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２４年　５月２１日現在

機関番号：１１３０１
研究種目：挑戦的萌芽研究
研究期間：2009～2011
課題番号：21656096
研究課題名（和文）　低レイヤ低コスト高セキュアな通信プロトコルの開発

研究課題名（英文）　Development of Low-Layer Low-Cost Highly-Secure Communication Protocols

研究代表者
曽根　秀昭（SONE HIDEAKI）
東北大学・サイバーサイエンスセンター・教授
研究者番号：40134019

研究成果の概要（和文）：本研究は，近距離での秘密鍵の共有と，遠距離での秘密鍵の活用という二つの手法を確立し，それぞれを組み合わせることによって，低レイヤ低コスト高セキュアな通信の実現を目指すものである。すなわち，本研究の主要な成果は，廉価なケーブルなどを用いてセキュリティを確保する上で重要なメカニズムを明らかにしたことと，共有済みの秘密鍵を用いた秘密増幅のプロトコルの開発に成功したことである。

研究成果の概要（英文）：To achieve low-layer low-cost highly-secure communications, we investigated secret key agreement at close range and developed a method to utilize shared secret keys. That is, one of main results was to clarify mechanisms of low-cost equipment, say cables, for accomplishing security, and the other was to design a protocol for privacy amplification using such shared secret keys.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2009 年度	1,200,000	0	1,200,000
2010 年度	700,000	0	700,000
2011 年度	800,000	240,000	1,040,000
年度			
年度			
総　計	2,700,000	240,000	2,940,000

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：暗号・セキュリティ，セキュア・ネットワーク，暗号・認証等，情報システム

１．研究開始当初の背景

情報セキュリティを確保する上で，暗号技術がこの現代社会において広く用いられていることは言を待たず，研究開始当時にあっても状況は同様であり，例えば共通鍵暗号方式である AES や公開鍵暗号方式である RSA などが情報化社会を支える重要な基盤技術として利用されている。

これらの暗号技術の安全性は，数学的（計算量的）に難しい問題に依存していたり，現時点で知られている解読アルゴリズムや利用可能な計算資源では解読できないという状況に依存していたりする。すなわち，将来にわたり安全であることを保証することはできず，実際に暗号の危殆化問題には大きな関心が集められている。

一方，上のような安全性の根拠とは異なる視点から，暗号技術の安全性を確保しようとする既存研究が，本研究の開始以前から存在しており，研究代表者はそちらをターゲットとして研究を進めるべく，研究課題を提案し，採択に至った次第である。すなわち，その安全性を物理的な性質や情報理論などに求めるセキュアな通信プロトコルの開発を目指すことを研究開始当初に思い描いていた。より具体的には次に記載する通りである。

本研究については次章以降で詳しく記述するが，研究開始当初の背景として，本研究のスコープと類似した研究の動向の一例を挙げるとすると，指向性アンテナや無線 LAN（IEEE802.11）を利用した秘密鍵共有法が知られている（例えば，文献[A05]）。これらの既存研究では，秘密鍵を共有したい端末間における電波伝播特性や端末の位置情報を撹乱することで安全性を担保しようとている。すなわち，これらの研究は，低レイヤプロトコルにおける物理的性質などに根拠を置いた情報理論的な安全性を追求しようとしている。言い換えると，RSA 公開鍵暗号や AES ブロック暗号などのように計算の難しさに安全性の根拠を置こうとする暗号方式とは一線を画く研究ストリームである。

研究代表者は，研究開発当初より環境電磁工学を専門としており，それまでメタルケーブルの周囲磁界漏洩やスイッチ接点動作時のノイズ発生などの現象を解析・研究し，それらの物理的な性質を実験的あるいは理論的に解明してきた。そのため，研究開発当初において，このような知見を活かすことで，全く新しい秘密鍵共有法やプロトコルの要素技術の考案・開発等を進めることを念頭に置いていた。

[A05] T. Aono, et al., Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels, IEEE Transactions on Antennas and Propagation, 53(11), 3776-3784, 2005.

２．研究の目的

本研究は，研究課題名「低レイヤ低コスト高セキュアな通信プロトコルの開発」が象徴するように，メタルケーブルなどの「低コスト」な通信媒体を活用し，それら「低レイヤ」プロトコルにおける物理的性質などに基づき，「高セキュア」な情報通信を実現する秘密鍵共有法やプロトコルの開発を主要な目的としている。

例えばメタルケーブルにおける通信路としての相反性や周波数特性を巧みに利用し，同軸ケーブルなどを使った秘密鍵共有のための手法の開発や，安全性の確保のために必要なパラメータの導出などが課題となる。また，昨今話題となっているサイドチャネル攻撃に対する研究もまた極めて重要であり，廉価な器材を用いて情報セキュリティを確保しようする場合に求められる，それらの物理的あるは電磁気学的な性質やメカニズムを明らにする必要がある。

また，高セキュアな情報通信を実現するために，共有済みの秘密鍵をうまく活用して，遠隔での秘密増幅の手法を確立することが重要であり，そのようなプロトコルの開発が望まれる。

３．研究の方法

本研究は，大きく分けると次の二つの側面から安全な通信手法の確立を目指すものである。

(1) 至近距離での，セキュリティ確保のために必要なメカニズムの解明
(2) 遠距離における，共有済み秘密鍵を活用した，安全な情報通信プロトコルの開発

すなわち，至近距離では物理的な安全性を追求し，遠距離では，至近距離で生成した秘密鍵を活用するというアイデアである。より具体的には次に記述する通りである。

まず，前者については，UTP ケーブルや USB ケーブル，あるいは同軸ケーブルなどといった廉価なケーブルや，赤外線その他の廉価な通信ポートを活用した，セキュリティの確保の手法とその安全性を担保するメカニズムやパラメータを詳細に検討する。スーパーコンピュータを使った大規模な電磁界計算を行うなどして，必要なパラメータやその値について明らかにしていく。特にコモンモード電流にも着目し，研究代表者の専門とする環境電磁工学の知見を活かし，スーパーコンピュータを使った大規模なシミュレーションを行うなどして，通信プロトコルの開発に資することを実現する。

次に後者について言及する。まず秘密鍵の共有状況に関するモデル化や定式化を行うとともに，グラフ理論や情報理論の既存の手法を見極め，遠隔間での高セキュア通信のためのプロトコルの開発や，マルチパーティにおける秘密増幅という問題の解決を目指す。また，定式化した秘密鍵の共有状況に関するモデルのもとで，より効率的な高セキュア通信のためのプロトコルを開発する。

以上の要素技術が実現すると，本研究の着想に至ったきっかけそのものであるが，次のことが可能となる。まず状況として，離れた場所に住む花子さんと太郎さんが安全な通信を行いたいとしよう。このとき，もし花子さんと太郎さんが会議や集会などでたびたび直接会うような間柄であれば，物理的に同じ場所にいるときに，お互いのノートパソコンを直接接続して，秘密鍵の基になる大量の

秘密情報を交換しておくことができる。そうすれば，それぞれ自分の住んでいる場所に戻った後で，共有しておいた情報を秘密鍵に活用することにより，遠隔間のネットワーク越しでも安全な通信を行うことができる。

さらには，花子さんおよび太郎さんを含む多人数のコミュニティが存在するとき，多人数による遠隔間での秘密増幅の手法が確立できれば，より安全な通信が可能となり，しかも，生成される秘密鍵の安全性は物理的な性質や情報理論に依存することになり，その応用範囲は広いと考えられる。

４．研究成果

本研究は，繰り返しになるが，研究課題名「低レイヤ低コスト高セキュアな通信プロトコルの開発」が示すように，廉価な各種ケーブルなどの「低コスト」な通信媒体を活用し，それら「低レイヤ」プロトコルにおける物理的性質などに基づき，「高セキュア」な情報通信を実現する秘密鍵共有法やプロトコルの開発を主要な目的とし，環境電磁工学の知見を活かすことにより至近距離での低レイヤ低コストな秘密鍵共有に必要な条件を明らかにするとともに，共有済み秘密鍵を活用した遠距離での高セキュアな情報通信プロトコルを開発するものである。

初年度は，各種ケーブルを使った安全な秘密鍵共有法の確立を目指し，ケーブルおよびその周辺における電磁界分布の実験的測定，あるいはスーパーコンピュータを活用した大規模な電磁界シミュレーションを行い，そのモデル化や現象の解明を行った。これらの成果は，電子情報通信学会における総合学会や研究会で発表しており，また，IEEE International Symposium on Electromagnetic Compatibility (EMC) 2010 での発表・採録が決定した。この実験およびシミュレーション結果により，ケーブルを用いて秘密鍵共有を行う際に有用なパラメータのいくつかが明らかになり，秘密鍵共有法や安全性強化の実現に向けて，有力な要素技術が得られた。

また，赤外線 USB アダプタを購入し，実際に実験を行いつつ，赤外線通信ポートを活用した，秘密鍵共有の手法を検討した。より具体的には，実験と理論の両面から，通信で用いる赤外線の強度を利用し，二者間で秘密情報を共有できるための条件を検討した。同時に，それを実現するための通信プロトコルも検討している。さらに，秘密鍵の共有状況に関するモデル化や定式化を検討した。

翌年度は，本研究課題の主要なテーマの一つである「高セキュア」な情報通信を実現する秘密鍵共有法について，秘密鍵の共有状況に関するグラフ理論的モデル化と定式化を行うとともに，グラフ理論の分野で古くから知られている st-numbering という手法を応用することにより，二者間において秘密増幅を実現するマルチパーティ通信プロトコルを開発した。この成果については，論文誌 International Journal of Foundations of Computer Science への採録が決定し，翌年掲載された。

また，前年度に引き続き，各種ケーブルを使った安全な秘密鍵共有法の確立を目指し，ケーブルおよびその周辺における電磁界分布の測定等を行い，そのモデル化や現象の解明を行った。特に，電源ケーブルの接地・非接地における詳細な分析を行い，情報セキュリティを確保する上でもアース線の接地が重要であることを示すとともに，低レイヤにおける高セキュア維持のために重要な技術を得ることができた。この成果は，電子情報通信学会論文誌Bに公表している。7月には，前年度 accepted を受けた発表を国際会議 IEEE EMC 2010 で行い，低コストな通信媒体であるケーブルとコネクタのモデル化に関する成果を公表した。

最終年度は，前年度までに得られた成果をさらに進展させるため，ケーブルを使った安全な通信を保証する上で，特にケーブルの接続部であるコネクタとそれら周辺のコモンモード電流に着目し，スーパーコンピュータを使った電磁界計算等により，良好な通信を保つために必要となるコネクタの接触性能要件に関する検討を行い，成果を IEICE Trans. Electronics に公表した。加えて，セキュアな通信を実現するためには，秘密情報が機器外部に放射電磁波をサイドチャネルとして漏えいするようなことが起きてはならないが，通信に用いる信号強度によっては，秘密

情報を含むコモンモード電流と背景ノイズの比率（SNR）が大きく変化し，情報が漏えいする危険性が生ずる恐れがあることから，SNR と情報の漏れやすさの関係を詳細に解析し，IEEE EMC 2011 において成果を公表した。これらの成果により，低レイヤ通信媒体における高セキュア通信のための条件を確立した。

また，前年度までに定式化している秘密鍵の共有状況に関するモデルのもとで，共有済み秘密鍵を活用した遠距離での高セキュア通信プロトコルの効率を上げる手法を考案した。

以上の三年間の成果により，低レイヤ低コスト高セキュアな通信に資することができた。

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 5 件）

① Takaaki Mizuki, Satoru Nakayama, and Hideaki Sone, An Application of st-Numbering to Secret Key Agreement, International Journal of Foundations of Computer Science, 査読有, vol.22, 2011, pp.1211-1227.

② Yu-ichi Hayashi, Yoshiki Kayano, Takaaki Mizuki, Hideaki Sone, and Hiroshi Inoue, A Contact Conditions in Connectors that Cause Common Mode Radiation, IEICE Trans. Electronics, 査読有, vol. E94-C, 2011, pp.1369-1374.

③ Taishi Ikematsu, Yu-ichi Hayashi, Takaaki Mizuki, Naofumi Homma, Takafumi Aoki, and Hideaki Sone, Suppression of Information Leakage from Electronic Devices Based on SNR, IEEE International Symposium on Electromagnetic Compatibility 2011, 査読有, 2011, pp.920-924.

④ Yu-ichi Hayashi, Songping Wu, Jun Fan, Takaaki Mizuki, and Hideaki Sone, Modeling Connector Contact Condition Using a Contact Failure Model with Equivalent Inductance, IEEE International Symposium on Electromagnetic Compatibility 2010, 査読有, 2010, pp.743-747.

⑤ 衣川昌宏，林優一，水木敬明，曽根秀昭，アース線の非接地が情報漏えいに与える影響の測定，電子情報通信学会論文誌B，査読有，vol. J93-B, 2010, pp.1559-1561.

〔学会発表〕（計 6 件）

① 松田和樹，林優一，水木敬明，曽根秀昭，コネクタ接触境界における電流路の変化とインダクタンス増加の関係，電子情報通信学会総合大会，2012 年 3 月 22 日，岡山大学.

② 衣川昌宏，林優一，水木敬明，曽根秀昭，電源線非接地が漏洩情報の取得性に与える影響に関する検討，電子情報通信学会ソサイエティ大会，2010 年 9 月 17 日，大阪府立大学.

③ 林優一，水木敬明，曽根秀昭，コネクタ接触不良部における電流分布に関する考察，電子情報通信学会総合大会，2010 年 3 月 17 日，東北大学.

④ 林優一，水木敬明，曽根秀昭，漏洩電磁界による情報システムセキュリティ低下の問題，電子情報通信学会総合大会，2010 年 3 月 16 日，東北大学.

⑤ Yu-ichi Hayashi, Songping Wu, Jun Fan, Takaaki Mizuki, Hideaki Sone, Effect of Contact Point Distribution to the High-Frequency Impedance on a Coaxial Connector, 電子情報通信学会機構デバイス研究会国際セッション，2009 年 11 月 20 日，日本工業大学神田キャンパス.

⑥ 大村孔平，林優一，水木敬明，曽根秀昭，情報機器に接続された線路が機器からの電磁的情報漏洩に与える影響，電子情報通信学会環境電磁工学研究会，2009 年 10 月 22 日，岩手県八幡平市.

６．研究組織
(1)研究代表者
曽根　秀昭（SONE HIDEAKI ）
東北大学・サイバーサイエンスセンター・教授
研究者番号：40134019

(2)研究分担者
水木　敬明（MIZUKI TAKAAKI）
東北大学・サイバーサイエンスセンター・准教授
研究者番号：90323089

林　優一（HAYASHI YU-ICHI）
東北大学・工学研究科・COE フェロー
研究者番号：60551918