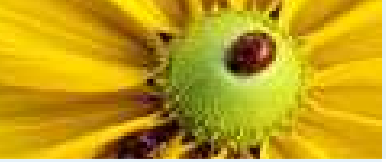
Privacy-Preserving Electronic Transactions

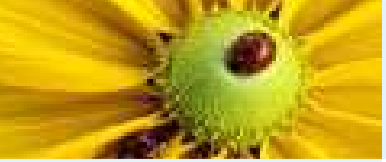
René Peralta
Computer Security Division
National Institute of Standards and Technology

November 2011



Beyond encrypting and hashing.

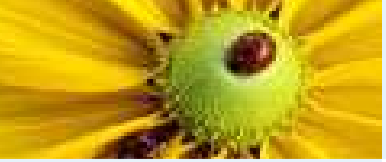
Some hard problems.



Beyond encrypting and hashing.

Some hard problems.

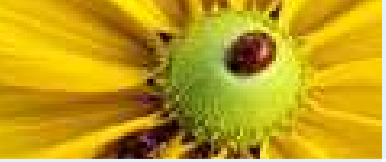
- Encrypted medical databases.



Beyond encrypting and hashing.

Some hard problems.

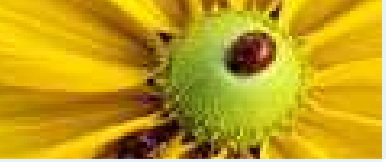
- Encrypted medical databases.
- Digital cash.



Beyond encrypting and hashing.

Some hard problems.

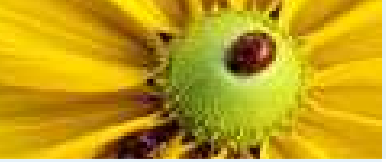
- Encrypted medical databases.
- Digital cash.
- Secure Internet voting.



Beyond encrypting and hashing.

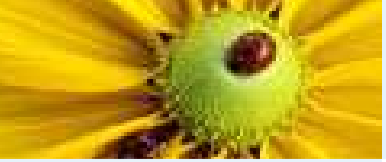
Some hard problems.

- Encrypted medical databases.
- Digital cash.
- Secure Internet voting.
- and much more ...



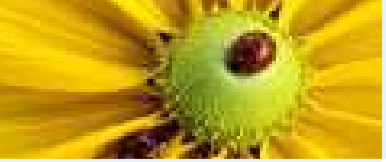
Problem abstraction

- A set of actors with private inputs would like to compute a function of these inputs.



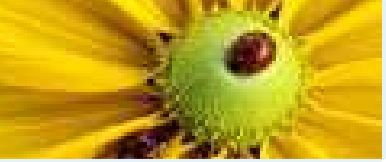
Problem abstraction

- A set of actors with private inputs would like to compute a function of these inputs.
- Example: **voting**.



Problem abstraction

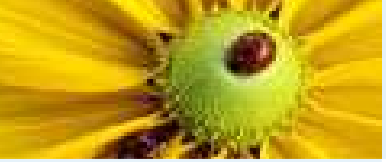
- A set of actors with private inputs would like to compute a function of these inputs.
- Example: **voting**.
- Can this be done while keeping the inputs private?



Problem abstraction

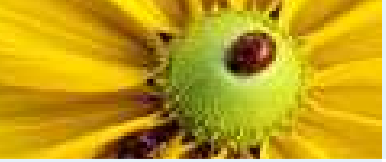
- A set of actors with private inputs would like to compute a function of these inputs.
- Example: **voting**.
- Can this be done while keeping the inputs private?

SECURE MULTI-PARTY COMPUTATION.



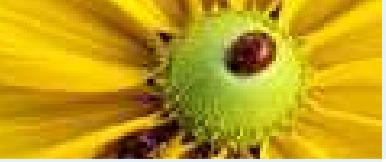
Milestones

- Danish sugar beet auctions.



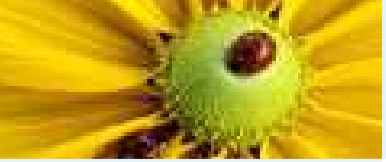
Milestones

- Danish sugar beet auctions.
- (Pinkas et. al.) Secure evaluation of an AES encryption.



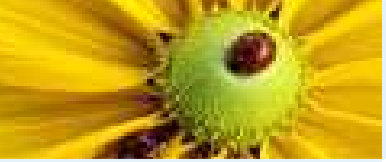
Milestones

- Danish sugar beet auctions.
- (Pinkas et. al.) Secure evaluation of an AES encryption.
- IARPA projects.



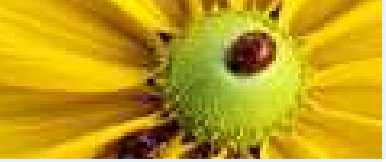
Privacy protection in electronic commerce

- During an electronic transaction, reveal as little as is necessary to complete the transaction.



Privacy protection in electronic commerce

- During an electronic transaction, reveal as little as is necessary to complete the transaction.
- Make your transactions unlinkable to you and to each other.

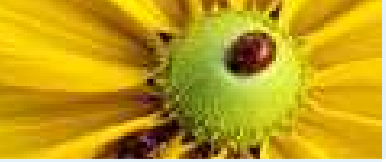


NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE

Enhancing Online Choice, Efficiency, Security, and Privacy

APRIL 2011

THE WHITE HOUSE
WASHINGTON



Example: majority of three

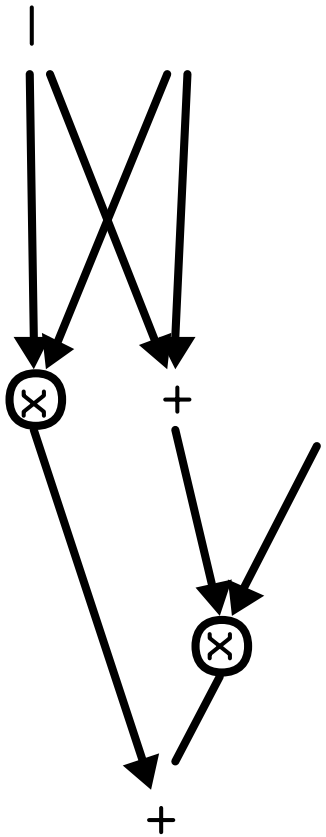
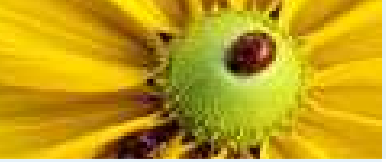
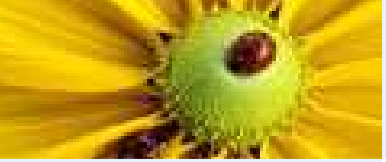


Figure 1: The problem reduces to providing valid bit commitments for each of the wires of the circuit and opening the output.



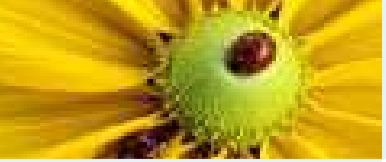
The bottleneck

- Multiplication is hard, addition easy.



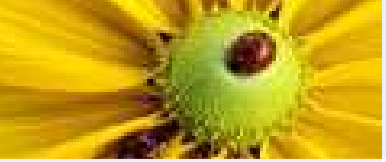
The bottleneck

- Multiplication is hard, addition easy.
- Multiplication forces interaction



The bottleneck

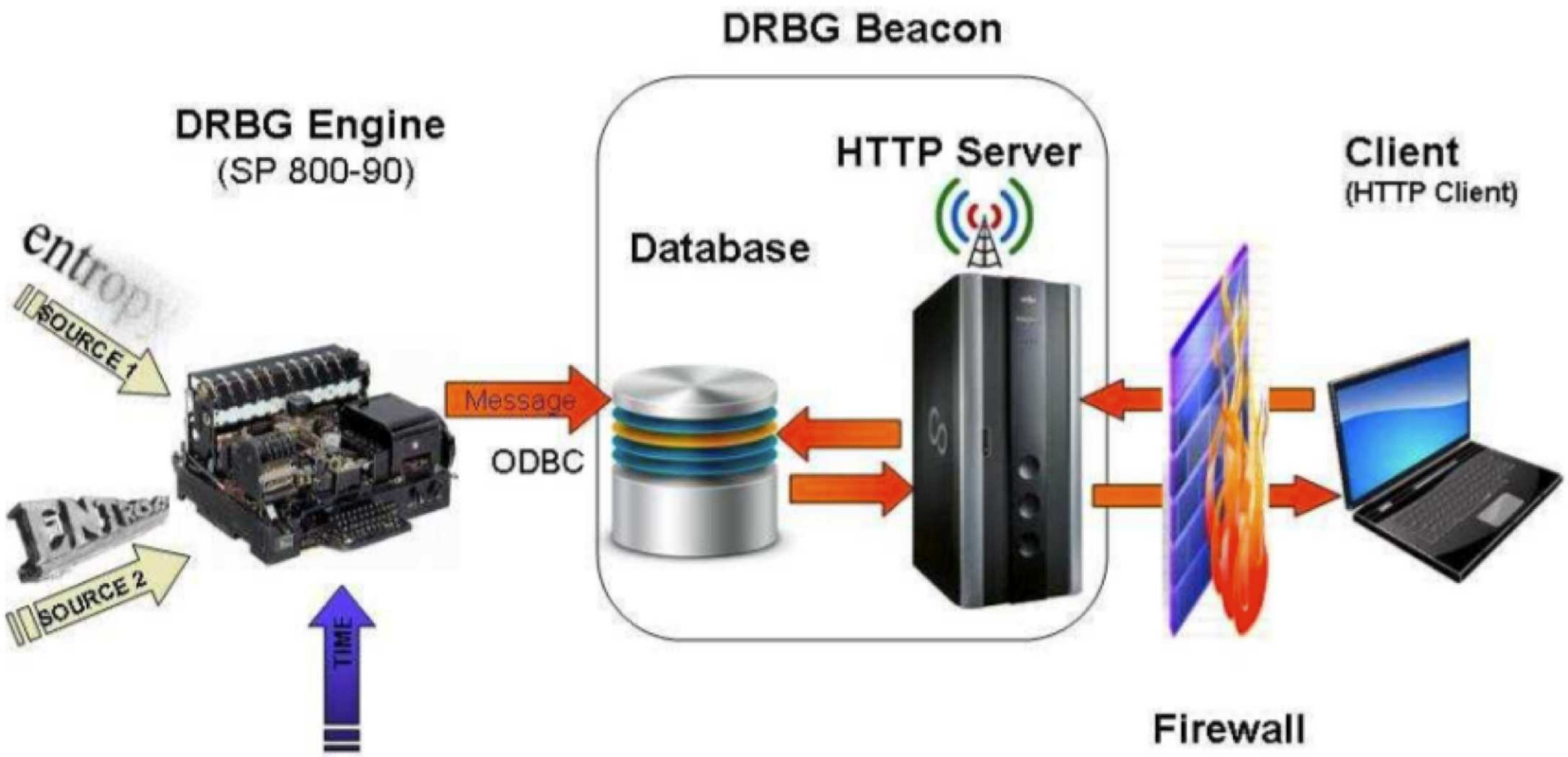
- Multiplication is hard, addition easy.
- Multiplication forces interaction **in the standard transaction environment**.

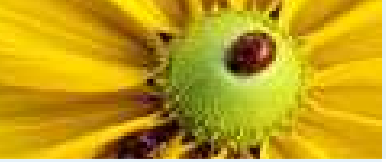


The bottleneck

- Multiplication is hard, addition easy.
- Multiplication forces interaction **in the standard transaction environment**.
- Let's enhance the environment.

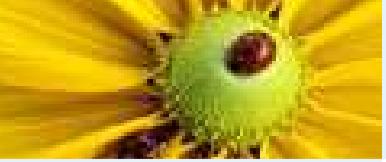
Prototype architecture.





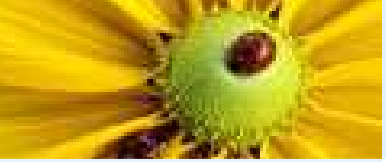
Set certification

- How about an online service that certifies encrypted values have a given property.

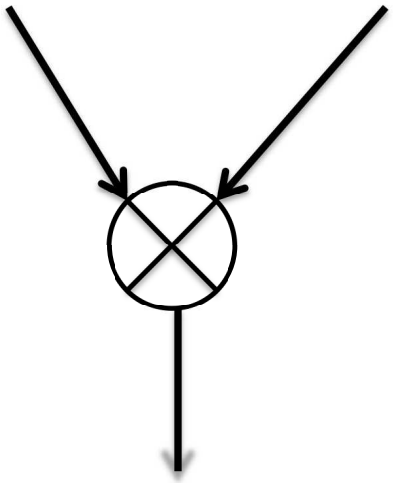


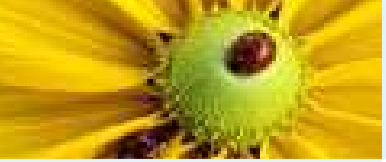
Set certification

- How about an online service that certifies encrypted values have a given property.
- The property is generic. It does not reveal information about any particular attribute of the user.

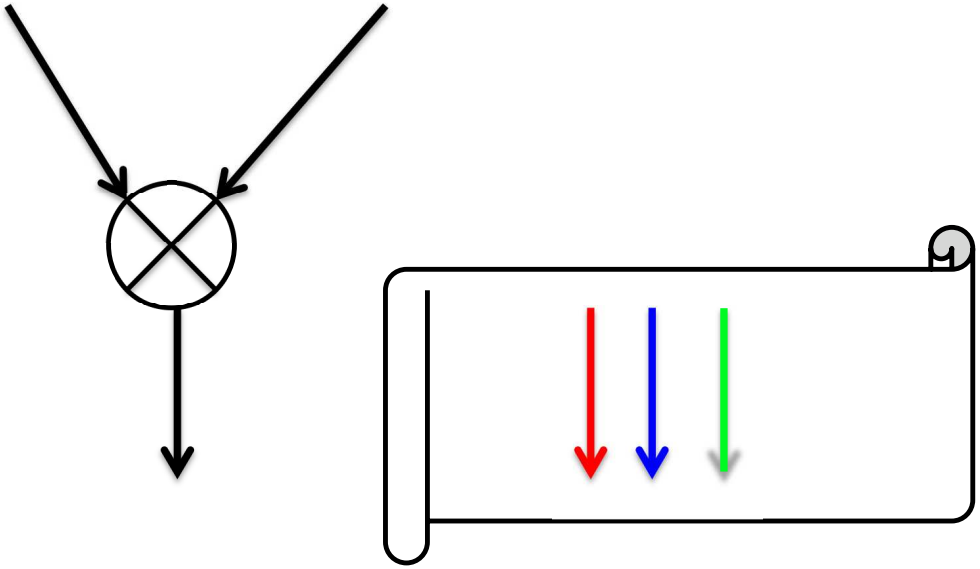


Set certification

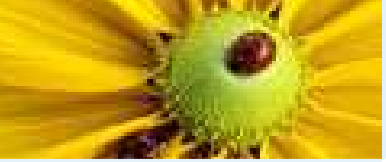




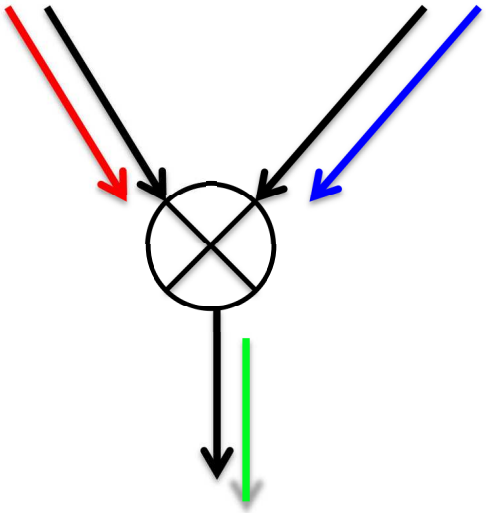
Set certification

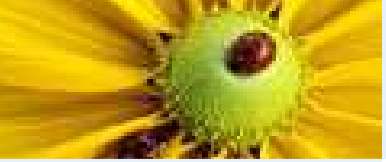


Certify as belonging to the set {000,010,100,111}



Set certification





THANK YOU.