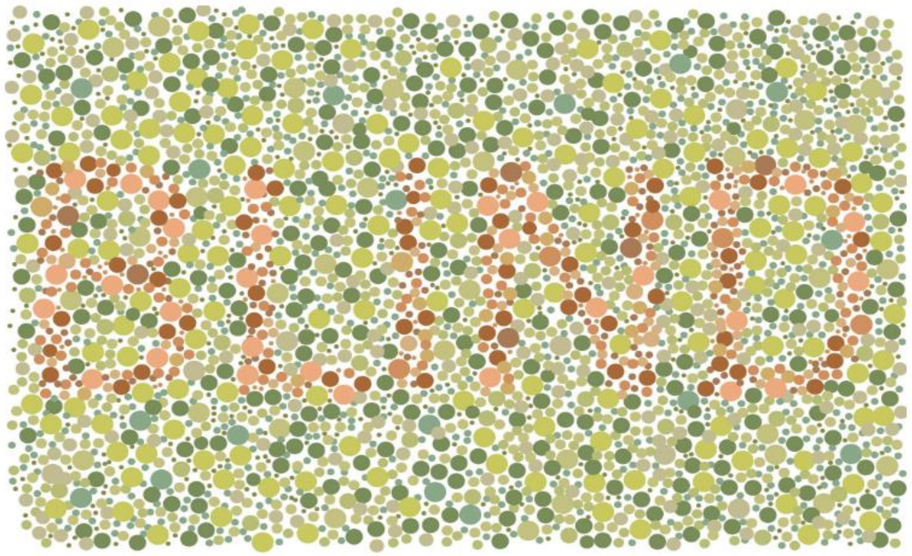
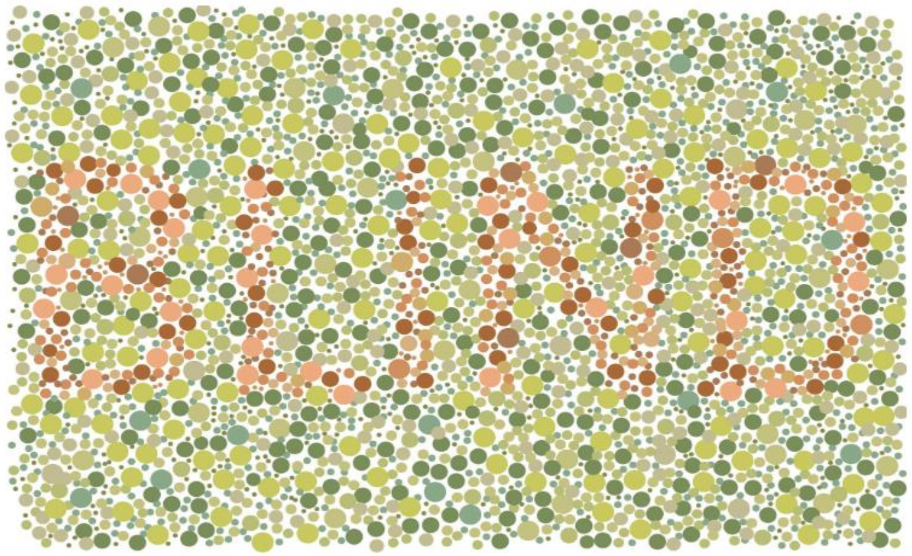
Some Knowledge about Zero Knowledge

June 25, 2019



DC4420

Faye



Introduction

Name: Faye

Academic Current: 2nd Year PhD student ISG Royal Holloway

Academic Background: BSc Hons Mathematics, MSc Mathematics Cryptography and Communications

Industry Experience: Various Security Roles in Financial Services, Aviation, Commodities, and Central Government

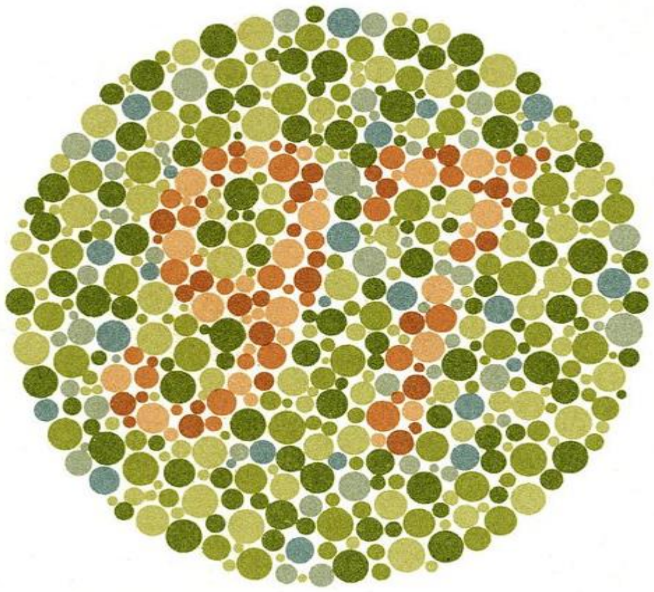
DC4420 Experience: October 2017 Presented an NP-Hard Proof-of-Useful Work for Cryptocurrency Mining based on the Travelling Salesman Problem
(now peer reviewed and published
https://dl.acm.org/citation.cfm?id=3211943)

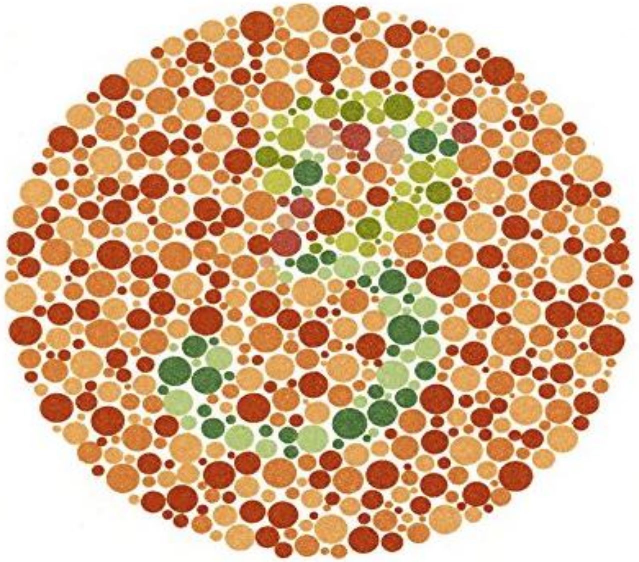
Latest Update: June 2019, ACM CCS `19 Submission accepted! '*You Shall Not Join: A Measurement Study of Cryptocurrency Peer-to-Peer Bootstrapping Techniques*'. Publication Forthcoming.

Audience Questions

Any Mathematicians?

Anyone COLOUR BLIND?





Presentation Outline

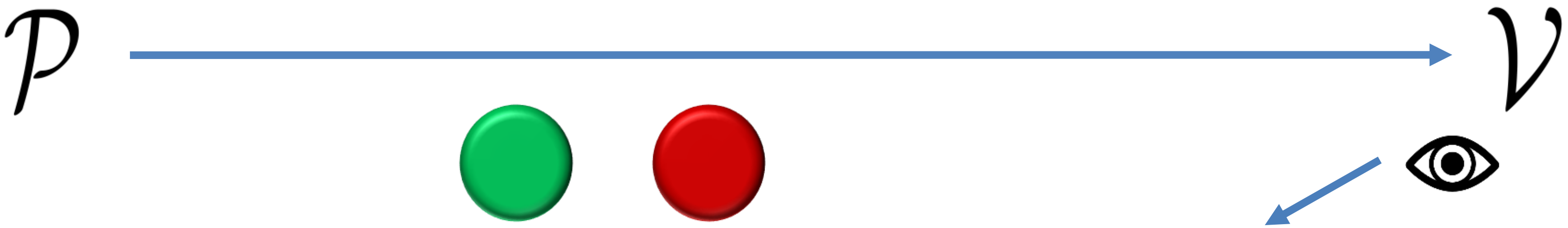
1) Interactive Zero Knowledge Proofs: Colour Blind Gatekeeper

2) Introduction to Quadratic Residues

3) Interactive Zero Knowledge Proofs: Quadratic Residuosity

4) My Research, Perfect Squares over the Integers

Interactive Zero Knowledge Proof: The Colour Blind Gatekeeper

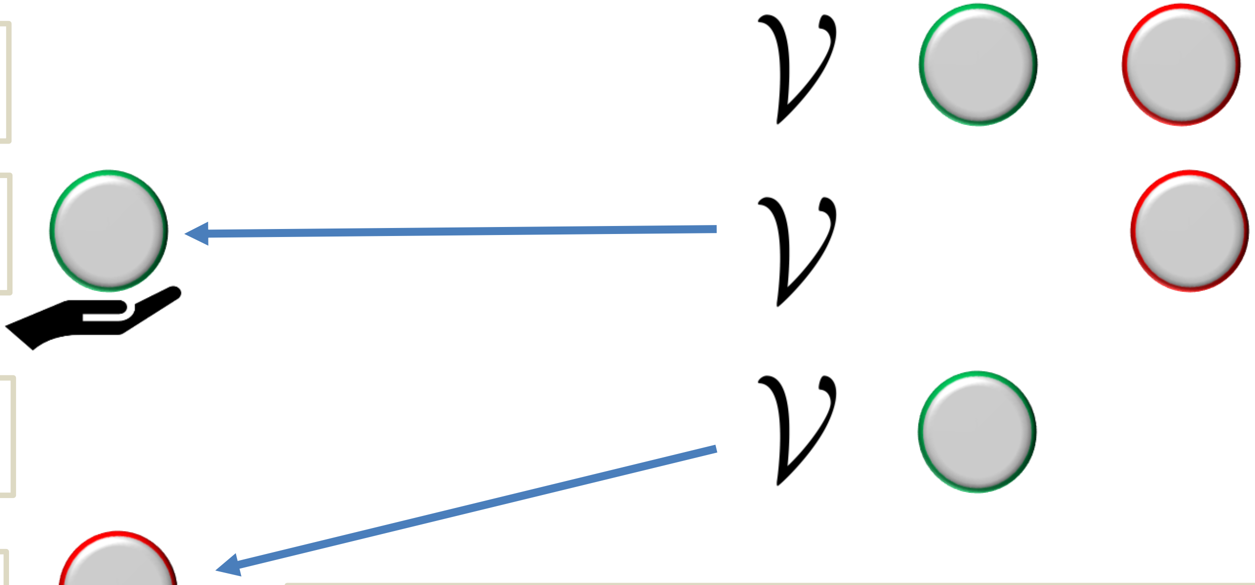


1) You give a green ball and a red ball to a colour blind gatekeeper and claim you have a special power

2) The colour blind gatekeeper simply sees 2 grey balls

3) To prove your special power you ask $\mathcal{V}$ to put the 2 grey balls behind her back

4) You then ask $\mathcal{V}$ to select 1 of the balls and put it in your hand. You can see colour, so you see the green ball



5) You ask $\mathcal{V}$ to take the ball behind her back again and to keep note of which ball she gave you.

6) Now ask $\mathcal{V}$ with equal probability, to either return the original ball she showed to you or switch balls.

7) $\mathcal{V}$ asks 'Is this the original ball I showed you?

8) You answer: 'No, it is the other ball', Probability of guessing right $\frac{1}{2^1} = \frac{1}{2}$

Interactive Zero Knowledge Proof: The Colour Blind Gatekeeper

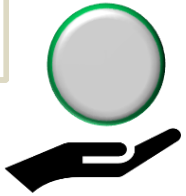
$\mathcal{P}$ → $\mathcal{V}$

9) Again ask $\mathcal{V}$ with equal probability, to either return the same ball to you or switch balls.

$\mathcal{V}$

10) $\mathcal{V}$ asks 'Is this the original ball I showed you?

11) You answer: 'Yes', Probability of guessing right 2 times $\frac{1}{2^2} = \frac{1}{4}$



$\mathcal{V}$

12) $\mathcal{V}$ asks 'Is this the original ball I showed you?

13) You answer: 'Yes', Probability of guessing right 3 times $\frac{1}{2^3} = \frac{1}{8}$

Repeat this challenge n times, and the probability of guessing right n times is $\frac{1}{2^n}$

IE: If you repeat this n = 40 times, the probability of guessing right every time is approximately 1 in a trillion.

Why is this Zero Knowledge

Complete: If $\mathcal{P}$ provides a true statement i.e. the ball was the original or it was switched, then an honest $\mathcal{V}$ (one who honestly notes whether the ball was the original or switched) will be convinced that $\mathcal{P}$ provided a true statement.

Sound: If a *cheating* $\mathcal{P}$ shows up who cannot see colour, and tries to repeat the same challenge to convince $\mathcal{V}$ over multiple iterations that the ball was the original or switched, he will only succeed with negligible probability.

Zero Knowledge: At the end of each interaction $\mathcal{V}$ only learns whether or not $\mathcal{P}$ could tell if she switched the ball from the original or not. What $\mathcal{V}$ does not learn is which ball is green or which ball is red, she still only sees two grey balls.

i.e. $\mathcal{V}$ does not gain the secret power of being able to see COLOUR at the end of the proof

How do I turn green and red balls into a mathematically rigorous cryptographically secure system capable of Interactive Zero Knowledge Proofs?

One method is to use Quadratic Residues.

What is a Quadratic Residue?

Linear Congruence Relations

Let $y, r \in \mathbb{Z}$, and let p be an odd prime.

Then we say 'y is congruent to r mod p' and denote it as follows:

$$y \equiv r \mod p$$

$$\text{e.g. set modulus } p = 7$$

$$0 \equiv 7 \equiv 399 \mod 7$$
$$1 \equiv 8 \equiv 386 \mod 7$$
$$2 \equiv 9 \equiv 457 \mod 7$$
$$3 \equiv 10 \equiv 318 \mod 7$$
$$4 \equiv 11 \equiv 613 \mod 7$$
$$5 \equiv 12 \equiv 460 \mod 7$$
$$6 \equiv 13 \equiv 272 \mod 7$$

Quadratic Congruence Relations Modulo a Prime

Let $y, r \in \mathbb{Z}$, and let p be an odd prime.

Then we say y^2 is congruent to r mod p and denote it as follows:

$$y^2 \equiv r \mod p$$

Quadratic residues are for modulus $p = 7$:

$$0^2 \equiv 0 \mod 7$$
$$1^2 \equiv \underline{1} \mod 7$$
$$2^2 \equiv \underline{4} \mod 7$$
$$3^2 \equiv 9 \equiv \underline{2} \mod 7$$
$$4^2 \equiv 16 \equiv \underline{2} \mod 7$$
$$5^2 \equiv 25 \equiv \underline{4} \mod 7$$
$$6^2 \equiv 36 \equiv \underline{1} \mod 7$$

$$\{\underline{1}, \underline{2}, \underline{4}\} = \mathcal{QR}_7 =$$

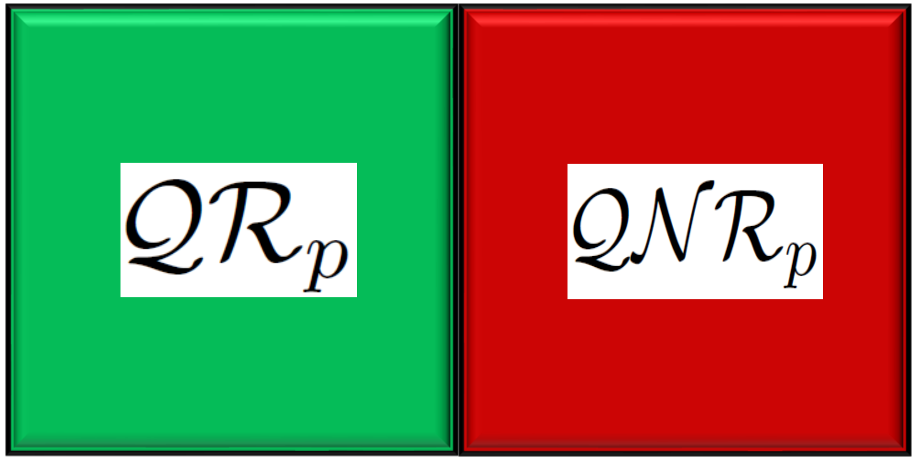
$$\{3, 5, 6\} = \mathcal{QNR}_7 =$$

Quadratic Residues Modulo a Prime

Number of Quadratic Residues and Quadratic Non Residues

$$|\mathcal{QR}_p| = \frac{|\mathbb{Z}_p^*|}{2} = \frac{p-1}{2} = |\quad|$$

$$|\mathcal{QNR}_p| = \frac{|\mathbb{Z}_p^*|}{2} = \frac{p-1}{2} = |\quad|$$



Quadratic Residuosity and the Jacobi Symbol

$$\mathcal{J}_p(r) = \begin{cases} +1, \text{if} r \in \mathcal{QR}_p \\ -1, \text{if} r \in \mathcal{QNR}_p \end{cases}$$

Properties of the Jacobi Symbol

The Jacobi Symbol is a completely multiplicative function.

A	B	A **XOR** B
0	0	0
0	1	1
1	0	1
1	1	0

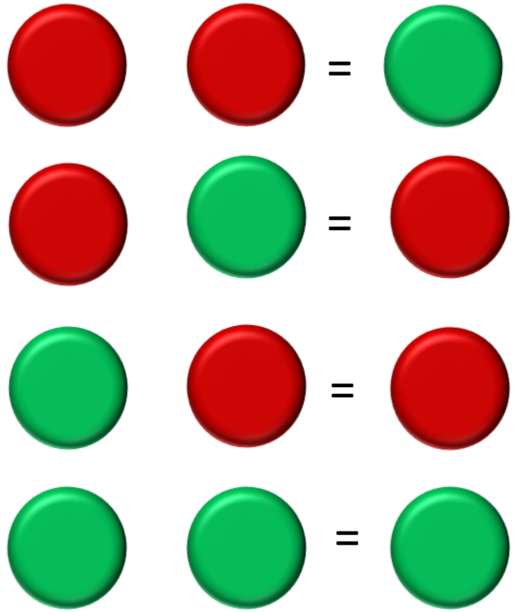
Let $r_1, r_2 \in \mathcal{QNR}_p$
and $r_3, r_4 \in \mathcal{QR}_p$

$$(\mathcal{J}_p(r_1))(\mathcal{J}_p(r_2)) = \mathcal{J}_p(r_5) \in \mathcal{QR}_p \text{ i.e. } (-1)(-1) = +1$$

$$(\mathcal{J}_p(r_1))(\mathcal{J}_p(r_3)) = \mathcal{J}_p(r_6) \in \mathcal{QNR}_p \text{ i.e. } (-1)(+1) = -1$$

$$(\mathcal{J}_p(r_3))(\mathcal{J}_p(r_1)) = \mathcal{J}_p(r_7) \in \mathcal{QNR}_p \text{ i.e. } (+1)(-1) = -1$$

$$(\mathcal{J}_p(r_3))(\mathcal{J}_p(r_4)) = \mathcal{J}_p(r_8) \in \mathcal{QR}_p \text{ i.e. } (+1)(+1) = +1$$



cryptosystem has a homomorphic property of an XOR

Quadratic Residues Modulo a Composite

Quadratic Residuosity and the Jacobi Symbol

Let $N = pq$, where p and q are distinct odd primes.

$$\mathcal{J}_N(r) = \begin{cases} +1, \text{if } r \in \mathcal{QR}_N^{+1} \vee r \in \mathcal{QNR}_N^{+1} \\ -1, \text{if } r \in \mathcal{QNR}_N^{-1} \end{cases}$$

Quadratic Residues Modulo a Composite

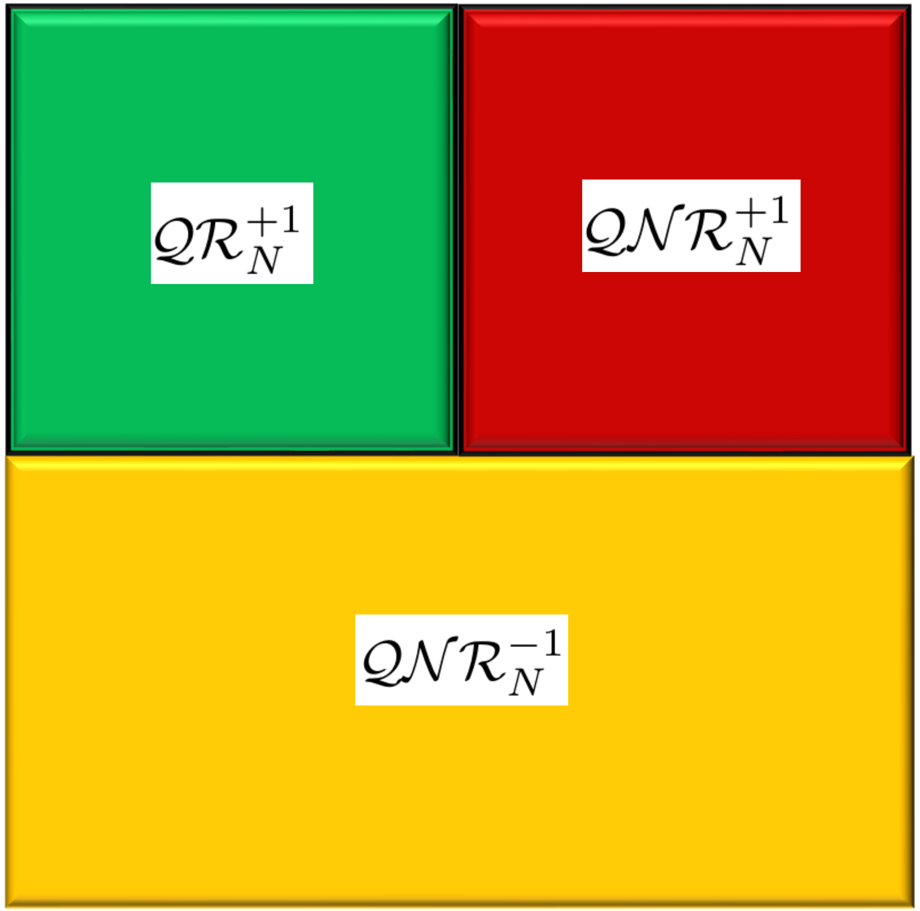
Number of Quadratic Residues and Quadratic Non Residues

$$|\mathbb{Z}_N^*| = \phi(N) = (p-1)(q-1), \text{ Euler's Totient Function}$$

$$|\mathcal{QR}_N^{+1}| = \frac{|\mathbb{Z}_N^*|}{2} = \frac{\phi(N)}{4} =$$

$$|\mathcal{QNR}_N^{+1}| = \frac{|\mathbb{Z}_N^*|}{2} = \frac{\phi(N)}{4} =$$

$$|\mathcal{QNR}_N^{-1}| = \frac{|\mathbb{Z}_N^*|}{2} = \frac{\phi(N)}{2} =$$



How do you Calculate the Jacobi Symbol Modulo p?

1) Brute Force Enumeration (Small p only)

$$1^2, 2^2, \ldots, (p-1)^2 \mod p$$

2) Use Euler's Criterion (runs in polynomial time, $\forall\, p$)

If $r^{\frac{p-1}{2}} \equiv 1 \mod p$

Output: $\mathcal{J}_p(r) = +1$ i.e. $r \in \mathcal{QR}_p$

Else

Output : $\mathcal{J}_p(r) = -1$ i.e.$r \in \mathcal{QNR}_p$

How do you Determine Quadratic Residuosity Modulo N = pq?

Use Euler's Criterion (runs in polynomial time, $\forall\, p, q$)

If $r^{\frac{p-1}{2}} \equiv 1 \mod p$ AND $r^{\frac{q-1}{2}} \equiv 1 \mod q$

Output: $r \in \mathcal{QR}_N$

Else

Output : $r \in \mathcal{QNR}_N^{+1}$

This result relies on The Chinese Remainder Theorem Isomorphism

$$\mathbb{Z}_N^* \simeq \mathbb{Z}_p^* \times \mathbb{Z}_q^*$$

- The Jacobi symbol of a number can be computed in polynomial time for a composite modulus N.
- Recall $\mathcal{J}_N(r) = +1$ can represent both $\mathcal{QR}_N$ and $\mathcal{QNR}_N^{+1}$ with equal probability.
- This is the crux of the Quadratic Residuosity Problem.

Creating a Zero Knowledge Proof Cryptosystem based on the Quadratic Residuosity Problem

Now we have the elements required for a ZKP cryptosystem!

Proceed as follows:
$(pk, sk) \leftarrow \mathsf{Gen}(1^\kappa)$

- Generate 2 κ-bit primes p and q.
- Flip a fair coin κ-times, then run the AKS primality test or similar.
- Calculate the modulus $N = pq$.

Prime Number Theorem tells us that the distribution of primes is:

$$\pi(x) \sim \frac{x}{\ln(x)}$$

i.e. for any number $\leq x$ the probability that it is prime is $\approx \frac{1}{\ln(x)}$

Interactive ZKP: The Quadratic Residuosity Blind Gatekeeper

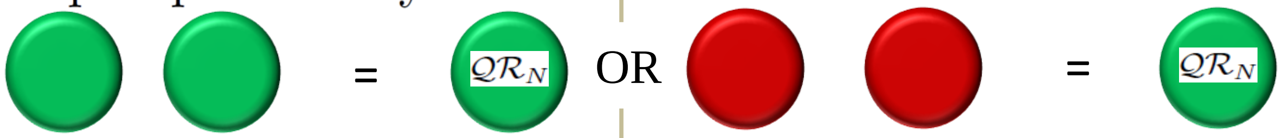
$\mathcal{P}$ $\longrightarrow$ $\mathcal{V}$

1) Give $pk = (N, \mathcal{QNR}_N^{+})$ to $\mathcal{V}$ and claim you have a special power. Knowing p and q is your special power.

2) $pk = (N, \mathcal{QNR}_N^{+})$

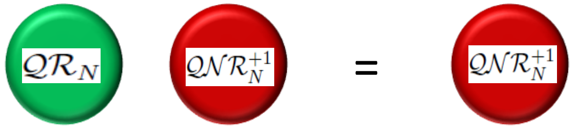
3) To prove your special power ask $\mathcal{V}$ to do the following:
$y \leftarrow \mathbb{Z}_N^*$ i.e. randomly select y.

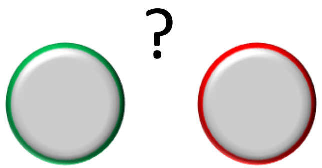
Then do one of two things with equal probability:
i) $(y)(y) \equiv y^2 \equiv r \mod N$



OR

ii)$(y^2)(\mathcal{QNR}_N^{+1}) \equiv r \mod N$



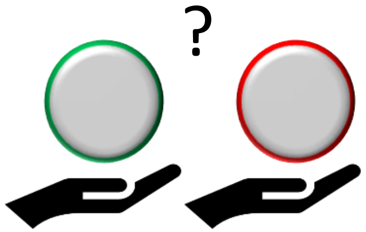


4) $\mathcal{V}$ then gives you an output r, and asks you: '*Did I give you a $\mathcal{QR}_N$ OR a $\mathcal{QNR}_N^{+1}$?*'

Interactive ZKP: The Quadratic Residuosity Blind Gatekeeper

$\mathcal{P} \longrightarrow \mathcal{V}$

5) Because you know p and q you run Euler's Criterion and determine the Quadratic Residuosity of r and tell $\mathcal{V}$.



6) $\mathcal{V}$ then repeats this test n times as necessary.

7) After n trials, the chance you guessed Quadratic Residuosity correctly for all trials is $\frac{1}{2^n}$.

Why is this Zero Knowledge

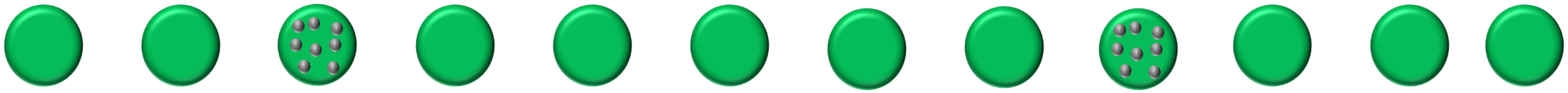
Complete If $\mathcal{P}$ provides a true statement i.e. that r is either a $\mathcal{QR}_N$ or a $\mathcal{QNR}_N^{+1}$, then an honest $\mathcal{V}$ (one who honestly notes which option was chosen) will be convinced that $\mathcal{P}$ provided a true statement.

Sound If a *cheating* $\mathcal{P}$ shows up, who does not know p and q, tries to repeat the same challenge to convince $\mathcal{V}$ over multiple iterations that he knows the quadratic residuosity of r, he will only succeed with negligible probability.

Zero Knowledge At the end of each interaction $\mathcal{V}$ only learns whether or not $\mathcal{P}$ could tell if she chose option i) or option ii). What $\mathcal{V}$ does not learn is what the value of p and q are.

i.e. $\mathcal{V}$ does not gain the secret power of being able to determine the Quadratic Residuosity of any arbitrary r (providing it was not one she chose as a test before) at the end of the proof.

My Research: Green Spotty Balls aka Perfect Squares over the Integers

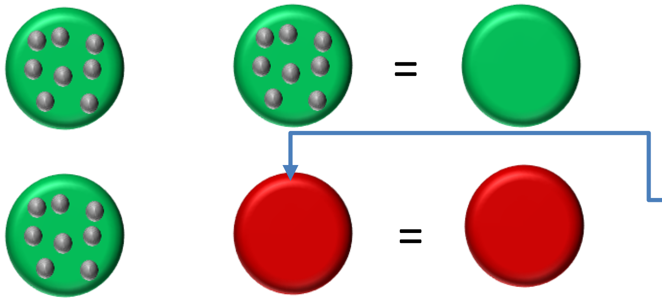


Some of the green balls have spots on them, which are visible to everyone.

These green spotty balls are the Perfect Squares over the Integers.

The Perfect Squares over the Integers are $\mathcal{QR}_N$ for any modulus.

Exploit the multiplicative property of the Jacobi symbol to learn another $\mathcal{QR}_N$ or $\mathcal{QNR}_N^{+1}$



$\boxed{pk = (N, \mathcal{QNR}_N^{+})}$

What are The Perfect Squares over the Integers

There are exactly $\lfloor \sqrt{N} \rfloor$ perfect squares $\leq N$.

$$\mathcal{PS}_N = \{1^2, 2^2, \ldots, \lfloor \sqrt{N} \rfloor^2\}$$

These are $\mathcal{QR}_N \; \forall \; N$ - excluding coprime elements of N

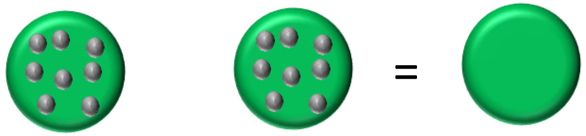
Let $N = (5)(7) = 35$, where $\lfloor \sqrt{35} \rfloor = 5$

$$\mathcal{PS}_{35} = \{1^2, 2^2, 3^2, 4^2\} = \{1, 4, 9, 16\}$$

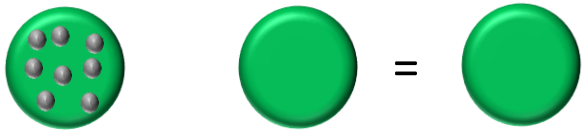
Exclude $\{5^2\} = \{25\}$ because $\gcd(25, 35) \neq 1$

These are all $\mathcal{QR}_{35}$. The other $\mathcal{QR}_{35}$ are $\{11, 29\}$.

$$(9)(9) \equiv 81 \equiv 11 \mod 35$$



$$(9)(11) \equiv 99 \equiv 29 \mod 35$$



Brute Force Enumeration and IND-CPA

Goal to use The Perfect Squares over the Integers to *do better* than Brute Force Enumeration.

Look at the IND-CPA (Indistinguishability under Chosen-Plaintext Attack) of the cryptosystem i.e. consider the *negligible* advantage

IZKP based on first IND-CPA *semantically* secure cryptosystem - Goldwasser-Micali

Not a heavily utilized PKC because ciphertext expansion is $\log_2 N$

Perfect Squares over the Integers vs. GNFS (General Number Field Sieve)

$\mathcal{PS} \in \mathbb{Z}$

Distinguishability of Ciphertexts: $\mathcal{A}$ able to distinguish between two chosen plaintexts with non-negligible probability.

Partial Break: $\mathcal{A}$ can determine particular information about the plaintext given ciphertext with non-negligible probability.

GNFS

Total Break: $\mathcal{A}$ determines sk and can decrypt any ciphertext

Demo (if time)

Questions ?

PQC refer to *The Impact of Quantum Computing on Present Cryptography* – Mavroeidis et al, 2018

Thank You

conqueringgeneral@yandex.com