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　元 年　 ６ 月 １０ 日現在

機関番号：１５３０１
研究種目：基盤研究(C)（一般）
研究期間：2016～2018
課題番号：１６Ｋ００１８５

研究課題名（和文）時限付き鍵管理による組織内データの漏洩対策に関する研究

研究課題名（英文）Protection against internal leakage of sensitive data using a time-bounded key management system

研究代表者
栗林　稔（Kuribayashi, Minoru）

岡山大学・自然科学研究科・准教授

研究者番号：５０３４６２３５

交付決定額（研究期間全体）：（直接経費）　　3,500,000円

研究成果の概要（和文）：通常の暗号技術だけでは，内部犯行により生じる情報漏洩に対して，復号鍵を持った犯人には全く効果がない．本研究では，組織内の機密データに対する漏洩対策として，許可のない者は暗号化されたデータを閲覧できず，許可を受けた者もファイルを復号した際にファイル内に指紋情報が残るような管理システムを提案した．ファイル内に情報を忍ばせる技術として，PDF文書ファイルへの情報埋め込み方式を考案し，システム上で動作確認を行った．更に，電子指紋符号で符号化した指紋情報において，不正コピーから抽出された符号語から，攻撃戦略を推定する手法を考案し，最適な検出器の実現にも成功した．

研究成果の学術的意義や社会的意義
本研究により，機密データの管理システムにおいて，暗号化ツールだけでは防ぐことが難しかったスパイのような内部犯罪者による情報漏洩対策を施すことを可能にした．本成果では，漏洩自体を防ぐことは困難であるが，漏洩した場合にそのファイルを検挙できれば，不正者が誰であるかを特定することが可能である．それゆえ，本システムが導入されていることが広く認識されれば，情報漏洩の抑止に繋がるものと考えられる．本システムは，クラウド環境においても比較的高速に動作させることが可能であり，適用できる範囲は広い．安全なデータ管理において，本研究で得られた成果を応用させれば，産業スパイによる情報漏洩抑止が期待できる．

研究成果の概要（英文）：It is difficult to prevent a malicious user who has privilege in an organization from leaking sensitive data even if an encryption tool is used. In this study, we proposed a secure data management system which gives permission for users by access control technique based on cryptographic tools and allows a system manager to identify traitors from leaked file. The traceability is realized by embedding digital fingerprint of the user who access to the file. We proposed a method for embedding such a fingerprint into PDF document and implement on a management system. The fingerprint is encoded by a collusion secure code so as to tolerate a collusion attack by a coalition of traitors. We proposed an optimal detector by estimating the collusion strategy and the number of traitors from the information extracted from a pirated copy.

研究分野：マルチメディアセキュリティ

キーワード：電子指紋　結託耐性符号　暗号プロトコル　電子透かし　高機能暗号

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

企業や行政機関内で保管されている機密情報や個人情報の管理は細心の注意を払っていても，ネットワークを経由したサイバー攻撃によって漏洩してしまう恐れが最近は高まっている．物理的にネットワークから隔離できないサービスの場合には，ソフトウェアの脆弱性の性格を考えると漏洩を完全に防ぐことは困難であると思われる．技術的な対策として，定期的なソフトウェアのアップデートを施すだけでなく，重要なデータは暗号化した状態で保管するなどの措置が求められる．しかし，内部犯行により生じる漏洩事件については，たとえ高度な暗号処理がなされていたとしても，復号鍵を持った犯人には全く効果がない．

漏洩したデータを詳しく調べると犯人に関する情報が得られる仕組みを導入できれば，少なくとも犯人を検挙することは可能である．データ漏洩を完全に防ぐことは難しいが，この技術の存在が一般にも広く知られるようになれば，犯行を抑止できると期待される．

これまで国内外での研究では主に，不正者を追跡するための情報をどのように作成するかについて議論がなされてきた．しかも，マルチメディアコンテンツに特化していたり，暗号化・復号の鍵のみを対象としているなど，その流通過程や管理体制などについては考慮されていなかった．個別の環境においては威力を発揮したとしても，実運用という意味では仮定している環境や攻撃モデルが現実と乖離しているため，不正者を特定できない恐れがある．

２．研究の目的

ディジタルデータの不正流出や海賊版コンテンツの蔓延に対して，流出元を特定できる電子指紋技術が研究されている．主にマルチメディアコンテンツをターゲットに信号処理的なアプローチや符号理論的なアプローチなどが考案されてきた．本研究では，機密情報や個人情報などのデータに対して，暗号化による情報保護に加えて電子指紋技術を組み合わせた，情報管理システムの構築を目的とする． また，流出元及び不正者の特定を可能であることを科学的に示すことで，不正行為自体を積極的に抑止できるシステムの実現を目指す．

３．研究の方法

システム内に登録されているユーザが，ファイルを開く際に行う処理に応じて，ユーザの指紋情報がファイルに痕跡として残るように，暗号化処理とユーザに割り当てる復号鍵を管理する方法を開発する．申請者が以前に提案したブロードキャスト型のシステムを基本として，時限付き鍵管理の仕組みを組織内のユーザ管理に適用できるように修正する．このアイディアを基に理論的にセキュリティ面に問題がないかを確認しつつ，効率的に実現できるシステムを構築していく．実際にシステムを動かしながら，その実用性を評価する．

４．研究成果

組織内の機密データに対する漏洩対策として,暗号技術を用いたアクセス権を制御するシステムの構築と,内部の許可を受けた利用者による不正漏洩を防ぐシステムの構築を目指した方式を提案した．高機能暗号を利用してアクセス構造を2重にして，許可のない者には暗号化されたデータを閲覧できないようにして,更に許可を受けた者もファイルを復号した際に,使用した鍵によってファイル内にその利用者を特定する情報が残るような管理システムを提案した．

ファイル内に情報を忍ばせるための技術として，PDF文書ファイルへの情報埋め込み方式を考案した．埋め込み可能な容量と視覚的な品質の劣化，秘匿性のトレードオフにおいて，既存手法に比べて良好な特性を示すことを数量的に示した．MS-Wordファイルから変換して作成したPDFファイル，およびLatexで作成した文書ファイルを変換したPDFファイルにおいて，自動的に処理を行えるシステムを構築し，動作確認を行った．

複数の利用者による結託攻撃を想定して，埋め込む情報を電子指紋符号で符号化し，不正者の特定をするための手法も考案した．特に結託攻撃によって改変された符号語から，行われた攻撃戦略を推定する手法を考案し，最適な検出器の実現に成功した．

以上の管理システムにおいて，それぞれの基幹技術を確立させるだけでなく，実装して全体としての処理コストを見積もった．標準化されたPDFファイル規約に応じて処理するため，そのフォーマットを検証するためのツールにおける処理時間が比較的長くなってしまうが，提案システムにおける処理自体は数百ミリ秒程度で動作させることが可能であり，実用的な範囲内で実装できたと考えている．

５．主な発表論文等

1. M. Kuribayashi and N. Funabiki, "Decentralized tracing protocol for fingerprinting system," APSIPA Trans. Signal and Information Processing, vol.8, 8 pages, 2019. DOI: 10.1017/ATSIP.2018.28（査読有り）

2. M. Kuribayashi, T. Fukushima, and N. Funabiki, "Robust and secure data hiding for PDF text document," IEICE Trans. Information and Systems, vol.E102-D, no.1, pp.41-47, 2019. DOI: 10.1587/transinf.2018MUP0003 （査

読有り)

3. M. Kuribayashi, "Bias-based binary fingerprinting code under erasure channel," IEEE Signal Processing Letters, vol.25, no.9, pp.1423-1427, 2018. DOI: 10.1109/LSP.2018.2863034 (査読有り)

4. M. Kuribayashi and N. Funabiki, "Fingerprinting for multimedia content broadcasting system," Elsevier J. Information Security and Applications, vol.41, pp.52-61, 2018. DOI: 10.1016/j.jisa.2018.06.002 (査読有り)

5. M. Kuribayashi, T. Fukushima, and N. Funabiki, "Data hiding for text document in PDF file," The 13th Int. Conf. Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP2017), pp.390-398, 2017. (査読有り)

〔雑誌論文〕(計 9件)

1. M. Kuribayashi and N. Funabiki, "Decentralized tracing protocol for fingerprinting system," APSIPA Trans. Signal and Information Processing, vol.8, 8 pages, 2019. DOI: 10.1017/ATSIP.2018.28 (査読有り)

2. M. Kuribayashi, T. Fukushima, and N. Funabiki, "Robust and secure data hiding for PDF text document," IEICE Trans. Information and Systems, vol.E102-D, no.1, pp.41-47, 2019. DOI: 10.1587/transinf.2018MUP0003 (査読有り)

3. M. Kuribayashi, "Bias-based binary fingerprinting code under erasure channel," IEEE Signal Processing Letters, vol.25, no.9, pp.1423-1427, 2018. DOI: 10.1109/LSP.2018.2863034 (査読有り)

4. M. Kuribayashi and N. Funabiki, "Fingerprinting for multimedia content broadcasting system," Elsevier J. Information Security and Applications, vol.41, pp.52-61, 2018. DOI: 10.1016/j.jisa.2018.06.002 (査読有り)

5. M. Kuribayashi and N. Funabiki, "Universal scoring function based on bias equalizer for bias-based fingerprinting codes," IEICE Trans. Fundamentals, vol.E101-A, no.1, pp.119-128, 2018. DOI: 10.1587/transfun.E101.A.119 (査読有り)

6. V. B. Joshi, M. S. Raval, and M. Kuribayashi, "Reversible data hiding based compressible privacy preserving system for color image," Springer Multimedia Tools and Applications, vol.77, no.13, pp.16597-16622, 2018. DOI: 10.1007/s11042-017-5230-8 (査読有り)

7. H. G. Schaathun and M. Kuribayashi, "Obfuscation in digital fingerprinting," Int. J. Information and Coding Theory, vol.4, no.2/3, pp.185-200, 2017.DOI: 10.1504/IJICOT.2017.083845

8. M. Kuribayashi, S. Shigemoto, and N. Funabiki, "DCT-OFDM watermarking scheme based on communication system model," IEICE Trans. Fundamentals, vol.E100-A, no.4, pp.944-952, 2017. DOI: 10.1587/transfun.E100.A.944 (査読有り)

9. M. Kuribayashi and M. Morii, "Aesthetic QR code based on modified systematic encoding function," IEICE Trans. Information and Systems, vol.E100-D, no.1, pp.42-51, 2017. DOI: 0.1587/transinf.2016MUP0002 (査読有り)

〔学会発表〕(計 29件)

1. M. Kuribayashi, S. Suma, N. Funabiki, "Efficient decoding algorithm for cyclically permutable code," 2018 IEEE Information Theory Workshop (ITW2018), pp.310-314, 2018. (査読有り)

2. T. Yasui, M. Kuribayashi, N. Funabiki, and I. Echizen, "Estimation of collusion attack in bias-based binary fingerprinting code," Asia-Pacific Signal and Information Processing Association Anual Sumit and Conf. (APSIPA ASC 2018), 2018. (査読有り)

3. M. Kuribayashi, T. Ueda, and N. Funabiki, "Secure data management system with traceability against internal leakage," Asia-Pacific Signal and Information Processing Association Anual Sumit and Conf. (APSIPA ASC 2017), pp.1486-1494, 2017. (査読有り)

4. T. Ueda, M. Kuribayashi, and N. Funabiki, "Fingerprinting system for secure manegement of sensitive data," The 12th Int. Workshop on Security (IWSEC2017), Poster Session, 2017. (査読有り)

5. T. Fukushima, M. Kuribayashi, and N. Funabiki, "Imperceptible watermarking scheme with large capacity considering the internal structure of PDF file," The 12th Int. Workshop on Security (IWSEC2017), Poster Session, 2017. (査読有り)

6. M. Kuribayashi, T. Fukushima, and N. Funabiki, "Data hiding for text document in PDF file," The 13th Int. Conf. Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP2017), pp.390-398, 2017. (査読有り)

7. M. Kuribayashi, E.-C. Chang and N. Funabiki, "Watermarking with fixed decoder for aesthetic 2D barcode," 15th Int. Workshop Digital-forensics and Watermarking (IWDW2016), LNCS 10082, pp.379-392, Springer-Verlag, 2017. (査読有り)

8. 安井達哉, 栗林稔, 舩曳信生, "雑音環境における電子指紋符号に対する結託攻撃の攻撃戦略推定," 信学技報, EMM 3月, 2019.

9. 河田健斗, 栗林稔, 舩曳信生, "CNN を用いた CG と写真を識別するためのパッチサイズの考察," 信学技報, EMM 3月, 2019.

10. M. Kuribayashi and N. Funabiki, "Delegated tracing protocol for asymmetric fingerprinting," The 2019 Symp. on Cryptography and Information Security (SCIS2019), 2019.

11. M. Kuribayashi and N. Funabiki, "Optimal error correcting decoder with self-synchronization capability," Technical Report of IEICE, EMM, Jan., 2019.

12. 福島拓哉, 栗林稔, 舩曳信生, "PDF 文書に対する電子指紋システムへの適用を考慮した行セグメント分割埋め込み法," 信学技報, EMM 11月, 2018.

13. 上田貴大, 栗林稔, 舩曳信生, "組織内の情報漏洩を抑止するための電子指紋システムの実装評価," 信学技報, EMM 11月, 2018.

14. 安井達哉, 栗林稔, 舩曳信生, "電子指紋符号における不正者検出のための動的戦略推定," 信学技報, EMM 9月, 2018.

15. 須磨尚大, 栗林稔, 舩曳信生, "Cyclically Permutable Code の同期回復と誤り訂正に関する考察," 信学技報, EMM 5月, 2018.

16. 栗林稔, 村上元貴, 舩曳信生, "画像の局所的な特徴を考慮したデザイン QR コードに関する考察," 信学技報, EMM 5月, 2018.

17. 安井達哉, 栗林稔, 舩曳信生, "電子指紋符号における結託攻撃の戦略推定," 信学技報, EMM 3月, 2018.

18. 小浦啓太郎, 栗林稔, 舩曳信生, "量子化テーブルの特徴を考慮した JPEG 圧縮履歴の解析," 信学技報, EMM 3月, 2018.

19. 栗林稔, "データハイディング技術における攻撃耐性 ～ ロバスト性と安全性 ～" 信学技報, EMM 3月, 2018.

20. M. Kuribayashi and N. Funabiki, "A study of tracing algorithm for fingerprinting code considering erasure symbols," Technical Report of IEICE, EMM Jan., 2018.

21. M. Kuribayashi, Vaibhav B. Joshi, Mehul S. Raval, "Compression-friendly reversible data hiding for privacy protection," Technical Report of IEICE, EMM Nov., 2017.

22. 重本章吾，栗林稔，舩曳信生，"誤り訂正符号を用いたDCT-OFDM型電子透かし方式の耐性向上に関する考察," 信学技報，EMM 11月，2017.

23. 山下晃一郎，栗林稔，舩曳信生，"電子透かし方式の安全性を高めるための難読化処理に関する考察," 信学技報，EMM 11月，2017.

24. 福島拓哉，栗林稔，舩曳信生，"PDFファイルの内部構造を考慮した大容量電子透かし法," 信学技報，EMM 5月，2017. 2017年度 EMM研究会 学生研究賞受賞

25. 上田貴大，栗林稔，舩曳信生，"組織内からの情報漏洩対策のための電子指紋システムの提案," 信学技報，EMM 5月，2017.

26. M. Kuribayashi and N. Funabiki, "Universal scoring functions for bias-based fingerprinting code under relaxed marking assumption," The 2017 Symp. on Cryptography and Information Security (SCIS2017), 2017.

27. 行地将智，栗林稔，Ee-Chien Chang，舩曳信生，石原信也，"任意の画像のQRコード化とそのアプリ開発," 信学技報，EMM 11月，2016.

28. 重本章吾，栗林稔，舩曳信生，"雑音特性を考慮した電子透かし方式への誤り訂正符号の適用と考察," 信学技報，EMM 7月，2016.

29. 山下晃一郎，栗林稔，舩曳信生，"ケルクホフスの原理に基づく電子透かし方式の安全性において特徴選出および信号処理の重要性," 信学技報，EMM 7月，2016.