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　３０　年　　８　月　２９　日現在

機関番号：　１７１０２
研究種目：　基盤研究(B)（一般）
研究期間：　2015～2017
課題番号：　１５Ｈ０２７１１

研究課題名（和文）分権管理型暗号認証基盤の構築と応用システムの設計と解析

研究課題名（英文）Decentralized cryptographic infrastructure: Design and Analysis of Applied Systems

研究代表者

櫻井　幸一（SAKURAI, KOUICHI）

九州大学・システム情報科学研究院・教授

研究者番号：６０２６４０６６

交付決定額（研究期間全体）：（直接経費）　　14,200,000円

研究成果の概要（和文）：(1)ビットコインに対する攻撃を解析し、その成果はジャーナル論文IEEE TRANS ON INFORMATION FORENSICS AND SECURITY に掲載された。
(2)RSA暗号の公開鍵へID情報を埋め込む手法を応用した分権暗号基盤の設計を精密化し、その安全性の数学的な解析を与えた。この成果はJournal of Information Security and Applicationsへ投稿した。
(3)ブロックチェーンに関するワークショップを ACM AsiaCCS2017(オスロ)付随会議として立ち上げた。。第2回をAsiaCCS2018(韓国・6月)で開催した。

研究成果の概要（英文）：（1）Our main contribution is now published in IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY as "Bitcoin Block Withholding Attack: Analysis and Mitigation",
(2) We design a decentralized Public-Key Infrastructure by using Identity-Embedding Method with RSA,and investigate the mathematical proof on its security. This contribution is now submitted to Journal of Information Security and Applications
(3) We have set up Workshop on Blockchain, Cryptocurrencies and Contracts associated with ACM AsiaCCS. The 1st (2017) was held in Oslo(Norway), and the 2nd (2018) in Inchon(Korea) .

研究分野：　サイバーセキュリティ

キーワード：　仮想通貨　暗号　認証　分散計算　IDベース暗号　ビットコイン　ブロックチェーン　グラフ問題

１．研究開始当初の背景

[1]学術的背景

インターネット上の新しい仮想通貨ビットコインが注目されている。2014 年２月には、ビットコインの取引を行うマウントゴックスの破綻で、一躍有名になったことは記憶に新しい。

暗号技術を用いた電子現金は、1990 年代に盛んに研究された。暗号学者 D.Chaum は、ブラインド署名(1982)と呼ばれる RSA 暗号を利用した匿名化技術を開発し、電子媒体の２重コピー防止に成功し独自の電子現金システムを設計、自らベンチャー会社 DigiCash(1990)も創業した。以降多くの電子現金は匿名性を重視し、ブラインド署名による２重コピー防止技術を踏襲している。NTT の暗号研究者・岡本と太田が設計したユニバーサル電子現金(CRYPTO’91)は、公開鍵暗号技術を駆使し分割可能性など多機能な、もっと現金に近い方式といわれ、日本銀行と NTT が試作システム開発とパイロット試行も展開した(1998 年)。

これらの電子現金に利用される暗号技術は、公開鍵認証基盤に基づく中央管理型であった。秘密分散技術などをつかって、管理する中央機関を分割する分散型も研究開発され、その必要性から基盤となる暗号技術とその理論は、1990 年代飛躍的に進歩した。

ここでいう現金とは、日本銀行券に相当する紙幣・貨幣で、政府や信頼できる機関が管理・発行するものをいう。これに対して、ビットコインは、紙幣ではなく、金（Gold 金塊）をモデル化していることが、従来の電子現金と大きく異なる。ビットコインは以下のような実在の金と同等の性質を有する：a)埋蔵量には限りがあり、発掘する必要がある。b)その価値は、相場に依存し変動する c)匿名である d) 分割できる。 さらにビットコインの場合は、電子通貨なので、インターネットで取引が可能であり、政府が管理しないため、実質の国境がない。

従来の電子現金と異なりビットコインには、特権のある管理者は存在せず、参加者(ユーザー）がお互い/全員を相互監視するシステムを、P2P 型ネットワークで実現している。この分権(decentralized)管理型のセキュリティ基盤は、PKI 以前の PGP(Pretty Good Privacy)暗号システムが起源にあるが、この誰もがコインの発行者になれ、特定の管理者を仮定しないとことが、ビットコインの普及を大きく成功させることになる。

[海外の研究動向]　ビットコイン自体は、既存の P2P 型ネットワークとハッシュ連鎖を使用したよく知られた暗号技術であるが、その急速な普及・成功により、それまでは論文・試作レベルであった参加者全員が民主的に管理する分権型(decentralized)システムが再注目されることとなる。

ビットコインに刺激されて、ビットコインのそのものの安全性やプライバシーの研究や、ビットコインの変形・亜種の提案などが、海外を中心にはじまっている。著名な暗号学者 Adi Shamir などが率先して、ビットコインに関する研究論文を発表し、また多くの学者らが、P2P 型インフラサービスの研究に注目しはじめている。伝統ある WEIS(Workshop of Economics and Information Security) での研究論文の発表も活発であり、暗号経済国際会議 Financial Crypto ではビットコインに特化したワークショップが 2014 年からはじまり 10 件の査読付き講演、パネル討論やポスター発表が行われている。

[国内の研究状況]ビットコインに刺激されて、仮想貨幣(Virtual money)や暗号通貨(Crypto-Currency)の啓発書や解説論文は登場している。しかし、日本国内での学術研究発表は、きわめてすくないのが現状である。(IACR-ePrint ビットコイン関係論文：2013 年 8 件、2014 年 10 月末当時 12 件、しかし日本人著者は無.)

[研究代表者のグループ]　研究代表者は、鍵供託（key-escrow）のないIDベース暗号の開発のため、2012年からLenstraのRSA 法への情報埋め込みアルゴリズムに着目し、研究をはじめてきた[A Method for Embedding Secret Key Information in RSA Public Key and Its Application″, 6th International Workshop on Advances in Information Security (IMIS2012)]。提案した公開鍵認証基盤システムを、既存のPKIと比較し、電子選挙などのプライバシー保護機能を有することも発見し[電子現金プロトコルを用いた著作権管理システムの提案, コンピュータセキュリティシンポジウム(CSS2013)3D2-3]、さらに著作権保護システムの構築へと応用した[RSA 暗号の公開鍵への所有者情報埋め込み手法と その著作権管理システムへの応用, 第65回 Computer Security Group (CSEC) 研究発表会 No.3, 2014]。現時点では、その設計した基盤を、分権型個人情報管理方式として抽出し、理論的安全性を解析しているところである[分散型アイデンティティ管理スキームとその RSA 及び 離散対数系暗号による実現, コンピュータセキュリティシンポジウム (CSS2014) 3E2-1]。

[3]学術的特色・独創性:

研究代表者の動機は、ID（個人情報）ベース型暗号にある、ただし現在主流の楕円ペアリング暗号を利用したものではない。RSA 暗号の法(modulus)に ID 情報を埋め込む Lenstra アルゴリズムの改良や解析は、研究代表者による実験[Sak2013b]や、数理学者によっても研究されている[X.Meng “On RSA moduli with half of the bits prescribed” J. Number Theory,133(1),2013.]。しかし、暗号システムへの応用は、10 年前の Lai らの研究[CS Laih and KY Chen. Generating visible RSA public keys for pki. International Journal of Information Security, 2(2), 2004]が唯一であり継承する研究がなかった。学術的には、埋め込み情報の一意化問題の解決や理論的安全性証明が、暗号理論の観点から興味深い。さらに、RSA 暗号以外への公開鍵暗号系にも、類似の ID 埋め込みが可能かは、暗号理論における未解決の重要課題であり挑戦課題の１つでもある。

２．研究の目的

本研究では、ビットコインのように参加者全員が分権管理できる独自の暗号認証基盤を設計し、公開鍵暗号基盤(PKI)に代表される中央管理型認証基盤との比較を行い、その長短所を明らかにする。また、設計した分権基盤上に、著作権保護システムの構築をはじめ、新たな流通サービスを提供する応用システムを提案し、その安全性や性能解析を行う。具体的には、研究代表者が取り組んできた鍵供託問題を解決すべく導入した RSA 公開鍵暗号の法(modulus)に個人 ID 情報を埋め込む認証基盤を土台として、ID 情報の一意性や公開鍵の単一保有(retention)など未解決課題の解決をめざす。また、従来から信頼できる第

三者機関を前提としている暗号システムや応用サービスを、分権管理型基盤上に（再）構築可能か、可能な場合には実装評価も行い、分権管理型基盤の利点と限界を解明する。

３．研究の方法

暗号・プライバシー・ネットワークセキュリティの専門家により混合研究グループを組織し、本課題に取り組む。これまでの２年間の準備研究と成果をもって、本申請研究期間は３年間とした。　研究代表者が設計している RSA 法への ID 埋め込みを利用した認証基盤とその上に構築した著作権管理システムを基に、既存方式の脆弱性解析、解析成果を意識した改良と再評価、類似関連研究との比較評価や最新研究成果の取り込みを行った。る。試みとしては[FVY2014]の手法を我々の提案に適用可能か、がまずあげられる。

４．研究成果

主要な成果を列挙する。

4A.国際会議で発表していた分権暗号認証の発展研究を Journal of Information Security and Applications へ投稿し、採録のための査読条件に、分担者の穴田が中心となり、加筆修正を行った。安全性の証明に関する素数分布の数学的な補題を中心に、国際会議版に加筆を行った。

----国際会議版(InTrust2014)-----

国際会議版"Identity-Embedding Method for Decentralized Public-Key Infrastructure"(in the proceedings of Trusted Systems - 6th International Conference,INTRUST 2014)で本報告者らは,RSA 暗号の公開鍵へアイデンティティ情報を埋め込む手法を提案した。

現在、公開鍵の信頼を形成する手法の主流は「階層型公開鍵基盤」であり、ITU-T が X.509 として規格化し広く利用されている。典型的な例はルート認証局による公開鍵信頼保証に基づく S/MIME 暗号化メールである。しかしながら、分散型台帳のブロックチェーン技術が世界的に研究開発されている現在、公開鍵信頼形成も分散型の技術が見直されるべきであると本報告者らは考えている。

1990 年代に提案され 2010 年頃までに掛けて（細々と）開発されてきた PGP (Pretty Good Privacy)は、WoT(Web-of-Trust)による分散型公開鍵信頼形成の技術である。

本報告者らによる上記の提案手法では，WoT で信頼形成に用いられているデジタル署名よりもデータ長が短く，ただしチャレンジ&レスポンスのインタラクションを必要とする認証手法を提案した。

提案手法は，RSA 暗号の公開鍵の一部である法 N に(1)公開鍵所有者のアイデンティティストリング　(2)公開鍵の保証人のアイデンティティストリング　(3)楕円曲線暗号の公開鍵 P、の三つのデータを埋め込むものである。ただし，RSA 暗号の法 N の素因数 p と公開鍵 P を関係：

x = [p mod p_0], ・・・①

P = g^(1/x),

により対応付ける（p_0 及び g は楕円曲線暗号の公開パラメータ）。また，法 N へのデータの埋め込みは Lenstra のアルゴリズム（ASIACRYPT'98）を用いる。加えて，国際会議版では法 N のビット長が 2048 ビットや 3072 ビットの具体的な値の場合に埋め込み可能なデータ長を提示した。

--- (Journal of Information Security and Applications, "Revision requested")

ジャーナル投稿版の新規差分（貢献）は次の３点である。

A) 楕円曲線暗号の秘密鍵 x の導出（式①）における x の確率分布の正当性証明

B) 鍵生成の計算機実装評価

C) ブロックチェーン技術への適用の提案

A)は、楕円曲線暗号では秘密鍵が鍵空間から一様ランダムにサンプリングされるべきところ，提案手法の導出でも確かにそうなっていることを示したものである。ディリクレの算術級数の素数定理をベースに数学的証明を与えた。

B)は，RSA 暗号の法 N へのデータ埋め込みを、提案手法のケースにおいて計算機実装し，鍵生成に要する時間を評価したものである。結果、2048 ビットでは 0.10 秒程度、3072 ビットでは 0.45 秒程度,7680 ビットでも 14.80 秒程度と、現実的な時間で鍵生成可能であることを説明した。また，2048 ビットの場合に埋め込みの事例を具体的なビット列で示した。

C)は，ここ数年の「ブロックチェーンの分類」で論じられているところの"consortium"かつ"trusted"タイプに対し、提案手法を適用する可能性を論じたものである。公開鍵の保証人として"consortium"の代表者らを充当することで、分散型信頼形成が可能であることを主張した。

4B.ビットコインの安全性評価、および改良と解析

4B-1) ビットコイン・マイニングにおける追加報酬を用いたブロック保留攻撃を考察した。これは利己的マナーが、1 つのプールが他を攻撃 し、報酬を得るというものである。我々は、いくつかの異なるシナリオの下での戦略において、利己マイナーが得る金銭報酬の量的 解析を行い、攻撃者が最大の利益を得るいくつかの条件と戦略を明らかにした。

4B-2)マイニングの作業証明には、一方向性ハッシュ関数に関する計算困難な問題が利用されている。ビットコインの安全性の観点から、マイニングを複数回行った時に要する時間の分散は小さいほうが望ましい. しかし、ハッシュ関数を利用しているビットコインは、この計算時間の分散が大きいという課題がある。我々は、この課題を解決すべく、計算問題をグラフクリーク探索に置き換えた新しい方式 を提案した。ハッシュ関数を利用する原方式との理論比較を行い、確かに分散が小さくなるという優位性を、計算機実験においても検証した。

4B-3) もう一つの改良として、マイニングの作業証明自体を、回収可能性(Retrievability)の証明に置き換える方式の改良も行った。このアイデアを利用したビットコインの改良として、Permacoin がすでに提案されている。我々は、このデータ管理法に局所化を導入するこ とで、記憶容量やネットワーク通信負荷の面で、Permacoin よりも、すぐれた性能を達成できることを理論的に解析した。

4C) ビットコインに対する攻撃を解析し、2015 年と 2016 年に発表した国際会議論文(特任助教の BAG, インド統計研究所の Ruj との共同研究)を発展させた ジャーナル論文"Bitcoin Block Withholding Attack:

Analysis and Mitigation″ が 、 IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY に掲載され た(2017 年 8 月)。
---この IEEE Trans 論文の概要----
ここでは、2 つの問題に取り組んだ。: まず、Bitcoin におけるブロック保留 (BWH) 攻撃の変形を研究し、次に Bitcoin における既存の BWH 攻撃のすべてを防ぐ対策案を提案する。一般に、あるプールと結びついている別のプールを攻撃し、後者を攻撃するために元の採掘プールから報酬を受け取る、利己的な Bitcoin 採掘者の戦略を解析する。この攻撃を「スポンサードブロック源泉徴収攻撃」と名付けた。本研究では、この戦略を異なるシナリオで適用することで、利己的な採掘者が得ることができる金銭的インセンティブの定量的分析を行った。特定の状況下では、攻撃者はいくつかの戦略を採用し、計算能力を効果的に利用することで収益を最大化できることを証明した。また、攻撃者がより多くのインセンティブを獲得すべく両方のプールを攻撃するために、この戦略を使用する危険性があることも示した。
さらに重要な考察として、マイニングプールでの源泉徴収攻撃を効果的に阻止できる戦略も明らかにした。

4D. 穴田 啓晃, 松島 智洋, 川本 淳平, バグ・サミラン, 櫻井幸一: ″スケーラブルなプルーフ・オブ・ワークのためのグラーフクリー ク・マイニングの分散の解析″, (2017 年暗号と情報セキュリティシンポジウム)で、Bitcoin において重要な計算困難問題のインスタ ンスの解を競争的に探索するステップ, いわゆる″マイニング″についてその統計的性質を調査・解析した.結果, マイニングの時間が 統計的には指数分布に従うという事実を確認した.更に, 研究代表者らの仕事で提案された″グラフクリーク・マイニング″に着目し, 計算機実験を行った.結果, マイニングの時間の分散が小さくなる傾向を確認した.これにより, マイニングの時間の分散を制御可能であるとの見通しを得た.

副産物：国際連携・共同研究
Bag は、九大工学部の国際共同研究基金の支援を受けて、以前から JST 国際共同研究でも交流実績のあるインド統計研究所から１年間のポスドクとして招聘できた。短期間であったが、仮想通貨に関する本プロジェクトのテーマに興味を示し、国際会議２件と IEEE Trans.ジャーナルを発表する成果を得た。（その後、英国・New Castle 大の助教に移籍し、現在に至る。）

1st ACM Workshop on Blockchain, Cryptocurrencies and Contracts (BCC'17)
JSPS 日印交流で研究実績のあるインド統計研究所 Sushimita Ruj と、ブロックチェーンに関する国際ワークショップを検討していたが、本研究活動の一環として、AsiaCCS2017(New York 大・アブダビ校)との連携開催の運びとなり発足させた。AsiaCCS は、下名も数年前から Steering 委員の一員として参画し、2014 年には NICT の協力を持って京都で開催した。New York 大・アブダビ校では、準備として、１年前の 2016 年４月に、諮問委員会を招待した Security Cyber Workshop を開催しており、下名を含む、招待された８名が講演を行っていた。
1st BCC のワークショップ長として、Ruj と下名、それにマイクロソフトバンガロール研究所の Satya LOKAM の３名で対応した。LOKAM は、Ruj が学生時代にインターンシップの指導を受けた間柄ということで、今回紹介を受けた。
BCC は初回かつ、FC2018 や IEEE Euro S&P でもブロックチェーンワーク新設と時期的に重なったということもあって、投稿総数は 17 件、採択は１件のみ、加えて２件を short で採択した。招待講演は、マイクロソフト側の支援を受けて２件、また、パネル討論を行う予定。さらに AsiaCCS 本会議では、NEC 欧州研究所から、Dr.Karame が、チュートリアル講演 On the Security of PoW-based Blockchains Ghassan Karame (NEC) and Alexandra Dmitrienko (ETH, Switzerland) を行なった。

2nd ACM Workshop on Blockchain, Cryptocurrencies and Contracts (BCC'18)
6 月に韓国・仁川で開催されたばかりであり、ここに報告しておく。
2017 年からの開催であり今年で２回目、プログラム委員長は前回と同じく、Ruj と下名、それにマイクロソフトバンガロール研究所の Satya LOKAM の３名で対応した。投稿件数 21 件、うち採択が７件となった。また招待講演１つを企画できた。昨年度は、投稿件数は 17 件、採択は１件のみ、加えて２件を short で採択あったことを考えると、投稿数は確実に伸びて、投稿論文の質も上がってきたと言える。2019 年の AsiaCCS は、ニュージーランドがホストすることが内定しており、BCC ワークショップも継続して連携開催を計画している。

その他の国際会議：欧州の ESORICS にも参加し、初回となる Workshop on Cryptocurrencies and Blockchain Technology に参加し、情報収集と研究交流を行った。12 月には、インド統計研究所で開催されたブロックチェーンワークショップに参加した。これは、マイロソフト（バンガロール研究所）の支援を受けて、博士以上の若手研究者２０名以上が、参加助成を受けての研究集会であった。米国などからは、ビデオと skype の併用発表、インド政府やベンガル地区３人の IT 系役人を招いてのパネル討論など、充実していた。インド以外からは、ベルギーの Preneel 教授と代表者の２人の発表であった。また、IEEE では、ブロックチェーン単独の会議がはじまった：2018 IEEE International Conference on Blockchain, Helifax, Canada, July 30-August 03, 2018.日本からは、下名が唯一、プログラム委員として参画したが、１８０件以上の投稿があり、この分野の劇的な研究者の増加が明らかとなった。

現状と今後の課題
本研究では、ビットコインやブロックチェーンの登場に刺激され、新たな暗号認証基盤の構築を研究した。しかし、この数年間で、暗号通貨に関する社会の状況が激変した。ビットコインを合法化する国が増え、類似の暗号通貨も数千種以上提案されている。利便性だけでなく、安全性や匿名性の強化をうたった方式も多い。しかし、多くは、提案・実装者による自己評価/ホワイトペーパーに留まっている。逆に、ビットコインに関しては、その採掘検証計算過程の遅延が原因となって、当初から危惧されていたハードフォーク問題が現実となり、分裂騒動が絶えないが、利

用者間の合意と暫定的なシステム対応とで、なんとか乗り切っている現状にある。この現状を踏まえると、新規提案よりも、既存提案の安全性や匿名性評価を、客観的に与えることが、社会的にも重要と考える。
その一方で、量子計算機の登場を前提にした、耐量子暗号の研究が急激に進む中、暗号通貨の長期利用や耐量子性の解析が、ほとんど議論されていないことを踏まえて、耐量子暗号通貨の設計と安全性評価も課題である。
[国内外の研究動向] 国内では学術研究よりも、金融機関を中心に仮想通貨のビジネス展開やコンソシームが先行している。海外では、ACMやIEEEの主要セキュリティ会議の併設ワークショップという形で研究集会が形成されはじめた。大学の暗号研究者も、金融関係からの支援を受け、仮想通貨の研究 projectを開始、成果がでた学者は、国際会議で積極的に発表している。しかし、安全性の解析は、学会レベルでも検討が始まっているが、徹底した議論ができている状況ではない[Zhang-Preneel,CoNEXT17]。
分散計算や多者間計算は、暗号理論においても活発に研究されてきた。しかし、ビットコインはP2P型計算であり、参加者数が、数千から数万人、中には、上限のない仮想通貨を目指すものもあり、分散暗号として、新たなアプローチが必要とされるため、今後の課題である。
長期利用可能署名や耐量子暗号は、暗号原理や暗号メカニズムとしては、研究されてきた。しかし、これらを仮想通貨にまで適用する試みはまだなく、挑戦課題である。

最後にブロックチェーンのデータ検索に関する最新動向を述べて(研究分担のフォンによる調査)、さらなる設計と実装は今後の課題としておく。
ブロックチェーン技術は、ビットコインを始めとしてサプライチェーン[1]など、幅広く応用され始めた。しかし、これらの応用では、処理されるレコードが多くて、オリジナルのブロックチェーン技術はスケーラビリティが足りない問題がある[2]。具体的に言えば、多くのアプリケーションでは、Bitcoin のように分散されたものを使用できるが、大量の任意のデータを短時間で、不変に、低遅延で格納することができない。例えば、クレジットカードVISAは秒ごとに4,000～6,000トランザクションの処理能力を持っているに対して、ビットコインは秒ごとに7トランザクションしか処理できない[3]。
BigchainDB はスケーラブルなブロックチェーンデータベースで、分散化、不変性、アセットの作成と転送のための API (組み込みサポート) を含むブロックチェーン特性を持ったビッグデータデータベースである。言い換えると、BigchainDBは、1秒あたり数百万トランザクションを処理可能である大規模なデータベースを土台に、分散化、不変性、アセット作成と転送などのブロックチェーン特性を追加したものである。すなわち、BigchainDBは分散型RDBMSとブロックチェーンのよいとこどりをしたスケーラブルな分散型ブロックチェーンデータベースで、ブロックチェーンデータをRDBMS形式で提供できる[4, 5]。
BigchainDBには一般的なRDB (Relational Database System) の「テーブル」のような概念はなく、「トランザクション」という単位 (RDB でいう「レコード」のような単位) でデータを追加していく。従って、ユーザーの情報や経歴の情報などは全て「トランザクション」で扱われる。この「トランザクション」には、こちらで指定したデータを入れることができるため、「デジタルアセット」という側面も持っている。 また、その「トランザクション」(デジタルアセット) の所有権を保持しているユーザーであれば「トランザクション」の ID を知ることができ、中身を参照できる。しかし、十分にデータの改ざんが困難になったといえる。
参考URL
[1]
https://www.ibm.com/blockchain/supply-chain/
[2]
https://blockchainexe.com/blockchain_problem/
[3]https://blockchainexe.com/whitepaper1/
[4]
http://gaiax-blockchain.com/bigchaindb
[5]https://www.ossnews.jp/oss_info/article.html?oid=7594

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)［全て査読有り］

1. Samiran BAG, Sushmita RUJ and Kouichi SAKURAI “Bitcoin Block Withholding Attack: Analysis and Mitigation,” IEEE Transactions on Information Forensics and Security 2017, pp. 1967 - 1978
2. Samiran BAG, Kouichi SAKURAI “Yet Another Note on Block Withholding Attack on Bitcoin Mining Pools” Proc. Information Security - 19th International Conference, ISC 2016, Honolulu, HI, USA, September 3-6, 2016, Lecture Notes in Computer Sciences, Springer 9866, pp. 167-180, Springer 2016
3. Binanda Sengupta, Samiran Bag, Sushmita Ruj, Kouichi Sakurai “Retricoin: Bitcoin based on compact proofs of retrievability” Proceedings of the 17th International Conference on Distributed Computing and Networking (ICDCN2016), Singapore, January 4-7, ACM 2016. 14:1-14:10.
4. Samiran BAG, Sushmita RUJ and Kouichi SAKURAI “On the Application of Clique Problem for Proof-of-Work in Cryptocurrencies” Proc. of the 11th International Conference on Information Security and Cryptology (Inscrypt 2015), November 1-3, 2015, Beijing, China. Lecture Notes in Computer Sciences,9589, pp.226-297 Springer 2016

〔学会発表〕(計10件)

1. 穴田啓晃(*), 櫻井幸一：「ブロックチェーンの暗号論的要素技術の分類」, 2018年暗号と情報セキュリティシンポジウム予稿集, 4F1-5.新潟市, 2018年1月26日.

2. 穴田啓晃(*), **櫻井幸一**：「ブロックチェーンにおける計算困難問題の困難さを制御する方式の調査」,第 79 回コンピュータセキュリティ研究発表会研究報告集, 2017-CSEC-79(5), pp.1-5.福岡市（九州大学　伊都キャンパス　サイバーセキュリティセンター）, 2017 年 12 月 4 日.
3. 穴田 啓晃(*), 松島 智洋, 川本 淳平, バグ・サミラン, **櫻井幸一** スケーラブルなプルーフ・オブ・ワークのためのグラーフクリーク・マイニングの分散の 解析 2017 年暗号と情報セキュリティシンポジウム予稿論文集, 1F2-5,
4. 松本 晋一, 穴田 啓晃, フォン ヤオカイ, **櫻井 幸一**: 暗号通貨に関する IACR サマースクール及び ECRYPT ワークショップ参加報告 コンピュータセキュリティシンポジウム 2016 予稿論文集 2C4-4
5. Binanda SENGUPTA, Samiran BAG(*ポスター説明者), Sushmita RUJ, and **Kouichi SAKURAI** Bitcoin Based on Compact Proofs of Retrievability The 10th International Workshop on Security (IWSEC2015), Todaiji Cultural Center, 日本,2015 年 8 月 26 日-28 日.(国際学会)
6. フォン ヤオカイ(*), 松本 晋一, 穴田 啓晃, 川本 淳平, **櫻井 幸一**, 次世代暗号通貨プラットフォーム Ethereum の実験的評価, コンピュータセキュリティシンポジウム 2015 (CSS2015), 2015.10.23
7. 松島智洋(*), 穴田啓晃, 川本淳平, バグ・サミラン, **櫻井幸一**, グラフクリーク探索問題に対するビットコイン・マイニングの評価 火の国情報シンポジウム 2016 予稿集. 4B-2
8. ハ゛グ サミラン(*), ルジ スシミタ, **櫻井 幸一** “ビットコイン・マイニングにおける追加報酬を用いたブロック保留攻撃” 第 33 回暗号と情報セキュリティシンポジウム(SCIS2016)予稿集, 1A2- 5, 熊本, 2016 年 1 月.
9. Samiran BAG(*), Sushmita RUJ and **Kouichi SAKURAI,** “Revisiting Block Withholding Attack in Bitcoin Cryptocurrency” Computer Security Symposium 2015 (CSS2015), 3C3-3, October 21-23, 2015, Nagasaki, Japan.
10. Samiran BAG(*), Sushmita RUJ and **Kouichi SAKURAI** “pplication of Graph Problem for Bitcoin Mining ” Computer Security Symposium 2015 (CSS2015), 3C3-2, October 21-23, 2015, Nagasaki, Japan.

〔図書〕（計 0 件）
〔産業財産権〕
○出願状況（計 0 件）
○取得状況（計 0 件）

〔その他〕
A. 九州大学-研究者情報［櫻井 幸一（教授）システム情報科学研究院 http://hyoka.ofc.kyushu-u.ac.jp/search/details/K000220
B. 九州大学サイバーセキュリティセンター 高度セキュリティ技術研究部門 櫻井幸一
https://cs.kyushu-u.ac.jp/ja/organization/atc/kouichi-sakurai/
C. SAKURAI Lab.
http://itslab.inf.kyushu-u.ac.jp/index-j.html

6. 研究組織
(1)研究代表者
櫻井　幸一（SAKURAI, Kouichi）
九州大学・システム情報科学研究院・教授
研究者番号:60264066

(2)研究分担者
2-1) 穴田 啓晃（ANADA, Hiroaki）教授
長崎県立大学・情報セキュリティ学部
研究者番号：40727202

2-2) 馮 尭楷（FENG, Yaokai),
九州大学・システム情報科学研究院 助教
研究者番号：60363389

2-3) 川本 淳平（KAWAMOTO, Junpei）
九州大学・システム情報科学研究院 助教
研究者番号：10628473
ただし、27 年度のみ参画、H28 年～海外転出

(3)連携研究者:
西出 隆志（NISHIDE, Takashi）
筑波大学・システム情報系・准教授
研究者番号:70570985

(4)研究協力者
Moti Yung（米国グーグル兼コロンビア大学, [現在]スナップチャット社)
Dieter Gollmann（ハンブルグ工科大学・教授)
Kurt SAUER（九州大学・社会人博士後期課程）

以上。