An Annotated Bibliography of Practical Secure Computation

Mike Rosulek: rosulekm@eecs.oregonstate.edu

http://tinyurl.com/mpc-annotated
This contains annotated bibliography entries of research papers in practical secure computation. Initially, the site will focus on two-party computation using garbled circuits and cut-and-choose techniques. See this page for more information about this project.

Disclaimer: The current selection of papers is somewhat arbitrary, so do not use a paper's presence/absence on this site as any indicator of that paper's importance. The site is very much a work in progress, and writing bibliography entries is somewhat of a "spare time" activity for its maintainer. There are perhaps hundreds of great papers that are egregiously missing from the site, and should be included. In the mean time, I would gladly accept corrections of factual errors, as well as contributed bibliography entries! Check out the guidelines for bibliography entries.

VIEW ALL 39 PAPERS:

View all papers, by category, author names, publication date, recently added, recently updated.

Quick list (tooltips contain title / author):

[AL10] [ALS13] [AO12] [BFKL13] [BHR12] [CGH12] [FJAN13] [GK00MB12] [HKL12] [HP10] [HEKKS11] [HOPD10] [KCS07] [KOH13] [KOS05] [KL12] [KL14] [KOS06] [KOS08] [KSO12] [KKS12] [L13] [LDP07] [LDP09] [LIP12] [LPS08] [MF04] [MPS04] [MR11] [PSW09] [R12] [S811] [S813] [SZ13] [V76] [Y96]

Search papers: 505

CATegories IN THE DATABASE:

Circuit constructions & optimizations: 2 papers

Circuits of interest to secure computation. Fundamentals aspects of circuits in general that affect their

Bibliography Categories

- Circuit constructions & optimizations
- Cut-and-choose mechanisms
- Garbling methods
- Oblivious transfer extensions
- Reference works
- Security models
- Special-purpose protocols
Who’s it for?
- Anyone interested in “practical” aspects of MPC
- ... who knows enough crypto to have seen MPC definitions
- Your first-year PhD advisees
Who’s it for?
- Anyone interested in “practical” aspects of MPC
- ... who knows enough crypto to have seen MPC definitions
- Your first-year PhD advisees

What’s there?
- Short summaries of 30 papers and counting
- Glossary
EXTENDING OBLIVIOUS TRANSFERS EFFICIENTLY

Yuval Ishai, Joe Kilian, Kobbi Nissim, Erez Petrank
CRYPTO 2003 [pdf] [bibtex]

Introduces the concept of OT extension. It is well known that oblivious transfer (OT) cannot be based on symmetric-key primitives alone (in a black-box way). Hence OT protocols necessarily rely on expensive public-key operations. OT extension is a method for obtaining a large number of effective OTs using only a small number of "base" OTs (depending only on the security parameter) plus symmetric-key operations, minimizing the cost of OT in an amortized sense.

The protocol achieves $n$ instances of 1-out-of-2, $k$-bit string OT, using only $k$ instances of 1-out-of-2, $n$-bit string OT, where $k$ is the security parameter. Note that it is trivial to extend the bit length of an OT by transferring (via a base OT) a length-$k$ seed to a PRG and masking a longer message with the PRG output (this variant of OT extension is due to Beaver). Hence, the important parameter is that a small, fixed number $k$ of OTs is extended to an arbitrarily larger number $n$ of OTs.

1. The receiver chooses a random $n \times k$ matrix $T$ of bits and a string $r \in \{0, 1\}^n$ denoting his choice bits in the $n$ logical OTs. The sender chooses random string $a \in \{0, 1\}^k$.

2. Let $T_{i,j}$ denote the $j$th column of $T$ (an $n$-bit string). The parties use the base OTs (in the opposite direction!), with the receiver providing messages $T_{i,j}$ and $T_{i,j} \oplus r$, and the sender providing choice bit $s_j$.

3. Let $Q$ denote the matrix that the sender receives from these base OTs (received column-wise). Let $Q_{i,:}$ denote the $i$th row of $Q$. The important part of the protocol is that $Q_{i,:}$ is either $T_{i,:}$ or $T_{i,:} \oplus s_i$ depending on the receiver's choice bit $r_i$.

4. To execute the $i$th logical OT, the sender encrypts the two messages $m_0, m_1$ under one-time pads with keys $H(i \parallel Q_{i,:})$ and $H(i \parallel Q_{i,:} \oplus s)$, respectively, where $H$ is a random oracle. Exactly one of those masks is $H(i \parallel T_{i,:})$, according to the receiver's choice bit, so the receiver can unmask his desired message. The other mask is $H(i \parallel T_{i,:} \oplus s)$, where $s$ is unknown to the receiver.

Note that, besides the base OTs, the only other operations are calls to the random oracle $H$. The protocol is secure against semi-honest adversaries. A cut-and-choose technique can be used to provide security in the malicious setting.

For simplicity, the hash function $H$ is assumed to be a random oracle. More concretely, the protocol requires that the joint distribution of $t_1, t_2, \ldots, t_n$ and $H(1 \parallel t_1 \oplus a), H(2 \parallel t_2 \oplus s), \ldots, H(n \parallel t_n \oplus a)$ be pseudorandom where $a$ is unknown. This security property is called correlation-robustness.

Categories:
- OTExtension
Testimonials:

▶ “Finally there is a website that can supervise my students for me.” — Payman Mohassel
▶ “Will it count towards tenure?” — My wife
Testimonials:

- “Finally there is a website that can supervise my students for me.” — Payman Mohassel
- “Will it count towards tenure?” — My wife

Bugs:

- I don’t know every relevant paper in the area
- Writing summaries takes time
- Current focus on garbled-circuit 2PC only
- I probably don’t know what “practical” means
Testimonials:

- “Finally there is a website that can supervise my students for me.” — Payman Mohassel
- “Will it count towards tenure?” — My wife

Bugs:

- I don’t know every relevant paper in the area
- Writing summaries takes time
- Current focus on garbled-circuit 2PC only
- I probably don’t know what “practical” means

A plea for help:

- What papers are embarrassingly absent?
- Better yet, contribute summaries!
- What else would make this a helpful resource?