T-79.514 Special Course on Cryptology / Privacy-Preserving Data Mining

Comments on "Private Selective Function Evaluation"

Alexey Vyskubov

In this notes, we briefly review [1], based on [2].

1 Introduction

This section briefly describes the problem from intuitive and practical point of view. Description is clear and understandable.

In the middle of this section the definition of a protocol for selective private function is given. It would be better to divide it in a few sentences as at the current state it consist of one rather long sentence which is not easy to understand.

The definition also mentions that m-argument function f is known to both the client and server so remark few lines below ("We will, however, assume that the function f is known to server...") is not necessary.

2 Selective Private Function Evaluation

"The servers have a common input $x = D^n$" is a typo and should be changed to "$\ldots x \in D^n$".

I suggest to change "The simulator is given the data x..." to "...database x".

Notation F for the set of allowable functions is not good as F afterwards represents some finite field.

In definition of strong security, it is not clear what is f.

I suggest to change "deviates from protocol" in the definition of malicious party to "may deviate from protocol".

The difference between communication complexity and the number of rounds probably should be explained.

3 Multi-server Protocols Based on Polynomial Evaluation

This section describes a straightforward protocol for selective private function evaluation in multi-server model. Some things in this section should be clarified as it is the most complex part of the review.

In previous section the function f was defined as $f : D^m \to A$ where A was some set. Here f is defined as $f : D^m \to D$. Was it intended?

Maybe someone can benefit (me for sure) from alternative definition of polynomial P_0. It is possible to define it without "conditional" part: notice that

$$p(z_k, j_k) = z_k j_k + (1 - z_k)(1 - j_k).$$

It also should be clarified why $P_0(i_1, \ldots, i_l) = x_i$. It is important because justifies the choice of l.

The definition of $P_{g,\text{left}}$ has an error. Notice that $P_0(i_1, \ldots, i_k)$ is not defined as k is not defined. Even if k is changed to l the definition is still wrong, as in this case $P_{g,\text{left}}$ will be a constant not a polynomial of non-zero degree. The right definition should look like

$$P_{g,\text{left}} = P_0(z_{i,1}, \ldots, z_{i,l}),$$

where $z_{i,k}$ are variables. The equation for P should be changed accordingly.

4 Protocols Based on Private Simultaneous Messages

This section starts with the explanation of private simultaneous messages model. The explanation is very clear and easy to read; the idea to illustrate the

notion of communication complexity for this model using very simple example is really good and helps reader to feel what is happening; I'd only suggest to define l before its usage (not a big deal, as it is defined immediately in the next sentence).

In "...send in the underlying protocol on input x_i" probably x_{i_j} was meant.

5 Protocols Based on General Multi-party Computation

This section describes three more protocols, all of them are based on the idea of dividing problem into two phases: input selection and usage of standard multi-party methods.

I would like to object against usage of construction "beaked down". It is easy to understand what author meant but I failed to find reasonable meaning for word "beak" (or "beaked down") in a Really Big Dictionary[1].

In subsection 5.2 it would be nice to have a couple of words about what S is.

In subsection 5.3 the closing parenthesis in the definition of virtual database y is on the wrong place (typed as index).

6 Some typos

I noticed few typos and have few suggestion concerning language style.

In Introduction: "the database owners are require**d**".

In Introduction: comma after "A protocol for selective private function evaluation" should be removed.

In Introduction: I'd change "to privately receive" to "to receive privately".

In Introduction, last paragraph: "the" before "security notions" probably should be removed.

In section 2: "The client wants to obtain...", I'd put a comma before "while".

In section 2: "any collusion ...of the servers learn**s** nothing."

In section 2, two times: "of allowable function**s** F".

In section 3: "The servers define ..., where as follows" — "where" probably should be removed.

In section 4: "...lets a receiver **to** retrieve m...".

The same sentence: "...such that the server..." probably should be changed to "...in a such way that the server...".

[1] Collins Concise Dictionary, 1740 pages.

7 Conclusion

My overall impression of the survey was very positive. It was easy to read and understand; moreover, links to additional information are provided.

References

[1] J. Wallén. Private selective function evaluation. Survey for the seminar T-79.514: Special Course on Cryptology / Privacy Preserving Data-Mining at HUT, 12 November 2003.

[2] R. Canetti, Y. Ishai, R. Kumar, M. Reiter, R. Rubinfeld, R. Wright. Selective private function evaluation with application to private statistics. In *Twentieth ACM Symposium on Principles of Distributed Computing (PODC)*, 2001.