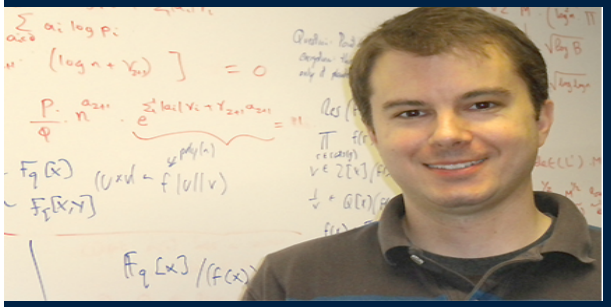
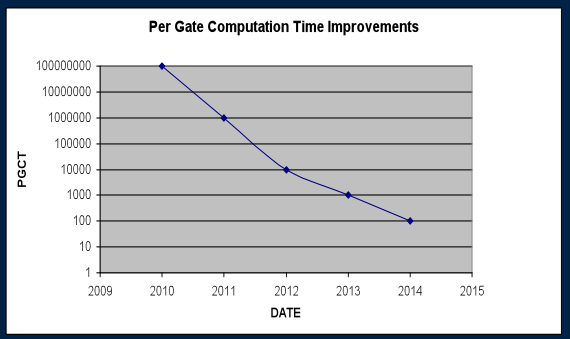
Computing on Encrypted Data

Fully Homomorphic Encryption

Can we perform operations on encrypted data in the Cloud without having to first decrypt it?



Theoretical Solution first proposed
by Craig Gentry (IBM) in 2009
- prompted quotes like "Not in my lifetime"
because scheme was inefficient
and difficult to implement

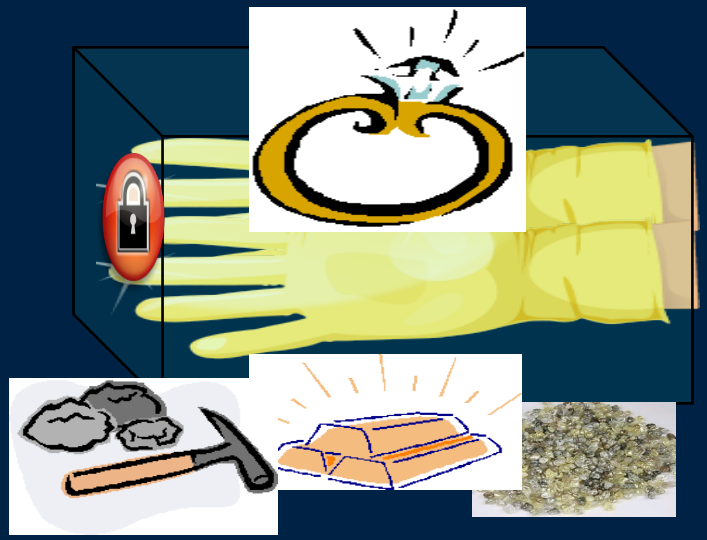


Rapid improvements to the theory have been made and the efficiency of the new schemes make practical implementations possible.

Can we produce a practical demonstration using Field Programmable Gate Arrays to accelerate performance ?

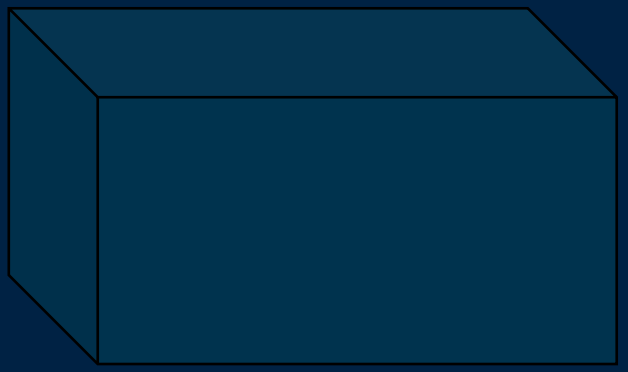
Gentry's Scheme (Analogy) – Alice's Jewellery Store

- Alice wants to produce jewellery doesn't trust her workers not to steal raw materials - so she devises a plan.
- Create a box with in which to place the raw materials - workers can manipulate without being able to extract any material
- She puts the raw materials in the box and locks it
- The Workers produce the jewellery



Alice gets the Jewellery

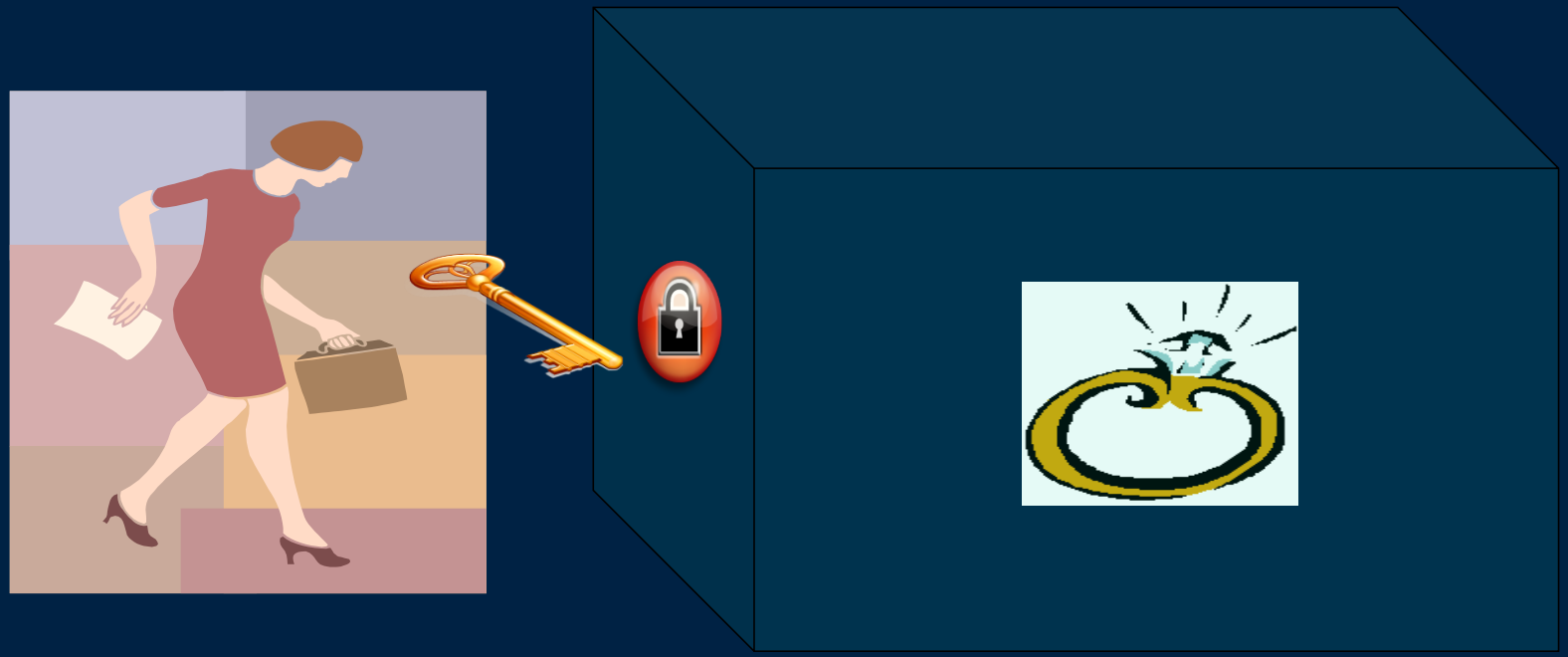
Alice gets the Jewellery



The problem and Gentry's Solution

- As the workers manipulate the raw materials the gloves get stiffer until it becomes impossible to work
- Alice takes the original key and puts it in a larger box
- She then adds the partially completed jewellery in its box
- The workers can open the original box and continue working until the gloves stiffen again
- Alice repeats the process until the job is done

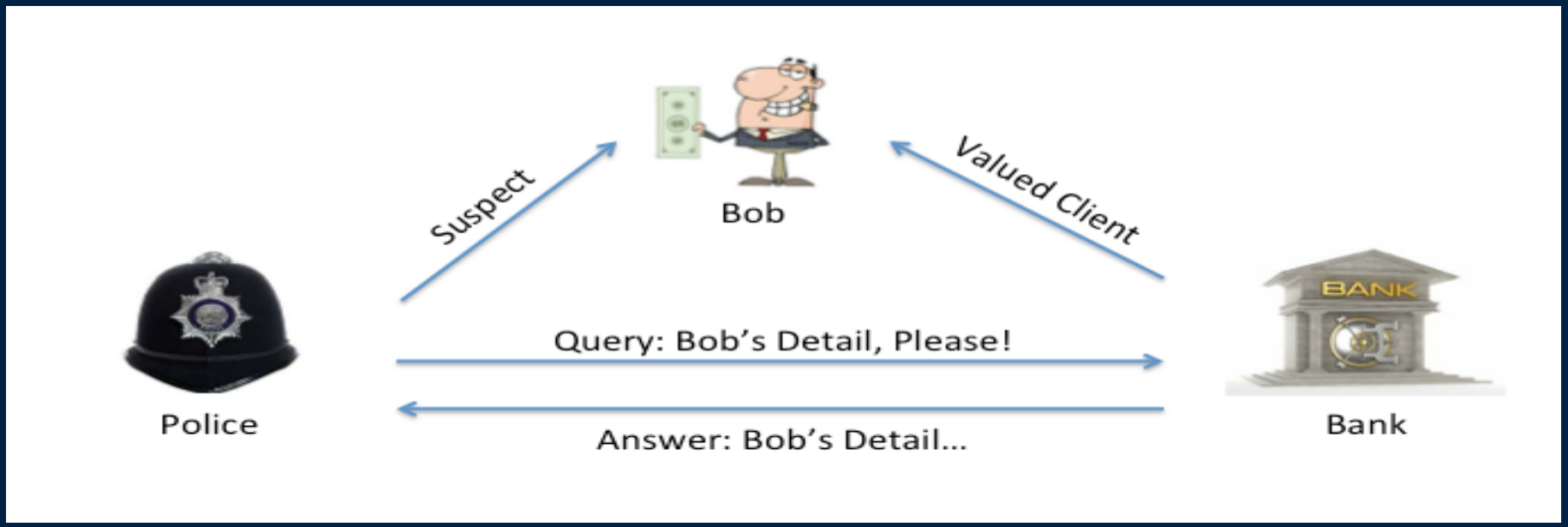
Alice gets the Jewelry



What can you do that's new?

Oblivious Transfer

Can A ask a question of B without revealing the question?
Can B can give the correct answer without knowing what answer was given?



Private Set Intersection – Blue on Blue Scenario

Each party only learn possible track conflicts

Exchange Encrypted Tracks

Challenges of Fully Homomorphic Programing

- Requires a different mindset from traditional programing models
- Need code development tools to hide the complexity