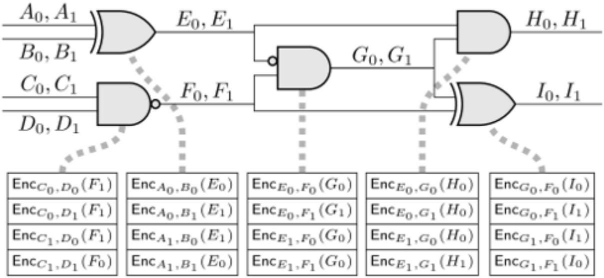
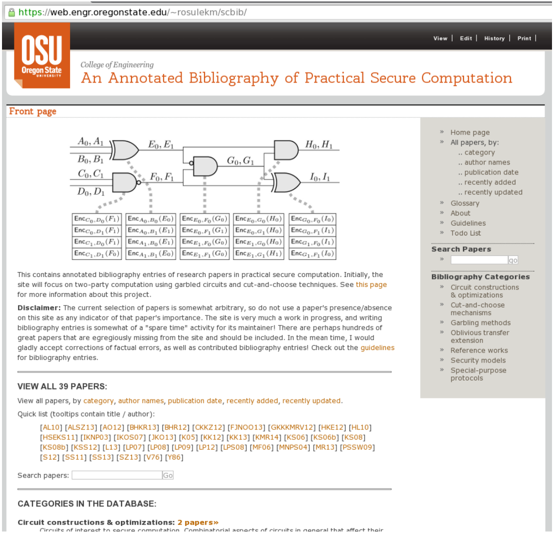
An Annotated Bibliography of Practical Secure Computation

Mike Rosulek : rosulekm@eecs.oregonstate.edu



http://tinyurl.com/mpc-annotated



$\mathsf{Enc}_{C_0,D_0}(F_1)$	$\mathsf{Enc}_{A_0,B_0}(E_0)$	$\mathsf{Enc}_{E_0,F_0}(G_0)$	$\mathsf{Enc}_{E_0,G_0}(H_0)$	$\mathsf{Enc}_{G_0,F_0}(I_0)$
$\mathsf{Enc}_{C_0,D_1}(F_1)$	$\mathsf{Enc}_{A_0,B_1}(E_1)$	$\mathsf{Enc}_{E_0,F_1}(G_1)$	$\mathsf{Enc}_{E_0,G_1}(H_0)$	$\mathsf{Enc}_{G_0,F_1}(I_1)$
$\mathsf{Enc}_{C_1,D_0}(F_1)$	$\mathsf{Enc}_{A_1,B_0}(E_1)$	$\mathsf{Enc}_{E_1,F_0}(G_0)$	$\mathsf{Enc}_{E_1,G_0}(H_0)$	$\mathsf{Enc}_{G_1,F_0}(I_1)$
$\mathsf{Enc}_{C_1,D_1}(F_0)$	$\mathsf{Enc}_{A_1,B_1}(E_0)$	$\mathsf{Enc}_{E_1,F_1}(G_0)$	$\mathsf{Enc}_{E_1,G_1}(H_1)$	$\mathsf{Enc}_{G_1,F_1}(I_0)$

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] [ALSZ13] [AO12] [BHKR13] [BHR12] [CKKZ12] [FJNOO13] [GKKKMRV12] [HKE12] [HL10] [HSEKS11] [IKNP03] [IKOS07] [JKO13] [K05] [KK12] [KK13] [KMR14] [KS06] [KS06b] [KS08] [KS08b] [KSS12] [L13] [LP07] [LP08] [LP09] [LP12] [LPS08] [MF06] [MNPS04] [MR13] [PSSW09] [S12] [SS11] [SS13] [SZ13] [V76] [Y86]

Search papers: Go

CATEGORIES IN THE DATABASE:

Circuit constructions & optimizations: 2 papers»

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

- Home page
- All papers, by:
  - .. category
  - .. author names
  - .. publication date
  - .. recently added
  - .. recently updated
- Glossary
- About
- Guidelines
- Todo List

Search Papers

go

Bibliography Categories

- Circuit constructions & optimizations
- Cut-and-choose mechanisms
- Garbling methods
- Oblivious transfer extension
- 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, ℓ-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 transfering (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 $s \in \{0,1\}^k$.
2. Let $T_{*,j}$ denote the jth column of T (an n-bit string). The parties use the base OTs (in the opposite direction!), with the receiver providing messages $T_{*,j}$ and $T_{*,j} \oplus r$, 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 ith row of Q. The important part of the protocol is that $Q_{i,*}$ is either $T_{i,*}$ or $T_{i,*} \oplus s$, depending on the receiver's choice bit r_i.
4. To execute the ith logical OT, the sender encrypts the two messages m_0, m_1 under one-time pads with keys $H(i \| Q_{i,*})$ and $H(i \| Q_{i,*} \oplus s)$, respectively, where H is a random oracle. Exactly one of these masks is $H(i \| T_{i,*})$, according to the receiver's choice bit, so the receiver can unmask his desired message. The other mask is $H(i \| T_{i,*} \oplus s)$, 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

$$t_1, t_2, \ldots, t_n \text{ and } H(1\|t_1 \oplus s), H(2\|t_2 \oplus s), \ldots, H(n\|t_n \oplus s)$$

be psuedorandom where s 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?