2019年度S1/S2　学術フロンティア講義　数理工学のすすめ
レポート問題（2019年5月9日）

縫田　光司（工学部計数工学科）

以下の問題の中から1問を選び解答せよ。

問1　AさんとBさんが、それぞれ知人10人の電話番号を持っているとする（「10人の電話番号を持っている」ことは互いに既に知っているものとする）。ここで、「Aさんの持つ電話番号とBさんの持つ電話番号のうち共通するもの」を秘密計算によって調べたい。そのために以下の手順を考える。

1. まずAさんとBさんは、以降の手順で用いる何らかの単射な関数H（単射とは、$m \neq n$であれば$H(m) \neq H(n)$となること）を決める。
2. Aさんは、自分の持つ電話番号$a_1, \ldots, a_{10}$について、$x_1 = H(a_1), \ldots, x_{10} = H(a_{10})$を計算して、$x_1, \ldots, x_{10}$を（ランダムな順番で）Bさんに送る。
3. Bさんは、自分の持つ電話番号$b_1, \ldots, b_{10}$について、$y_1 = H(b_1), \ldots, y_{10} = H(b_{10})$を計算して、$y_1, \ldots, y_{10}$を（ランダムな順番で）Aさんに送る。
4. Aさんは、$x_1, \ldots, x_{10}$のうち集合$\{y_1, \ldots, y_{10}\}$に属するものを$x_{i_1}, \ldots, x_{i_k}$とする。このとき$a_{i_1}, \ldots, a_{i_k}$が両者に共通する電話番号となる。
5. Bさんは、$y_1, \ldots, y_{10}$のうち集合$\{x_1, \ldots, x_{10}\}$に属するものを$y_{i_1}, \ldots, y_{i_k}$とする。このとき$b_{i_1}, \ldots, b_{i_k}$が両者に共通する電話番号となる。

実は、この手順は秘密計算として安全ではない。その理由を説明せよ。（ヒント：扱っている入力データが「実在する電話番号」であることが関係している。）

問2　nを正の整数とする。nビットを入力として1ビットを出力するどのような関数$f\colon \{0,1\}^n \to \{0,1\}$も、「2ビットに対する論理積（AND）」「2ビットに対する論理和（OR）」「1ビットに対するビット反転（NOT）」およびいくつかの定数ビットの組み合わせで表せることを証明せよ。

問3　既に世の中に存在する科学技術や、今後実現することが予想される科学技術の中で、秘密計算を応用できれば有益であると自身が考える技術の具体例を二つ挙げ、各々についてその理由を考察して述べよ。

＊なお、本講義に用いたスライドを、researchmapの縫田のページ `https://researchmap.jp/nuida/` の「資料公開」のコーナーで公開しています。

（以上）