Generalized Obfuscation of Programs

R. Canetti (IBM) and R. Dakdouk (Yale), Eurocrypt 2008

NSF Grant CNS-0331548 (PIs: Feigenbaum, Kannan, Silberschatz)

Problem

Program obfuscation is an important cryptographic concept with practical applications such as software protection. However, the only obfuscators previously known were for a simple class of functions, namely point functions.

Approach

We develop techniques for obfuscating a larger class of programs, namely multibit point functions. We do so by using known algorithms for obfuscating point functions. Perfectly one-way (POW) functions are used in an essential way.

Approach and Impact

<table>
<thead>
<tr>
<th>New Approach</th>
<th>Research Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obfuscating complex functions based on</td>
<td>Security guarantees for Digital Lockers and other</td>
</tr>
<tr>
<td>obfuscating simpler functions</td>
<td>practical applications</td>
</tr>
<tr>
<td>Realizing the importance of composability</td>
<td>Opening the way for obfuscating more complex functions</td>
</tr>
</tbody>
</table>

Technical Description

We concatenate the obfuscation of point functions to achieve multibit output. However, proving security requires some composability properties of the primitive obfuscator. We show that obfuscation of point functions is not composable in general. Thus, under various composability assumptions, we show the following results.

Results

- The construction is a composable obfuscator of multibit point functions if the primitive is a composable obfuscator of point functions.
- The construction is an obfuscator if the primitive is a statistical POW function.
- The construction is a weak obfuscator (where the output, y, is independent of the input, x) if the primitive is a computational POW function.