摘要

分散ネットワークで、セキュア関数計算(Secure Multiparty Computation、 SMC)は、参加者によって常に必要だ。 入力の独立、計算の正確性と、入出力から計算された情報以外の関係者に明らかにされないのを確実にしている間、彼らは彼らの入力でのいくつかの関数を計算したがっている。 この論文では、私たちは電子入札、データベース、およびワイヤレスセンサネットワークのアプリケーションで、いくつかの特定の問題を目ざしている。 彼ら全員は、一般的なSMC問題に属しています。 これらの問題によって、私たちは前の結果より低い複雑度と強いセキュリティでソリューションを提案する。 具体的には、私たちの研究は以下の4つの部分で構成される：

1）私たちは、多商品のプライベートな入札などのアプリケーションで会うことができるセキュア両方ベクトル優位(Secure Two-party Vector Dominance、STVD)の問題を取り組む。一連の商品のために、アリスには、入札ベクトル$(a_1, a_2, \ldots, a_n)$がある、そして、ボブには、価格ベクトル$(b_1, b_2, \ldots, b_n)$がある。 優位関係 $\{a_i \geq b_i | i=1, \ldots, n\}$があれば、彼らはベクトルでプライバシーを守っている間、取引するでしょう。 STVDの前の結果は、正確性で厳しい議論を欠くか、機密情報を漏らすか、または悪意がある行為を防ぎ難い。 この論文では、私たちは加法的な準同形の暗号化に基づいて、準誠実なモデルのために、STVDプロトコルを提案する。 そして、私たちは、効率的なゼロ知識証拠による悪意があるモデルの安全なプロトコルになるようにそれを修繕する。

2）私たちはプライバシーを保護したセット交差（Privacy Preserving Set Intersection、PPSI）の問題を取り組む。 そこでは、Nパーティーが個人的なデータセットの交差以外のデータを全く知らない。 これは多くのアプリケーションで広く必要なタスクです。 私たちは加法的な準同形の暗号化に基づいて効率的なプロトコルを提案する。 敵手が準誠実であり、任意のパーティーを制御すると仮定しながら、プロトコルはまず第一に、構造される。 そして、そのプロトコルは、敵手の悪意がある行為に妨げるために広がられる。 参考文献「36」、「62」と「63」の結果との比較で、準誠実と悪意があるモデルでは、私たちのPPSIプロトコルは小さい計算と通信コストを達成する。

3）私たちは、Nパーティーで水平に分割されたデータベースのシナリオで、プライバシーを保護したタプルマッチング（Privacy Preserving Tuple Matching、PPTM）の問題を取り組む。 そのシナリオでは、各パーティーは割り当てられたタプルを持つ、そして、すべてのタプルには、同じセットの属性がある。 どんなパーティーも自身のプライバシーのために自身のタブルを公布しないという条件の下で、各パーティーは、すべての属性でタプルが相手のものに合うかどうか決定する。 私たちは、また、同じ技術で別の関連する問題(Privacy Preserving Threshold Attributes Matching、PPTAM)を解決することができるのを示します。中規模アプリケーションにおける実験で、私たちのPPTMプロトコルは、前の結果と比較するとおよそ80%の計算時間を節約する。 それには、数秒以内に転送することができる回線容量が増加する。 参考文献「62」の技術から解決策を派生することができるが、知っている限り、私たちは1番目にそのPPTAM問題を取り組む。 派生している解決策と比べて、私たちのPPTAMプロトコルはおよそ71.3%の計算時間と75%の通信時間を節約する。 私たちの2つのプロトコルが準誠実なモデルで安全であると立証される。

4）オリジネタのプライバシーとセンス領域プライバシーを含んで、私たちは無線のセンサネットワークにおける二つ衝突しているプライバシー問題を議論する。 ますます多くのセンサネットワークが人々が住んで、研究して、働いている場所で配備されるでしょう。 これらのセンサネットワークは、いつでもどこでも情報にアクセスするの便利を私たちにもたらす。 しかし、彼らは私たちの声、動き、または体温を監視する。 無線のセンサネットワークという状況で、人々は彼らのプライバシーに関するダイナミックな心配を持つ。 同時に、センサが目に見えなくなるだろうか、または自分たちのプライバシーのため隠される。 私たちは無線のセンサネットワークで人々の一般的な計画を提案する、それらが彼らの私的な活動のときに警戒するかどうかを意識する。 私たちの計画は、構造ブロックとして私たちの論文の最初の部分で達成するSTVDプロトコルを使用する。 また、それには、一般性と秘密性の特徴がある。