

C10 秘匿共通集合計算プロトコルを用いた就職活動支援システム“JHT”

香川 大介

1. はじめに

就職活動をする上で、友人と共通の志望企業が分かればその人と情報の共有や相談など就職活動に有益である。しかし、自分の志望企業のリストをホームページ上で公開すると共通の志望企業以外にも分かってしまう。

そこで、本研究では、[1]の手法を応用し、それぞれの志望企業を隠したまま、共通の志望企業のみを抽出するシステム”Job Hunting Together(JHT)”を構築する。

2. 提案方式

各ユーザが自分専用のサーバを運用している。それぞれクライアント、サーバの役割に分かれて、秘匿共通暗号計算プロトコルを用いて共通の志望企業を得る。

2.1 秘匿共通集合暗号計算プロトコル[1]

集合を多項式で表し、暗号文同士の加法、乗法が平文や秘密鍵なしで行える準同型暗号を利用し、共有集合を求める。

2.2 Job Hunting Together(JHT)実行例

二人の参加者クライアント(C)とサーバ(S)は企業名フォーマットに従ったテキストファイルを持つ。

Step1: Sは自分のサーバに接続 JHTSを起動させ、自分の志望企業リスト“S.txt”を入力する。

Step2: C は“JHTC”を起動させ、相手サーバのアドレス・ポート番号、自分の志望企業リストを次のように入力する。

address “noisy.cs.dm.u-tokai.ac.jp” port “1112” file “C.txt”

実行の結果の例を 図 1 に示す。

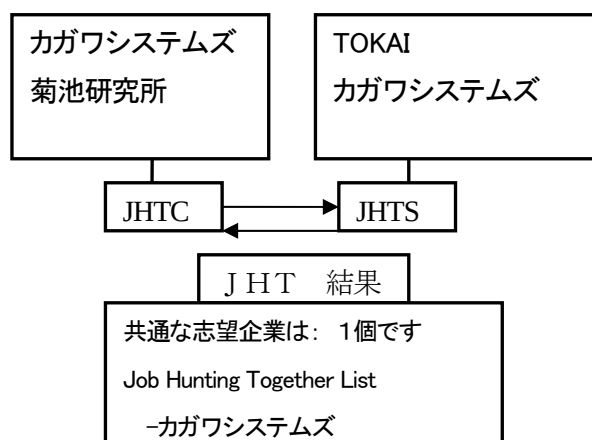


図 1: JHT 実行例

3. 評価実験

実データを本システムに適用し各被験者のプライバシーを犯すことなく共通志望企業をすべて求めることを実験目的とする。

3.1 共通志望企業の抽出

本研究の 5 人の被験者(A-E)に総当りの組み合わせで JHT を使用してもらい、Aについて共通志望企業の割合を図 2 に示す。共通志望企業の割合平均は 8.5%であった。志望企業数が 12 社程度あれば共通企業が 1 社でくる計算である。

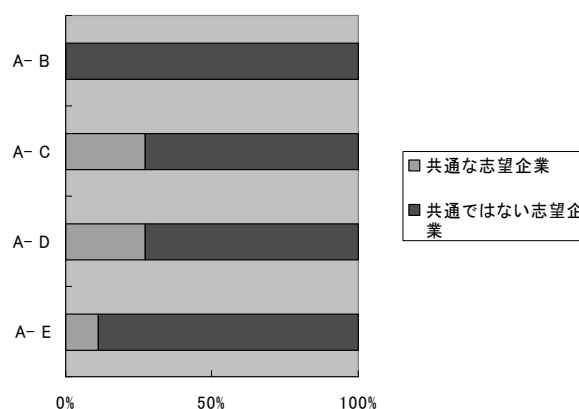


図 2: 抽出された共通志望企業の割合

4. おわりに

秘匿共通暗号計算プロトコルを用いることで、お互いに志望企業リストを秘匿したまま共通な志望企業の抽出が可能になった。本方式では全ユーザは正直に志望企業を入力することを前提にしている。今後の発展としては二者間ではなく一対多で使用できる拡張やより規模の大きな学科内の実験がある。

参考文献

[1] M. J. Freedman, K. Nissim, and B. Pinkas “Efficient Private Matching and Set Intersection”, EUROCRYPT, pp.1-19, 2004.