Functions Used in Private Lookup Protocols Possibly Suitable for Implementation on an FPGA

Peeter Laud

May 6, 2015

In this note we give a step-by-step instruction for evaluating some computationally heavy functions that appear in the private lookup protocols proposed in [1, 2]. In a private lookup protocol, we are given a vector v of length m, which is either public, or shared among the computation parties. We are also given an index j, which is private — i.e. it is shared among the computation parties. We want to output the shares of v_j.

Let $\mathbb{N}$ denote the set of natural numbers. Let $\mathbb{F}$ be any finite field. In the protocols of [1, 2], $\mathbb{F}$ is the set containing both the elements of v, as well as the indices j.

The complex computation performed in the online phase of the basic lookup protocol is depicted in Alg. 1. The computation in the online phase of an improved protocol is depicted in Alg. 2.

```
Data: $z \in \mathbb{F}$, $m \in \mathbb{N}$
Data: $y_0, \ldots, y_{m-1} \in \mathbb{F}$
Result: The share of a party
return $\sum_{i=0}^{m-1} z^i \cdot y_i$
```

Algorithm 1: Computations in the online phase of [1, Alg. 1]

```
Data: $z \in \mathbb{F}$, $m \in \mathbb{N}$
Data: $r_0, \ldots, r_{m-1} \in \mathbb{F}$
Data: $c_0, \ldots, c_{m-1} \in \mathbb{F}$
Result: The value to be shared in an SSS-based ABB
return $\sum_{i=0}^{m-1} z^j \cdot r_j \cdot c_j$
```

Algorithm 2: Computations in the online phase of [1, Alg. 6]

There are also computations during the vector-only phase that may be sped up. These are best described as follows. Let $m \in \mathbb{N}$ and $v_1, \ldots, v_m \in \mathbb{F}$. Let $j_1, \ldots, j_m \in \mathbb{F}\backslash\{0\}$ be the indices that we want to use to refer to the elements of the vector $\vec{v}$. Typically, if $\mathbb{F} = \mathbb{Z}_p$ for some prime p, then $j_i = i$. But if $\mathbb{F}$ is a different kind of field, then maybe we have defined the indices $j_1, \ldots, j_m$ differently. Let V be the *Vandermonde matrix*:

$$V = \begin{pmatrix} 1 & j_1 & j_1^2 & \cdots & j_1^{m-1} \\ 1 & j_2 & j_2^2 & \cdots & j_2^{m-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & j_m & j_m^2 & \cdots & j_m^{m-1} \end{pmatrix} .$$

The **computational task** is to find the vector $V^{-1} \cdot (v_1, \ldots, v_m)^{\mathrm{T}}$.

References

[1] Peeter Laud. A Private Lookup Protocol with Low Online Complexity for Secure Multiparty Computation. To appear in the post-proceedings of ICICS'14.

[2] Peeter Laud and Jan Willemson. Universally composable privacy preserving finite automata execution with low online and offline complexity. Cryptology ePrint Archive: Report 2013/678. http://eprint.iacr.org/2013/678