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 6 月 8 日現在

機関番号：１２１０１
研究種目：基盤研究（B）
研究期間：2009 ～ 2011
課題番号：２１３００００１
研究課題名（和文）　鍵が不要かつ無条件に安全な暗号伝送方式に関する研究

研究課題名（英文）Research on unconditionally secure message transmission scheme with no keys

研究代表者
黒澤　馨　（Kaoru Kurosawa）
茨城大学・工学部・教授
研究者番号：60153409

研究成果の概要（和文）：無条件に安全な暗号伝送方式(PSMT)のモデルにおいては、送信者と受信者の間に n 本のチャネルが存在し、送受信者は事前に鍵を共有していない。敵は無限大の計算能力を有し、n 本のチャネルのうちのある部分集合を盗聴、改ざんできる。本研究では、いくつかの敵のモデルに対し、ラウンド数が最小で効率のよい PSMT および almost PSMT を構成した。

研究成果の概要（英文）：In the model of Perfectly Secure Message Transmission schemes (PSMT), there are n channels between the sender and receiver who share no keys. Adversaries are infinitely powerful, and can corrupt some subset of n channels. In this research, round optimum PSMT and almost PSMT have been constructed for some class of adversaries.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2009 年度	1,800,000	540,000	2,340,000
2010 年度	1,700,000	510,000	2,210,000
2011 年度	1,700,000	510,000	2,210,000
総　計	5,200,000	1,560,000	6,760,000

研究分野：現代暗号理論
科研費の分科・細目：情報学・情報学基礎
キーワード：無条件安全性、メッセージ伝送、ラウンド数, 秘密分散共有法

１．研究開始当初の背景

(1) 無条件に安全なメッセージ伝送とは：ＲＳＡ暗号などの公開鍵暗号系は、素因数分解や離散対数問題が困難という仮定に基づいている。しかし、計算機科学の進歩、あるいは量子コンピュータの実用化などにより、これらの計算量的仮定が成り立たなくなるかもしれない。一方、共通鍵暗号系においては、送信者と受信者がどうやって事前に秘密鍵を共有するか、という根本的問題が存在する。

したがって、秘密鍵が不要でかつ無条件に安全な（敵が無限大の能力を有しているとしても安全な）暗号伝送系を構成できることが望ましい。Dolev 等は、送受信者間に n 本のチャネルが存在し、敵は高々 t 本しか盗聴・改ざんができない、というモデルにおいては、そのような暗号系を構成できることを

示した。今日のインターネットにおいては、送受信者間に多くのチャネルが存在する。また、敵はこれら全てのチャンネルを盗聴・改ざんできるはずがないと考えられる。

このような暗号系は、完全秘匿性および完全信頼性（受信者は平文を正しく受信できる）という２つの条件を満たすとき、「完全に安全な(t,n)閾値型暗号伝送方式」と呼ばれる。現在知られている全ての公開鍵暗号は、いつしか破られてしまう危険性を考えると、このような暗号伝送方式を研究する意義はきわめて大きい。

(送信者)→n 本のチャンネル→(受信者)
↑
敵
(高々t 本を盗聴、改ざん)

さらに、この方式はマルチパーティ・プロトコルに対しても重要な役割を果たす。各参加者 P_i が自分の秘密 x_i を秘密にしたまま、お互いに協力して関数 $f(x_1,\cdots,x_n)$ の値のみを正しく計算するプロトコルをマルチパーティ・プロトコルという。（たとえば、選挙。）無条件に安全なマルチパーティ・プロトコルを実現するためには、参加者の全てのペア間に秘密通信路が存在しなければならない。しかし、そうでない場合でも、この方式を適用すれば、各ペア間に秘密通信路と同等の機能を確保できることになる。

$n \geqq 3t+1$ の場合は、「完全に安全な(t,n)閾値型暗号伝送方式」を 1 ラウンドで効率よく実現できることが知られている。一方、$n \geqq 2t+1$ の場合は、2 ラウンドあれば実現できる。しかし、後述するように、$n=2t+1$ に対する構成法は非常に難しい問題であった。(1 ラウンド方式：単に送信者がデータを送信する。2 ラウンド方式：まず受信者が送信し次に送信者が送信する。)

$n=2t+1$ の場合、伝送レートの下界は n であることが、Rangan らによって示されている。Agarwal, Cramer and de Haan は、2 ラウンドかつ伝送レートが O(n) となる方式を示した。すなわち、ラウンド数、伝送レートは共に最適である。しかし、彼らの方式においては、計算時間が n の指数関数となってしまう。

(2) 申請時に既に得ていた成果：黒澤は、Eurocrypt 2008 において、$n=2t+1$ に対する上記の open problem を解決した。すなわち、擬似次元、擬似基底という概念を導入することにより、計算時間が n の多項式時間となる方式を構成したのである。なお、Eurocrypt は、現代暗号理論の分野において CRYPTO と並び最もレベルの高い国際会議である。

一方、1 ラウンドの「完全に安全な方式」を $n=2t+1$ に対し構成することは不可能である。これに対し、黒澤は ICITS 2007 において、「ほとんど安全な方式」であれば、構成できることを示した。

２．研究の目的

本研究は、黒澤のこれまでの成果を基に、より効率の高い方式をより現実的な敵のモデルに対し開発し、さらに各パラメータの限界式を導出することを目指すものである。

(1) ラウンド数、伝送レート以外のパラメータ（平文の長さ、計算時間等）の最適化を図る。
(2) より現実的な非閾値型の敵に対し、安全でかつ効率のよい方式を開発する。
(3) 盗聴はできるが改ざんできないチャネルを 1 本追加したモデルについて検討する。
(4) Verifiable secret sharing scheme (VSS) への応用を図る。汎用的なマルチパーテ

ィプロトコルは VSS に基づいているため、これはマルチパーティプロトコルの効率化につながる。

３．研究の方法

黒澤の長年の共同研究者であり、かつ現代暗号理論の分野において卓越した業績をあげているロンドン大学のYvo Desmedt教授、Waterloo大学(カナダ)のDouglas Stinson教授、カルガリー大学（カナダ）のRei Safavi-Naini教授、及び本分野の世界的権威であるインド工業大学のRangan教授らと密接に議論を重ね、本研究に関する視野を広げた。

また、Rangan教授の教え子であるAshish Choudhury博士および Arpita Patra博士とは、具体的に共同研究を行った。

４．研究成果

無条件に安全な暗号伝送方式(PSMT)のモデルにおいては、送信者と受信者の間にn本のチャネルが存在し、送受信者は事前に鍵を共有していない。敵は無限大の計算能力を有し、n本のチャネルのうちのある部分集合を盗聴、改ざんできる。

(送信者)→n 本のチャンネル→(受信者)
↑
敵
(n 本中のある部分集合を盗聴、改ざん)

ここで、敵が盗聴、改ざんできるようなチャネルの部分集合Bの族Γを敵構造と呼ぶ。

どのような B_i, $B_j \in \Gamma$ に対しても

$B_i \cup B_j \neq \{1, \cdots, n\}$

となるとき、敵構造ΓはQ2を満たすという。また、どのような B_i, B_j, $B_k \in \Gamma$ に対しても

$B_i \cup B_j \cup B_k \neq \{1, \cdots, n\}$

となるとき、敵構造ΓはQ3を満たすという。n≧2t+1はQ2の特殊な場合であり、n≧3t+1はQ3の特殊な場合である。

(1) 敵構造がQ2の場合に対するPSMTの構成:
Kumarらは、Q2という条件を満たす敵構造に対しPSMTの構成法を示したが、データのやりとりに多くのラウンド数を必要とした。本研究では、Q2を満たす敵構造に対し、３ラウンドで済む多項式時間のPSMTを開発した。また、２ラウンドで済む非多項式時間PSMTを開発した。

Kumarら	ラウンド数大
本研究	３ラウンド（多項式時間）
本研究	２ラウンド（非多項式時間）

敵構造がQ2の場合に対するPSMT

(2) 敵構造がQ2の場合に対する almost PSMTの構成: 小さい復号誤り確率を許すようなPSMTをalmost PSMTと呼ぶ。本研究では、Q2を満たす敵構造に対し、１ラウンドで済む多項式時間のalmost PSMTを開発した。

	1 round	2 round	3 round
PSMT	×	本研究 非多項式	本研究 多項式
Almost PSMT	本研究		

敵構造がQ2の場合に対する almost PSMT

(3) ラウンド数最小のVSSの構成とそのPSMTへの応用：デーラーの不正をも検出できるような秘密分散共有法のモデルを verifiable secret sharing schemes (VSS) という。

秘密s→ デーラー（不正）

→ sをn人の参加者に分散（不正）

→ sを再構成

従来、閾値型の敵に関するVSSのラウンド数が知られていた。これを、非閾値型の敵に拡張した。すなわち、2 round VSSが存在する必要十分条件は、敵構造がQ4を満たすときである。3 round VSSが存在する必要十分条件は、敵構造がQ3を満たすときである。提案方式は、効率も良い。さらに、提案する方式の特殊な場合として、n=3t+1を満たす閾値的な敵に対し、従来より効率のよい3 round VSSが構成できることを示した。

	2 round	3 round
閾値型（従来）	n>4t	n>3t
非閾値型（本研究）	Q4	Q3

VSSのラウンド数

(4) 誤り復元可能な秘密分散共有法の構成とそのPSMTの応用：n人の参加者の中に不正者がいるような秘密分散共有法を考える。

秘密s→ デーラー(honest)

→ sをn人の参加者に分散（不正）

→ sを再構成

すなわち、再構成段階において公開されたシャア(v_1, …, v_n)のうち、いくつかは正しくない。このような(v_1, …, v_n)から秘密sを正しく復元できる方式を、誤り復元可能と呼ぶ。本研究では、秘密分散共有法が誤り復元可能である必要十便条件は、敵構造がQ3という条件を満たすことであることを証明した。次に、これを利用し、Q３を満たす敵構造に対し、１ラウンドで済む多項式時間のPSMTを開発した。従来のPSMTは、指数時間であった。

	1 round
従来	指数時間
本研究	多項式時間

Q３を満たす敵構造に対するPSMT

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 Kaoru Kurosawa: Round-efficient perfectly secure message transmission scheme against general adversary. Des. Codes Cryptography 63 (2): 199-207 (2012) 査読有
② Ashish Choudhury, Kaoru Kurosawa, Arpita Patra: Simple and Efficient Single Round almost Perfectly Secure Message Transmission Tolerating Generalized Adversary. ACNS 2011: 292-308(2011) 査読有
③ Ashish Choudhury, Kaoru Kurosawa, Arpita Patra: The Round Complexity of Perfectly Secure General VSS. ICITS 2011: 143-162(2011) 査読有
④ Kaoru Kurosawa: General Error Decodable Secret Sharing Scheme and Its Application. IEEE Transactions on Information Theory 57 (9): 6304-6309 (2011) 査読有
⑤ Kaoru Kurosawa, Kazuhiro Suzuki: Truly efficient 2-round perfectly secure message transmission scheme. IEEE Transactions on Information Theory 55 (11):, 5223-5232 (2009) 査読有

〔学会発表〕（計 1 件）

① Kaoru Kurosawa: Cryptography for Unconditionally Secure Message Transmission in Networks. CANS 2010, 2010.12.12-14 Kuala Lumpur, Malaysia （招待講演）

６．研究組織

(1)研究代表者
黒澤　馨　（Kaoru Kurosawa）
茨城大学・工学部・教授
研究者番号：60153409