Functional Encryption with Bounded Collusions via Multi-Party Computation

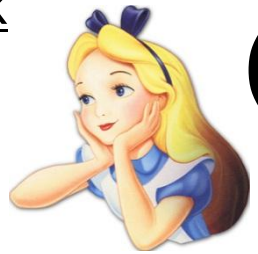
Sergey Gorbunov
Vinod Vaikuntanathan
} University of Toronto

Hoeteck Wee
} George Wash. U.

Functional Encryption

[Sahai-Waters'05, Boneh-Sahai-Waters'11, O'Neill'10…]

mpk



(M)

Alice

msk

Bob

Enc(M)

SK_{F1},SK_{F2},…

Charlie

"I can compute **F1(M),F2(M),…**", but learn **nothing else about M**

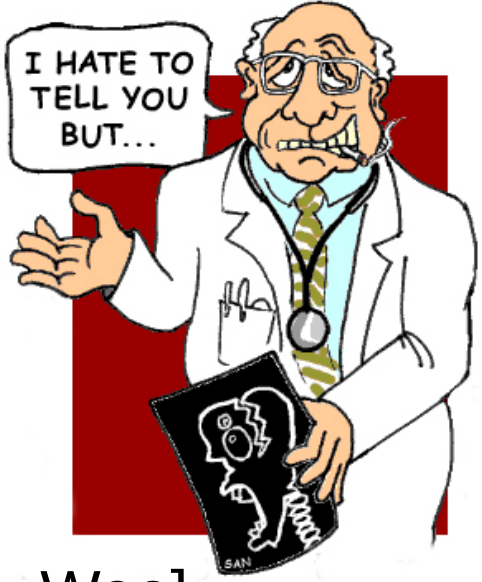
Big Question:

Can we construct Functional Encryption for all functions?

State of the art:

- **(anonymous) Identity-Based Encryption:** [S'82,BF'01,BDOP'04,BW'06]
- **Attribute-based Encryption:** Boolean formulas [GPSW'06,LOSTW'10,…]
- **Predicate Encryption:** inner products [KSW'08,…]

Our Result 1:



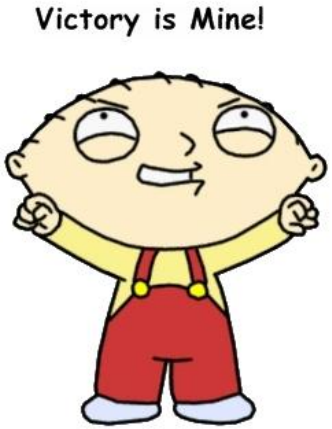
THEOREM [Agrawal, Gorbunov, Vaikuntanathan, Wee]

General Unbounded query FE is IMPOSSIBLE

- Even in a weak non-adaptive simulation def.
- For Pseudo-Random Functions (where M=seed and F_i=PRFinput)
- Generalizes to “incompressible” functions

* Concurrent , *incomparable*, work by Persiano et al.

Our Result 2:



[G., Vaikuntanathan, Wee]: **q-bounded Functional Encryption for *all functions*!**

Previously:

- **q-bounded IBE**
  [DKXY'01, CHHIKRSV'07, GLW'12]

Main Motivation:

- Bounded number of adversaries (having SK_{F1}, SK_{F2},.., SK_{Fq}) collude to learn "anything else" about message M

q-bounded Functional Encryption for Any Function

1-FE for arbitrary circuits [SS'10, Yao'86]

Using MPC [BGW'88]

q-FE for degree-D circuits

DONE!

FE Bootstrapping Theorem:
Using Randomized Encodings
[AIK'05,Yao'86]

DONE!

q-FE for arbitrary circuits

unbounded-FE for arbitrary circuits

q-bounded Functional Encryption for <u>Any Function</u>

1-FE for arbitrary circuits [SS'10, Yao'86]

Using MPC [BGW'88]

DONE!

q-FE for degree-D circuits

FE Bootstrapping Theorem:
Using Randomized Encodings
[AIK'05,Yao'86]

DONE!

q-FE for arbitrary circuits

~~unbounded-FE for arbitrary circuits~~