合理的な秘密分散における不可能性とその回避方法

安永 憲司

† 九州先端科学技術研究所
814-0001 福岡市早良区百道浜 2-1-22 福岡 SRP センタービル 7 階
yasunaga@isit.or.jp

あらまし 合理的な秘密分散とは，秘密分散の復元フェーズにおいて，秘密の復元を独占したいと考えるプレイヤーを想定する問題であり，これまでに様々なプロトコルおよび不可能性の結果が知られている．本稿では，その不可能性を再考し，その回避方法を考える．

Impossibility Results for Rational Secret Sharing and Their Avoidance

Kenji Yasunaga

†Institute of Systems, Information Technologies and Nanotechnologies (ISIT)
Fukuoka SRP Center Building 7F, 2-1-22, Momochihama, Sawara-ku, Fukuoka 814-0001, JAPAN
yasunaga@isit.or.jp

Abstract Rational secret sharing is a problem for secret sharing in which each player wants to recover the secret exclusively. A lot of protocols and impossibility results for rational secret sharing have been presented. In this article, we review the impossibility results and consider their avoidance.

1 はじめに

分散プロトコルを設計する際に問題となるのは，参加者がプロトコルから逸脱する可能性である．プロトコルからの逸脱をモデル化する方法として大きく 2 つの方法が存在する．1 つ目は，暗号理論で考えられているモデル化である．あるプレイヤーは正直者であり，その他のプレイヤーは悪者だと考える．つまり，正直者はプロトコルに従うが，その他のプレイヤーは任意の逸脱を行うと考える．2 つ目は，ゲーム理論で考えられているモデル化である．すべてのプレイヤーは合理的であると考え，プレイヤーは自分の利益のためにプロトコルから逸脱をすると考える．

最近，暗号理論のモデルとゲーム理論のモデルを組み合わせたモデルが注目され，研究されている．本研究では，その中でも，合理的な秘密分散と呼ばれている問題を扱う．

秘密分散法は，暗号プロトコルの 1 つであり，秘密を安全に分散させることを目的とする．最も有名な秘密分散法は，Shamir [15] によって提案されたものである．この秘密分散法は，閾値型秘密分散法として知られている．(t, n) 閾値型秘密分散法では，秘密 s を n 個のシェアに分散し，そのうち t 個が集まれば秘密 s が復元でき，また，t 個未満のシェアからは s に関する情報が一切漏れないという性質を持つ．

合理的な秘密分散とは，秘密分散プロトコルを実行する際に，それを実行するプレイヤーが合理的であると考える問題である．この問題は，2004 年に Halpern と Teague [6] によって導入された．まず，秘密からシェアを作るフェーズはディーラーと呼ばれる正直なプレイヤーが実行すると仮定する．そして，秘密 s から作られた n 個のシェアは n 人のプレイヤーにそれぞれ配られると仮定する．その後，t 人以上の

プレイヤーが集まった後，それぞれがシェアを出し合うことで秘密を復元することを考える．Halpern と Teague は，この設定のもと，以下のような合理性をもつプレイヤーを考えた．

1. 各プレイヤーは正しく秘密を復元したい．
2. より少ない人数で秘密を復元したい．

つまり，各プレイヤーは秘密の復元を少ない人数で行いたいと考えるプレイヤーである．別の言い方をすれば，秘密の復元を独占したいと考えるプレイヤーである．この合理性自体は，比較的自然のように見える．では，既存の秘密分散プロトコルは，このような合理的なプレイヤーに対してどのように実行されるのだろうか．Halpern と Teague は，Shamir の秘密分散法では，秘密の復元ができないという考察を行った．

Halpern と Teague によって提起された合理的な秘密分散という問題は，その後多くの研究者の注目を集め，これまでに様々なプロトコルが提案されている [6, 5, 10, 1, 8, 9, 11, 12, 4, 2, 13]．また，プロトコルの提案と同時に，様々な不可能性に関する結果も知られている [6, 9, 2]．

特に，不可能性に関しては比較的強い結果が示されており，合理的な秘密分散という問題の難しさが明らかになっている．また，否定的な結果が先行しているために，合理的な秘密分散という問題に対する興味自体が暗号理論分野において失われているという印象がある．

そこで，本研究では，合理的な秘密分散における不可能性の結果を再考し，その回避方法についての検討を行う．

2 Halpern と Teague の考察

まず，Halpern と Teague [6] が行った，Shamir の秘密分散法が正しく実行されないと考える理由について説明する．

合理的なプレイヤーの行動を分析するのがゲーム理論である．ゲーム理論では，各プレイヤーがある行動をとるとき，それが均衡状態にあるか否かで，その行動の尤もらしさを議論する．最も有名な均衡概念が *Nash* 均衡である．

ある戦略が Nash 均衡であるとは，各プレイヤーにとって，自分以外のプレイヤーがその戦略に従うと仮定したとき，自分はいかなる戦略をとったとしても，利得を真に高めることができない状態のときである．つまり，他のプレイヤーがその戦略に従うと仮定すれば，自分にとってもその戦略に従うことが利得を最大化させることになり，その戦略をとることは合理的であるという考え方である．

Nash 均衡という概念を踏まえ，まずはじめに，(n,n) 閾値型秘密分散法を合理的なプレイヤーが実行すること考える．秘密分散の復元フェーズでは，集まった n 人それぞれが自分のシェアを出すことを求められる．ここで，議論を簡単にするため，各プレイヤーは認証付きのシェアを保持していると考える．つまり，各プレイヤーが与えら得たシェアから別の正当なシェアを作ることは，無視できる確率を除けば不可能だと仮定する．ちなみに，秘密分散を認証付きにする方法はよく知られている [16]．シェアが認証されていると仮定すると，各プレイヤーが選択可能な行動は，実質的に 2 つしかない．「(正しい) シェアを出す」か，「シェアを出さない」か，である．このとき，正しくシェアを出すというのが秘密分散プロトコルで指定されている行動である．しかし，この行動 (戦略) は，Nash 均衡でないことがわかる．自分以外の $n-1$ 人が戦略に従うと仮定する．つまり，$n-1$ 人は正しくシェアを出す．このとき，もし自分もシェアを正しく出せば，全員 n 個のシェアを手に入れることになり，n 人全員が秘密を復元できる．しかし，もし自分がシェアを出さなかった場合，この場合は，自分自身は手元にあるシェアと他の $n-1$ 個のシェアから秘密を復元できるが，その他のプレイヤーは $n-1$ 個のシェアしか手に入らず，(n,n) 閾値型秘密分散の性質から，秘密は正しく復元されず，かつ秘密に関する情報は一切手に入らない．つまり，自分が選択する行動としては，「シェアを出さない」ことのほうが利得が高くなる．したがって，「シェアを出す」という戦略は Nash 均衡ではないのである．

次に，(t,n) 閾値型秘密分散 $(t<n)$ の場合を考える．この場合，自分以外の $n-1$ 人が正しくシェアを出すと仮定すると，閾値 t が $n-1$ 以下であるため，自分がどのような行動をとるかに関わらず，シェアは t 個以上出されることとなり，秘密が復元できる．シェアを出すときと出さないときの利得に差がないため，この場合，「シェアを出す」という戦略は Nash 均衡である．しかし，この Nash 均衡は本当に尤もらしい行動なのだろうか．Nash 均衡を議論する際は，自分以外のプレイヤーが戦略にしたがうと

仮定していたが，それ以外のすべての可能性のある状況も考えてみる．つまり，自分以外のプレイヤーが任意の戦略をとる場合を考える．すると，どのような状況を考えたとしても,「シェアを出す」方が「シェアを出さない」よりも利得が高くなる状況は存在せず，また，ある状況においては,「シェアを出さない」方が真に利得が高くなることがわかる．(真に利得が高くなるのは，上の (n,n) のような状況のときである.) このようなとき，ゲーム理論では,「シェアを出す」という戦略は「シェアを出さない」という戦略に弱支配されるという．弱支配される均衡は安定的な均衡ではないと考えられる．なぜなら，弱支配される戦略から，それを弱支配する戦略に変更することは尤もらしいと考えられるからである．したがって，(t,n) 閾値型の場合も,「シェアを出す」という戦略は，Nash 均衡ではあるが，弱支配される戦略であるため，安定的な均衡ではないと考えられる．

3 解概念に関する既知の考察

3.1 弱支配戦略の逐次除去

Halpern と Teague [6] は，弱支配される Nash 均衡を安定的な均衡と認めないために，弱支配戦略の逐次除去という概念を考えた．この概念は，弱支配される戦略を逐次的に除去した結果残った戦略のことを指している．すると，(t,n) 閾値型 $(t<n)$ の場合で「シェアを出す」という戦略は，弱支配されるためこの均衡概念を満たさない．また，彼らは，プレイヤー間に秘匿通信路等を仮定することで,「シェアを出す」ことが弱支配戦略の逐次除去を満たすようなプロトコルを提案している．

その後のいくつかの研究 [6, 1, 5, 8, 2] において，弱支配戦略の逐次除去は，安定的な均衡概念の 1 つとして考えられてきた．

しかし，Kol と Naor [9] は，弱支配戦略の逐次除去という概念の不十分さを指摘した．彼らは，ある悪い戦略が，弱支配戦略の逐次除去を満たしていることを示した．具体的には,「一度きり (talk-once)」と呼ばれる戦略で，最初のラウンドではシェアを正しく出し，その後はシェアを出さないという戦略である．例えば,「常にシェアを出さない」という戦略はこの「一度きり」戦略を弱支配していない．なぜならば，プレイヤー i 以外が以下に述べる戦略をとるときは，プレイヤー i にとっては「一度きり」戦略の方が真に利得が高くなるからである．その戦略とは，最初のラウンドはシェアを出さず，次のラウンドはプレイヤー i が最初のラウンドでシェアを出したときに限りシェアを出す，というものである．他のプレイヤーがこの戦略に従うと仮定すれば，プレイヤー i にとっては「一度きり」戦略をとれば秘密の復元を独占できるのである．

3.2 結託耐性 Nash 均衡

通常の Nash 均衡では，各プレイヤーごとに逸脱の可能性を考えてきた．つまり，他のプレイヤーと結託することは考えていない．Abraham ら [1] は，プレイヤー同士の結託を考慮した Nash 均衡を考えた．つまり，ある一定人数で結託したとしても，真に利得を高める戦略が存在しないかどうかを考える．特に，k 人以下の任意の結託を考えたとして，真に利得を高める戦略が存在しないとき，その戦略のことを，結託耐性 k の *Nash* 均衡と呼ぶ．結託耐性 1 の Nash 均衡は，通常の Nash 均衡と一致する．

3.3 逆向き帰納法に対する耐性

Kol と Naor [8] は，計算量的な結託耐性を考え，さらにそれを強化した概念を提案した．暗号技術を利用すると，無視できる確率でその暗号技術を破れる可能性がある．それらを考慮した上で結託耐性 Nash 均衡は自然に定義可能である．しかし，Kol と Naor は，計算量的に安全な暗号技術を利用すると，逆向き帰納法（4.1 節を参照）の問題が出てくることを指摘した．計算量的に安全な暗号技術を利用するとき，プロトコルのラウンド数を指数関数的に大きくすることはできない．なぜなら，ある時点で暗号技術の安全性が破られてしまうからである．つまり，計算量的に安全な暗号技術を利用する限り，プロトコルが終了するためのラウンド数はある固定されたラウンド数以下である．固定されたラウンド数以下で終了するということは，逆向き帰納法が適用されてしまう．

この問題を回避するため，Kol と Naor は，逆向き帰納法に耐性のある均衡概念を提案した．まず，復元フェーズプロトコルでは，秘密が復元されるまでプロトコルを繰り返し実行していることに着目した．そして，その戦略に従った場合の任意の繰り返し後（ただし，プロトコル終了

でない場合) において，それが結託耐性 Nash であるという均衡概念を提案した．その戦略に従っている限りは，どのラウンドにおいても Nash 均衡であるため，逆向き帰納法の議論は適用されない．

この概念は，復元フェーズプロトコルが，あるプロトコルの繰り返しであると仮定しているため，それ以外の形で復元を行うプロトコルには適用できない．また，Kol と Naor [8] も論文中で明示しているが，彼らは，この概念が安定的な均衡のために十分なものとは考えていない．なぜならば，Shamir の (t,n) 閾値型秘密分散法も，$t<n$ かつ復元フェーズに $t+1$ 人以上のプレイヤーがいる場合は，この均衡概念を満たすからである．2 節で議論したとおり，このプロトコルは弱支配される Nash 均衡であり，安定的な均衡とは考えられない．

3.4 狭義 Nash 均衡

Kol と Naor [9] は，弱支配戦略の逐次除去が不十分であることから，新たな均衡概念として狭義 *(strict) Nash* 均衡を導入した．この概念は，他のプレイヤーがその戦略に従う限り，その戦略以外の戦略をとると利得が真に下がることを保証している．つまり，ゲームにおいて十分に軽微な変更があったとしても，元々の戦略に従うことが望ましいことを保証しているともいえる．3.1 節で議論した「一度きり」戦略は，他のプレイヤーにシェアを出さない可能性がわずかでも存在すれば,「シェアを出さない」戦略の方がよい戦略となるため，狭義 Nash 均衡ではない．狭義 Nash 均衡は，Nash 均衡や弱支配戦略の逐次除去といった均衡概念を含んでいる強い概念である．

また，Kol と Naor [9] は，狭義 Nash 均衡を議論する際には，居残り回避 *(linger avoiding)* 戦略だけを考慮すべきだと主張している．これは技術的な理由のためである．居残り回避戦略とは，秘密を復元した場合は直ちにプロトコルから離れるという戦略のことであり，もし居残り回避でない戦略が他のプレイヤーの戦略に対する最適反応である場合，それを居残り回避にした戦略もまた最適反応になる．複数の最適反応が存在すると，1 つの戦略が狭義 Nash 均衡であることを主張できなくなる．そのため，居残り回避戦略の中から狭義 Nash 均衡の戦略を探すべきだと主張しているのである．

狭義 Nash 均衡を議論する際には，上記の問題が必ず出てくる．Fuchsbauer ら [4] は，計算量的な狭義 *Nash* 均衡を導入し，議論しているが，別の方法で上記の問題に対処している．

3.5 純合理性による遂行

Micali と shelat [11] は，弱支配戦略の逐次除去によって残った任意の戦略の組み合わせが，望ましい性質を持つことを保証するような均衡概念を考えた．この概念が，Nash 均衡や狭義 Nash 均衡よりも望ましいと考えられるのは，他のプレイヤーに対する信条を考慮しなくていい点である．Nash 均衡を議論する際は，他のプレイヤーがその戦略に従っているという仮定をしている．つまり，自分の合理性だけでなく，他のプレイヤーに対する信条にも依存していると言える．一方で，Micali と shelat が考えた概念では，他のプレイヤーに対する信条は考慮せずに，望ましい結果が得られる．その意味で純合理性によって遂行可能な均衡概念なのである．

彼らは，この均衡を達成するプロトコルを提案しているが，通信路に対して強力な仮定を必要とし，また，$(2,2)$ 閾値型秘密分散だけを考えており，n 人プロトコルへの一般化が可能かどうかは不明である．

4 不可能性に関する既知の結果

4.1 ラウンド数

Halpern と Teague [6] は，復元フェーズのラウンド数があらかじめ固定されてあるプロトコルでは，安定的な均衡をもつ合理的な秘密分散は実現できないことを示した．例えば，r ラウンドでプロトコルが終了するとしよう．このとき,「シェアを出さない」ことは,「シェアを出す」ことを弱支配するため，悪い結果を導かない．そのため，r ラウンド目では，シェアを出さなくてもよいことになる．そうすると，実質的に $r-1$ ラウンド目が最終ラウンドと考えられる．しかし，同様に考えていくと，$r-1, r-2, \ldots, 1$ とすべてのラウンドでシェアを出さなくてもよいことになる．この議論は，時間を遡るように行われるため，逆向き帰納法 *(backward induction)* と呼ばれている．ただし，この議論は，ラウンド数 r があらかじめ固定されている場合だけに適用できるため，ラウンド数が確率的に決まる

プロトコルには適用されない．

ラウンド数の下界は，Asharov と Lindell [2] の不可能性の議論の中で導出されている．これについては 4.3 節 および 4.4 節で述べる．

4.2 シェアサイズ

Kol と Naor [9] は，シェアサイズが有限の場合，プロトコルに暴露点がない限り，居残り回避戦略は Nash 均衡にならないことを示した．暴露点とは，すべてのプレイヤーが認識可能な時点であり，その時点ではあるプレイヤーが秘密を復元しておらず，その時点以降はすべてのプレイヤーが秘密を復元している，そのような点である．暴露点があるプロトコルは問題であると考えられる．なぜならば，暴露点においてプレイヤーたちは何も行動しないことが尤もらしいと考えられるからである．しかし，暴露点以降ではすべてのプレイヤーが秘密を復元するため，暴露点においても何らかの情報が明らかにされないとおかしい．

Kol と Naor [9] は上記の不可能性結果を，合理的な秘密分散よりも一般的な合理的な多者間計算の結果として示している．合理的な多者間計算では，各プレイヤーが入力を保持しており，各プレイヤーは n 入力関数 f に対して，$f(x)$ を手に入れたいと考えている．ここで，$x = (x_1, \ldots, x_n)$ であり，x_i はプレイヤー i の入力を表す．上記の不可能性の結果をより一般的に言い換えると，非定数関数 f が有限定義域の場合，プロトコルに暴露点がない限り，居残り回避戦略は Nash 均衡にならない，となる．

4.3 効用関数との依存性

多くの既存プロトコル [6, 1, 5, 8, 9, 4] では，プロトコルの設計時に各プレイヤーの効用関数の具体的な値を知る必要がある．しかし，効用の具体的な値というのは公の知識ではないため，全プレイヤーに関して正確に知ることは難しいと考えられる．Asharov と Lindell [2] は，プロトコルと効用関数の依存関係について研究を行った．ここで，U^+ を秘密の復元を独占したときの効用，U^f を他のプレイヤーが間違った秘密を復元したときの効用を表すものとする．このとき，U^+ や U^f の値とプロトコルとの関係性を調べた．そして，各プレイヤーについて任意の U^+ (または U^f) に対して正しく動作するプロトコルのことを U^+ 独立 (または U^f 独立) なプロトコルと呼ぶ．

Asharov と Lindell [2] は，合理的な秘密分散の性質と，通常の暗号学的な安全性との関係を明らかにした．具体的には，$n = 2$ のとき，U^+ 独立なプロトコルは，悪意のある敵対者に対して（通常の暗号学的な意味で）完全公平性を達成し，また，U^f 独立なプロトコルは，悪意のある敵対者に対して正しさを達成することを示した．直観的に説明すると，U^+ 独立なプロトコルとは，秘密を独占できたときの効用がどんなに大きくても，プレイヤーとしてはプロトコルに従い，秘密を全員で復元することがよいと考えるプロトコルである．このようなプロトコルにおいては，公平性を破ることは無視できる確率でしかできないのである．また，U^f 独立なプロトコルとは，相手に間違った出力をさせたときの効用がどんなに大きくても，プレイヤーはプロトコルに従うことがよいと考える．このようなプロトコルにおいては，間違った出力をさせることは無視できる確率でしかできないのである．

上記の U^+ に関する結果と，Cleve の古典的結果である，非同時通信路における公平なコイン投げの不可能性 [3] を利用すると，非同時通信路において，$n = 2$ の場合，U^+ 独立なプロトコルは存在しないことがわかる．Asharov と Lindell は，この不可能性を，同時通信路に拡張している．彼らは，U^+ 独立性の不可能性を示すために，復元に必要な平均ラウンド数の下界が効用の具体的な値に依存することを示している点に注意したい．つまり，この結果は復元のためのラウンド数の下界を導出しているといえる．そして，この結果から，$n = 2$ の場合，復元のための平均ラウンド数を，効用の値に依存しない独立した値にすることが不可能であることがわかる．

また，既存のプロトコルのいくつか (例えば [5, 9]) は，同時通信路において U^f 独立であるが，非同時通信路においてそのようなプロトコルが存在するか否かは不明であった．Asharov と Lindell は，$n = 2$ の場合，非同時通信路においても U^f 独立は不可能であることを示した．

4.4 結託耐性

Asharov と Lindell は $n = 2$ の場合について様々な不可能性を示しているが，この場合の不

可能性に帰着させることで，結託耐性 $\lceil \frac{n}{2} \rceil$ の場合の不可能性も示すことができる．つまり，結託耐性 $\lceil \frac{n}{2} \rceil$ のプロトコルで U^+ 独立なものは，同時通信路であっても存在しない．(復元のための平均ラウンド数に関しても，結託耐性 $\lceil \frac{n}{2} \rceil$ のプロトコルでは効用の値に依存しないものは存在しないことがいえる．)

4.5 補助入力

通信路に対する仮定として，同時同報通信路は暗号学的にも非常に強力な仮定である．そのため，非同時同報通信路を仮定する方が望ましいが，この通信路を仮定して提案されたプロトコル [8, 9, 4, 7] では，秘密に対する補助入力が問題となる．これらのプロトコルでは，各プレイヤーは秘密の候補となるものがまず与えられ，その時点ではそれが秘密かどうかは確定できず，その後，それが実際に秘密であったという事実が判明するという共通の性質を持つ．そのため，プレイヤーが秘密に対する事前情報を持ち，秘密の候補から本当の秘密を特定することができる場合，これらのプロトコルは正しく動作しないのである．非同時同報通信路におけるこの性質は避けられないものであるということも示されている [2].

5 問題の定式化に関する議論

合理的な秘密分散という問題の定式化について，いくつものバリエーションが存在する．また，どのような定式化が妥当なのかという問題は未だに議論の余地がある．

プレイヤーの選好は，まず秘密を復元したい，そしてより少ない人数で復元したいというものである．この制限から，ゲームの結果に対する選好の順序関係が決まる．最も好ましいのが自分 1 人で復元したときであり，その次が自分を含む 2 人で復元したときと続く．ただし，自分が復元できなかった場合に，他のプレイヤーの結果に対してどのような選好を持つかは定まっていない．また，自分を含む複数人が復元したとき，どのようなプレイヤーが復元することが望ましいのかも定まっていない．そして，この選好をどのような効用関数として表すべきかも定まっていない．既存プロトコルの多くは，効用関数に対して比較的少ない制限さえあれば動作を保証できるものが多い．そのため，選好や効用関数で不確定な部分があったとしても動作するのである．例えば，Fuchsbauer ら [4] のプロトコルでは，$U^+, U, U^-, U^{\text{random}}$ の 4 つの値がある関係を満たしていればプロトコルが正しく動作する．ここで，U^+ は，自分 1 人で復元したときの効用であり，U は，自分を含む複数人が復元したときの効用，U^- は，自分が復元できなかったときの効用である．また，U^{random} は，プロトコル実行前にランダムに秘密を推測したときに得られる期待効用である．これらの値に対して，$U^+ > U > U^-$ そして $U > U^{\text{random}}$ という関係を満たす必要がある．この制約自体は，とても自然である．

Halpern と Teague [6] が最初に定式化した際は，各プレイヤーは，ゲームの結果から秘密が復元できたか否かを決めることができると仮定していた．Abraham ら [1] は，この仮定を排除するため，各プレイヤーはゲームの最後に復元した秘密を出力することにした．こうすると，秘密に関して部分情報だけを知っていたような場合にも対応できる．

4.5 節で述べたとおり，非同時通信路を仮定するプロトコルでは，各プレイヤーは本当の秘密であるか否かを特定できる情報を持たないことを仮定する必要がある．この事実に対応した問題の定式化として，Fuchsbauer ら [4] は，ゲームのはじめに秘密が一様ランダムに選ばれ，そのランダムな秘密を当てるゲームとして，合理的な秘密分散問題を定式化している．このような定式化は，最初の問題設定からするとやや不自然に見えるかもしれないが,「秘密を復元した」ということを一般的に定式化することの難しさを表しているとも言える．

Micali と shelat [11] は，プレイヤーの出力として「特定不能」を意味する “?” を許す場合を考えた．これは，プレイヤーが正しい秘密か否かが不明な場合，ランダムに秘密を推測するのではなく，“?” を出力する方が自然であるという考えにもとづいている．ただし，彼らは $n = 2$ の場合だけを考えているため，結果に対する選好の順序が完全に定まったが，一般の n の場合は，選好の順序は定まらない．

6 不可能性の回避

河内ら [7] は，非同時通信路において復元のための平均ラウンド数が効用の値と独立となるプロトコルを提案している．彼らのプロトコルは，

狭義 Nash 均衡の達成に成功しているが，結託耐性は $\lceil \frac{n}{2} \rceil - 1$ にとどまっている．この結託耐性は，Asharov と Lindell の不可能性の結果 [2] から，避けられないものであることがわかる．その意味で，このプロトコルの結託耐性は最適であるといえる．しかし，結託耐性が $\lceil \frac{n}{2} \rceil - 1$ であることは，問題を含むように思われる．以下で詳しく述べる．

6.1 河内ら [7] のプロトコル

彼らのプロトコルは以下の通りである．まず，$(\lfloor \frac{n}{2} \rfloor + 1, n)$ 秘密分散 S_1，$(\lceil \frac{n}{2} \rceil, n)$ 秘密分散 S_2，そして (n, n) の合理的な秘密分散 S_3 を用意する．分散フェーズでは，秘密 s' を S_1 で分散する．ただし，s' は確率 $1-\alpha$ で本当の秘密 s に等しく，それ以外の場合，ランダムな値に設定される．この α は，任意の小さな定数である．そして，S_2 を使って，s' が本物であるか否かという情報を秘密として分散させる．最後に，S_3 を使って，秘密 s を分散させる．復元フェーズでは，まず，S_1 のシェアを出すように求められる．ここで，$\lfloor \frac{n}{2} \rfloor + 1$ 個以上のシェアが出されたら，秘密 s' を復元できる．次に，復元した秘密が本物であるか否かを S_2 を使って確かめるのだが，最初のラウンドで n 個のシェアすべてが正しく出た場合に限り 2 ラウンド目に進むことにする．2 ラウンド目に進んだ場合，S_2 のシェアを出し，$\lceil \frac{n}{2} \rceil$ 個以上のシェアが出されれば，s' が本物であるか否かが判明する．本物であった場合はそこでプロトコル終了だが，そうでない場合，S_3 を使って s を復元する．しかし，S_3 で復元するラウンドに進むのは 2 ラウンド目で n 個のシェアがすべて正しく出た場合に限ることにする．つまり，全員が正しくシェアを出したにもかかわらず，偽物の秘密であった場合に限り，S_3 を使って s を復元するプロトコルを実行するのである．

6.2 結託耐性が小さいことの問題点

このプロトコルは，結託耐性 $\lceil \frac{n}{2} \rceil - 1$ の狭義 Nash 均衡を達成している．しかし，より望ましいように見える戦略が存在する．最初のラウンドで $\lfloor \frac{n}{2} \rfloor$ 個のシェアが出されたとき，それ以降のプレイヤーは自分のシェアを使えば，自力で秘密 s' を復元できるのである．その秘密は小さい確率 α で偽物ではあるものの，高い確率で本物であり，その秘密は最初の $\lfloor \frac{n}{2} \rfloor$ 人は手に入れることができないのである．つまり，全員で秘密を復元するよりも高い効用が得られると考えられる．この戦略は，プロトコルが狭義 Nash 均衡であることと矛盾するのだろうか．実際は矛盾していない．なぜならば，この戦略が実現するには，$n - \lfloor \frac{n}{2} \rfloor = \lceil \frac{n}{2} \rceil$ 人がプロトコルから逸脱する必要がある．しかし，ここでは結託耐性 $\lceil \frac{n}{2} \rceil - 1$ を考えるため，$\lceil \frac{n}{2} \rceil$ 人が逸脱する状況は考えないのである．

確かに矛盾しないとはいえ，上記の戦略はもっともらしいように思われる．つまり，これは，結託耐性 $\lceil \frac{n}{2} \rceil - 1$ という均衡概念が不十分であることを示した例といえる．その意味で，結託耐性は $n-1$ を達成することが望ましいといえる．しかし，定数ラウンド復元プロトコルで結託耐性 $n-1$ を達成するには，Asharov と Lindell の不可能性 [2] を回避する必要がある．

6.3 不可能性 [2] の回避方法

ここでは，効用関数にある仮定を追加することを考える．その仮定とは,「プレイヤーは偽物を復元することを非常に嫌がる」というものである．この仮定自体は自然なように思われる．また，既存研究においてこのような仮定は考えられていない．

上記の仮定を追加すれば，前節で示した問題が起きないことがわかる．最初のラウンドで $\lfloor \frac{n}{2} \rfloor$ 個のシェアが出されたとき，それ以降のプレイヤーは自分のシェアを使って秘密 s' を復元できるが，小さな確率 α で偽物である．偽物を復元することを非常に嫌がることを仮定しているため，それ以降のプレイヤーもシェアを出すことが最適な戦略である．

また，河内らのプロトコルにおいて S_1 を (n, n) 秘密分散，S_2 を (n, n) 秘密分散に置き換える．すると，修正されたプロトコルは，上記で追加した仮定のもと，結託耐性 $n-1$ を達成することがわかる．修正プロトコルでは，まず，(n, n) 秘密分散 S_1 を復元する．n 人目のプレイヤーは，自分のシェアを出さなくとも s' を復元できるが，それが偽物であることを非常に嫌がるため，シェアを正しく出し，次のラウンドに進む．2 ラウンド目では，(n, n) 秘密分散 S_2 を使って，s' が本物であるか否かを確かめる．n 人目のプレイヤーは，自分のシェアを出さなくともそれを確認できる．しかし，n 人目のプレイヤーがシェアを出さなかった場合は，それ

が本物だったことを意味する．なぜなら，偽物であった場合は，正しくシェアを出すことで S_3 を利用するラウンドに進む必要があるからである．つまり，n 人目のプレイヤーが出さなかったとき，他のプレイヤーは s' が本物であることを認識できるのである．上記の議論は，プレイヤー 1 人での逸脱を考えているが，$n-1$ 人が結託して逸脱することを考えても同じ議論が適用できる．

参考文献

[1] I. Abraham, D. Dolev, R. Gonen, and J. Y. Halpern. Distributed computing meets game theory: robust mechanisms for rational secret sharing and multiparty computation. In E. Ruppert and D. Malkhi, editors, *PODC*, pages 53–62. ACM, 2006.

[2] G. Asharov and Y. Lindell. Utility dependence in correct and fair rational secret sharing. *J. Cryptology*, 24(1):157–202, 2011.

[3] R. Cleve. Limits on the security of coin flips when half the processors are faulty (extended abstract). In J. Hartmanis, editor, *STOC*, pages 364–369. ACM, 1986.

[4] G. Fuchsbauer, J. Katz, and D. Naccache. Efficient rational secret sharing in standard communication networks. In D. Micciancio, editor, *TCC*, volume 5978 of *Lecture Notes in Computer Science*, pages 419–436. Springer, 2010.

[5] S. D. Gordon and J. Katz. Rational secret sharing, revisited. In R. D. Prisco and M. Yung, editors, *SCN*, volume 4116 of *Lecture Notes in Computer Science*, pages 229–241. Springer, 2006.

[6] J. Y. Halpern and V. Teague. Rational secret sharing and multiparty computation: extended abstract. In L. Babai, editor, *STOC*, pages 623–632. ACM, 2004.

[7] A. Kawachi, Y. Okamoto, K. Tanaka, and K. Yasunaga. Rational secret sharing for non-simultaneous channels. *IEICE Technical Report*, IT2012(7):41–46, May 2012.

[8] G. Kol and M. Naor. Cryptography and game theory: Designing protocols for exchanging information. In R. Canetti, editor, *TCC*, volume 4948 of *Lecture Notes in Computer Science*, pages 320–339. Springer, 2008.

[9] G. Kol and M. Naor. Games for exchanging information. In C. Dwork, editor, *STOC*, pages 423–432. ACM, 2008.

[10] A. Lysyanskaya and N. Triandopoulos. Rationality and adversarial behavior in multi-party computation. In C. Dwork, editor, *CRYPTO*, volume 4117 of *Lecture Notes in Computer Science*, pages 180–197. Springer, 2006.

[11] S. Micali and A. Shelat. Purely rational secret sharing (extended abstract). In Reingold [14], pages 54–71.

[12] S. J. Ong, D. C. Parkes, A. Rosen, and S. P. Vadhan. Fairness with an honest minority and a rational majority. In Reingold [14], pages 36–53.

[13] R. Pass and A. Shelat. Renegotiation-safe protocols. In B. Chazelle, editor, *ICS*, pages 61–78. Tsinghua University Press, 2011.

[14] O. Reingold, editor. *Theory of Cryptography, 6th Theory of Cryptography Conference, TCC 2009, San Francisco, CA, USA, March 15-17, 2009. Proceedings*, volume 5444 of *Lecture Notes in Computer Science*. Springer, 2009.

[15] A. Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979.

[16] M. N. Wegman and L. Carter. New hash functions and their use in authentication and set equality. *J. Comput. Syst. Sci.*, 22(3):265–279, 1981.