Garbled Circuits

Garbled circuits is a protocol that allows two parties to carry out arbitrary computation without revealing any information about their own inputs other than what is revealed in the final output. However, in this protocol the computation must be represented as boolean logic gates, each of which requires cryptographic operations to be generated and securely evaluated. The runtime cost is therefore linearly related to the number of logic gates involved. However, if the other party can be trusted with part of the input data, we can perform partial evaluation using the public inputs to produce a substantially smaller circuit, speeding up the overall process.

Example: Edit Distance

Suppose we have two input strings from two parties, with some private input characters redacted out, marked here with a '?'.

We can already reduce the size of computation by 20–33% even when 20–30% of the input is marked private.

Smith-Waterman Algorithm

Garbled Inputs

Evaluate

Oblivious Transfer

Create Logic Circuits

Garble

E(a_1, E(b_0, c_0))
E(a_1, E(b_1, c_1))
E(a_0, E(b_0, c_0))
E(a_0, E(b_1, c_0))

Other simple rewrite rules used
- Removing redundant branches
  \( \min(a + 3, b, a + 5) = \min(a + 3, b) \)
- Factoring
  \( \min(a + x, b + x) = x + \min(a, b) \)

Sometimes even more, depending on the pattern of private input data.

A := "AGTAA?GDC"
B := "AGTAA?GDC"
diff(A_2, ?) + diff(A_5, B_5) + 1

diff(A, ?) + diff(B, ?) + 1

http://mightbeevil.com/