高度セキュリティPBL

28G23027

川原尚己

解析6

薬剤の購入履歴の統計的調査に関してりようできる．薬の名前をそのまま書いてしまっては，その人がどんな薬を購入したのかわかってしまい，プライバシの観点から好ましくない．そこで，Elgamal暗号によって，薬の名前を暗号化してからデータベースに格納し，統計処理を行う．最後にElgamal暗号の準同型性を用いて，結果を復号すると，プライバシを保護しながら統計的解析が行える．