SCIS 2022 2022 Symposium on Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics, Information and Communication Engineers

データベースの等結合後に加重合計を求める秘密計算プロトコル
A Secure Protocol for Computing Weighted-Sum after Equijoin of Databases

富田 潤一 * 紀伊 真昇 * 濱田 浩気 * 市川 敦謙 * 千田 浩司 *
Junichi Tomida Masanobu Kii Koki Hamada Atsunori Ichikawa Koji Chida

キーワード キーワード 秘密計算、2 パーティ計算、加重平均、等結合

あらまし

共通の ID 集合に属する ID 列を主キーとするデータベースを持つ２つのパーティが、その ID 列を用いてそれらのデータベースの等結合を行い、なんらかの合意された集計結果を計算するという秘密計算は様々な場面で需要があると考えられる。本稿では、ID に付随するデータが整数値であり、データベースの等結合後に片方の整数を重みとして、もう片方の数値列に対する加重合計を計算する効率的なプロトコルを提案する。すなわち、等結合後にそれぞれの整数値列をベクトルとみて内積を計算するということである。そのような計算ができると、二者間が持つデータベースを等結合して得られるデータベース上でクロス集計表を計算することが可能である。

* NTT 社会情報研究所, 東京都武蔵野市緑町３丁目９－１１,