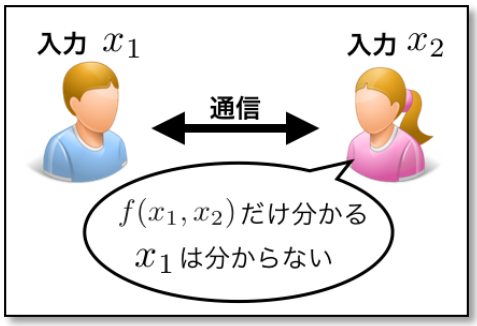
品川　和雅（Kazumasa Shinagawa）

所属（Domain）　情報科学領域（Domain of Computer and Information Sciences）
・博士後期課程社会インフラシステム科学専攻（Major in Society's Infrastructure Systems Science）

●研究テーマ（Research theme）
①カードベース暗号
（Card-based cryptography）
②秘密計算プロトコル
（Secure computation protocol）
③暗号理論の基礎理論
（Foundations of cryptography）

①気まずくならないように告白するにはどうしたらいいでしょう？実はカードを用いてお互いの気持ちを隠したまま「両想いかどうか」だけを明かすことができます。もし両想いでない場合でも、自分の気持ちを相手に知られることはありません。カードベース暗号は、このようなことをカードを使って実現する、パズル的な研究分野です。

How can you confess your feelings without making an embarrassing situation? Somewhat surprisingly, by using a deck of cards, it is possible to know whether you have feelings for each other while keeping your feelings hidden. Card-based cryptography is a puzzle-like research area that uses a deck of cards to compute some functions without revealing the secret inputs.

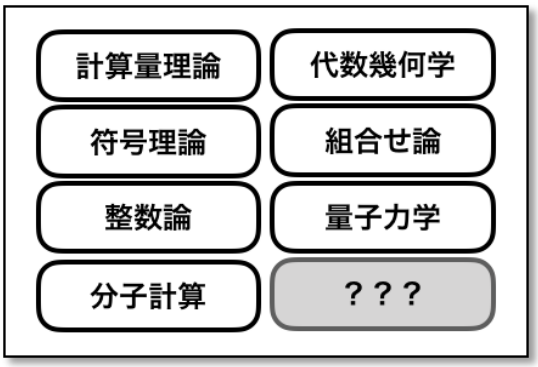


②秘密計算とは、入力情報を隠しながら分散計算を行う暗号技術です。上述のカードベース暗号は秘密計算の一種ですが、通常の秘密計算では情報通信によってプロトコルを実現します。数学的なトリックを用いて情報の秘匿性を達成しつつ、同時に有用な計算も行うことができます。

Secure computation enables us to compute a function without revealing the inputs. It is usually implemented by the use of communication over network although card-based cryptography uses cards. By using mathematical tricks, both the privacy of the inputs and the correctness of computation are achieved.

③暗号理論は上記のトピックを含む理論計算機科学の一分野です。特に暗号要素技術の実現可能性と不可能性を解明することは重要な課題です。また、異分野との融合による暗号理論の新しいフロンティアを開拓することも、暗号理論の適用範囲を拡大する上で重要です。

Cryptography is one of exciting research fields of theoretical computer science including the above topics. In particular, it is important to clarify the (in)feasibility of cryptographic primitives. It is also important to explore new frontiers of cryptography.



キーワード（Keyword）	暗号理論（Cryptography）秘密計算（Secure computation）
専門分野（Specialized Field）	暗号理論（Cryptography）
共同研究可能技術（Possible Technology of Cooperative research）	理論計算機科学（Computer science）数学（Mathematics）
関連論文・特許情報 website（Related articles･patent information）	https://info.ibaraki.ac.jp/Profiles/117/0011642/profile.html
研究設備（Research Facility）	
研究室URL（Lab. URL）	
E-mail	kazumasa.shinagawa.np92@vc.ibaraki.ac.jp