正清，松嶋　敏泰，ノンプレイヤキャラクタを伴うロールプレイングゲームの攻略法に関する一考察，電子情報通信学会論文誌，査読有，vol.J96-A, no.8, 2013, pp.572-581, http://ci.nii.ac.jp/naid/110009635646

〔学会発表〕（計　36　件）

① 増井　秀之，宮　希望，松嶋　敏泰，プライバシー保護機能を持つ分散型正則化ロジスティック回帰に関する一考察，電子情報通信学会パターン認識・メディア理解研究会(PRMU)，2016年1月21日～22日，大阪府吹田市

② 潮田　幹生，齋藤　翔太，松嶋　敏泰，潜在変数を仮定した多次元線形回帰モデルにおけるベイズ基準のもと最適なデータ予測に関する一考察，電子情報通信学会パターン認識・メディア理解研究会(PRMU)，2016年1月21日～22日，大阪府吹田市

③ 中野　雄斗，齋藤　翔太，松嶋　敏泰，半教師付き学習におけるベイズ基準のもと最適な予測の計算量削減方法に関する一考察，電子情報通信学会パターン認識・メディア理解研究会(PRMU)，2016年1月21日～22日，大阪府吹田市

④ 風間　皐希，鎌塚　明，松嶋　敏泰，Array-Errorモデルにおける軟判定復号に関する一考察，電子情報通信学会情報理論研究会(IT)，2016年1月18日～19日，大阪府大阪市

⑤ 中原　悠太，齋藤　翔太，松嶋　敏泰，メッセージ伝搬にもとづく疎な2部グラフ上のショートサイクル数え上げ法に関する研究，電子情報通信学会情報理論研究会(IT)，2016年1月18日～19日，大阪府大阪市

⑥ 斉藤　友彦，風間　皐希，新家　稔央，松嶋　敏泰，ランダムネットワーク符号化における不均一誤り訂正について，電子情報通信学会情報理論研究会(IT)，2016年1月18日～19日，大阪府大阪市

⑦ 堀井　俊佑，松嶋　敏泰，平澤　茂一，シンボルペア通信路における線形符号の線形計画復号法に関する一考察，第38回情報理論とその応用シンポジウム(SITA2015)，2015年11月24日～27日，岡山県倉敷市

⑧ 東　優太，鎌塚　明，吉田　隆弘，松嶋　敏泰，復元および再生成の条件を一般化した再生成符号に関する一考察，第38回情報理論とその応用シンポジウム(SITA2015)，2015年11月24日～27日，岡山県倉敷市

⑨ 鎌塚　明，松嶋　敏泰，Polar 符号の探索アルゴリズムを用いた復号法に関する一考察，第38回情報理論とその応用シンポジウム(SITA2015)，2015年11月24日～27日，岡山県倉敷市

⑩ 堀井　俊佑，松嶋　敏泰，平澤　茂一，シンボルペア通信路における2元線形符号の線形計画復号法について，電子情報

通信学会情報理論研究会(IT)，2015年9月4日，石川県加賀市

⑪ 齋藤　翔太，松嶋　敏泰，一般情報源に対するIntrinsic randomness問題における強逆定理のバリエーション，電子情報通信学会情報理論研究会(IT)，2015年7月13日～14日，東京都目黒区

⑫ Shota Saito, Nozomi Miya, Toshiyasu Matsushima, Fundamental Limit and Pointwise Asymptotics of the Bayes Code for Markov Sources, 2016 IEEE International Symposium on Information Theory(ISIT), 14-19 Jun. 2015, Hong Kong, China.

⑬ 齋藤　翔太，宮　希望，松嶋　敏泰，一般情報源に対するSlepian-Wolf符号化問題の2次の達成可能レート領域の別表現，電子情報通信学会情報理論研究会，2015年3月2日～3日，福岡県北九州市

⑭ 都築　遼馬，松嶋　敏泰，潜在変数によって表現された線形回帰モデルにおけるベイズ基準の下で最適な予測，第37回情報理論とその応用シンポジウム（SITA2014），2014年12月5日～9日，富山県黒部市

⑮ 堀井　俊佑，松嶋　敏泰，平澤　茂一，パラメータが複数存在するLinear Bandit に関する一考察，第37回情報理論とその応用シンポジウム（SITA2014），2014年12月5日～9日，富山県黒部市

⑯ 須子　統太，堀井　俊佑，小林　学，プライバシー保護機能を持つ分散型正則化最小二乗法について，第37回情報理論とその応用シンポジウム（SITA2014），2014年12月5日～9日，富山県黒部市

⑰ 中原　悠太，齋藤　翔太，鎌塚　明，松嶋　敏泰，消失中継通信路上でのDecode-and-Forward 型通信におけるパンクチャされた空間結合LDPC符号のユニバーサル性，第37回情報理論とその応用シンポジウム（SITA2014），2014年12月5日～9日，富山県黒部市

⑱ 大和田　歩，安田　豪毅，松嶋　敏泰，半教師付き学習における予測誤差に対するラベルなしデータの有効性に関する一考察，第37回情報理論とその応用シンポジウム（SITA2014），2014年12月5日～9日，富山県黒部市

⑲ 久保　航汰，齋藤　翔太，鎌塚　明，松嶋　敏泰，非線形コンバイナ型乱数生成器に対するSum - Product Algorithmを用いる攻撃に関する一考察，電子情報通信学会情報論的学習理論と機械学習研究会（IBISML），2014年11月17日～19日，愛知県名古屋市

⑳ Shota Saito, Nozomi Miya, Toshiyasu Matsushima, Evaluation of the Minimum Overflow Threshold of Bayes Codes for a Markov Source, 2014 International Symposium on Information Theory and Its Applications (ISITA2014), 26-29 Oct. 2014, Melbourne, Australia

㉑ Goki Yasuda, Nozomi Miya, Tota Suko, Toshiyasu Matsushima, Asymptotics of MLE-Based Prediction for Semi-Supervised Learning, 2014 International Symposium on Information Theory and Its Applications (ISITA2014), 26-29 Oct. 2014, Melbourne, Australia

㉒ Akira Kamatsuka, Shunsuke Horii, Toshiyasu Matsushima, Parallel Concatenation of Polar Codes and Iterative Decoding, 2014 International Symposium on Information Theory and Its Applications (ISITA2014), 26-29 Oct. 2014, Melbourne, Australia

㉓ Manabu Kobayashi, Masayuki Goto, Toshiyasu Matsushima, Shigeichi

Hirasawa, Robustness of Syndrome Analysis Method in Highly Structured Fault-Diagnosis Systems, 2014 IEEE International Conference on Systems, Man, and Cybernetics (SMC2014), 5-8 Oct. 2014, San Diego, CA, USA

㉔ 増井　秀之，都築　遼馬，宮　希望，松嶋　敏泰，パターン認識における AdaBoostの予測誤り率改善に関する一考察，電子情報通信学会情報論的学習理論と機械学習研究会（IBISML），2014年9月1日～2日，茨城県つくば市

㉕ 松嶋　敏泰，自己情報量の確率分布の眺め方　～n^{-1} と $n^{-1/2}$ と違うスケールで見てみると～，電子情報通信学会情報理論研究会，2014年7月17日～18日，兵庫県神戸市

㉖ Shunsuke Horii, Toshiyasu Matsushima, Shigeichi Hirasawa, Iterative Multiuser Joint Decoding based on ADMM, 2013 IEEE Global Conference on Signal and Information Processing (GlobalSIP), 3-5 Dec. 2013, Austin, USA

㉗ 齋藤　翔太，宮　希望，野村　亮，松嶋　敏泰，ベイズ符号のオーバーフロー確率における最小しきい値の評価，第36回情報理論とその応用シンポジウム (SITA2013)，2013年11月26日～29日，静岡県伊東市

㉘ 鎌塚　明，堀井　俊佑，松嶋　敏泰，Polar 符号を用いた並列連接符号化に関する一考察，第36回情報理論とその応用シンポジウム（SITA2013），2013年11月26日～29日，静岡県伊東市

㉙ 堀井　俊佑，松嶋　敏泰，平澤　茂一，凸最適化に基づいた相関のある複数行列の同時補完に関する一考察，第36回情報理論とその応用シンポジウム(SITA2013)，2013年11月26日～29日，静岡県伊東市

㉚ 吉田　隆弘，地主　創，松嶋　敏泰，分散情報の情報漏洩量に基づく一般的な再生成符号のクラスに対するストレージと修復バンドワイズに関する一検討，第36回情報理論とその応用シンポジウム（SITA2013），2013年11月26日～29日，静岡県伊東市

㉛ 山本　粋士，須子　統太，松嶋　敏泰，次数未知の多変数多項式回帰モデルにおけるベイズ予測，第36回情報理論とその応用シンポジウム（SITA2013），2013年11月26日～29日，静岡県伊東市

㉜ 安田　豪毅，宮　希望，須子　統太，松嶋　敏泰，半教師付き学習における一致推定量に基づく予測の漸近評価，第36回情報理論とその応用シンポジウム（SITA2013），2013年11月26日～29日，静岡県伊東市

㉝ 都築　遼馬，須子　統太，松嶋　敏泰，線形回帰モデルにおけるベイズ決定理論に基づく予測の近似手法，第36回情報理論とその応用シンポジウム（SITA2013），2013年11月26日～29日，静岡県伊東市

㉞ Shunsuke Horii, Tota Suko, Toshiyasu Matsushima, Shigeichi Hirasawa, Iterative Multiuser Joint Decoding based on Augmented Lagrangian Method, 電子情報通信学会情報理論研究会（IT），2013年9月27日，沖縄県宜野湾市

㉟ 堀井　俊佑，分散最適化手法の線型符号の復号への応用，電子情報通信学会誤り訂正符号のワークショップ，2013年9月25～26日，沖縄県宜野湾市

㊱ 吉田　隆弘，地主　創，松嶋　敏泰，分散情報の安全性を考慮した再生成符号のモデル化とその最適性に関する一検討，電子情報通信学会情報理論研究会（IT），2013年7月25日～26日，東京都新宿区

〔その他〕
松嶋研究室ホームページ
http://www.matsu.mgmt.waseda.ac.jp/

６．研究組織

(1)研究代表者

松嶋　敏泰（MATSUSHIMA, Toshiyasu）
早稲田大学・理工学術院・教授
研究者番号：３０２１９４３０

(2)研究分担者

なし

(3)連携研究者

浮田　善文（UKITA, Yoshifumi）
横浜商科大学・商学部・教授
研究者番号：７０３０８２０３

吉田　隆弘（YOSHIDA, Takahiro）
横浜商科大学・商学部・准教授
研究者番号：１０３２９１０４

野村　亮（NOMURA, Ryo）
専修大学・ネットワーク情報学部・准教授
研究者番号：９０３２９１０２

須子　統太（SUKO, Tota）
早稲田大学・社会科学総合学術院・准教授
研究者番号：４０４０９６６０

堀井　俊佑（HORII, Shunsuke）
早稲田大学・グローバルエデュケーション
センター・助教
研究者番号：００５５２１５０