Post-Quantum Merkle Puzzles

Cryptography Research Seminar

Kimia Shaban

University of Waterloo

March 3rd/2023

Public-Key Cryptography

- Public-key cryptography uses the idea of keys for secure communication between any two parties, similar to symmetric-key cryptography, but the parties are allowed a public key that anyone can access.

Public-Key Cryptography

- Public-key cryptography uses the idea of keys for secure communication between any two parties, similar to symmetric-key cryptography, but the parties are allowed a public key that anyone can access.
- In this case secure communication is defined such that any two parties, Alice and Bob can communicate with each other, without an eavesdropper, Eve, being able to listen in without a significant computational cost.

Public-Key Cryptography

- Public-key cryptography uses the idea of keys for secure communication between any two parties, similar to symmetric-key cryptography, but the parties are allowed a public key that anyone can access.
- In this case secure communication is defined such that any two parties, Alice and Bob can communicate with each other, without an eavesdropper, Eve, being able to listen in without a significant computational cost.
- Suppose that Alice and Bob want to communicate securely. We can consider a pair (P_A, S_A) to be a tuple consisting of a public key, and a private key for Alice to decrypt messages.

Public-Key Cryptography

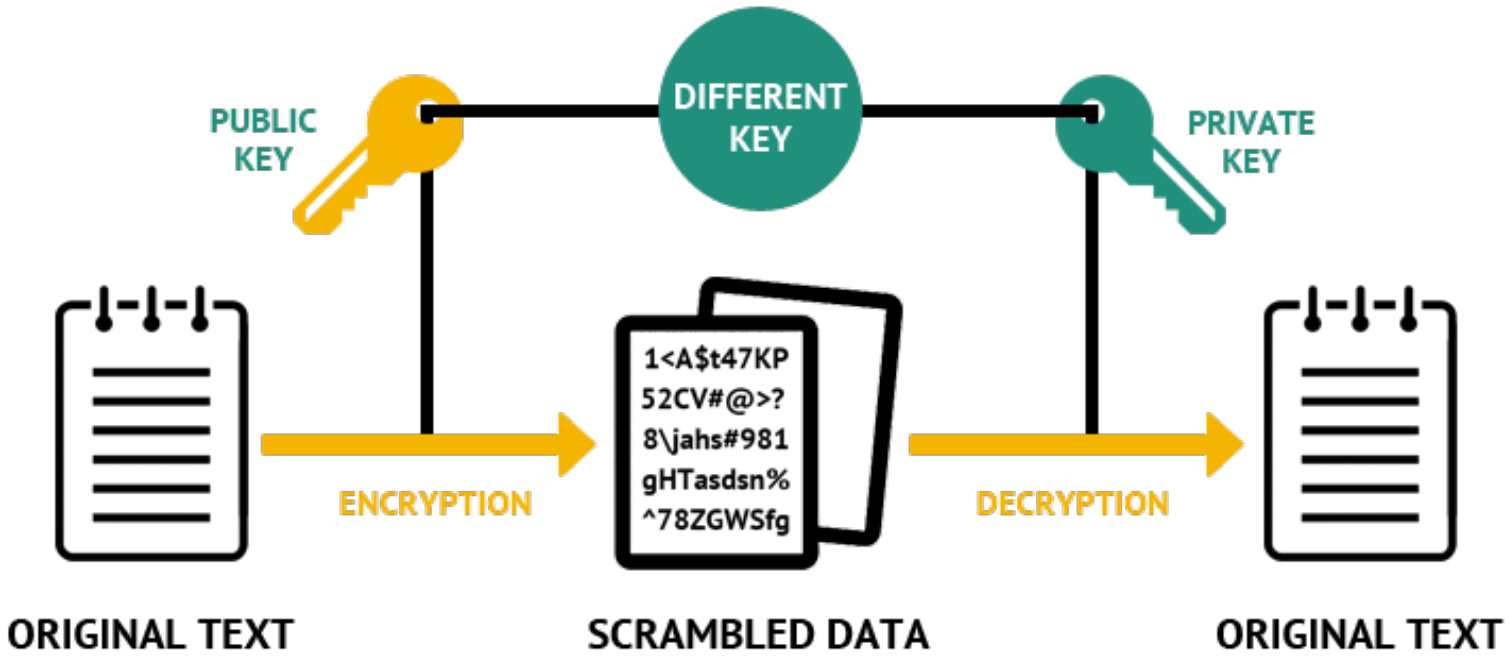
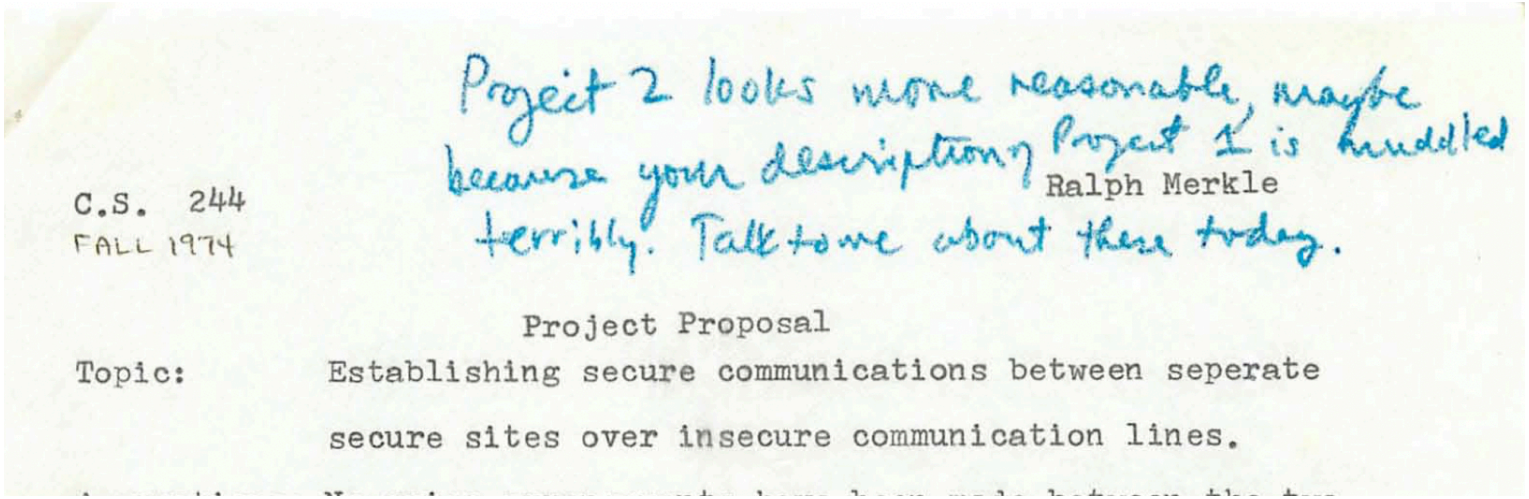


Figure 1: Understanding public-key cryptography (Image: SimpliLearn) [5]

Merkle Puzzles

- Merkle Puzzles was the first protocol to use the basis of public-key cryptography, and led to significant developments in the field.
- "It might seem intuitively obvious that if two people have never had opportunity to prearrange an encryption method, then they will be unable to communicate securely over an insecure channel. While this might seem intuitively obvious, I believe it is false. I believe that it is possible for two people to communicate securely without having made any prior arrangements that are not completely public." [7]

Merkle's First Draft Rejected



Project 2 looks more reasonable, maybe because your description of Project 1 is muddled terribly. Talk to me about these today.

Ralph Merkle

C.S. 244
FALL 1974

Project Proposal

Topic: Establishing secure communications between seperate secure sites over insecure communication lines.

Figure 2: Merkle's first draft was rejected in CS 244 at UC Berkeley [7]

Introduction to Merkle Puzzles

- Consider communication between two parties, Alice and Bob.

Introduction to Merkle Puzzles

- Consider communication between two parties, Alice and Bob.
- Alice creates N puzzles to send to anyone that wishes to communicate with her.

Introduction to Merkle Puzzles

- Consider communication between two parties, Alice and Bob.
- Alice creates N puzzles to send to anyone that wishes to communicate with her.
- Each puzzle is an encrypted message that takes a considerable amount of computational effort to solve (x), and Bob will be able to brute force the message to solve for the key. "Solving" each puzzle will allow the user to obtain an identifier n_i, and a secret symmetric key sk_i, where $1 \leq i \leq N$.

Merkle Puzzle Protocol

1. Alice creates N puzzles to send to anyone that wants to communicate with her. Solving every puzzle i will lead to a pair (n_i, sk_i). Each identifier and secret key is unique.
2. Alice sends all of the puzzles to Bob.
3. Using a random number generator, Bob selects a puzzle to brute force solve, and obtains (n_i, sk_i).
4. Bob encrypts a message p using sk_i, and sends it along with his identifier n_i.
5. Alice receives the message and n_i, and hence knows which secret symmetric key Bob is using.
6. Alice and Bob can now communicate over an authenticated channel.

Merkle Puzzle Protocol

Introducing, Alice and Bob!

Figure 3: Alice and Bob prior to beginning communication

Merkle Puzzle Protocol

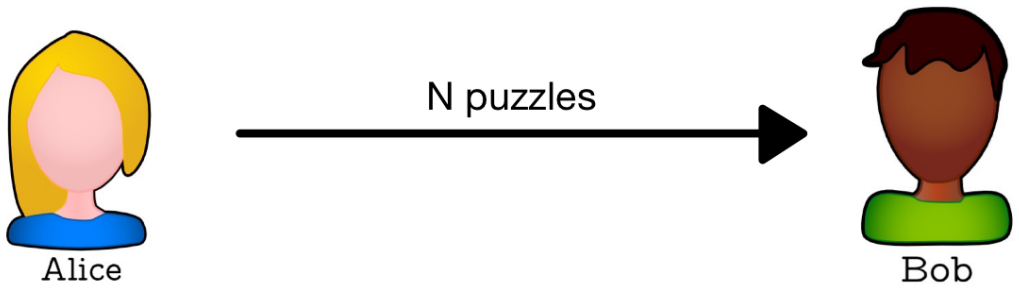


Figure 4: Alice sends Bob her N puzzles

Merkle Puzzle Protocol

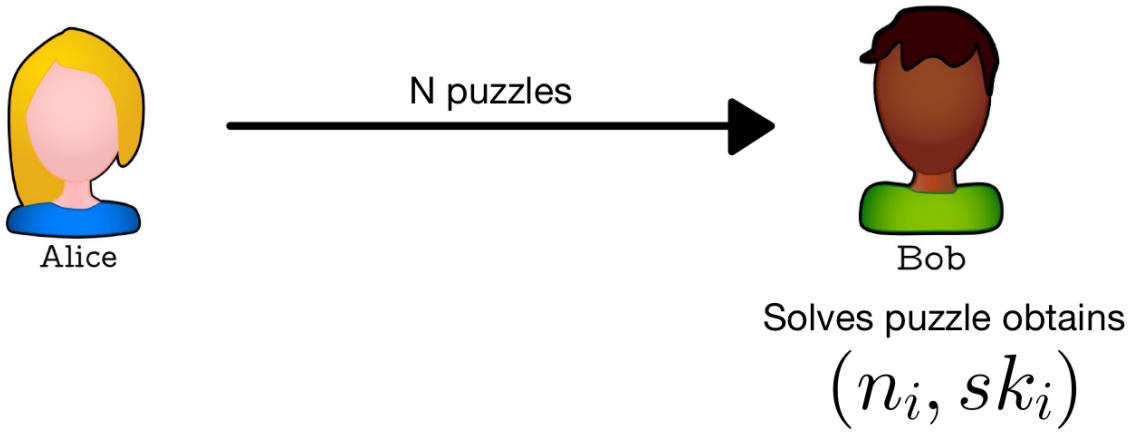


Figure 5: Bob randomly selects a puzzle and solves it

Merkle Puzzle Protocol

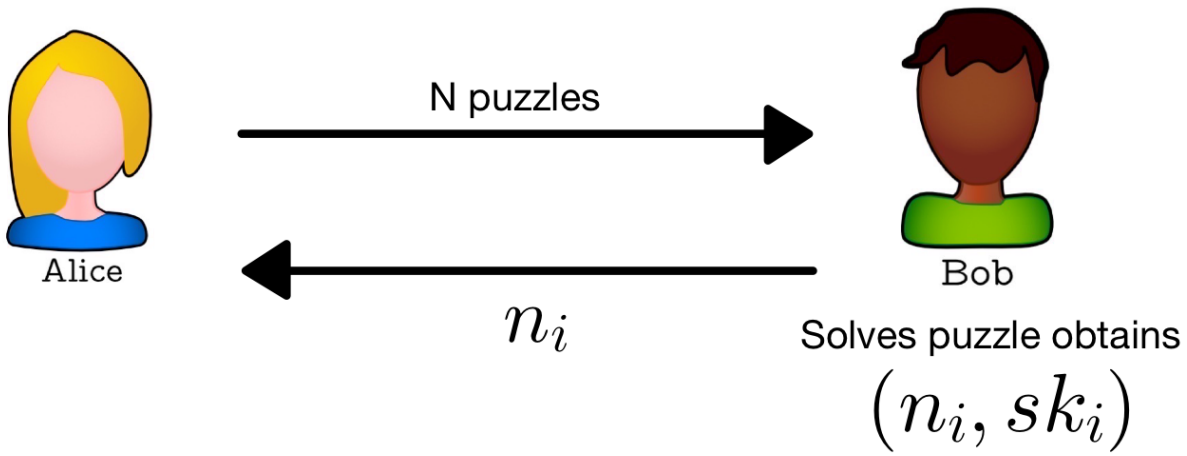


Figure 6: Bob sends back his identifier n_i to Alice

Merkle Puzzle Protocol

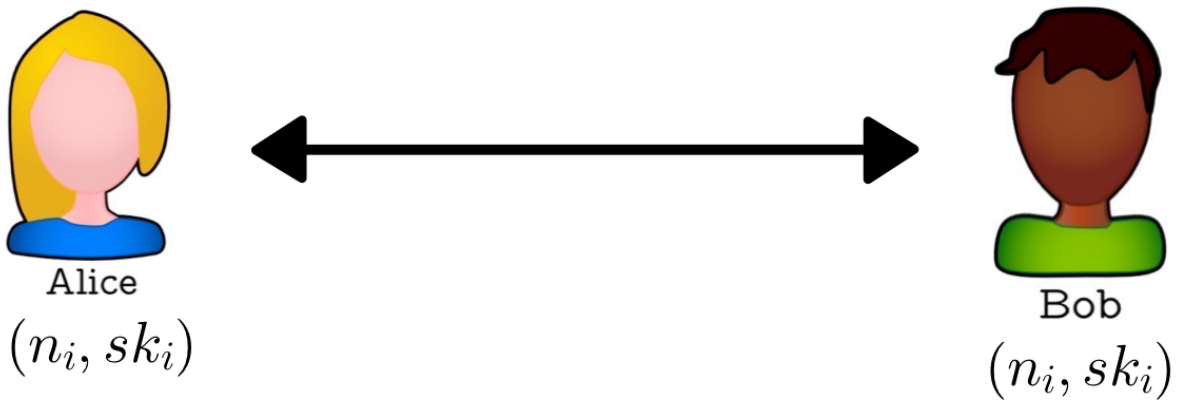


Figure 7: Alice and Bob now have a secret key to communicate

Merkle Puzzle Protocol

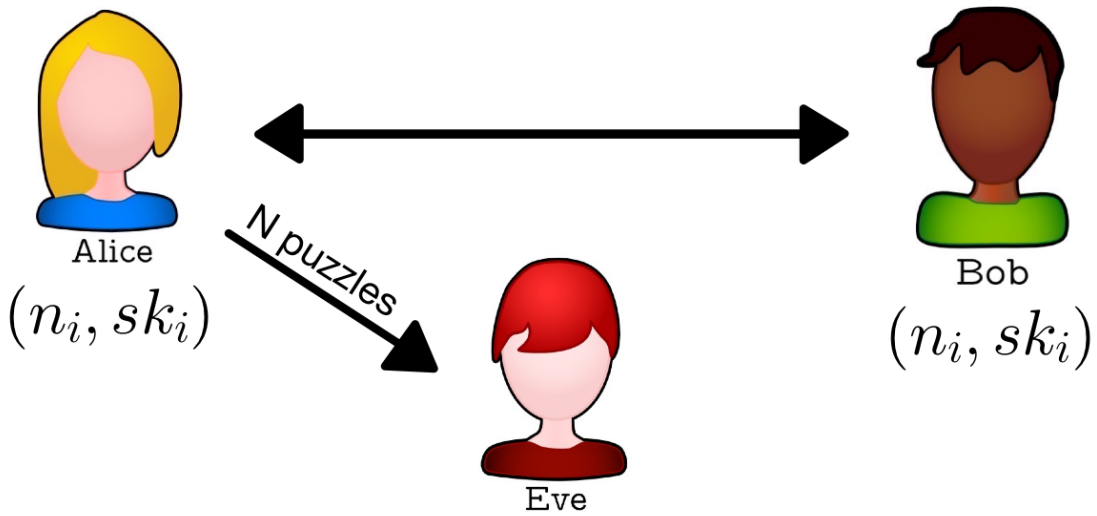


Figure 8: Eve is able to receive all N puzzles from Alice

Merkle Puzzle Protocol

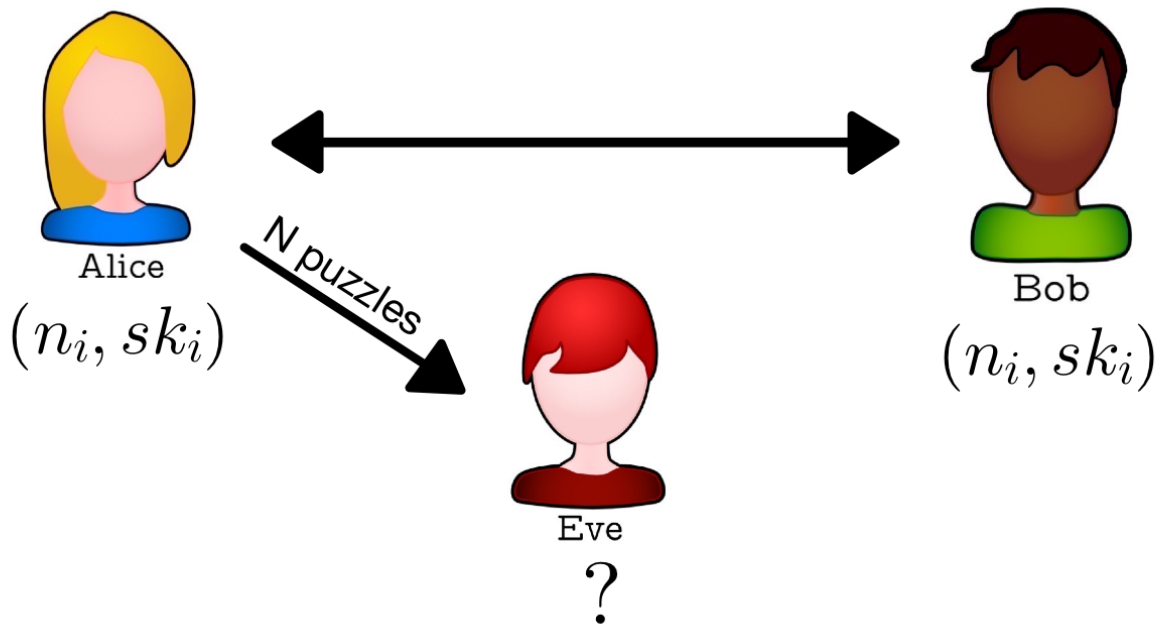


Figure 9: Eve has to solve all N puzzles to possibly figure out the secret key sk_i

Security of Merkle Puzzles in the Classical World

Theorem: Security of Merkle Puzzles

Merkle puzzles only require $O(n^2)$ queries from an adversary to an oracle to break the protocol.

- This bound comes from Barak and Mahmoody (2008) [1], who stated that any key agreement in the random oracle model with at most n queries to the oracle, can be broken by an adversary, who makes $O(n^2)$ queries to the oracle.

Security of Merkle Puzzles in the Classical World

Theorem: Security of Merkle Puzzles

Merkle puzzles only require $O(n^2)$ queries from an adversary to an oracle to break the protocol.

- This bound comes from Barak and Mahmoody (2008) [1], who stated that any key agreement in the random oracle model with at most n queries to the oracle, can be broken by an adversary, who makes $O(n^2)$ queries to the oracle.
- If Alice sends Bob N puzzles, each requiring m computational steps to solves, then while Bob can determine a secret key in $O(N + m)$ time. In order to determine Alice and Bob's secret key, Eve must complete $O(N * m)$ steps. Since $m << N$, this has an upper bound of $O(N^2)$.

Security in Classical Case

- Therefore, the Merkle puzzle protocol required quadratic effort by the adversary to break in the classical case. It does not guarantee that an eavesdropper will never be able to understand the messages between Bob and Alice, but this will a quadratic amount of effort to break.
- This is **extremely insecure**.

Merkle Puzzles Using Random Oracles

- The goal here is to reformulate the original protocol using a random oracle model.

Merkle Puzzles Using Random Oracles

- The goal here is to reformulate the original protocol using a random oracle model.
- An oracle (a black box) is meant to be public, and accessible by all parties. An oracle is defined to be a truly random function, based on a uniform distribution, that is well-defined.

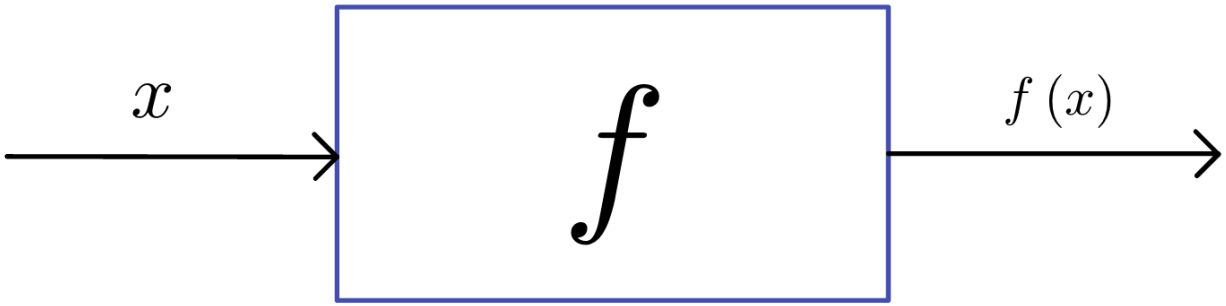
Merkle Puzzles Using Random Oracles

- The goal here is to reformulate the original protocol using a random oracle model.
- An oracle (a black box) is meant to be public, and accessible by all parties. An oracle is defined to be a truly random function, based on a uniform distribution, that is well-defined.
- For every unique query x in the input space, the oracle will determine a unique random output y, and will output y every time x is queried.

Merkle Puzzles Using Random Oracles

- The goal here is to reformulate the original protocol using a random oracle model.
- An oracle (a black box) is meant to be public, and accessible by all parties. An oracle is defined to be a truly random function, based on a uniform distribution, that is well-defined.
- For every unique query x in the input space, the oracle will determine a unique random output y, and will output y every time x is queried.
- These do not exist in the real world!

Random Oracle Model



x	$f(x)$
x_1	y_1
x_2	y_2
$\vdots$	$\vdots$
x_n	y_n

Merkle Puzzles Using Random Oracles

- We set n as the security parameter, and define $H : [n] \times [n] \mapsto \{0,1\}^n \times \{0,1\}^m$ to be an oracle.

Merkle Puzzles Using Random Oracles

- We set n as the security parameter, and define $H : [n] \times [n] \mapsto \{0,1\}^n \times \{0,1\}^m$ to be an oracle.
- Let $x_i \in \{0,1\}^m$ be the secret symmetric key of the i^{th} puzzle, where $a_1, \ldots, a_n$ are the puzzles sent from Alice to Bob.

Merkle Puzzles Using Random Oracles

- We set n as the security parameter, and define $H : [n] \times [n] \mapsto \{0,1\}^n \times \{0,1\}^m$ to be an oracle.
- Let $x_i \in \{0,1\}^m$ be the secret symmetric key of the i^{th} puzzle, where $a_1, \ldots, a_n$ are the puzzles sent from Alice to Bob.
- We randomly select $k \leftarrow [n]$, and set $a_i = (H_1(i,k), H_2(i,k) \oplus x_i)$. In this case, we have that H_1 acts on the first n bits of the output of H, and H_2 acts on the last m bits.

Merkle Puzzles Using Random Oracles

- We set n as the security parameter, and define $H : [n] \times [n] \mapsto \{0,1\}^n \times \{0,1\}^m$ to be an oracle.
- Let $x_i \in \{0,1\}^m$ be the secret symmetric key of the i^{th} puzzle, where $a_1, \ldots, a_n$ are the puzzles sent from Alice to Bob.
- We randomly select $k \leftarrow [n]$, and set $a_i = (H_1(i,k), H_2(i,k) \oplus x_i)$. In this case, we have that H_1 acts on the first n bits of the output of H, and H_2 acts on the last m bits.
- Let $P_1 = (h_1^1, h_2^1), \ldots, P_n = (h_1^n, h_2^n)$. Bob will randomly pick a puzzle P_j and will query the oracle on all $k \in [n]$ such that $H(j,k) = (h_1^j, h_2)$.

Walking Through Random Oracle Model

Figure 11: Alice creates her puzzles

Walking Through Random Oracle Model

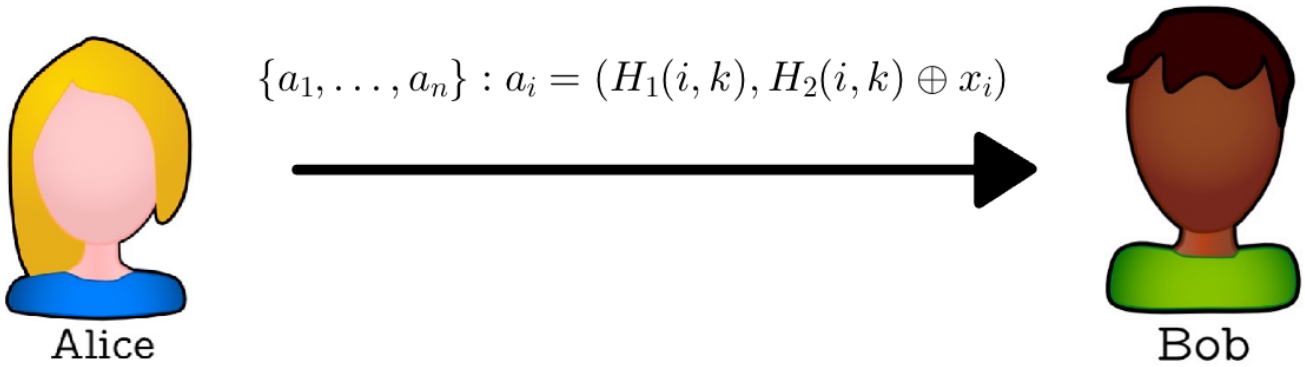


Figure 12: Alice sends her puzzles to Bob in an authenticated channel

Walking Through Random Oracle Model

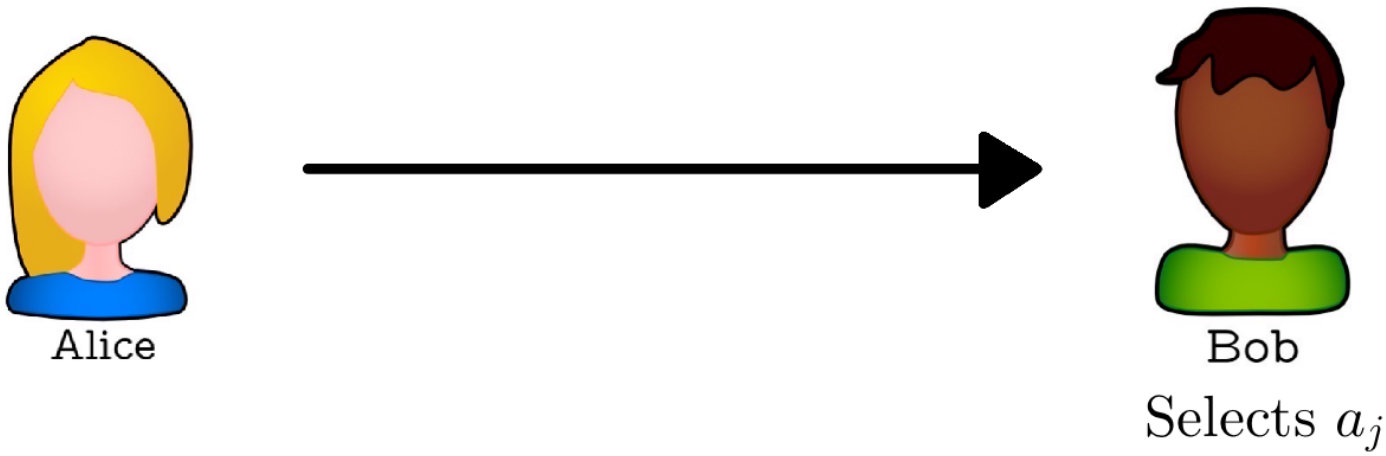
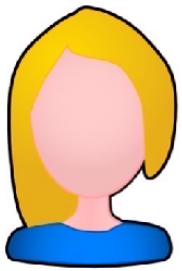


Figure 13: Bob selects a random puzzle

Walking Through Random Oracle Model



Alice

Bob

For all $k \in [n]$, query $H(j,k)$
until $H(j,k) = (h_1^j, h_2)$

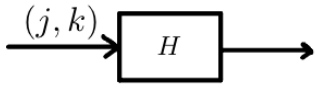


Figure 14: Bob begins to query H

Walking Through Random Oracle Model

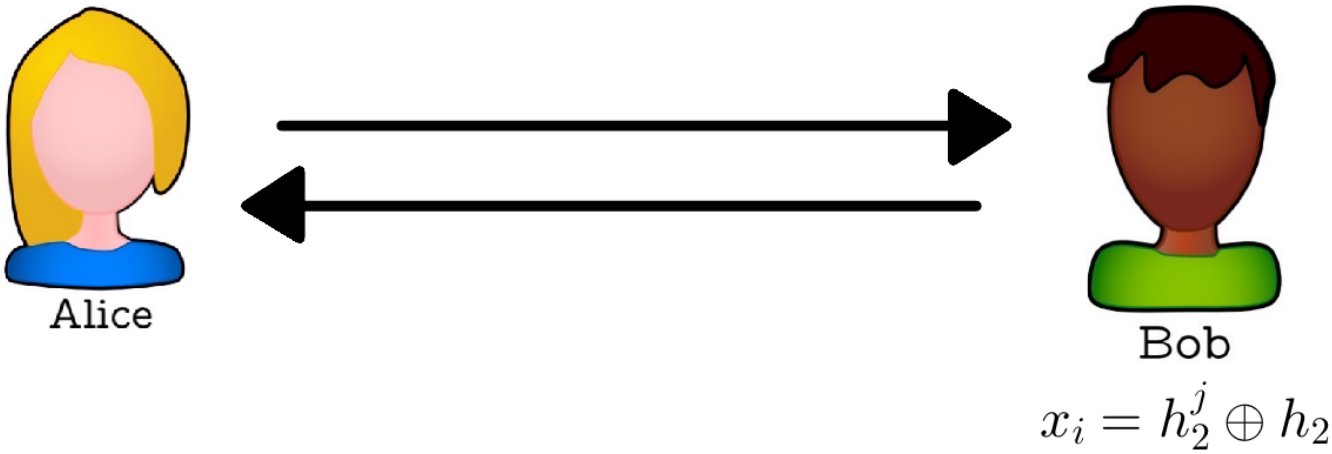


Figure 15: Bob determines the key x_i and is now able to communicate with Alice

Walking Through Random Oracle Model

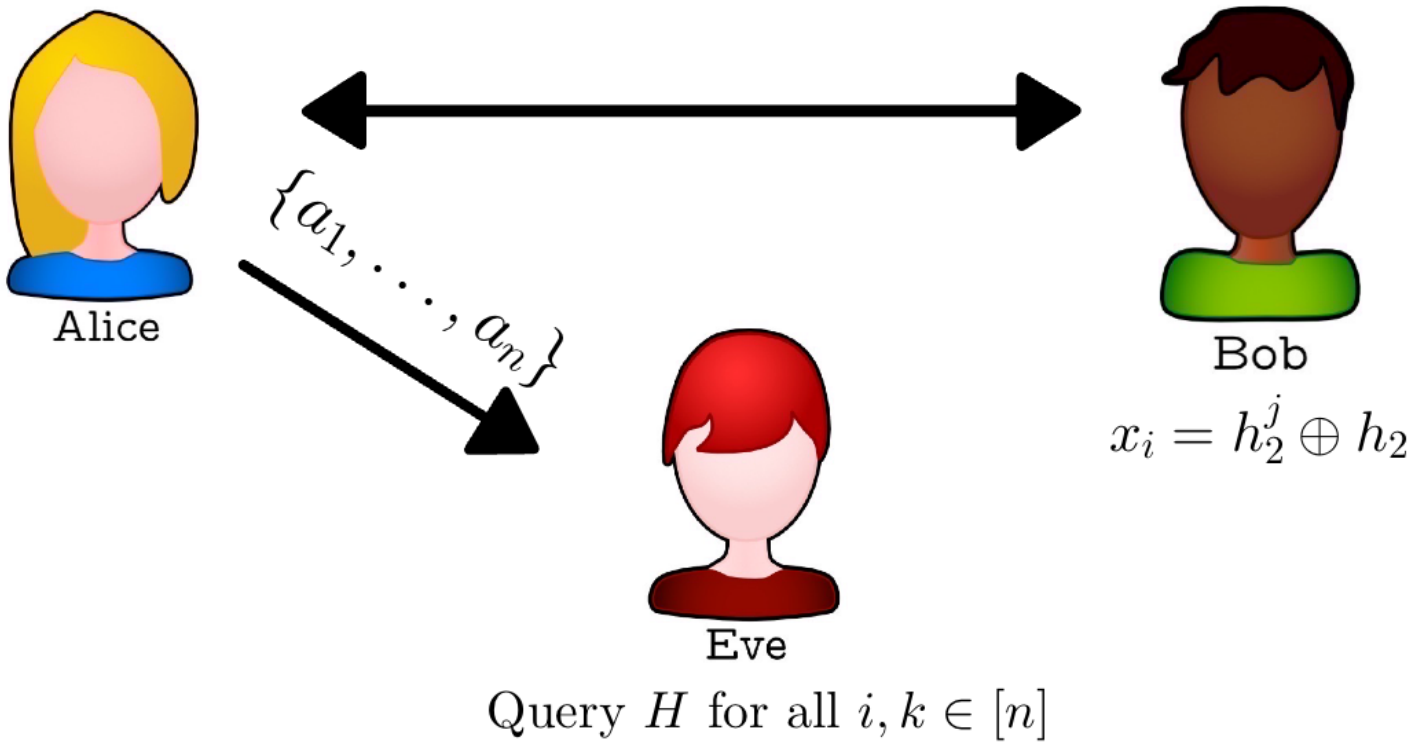


Figure 16: Eve has to make $O(N^2)$ queries to the oracle

Merkle Puzzles Using Random Oracles

- Once Bob has found such k, he will solve for $x_i = h_2 \oplus h_2^j$. Alice and Bob have now established a secret symmetric key.

Merkle Puzzles Using Random Oracles

- Once Bob has found such k, he will solve for $x_i = h_2 \oplus h_2^j$. Alice and Bob have now established a secret symmetric key.
- Given that $k \in [n]$, there are most n queries made by Bob to find such k such that $H(j, k) = (h_1^j, h_2)$. Therefore, this follows the necessary condition to satisfy a key agreement in at most n queries to an oracle.

Merkle Puzzles Using Random Oracles

- Once Bob has found such k, he will solve for $x_i = h_2 \oplus h_2^j$. Alice and Bob have now established a secret symmetric key.
- Given that $k \in [n]$, there are most n queries made by Bob to find such k such that $H(j, k) = (h_1^j, h_2)$. Therefore, this follows the necessary condition to satisfy a key agreement in at most n queries to an oracle.
- Following from this construction, it is possible to use the proof by Barak and Mahmoody to prove the optimality of Merkle puzzles.

Quantum Attacks on Merkle Puzzles

- The significant computational effort required to break the Merkle puzzle protocol does not hold in the quantum case.
- A generalization of Grover's algorithm by Boyer, Brassard, Høyer and Tapp (1996) [2] named the BBHT algorithm and Grover's algorithm is able to significantly reduce the time required to break a Merkle puzzle protocol.

Quantum Attack Using Grover's Algorithm

- Therefore, in $O(\sqrt{N})$ queries, we are able to achieve the index of the puzzle with the identifier n_i.

Quantum Attack Using Grover's Algorithm

- Therefore, in $O(\sqrt{N})$ queries, we are able to achieve the index of the puzzle with the identifier n_i.
- This renders Merkle puzzles significantly less secure in the Quantum world.

Quantum Attack Using Grover's Algorithm

- Therefore, in $O(\sqrt{N})$ queries, we are able to achieve the index of the puzzle with the identifier n_i.
- This renders Merkle puzzles significantly less secure in the Quantum world.
- There is a modification to Merkle puzzles for the quantum world, however its best case requires the adversary makes only $O(N^{13/12})$ queries to the oracle.

Disadvantages to Merkle Puzzles

- Overall, the security being offered even in the classical case and the quantum modification of the Merkle puzzle protocol is still very low compared to other cryptographic protocols.
- While it is possible to improve the ratio between the legitimate effort and the effort required by the adversary, there do exist better protocols for privacy and security.

[1] Boaz Barak and Mohammad Mahmoody. "Merkle's Key Agreement Protocol is Optimal: An $O(n^2)$ Attack on any Key Agreement from Random Oracles". In: *arXiv preprint arXiv:0801.3669* (2008).

[2] Michel Boyer et al. "Tight bounds on quantum search". In: *Proceedings of the Workshop on Physics of Computation: PhysComp' 96*. 1996, pp. 36–43.

[3] Gilles Brassard et al. "Merkle puzzles in a quantum world". In: *Annual Cryptology Conference*. Springer. 2011, pp. 391–410.

[4] Bartholomew Furrow. "A panoply of quantum algorithms". In: *arXiv preprint quant-ph/0606127* (2006).

[5] Baivab Kumar Jena. *Digital Signature Algorithm (DSA) in Cryptography: How It Works and Advantages*. `https://www.simplilearn.com/tutorials/cryptography-tutorial/digital-signature-algorithm`. 2019.

[6] Kearon. *Alice And Bob Area*. https://www.cleanpng.com/png-clip-art-scalable-vector-graphics-alice-and-bob-po-6428595/.

[7] Ralph Merkle. *Project Proposal 2 CS 244*. http://www.ralphmerkle.com/1974/SecondCS244projectProposal.pdf. 1974.

Thanks!