A Few Thoughts on New Functionalities and Obfuscation

Brent Waters

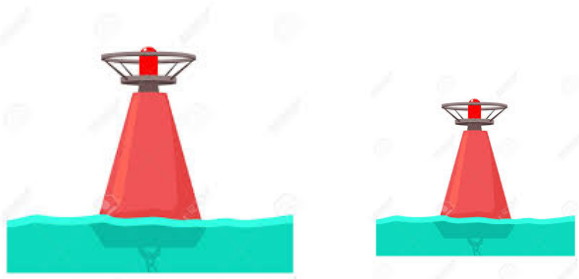
THE UNIVERSITY OF
TEXAS
AT AUSTIN

Goal:

High Functionality & Understood Assumptions

Obfuscation

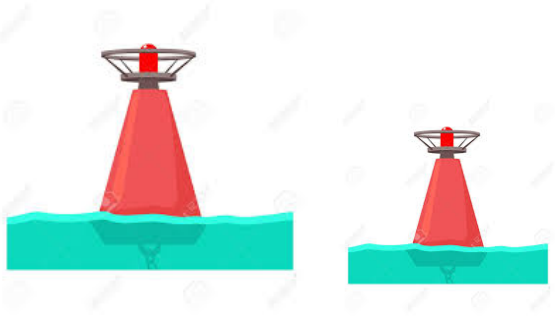
Assumptions



- Immunized MMaps
- “LWE-inspired” candidates
- Bilinear maps + Special Property PRGs

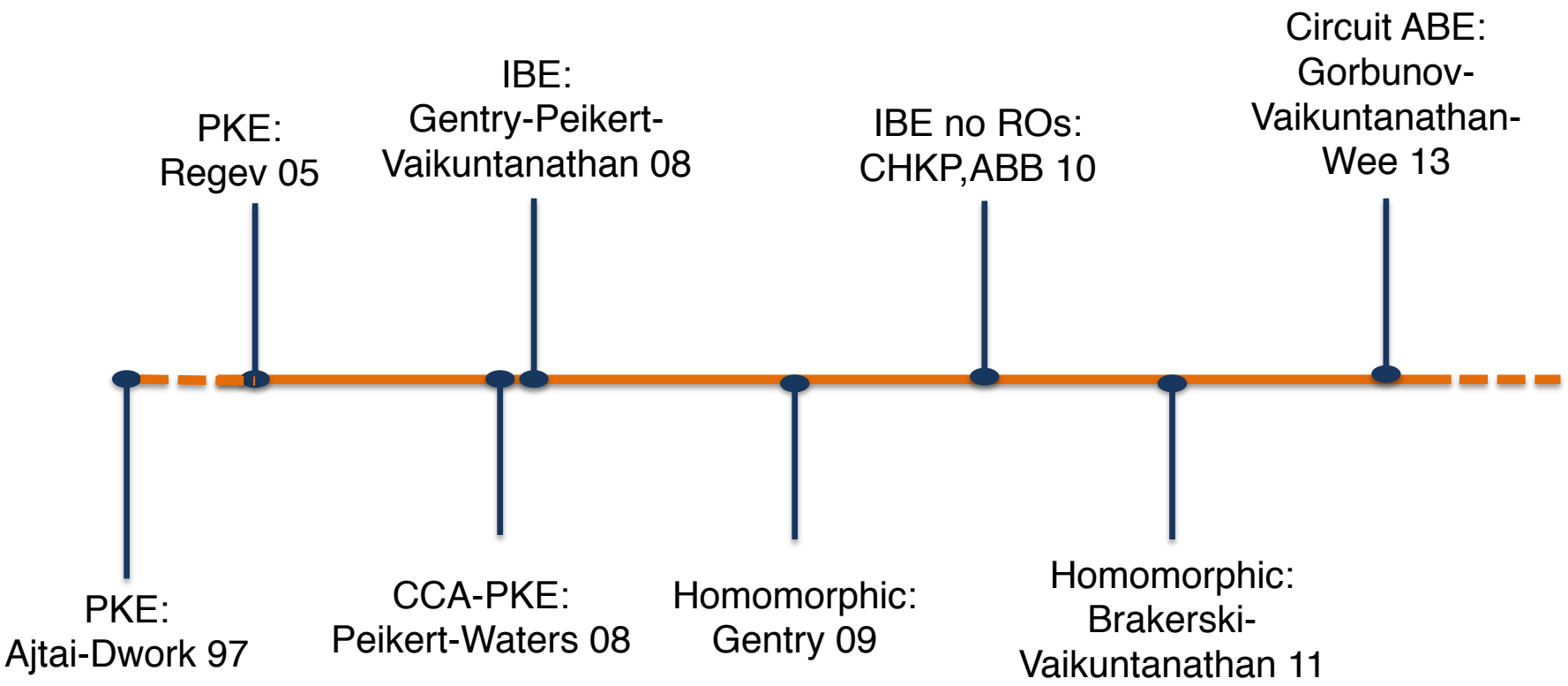
LWE

New Functionality

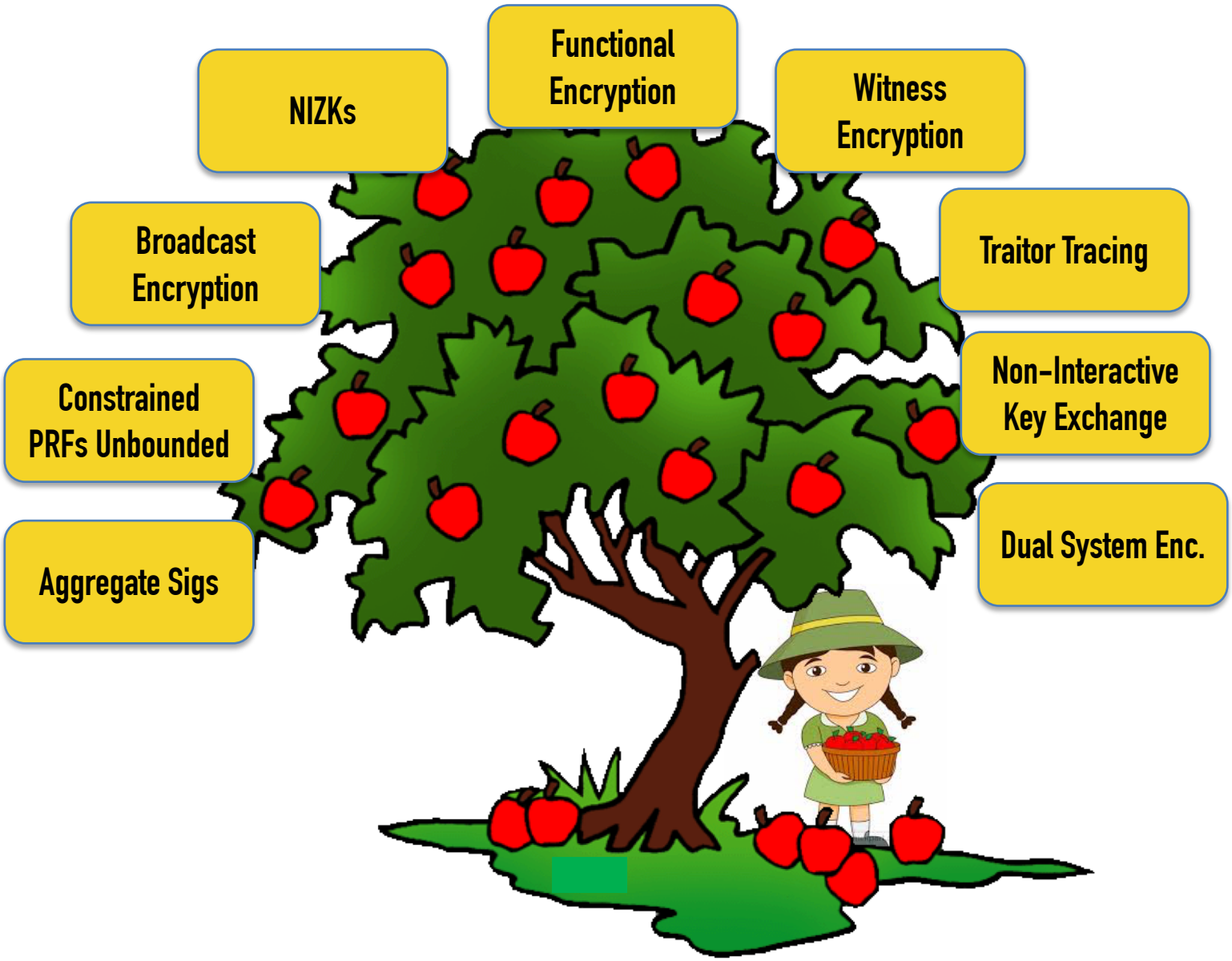


Idea: Applications lead to techniques to more applications…

LWE Functionality Timeline

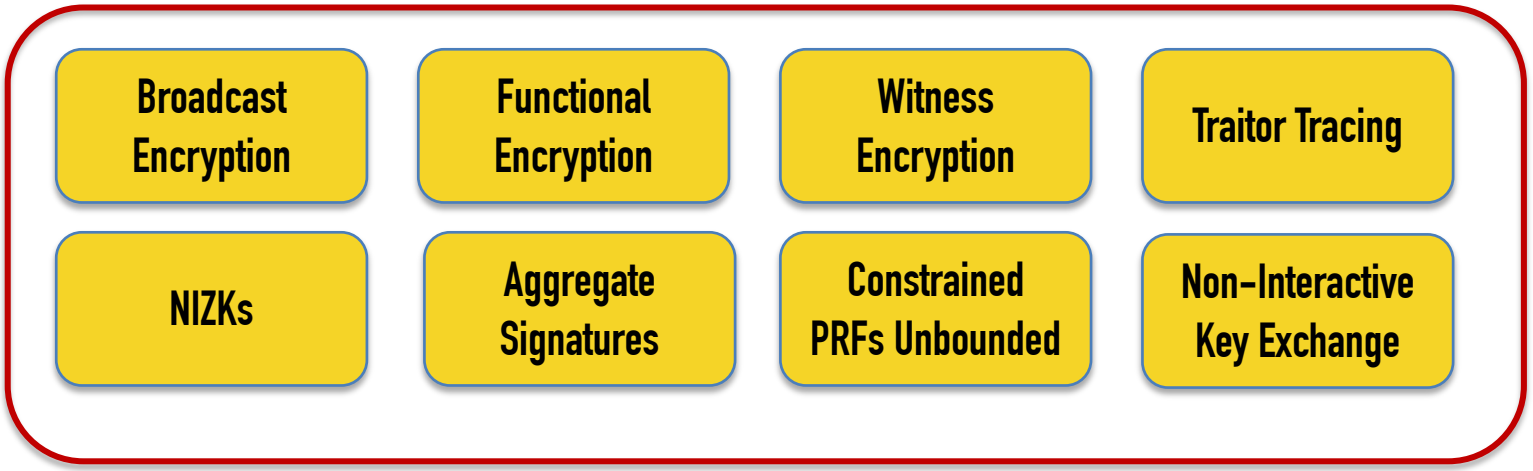


Target Challenges



Big Challenges

"Definition" : Primitive is iO/LWE-complete if techniques might lead to indistinguishability obfuscation from LWE



(Some) Recent Results

(1) Circular Security Separation/Lockable Obfuscation

(2) Traitor Tracing

(3) NIZK via Fiat-Shamir

(Some) Recent Results

(1) Circular Security Separation/Lockable Obfuscation

(2) Traitor Tracing

(3) NIZK via Fiat-Shamir

Good News: New functionality from LWE!

Bad News: Unclear next steps;
LWE mechanisms limited

Status

(1) Still hacking away

(2) Candidate problems: Broadcast, dual system, aggregate sigs, constrained PRFs

(3) Common sticking points, go back to same issues

(4) Pull out lower level conjectures/ideas

Panel

Can funny PRGs be used (directly) for other applications?

New assumptions suffer from prior history from outsiders view? (Fool me once…)