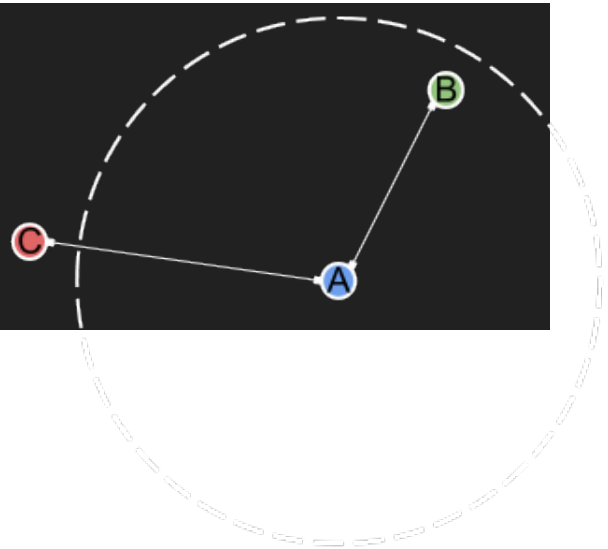
Privacy-preserving Location Proximity

Per Hallgren, Chalmers Univ. Gothenburg

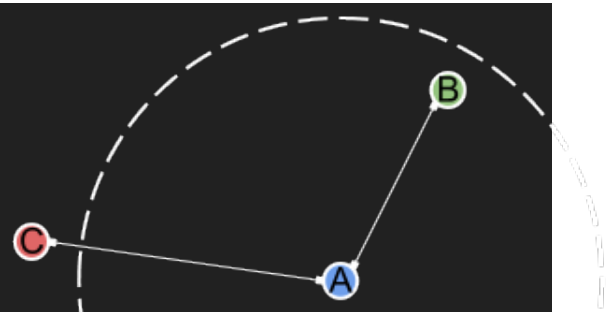
Martín Ochoa, Siemens AG (Recently TUM)
Andrei Sabelfeld, Chalmers University of Technology

TOC



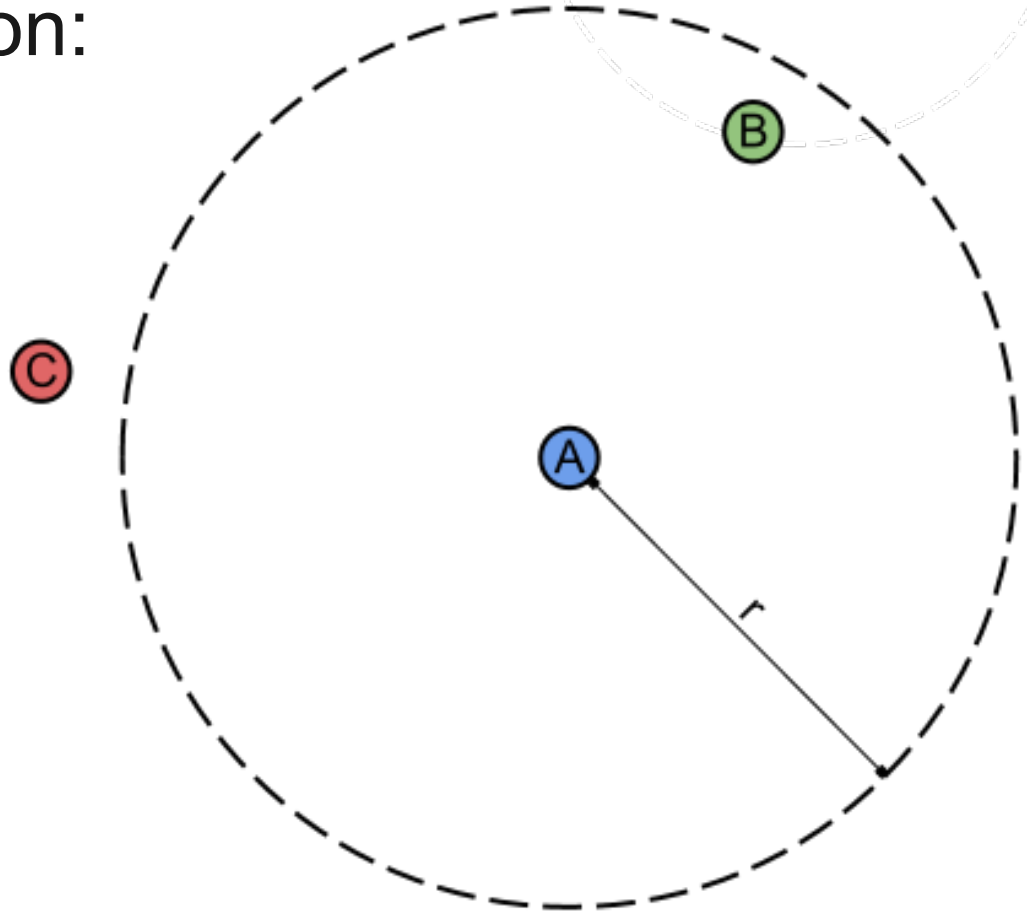
1. Background
2. Protocol
3. Theoretical Evaluation
4. Practical Evaluation

Proximity Testing

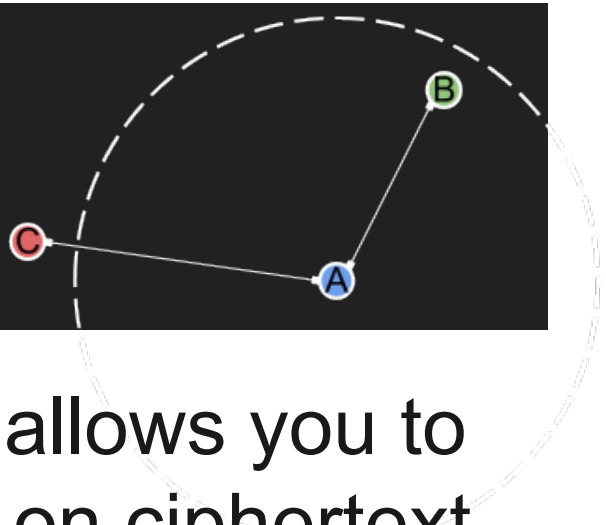


Answers the question:

"Am I close?"



Homomorphic Encryption



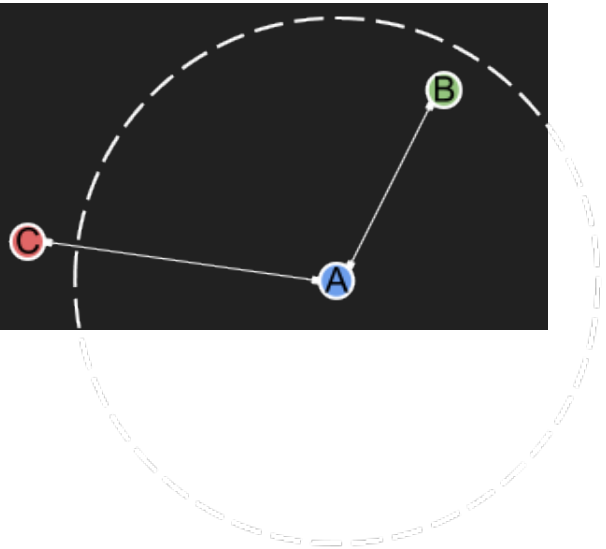
A homorphic encryption scheme allows you to perform decipherable operations on ciphertext.

RSA: $E(x) = x^e \bmod m$

RSA is *multiplicatively* homomorphic

$E(x) \times E(y) = x^e \times y^e \bmod m = (x \times y)^e \bmod m = E(x \times y)$

Homomorphic Encryption



Paillier: $E(x) = g^x \bmod m$

Paillier is *additively* homomorphic

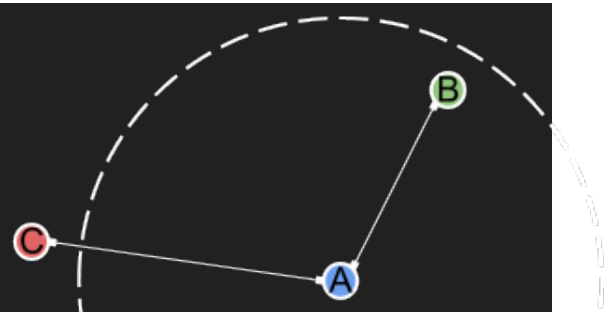
$E(x) \times E(y) = g^x \times g^y \bmod m = g^{x+y} \bmod m = E(x+y)$

Paillier also has this exiting property

$E(x)^y = (g^x)^y \bmod m = g^{x \times y} \bmod m = E(x \times y)$

Protocol

Mission Statement

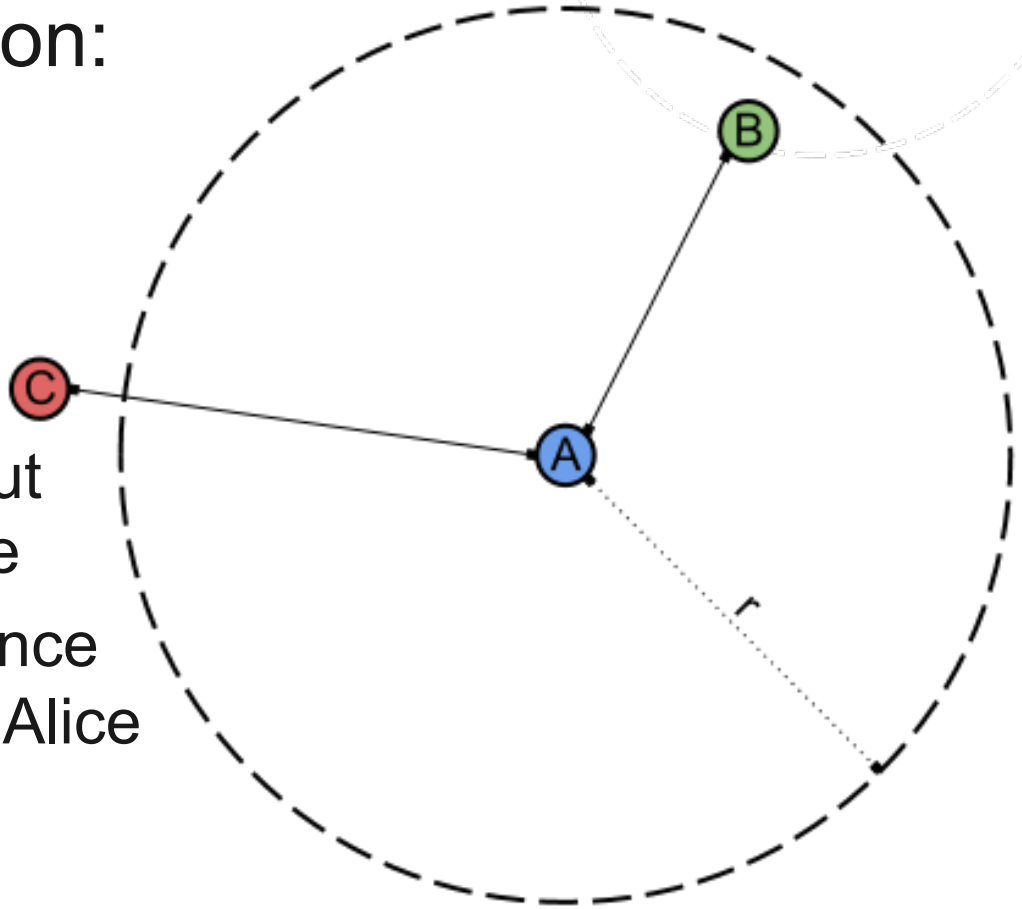


Answers the question:

"Am I close?"

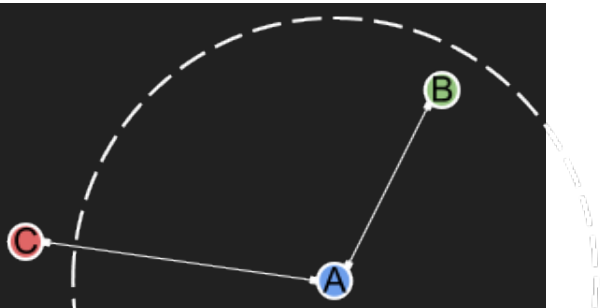
Without disclosing:

- Any information about Alice to Bob or Claire
- The position or distance of Bob and Claire to Alice



Protocol

Mission Statement

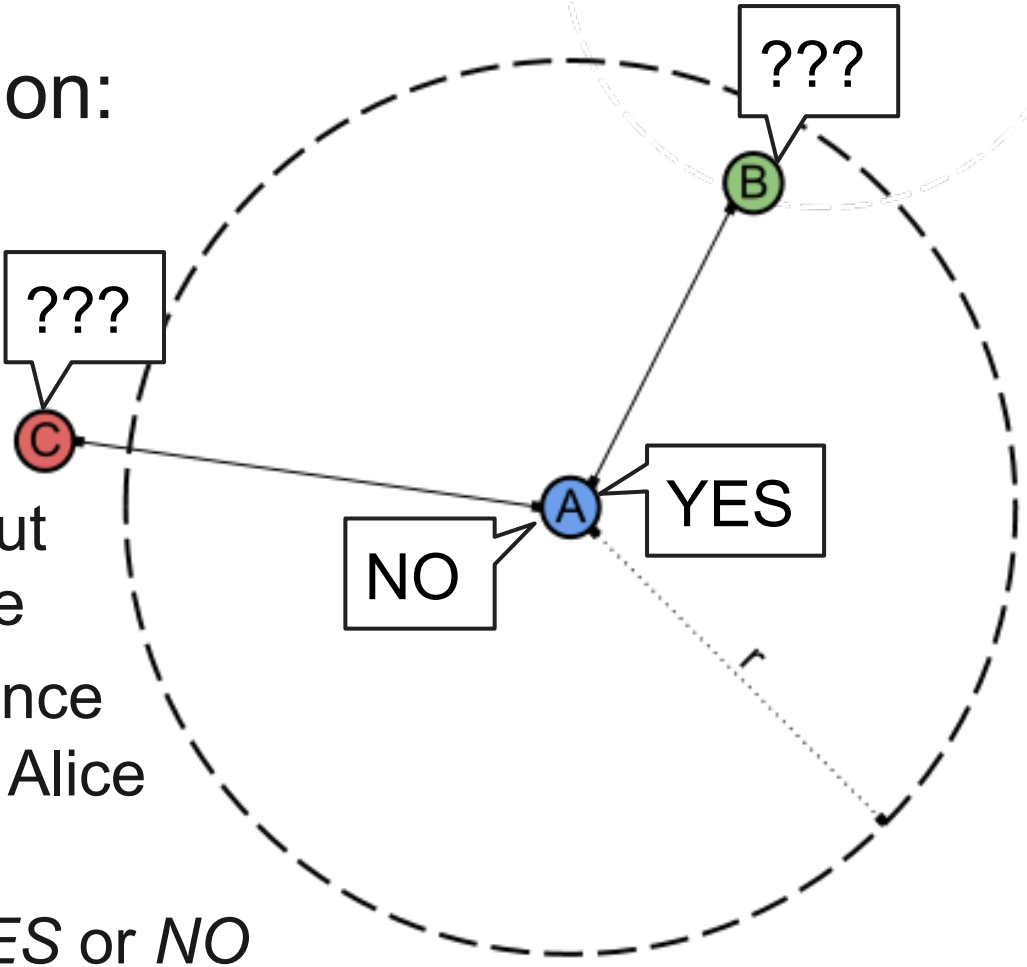


Answers the question:

"Am I close?"

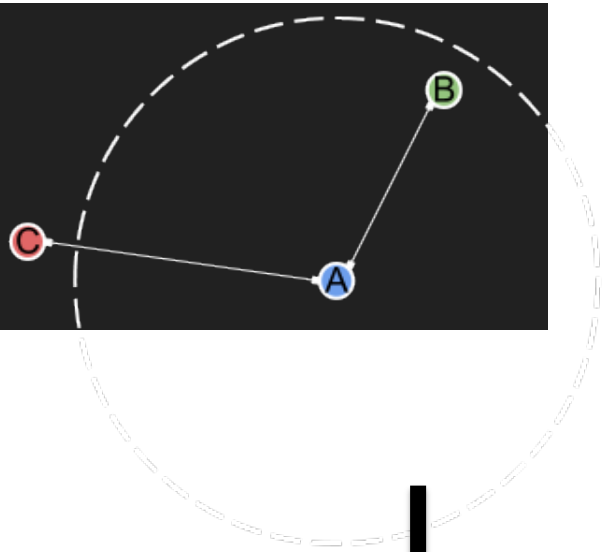
Without disclosing:

- Any information about Alice to Bob or Claire
- The position or distance of Bob and Claire to Alice



We **ONLY** say either *YES* or *NO*

Protocol
Outline



We **ONLY** say either *YES* or *NO*

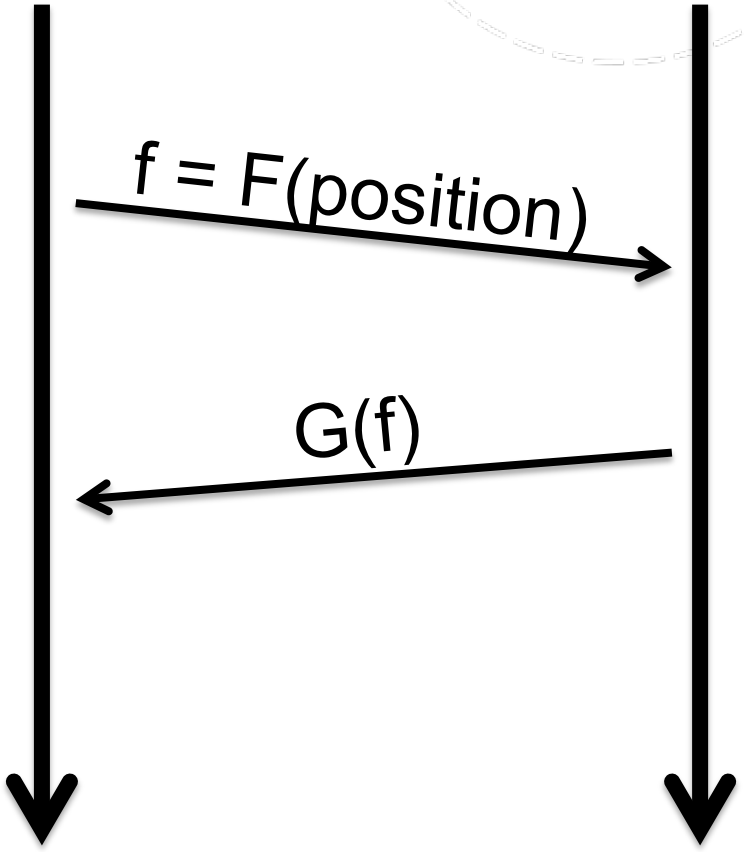
Alice

- Sends *encrypted* info to Bob

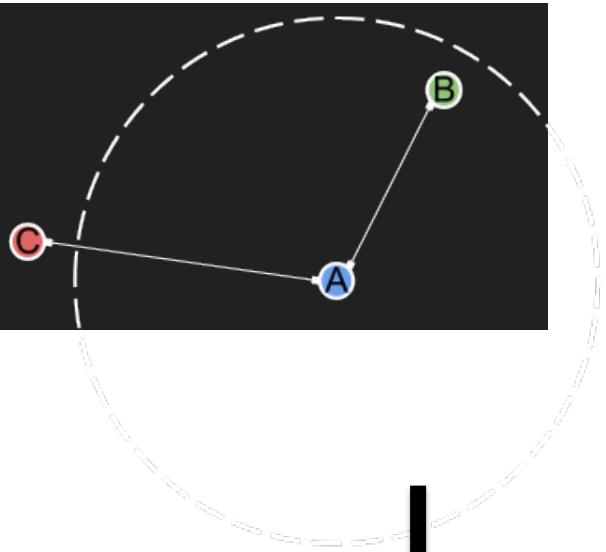
Bob

- Computes distance
- Sends boleanized distance

Done!



Protocol
Outline



We **ONLY** say either *YES* or *NO*

Alice:

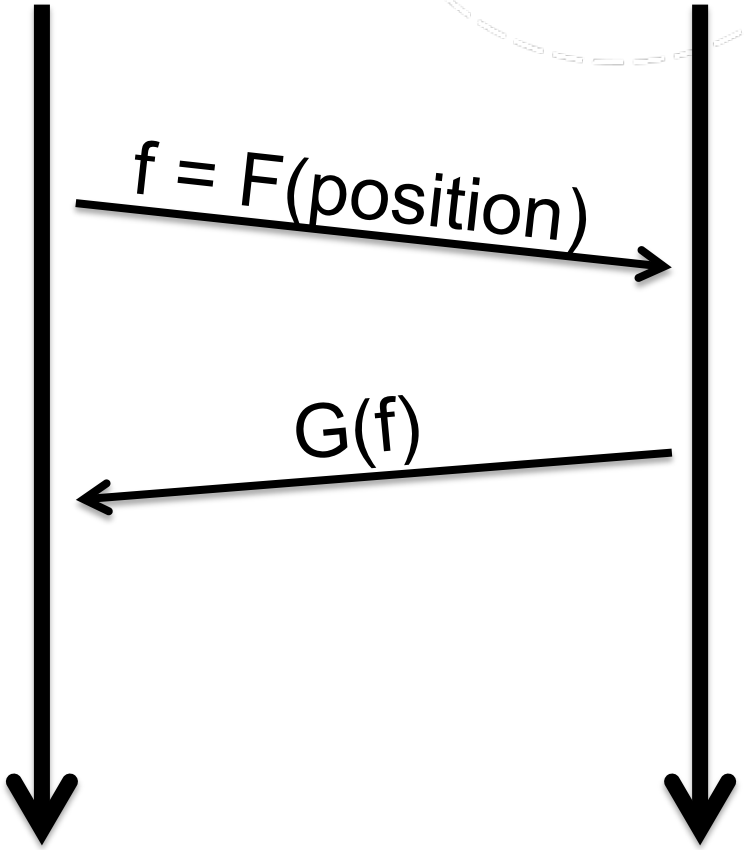
2 Sends *encrypted* info to Bob

Bob

1 Computes distance

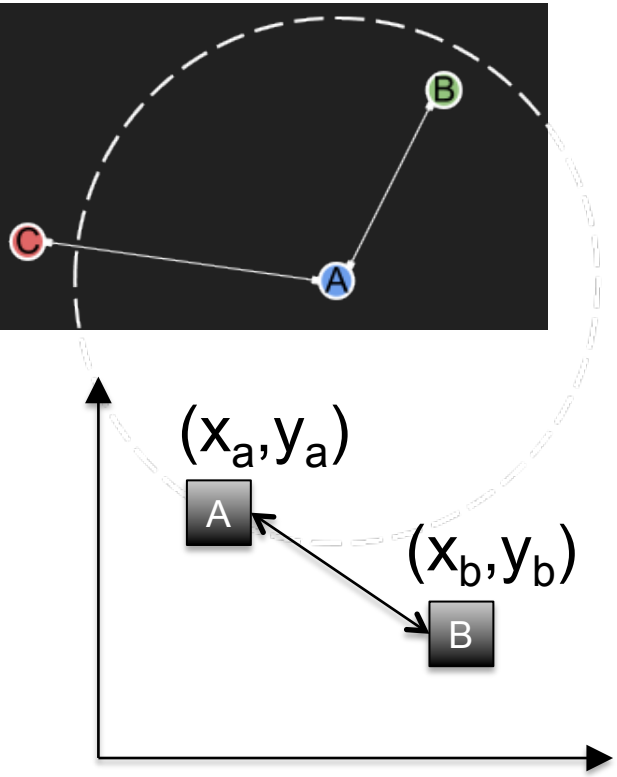
3 Sends boleanized distance

Done!



Protocol

Distance Calculation



Trivial Geometry

Distance from A to B:

$$d = \sqrt{(x_a - y_b)^2 + (y_a - y_b)^2}$$

$$D = (x_a - y_b)^2 + (y_a - y_b)^2$$

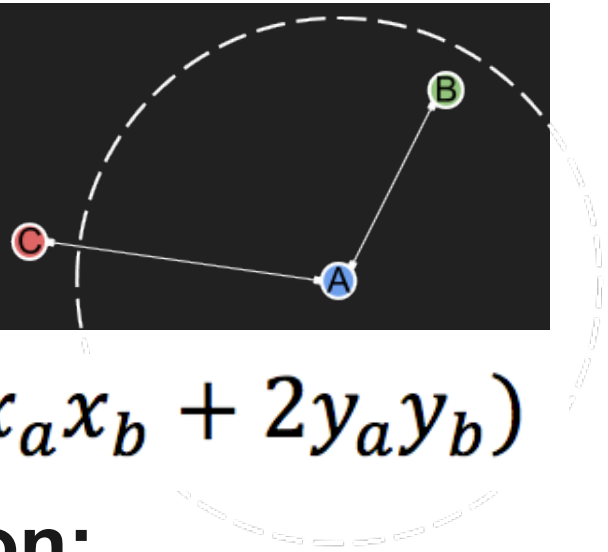
Expand & rewrite as:

$$D = x_a^2 + x_b^2 + y_a^2 + y_b^2 - 2x_a x_b - 2y_a y_b$$

$$D = x_a^2 + y_a^2 + x_b^2 + y_b^2 - (2x_a x_b + 2y_a y_b)$$

Protocol

Distance Calculation



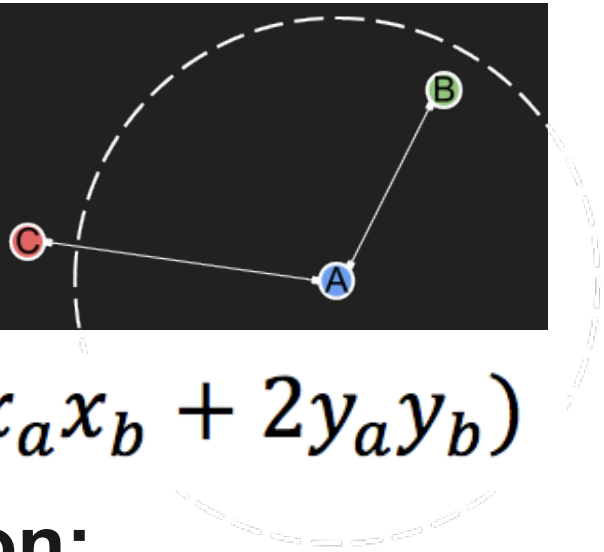
$$D = x_a^2 + y_a^2 + x_b^2 + y_b^2 - (2x_a x_b + 2y_a y_b)$$

Using Homomorphic Encryption:

$$E(D) = E\left(x_a^2 + y_a^2 + x_b^2 + y_b^2 - (2x_a x_b + 2y_a y_b)\right)$$

Protocol

Distance Calculation



$$D = x_a^2 + y_a^2 + x_b^2 + y_b^2 - (2x_a x_b + 2y_a y_b)$$

Using Homomorphic Encryption:

$$E(D) = E\left(x_a^2 + y_a^2 + x_b^2 + y_b^2 - (2x_a x_b + 2y_a y_b)\right)$$

Recall!

Paillier is *additively* homomorphic

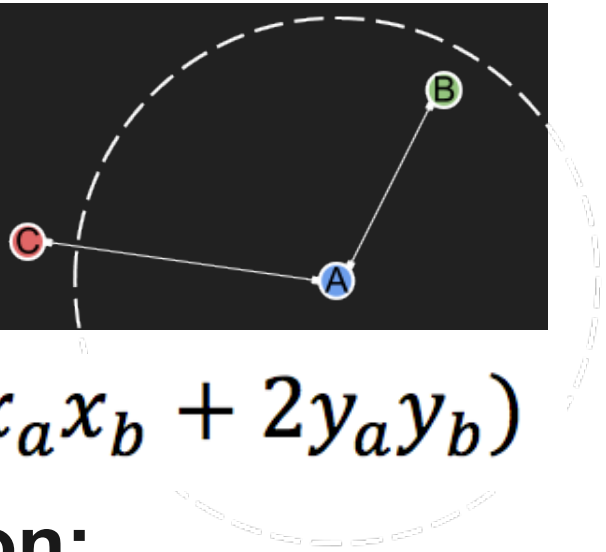
$E(x) \times E(y) = g^x \times g^y \bmod m = E(x+y)$

And thus:

$E(x) / E(y) = g^x / g^y \bmod m = E(x-y)$

Protocol

Distance Calculation



$$D = x_a^2 + y_a^2 + x_b^2 + y_b^2 - (2x_a x_b + 2y_a y_b)$$

Using Homomorphic Encryption:

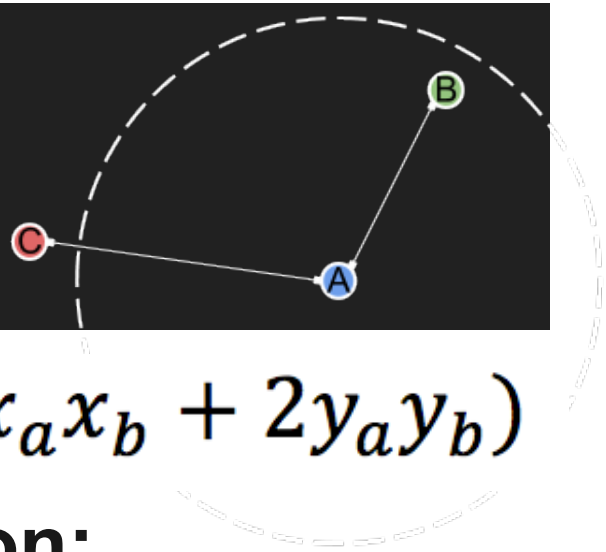
$$E(D) = E\left(x_a^2 + y_a^2 + x_b^2 + y_b^2 - (2x_a x_b + 2y_a y_b)\right)$$

$$E(D) = \frac{E\left(x_a^2 + y_a^2 + x_b^2 + y_b^2\right)}{E(2x_a x_b + 2y_a y_b)}$$

$$E(D) = \frac{E(x_a^2 + y_a^2)E(x_b^2 + y_b^2)}{E(2x_a x_b)E(2y_a y_b)}$$

Protocol

Distance Calculation



$$D = x_a^2 + y_a^2 + x_b^2 + y_b^2 - (2x_a x_b + 2y_a y_b)$$

Using Homomorphic Encryption:

$$E(D) = \frac{E(x_a^2+y_a^2)E(x_b^2+y_b^2)}{E(2x_a x_b)E(2y_a y_b)}$$

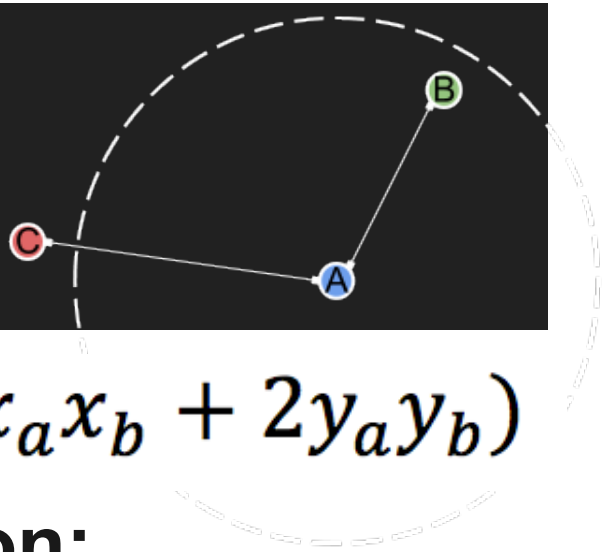
Recall!

Raising a cipher text to a plaintext is multiplication

$E(x)^y = (g^x)^y \bmod m = g^{x \times y} \bmod m$

Protocol

Distance Calculation



$$D = x_a^2 + y_a^2 + x_b^2 + y_b^2 - (2x_a x_b + 2y_a y_b)$$

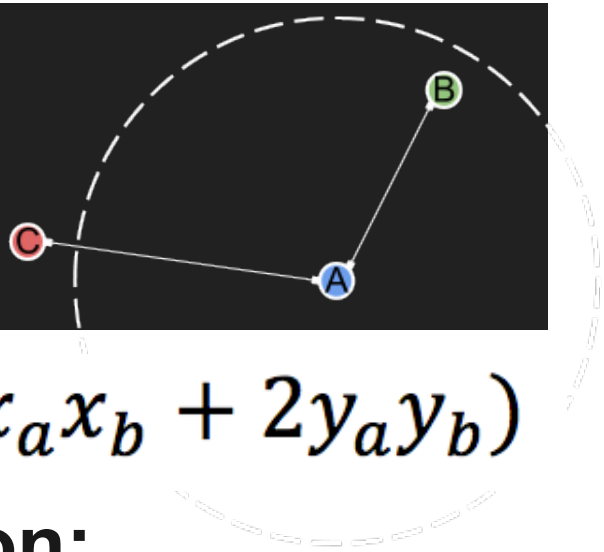
Using Homomorphic Encryption:

$$E(D) = \frac{E(x_a^2+y_a^2)E(x_b^2+y_b^2)}{E(2x_a x_b)E(2y_a y_b)}$$

$$E(D) = \frac{E(x_a^2+y_a^2)E(x_b^2+y_b^2)}{E(2x_a)^{x_b}E(2y_a)^{y_b}}$$

Protocol

Distance Calculation



$$D = x_a^2 + y_a^2 + x_b^2 + y_b^2 - (2x_a x_b + 2y_a y_b)$$

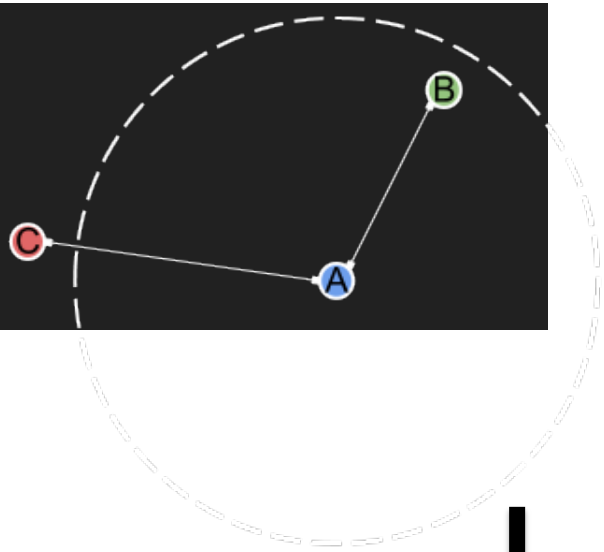
Using Homomorphic Encryption:

$$E(D) = \frac{E(x_a^2+y_a^2)E(x_b^2+y_b^2)}{E(2x_a x_b)E(2y_a y_b)}$$

$$E(D) = \frac{E(x_a^2+y_a^2)E(x_b^2+y_b^2)}{E(2x_a)^{x_b}E(2y_a)^{y_b}}$$

Protocol

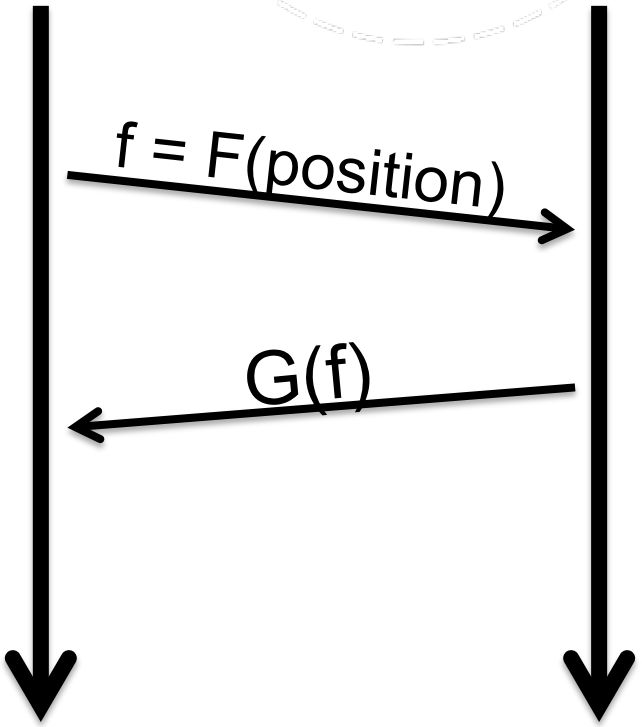
Distance Calculation



$$E(D) = \frac{E(x_a^2+y_a^2)E(x_b^2+y_b^2)}{E(2x_a)^{x_b}E(2y_a)^{y_b}}$$

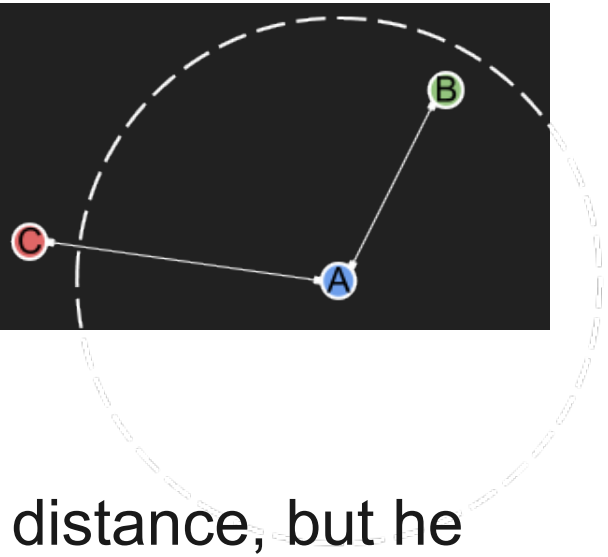
F(position)

$$E(x_a^2 + y_a^2) \parallel E(2x_a) \parallel E(2y_a)$$



Protocol

Distance Obfuscation

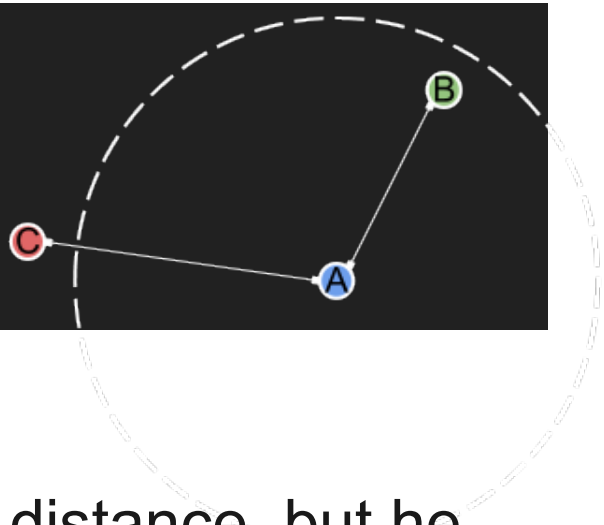


How to obscure the distance?

Now we know how Bob can compute the distance, but he doesn't want to tell Alice what the distance is!

Protocol

Distance Obfuscation



How to obscure the distance?

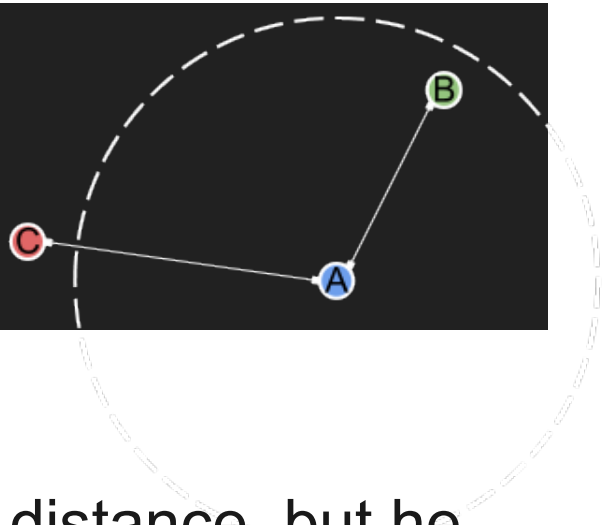
Now we know how Bob can compute the distance, but he doesn't want to tell Alice what the distance is!

- Oblivious comparison:

  (D-x) * rand()

Protocol

Distance Obfuscation



How to obscure the distance?

Now we know how Bob can compute the distance, but he doesn't want to tell Alice what the distance is!

- Oblivious comparison:

  (D-x) * rand()

$$\left(\frac{E_{K_A}(D)}{E_{K_A}(x)} \right)^{\rho}$$

Protocol

Distance Obfuscation

How to obscure the distance?

Now we know how Bob can compute the distance, but he doesn't want to tell Alice what the distance is!

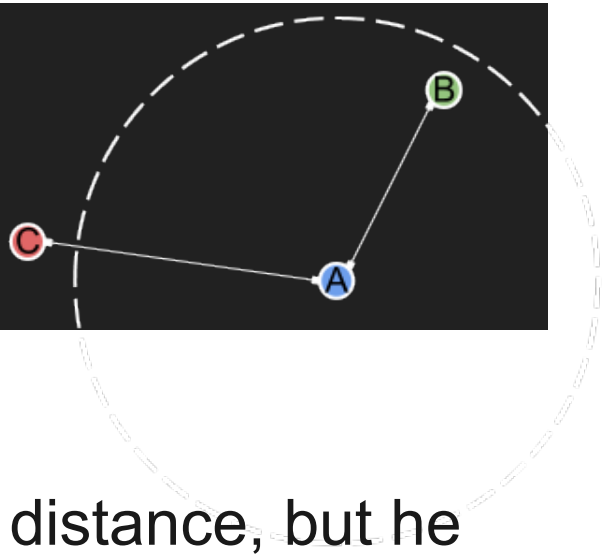
- Oblivious comparison:

  (D-x) * rand()

- For every x < r^2!

Protocol

Distance Obfuscation



How to obscure the distance?

Now we know how Bob can compute the distance, but he doesn't want to tell Alice what the distance is!

- Oblivious comparison:

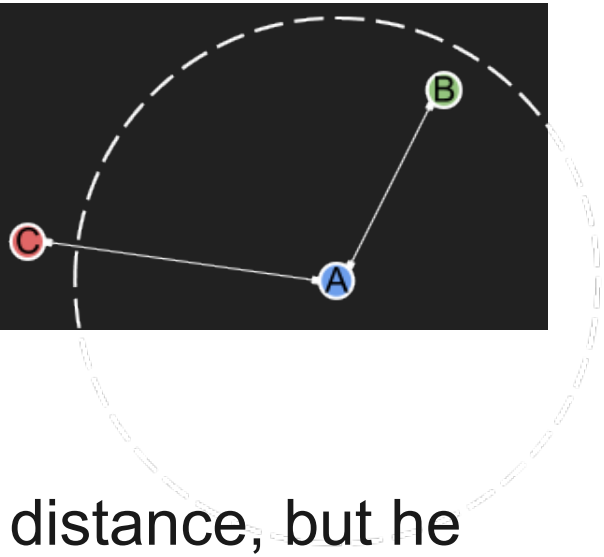
  (D-x) * rand()

- For every x < r^2!

$$\left(\frac{E_{K_A}(D)}{E_{K_A}(0)}\right)^{\rho_0} :: \left(\frac{E_{K_A}(D)}{E_{K_A}(1)}\right)^{\rho_2} :: \cdots :: \left(\frac{E_{K_A}(D)}{E_{K_A}(r^2)}\right)^{\rho_{r^2}}$$

Protocol

Distance Obfuscation



How to obscure the distance?

Now we know how Bob can compute the distance, but he doesn't want to tell Alice what the distance is!

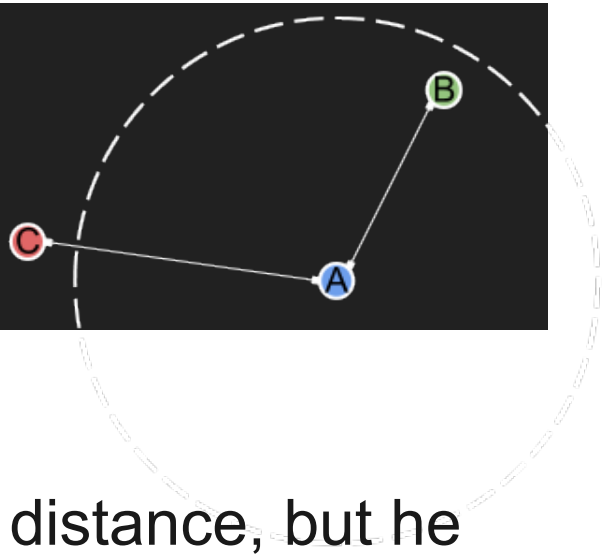
- Oblivious comparison:

  (D-x) * rand()
- For every x < r^2!
- Is this enough?

$$\left(\frac{E_{K_A}(D)}{E_{K_A}(0)}\right)^{\rho_0} :: \left(\frac{E_{K_A}(D)}{E_{K_A}(1)}\right)^{\rho_2} :: \cdots :: \left(\frac{E_{K_A}(D)}{E_{K_A}(r^2)}\right)^{\rho_{r^2}}$$

Protocol

Distance Obfuscation



How to obscure the distance?

Now we know how Bob can compute the distance, but he doesn't want to tell Alice what the distance is!

- Oblivious comparison:

  (D-x) * rand()
- For every x < r^2!
- Is this enough? **NO!**

$$\left(\frac{E_{K_A}(D)}{E_{K_A}(0)}\right)^{\rho_0} :: \left(\frac{E_{K_A}(D)}{E_{K_A}(1)}\right)^{\rho_2} :: \cdots :: \left(\frac{E_{K_A}(D)}{E_{K_A}(r^2)}\right)^{\rho_{r^2}}$$

Protocol

Distance Obfuscation

How to obscure the distance?

Now we know how Bob can compute the distance, but he doesn't want to tell Alice what the distance is!

- Oblivious comparison:

  (D-x) * rand()
- For every x < r^2!
- Is this enough?
- Also shuffle!

Protocol

Distance Obfuscation

How to obscure the distance?

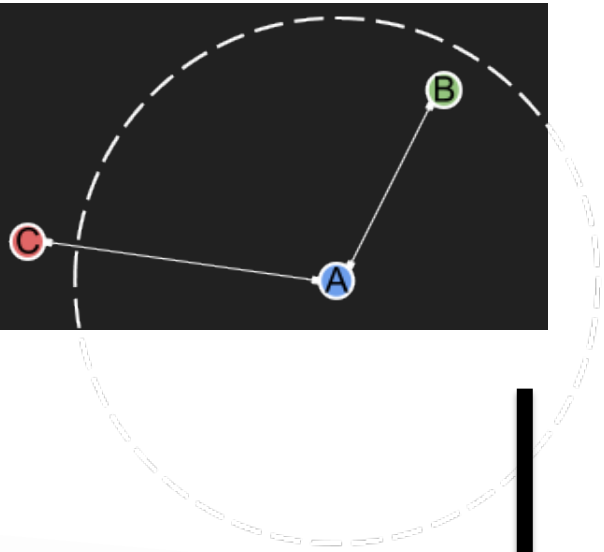
Now we know how Bob can compute the distance, but he doesn't want to tell Alice what the distance is!

$$\gamma = \left(\frac{E_A(D)}{E_A(0)}\right)^{\rho_0} :: \left(\frac{E_A(D)}{E_A(1)}\right)^{\rho_2} :: \cdots :: \left(\frac{E_A(D)}{E_A(r^2)}\right)^{\rho_{r^2}}$$

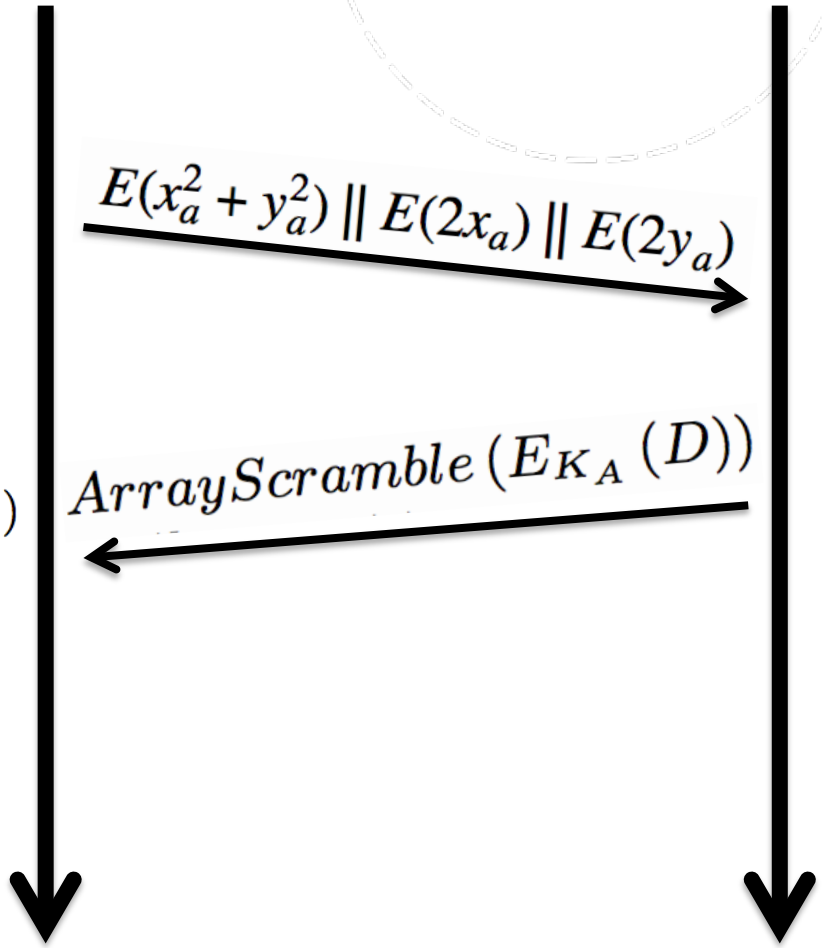
$$\alpha = \texttt{scramble}(\gamma)$$

Protocol

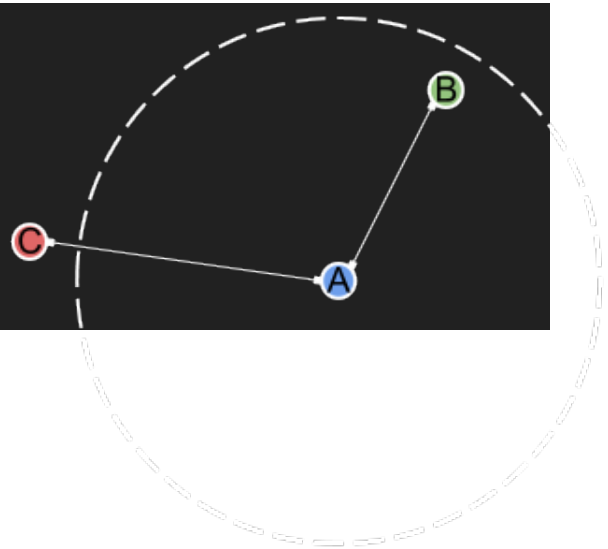
Final Result



1: $\mathbf{A} \rightarrow \mathbf{B}\ E_A(2x_a) :: E_A(2y_a) :: E_A(x_a^2 + y_a^2)$
2: $\mathbf{B} \rightarrow \mathbf{A}\ \alpha = ArrayScramble\left(E_A\left(D\right)\right)$
3: $\mathbf{A}$ executes `any` $([D_A\left(c\right) == 0$ `for` c `in` $\alpha])$



Theoretical Evaluation



Runtime Analysis

Paillier

Encryption: O(log(n) * M(n))

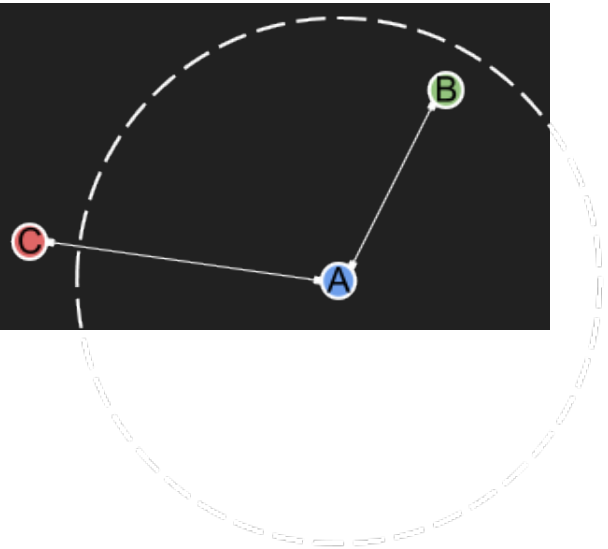
Decryption: O(log(n) * M(n))

Alice1: O(3log(n) * M(n))

Bob: O(r^2 * log(n) * M(n))

Alice2: O(r^2 * log(n) * M(n))

Theoretical Evaluation

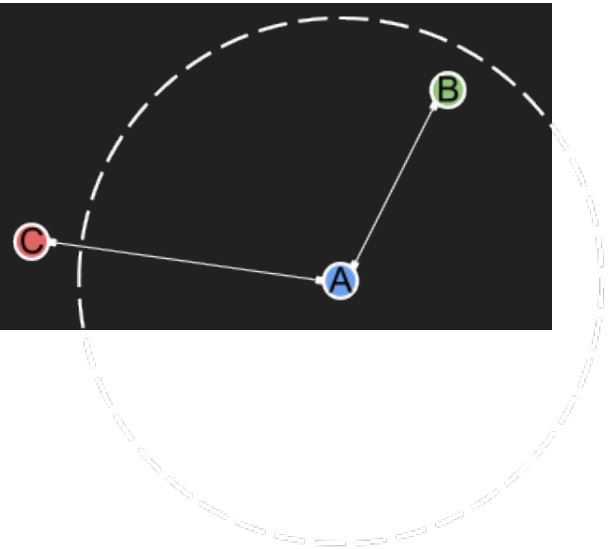


Size Analysis

Paillier ciphertext: O(log(n))

Size of response from Bob: O(r^2 * log(n))

Practical Evaluation



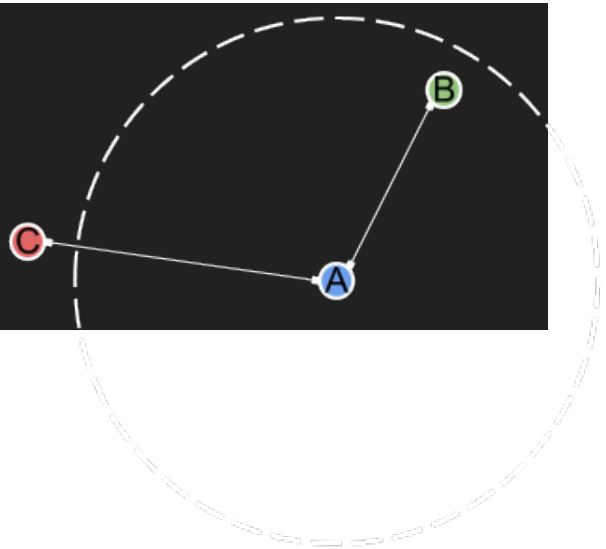
Proof of concept

Small server-client application

Server relays messages to appropriate clients

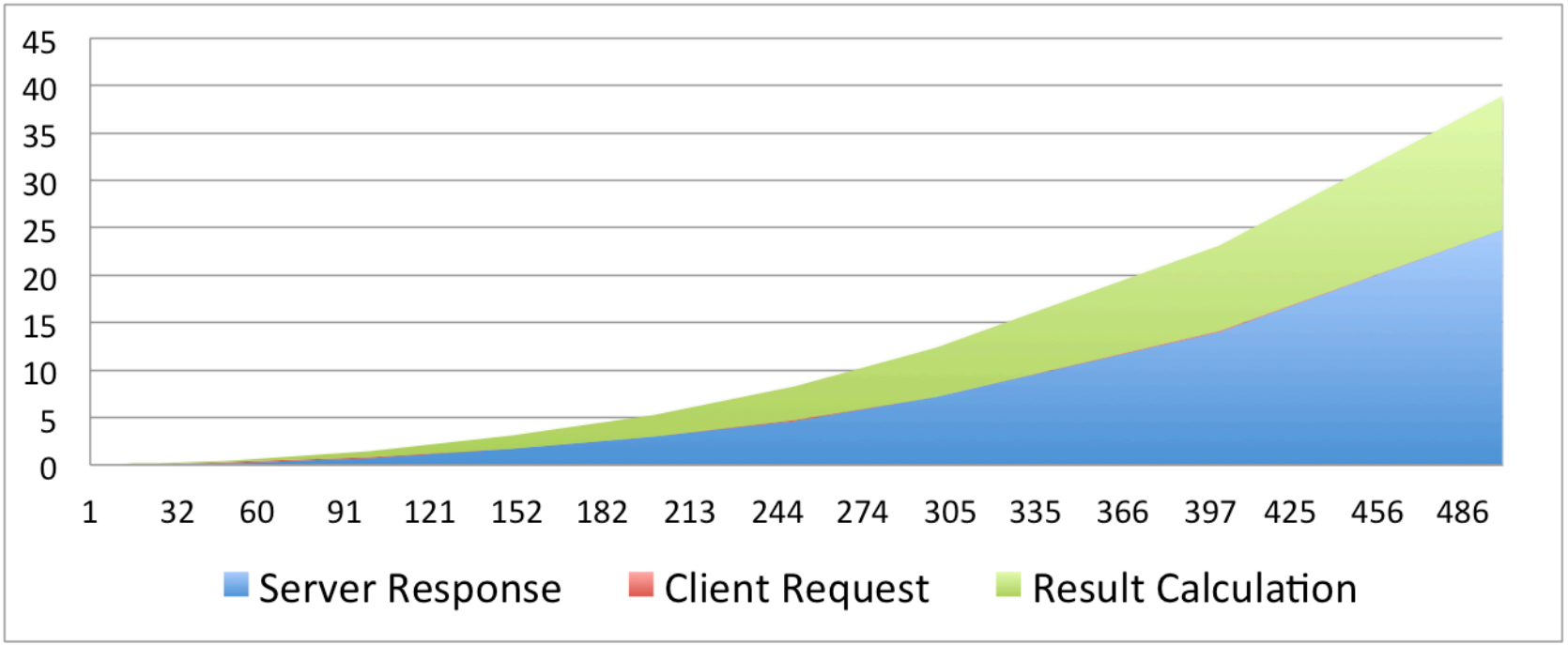
All clients are interested in each other

Practical Evaluation

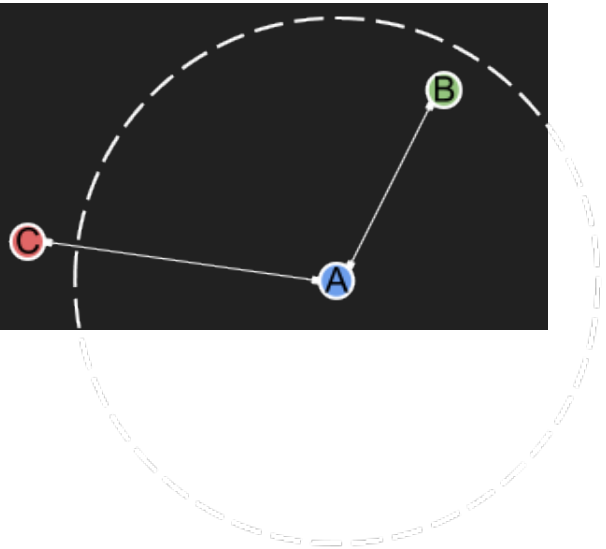


Benchmarks

80 bit key



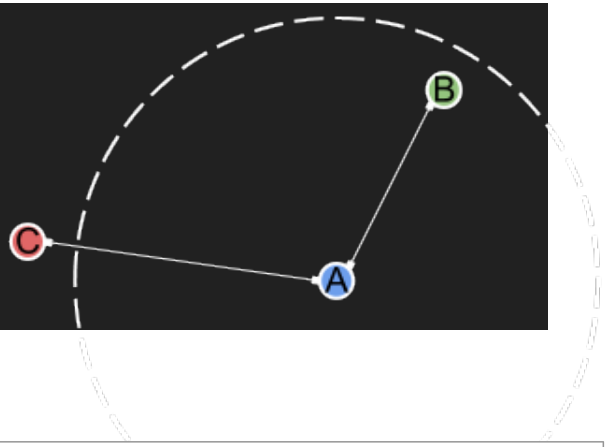
Practical Evaluation



Benchmarks

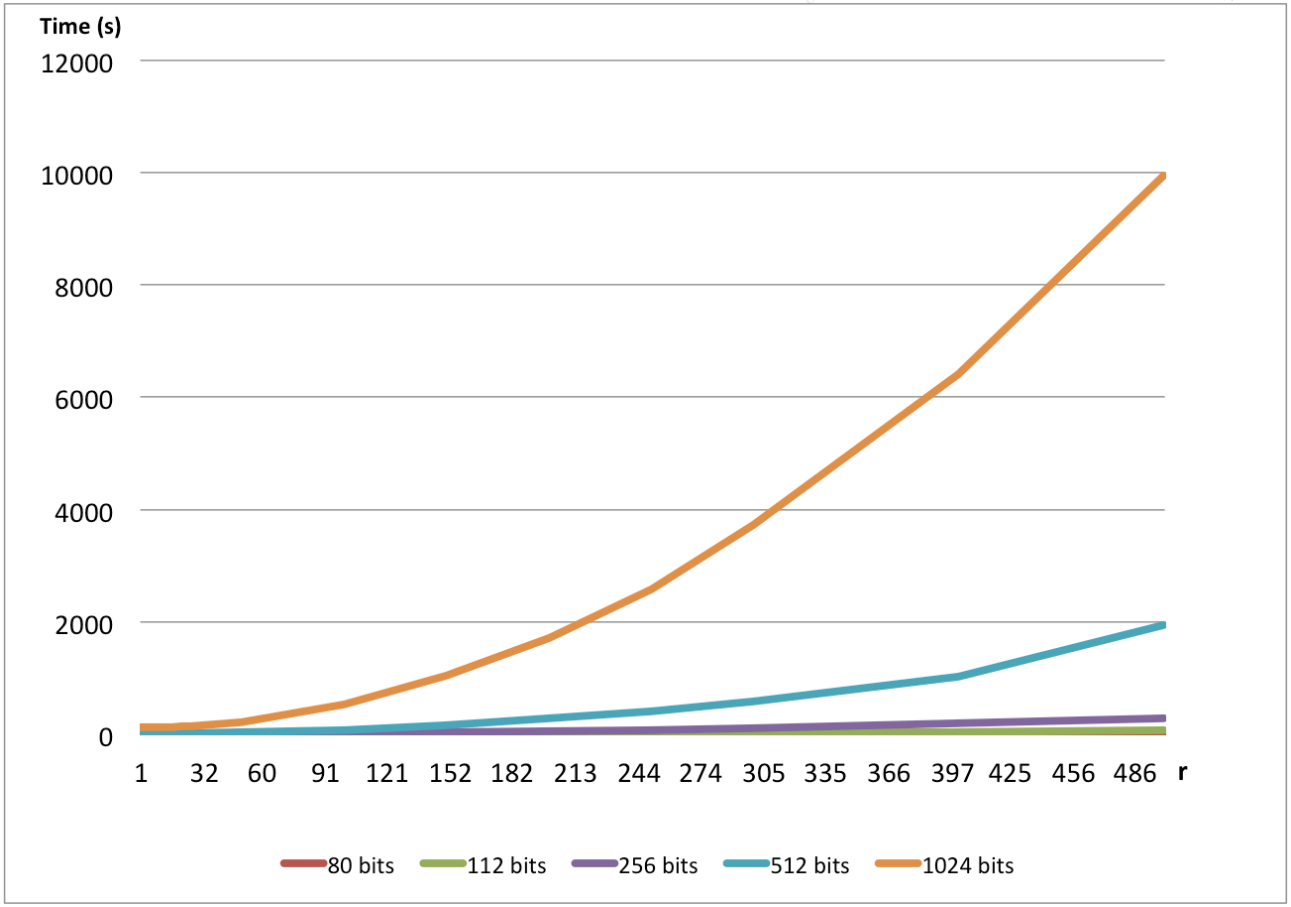
1024 bit key

Practical Evaluation

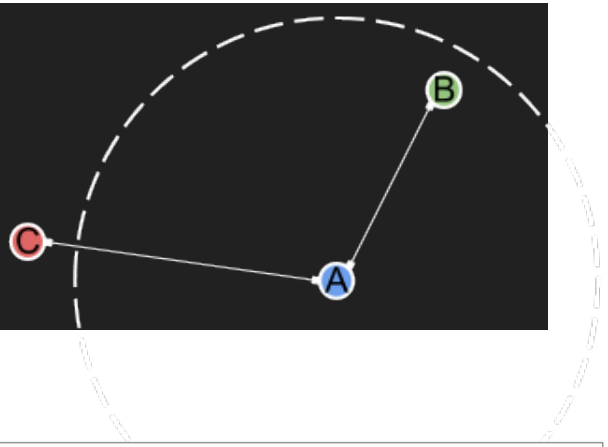


Benchmarks

Keysize comparison



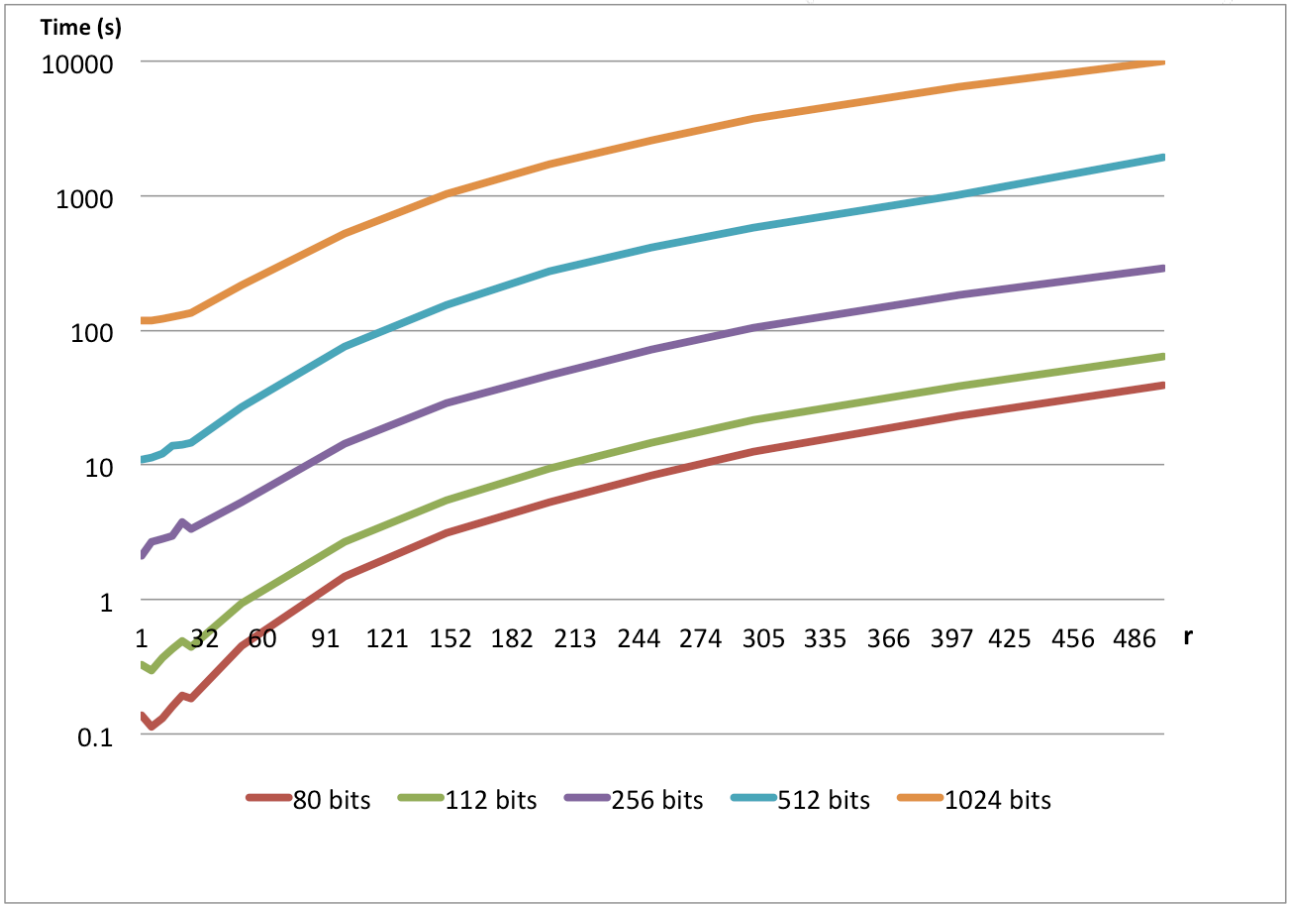
Practical Evaluation



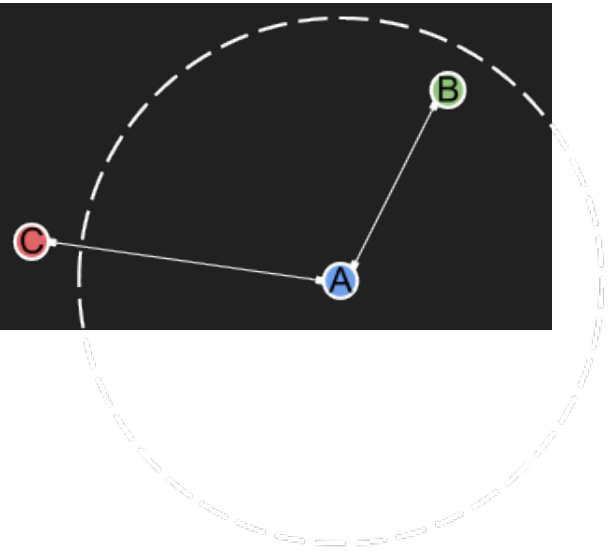
Benchmarks

Keysize comparison

Log scale



Thank You!



Questions?

Thank You!