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　５ 年　 ６ 月 １６ 日現在

機関番号：２１６０２
研究種目：基盤研究(C)（一般）
研究期間：2019～2022
課題番号：１９Ｋ１１８３１

研究課題名（和文）秘密分散法の効率化に関する研究

研究課題名（英文）On improving efficiency of secret sharing schemes

研究代表者
渡辺　曜大（Watanabe, Yodai）

会津大学・コンピュータ理工学部・上級准教授

研究者番号：７０３６０６７５

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：秘密分散法とは，資格を有する参加者集合のみが復元できるように秘密情報を分散暗号化するための暗号技術であり，重要な情報に対する安全なアクセス制御を実現するための核となる技術です．本研究では，人間の目や耳を用いて復号演算を実行することのできる一風変わった秘密分散法（前者を視覚復号型秘密分散法，後者を聴覚復号型秘密分散法と呼びます）について，一般的な構成法の安全性を理論的に評価し，さらに，具体的な構成法を取り上げて，復元画像・復元音声の品質（前者については視覚認証に適用した際の改ざん検出確率，後者については雑音による音質劣化の程度）を実験により調べました．

研究成果の学術的意義や社会的意義
本研究では，ディスプレイをもたない端末と人間の間の安全な通信を保証することを目的とした視覚認証における，敵対者による改ざんの検出確率を向上させるために，複数画像を暗号化する視覚復号型秘密分散法を適用する手法を提案し，実験により高い確率で改ざん検出に成功するための条件（パラメータ）を調べました．さらに，聴覚復号型秘密分散法を具体的な構成法にもとづいて実装し，条件（パラメータ）を変化させながら復元音声の品質を人間自身や音質評価指標によって評価しました．これにより，これらの秘密分散法の効率的な実装のための指針（適切なパラメータの選び方）が得られることが期待できます．

研究成果の概要（英文）：The secret sharing scheme is a cryptosystem which encrypts a secret into multiple pieces, called shares, so that only qualified combination of shares can be employed to recover the secret. There exist curious secret sharing schemes whose decryption can be performed by a human. In this study, the security of general constructions of such curious secret sharing schemes was theoretically evaluated, and the quality of the recovered image and recovered audio given by specific constructions was experimentally examined.

研究分野：暗号

キーワード：秘密分散　暗号

１．研究開始当初の背景

秘密分散法とは，以下の 2 つの条件をみたすように秘密情報を暗号化して複数の参加者に分配する暗号技術である：① 資格を有する参加者集合（有資格集合）は秘密情報を完全に復元できるが，② 資格のない参加者集合（禁止集合）は秘密情報に関するいかなる部分情報も得ることができない．秘密情報が分散暗号化され，各参加者に分配される情報のことを分散情報と呼ぶ. 秘密分散法の典型的な例は, 参加者 n 人のうち k 人以上からなる集合が有資格集合，k-1 人以下からなる集合が禁止集合となるもので, (k,n)しきい値型秘密分散法とよばれる．適切に設計された秘密分散法は，情報の漏えいと紛失を同時に防ぐことが可能であり，重要な情報に対するアクセス制御を実現するための核となる技術である．

２．研究の目的

秘密分散法の特性を評価する上で重要なパラメータの一つに情報比がある．これは，分散情報のサイズ（ビット長）を秘密情報のサイズで割ったもので，小さければ小さいほど良い．秘密分散法に関する重要な未解決問題として，この情報比の最適性の問題，および，計算量的秘密分散法の存在性の問題が挙げられる．これらの問題は，単に実用上重要なだけでなく，例えば，ある特別な計算量的秘密分散法の存在が暗号学におけるもっとも主要な未解決問題の一つを解決することが知られており，学術の立場からも重要である．本研究の目的は，これらの重要な未解決問題を念頭に，秘密分散法の効率性に関して新しい知見を得ることである．

３．研究の方法

秘密分散法には，人間の目あるいは耳を使って復号が可能な一風変わったものが存在する．前者を視覚復号型秘密分散法，後者を聴覚復号型秘密分散法とよぶ．視覚復号型秘密分散法では，秘密情報は画像（白黒画像）であり，これを暗号化して生成された白黒画像を透明なシートに印刷したものが各参加者に分配される分散情報になる．復号は資格を有する参加者集合に属する参加者が持ち寄った透明なシート（分散画像）を重ね合わせ，現れた画像を人間の目で判別することにより行われる．一方，聴覚復号型秘密分散法では，分散情報は音声であり，復号は資格を有する参加者集合に属する参加者が持ち寄った音声（分散音声）を同時再生し，合成された音声を人間の耳で判別することにより行われる．上述の重要な未解決問題に対して完全な解答を与えることは難問であるため，本研究ではまず，具体的な秘密分散法としてこの視覚復号型秘密分散法および聴覚復号型秘密分散法を取り上げ，その効率性に関して新しい知見を得ることを目指す．

４．研究成果

(1) 聴覚復号型秘密分散法[f]

視覚復号型秘密分散法において秘密情報および分散情報はともに画像であるのに対し，聴覚復号型秘密分散法では分散情報が音声であることは共通しているが，何を秘密情報とするかに応じて以下の 2 つのタイプが存在する：(i) 2 進文字列を暗号化する聴覚復号型秘密分散法[b]，(ii) 音声情報を暗号化する聴覚復号型秘密分散法[j]．本研究では，人間が耳で聞いて理解しやすい(ii)を扱う．研究[f]において，単なる分散音声の和から重み付きの和に一般化された復号関数に関して，しきい値型聴覚復号型秘密分散法の一般的な構成法を与え，その安全性を秘密音声と分散音声の相関（相互情報量）を調べることによって理論的に評価した．（この構成法の情報比は 1 であり，情報比に関して最適なものになっている．）次に，復号された秘密音声の品質の目安として，信号雑音比と暗号化関数のパラメータとの関係を調べた．さらに，具体的な構成法として，暗号化関数に特別な形の行列（Vandermonde 行列）を用いる方式を取り上げ，計算機実験により，しきい値型聴覚復号型秘密分散法の定義，特に，その雑音耐性の定義の妥当性について調べた．具体的には，聴覚復号型秘密分散法の暗号化関数の標準的な実装において不可避的に存在する丸め誤差と桁あふれ誤差に注目し，聴覚復号型秘密分散法のパラメータを変化させて適当な秘密音声に対して分散音声を生成して，復号音声の品質と雑音耐性との間の関係を調べた．その結果，桁あふれ誤差がほとんどなく丸め誤差が支配的である状況においては，雑音耐性と復号音声の品質の間には正の相関が見て取れるが，桁あふれ誤差が一定程度の割合で存在する状況では，雑音耐性と復号音声の品質の間の相関が低いことが分かった．したがって，雑音耐性の定義を桁あふれ誤差の出現確率を取り入れる形に改良する必要がある．そこで，雑音耐性に桁あふれ誤差の発生確率の期待値によって定まる項を付加する修正を加えて，再度，雑音耐性と復号音声の品質の間の相関を調べた．ここで，復号音声の品質の評価には，客観音質評価指標である ViSQOL[e]（主観音質評価値と高い相関をもつことが知られている）を用いた．その結果，上記の修正により，修正前と比較して，音質評価指標との相関（Spearman の順位相関係数(SRCC)，非線形変換後の Pearson の積率相関係数(PLCC)・二乗平均平方根誤差(RMSE)のいずれも）が高くなることが確認できた．

(2) 視覚復号型秘密分散法

複数の秘密情報を許容したアクセス構造を実現する視覚復号型秘密分散法[i]の適用先候補として，先行研究により提案されている視覚認証[g]が挙げられる．ここで，視覚認証と

は，ユーザーがICカードのようなディスプレイをもたない端末により店頭で決済を行う際に（ここで，店は潜在的な敵対者と考える），視覚復号型秘密分散法を利用することにより人間・端末間の通信の認証を実現しようというものである．このとき，通信路は敵対者の完全な制御下にあると考えなければならないが，安全な通信路を仮定せずにこの問題を解決するのは難しく，現在のところ，視覚認証がこの問題の唯一の解である．通常の（単一の秘密画像を暗号化する）視覚復号型秘密分散法を用いた視覚認証[g]において，敵対者による改ざんを検出するための一つの方法として，秘密画像を 2 つの領域に分割して，一方をメッセージに，他方を改ざん検出に用いることが提案されている．ここで，黒画像中の白画素は検出しやすいことを利用するために，秘密画像の改ざん検出領域には完全な黒画像を用いる．このとき，メッセージ領域と改ざん検出領域をランダムに選べば，改ざんには相当数の画素の変更が必要であるという仮定の下でほぼ 1/2 の確率（どちらの領域であるかの推測が当たる確率）で改ざんを検出できることになる．一方，複数の秘密画像を暗号化する視覚復号型秘密分散法を用いると，メッセージ画像と改ざん検出画像の 2 つの秘密画像を暗号化することによって，メッセージ領域と改ざん検出領域を同一にとることができ（その代わり，復元メッセージ画像のコントラストが1/4になる），上記の仮定の下で改ざん検出確率がほぼ 1 となることが期待できる．この視覚認証について，実際にディスプレイに表示した分散画像に OHP シートに印刷した分散画像を重ねて復元画像を判別する実験を実施することによって，改ざん検出の精度を調べた．一般に，ディスプレイの表示，プリンターによる印刷，人間による画像の重ね合わせそれぞれに誤差が存在するため，画素が小さすぎると改ざん検出用の黒画像が完全な黒画像には見えにくくなり，検出の精度が低下する．そこで，画素ピッチが 0.265㎜ であるディスプレイを用いて視覚認証の実験を実施し，分散画像の解像度に関してどの程度まで実用に耐えうるか調べた．1 回の実験では，改ざんを行うか否かを確率 1/2 で選択し，実際に人間が復号（ディスプレイに出力された分散画像に自身のもつ OHP シートを重ね合わせること）を行うことによって，改ざんの有無を識別できるかどうか調べ，これを複数回繰り返した．ここで，改ざんが選択された場合は，改ざん検出画像（改ざんがなければ完全な黒画像となる）中のランダムな位置に 1 つの白画素が生じるように分散画像の改変を行った．その結果，分散画像の 1 画素に対してディスプレイの 2*2=4 画素を対応させれば，実験した範囲において，改ざんの有無を 100%識別できる（復元画像が完全な黒画像か否か判別できる）ことが分かった．この他に，視覚復号型秘密分散法の基礎行列をすべて列挙する全数探索により，安全で正のコントラストをもつ視覚復号型秘密分散法の分布を計算機実験により調べた．

上記(1)(2)の成果により，視覚認証や聴覚復号型秘密分散法の効率的な（要求される特性に対して無駄のない）実装のための指針が得られることが期待できる．これらに加えて，さらに，以下の成果を得た．

(3) 量子乱数抽出[k]，安全性概念の分離[l]

乱数抽出とは，与えられた情報源から，情報源と相関を持つ副情報に対してほぼ一様に分布する鍵を抽出する技術のことである．研究[k]において，通常（例えば[h]）とは異なる平滑化に基づく量子衝突エントロピーによって抽出可能な鍵長が定まる量子乱数抽出を与えた．衝突エントロピーが劣加法的であるという事実に基づき，付加副情報に関して最大化された量子衝突エントロピーを導入し，これが漸近的に最適であることを示した．そこで導かれた下界は，条件付けられていない 2 つのエントロピーの差の形であらわされ，したがって，その評価は，全系上および副情報の周辺系上の 2 つの量子状態の固有値問題に帰着されることになる．なお，量子乱数抽出の応用例としては，量子鍵配送が挙げられる．量子鍵配送とは，情報理論的に安全な乱数（鍵）の共有を実現する現在最も実用化に近い量子情報技術であり，本研究課題で扱っている秘密分散法を含む情報理論的に安全な暗号の効率的な実装に役立つことが期待できる．

さらに，公開鍵暗号の頑強性(non-malleability)の定式化の間に成り立つ関係について以下の結果を得た．ここで，頑強性[c]とは，敵対者が受け取った暗号文から，対応する平文同士が何らかの関係をもつように別の暗号文を生成することができないという，暗号文の改変に対する耐性を保証する安全性概念である．頑強性は公開鍵暗号系以外のさまざまな暗号プリミティブに対しても定式化されており，秘密分散法に関しても頑強性が定式化され，頑強なしきい値型秘密分散法の構成法が与えられている[d]．公開鍵暗号の頑強性には，それがシミュレーションにもとづくか比較にもとづくか，あるいは，敵対者の生成する暗号文が正規のものでなければならないという正規暗号文条件を課すか課さないかに応じて複数の定式化が存在する．これらの定式化に加えて，並列暗号文攻撃(parallel chosen-ciphertext attack)に対する識別不可能性(indistinguishability)と呼ばれる定式化も提案されている．これら 3 つの定式化は，正規暗号文条件を課さなければ同値であることが知られている[a]が，正規暗号文条件を課した場合は，最も強力な攻撃モデルに対してはこれらの同値性が知られているものの，弱い攻撃モデルにおけるこれらの定式化の間の関係はいまだ未解決である．そこで，研究[l]において，弱い攻撃モデルにおいてはこれらの定式化が分離することを示した．さらに，並列暗号文攻撃に対する強秘匿性(semantic

security)を導入し，これが，頑強性と同値であることを示した．これにより，並列暗号文攻撃に対しては，正規暗号文条件のもとで強秘匿性と識別不可能性が分離する（この 2 つは多くの状況において同値であることが示されている）ことが分かった．

＜引用文献＞

[a] M. Bellare and A. Sahai: Non-malleable encryption: Equivalence between two notions, and an indistinguishability-based characterization, Proceedings of Advances in Cryptology - CRYPTO '99, Lecture Notes in Computer Science, vol. 1666, 519-536, 1999.

[b] Y. Desmedt, S. Hou and J.-J. Quisquater: Audio and optical cryptography, in Proceedings of Advances in Cryptology - Asiacrypt '98, Lecture Notes in Computer Science, vol. 1514, Springer-Verlag, 392-404, 1998.

[c] D. Dolev, C. Dwork and M. Naor: Non-malleable cryptography, SIAM Journal on Computing 30(2), 391-437, 2000.

[d] V. Goyal and A. Kumar: Non-malleable secret sharing, in Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing (STOC 2018), 685-698, 2018.

[e] A. Hines, J. Skoglund, A. C. Kokaram and Naomi Harte: ViSQOL: an objective speech quality model, EURASIP Journal on Audio, Speech, and Music Processing 2015, 13, 2015.

[f] T. Ishizuka and Y. Watanabe: Threshold audio secret sharing schemes encrypting audio secrets, 2020 IEEE International Workshop on Information Forensics and Security (WIFS 2020), 1-5, 2020.

[g] M. Naor and B. Pinkas: Visual authentication and identification, in Proceedings of Advances in Cryptology - Crypto '97, Lecture Notes in Computer Science, vol. 1294. 322-336, 1997.

[h] R. Renner and R. Konig: Universally composable privacy amplification against quantum adversaries," in in Proceedings of Theory of Cryptography Conference - TCC 2005, Lecture Notes in Computer Science, vol. 3378, 407-425, 2005.

[i] M. Sasaki and Y. Watanabe: Visual secret sharing schemes encrypting multiple images, IEEE Transactions on Information Forensics and Security 13(2), 356-365, 2018.

[j] S. Washio and Y. Watanabe: Security of audio secret sharing scheme encrypting audio secrets with bounded shares, in Proceedings of the 39th IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2014), 7396-7400, 2014.

[k] Y. Watanabe: Randomness extraction via a quantum generalization of the conditional collision entropy, IEEE Transactions on Information Theory 66(2), 1171-1177, 2020.

[l] Y. Watanabe: Separations among formulations of non-malleable encryption under valid ciphertext condition, IACR Cryptology ePrint Archive 2023/477, 2023. https://ia.cr/2023/477

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　1件）

1．著者名 Yodai Watanabe	4．巻 66
2．論文標題 Randomness extraction via a quantum generalization of the conditional collision entropy	5．発行年 2020年
3．雑誌名 IEEE Transactions on Information Theory	6．最初と最後の頁 1171～1177
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIT.2019.2953155	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 －

〔学会発表〕　計1件（うち招待講演　0件／うち国際学会　1件）

1．発表者名 Tetsuro Ishizuka and Yodai Watanabe
2．発表標題 Threshold audio secret sharing schemes encrypting audio secrets
3．学会等名 2020 IEEE International Workshop on Information Forensics and Security (WIFS)（国際学会）
4．発表年 2020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
研究分担者	前田　多可雄 (Maeda Takao) (00264565)	会津大学・コンピュータ理工学部・教授 (21602)	

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