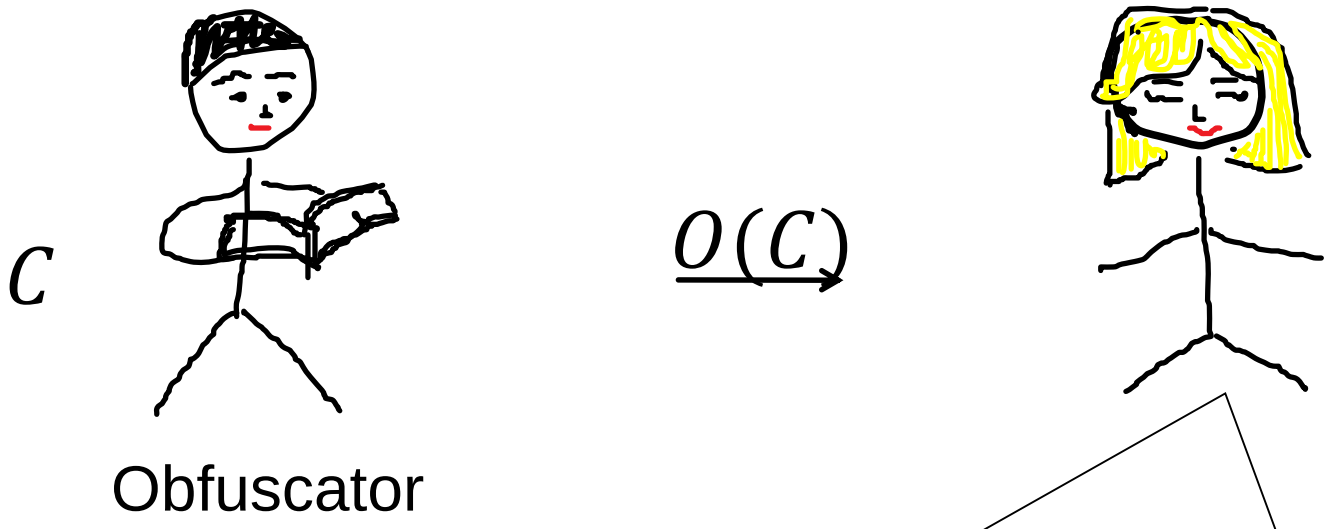
Candidate Indistinguishability Obfuscation, Or Sell Apple, Buy Samsung

SANJAM GARG
CRAIG GENTRY
SHAI HALEVI
MARIANA RAYKOVA
AMIT SAHAI
BRENT WATERS

To appear at FOCS 2013

Disclaimer: No legal responsibility is being taken for this advice.

Indistinguishability Obfuscation (IO) [BGIRSVY01]



IO for NC_1

- Implies Indistinguishability Obfuscation for general circuits
- Functional Encryption for general circuits
  - Under arbitrary collusion

Realizing IO for NC_1

- Start with Killian/Barrington randomized encoding of circuit
- Express in terms of matrix products
- Add additional randomization and algebraic structure

- Hide the values and limit computation by doing everything under Multilinear Maps.

Highly Confidential

Just What the Samsung Needs...

Subject: [...] library-based platform for Functional Encryption

Date: Wed, 31 Jul 2013 05:20:20

[...] We've based our complete secure and trustable solutions right now for [...] stack, which Samsung has published [...]. However as we all understand, your approach is the missing component to make this actually happen [...]

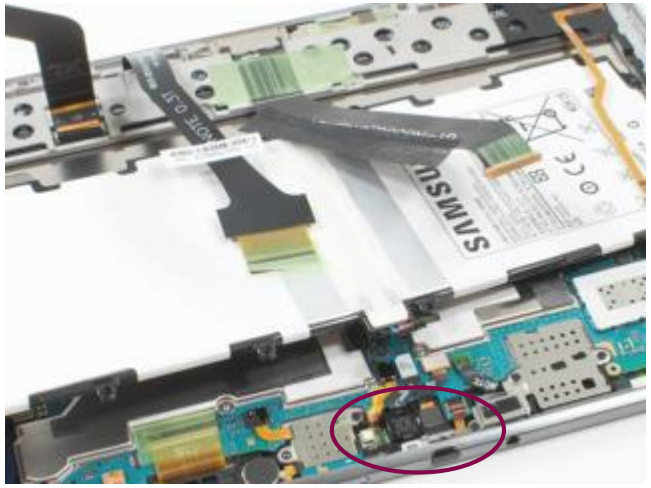
Just What the Samsung Needs...

Subject: [...] library-based platform for Functional Encryption

Date: Wed, 31 Jul 2013 05:20:20

[...] We've based our complete secure and trustable solutions right now for [...] stack, which Samsung has published [...]. However as we all understand, your approach is the missing component to make this actually happen [...]

Samsung Galaxy VII



A few hundred cores.

Added Advantage

- Makes software infringement easy for Samsung..

- Can copy arbitrary software that is functionally equivalent to Apple's without leaving trace of the same.

Added Advantage

- Makes software infringement easy for Samsung..

- Can copy arbitrary software that is functionally equivalent to Apple's without leaving trace of the same.

Open Problem: Samsung can not infringe on the obfuscation technology itself. ☹

Crypto Wars III

- Now that we have obfuscation Samsung is going to be back in business.