数理解析研究所講究録
906巻 1995年 244-248

情報を意図的に改変する可能性のある通信路における安全な通信プロトコルのLFKNプロトコルによる改良について

坂本 直志
一橋大学 情報処理センター
sakamoto@cc.hit-u.ac.jp

概要

情報を送受する通信路の振舞いが保証されないような状況での通信を考える。このような通信路に対して、果たして通信自体が可能なのだろうか？

[坂本93]ではこのような仮定に対し、安全な通信とは情報が改変されて伝わることがないことと捉え、通信路のモデルを計算機として考えた場合、

1. 能力的に通信路と送信者が等価なら安全な通信は存在しないことを示し
2. また、計算時間が確率的多項式時間で制限されるなら、安全な通信があることを示した。

但し、このプロトコルは送信者、受信者に莫大な計算量が必要となる。

本論文では受信者の計算量を送信者と計算量が異なることがまだ示されてない程度まで減らした安全な通信を提案した。但し、検証者なる送信者と同等程度の計算量を持つものが新たに必要となった。

1 はじめに

[坂本93]では従来の暗号理論と枠組の違う、通信路が故意に情報を伝えなかったり改変した情報を伝えたりするかもしれない、悪意のある存在ととらえた上での通信の安全性について議論し、ある条件下では安全なプロトコルが存在することを構成的に与えた。

従来の古典的な暗号理論などのとらえ方では、通信が安全であるとは、情報が正しく送られることと、その情報が洩れないことの2つを意味するが、ここでいう安全性は、前者の条件を実現することのみに焦点をしぼった。

悪意を持つ通信路において通信を行う場合、通信の結果として次の5つの場合が考えられる。

1. 受信者は情報を全く受け取らない。
2. 受信者は改変された情報を受け取り、それが改変された情報であるということには気づかない。
3. 受信者は改変された情報を受け取るが、それが改変された情報であることに気づく。
4. 受信者は改変されない正しい情報を受け取る。
5. 受信者は改変されない正しい情報を受け取るが、それが改変された情報であると誤認する。

このうち 4 はいちばん望ましい状況、2 はいちばん望ましくない状況であり、1、3、5 はその中間である。我々は、受信者の不利益になる場合として 2 だけを考えることとし、2 が起こらないことを安全な通信の条件とする。ただし、通信路において何も情報の改変が行われなかったのに 5 の条件が成り立つと、受信者が何も情報を受けとらない状態が自明な安全な通信になってしまうが、これは通信とはみなせないので、安全性とは別に改変が行われなかった時は 4 の条件が高い確率で成り立つようなプロトコルを考えることとする。

[坂本93]では、通信路のモデルとして、通常の計算機のモデルを用い、情報を伝達するのに必要な時間を制限することにより通信路に条件を付加した。通信路を通信の時に与えるパラメータに対して確率的多項式時間限定とすると、送信者と受信者が決定性二重指数時間程度の計算能力を持つことで安全な通信が行えることを示した。通信路と送信者が同等の計算能力を持つと、送信者を通信路がシミュレートできるため、通信路の意図した情報を受信者に受信させることが可能になるので、通信路と送信者の計算能力は真に異なることが必要であるが、受信者について大きな計算量が必要か否かは未解決であった。

最近示された通信のプロトコルの計算量の結果として、Interactive Proof の結果がある。Interactive Proof は証明者と検証者が互いに通信を行い、人力がある集合に入ることを証明者が検証者に納得させるゲームである。検証者が確率的多項式時間の計算の制限を受けている場合に検証者が納得可能な集合の複雑さが、近年 LFKN プロトコルというプロトコルが開発されたことにより、証明者が1人の場合は決定性多項式領域の複雑さ、証明者が2人以上で互いに独立している場合は非決定性指数時間の複雑さであることが示された。[Sha90],[BFL90]

本論文では、この Interactive Proof の結果を利用し、送信者と受信者とが Interactive Proof を行うこと

により受信者単独でする計算よりも複雑な計算を可能にし、受信者の計算量を減らした安全なプロトコルを提案した。但し、通信路の計算量を決定性多項式時間と仮定すると、1 prover の Interactive Proof の結果を利用する時に安全な通信を保証するには決定性多項式領域の複雑さが真に決定性多項式時間の計算量とが異なることを保証しなければならないが、これは計算量理論において重要な未解決問題であり、そのため、証明者を1人としたプロトコルを利用した安全なプロトコルは構成できなかった。本論文で提案したプロトコルで用いたプロトコルは、決定性多項式時間と真に異なっていることが示されている非決定性指数時間の計算が可能な 2 prover の Multiple-Prover の Interactive Proof のプロトコルである。そのため、受信者の計算量は確率的多項式時間まで落ちたが、送信者の他に、同等の高い計算能力を持った送信者と確率的に独立な検証者が必要になっている。

2 基本的な定義

Σ を 2 文字 0,1 よりなるアルファベットとし、'?' を Σ に含まれないある文字とする。Σ の文字列の連接演算を $\cdot$ で表し、空文字列を λ で表す。$\Sigma^0 = \{\lambda\}$, $\Sigma^n = \Sigma^{n-1} \cdot \Sigma$ とし、$\bigcup_{i\geq 0}\Sigma^i$ を Σ^* で表す。文字列のあいだの長さ優先の辞書式順序を $<_{\mathrm{can}}$ で表す。Σ^* の元 s に対して $t = s+1$ とは $<_{\mathrm{can}}$ に対して s より大きい最小の Σ^* の元とする。Σ^* の要素の列 $x_1, x_2, \ldots, x_k$ を Σ^* のある要素 $\langle x_1, \ldots, x_k\rangle$ で表現する方法を 1 つ決めておく。

文字列の長さ l が暗黙に決まっている場合に、数 n に対し、$\#n$ は n の Σ 上の表現で長さが l の文字列を表す。

3 プロトコルに関する定義

本節では、プロトコルとそれによる通信に関する基本概念について定義する。

プロトコルのモデルとして、通信の回数の数だけ用意された通信用 Turing 機械の列を用い定義する。通信用 Turing 機械は、通常の Turing 機械にさらに入力チャンネルという読み込み専用のテープヘッドと出力チャンネルという書き込み専用のテープヘッドを一対以上持ち、他の Turing 機械とテープを入力チャンネルと出力チャンネルの対で共有し、データを送受する。

[定義 3.1] 送信者は通信用 Turing 機械の列で $\boldsymbol{S}(j) = \langle S_1, S_2, \cdots\rangle$ で表す。j は送信すべき情報である。各 S_i は入力チャンネルを 1 つ持ち、S_1 から S_{i-1} までに入力チャンネルに入力された値と入力チャンネルの内容により、出力チャンネルに出力する。

[定義 3.2] 受信者は通信用 Turing 機械の列で $\boldsymbol{R}(n) = \langle R_1, R_2, \cdots\rangle$ で表す。n は通信パラメタである。各 R_i は入力チャンネルと出力チャンネルを 2 つずつ持ち、R_1 から R_{i-1} までに入力チャンネルに入力された値と入力チャンネルの内容により、出力チャンネルに出力する。

なお、受信者はプロトコルの最後の通信用 Turing 機械は出力を持ち、'?' か受信した情報を出力する。

[定義 3.3] 検証者は通信用 Turing 機械の列で $\boldsymbol{V} = \langle V_1, V_2, \cdots\rangle$ で表す。各 V_i は入力チャンネルを 1 つ持ち、V_1 から V_{i-1} までに入力チャンネルに入力された値と入力チャンネルの内容により、出力チャンネルに出力する。

[定義 3.4] 通信路は通信用 Turing 機械の列で $\boldsymbol{C} = \langle C_1, C_2, \cdots\rangle$ で表す。各 C_i は入力チャンネルと出力チャンネルを 2 つずつ持ち、C_1 から C_{i-1} までに入力チャンネルに入力された値と入力チャンネルの内容により、出力チャンネルに出力する。

honest な通信路 $\boldsymbol{C}^*$ とは入力チャンネル $I_{\boldsymbol{A}}, I_{\boldsymbol{B}}$ と出力チャンネル $O_{\boldsymbol{A}}, O_{\boldsymbol{B}}$ に対して、通信相手 $\boldsymbol{A}, \boldsymbol{B}$ とは $I_{\boldsymbol{A}}, O_{\boldsymbol{A}}$、$I_{\boldsymbol{B}}, O_{\boldsymbol{B}}$ でそれぞれテープを共有している時、$I_{\boldsymbol{A}}$ で読み込んだデータを $O_{\boldsymbol{B}}$ に、$I_{\boldsymbol{B}}$ に読み込んだデータを $O_{\boldsymbol{A}}$ に出力する通信路を指す。

[定義 3.5] $\boldsymbol{S}, \boldsymbol{C_S}, \boldsymbol{R}, \boldsymbol{C_V}, \boldsymbol{V}$ により構成される通信プロトコルを $(\boldsymbol{S}(j); \boldsymbol{C_S}; \boldsymbol{R}(n); \boldsymbol{C_V}; \boldsymbol{V})$ と表し、$(\boldsymbol{S}(j); \boldsymbol{C_S}; \boldsymbol{R}(n); \boldsymbol{C_V}; \boldsymbol{V}) = k$ は通信の結果受信者が k を出力したことを示し、$\Pr[(\boldsymbol{S}(j); \boldsymbol{C_S}; \boldsymbol{R}(n); \boldsymbol{C_V}; \boldsymbol{V}) = k]$ はプロトコルに確率的な計算が使われる時、通信の結果受信者が k を出力する確率を表す。全て決定的な計算が行われる場合でも確率は 0 か 1 の値で定義されるものとする。

このようなプロトコルに対して安全性を定義する。

[定義 3.6] 検証者つきの通信プロトコル $\langle \boldsymbol{S}, \boldsymbol{R}, \boldsymbol{V}\rangle$ が条件 X に対して安全であるとは、

1. honest な通信路 $\boldsymbol{C}^*_{\boldsymbol{S}}, \boldsymbol{C}^*_{\boldsymbol{V}}$ に対して任意の $c > 0$, n, $1 \leq j \leq n$ に対して
$$\Pr[(\boldsymbol{S}(j); \boldsymbol{C}^*_{\boldsymbol{S}}; \boldsymbol{R}(n); \boldsymbol{C}^*_{\boldsymbol{V}}; \boldsymbol{V}) = j] > 1 - \frac{1}{n^c}.$$
2. 条件 X を満たす任意の通信路 $\boldsymbol{C_S}, \boldsymbol{C_V}$ と $c > 0$ に対して十分大きい任意の n と任意の, $1 \leq j \leq n$, に対して
$$\Pr[(\boldsymbol{S}(j); \boldsymbol{C_S}; \boldsymbol{R}(n); \boldsymbol{C_V}; \boldsymbol{V}) = j \mid (\boldsymbol{S}(j); \boldsymbol{C_S}; \boldsymbol{R}(n); \boldsymbol{C_V}; \boldsymbol{V}) \neq ?] > 1 - \frac{1}{n^c}$$

4 プロトコルと証明

この節では条件を満たすプロトコルを示し、条件を満たすことを証明する。

まず通信路の条件に関して必要な定義を述べる。

[定義 4.1] 通信路 $C = \{C_1, C_2, \cdots\}$ が多項式時間限定であるとは、ある多項式 p が存在し、任意の通信に関して、各 $C_1, C_2, \cdots$ が出力を出すのに各入力チャンネルに入力される文字列のうち最大の長さ n に対して、出力する時間が $p(n)$ 時間で抑えられることをいう。

次に本研究で提案するプロトコルに使用する集合を定義し、その性質を調べる。

[定義 4.2] $Ind(n,i)_{m,l}$ は次のような帰納的手順で作られた集合である。

- $m = 1$ のとき
  $Ind(n,i)_{1,l}$ は、数 l の長さ n の encoding と、長さ n の辞書式順序で l 番目の文字列 s の連接である $\langle \#l, s\rangle$ 1 つからなる集合である。
- $m > 1$ のとき
  i) $V = \{\langle \#p, s\rangle \mid 1 \le p \le m-1,\ s \in \Sigma^n\}$ に対して $u, v \in V$ が隣接しているとは、ある $k(1 \le k \le i)$ が存在し、Turing 機械 M_k に 0^n と u を入力し、2^n 時間シミュレートした時、v を出力することであると定義する。
  V の要素を頂点と呼び、u と v が上の意味で隣接している時は u から v へ辺が出ているという。互いに隣接しないとは、u と v も、v と u も隣接していないことをいう。
  ii)

$$\begin{aligned} W_1 &= Ind(n,i)_{m-1,1}, \\ W_2 &= Ind(n,i)_{m-1,2}, \\ &\vdots \\ W_{i+1} &= Ind(n,i)_{m-1,i+1} \end{aligned}$$

  とし、

$$\max_{\substack{\langle \#num, s\rangle \in W_j \\ (1 \le j \le i+1)}} \{s\} + 1$$

  を t とする。
  $s \in \Sigma^n|_{\ge t}$ に対して $\langle \#m, s\rangle$ で、$Ind(n,i)_{m,1}, \cdots, Ind(n,i)_{m,l-1}$ に含まれていず、ある j に対して W_j の全ての要素と $\langle \#m, s\rangle$ が互いに隣接していない最小の s に対して $Ind(n,i)_{m,l} = W_j \cup \langle \#m, s\rangle$ とする。

このようにして定義した $Ind(n,i)_{m,l}$ には次のような性質がある。

[補題 4.3] $\langle \#p, s\rangle \in Ind(n,i)_{m,l}$ に対して、

$$\frac{(p-1)(p-2)}{2}i^2 + (p-2)^2 i + (p-1)(l+i) + 1 \le s \le \frac{p(p-1)}{2}i^2 + (p-1)^2 i + pl$$

(証明) $Ind(n,i)_{m,l}$ に含まれる $\langle \#p, s\rangle$ で取り得る最大の s の番号を $S_{p,l}$ と置く。

$p = 1$ の時は

$$S_{1,l} = l \tag{1}$$

となるのは明らか。

まず、$S_{p,1}$ について考えると、s の取り方から、$Ind(n,i)_{p-1,1}, \cdots, Ind(n,i)_{p-1,i+1}$ の中で取り得る最大の値 $S_{p-1,i+1}$ よりも大きくなるので、

$$S_{p-1,i+1} + 1 \le s \tag{2}$$

となる。

各 $W_j = Ind(n,i)_{p-1,j}$ と隣接する点の数は $|W_j| = p-1$ より W_j から出ている辺は $(p-1)i$ 本で、$W_1, \cdots, W_{i+1}$ から出る辺の総数は $(p-1)i(i+1)$ 本である。よって、$(p-1)i(i+1)+1$ 個頂点がある場合は少なくとも一つの頂点はどの W_j からも辺が入っていない。一方、一つの頂点からは i 本しか辺が出ないので、ある W_j とは互いに隣接していないことになる。つまり、

$$S_{p-1,i+1} + 1 \le s \le S_{p-1,i+1} + (p-1)i(i+1) + 1 \tag{3}$$

要するに

$$S_{p,1} = S_{p-1,i+1} + (p-1)i(i+1) + 1 \tag{4}$$

である。この手続きでは $\#p$ の付く文字列は 1 つ、番号の小さい $Ind(n,i)_{p-1,j}$ も 1 しか消費しないので、$S_{p,2}$ を考える時は、W_j として用意する集合は $Ind(n,i)_{p,1}$ で使われたものを 1 つ除いて、$Ind(n,i)_{p-1,j}$ を $i+1$ 個用意し、文字列も同様に 1 つ用意すればいいので、$S_{p,2} = S_{p-1,i+1+1} + (p-1)i(i-1) + 1 + 1$ つまり、

$$S_{p,l} = S_{p-1,i+l} + (p-1)i(i+1) + l \tag{5}$$

1式、5式より

$$\begin{aligned} S_{p,l} &= S_{p-1,l+i} + (p-1)i(i+1) + l \\ &= S_{1,l+(p-1)i} + \sum_{q=1}^{p-1} qi(i+1) + l + (p-q-1)i \\ &= l + \frac{p(p-1)}{2}i^2 + (p-1)l + (p-1)^2 i \\ &= \frac{p(p-1)}{2}i^2 + (p-1)^2 i + pl \end{aligned}$$

求めた $S_{p,l}$ により、

$$S_{p-1,l+i} + 1 \le s \le S_{p,l}$$

を得る。 □

[補題 4.4] n に対して $Ind(n,i)_{m,l}$ は $\mathrm{DTIME}(2^{n^{O(1)}})$ に属する。

(証明) 省略 □

[補題 4.5] $\mathrm{ex}(0)=1, \mathrm{ex}(n)=2^{\mathrm{ex}(n-1)}$ とする。

任意の多項式時間限定 Turing 機械 M に対して、有限の場合を除いて全ての n に対して、n を越えない最大の $\mathrm{ex}(j)=N$ となる N に対して $\langle \#p,s\rangle \in Ind(N,N)_{N,1}$ を入力した時、N の多項式時間の計算について、$q\neq p$, $\langle \#q,t\rangle \in Ind(N,N)_{N,1}$ となる $\langle \#q,t\rangle$ を出力しない。

(証明) Turing 機械のインデックスを k, この Turing 機械の実行時間を抑える多項式を $poly(\cdot)$ とする。

そのとき、ある、$k<N$, $poly(N)<2^N$ となる N に対して、$M_k(\langle \#p,s\rangle)=\langle \#q,t\rangle$ なる $\langle \#p,s\rangle, \langle \#q,t\rangle \in Ind(N,N)_{N,1}$ が存在したとする。しかし、そのような $\langle \#p,s\rangle, \langle \#q,t\rangle$ は $Ind(N,N)_{N,1}$ の定義により隣接することになり、$Ind(N,N)_{N,1}$ に含まれないので矛盾である。 □

送信者を $\boldsymbol{S}$, 受信者を $\boldsymbol{R}$, 検証者を $\boldsymbol{V}$, 送信者と受信者間の通信路を $\boldsymbol{C_S}$, 受信者と検証者間の通信路を $\boldsymbol{C_V}$ とし、Ind を利用したプロトコルを図 1 に示す。

[定理 4.6] 1のプロトコルは通信路が決定性多項式時間限定であり、2 つの通信路が通信ができない場合に安全である。

(証明) LFKN プロトルに入る前では、Ind の性質より、任意の通信路に対して、有限の場合を除いて Ind の集合に属する要素から、他の要素は計算できないので、次の 2 つの

1. 正しく情報を送る
2. 受けとったものと異なる情報を送る

場合があるが、異なる情報を送った場合は必ず Ind に含まれない。

さて、LFKN プロトコルは Interactive Proof なので、次の性質に従う。

1. 入力 x が L に含まれる時、任意の c に対してある証明者が存在して、検証者は $x\in L$ を $1-1/|x|^c$ 以上の確率で納得する。
2. 入力 x が L に含まれない時、任意の c と任意の証明者とに対して、検証者は $x\in L$ は $1/|x|^c$ 以下の確率でしか納得しない。

この性質により、受信者が受けとった $\langle \#p,s\rangle$ に対して、$\langle \#p,s\rangle \in Ind(N,N)_{N,1}$ であるものに対しては正しい通信を実行した時だけ $\langle \#p,s\rangle$ を受けとるが、$\langle \#p,s\rangle \notin Ind(N,N)_{N,1}$ であるものに対してはどのような通信を実行しても低い確率でしか $\langle \#p,s\rangle$ を受けとらない。

よって、改変された情報については、有限の場合を除き全てのパラメータに対して $\langle \#p,s\rangle \notin Ind(N,N)_{N,1}$ であるものだけを受けとるので、改変された情報を受けとる確率は低い。 □

5 まとめ

前回の論文に対して受信者の計算量を減らしたプロトコルを提案したが、通信路は決定性の振舞いに制限され、高い計算能力を持つ検証者なる第三者が必要になり、目的は果たしたが、果たして改良になったかどうかはいろいろ評価があるかも知れない。

根本的に検証者をなくすなどのこれ以上の改良は P $\neq$ PSPACE が証明されるなどの計算量理論の発展を待たなければならない。

今後は通信路が確率的な振舞いをする場合の分析が必要であろう。

参考文献

[ALM+92] S. Arora, C. Lund, R. Matwani, M. Sudan, and M. Szegedy. On the intractability of approximation problems. *Proc. 33st FOCS*, pp. 14–23, 1992.

[BDG88] J. L. Balcázar, J. Díaz, and J. Gabarró. *STRUCTURAL COMPLEXITY I*. Springer-Verlag Berlin Heidelberg, 1988.

[BDG90] J. L. Balcázar, J. Díaz, and J. Gabarró. *STRUCTURAL COMPLEXITY II*, chapter 6 Bi-Immunity and Complexity Cores. Springer-Verlag Berlin Heidelberg, 1990.

[BF91] L. Babai and L. Fortnow. Arithemetization: a new method in structural complexity theory. *Computational Complexity*, Vol. 1, pp. 41–66, 1991.

[BFL90] L. Babai, L. Fortnow, and C. Lund. Nondeterministic exponential time has two-prover interactive protocoles (extended abstract). *Proc. 31st FOCS*, pp. 16–25, 1990.

[BGKW88] M. Ben-Or, S. Goldwasser, J. Kilian, and A. Wigderson. Multi-prover interactive proofs: How to remove the intractability assumptions. *Proc. 20th STOC*, pp. 113–131, 1988.

[BGS75] T. Baker, J. Gill, and R. Solovay. Relativizations of the $P=?NP$ question. *SIAM J. Compt.*, Vol. 4, pp. 431–442, 1975.

S	C_S	R	C_V	V
送信データを p とする。		パラメータを n とする n を越えない $\mathrm{ex}(m) = N$ となる数を N とする		
	$\leftarrow$	0^N を送信者に送る		
送られてきた文字列が 0^N 型で、 $N = \mathrm{ex}(m)$ なる数であれば、 $\langle \#p, s \rangle \in Ind(N, N)_{N,1}$ なる s を求め、$\langle \#p, s \rangle$ を送る	$\rightarrow$			
		送られてきた文字列の長さが $2N$ で、$\langle \#p, s \rangle$ 型の データなら、検証者に送る	$\rightarrow$	
				送られてきた文字列が $\langle \#p, s \rangle$ なら検証を以下行う

以下、通信路を介して 2 prover により $\langle \#p, s \rangle \in Ind(N, N)_{N,1}$ が正しいことを LFKN プロトコルによる Interactive Proof により受信者に納得させる。受信者は $\langle \#p, s \rangle \in Ind(N, N)_{N,1}$ を納得したら、p を受信データとして受けとる。

図 1: プロトコル

[BM88] L. Babai and S. Moran. Arthur-merlin games: a randomized proof system, and a hierarchy of complexity classes. *JCSS*, Vol. 36, pp. 254-276, 1988.

[GMR89] S. Goldwasser, S. Micali, and C. Rackoff. Knowledge complexity of interactive proof systems. *SIAM J. Comput.*, Vol. 18, pp. 186-208, 1989.

[LFKN90] C. Lund, L. Fortnow, H. Karloff, and N. Nisan. Algebraic methods for interactive proof systems. *Proc. 31st FOCS*, pp. 1-10, 1990.

[Pap83] C. Papadimitriou. Games against nature. *Proc. 24th FOCS*, pp. 446-450, 1983.

[Sha90] A. Shamir, *IP = PSPACE*. *Proc. 31st FOCS*, pp. 11-15, 1990.

[坂本 93] 坂本直志. 情報を意図的に改変する可能性のある通信路における安全な通信について. *IEICE*, Vol. J76-D I, No. 11, pp. 621-630, November 1993.