Point Obviouscation

Daniel J. Bernstein, Andreas Hülsing, Tanja Lange,
and Ruben Niederhagen

December 9, 2014

Challenge announced at CRYPTO 2014 rump session:

Page 11 from `http://crypto.2014.rump.cr.yp.to/bca480a4e7fcdaf5bfa9dec75ff890c8.pdf`:

Everybody loves (virtual black-box / indistinguishability) obfuscation. . . so we implemented it!

Implementation combines ideas from various obfuscation papers and uses CLT multilinear map scheme

It is slow. . . but not as slow as you might think

Example: To obfuscate a 16-bit point function (i.e., 16 OR gates) with 52 bits of security using an Amazon EC2 machine with 32 cores:

- Obfuscation time: $\approx$ 7 hours
- Evaluation time: $\approx$ 3 hours
- Obfuscation size: 31 GB

$\Longrightarrow$ **it's almost nearly practical**

Challenge announced at CRYPTO 2014 rump session:

Page 14 from http://crypto.2014.rump.cr.yp.to/bca480a4e7fcdaf5bfa9dec75ff890c8.pdf:

Code is available: https://github.com/amaloz/ind-obfuscation

ePrint version should be up at some point

For the cryptanalysts in the audience: We have an obfuscated 14-bit point function on Dropbox[1] — learn the point and you win!

[1] https://www.dropbox.com/s/85d03o0ny3b1c0c/point-14.circ.obf.60.zip

Breaking the challenge:

- 14-bit point function,
- “60 bits of security”,
- obfuscation size: 25 GB.

Breaking the challenge:

- 14-bit point function,
- “60 bits of security”,
- obfuscation size: 25 GB.

Attack component	Real time
Initial procrastination	a few days
First attempt to download challenge (failed)	82 minutes

Breaking the challenge:

- 14-bit point function,
- "60 bits of security",
- obfuscation size: 25 GB.

Attack component	Real time
Initial procrastination	a few days
First attempt to download challenge (failed)	82 minutes
Subsequent procrastination	40 days + 40 nights
Fourth attempt to download challenge (succeeded)	about an hour

Breaking the challenge:

- 14-bit point function,
- "60 bits of security",
- obfuscation size: 25 GB.

Attack component	Real time
Initial procrastination	a few days
First attempt to download challenge (failed)	82 minutes
Subsequent procrastination	40 days + 40 nights
Fourth attempt to download challenge (succeeded)	about an hour
Original program evaluating one input	245 minutes
Original program evaluating all inputs on one PC	(extrapolated) 7.6 years

Breaking the challenge:

- 14-bit point function,
- "60 bits of security",
- obfuscation size: 25 GB.

Attack component	Real time
Initial procrastination	a few days
First attempt to download challenge (failed)	82 minutes
Subsequent procrastination	40 days + 40 nights
Fourth attempt to download challenge (succeeded)	about an hour
Original program evaluating one input	245 minutes
Original program evaluating all inputs on one PC	(extrapolated) 7.6 years
Copying challenge to cluster	about an hour
Our faster program evaluating one input	4.85 minutes

Breaking the challenge:

- 14-bit point function,
- "60 bits of security",
- obfuscation size: 25 GB.

Attack component	Real time
Initial procrastination	a few days
First attempt to download challenge (failed)	82 minutes
Subsequent procrastination	40 days + 40 nights
Fourth attempt to download challenge (succeeded)	about an hour
Original program evaluating one input	245 minutes
Original program evaluating all inputs on one PC	(extrapolated) 7.6 years
Copying challenge to cluster	about an hour
Our faster program evaluating one input	4.85 minutes
First successful break of challenge on 20 PCs	23 hours

Breaking the challenge:

- 14-bit point function,
- "60 bits of security",
- obfuscation size: 25 GB.

Attack component	Real time
Initial procrastination	a few days
First attempt to download challenge (failed)	82 minutes
Subsequent procrastination	40 days + 40 nights
Fourth attempt to download challenge (succeeded)	about an hour
Original program evaluating one input	245 minutes
Original program evaluating all inputs on one PC	(extrapolated) 7.6 years
Copying challenge to cluster	about an hour
Our faster program evaluating one input	4.85 minutes
First successful break of challenge on 20 PCs	23 hours
Further procrastination ("this is fast enough")	about half a week
Our faster program evaluating all inputs on 21 PCs	34 minutes
Second successful break of challenge on 21 PCs	19 minutes

Challenge announced at CRYPTO 2014 rump session:

Page 11 from `http://crypto.2014.rump.cr.yp.to/bca480a4e7fcdaf5bfa9dec75ff890c8.pdf`:

Everybody loves (virtual black-box / indistinguishability) obfuscation. . . so we implemented it!

Implementation combines ideas from various obfuscation papers and uses CLT multilinear map scheme

It is slow. . . but not as slow as you might think

Example: To obfuscate a 16-bit point function (i.e., 16 OR gates) with 52 bits of security using an Amazon EC2 machine with 32 cores:

- Obfuscation time: $\approx$ 7 hours
- Evaluation time: $\approx$ 3 hours
- Obfuscation size: 31 GB

$\Longrightarrow$ **it's almost nearly practical**

Our paper will be online soon.