Criptografia e Teoria dos Jogos

Fábio Harada Kubo

Universidade Estadual de Campinas

Conteúdo

1. Introdução

2. Noções de Criptografia

3. Influência de Criptografia em Teoria dos Jogos

4. Conclusão

Introdução

Noções de Criptografia

MPC (Multi-Party Computation)

Problema:

- N agentes que querem calcular uma função $f(t_1, ..., t_N) = s$

MPC (Multi-Party Computation)

Problema:

- N agentes que querem calcular uma função $f(t_1, ..., t_N) = s$
- Agente i é responsável pela entrada t_i

MPC (Multi-Party Computation)

Problema:

- N agentes que querem calcular uma função $f(t_1, ..., t_N) = s$
- Agente i é responsável pela entrada t_i
- Objetivo: nenhum agente pode deduzir informações além do par (t_i, s)

MPC (Multi-Party Computation)

Problema:

- N agentes que querem calcular uma função $f(t_1, ..., t_N) = s$
- Agente i é responsável pela entrada t_i
- Objetivo: nenhum agente pode deduzir informações além do par (t_i, s)
- Probabilístico: $s = f(t_1, ..., t_N, r)$

MPC (Multi-Party Computation)

Problema:

- N agentes que querem calcular uma função $f(t_1, ..., t_N) = s$
- Agente i é responsável pela entrada t_i
- Objetivo: nenhum agente pode deduzir informações além do par (t_i, s)
- Probabilístico: $s = f(t_1, ..., t_N, r)$
- Múltiplas saídas: $(s_1, ..., s_N) = f(t_1, ..., t_N)$

MPC (Multi-Party Computation)

Problema:

- N agentes que querem calcular uma função $f(t_1, ..., t_N) = s$
- Agente i é responsável pela entrada t_i
- Objetivo: nenhum agente pode deduzir informações além do par (t_i, s)
- Probabilístico: $s = f(t_1, ..., t_N, r)$
- Múltiplas saídas: $(s_1, ..., s_N) = f(t_1, ..., t_N)$

Os Agentes:

- Honestos
- Honestos mas curiosos
- Maliciosos
- Adversário A que controla $k < n$ agentes

Segurança do MPC

Definição

Seja f uma função de n entradas e π um protocolo que calcula a função f. Dado um adversário A que controla um conjunto de agentes, defina $REAL_{A,\pi}(t)$ como a sequência de saídas dos agentes honestos resultante da execução de π no vetor de entrada t sob o ataque de A, com adição da saída de A. Similarmente, dado um adversário $A^{'}$ que controla um conjunto de agentes, defina $IDEAL_{A^{'},f}(t)$ como a sequência de saídas dos agentes honestos avaliado por um agente confiável no vetor de entrada t, acrescido da saída de A. Dizemos que π calcula com segurança f se, para todo adversário A, existe um adversário $A^{'}$ que controla os mesmos agentes em um modelo ideal, tal que, para qualquer vetor de entrada t, temos que a distribuição de $REAL_{A,\pi}(t)$ é "indistinguível"da distribuição de $IDEAL_{A^{'},f}(t)$.

Noções mais fraca de segurança

- Todos os agentes honestos recebem sua saída (Output Delivery)
- Justiça: se um agente recebe sua saída, todos os agentes honestos também recebem
- Corretude e Privacidade

Resultados existentes para MPC

- Assumindo que A é computacionalmente limitado e que existe canais seguros e um canal de broadcast seguro
  - $k < \frac{n}{2}$, todos os agentes honestos recebem sua saída
  - $k < n$, garante-se corretude e privacidade
  - $k < n$, e assumindo o uso de envelopes, garante-se justiça
- Assumindo que A não é computacionalmente limitado
  - Assumindo canais seguros, garante-se output delivery para $k < \frac{n}{3}$
  - Assumindo segurança na comunicação entre agentes e no broadcast, então é garantido output delivery para $k < \frac{n}{2}$ (possivelmente com erros!)
  - Assumindo envelopes, urnas e broadcast seguro, então para $k < n$ é garantido output delivery

Influência de Criptografia em Teoria dos Jogos

Jogos com mediador

Um jogo com mediador consiste em:

- N jogadores
- Cada jogador possui estratégias S_i e utilidades u_i
- Fase 1: Mediador escolhe um perfil de estratégias $s = (s_1, ..., s_n)$ de acordo com uma distribuição de probabilidades M
- Fase 2: Jogadores decidem se utilizam a estratégia definida pelo mediador ou não

Definição

Uma distribuição M é um equilíbrio correlacionado se para toda estratégia s no suporte de M, para qualquer jogador i e estratégia $s_i^{'}$, temos que:

$$U_i(s_i^{'}, s_{-i}|s_i) < U_i(s_i, s_{-i}|s_i)$$

onde $U_i(s_i^{'}, s_{-i}|s_i)$ é a utilidade esperada do jogador i, dado que ele opta pela estratégia $s_i^{'}$ após receber a recomendação s_i e todos os outros jogadores optam pela estratégia s_{-i},

Equilíbrio computacional

Jogos estendidos:

- Fase preliminar: jogadores podem-se comunicar em um modelo de comunicação
- Terminada a fase preliminar, o jogo original inicia

Como definir um equilíbrio adequado para esse caso?

- Todas as comunicações e cálculos são feitos em tempo polinomial
- A fase preliminar é baseada em um problema difícil de criptografia

Definição

Um equilíbrio computacional de Nash é um conjunto de estratégias $(x_1^*, ..., x_n^*)$, onde cada estratégia é eficiente em λ tal que para cada jogador i e estratégia alternativa eficiente x_i, temos que

$$u_i(x_i^*, x_{-i}^*) \geq u_i(x_i, x_{-i}^*) - \epsilon$$

K-Resiliência

Definição

Um perfil de estratégias independentes $(x_1^*, ..., x_n^*)$ é um k-resiliente equilíbrio de Nash de um jogo G, se para toda para todo jogador i que pertence a qualquer coalizão C, tal que $|C| \leq k$, e para toda estratégia alternativa x_C de membros de C, temos que:

$$u_i(x_C^*, x_{-C}^*) \geq u_i(x_C, x_{-C}^*)$$

- Qualquer desvio não é benéfico para jogadores fora da coalizão
- Ex ante: A conspiração só pode ser feita antes da ação do mediador M
- Interim: A conspiração pode ocorrer depois da ação do mediador

Como remover o Mediador utilizando MPC

Teorema

Se x é um k-resiliente equilíbrio correlacionado de um jogo especificado por uma função f, e π é um protocolo MPC (com output delivery) que calcula com segurança f contra uma coalizão de até k agentes não limitados computacionalmente, então executar π na fase preliminar leva a um jogo estendido k-resiliente com as mesmas utilidades de x.

Conclusão

Dúvidas?

Obrigado!