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

平成　２９　年　　６　月　２６　日現在

機関番号：　１２１０３
研究種目：　基盤研究(C)（一般）
研究期間：　2012～2016
課題番号：　２４５００００５

研究課題名（和文）双線形写像を用いた匿名認証方式の基盤構築

研究課題名（英文）The Construction for Anonymous Authentication Scheme using Bilinear Pairing

研究代表者
岡本　健（Okamoto, Takeshi）

筑波技術大学・保健科学部・准教授

研究者番号：００３４９７９７

交付決定額（研究期間全体）：（直接経費）　　4,100,000円

研究成果の概要（和文）：本研究では、双線形写像を用いたブロードキャスト暗号の基盤技術を構築した。提案方式では、送信者が自身の秘密鍵を用いて暗号文を生成することにより、受信者が送信者の本人認証とメッセージ認証を行うことができる。さらに、提案方式を応用し、1-out-of-n 署名と検証者指定署名の特徴をあわせた署名方式が構築できることを示した。提案方式に対し定量的な評価についても行った。
また匿名認証の要素技術として利用するため、CAPTCHAの研究についても取り組んだ。本研究では、複数階数のマルコフ連鎖に基づき新規に生成された機械合成文を自然文として用いることで、数に制限のない作問を生成することが可能になった。

研究成果の概要（英文）：In this research, we study broadcast encryption using bilinear pairing. In our scheme, a sender encrypts data using his private key. This allows the receiver to authenticate the sender and the message. Furthermore, we consider the efficient signature scheme combining both functions of 1-out-of-n signatures and designated-verifier signatures.
We also study CAPTCHA to use the fundamental technique of anonymous authentication. The current CAPTCHA mainly uses perceptual recognition with images or sounds, but it is difficult for visually or hearing-impaired people to leverage it. We propose a new identification scheme. Our scheme uses a verbal question which is identification of natural sentences and word salads. We generate natural sentences as word salads which are generated by the Markov chain with multi-state. Such sentences are generated almost unbounded volume by using online documents and it is hard for adversaries to find them by search engine.

研究分野：　情報セキュリティ

キーワード：　暗号　電子署名　相手認証　匿名認証　ペアリング　CAPTCHA

１．研究開始当初の背景

(1) 匿名認証

現在、インターネットに代表される広域網を使った通信インフラが発達し、その上でさまざまなシステムが実現されている。特にクラウドを用いた各種サービスが広く展開されており、利用者の利便性向上に寄与している。このようなシステムにおいて、情報の価値を保つためには、暗号・認証技術といったセキュリティ技術が必要である。特に電子署名に代表される認証処理は、情報の正当性を確保するうえで、必要不可欠な技術となっている。

しかしながら、現在の認証処理システムは、署名の作成時や、検証を行う際に、利用者の個人情報が流出するリスクがある。例えばインターネットの電子商取引において、顧客がネット上の店で買い物をする際、現在のシステムでは、顧客は店に対して住所や氏名、クレジットカード番号などの個人情報を提示している。この情報が顧客の意図しないところで再配布され、顧客のプライバシ侵害や経済的な損失を引き起こす事件が起きている。法律面では 2005 年から個人情報保護法が全面的に施行されたが、技術面ではまだ整備されていない部分も多く、個人情報の漏洩事件は規模の大小にかかわらず現在でも多発しているのが現状であり、このことが大きな社会問題となっている。

このような問題を解決するため、情報セキュリティの分野では、「匿名認証」と呼ばれるいくつかの方式が提案されている。例えば、リング署名[1]の場合、検証段階において、検証者は署名者が「あるグループに所属している」ことは確認できるが、「誰であるか」まではわからない。これを応用すると、顧客は自身の身元を特定されないまま、ネット上にある商品の購入が可能になる。

ただし、現在の匿名認証システムは、多くの問題点を抱えている。具体的には各種の匿名認証方式において、

·署名作成までにかかる手間が煩雑で現実的ではない

·検証時において、取り扱うパラメータが多く、伝送量が飛躍的に増大する

などの課題があり、未だに実用化に適した決定的な方式は提案されていない。また、実ネットワークに対する匿名認証方式の安全性についても、十分な解析・評価はなされていない。

(2) CAPTCHA

匿名認証の要素技術として利用するため、CAPTCHA の研究についても従事した。2 者間の対話において、回答者が人間であるか、あるいは人工知能による自動プログラム（通例「ロボット」と称される）であるかを判別するテストは「人間ロボット判別テスト」と呼ばれている。このテストは、今日のネット上において個人認証手続きで多用されている。その目的は、パスワード認証に対する総当たり攻撃や、アカウントの大量生成、多重投票といった不正を目的とするロボットが、短時間に大量にアクセスできないようにするためである。人間ロボット判別テストでは一般に、人間には容易に解けるが、現在のロボットでは解くことが難しい AI (Artificial Intelligence、人工知能) 問題を用いる。

このようなテストの代表例として、歪んだ文字画像を読み取らせる CAPTCHA (Completely Automated Public Turing Test To Tell Computers and Humans Apart) [2] がある。サーバ(計算機)は歪曲やノイズが付加された文字列の画像を作り、利用者にその文字列を判読させ回答させる。これは、人間の画像認識能力が現状のロボットより上回っているという仮定に基づく。また、視覚障害者向け認証システムとして、変形した音声を利用者に聞き取らせる方式もある。

本研究で取り組む問題は、既存の人間ロボット判別テストの多くが、特定の知覚チャンネルに限定して作られているため、その知覚に障害がある利用者の障壁になっている点である。知覚チャンネル依存という問題点を解消し、知覚障害によらず誰でも利用できる人間ロボット判別テストの作成手法の確立が求められる。

２．研究の目的

(1) 匿名認証

本研究では、「ペアリング」と呼ばれる双線形写像を用いることにより、個人情報を外部に漏らすことなく安全な認証処理を実現できる匿名認証の基盤技術構築を目的とする。ペアリングとは双線形写像 $e:G1\times G2\to GT$ を満たす非退化な一方向写像であり、$e(aP,Q)=e(P,aQ)=e(P,Q)^a$ という性質を持つ。ここで、$G1,G2,GT$ は同じ位数を持つ群, a は整数, $P\in G1,Q\in G2$ である。また、現在の計算機環境に適した匿名認証システムを構築し、性能評価実験を行う。このような取り組みにより、電子商取引、電子投票、電子アンケートなど、高い匿名性が求められるシステムにおいて、利用者の個人情報を開示することなく、安全に運用できる匿名認証方式の実現を目指す。

本研究では、実社会において安全かつ実用的な匿名認証基盤を構築し、前述の問題点を解決することを目的とする。このために、解決するためのアプローチとして、

·既存の匿名署名に対し、手間がかからず、伝送効率のよい方式を提案する

·従来は持っていなかった有益な特徴を持つ匿名署名を提案する

などの取り組みを行う。

現在はある特殊な楕円曲線上のペアリングが主に使われているが、この関数の一方向性が危殆化したときのことを考慮し、新たな双線形写像についても検討を行う。候補の一つとなるものは、超楕円曲線上の双線形写像であり、攻撃のアプローチが従来と異なると

共にステップ数が通常の楕円曲線ペアリングよりも少なくなる可能性がある。ただし、1 ステップの演算量が楕円曲線上の演算よりも大きいため、これを小さくする工夫が必要になる。

また、汎用端末や携帯電話によるシステムの実装・性能評価についても取り組むことにより、副次的な結果として、ペアリング暗号系の有効性についても検証する。特に、ペアリングの型や暗号プロトコルの違いによって生じる実装上の特性や問題点を考察し、明確にしていく。

(2) CAPTCHA

本研究では、人間ロボット判別テストの有益な構成手法の確立を目的とする。本研究では、バリアフリー要件を満たすため、文意文脈解釈問題を用いる。さらに、知識非依存性要件を満たすため、人間が作った文と機械が生成した文との間で人間が感じる違和感を利用した方式に着目する。しかしながら、不自然な文の識別問題は、識別性要件と問題新規性要件の達成が課題となる。

本研究では、この問題を解決するため、階数 N の大きいマルコフ連鎖から生成される機械合成文を、自然な文として扱うことを検討する。

３．研究の方法

(1) 匿名認証

・理論的研究：既存の匿名認証方式の問題点と有益性を解析する。このとき、楕円曲線理論から派生可能な暗号関数を導出し、匿名認証への適用可能性を考察する。また、使用する楕円曲線のパラメータ等を変えることにより、有益な匿名性を持たせることができないか検討する。

・アルゴリズムの実装：匿名認証を行う演算処理について、新しいアルゴリズムを提案する。得られたアルゴリズムに対し、汎用計算機や開発用ソフトウェアを用いて実装し、多面的な評価を行う。アルゴリズムの高速化についても、この枠組みで十分な検討を行う。高速なアルゴリズムを実現するための主な取り組みについては、アルゴリズムで用いる演算に対し、(a)演算の種類を削除する、(b)演算の計算量を削減する、という 2 種類のアプローチで考察を行う。

・プロトコルの研究：最初に、共通要素的なプロトコルを利用して、現在使われている多くの代表的暗号プロトコルに対し、ペアリングを用いたプロトコルへの置き換えを検討する。SSL への応用はその候補のひとつで、その中に含まれている暗号プロトコル部分をペアリングのプロトコルに置き換えて評価を行う。これにより、実用面において、相互通信の回数や帯域、メモリなどの大幅減少が見込めるため、どの程度の削減か定量的に評価する。次にプロトコルを実用化する際に重要な役割を果たす電子決済サービスへの適用など、従来の匿名認証の更なる高機能化を目指す。

・統合化システムの構築

これまでの成果をまとめて、一つのシステムに統合化する。また、得られた成果に対する総合的な評価を行い、必要に応じてシステムの改良を行う。実用システムの実現は、実社会で求められる匿名認証の解決手段、またはその普及のためにも重要であると考え、重点的に取り組む。

(2) CAPTCHA

2 者間 N 階ワードサラダは、素材文章から抜き出された N-gram の形態素で構成される。従って、階数 N が大きければ、小さい場合に比べて、人間には自然な文と認識されやすい。一方で、ワードサラダを自然な文として利用するには、単に N を大きくするだけでは解決しない。N=5 における連鎖する形態素の平均パタン数は、ほぼ 1.0 である。つまり、これらの素材文章から 5 階ワードサラダを生成すると、単に素材文章の一部が切り出される確率が高い。攻撃者は、検索結果から問題に回答できてしまう。対策として、階数を小さくしていくことで、連鎖する形態素の平均パタン数を増やし、素材文章に存在しない文字列を、新規文として生成できる。しかしながら回数が小さくなりすぎると、人間は、不自然な文と識別できなくなるため実験などにより適切なパラメータを模索する。また、連鎖する形態素の平均パタン数は、N=3,4 でも 1.0 近くに収束するので、適切な階数調整ができない可能性がある。

階数による文の自然さの調整は、別な問題もある。例えば、1 階ワードサラダを不自然な文とし、4 階ワードサラダを自然な文とする。これらのワードサラダをウェブ検索すると、使用した文章源が検索結果に現れる頻度は、後者の方が高いと推測される。提案方式や実験においてはこれらの点を十分考慮する必要がある。

４．研究成果

(1) 匿名認証

本研究では、送信者に認証機能を付加したブロードキャスト暗号方式を提案した。提案方式は、BGW 方式と署名を単純に組み合わせるのではなく、暗号化の際に送信者の秘密鍵を明示的に利用する。また、ユーザ秘密鍵のサイズとヘッダのサイズのいずれも固定サイズであり、ユーザ数に影響されない。また送信者の本人認証を行うため、BGW 方式をそのまま使用する場合より、ユーザは暗号化されたデータに対して信頼を持つことができる。特に、暗号化されたデータがコンピュータウイルスである場合など、ユーザが復号後に被害をこうむる可能性を考慮すると、送信元確認の重要性が大きい。詳細なプロトコルについては、紙面の制約のため省略し、ここでは提案方式の性能評価について記載する。

・秘密鍵のサイズ：提案方式では、BGW 方式と同様に、ユーザの秘密鍵は $G1$ の元 1 個

分である。全体的なサイズは全ユーザ数 N に影響されず、固定サイズとなる。BGW 方式と既存署名方式を組み合わせると、それぞれの秘密鍵が必要となるため、サイズが比較的大きくなる。

・ヘッダのサイズ：提案方式のヘッダは $G1 \times G1 \times Zq \times Zq$ の元である。全体的なサイズは、全ユーザ数 N と送信者が選択したユーザ数 s のいずれにも影響されず、固定サイズとなる。

・公開情報のサイズ：公開情報のサイズ BGW 方式は公開情報のサイズが $G1$ の元 $2N+1$ 個分であるのに対し、提案方式は $3N$ 個分である。すなわち、提案方式は BGW 方式と比較して約 1.5 倍の情報公開が必要であり、全ユーザ数 N に比例する。しかし，BGW 方式と既存署名方式を組み合わせると、それぞれの公開鍵が必要となるため、提案方式よりサイズが大きくなる。

また、提案方式を応用し、1-out-of-n 署名と検証者指定署名の両機能を持った署名方式を提案した。さらに、署名のサイズが参加者の数 n に依存しないことを示した。提案方式は、署名者の指定したユーザのみが署名者の所属を特定可能であり、署名者個人の特定は困難である。この特徴は、アンケートや内部告発など、署名者の匿名性と検証者の限定が求められるシステムに有効であると考えられる。

(3) CAPTCHA

Google ウェブ検索を用いて、実験用プログラムが生成したワードサラダの検索結果を評価した。評価値は、「-1：文章源が第一候補として検出された」、「0：文章源は第二候補以降だが、最初のページに検出された」、「1：文章源は特定されない、または第二ページ以降で検出された」とした。また、等分散を仮定した有意水準 5% の t 検定結果というように定量的な実験結果を得た。

次に使用した素材文章から生成したワードサラダについて、再現性を確認した。1 階ワードサラダと[2,3], [2,4]階ワードサラダの検索結果に有意性はないが、文章源が特定される場合が見受けられた。文章源を特定できれば、攻撃者はその形態素 N-gram の分布を調査し、回答のヒントになってしまい、安全性が低下する。この対策として、複数種類の文書をまとめて素材文章とした結果を得た。1 階ワードサラダと[2,4] 階ワードサラダの検索結果に有意性はなく、かつ文章源の特定確率も 10%以下となった。文章源が特定されるようなワードサラダについては、事前にフィルタリングし、作問には使用しない。N=1,[2,4]と N=4 の検索結果が異なることから、複数階数を用いたワードサラダ生成法の有用性がわかった。また、N=[2,4]と N =[2,3], [3,4]では、前者の方が N=1 の結果に近いことから、品詞・活用形を用いたマルコフ連鎖の効果も確認できた。多様な素材文章からワードサラダを生成しても、結果が変わらないため、提案手法は十分な識別要件を満たす。

問題文としての新規性の評価には、生成されるワードサラダが過去に生成されたものと一致しないことを確認した。結果として、文章源が特定される作問に不向きなワードサラダの生成確率は 10 % である。生成したワードサラダの 90 %が問題文として使用できるため、提案手法は、問題新規性要件を満たすと考えられる。

また、セキュリティ技術の特定知覚への依存の問題を取り上げ、代表例である人間ロボット判別テストでの要件を論じ、文意文脈解釈問題による実現の問題点を指摘した。提案方式は、複数階数による形態素のマルコフ連鎖モデルと、品詞・活用形によるマルコフ連鎖モデルを生成する。本モデルを用いることで、人間には比較的自然な文でありながら、新規性が高く検索による攻撃に耐性のあるワードサラダが生成できる。また、各種実験を通して、提案手法の有用性を示した。

<引用文献>

① R.Rivest, A.Shamir and Y.Tauman: How to leak a secret, Proceeding of Asiacrypt, Lecture Notes in Computer Science (LNCS) 2248, Springer, pp.552-565, 2001.

② The official captcha site, http://www.captcha.net/.

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 4 件）

① 山口通智, 岡本健, 菊池浩明：機械合成文の不自然度相対識別問題に基づく CAPTCHA の提案, 情報処理学会論文誌, Vol.56, No.9, pp.1834-1845, 2015.

② M.Yamaguchi, T.Okamoto and H.Kikuchi: CAPTCHA System by Differentiating the Awkwardness of Objects, In Proceedings of International Conference on Network-Based Information Systems (NBiS2015), Publisher IEEE, pp.257-263, 2015.

③ M.Yamaguchi, T.Nakata, H.Watanabe, T.Okamoto and H.Kikuchi: Vulnerability of the Conventional Accessible CAPTCHA used by the White House and an Alternative Approach for Visually Impaired People, In Proceedings of IEEE International Conference on Systems, Man, and Cybernetics (SMC2014), pp.3946-3951,

2014.

④ M.Yamaguchi, T.Nakata, T.Okamoto and H. Kikuchi: An Accessible CAPTCHA system for People with Visual Disability − Generation of Human/Computer Distinguish Test with Documents on the Net, In Proceedings of 16th International Conference on Human-Computer Interaction (HCII2014) , Lecture Notes in Computer Science (LNCS) 8516, Springer, pp.119-130, 2014.

〔学会発表〕（計 5 件）

① 山口通智, 岡本健, 菊池浩明：不自然さの識別問題を用いた CAPTCHA に関する研究, 第 29 回情報通信システムセキュリティ(ICSS)研究会, 信学技報, Vol.114, No. 489, ICSS2014-72, pp.55-60, 電子情報通信学会, 2015.

② 山口通智, 岡本健：人間ロボット判別テストのバリアフリー化のための言語的作問とその自然文生成技法, コンピュータセキュリティシンポジウム (CSS2013) , pp.941-948, 3D3-3, 情報処理学会, 2013.

③ 山口通智, 中田亨, 岡本健：ユーザ認証での画像視認テストを代替する言語的テスト, 感覚代行シンポジウム 2013, No.4, 2013.

④ 山口通智, 中田亨, 岡本健：インターネット上に湧出する文章の特徴とそのチューリングテストのバリアフリー化への利用, 情報科学技術フォーラム(FIT2013), 第 3 分冊, pp.669-670, K-049, 情報処理学会, 2013.

⑤ 山口通智, 左瑞麟, 岡本健, 岡本栄司：署名者の追加が容易な k-out-of-n リング署名, Symposium on Cryptography and Information Security (SCIS2013), 2A2-4, 2013.

６．研究組織

(1)研究代表者

岡本 健（OKAMOTO, Takeshi）
筑波技術大学・保健科学部・准教授
研究者番号：00349797