様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２５年　５　月　２１　日現在

機関番号：３２６８９
研究種目：基盤研究（C）
研究期間：2010 ～ 2012
課題番号：22560395
研究課題名（和文）　確率推論アルゴリズムに基づいたストリーム暗号への統一的攻撃法に関する研究
研究課題名（英文）　A Study on Unified Attack against Stream Ciphers based on Probabilistic Inference Algorithms
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

研究成果の概要（和文）：ストリーム暗号の攻撃は疑似乱数生成器の攻撃に帰着される．本研究では，疑似乱数生成器に対する攻撃を「攻撃目標の変数の選択とその順序」と「攻撃のために用いる局所関係の選択」という2点で分類し，問題を統一的な視点から眺めることで，確率推論アルゴリズムに基づく精度の良い効率的な攻撃法を提案した．さらに，現在得られている確率推論の知見で攻撃が可能となる擬似乱数生成器のクラスを明らかにした．

研究成果の概要（英文）：Attack against Stream Cipher reduces to attack against a pseudo random generator. In this study, attack against a pseudo-random number generator was classified based on the choice of target variables and its order and the choice of the local relationships used for attack. We proposed efficient and accurate attack algorithms based on probabilistic inference by studying the problem in unified framework. We revealed the class of pseudo-random number generators that we can attack against based on the acquired knowledge of probabilistic inference so far.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2010 年度	1,600,000	480,000	2,080,000
2011 年度	1,100,000	330,000	1,430,000
2012 年度	700,000	210,000	910,000
年度			
年度			
総　計	3,400,000	1,020,000	4,420,000

研究分野：工学
科研費の分科・細目：電気電子工学，通信・ネットワーク工学
キーワード：ストリーム暗号，確率推論，確率伝搬

１．研究開始当初の背景

ストリーム暗号に対する攻撃は疑似乱数生成器に対する攻撃に帰着される．有名な攻撃法の１つとして相関攻撃が挙げられるが，相関攻撃を含むストリーム暗号に対する攻撃の研究は，以下のように，本来解くべき問題というものを十分吟味せずに手法ありきの形で行われてきた．

・新しい攻撃法が発見される
・上記の攻撃法に耐性をもつ疑似乱数生成器が開発される

このようなアプローチによる研究では，新しい擬似乱数の生成方式を発見したとしても，それに対する新たな攻撃法がいつ発見さ

れるかわからず，暗号が破られる危険性が常に付きまとうという問題点が挙げられる．

２．研究の目的

従来の相関攻撃では，疑似乱数生成器における関数関係の局所的な情報のみが利用されていた．このように局所的関係を利用して推定を行い，低い計算量で高い性能を得る方法は，符号理論や統計力学などで確率推論のアルゴリズムとして盛んに研究されていた．

本研究では，上記の点を踏まえて疑似乱数生成器に対する攻撃を以下の２点で分類することを考えた．

・攻撃目標の変数の選択とその順序
・攻撃のために用いる局所関係の選択

このように，問題を統一的な視点から眺め，単に新たな攻撃法を考えるというだけでなく，その攻撃法に対して脆弱な条件を解明し，新たな安全性の指標を示すことを目的とした．

３．研究の方法

(1) ストリーム暗号の攻撃に関する数理モデルの構築

数理モデルの構築に際してまず，従来提案されている疑似乱数生成器において，入力と出力の間に存在する関数関係としてどのような構造が存在するか，という視点で従来研究の調査・整理を行った．特に，グラフィカルモデルとして表現することで関数関係の抽出を行った．次に，ストリーム暗号に対する従来の攻撃法を先に述べた２つの視点で分類し，整理した．

(2) 構築された数理モデル上での攻撃法の設計

確率的な関数による近似を行う場合の最適な攻撃法の定式化については，多端子情報理論の結果に加えて統計的決定理論および学習理論の結果を融合することで研究を進めた．このような攻撃法は莫大な計算量がかかることが予想されたため，符号理論や通信理論で用いられている効率的な近似アルゴリズムである確率推論アルゴリズムを応用した．

(3) 新たな攻撃に耐性をもつ疑似乱数生成器の設計

(2)で提案された攻撃アルゴリズムに対して耐性をもつ疑似乱数生成器の設計を行った．特に，既存の攻撃法に対する耐性を失わずに，新たな攻撃法に対する耐性をもつような疑似乱数生成器の設計を考える必要があった．

４．研究成果

問題を２．研究の目的で挙げた視点から統一的に眺めることで，現在得られている確率推論の知見で攻撃が可能となる擬似乱数生成器のクラスが明らかになった．例えば，相関攻撃やそれを改良した高速相関攻撃は本研究の枠組みで捉えることができる．さらに，今後発見される攻撃法も上記の２点で説明可能であると考えられる．手法のみを考えていると，他の攻撃法は考慮されないが，統一的な視点で問題を扱うことで，他の分野で数多くの知見が得られている確率推論アルゴリズムに基づいた様々な攻撃法を考えることができた．

今後の展望としては，本研究の着想とアプローチをストリーム暗号だけではなく，様々な情報セキュリティ分野へと拡張することが考えられる．さらに，より広い周辺研究分野の成果を応用し，理論的に最適な攻撃法の導出のみでなく，安全性と利便性のトレードオフの理論的な解析も行っていく必要がある．本研究の過程で開発した効率的確率計算アルゴリズムのソフトウェアは，上記の研究についても，基本的な部分ではある程度利用可能であると考えられる．

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　33　件）

① Yoshifumi Ukita, Toshiyasu Matsushima, Shigeichi Hirasawa, A Study on the Degrees of Freedom in an Experimental Design Model Based on an Orthonormal system, IEICE Trans. Fundamentals, 査読有, Vol.E96-A, No.2, 2013, 658-662 DOI:10.1587/transfun.E96.A.658

② Yoshifumi Ukita, Toshiyasu Matsushima, A Note on Relation between the Fourier Coefficients and the Effects in the Experimental Design , Journal of Communication and Computer, 査読有, Vol.9, No.7, 2012, 830-836 http://www.davidpublishing.com/davidpublishing/Upfile/8/16/2012/2012081670604297.pdf

③ 吉田隆弘，地主創，松嶋敏泰，ランプ型鍵事前配布方式の一般化と最適な構成法について，電子情報通信学会論文誌Ａ，査読有，J95-A, No.10, 2012, 723-736 http://ci.nii.ac.jp/naid/110009518237

④ Ryo Nomura, Toshiyasu Matsushima, An Analysis of Slepian-Wolf Coding Problem Based on the Asymptotic Normality, IEICE Trans. Fundamentals, 査読有, E94-A, 2011, 2220-2225 DOI:10.1587/transfun.E94.A.2220

⑤ Ryo Nomura, Toshiyasu Matsushima, On the Overflow Probability of Fixed-to-Variable Length Codes with

Side Information , IEICE Trans. Fundamentals, 査読有, E94-A, 2011, 2083-2091
DOI: 10.1587/transfun.E94.A.2083

⑥ Shunsuke Horii, Toshiyasu Matsushima, Shigeichi Hirasawa, A Note on the Linear Programming Decoding of Binary Linear Codes for Multiple-Access Channel, IEICE Trans. Fundamentals, 査読有, E94-A, no.6, 2011, 1230-1237
DOI:10.1587/transfun.E94.A.1230

⑦ 前田康成 , 吉田秀樹 , 鈴木正清 , 松嶋敏泰, 学習データが少量しかない場合の文書分類方法に関する一考察, 電気学会論文誌 C , 査読有, Vol.131, No.8, 2011 , 1459-1466
https://www.jstage.jst.go.jp/article/ieejeiss/131/8/131_8_1459/_pdf

⑧ Yoshifumi Ukita, Toshiyasu Matsushima, A Description of Experimental Design on the Basis of an Orthonormal System,Applications of Digital Signal Processing, Applications of Digital Signal Processing,査読有,Chapter 18, 2011, 365-378
DOI: 10.5772/26486

⑨ Shunsuke Horii, Toshiyasu Matsushima, Shigeichi Hirasawa, A Note on the Branch-and-Cut Approach to Decoding Linear Block Codes,IEICE TRANSACTIONS on Fundamentals of Electronics , Communications and Computer Sciences, 査読有, Vol.E93-A, No.11, 2010, 1912-1917
DOI: 10.1587/transfun.E93.A.1912

⑩ Yoshifumi Ukita , Tomohiko Saito , Toshiyasu Matsushima , Shigeichi Hirasawa, A Note on a Sampling Theorem for Functions over $GF(q)^n$ Domain,IEICE Trans. Fundamentals,査読有,Vol.E93-A,no.6, 2010, 1024-1031
DOI:10.1587/transfun.E93.A.1024

⑪ Yoshifumi Ukita, Toshiyasu Matsushima, Shigeichi Hirasawa, Estimation of the Effects in the Experimental Design using Fourier Transforms,IEICE Trans. Fundamentals,査読有,Vol.E93-A,no.11, 2010, 2077-2082
DOI:10.1587/transfun.E93.A.2077

⑫ 前田康成, 雨宮康二, 小林直人, 吉田秀樹, 鈴木正清, 松嶋敏泰, マルコフ決定過程の動作時間と受信バッファ容量が有限の選択再送 ARQ への適用, 電子情報通信学会論文誌 A, 査読有, Vol.J93-A, No.8, 2010, 572-578
http://ci.nii.ac.jp/naid/110007686275

⑬ 吉田隆弘, 松嶋敏泰, 今井秀樹, 複数の鍵配送センターを用いたランプ型鍵事前配布方式,電子情報通信学会論文誌 A, 査読有,Vol.J93-A,No.4,2010,277-288
http://ci.nii.ac.jp/naid/110007610181

⑭ Tota Suko , Toshiyasu Matsushima , Shigeichi Hirasawa , Asymptotic property of universal lossless coding for independent piecewise identically distributed sources , Journal of Discrete Mathematical Sciences & Cryptography, 査読有, Vol. 13, No. 4, 2010, 383-391
http://www.connectjournals.com/file_html_pdf/797804H_jdmsc358_383-391A.pdf

⑮ Tomohiko Saito, Toshiyasu Matsushima, Shigeichi Hirasawa , A Note on Automatic Construction Algorithms for Orthogonal Designs of Experiments Using Error-Correcting Codes, Journal of Discrete Mathematical Sciences & Cryptography, 査読有, Vol. 13, No. 4, 2010, 1024-1031
http://www.connectjournals.com/file_html_pdf/797704H_jdmsc353_369-381A.pdf

〔学会発表〕(計 34 件)

① 堀井俊佑, 須子統太, 松嶋敏泰, 木構造を仮定した信号に対する拡張ラグランジュ法に基づいた圧縮センシングについて, 第35回情報理論とその応用シンポジウム, 2012年12月11日～2012年12月14日, 大分県

② 小林学, 堀井俊佑, 松嶋敏泰, 平澤茂一, MIMO通信路に対するLDPC符号の線形時間ADMM復号, 第35回情報理論とその応用シンポジウム, 2012年12月11日～2012年12月14日, 大分県

③ Shunsuke Horii, Manabu Kobayashi, Toshiyasu Matsushima, Shigeichi Hirasawa, Fault Diagnosis Algorithm in Multi-Computer Systems based on Lagrangian Relaxation Method, 2012 International Symposium on Information Theory and its Applications (ISITA2012), 2012年10月28日～2012年10月31日, Hawaii, USA

④ Yuji Iikubo, Shunsuke Horii, Toshiyasu Matsushima, The Optimal Key Estimation of Stream Ciphers and Its Approximation Algorithm Based on a Probabilistic Inference, 2012 International Symposium on Information Theory and its Applications (ISITA2012), 2012年10月28日～2012年10月31日, Hawaii, USA

⑤ Yoshifumi Ukita, Toshiyasu Matsushima, Shigeichi Hirasawa, A Note on ANOVA in an Experimental Design Model Based on an Orthonormal System, IEEE International Conference on Systems, Man, and Cybernetics (SMC 2012), 2012年10月14日～2012年10月17日, Seoul, South Korea

⑥ 堀井俊佑, 松嶋敏泰, 多重アクセス通信に対する双対分解法に基づいた線形計画復号法, 電子情報通信学会情報理論研究会, 2012年09月27日～2012年09月28日, 群馬県

⑦ Ryo Nomura, Toshiyasu Matsushima , Information Spectrum Approach to Overflow Probability of Variable-Length Codes with Conditional Cost Function, 2012 IEEE International Symposium on Information Theory, 2012年07月01日～2012年07月06日, Massachusetts, USA

⑧ Yoshifumi Ukita, Toshiyasu Matsushima, Shigeichi Hirasawa, A Note on Relation Between the Fourier Coefficients and the Interaction Effects in the Experimental, 4th International Conference on Intelligent & Advanced Systems (ICIAS 2012), 2012年06月12日～2012年06月14日, Kuala Lumpur, Malaysia

⑨ 斉藤友彦, 浮田善文, 松嶋敏泰, 平澤茂一, 実験計画法に適した直交配列の線形計画限界, 情報処理学会第74回全国大会, 2012年03月06日～2012年03月08日, 愛知県

⑩ Yoshifumi Ukita, Toshiyasu Matsushima, A Note on Relation between the Fourier Coefficients and the Effects in the Experimental Design, The Eighth International Conference on Information, Communications and Signal Processing (ICICS 2011), 2011年12月13日～2011年12月16日, Singapore

⑪ 野村亮, 松嶋敏泰, Overflow Probability of Variable-length Codes with Unequal Costs on Code Symbols, 第34回情報理論とその応用シンポジウム, 2011年11月29日～2011年12月02日, 愛知県

⑫ 吉田隆弘, 地主創, 松嶋敏泰, 物理的特徴を用いた認証方式の統計的モデル化と安全性評価に関する一検討, 第34回情報理論とその応用シンポジウム, 2011年11

月29日～2011年12月02日，愛知県

⑬ Shunsuke Horii，Tota Suko，Toshiyasu Matsushima，Shigeichi Hirasawa，A Note on Linear Programming Based Communication Receivers，3rd International Castle Meeting on Coding Theory and Applications，2011年11月11日～2011年11月15日，Spain

⑭ 小林学，後藤正幸，松嶋敏泰，平澤茂一，文脈木重みづけ法を用いた文書分類の誤り確率について，電子情報通信学会非線形問題研究会，2011年11月09日～2011年11月11日，沖縄県

⑮ Yoshifumi Ukita，Toshiyasu Matsushima，Shigeichi Hirasawa，A Note on the Degrees of Freedom in an Experimental Design Model Based on an Orthonormal，IEEE International Conference on Systems，Man，and Cybernetics，2011年10月09日～2011年10月12日，Alaska，USA

⑯ Tomohiko Saito，Hiroshige Inazumi，Toshiyasu Matsushima，Disk Allocation Methods for Cartesian Product Files Using Unequal Error Protection Codes，IEEE International Conference on Systems，Man，and Cybernetics，2011年10月09日～2011年10月12日，Alaska，USA

⑰ 飯窪祐二，堀井俊佑，松嶋敏泰，確率推論アルゴリズムに基づくストリーム暗号の鍵推定に関する一考察，電子情報通信学会情報理論研究会，2011年07月21日～2011年07月22日，岡山県

⑱ 石井智，吉田隆弘，松嶋敏泰，PUFを利用した認証に対する統計的モデル化に関する一考察，電子情報通信学会情報理論研究会，2011年07月21日～2011年07月22日，岡山県

⑲ 吉田隆弘，地主創，松嶋敏泰，鍵配送センターの秘密情報の漏洩を考慮した情報量的に安全な鍵事前配布方式の一検討，電子情報通信学会，情報通信基礎サブソサイエティ合同研究会，2011年3月3日～2011年3月4日，大阪府

⑳ 吉田隆弘，地主創，松嶋敏泰，ランプ型鍵事前配布方式における参加者の記憶容量の下界と最適な構成法について，電子情報通信学会情報理論研究会，2011年 1月18日，奈良県

21 堀井俊佑，松嶋敏泰，平澤茂一，線形計画法に基づいたファクターグラフ上の推論アルゴリズムに関する一考察，電子情報通信学会情報理論研究会，2011年 1月18日，奈良県

22 斉藤友彦，稲積宏誠，松嶋敏泰，平澤茂一，不均一誤り訂正符号を用いた直積ファイルのディスク配置，電子情報通信学会情報理論研究会，2011年 1月18日，奈良県

23 斉藤友彦，浮田善文，松嶋敏泰，平澤茂一，A Linear Programming Bound for Unequal Error Protection Codes，2010 Australian Communications Theory Workshop,2010年12月2日～2010年12月6日，Melbourne，Australia

24 Ryo Nomura，Toshiyasu Matsushima，Achievable Condition in Resolvability Problem for Mixed Sources，第33回情報理論とその応用シンポジウム，2010年11月30日～2010年12月3日，長野県

25 須子統太，堀井俊佑，松嶋敏泰，平澤茂一，複数の相関のある情報源に対するベイズ符号化について，第33回情報理論とその応用シンポジウム，2010年11月30日～2010年12月3日，長野県

26 Shunsuke Horii，Tota Suko，Toshiyasu Matsushima，Shigeichi Hirasawa，Maximum likelihood detection for DS-CDMA using Gr¥{o}bner bases，第33回情報理論とその応用シンポジウム，2010年11月30日～2010年12月3日,長野県

27 Shunsuke Horii,Toshiyasu Matsushima，Shigeichi Hirasawa,Linear Programming Decoding of Binary Linear Codes for Multiple-Access Channel，電子情報通信学会情報理論研究会，2010年9月21日～2010年9月22日，宮城県

28 Yoshifumi Ukita,Toshiyasu Matsushima，A Note on Estimation of the Effects in the Experimental Design using Fourier Transforms，電子情報通信学会ソサエティ大会,2010年9月14日～2010年9月17日，大阪府

29 Yasunari Maeda, Hideki Yoshida, Masakiyo Suzuki, Toshiyasu Matsushima, Applying Markov Decision Processes to Selective-repeat ARQ with Finite Receiver Buffer, 2010 International Symposium on Multimedia and Communication Technology (ISMAC 2010), 2010年9月8日～2010年9月9日, Manila, Philippines

30 Ryo Nomura, Toshiyasu Matsushima, On the Overflow Probability of Lossless Codes with Side Information, 2010 IEEE International Symposium on Information Theory, 2010年6月13日～2010年6月18日, Austin, Texas, USA

31 Daiki Koizumi, Tota Suko, Toshiyasu Matsushima, On the Bayesian Forecasting Algorithm under the Non-Stationary Binomial Distribution with the Hyper Parameter Estimation, Ninth Valencia International Meeting on Bayesian Statistics, 2010年6月3日～2010年6月8日, Spain

32 Tota Suko, Shunsuke Horii, Toshiyasu Matsushima, Shigeichi Hirasawa, Bayes universal source coding scheme for correlated sources, IEEE African Winter School on Information Theory and Communications 2010, 2010年6月1日～2010年6月4日, South Africa

33 Tomohiko Saito, Yoshifumi Ukita, Toshiyasu Matsushima, Shigeichi Hirasawa, Linear Programming Bounds of Orthogonal Arrays for Experimental Designs, IEEE African Winter School on Information Theory and Communications 2010, 2010年6月1日～2010年6月4日, South Africa

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)連携研究者

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

野村　亮 (NOMURA RYO)
専修大学・講師
研究者番号：90329102